RAMCAP Plus℠

Risk Analysis and Management for Critical Asset Protection

Risk Management for Higher Education

ASME INNOVATIVE TECHNOLOGIES INSTITUTE, LLC

AIG

A report prepared by the ASME Innovative Technologies Institute, LLC, with support from AIG®.

The tragedies of the 2005 Gulf Coast hurricanes and the acts of violence that have struck the campuses of Virginia Tech, Delaware State University and other higher education institutions have underscored the need to gain a better understanding of the threats, risks and vulnerabilities of institutions of higher education due to large-scale crimes, natural disasters and other emergencies. To aid that effort, ASME-ITI and American Insurance Group (AIG), one of the world's largest insurance companies, are collaborating in the development of a risk assessment process that will ultimately result in information sharing and the spread of "best practices" among all institutions of higher learning.

This report on best practices will provide consistent and technically sound methodology to identify, analyze, and communicate risks on college and university campuses. More specifically, the methodology considers security and safety for individuals as well as the campus infrastructure, including buildings, laboratories, utilities and other resources for business continuity. This project is also intended to provide a forum for the exchange of safety and security measures that will allow all participating institutions to have access to the best available practices.

"Risk Management for Higher Education" was developed by ASME-ITI under an AIG grant.

ASME Innovative Technologies Institute, LLC

Acknowledgements

We would like to acknowledge the Advisory Committee that provided invaluable support and counsel in the development of the report through its meetings and the pilot projects.

Advisory Committee Chair
Richard Benson, Dean of Engineering
Virginia Tech

Mike Abbiatti, Associate Commissioner for Information and Learning Technology
Louisiana Board of Regents

Devin Broome, Executive Director of Information and Technology and Digital Media
University of Louisiana System

Jeff Charles, Director of Facilities
Santa Clara University

Rebecca Coleman, Director of Public Safety
Jackson State University

Chance Corbett, Emergency Management Coordinator
Auburn University

Brian P. Dolansky, Director of Campus Security
Westchester Community College

Christine Eick, Executive Director, Risk Management and Safety
Auburn University

Jim Hyatt, Project Director and Principal Investigator
National Campus Safety and Security Project
National Association of Colleges and University Business Officers

Gary Langsdale, University Risk Officer
Penn State University

Michael Lynch, Chief of Police
George Mason University

Jules Martin, Vice President for Public Safety
New York University

Mike Mastrangelo, Business Continuity Coordinator
The University of Texas System

Robert Pangborn, Vice President and Dean for Undergraduate Education
Penn State University

John Petrie, Assistant Vice President for Public Safety and Emergency Management
George Washington University Office of Risk Management

J. Edward (Ed) Poppell, Vice President of Business Affairs
University of Florida

Paul Pousson, Associate Director, Office of Risk Management
The University of Texas System

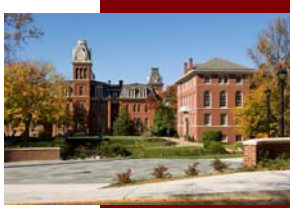
Christopher Rasmussen, Director of Policy Research
Midwestern Higher Education Compact

Terry Shoup, Professor of Mechanical Engineering
Santa Clara University

Todd Stewart, Executive Director
Director for the Program for International and Homeland Security
The Ohio State University-Mershon Center

We also acknowledge the graciousness of the universities and colleges which hosted the pilot projects, namely, George Mason University, Santa Clara University, University of Texas System - Permian Basin Campus at Odessa, University of Louisiana System, and Westchester Community College with the State University of New York. They volunteered their time and expertise to ensure the value of this report to the higher education community.

Table of Contents



Preface

Following the attacks of September 11, 2001, ASME (American Society of Mechanical Engineers) convened industry leaders at the request of the White House to address the requirements for protecting our Nation's critical infrastructure. The leaders' primary recommendation was to create a risk analysis and management process with a common methodology, terminology and metrics, to assist asset owners and government officials to compare risk within and across industry sectors. Such direct comparisons were seen as essential to support rational decision-making in allocating limited resources to reducing risk and enhancing resilience of critical infrastructure.

