

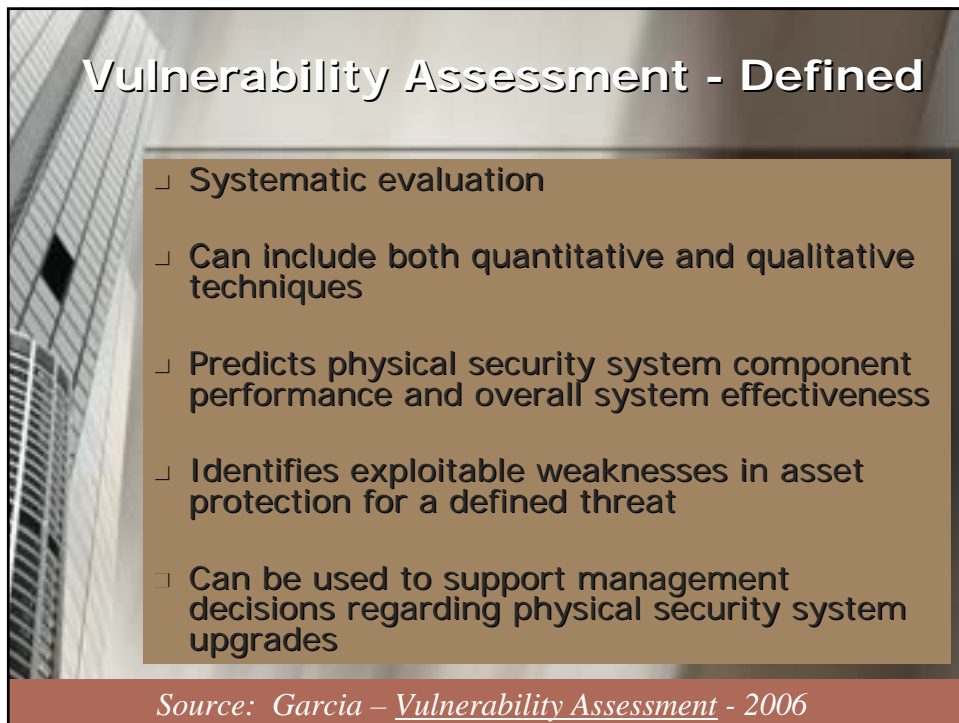


The slide features a background image of a modern skyscraper with a curved facade. In the upper right corner, there is a small inset image of two people in yellow raincoats looking at a document. The title 'Vulnerability Assessments' is centered in a large, orange font. Below the title, on the left, is a logo for 'SAFER' with the tagline 'MAKING COMMUNITIES SAFER' and silhouettes of three people. On the right, the presenter's name and affiliation are listed in white text on a dark red background.

# Vulnerability Assessments

Dr. Pam Collins  
Eastern Kentucky University  
October 2006

MAKING COMMUNITIES SAFER



The slide has a background image of a skyscraper. The title 'Vulnerability Assessment - Defined' is at the top in white. Below it is a list of five bullet points on a brown background. At the bottom, there is a source citation in white text on a dark red background.

## Vulnerability Assessment - Defined

- ┌ Systematic evaluation
- ┌ Can include both quantitative and qualitative techniques
- ┌ Predicts physical security system component performance and overall system effectiveness
- ┌ Identifies exploitable weaknesses in asset protection for a defined threat
- ┌ Can be used to support management decisions regarding physical security system upgrades

Source: Garcia – *Vulnerability Assessment* - 2006

## Variety of Vulnerability Assessment Models Currently in Use...

- Number and Types
- Department of Homeland Security
- Dept. of Energy/ Dept. of Defense
- Private Sector (Various Organizations)

## Example Algorithms

### Department of Homeland Security:

$$R=I \times p[T] \times p[V]$$

R=Consequences [C] x Likelihood [L] or C x L

[L] Likelihood=Probability p[T] Threat xp[V] Vulnerability

I = Impact

### Sandia National Labs (Vulnerability Assessment Model)

Risk is a function of S, LA, and LAS.

S= severity of consequences of an event.

LA= likelihood of adversary attack.

LS= likelihood of adversary attack and severity of consequences of an event.

LAS= likelihood of adversary success in causing a catastrophic event.



## DHS 10 Risk Methodology Evaluation Criteria

- 1) Clearly identify the infrastructure sector being assessed.
- 2) Specify the type of security discipline addressed, e.g. physical, information
- 3) Collect specific data pertaining to each asset
- 4) Identify critical/key assets to be protected
- 5) Determine the Mission impact of the Loss or Damage of the Asset.

