RAMCAP PLUS℠ FOR HIGHER EDUCATION SOFTWARE PROGRAM

The RAMCAP *Plus*℠ for Higher Education Sector Specific Methodology is being crafted as an interactive computer program that can be utilized by campus security and administrative personnel to perform a complete assessment of the main campuses as well as satellite campuses. The software will utilize a series of screens with drop-down menus for collecting information. All calculations necessary to perform the risk assessments are to be performed by this program. Online help and hyperlinks to references will be provided in a user-friendly interface.

The program is divided into major sections as described below. The user can complete each section individually and save the data input at any point so that multiple sessions can be used to complete the overall assessment. The steps of the program follow the RAMCAP *Plus*℠ seven-step process. A brief description of each section of the program follows.

1) Introduction

This section provides an overall description of the program. Background material is provided that describes what data is necessary and the individuals that should contribute to the assessment. This section contains:

- Introduction
- Add New Campus
- Scope and Executive Guidance
- Preparation for Completing Computer Program

2) Facility Information

This section records information relevant to the campus including location, points of contact, and general information.

3) Asset Characterization

The assets of the campus are input including:

- Residential
- Administration
- Academic
- Research Laboratory
- Public Health
- Childcare
- Special Needs
- Utilities
- Indoor Venue
- Outdoor Venue
- Agriculture

4) Threat Characterization and Assessment

This section of the program collects data on the three types of threats being considered:

- Natural Hazards
- Personal Threats
- Building Threats
- Public Health Threats

The program will supply information concerning the expected frequency of the event and the event magnitude. Pre-defined terrorist threats are included as well as natural, personal and threats that apply to the buildings and infrastructure. This information will be used to contribute to the risk assessment that follows.

5) Consequence Analysis

Based upon the data previously input the program will show pairs of assets and threats. The user is then required to enter the asset attractiveness. Note that an estimate of the worst reasonable case costs was input in Section 3, Asset Characterization. Costs should include both dollar cost and anticipated fatalities. The consequence estimate should be as complete as possible, including such things as replacement costs, loss of revenue, psychological, and indirect costs. The better the input, the more useful the results will be to the user.

The asset information from Section 3 is combined with the threat information from Section 4 to provide an estimate of the consequences of the applied threat to the selected asset. Thus the asset/threat pairs are evaluated. Those checked in the appropriate box are carried forward to the next step.

6) Vulnerability Analysis

In order to provide a basis for the program to estimate the vulnerability of the asset, the user will be asked to respond to a series of questions that relate to security procedures in place and natural hazards. This information will be used, along with data included in the program data base, to evaluate the vulnerability of each asset that was included in the asset characterization phase. Appendix B contains examples of the questions that must be answered by the user. The answers are weighted according to importance to risk level. The reference, from which the questions were derived, if applicable, is included in the appendix.

7) Risk Assessment

With the information collected to this point, the program will provide an estimate of the risk for each asset and produce a report. All of the necessary risk variables, C, V and T, have either been provided by the user or they are includes in the underlying methodology. Risk will be calculated for all asset/threat pairs. The results can be viewed in printed format or graphical output. (See *Figure 1*- Schematic of RAMCAP *Plus*℠ Campus Software)

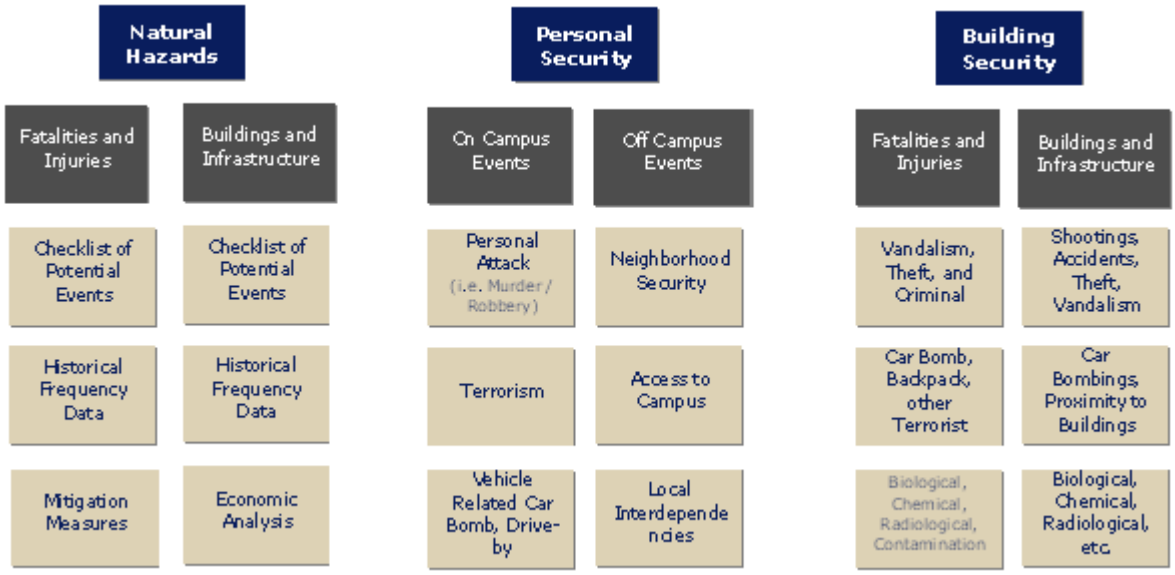

Figure 1. Schematic of RAMCAP *Plus*[SM] Campus Software

8) Risk Management

Using the risk assessment determined in the previous section, the user can now perform risk management studies. Since the risks are estimated in terms of dollars for loss for buildings and revenue, it will be possible to estimate a return on investment for proposed improvements in safety and security. The risk management tool will be very powerful in justifying expenditures for improvements to safety and security and mitigation of consequences.

9) Online Help

The software contains online help so that the user should not be required to refer to the written documentation. An example of the documentation is shown in Figure 2. This screen is accessed by clicking on the HELP button on the *Introduction* menu.

Ultimately, the RAMCAP *Plus*[SM] Campus Software will provide consistent and technically sound methodology to identify, analyze, quantify, and communicate risks of on college and university campuses. All types of threats are considered including an active shooter, a terrorist, and natural hazards (earthquake, hurricane, tornado, flood, etc.). The program provides for the calculation of risk as measured in dollars, casualties, and the ability of the university to function after an event. Through the software, the user will be able to evaluate various methods to reduce risk through countermeasures, mitigation strategies and resilience enhancements. The program will also document the risk evaluation and risk management process by creating a permanent report that can be easily updated as conditions change and facilities are added or removed from the campus.

Further Information

To learn more about the RAMCAP Plus[SM] Campus Software, please visit the ASME-ITI website (www.asme-iti.com) or contact ASME-ITI by phone (202-785-7499) or email (ITIinfo@asme.org).