In response to this recommendation, ASME developed the initial version of the RAMCAP *Plus*SM program. The seven-step methodology enables asset owners to perform self-assessments of their risks relative to specific attacks. Risk is defined as a function of the likelihood of attack, the vulnerability to the attacks and their consequences. With this information, alternative initiatives for reducing risk and enhancing resilience can be evaluated for their ability to reduce the vulnerability to, and likelihood of, adverse consequences of attack. The reductions in risks are the benefits of the initiatives that can be used in estimating the benefit/cost ratios and allocating resources to specific initiatives.

The initial version of RAMCAP *Plus*SM program was a generalized description of the process, which was circulated widely and reviewed extensively by panels of risk management and security experts. Consistent with its purpose as a self-assessment tool, the methodology was streamlined and simplified to serve as the guide for developing a series of sector-specific risk management tools, consistent with the general approach, using common processes, threats, metrics and methods, but tailored to the issues, technologies and culture of the respective industries. The methodology was designated in the *National Infrastructure Protection Plan (NIPP)* as an efficient process to support consistent assessments and with results that could be systematically and directly compared. The NIPP also broadened the definition of the concerns to include natural hazards, which later documents of the RAMCAP *Plus*SM program have included.

In 2003, the U.S. Department of Homeland Security (DHS) initiated the development of a series of sector-specific guidance documents, which have been completed for nuclear power plants and spent fuel transportation and storage, petroleum refineries, chemical manufacturing plants and liquid natural gas (LNG) off-loading terminals. In 2005 DHS contracted with ASME-ITI to develop additional sector-specific guidelines for the water and wastewater sector and dams and navigation locks. All seven of these guides have been completed and are in use as part of the national critical asset protection plan. The current project extends the RAMCAP *Plus*SM program to higher education facilities.

Executive Summary

This report, "Risk Management for Higher Education," provides a comprehensive risk assessment process that was developed under a grant from the American International Group, Inc. (AIG) for determining the risk to students and faculty at colleges and universities from all risks, natural and manmade, including crime. The methodology used to determine risk is based upon the RAMCAP *Plus*[SM] methodology developed by ASME-ITI. It is a quantitative risk assessment tool that was originally developed to assist in asset allocation for the protection of the nation's critical infrastructure. Initially the methodology was limited to terrorism events, but subsequently was extended to include all hazards, including natural disasters. The present adaptation of the methodology includes virtually all unforeseen scenarios that pose a risk to institutes of higher learning.

Natural hazards include hurricanes, earthquakes, tornadoes, flood, wildfires, severe winter storms, extreme heat and other hazards due solely to natural occurrences. Natural hazards can result in damage or destruction of property as well as injuries and fatalities to personnel.

Personal security is included to assist users in estimating the risk to individuals attending the campus with respect to threats caused by acts upon their person. Personal security includes acts such as murder, robbery, rape, assault, intimidation, hate crimes, etc. The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998 (formerly the Crime Awareness and Campus Security Act of 1990) requires that schools publish an annual report disclosing campus security policies and three years of selected crime statistics. This information is used to establish a risk level for the campus. The Clery statistics are used to determine risk based upon the population of the campus. In addition to the on-campus report, police statistics for the neighborhoods surrounding the campus are included whenever available.

Building security is treated as a separate class of risk in this methodology. While it is true that building security is included as part of the natural hazards assessment, it is convenient to separate natural hazards from man-made hazards because of the basic assumptions that are inherent in the risk calculation and the difference in the way risk reduction and prevention measures and mitigation techniques are applied. Building security includes both the damage to the building due to man-made events (it is assumed that fire is caused by personnel and not lightning, wild fire, etc., which are included in the natural hazard assessment) and the fatalities and injuries caused by the event.

Terrorism is also included in the building security assessment. The security of the facility will affect access to the building, classrooms, and the vulnerability of the faculty, students, employees and visitors on campus.

The methodology used to quantify risk is provided in the following sections. A sample of the numerous questions are provided that are used to estimate the vulnerability of a particular campus. This information is used to determine a quantitative vulnerability value that is used in the risk equation to calculate the risk for various threat scenarios considered.

ASME-ITI is grateful to the universities and colleges which hosted the Pilot Projects, namely, George Mason University, Santa Clara University, University of Texas System - Permian Basin Campus at Odessa, University of Louisiana System, and Westchester Community College with the State University of New York.