*Source: DHS / ODP Vulnerability Assessment Methodology Report – July 2003*



## DHS 10 Risk Methodology Evaluation Criteria

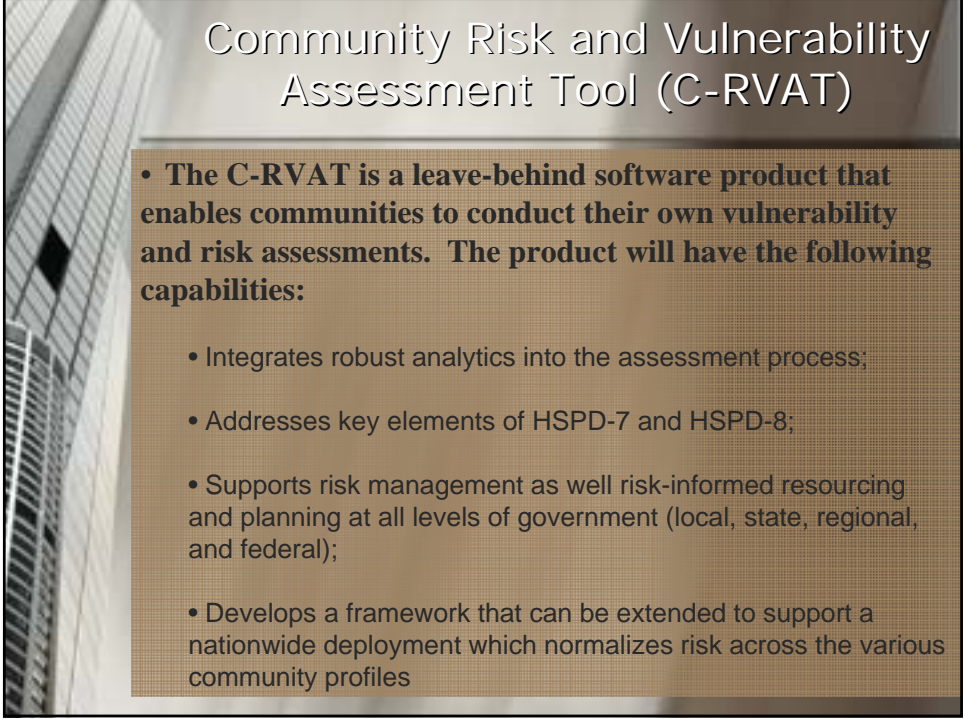
- 6) Conduct a Threat Analysis and Perform Assessment for Specific Assets
- 7) Perform a Vulnerability Assessment for specific threats
- 8) Conduct Analytical Risk Assessment and determine priorities for each asset
- 9) Low Cost to train and conduct
- 10) Recommendations for Countermeasures

*Source: DHS / ODP Vulnerability Assessment Methodology Report – July 2003*



## Example Vulnerability Assessment Models

- Community Risk and Vulnerability Assessment Tool (DHS)
- Department of Energy (Sandia National Laboratories)
- Department of Defense (U.S. Navy)
- Private Sector (*Various Organizations*)



## Community Risk and Vulnerability Assessment Tool (C-RVAT)

- **The C-RVAT is a leave-behind software product that enables communities to conduct their own vulnerability and risk assessments. The product will have the following capabilities:**
  - Integrates robust analytics into the assessment process;
  - Addresses key elements of HSPD-7 and HSPD-8;
  - Supports risk management as well risk-informed resourcing and planning at all levels of government (local, state, regional, and federal);
  - Develops a framework that can be extended to support a nationwide deployment which normalizes risk across the various community profiles

**PASCOM ASSESSMENT** Log Out

Community > **Assets** Threats Risk Analysis Reports

1. Identify critical assets 2. List assets 3. **Characterize assets** 4. Prioritize assets BACK NEXT

**ASSETS** INSTRUCTIONS

Name: **Chemical Plant** GENERAL CONTACT SECURITY RISK

Asset Type: Building  
Sector: Chemical

Address (line 1):  
Address (line 2):  
County:  
City:  
State:  
Zip:  
Cross Street 1:  
Cross Street 2:  
Latitude (Deg. Min. Sec.):  
Longitude (Deg. Min. Sec.):  
Distance to Perimeter: meters  
Line of Sight to Perimeter:  
Population:

Description:  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Purpose(s):