This report would not be complete without addressing the one topic which has the highest profile in the media and probably causes the most concern to everyone involved with campus security: the active campus shooter. The Advisory Committee for the development of these best practices provided invaluable support and counsel in the development of the report through its meetings and through the pilot projects. Additionally, they contributed to the compilation of best practices guidelines that are intended to reduce the consequences of active shooters on campus and eventually eliminate them. The best practices guidelines described here are based upon the Virginia Tech recommendations with some additions suggested by the Advisory Committee.

The development of best practice guidelines continues and it is our goal to improve the ability of higher education institutions to better understand and assess risks to individuals and campus infrastructure.

Rationale for Process

The results of the assessment will consist of three separate areas which include natural hazards, personal security, and building security. These three categories are discussed below.

Natural hazards include, but are not limited to, hurricanes, earthquakes, tornadoes, flood, wildfires, severe winter storms, extreme heat and other hazards due solely to natural occurrences. Natural hazards can result in damage or destruction of property as well as injuries and fatalities to personnel. The assessment of natural hazards is bifurcated into the estimate of property damage such as loss of buildings and infrastructure as well as the cost associated with lost revenue resulting from damage to physical property, deaths and injuries.

Property damage costs are estimated monetarily considering the value of replacement and repair to the physical facilities and lost revenue as a result of the loss of use of the buildings and infrastructure. Injuries and fatalities are not estimated directly and no monetary estimate is made. The risk to personnel is based upon historical data for the location and an evaluation of the preventative and mitigation measures in place at the campus. FEMA 443 provides an overview of the natural hazards that can affect a campus. For more information on FEMA 443, please see: (http://www.fema.gov/library/viewRecord.do?id=1565)

Personal security is intended to assist users in estimating the risk to individuals attending the campus with respect to threats caused by acts upon their persons. This will include acts such as murder, robbery, rape, intimidation, hate crimes, etc. The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998 (formerly the Crime Awareness and Campus Security Act of 1990) requires that schools publish an annual report disclosing campus security policies and three years worth of selected crime statistics. In addition to the on-campus report, police statistics for the neighborhoods surrounding the campus should be incorporated, when available. The program also contains questions that are used to assess how well the campus is insulated from crimes that occur in the surrounding areas. Personal security, as defined herein, also includes the risk due to terrorism on the campus and surrounding area.

The definition of terrorism derives from the basic underlying concept that a terrorist seeks to instill terror or fear into his/her victims. A terrorist is not limited to one who has a political or religious motive, but can include students who have a psychological imbalance, a grudge against a fellow student or professor, possible medical problems, etc. Terrorism is included as a part of the risk to personal security and building security.

Building security is treated as a separate class of risk in this methodology. While it is true that building security is included as part of the natural hazards assessment, it is convenient to separate natural hazards from man-made hazards. This is due to the basic assumptions that are inherent in the risk calculation and the difference in the way risk reduction and prevention measures and mitigation techniques are applied. In performing a natural hazards

analysis, the analyst has historical data that can be used to estimate the frequency of the events being considered. Further, it is assumed that the natural hazard will "attack" the campus in a random manner, as opposed to the terrorist or criminal that is presumably intelligent and will seek to optimize his/her opportunity to cause harm or be successful in the attempted malevolent act. Thus, unlike the natural event, the terrorist or criminal will attempt to attack in a manner and at a time that will produce the "worst reasonable case" scenario. Estimating risk due to terrorism is further complicated by the fact that the frequency of attack is difficult to predict. The relatively small number of terrorist attacks compared to natural hazards results in a much greater uncertainty in predicting when an attack will happen.

Building security includes both the damage to the building due to man-made events (it is assumed that fire is caused by personnel and not lightning strike, wild fire, etc. which are included in the natural hazard assessment) and the fatalities and injuries caused by the event. Terrorism is also included in the building security assessment because the security of the facility will affect access to the building, classrooms, and the vulnerability of the faculty, students and employees and visitors on the campus. A cost associated with building security risk is the loss of the facility (replacement and repair) and loss of revenue (no classes can be held in the damaged buildings, reducing income). FEMA 426-429 provide an excellent foundation for the development of this component of the methodology. To search the FEMA Library, please see the following link: (http://www.fema.gov/library/)

It is noted that this methodology is consistent with the National Infrastructure Protection Plan (NIPP), provided by the United States Department of Homeland Security.

Details of Process

General Approach: Natural Hazards

Natural hazards include earthquake, hurricane, tornado, flood and other threats that are often referred to as acts of God. Natural hazards assessment will include:

- Risk assessment of infrastructure
- Risks to individuals

Natural hazards are considered in the design of all infrastructure components that are constructed in accordance with building codes. The philosophy of the building codes is to design structures to withstand the effects of natural events that have a frequency of occurrence that is considered to be reasonable considering both the initial cost of construction and the cost of replacement. For example, because the frequency of earthquakes in southern Florida is extremely low, there are no seismic loading requirements for buildings located in this zone. However, wind loads on the Florida coast are much higher than in other parts of the United States because of the threat of major hurricanes. Similarly, the seismic design criteria for California is much higher than for Florida, but the wind loading requirements are lower.

The risk to a building is thus a function of location and the type of event being considered. It is assumed that buildings designed for California are capable of withstanding seismic events of a certain magnitude before the event significantly damages the structure. Therefore, the risk to a building must be based upon the likelihood that the natural event magnitude will exceed the design basis. The greater the extent to which the event exceeds the design basis, the greater the damage to the structure and, conversely, the lower the likelihood of the events occurring. This is the basic premise used to estimate risk due to natural hazards.

The methodology used to determine risk due to natural hazards as described above has already been incorporated into the Water Sector Specific Guidance (SSG) document that was submitted to the Department of Homeland Security in September 2007. The currently implemented procedure is based upon checklists for natural hazards threats that are contained in Federal Emergency Management Agency (FEMA) documents. The campus pilot applications that have been done to date have highlighted the need for improvement of the FEMA procedure. The natural hazards risk assessment procedure contained in the Water Sector SSG is included as an attachment to this report. Until the complete natural hazards analysis process can be implemented, the following improvements to the FEMA method will be incorporated into the natural hazards risk assessment methodology:

1) Frequency of an event will be determined for each specific campus location being evaluated based upon historical data from the National Weather Service, the United States Geological Survey (USGS), or another reliable source.

2) Damage factors will be incorporated as vulnerability questions. This will approximate the more detailed damage loss coefficients used in the more general natural hazards procedure.

The risk to individuals is based upon both the expected frequency of occurrence of the event and the historical casualty rate. Mitigation measures in place at the institution will be used to offset expected casualties.

Infrastructure risk (buildings and capital equipment) will be based upon the conventional risk equation,

$$R = T \times V \times C.$$

Where:

R is the risk expressed in dollars per year.

T is the threat frequency expressed in events per year.

V is the vulnerability of the asset. Vulnerability is defined as the probability that the threat to the asset, if initiated, will result in causing the calculated consequences.

C is the consequences of the event expressed in dollars. This will include replacement value of the facility, lost revenue to the institution, and other costs that can be attributed directly to the event.

Risk to individuals will be expressed as the likelihood of death or injury to the personnel at the institution. The risk will be evaluated by determining the expected frequency of the event and the vulnerability of the facility to the occurrence (considering factors such as building construction, plans for evacuation and shelter in place, warning capability, and safety plans, etc.). The geographical location of the facility will be considered as well as historical data for events such as earthquakes, hurricanes, tornadoes, floods, etc.

General Approach: Personal Security

Personal security includes all hazards not considered to be natural hazards that can result in harm to the individual. The term, as defined here, is used to denote security while moving about the campus, including travel to the campus, living on the campus, and attending functions on or near the campus (i.e., attending classes, attending sporting events, etc.). Security inside the buildings will be included in Facility Security.

Personal security includes bodily assault, robbery, hate crimes, intimidation, and

other forms of acts directed toward the person. Personal security statistics are kept by virtually all institutions. This data is typically available in the open literature. In addition to campus security, the security of the neighborhoods surrounding the institution is compiled, when available. This information is relevant to the overall security of the institution since students and faculty must have ingress and egress through the community.

In assessing personal security, only two of the three risk variables will be developed: threat frequency and vulnerability. The consequences of an attack on the person are not considered to be quantifiable. It is impossible to assign a value for loss of life or even less violent crimes upon the person, thus the ratings for personal security will be based upon the threat frequency (available from crime statistics), and the vulnerability of the institution, as measured by security measures in place.

Security measures include, but are not limited to, CCTV; emergency call stations; campus police including number, training level and hours deployed; campus layout and accessibility by outsiders; and many other factors. The details of these assessments will be developed in the course of this report.