School  
 **Chemical Plant**  
 Hiking Trail  
 Railroad Yard

**PASCOM ASSESSMENT** Log Out

Community Assets > **Threats** Risk Analysis Reports

1. Assess threats 2. Create scenarios 3. **Assess risks** 4. Evaluate vulnerability 5. Identify security issues BACK NEXT

**THREATS** INSTRUCTIONS

Scenario Name: **Chemical Plant/ Aerosol Anthrax**

Asset: **Chemical Plant**  
Threat: **Aerosol Anthrax**

Description:  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Risk Factors:

Contaminations	not set ?
Denial	
Intensifiable Effect	
Environmental Impact	
Replacement Cost Impact	
Business Continuity Impact	
Economic Impact	
National Strategic Importance Impact	
Emergency Response Function Impact	

**Chemical Plant/ Aerosol Anthrax**  
 Chemical Plant/ Major Earthquake  
 School / Cyber Attack  
 School / Pandemic Influenza

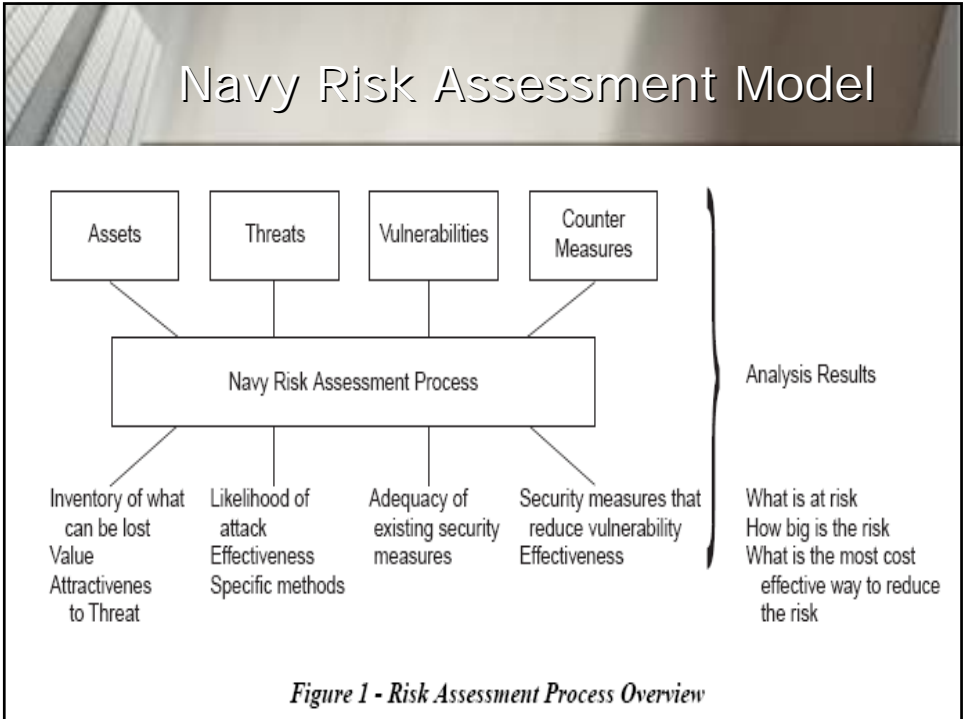


## Sandia National Laboratories Vulnerability Assessment Model (VAM)

The VAM has 12 basic steps:

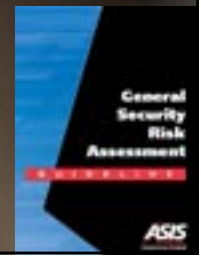
1. Screening for the need for a vulnerability assessment.
2. Defining the project.
3. Characterizing the facility.
4. Deriving severity levels.
5. Assessing threats.
6. Prioritizing threats.
7. Preparing for the site analysis.
8. Surveying the site.
9. Analyzing the system's effectiveness.
10. Analyzing risks.
11. Making recommendations for risk reduction.
12. Preparing the final report.

# Navy Risk Assessment Model



# Private Sector Approach

- Qualitative
- VS.
- Quantitative



## Conclusions / Questions

- Variety of Vulnerability Assessment Models
- Many have specific target facilities, such as chemical plants or schools.
- Users must select the model that best suits their security needs.

## Contact Information:

### **Dr. Pam Collins**

*Professor , Loss Prevention and Safety  
Executive Director, The Justice and Safety Ctr.  
Eastern Kentucky University  
50 Stratton Building / 521 Lancaster Avenue  
Richmond, KY 40475  
Office: (859) 622-8106 / Fax: (859) 622-8038  
E-mail: [PamCollins57@aol.com](mailto:PamCollins57@aol.com)*