General Approach: Facility Security

This section will consider all untoward events except so-called natural hazards. Facility security is considered in two parts: 1) security of the building to damage by events other than natural hazards, and 2) security of the individuals in the facilities. Part one, facility assessment, will consider how a particular event affects the physical structures and components. Part two, personnel security within the facility, considers the probability of injury or fatality when an individual is within the facility.

A true risk assessment of the physical infrastructure can be performed as it is possible to assign a dollar value to inanimate objects such as building structures, power plants, and other infrastructure components. The numerical (dollar cost), assessment of facility security with respect to injuries and deaths of students and faculty is not considered to be quantifiable.

Infrastructure risk (buildings and capital equipment) will be based upon the conventional risk equation discussed previously:

$$R = T \times V \times C$$

This component of facility security considers only the damage to the physical structures. For example, a car bomb could damage a building or infrastructure component as well as result in fatalities and severe injuries. An attack using a poisonous gas such as Sarin will not result in significant damage to the structure. However, an attack utilizing weaponized Anthrax can

render the building useless for an extended period of time. Experience with the Anthrax attacks on postal facilities in 2002 indicates that the clean-up process can be extremely expensive and result in loss of use of the facility for months. Buildings may be abandoned or relegated to other, less desirable, functions as a result of high restorative costs and/or psychological impact on students. The assessment in this section includes only the damage to the structures regardless of the type of event considered. Personnel will be considered as a separate issue.

Risk to individuals in facilities

Facility security is also important to the safety of the students and faculty and other employees and visitors in the buildings. The design features of a building such as the placement of windows, window protection, set-back from roads or vehicle barriers, can greatly influence the number of casualties incurred in an event. Security measures such as locked doors, escape portals, plans for sheltering in place, warning methods, etc., will also affect building security. The safety and security ranking for the buildings will depend upon the design of the structures and the type and extent of preventative and mitigation measures that are in place.

Risk from Active Shooters

This final report, "Risk Management for Higher Education," would not be complete without addressing the one topic which has the highest profile in the media and probably causes the most concern to everyone involved with campus security: the active campus shooter.

The goal of the Advisory Committee is to eliminate future shootings on campus to the greatest extent possible, to mitigate events that cannot be eliminated and to reduce the short and long term effects of an unavoidable occurrence.

Best practices for prevention and mitigation of shootings are currently being compiled. Due to the short duration of the project and the need to make sector specific guidance available for use, the Advisory Committee has decided to adopt the recommendations of the multiple Virginia Tech internal reviews as interim Best Practices. The Virginia Tech recommendations have been generalized to make them more broadly applicable to other campuses. The following sections are based upon the Virginia Tech reports but contain modifications intended to extend the applicability.

Note: Any discrepancies or errors introduced to the original Virginia Tech documents are purely unintentional and are solely the responsibility of the authors of this report.

For more information on the Virginia Tech reports, please see the following links:

- *Virginia Tech Review Panel Report:*
  - *http://www.vtreviewpanel.org/report/index.html*
- *Virginia Tech Information and Communications Infrastructure Report:*
  - *http://www.vtnews.vt.edu/documents/2007-08-22_communications_infrastructure.pdf*
- *Virginia Tech Security Infrastructure Working Group Report:*
  - *http://www.vtnews.vt.edu/documents/2007-08-22_security_infrastructure.pdf*
- *Virginia Tech Presidential Internal Review:*
  - *http://www.vtnews.vt.edu/documents/2007-08-22_internal_communications.pdf*

It is our intention to continue to develop this area and incorporate the work of other campus security agencies. We have tentatively divided the problem into three parts.

- Prevention
- Mitigation of Ongoing Events
- Mitigation of Aftermath of an Event

Part I: Prevention

Prevention has the greatest potential to save lives and could possibly be the least expensive. The following recommendations are based upon the Executive Summary excerpted from the Presidential Internal Review, submitted to President Charles Steger, President of Virginia Tech, on August 17, 2007. The recommendations provide a valuable template which will aid in the prevention of future shootings.

Background on Virginia Tech Recommendations

President Charles Steger requested an internal review conducted by a working group to examine the interface between the university's student counseling services, academic affairs, judicial affairs and the legal system. The Working Group was charged with examining "the existing systems and the interface between them; determining what constraints, legal and otherwise, hamper effective interaction among these areas." The Group consisted of 17 key personnel from the units in the overall system and focused its attention on examining Virginia Tech's capacity and efficacy in identifying, responding to and supporting at-risk students. The Group conducted its work through five methods: 1) full committee discussions; 2) one-on-one interviews between the Chair of the Working Group and individual personnel; 3) participation in a symposium with six national experts; 4) analysis and review of relevant educational policies and procedures at Virginia Tech and other educational institutions; and 5) analysis and review of relevant state and federal documents.

Recommendations

1) Refining University Counseling Centers and Care Teams

A university Counseling Center or Care Team can provide a central structure that can identify and serve students with serious behavioral problems and can help in responding to students at risk. It incorporates members from all key student affairs units and other units of the university when appropriate. It is recommended that it be a more formally recognized and visible structure in the university system and that its protocol be updated to reflect impending changes. Effectiveness of the operation could be enhanced by adding a law enforcement officer and representatives from the campus disabilities office as permanent team members and connecting academic affairs personnel more directly to the deliberations. In addition, steps need to be taken to ensure that at least one person on the Team has a comprehensive picture of the cases being considered and is authorized if there is need to share information with others internally and externally when appropriate.

2) Creating a Threat Assessment Team

A new structure is needed to complement the work of the Care Team for students who may pose a threat to others. It is recommended that a structure be created that has specific responsibility for threat assessment to strengthen the overall system for the consideration of the most complex cases. The Threat Assessment Team would be charged with conducting a comprehensive fact-based description of a distressed student and empowered with the authority to act in a timely manner, consistent with university policy and applicable law, if necessary.

3) Expanding Case Management Capacity

Increased capacity for follow up on students who have been considered by the Care Team or seen by Counseling Centers will strengthen services to students in need. Adding additional case managers will help improve follow-up services to students,

as well as facilitate the information flow regarding the case across units. These case managers will maintain a comprehensive picture of the student and focus on the implementation of interventions, coordination of services and the monitoring of the effectiveness of the interventions.

4) Improving Communication in the System

Effective communication among units regarding at-risk students is essential. There are a number of recommendations intended to enhance communication in the system including conducting on-going training for personnel on the application of the Family Educational Rights and Privacy Act (FERPA). Enhanced communication will aid discussion of cases, clarify public statements in university policy on how FERPA is applied, establish a central university contact who has a comprehensive picture of distressed students who have been assessed by the system, clarify policies for communicating with external agencies regarding acutely distressed students, and implement new policies for emergency notification to students.

5) Expanding Training of Administrators, Faculty, and Staff in Violence Prevention

The effort to raise the level of awareness regarding the considerable resources that are available to members of the university community in seeking assistance with distressed students is vital. It is recommended that additional training programs be directed to administrators, especially newly appointed ones, as they are key participants for bringing others in their unit up-to-date information related to campus safety. It is further recommended that new strategies be developed to raise the awareness of faculty and staff regarding the availability of resources for dealing with at-risk students and employees.

6) Extending the University-wide Violence Prevention Policy

A structure is needed that will help integrate the numerous university-wide efforts to enhance campus safety. It is recommended that a university level committee be formed that ensures that programs are in place to support the Campus and Workplace Violence Prevention Policy. The Committee would bring oversight from all precincts of the university, including student affairs, academic affairs, human resources, facilities and administrative services with regard to policy, operations and resources that are intended to create a coherent approach to ensuring a safe campus environment.

7) Building Community to Promote Individual and Community Well Being

A strong, vibrant and supportive community is essential in ensuring a safe campus environment. An environment that promotes civility, works toward the acceptance of others' differences, strives to include rather than exclude and provides assistance to those in need is fundamental to a safe campus. It is recommended that a more systematic approach be instituted that specifies campus-well being as a goal and ensures that the various efforts are connected. The coordination of this effort could be situated with the Committee for Campus and Workplace Violence Prevention that was recommended above.

These recommendations are systemic in nature and will involve deliberation by those offices directly affected by them in their day-to-day work to decide how best to incorporate the ideas. Moreover, these recommendations are only a piece of the larger picture and must be linked directly to other efforts that are underway to enhance campus safety. The careful coordination and integration of all efforts to promote campus safety is essential to ensure a comprehensive approach. Finally, any system implemented needs to be dynamic in nature to adjust to the changes that continually emerge from the needs of the university community and new lessons learned from on-going evaluation of the system and best practices of peers.

In another report presented by the Virginia Tech Review Panel to Governor Tim Kaine, two appendices contain additional relevant information that provides insight into the how shooters may be identified.

• Appendix M: *Red Flags, Warning Signs and Indicators* (See http://www.vtreviewpanel.org/report/report/31_APPENDIX_M.pdf)
•Appendix H: *Explanation of FIRPA and HIPPA Laws* (See http://www.vtreviewpanel.org/report/report/26_APPENDIX_H.pdf)

Part II: Mitigation of Ongoing Events

Mitigation of a shooting event is clearly not as desirable as prevention, but it would represent an improvement and could save lives. In our pilots we have been told that the "typical" shooting event lasts less than ten minutes. It is impossible to assemble a swat team in time to mitigate the shooting. Mitigation, as well as prevention to some extent, is highly dependent upon the security practices for the campus. The following is based on an excerpt from the Virginia Tech Security Infrastructure Working Group Report, Presidential Working Paper dated August 17, 2007.

Note: Any changes made are for the purpose of making these recommendations more broadly applicable to other companies.

Areas targeted for enhancement or improvements include:

Physical Infrastructure

- Remove and replace the hardware on all perimeter doors to mitigate the risk of doors being chained.
- Install interior locks on all general assignment classrooms and evaluate installation of locks on non-general assignment classrooms.

[1] The Virginia Tech Review Panel Report, August 2007

- Explore the installation of a centrally controlled electronic card key access system for all key academic and administrative facilities. This system will be used to secure buildings during nonworking hours. In the event of an emergency such a system would allow individual and groups of buildings to be locked remotely by the police department.
- Improve security or "hardening" of select campus offices through the installation of electronic card key access controls on interior doors, and monitoring of these offices by a closed circuit television system.
- Construct a state of the art Public Safety Building that will enhance university and emergency services capabilities by physically consolidating these units in a single facility.
- Explore the feasibility of deploying a centrally monitored closed circuit television (CCTV) system using video surveillance cameras at key locations on the campus.

Communication

- Provide mass notification in classrooms and other environments where other systems may not provide adequate notification. It is recommended that a simple electronic banner textual displays with audible alarms be installed in all classrooms where practicable.
- Explore the installation of LCD message boards within the entrances to key campus buildings, as well as outdoor illuminated message boards at major campus entrances. These displays would alert the campus to emergency situations and provide instructions on the appropriate actions to be taken.
- Create an electronic "people locator system" that members of the campus population could log on to after an emergency to post their status so that concerned relatives, friends and colleagues could receive updated information.
- Develop pre-written "templates" to help communicators craft emergency messages more expeditiously.

Emergency Preparedness

- Update campus emergency preparedness response plans.
- To prepare for potential emergencies increase the use of annual "table top" or simulation exercises by key campus units (e.g. police, rescue squad, physical plant, building coordinators, etc.). These exercises should involve faculty, students, and staff as well as law enforcement and public safety units from surrounding jurisdictions.
- Implement a building coordinator program whereby a person in each building is identified as the responsible party in the event of an emergency. All coordinators will be trained in appropriate emergency response and security processes and procedures. Central coordination and training will be the responsibility of the campus police department.
- Formally identify backups to key Policy Committee members who are unable to physically respond to campus emergencies. Also enhance communications with key Policy Committee members who are off campus when an emergency occurs.

Protocols

- Enhance security protocols that will explicitly highlight what to do in the event of an emergency. This will include posted signs in all classrooms and student services facilities, as well as inclusion of such material as part of new employee and student orientations.
- Create a security master plan for the campus and establish a campus security planning committee.

In order to implement the recommendations outlined in this report, the university should immediately initiate a program to fully cost and identify the funding sources necessary to implement the program. Possible fund sources could include increased state support, as well as a mandatory life/safety fee.

Part III: Mitigation of Aftermath of an Event

This relates to business continuity and ways to reduce the effects of the event. The consequences to a university may include loss of use of facilities, loss of prestige, and lower desirability rankings, loss of alumni support, adverse publicity. This area would probably fall into the purview of the business continuity as opposed to security. The following suggestions are provided as a starting point for further discussion.

- Having a plan for dealing with the media
- Resilience planning
- Reuse of buildings involved
- Reciprocity agreements between schools
- Response team in place

References & Bibliography

ASME Innovative Technologies Institute, LLC. "RAMCAP: The Framework." Version 2.0, May 2006.

Ayyub, Bilal, and McGill, William, and Kaminsky, Mark. "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework." Vol. 27, No. 4, 2007.

FEMA 426. "Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings". Published by Federal Emergency Management Agency, December 2003.

FEMA 427. "Risk Management Series: Primer for Design of Commercial Buildings to mitigate Terrorist Attacks." Published by Federal Emergency Management Agency, December 2003.

FEMA 428. "Risk Management Series: Primer to Design Safe School Projects in Case of Terrorist Attacks." Published by Federal Emergency Management Agency, December 2003.

FEMA 429. "Risk Management Series: Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings." Published by Federal Emergency Management Agency, December 2003.

FEMA 433. "HAZUS-MH Risk Assessment and User Group Series: Using HAZUS-MH for Risk Assessment – How-To Guide." Published by Federal Emergency Management Agency, August 2004.

FEMA 443. "Building a Disaster-Resistant University," Published by Federal Emergency Management Agency, August 2003.

National Infrastructure Protection Plan, 2006. The United States Department of Homeland Security.

"Report to the President on Issues Raised by the Virginia Tech Tragedy." Published by U.S. Department of Health and Human Services, Department of Education, and Department of Justice, June 13, 2007.

Virginia Tech. "Information and Communications Infrastructure: Confidential Presidential Working Paper." August 17, 2007.

Virginia Tech. "Mass Shootings at Virginia Tech April 16, 2007: Report of the Review Panel Presented to Governor Kaine, Commonwealth of Virginia." August, 2007.

Virginia Tech. "Presidential Internal Review: Working Group Report on the Interface between Virginia Tech Counseling Services, Academic Affairs, Judicial Affairs and Legal Systems." August 17, 2007.

Virginia Tech. "Security Infrastructure Working Group Report: Presidential Working Paper." August 17, 2007.

Disclaimer

The work is published with the understanding that the ASME-ITI, the American Society of Mechanical Engineers (ASME), and its editors are supplying information, but are not attempting to render engineering or other professional services. If such engineering or professional services are required, the assistance of an appropriate professional should be sought.

Neither ASME-ITI, the American Society of Mechanical Engineers (ASME), the Sponsor, nor any representatives or employees of those organizations make any warranty, expressed, or implied, regarding any facts or opinions contained or expressed in this document.

Neither ASME-ITI, the American Society of Mechanical Engineers (ASME), the Sponsor, nor any representatives or employees of those organizations make any warranty, expressed or implied, regarding the reliability or usefulness of any information, formula or process disclosed in this report.

Neither ASME-ITI, the American Society of Mechanical Engineers (ASME), the Sponsor, nor any representatives or employees of those organizations assumes any legal liability to any third party that reviews this report based upon the information, facts, opinions, formula or process expressed or disclosed in this report.

Neither ASME-ITI, the American Society of Mechanical Engineers (ASME), the Sponsor, nor any representatives or employees of those organizations represent or provide any warranty, expressed or implied that use of information, facts, opinions, formula or process expressed in this report will not infringe on any third party rights.

In no event will the ASME-ITI, the American Society of Mechanical Engineers (ASME), the Sponsor, or any representatives or employees of those parties assume any liability to any third party for any consequential damages, economic damages, personal injuries or property damages incurred by any third party that may arise, either directly or indirectly, from any facts, opinions, information, formula or process disclosed in this report. Nor shall those parties be responsible for any errors, omissions, or damages arising out of the use of information contained or disclosed in the report.

ASME Innovative Technologies Institute, LLC

The ASME Innovative Technologies Institute, LLC, (ASME-ITI) provides market-relevant engineering and technology-based products and services to the government, industry and academic markets.

ASME-ITI is a resource multiplier, enabling government, business and academia to quickly develop superior responses to critical issues and ideas.

ASME-ITI offers a broad range of services including:

- Risk Management
- Program and Project Management
- Research and Development
- Standards Development
- Training

ASME-ITI leverages the expertise of its staff with the strength of subject matter experts to address specific problems in the areas of homeland security and risk management.

For additional information regarding the RAMCAP Plus[SM] program or to request a copy of this document, please contact:

ASME Innovative Technologies Institute, LLC
1828 L Street NW Suite 906
Washington DC 20036-5104
Tel: (202) 785-7499
Fax: (202) 429-9417
Email: info@asme-iti.org