PORT SECURITY
RISK ASSESSMENT TOOL

USER MANUAL

ABS Consulting
AN ABS GROUP COMPANY

PSRAT PORT SECURITY RISK ASSESSMENT TOOL

USER MANUAL

PSRAT was developed for the
United State Coast Guard by
ABS Consulting

1525 Wilson Boulevard, Suite 625
Arlington, VA 22209 USA
+1 (703) 682-7373

Table of Contents

Table of Figures and Tables

1. Background

The Port Security Risk Assessment Tool (PSRAT) is a risk assessment tool and supporting process that enables analysts to quantify the risk of potential terrorist attacks to maritime assets operating within their area of responsibility. PSRAT was developed by ABS Consulting in cooperation with the United States Coast Guard (USCG), and currently distributed by the Asia-Pacific Economic Cooperation (APEC). PSRAT is based on a long standing, and industry standard, scenario-based risk assessment methodology.

PSRAT is intended to be an intuitive, user-friendly tool to quantify maritime terrorism risk in support of risk based decision making at the strategic, operational and tactical levels.

For the analysis process, PSRAT uses a phased approach in which the user lists potential targets, scores scenarios and view results/generates reports.

2. Introduction

The purpose of this manual is to illustrate how to use the various functions of the PSRAT tool and provide an overview of the underlying methodology used in PSRAT.

2.1. Formatting of Data Elements

PSRAT maintains a consistent formatting approach throughout the screens. The following provides a description of the formatting elements and their meaning:

White (editable) Galveston – Any column or data field that is white can be edited.
Turquoise (read-only) Vessel – Any column or data field that is turquoise may NOT be edited.
Orange (filter) TYPE – Drop down boxes with the purpose of filtering, sorting, or creating reports are orange. These orange drop down menus may not be edited, but they can be utilized by clicking the arrow at the right side of the field.
Maroon Underlined Text (Help text) CLASS – Headings that are maroon and underlined are links to definitions or helpful information.

2.2.Analysis Process

When PSRAT is newly deployed, a Tool Setup step process must be followed to customize the tool. Once this has been completed, the analysis process follows the short steps of (1) List Targets (2) Score Scenarios, and (3) Review Results. This process is illustrated in Figure 1. To ensure quality risk information, PSRAT analysts should involve subject matter experts and facility personnel to help evaluate the threat, vulnerability and consequence factors for each scenario.

Figure 1 – PSRAT Analysis Process

3. Getting Started

PSRAT is a highly-customized Microsoft Access® database. To run this application, you must have Microsoft Access® installed. To use the full functionality of this application you must have Microsoft Access 2007 ®. PSRAT's basic structure consists of two files with maritime names. The *Tug* that contains the business logic and drives the *Barge* data file through the analysis process, just as a Tug helps navigate barges through the port.

Tug/Processing file (tug.mdb). This file contains the logic used to perform the assessment. This file is commonly referred to as the Tug.
Barge/Data file (file name varies depending on location). This file contains the data associated with the targets within your area. This file is commonly referred to as the Barge.

Once launching PSRAT, you will work through six main screens during the PSRAT setup and analysis process. As seen in Figure 3, each screen serves multiple functions:

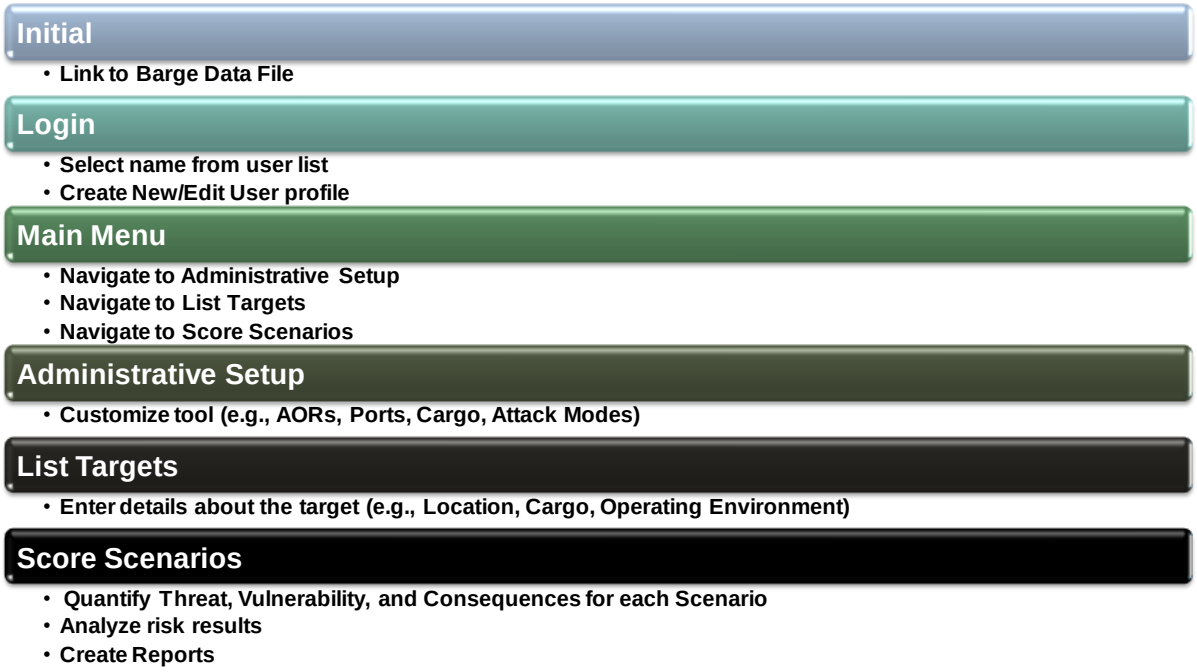


Figure 2 - Main PSRAT Screens

3.1. Launch PSRAT

To launch PSRAT, you must navigate to the PSRAT location on your computer. Once there, you must double-click on the "Tug.accde" file. This will launch the Tug's *Initial Screen* (Figure 5). This page is where you will be required to link the Tug to the Barge before you can proceed into the program.

3.2. Enable Content

Sometimes you will need to enable content on the *Tug* before you can link to the *Barge*. In order to do this, you will need to click the Security Warning "Options" button at the top of the screen (Figure 3).

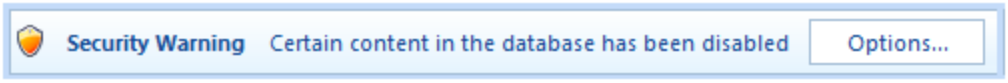


Figure 3 - Security Warning

Then on the Microsoft Office Security Options pop-up screen (Figure 4), select the "Enable this content" radio button. Click "OK" once selected.

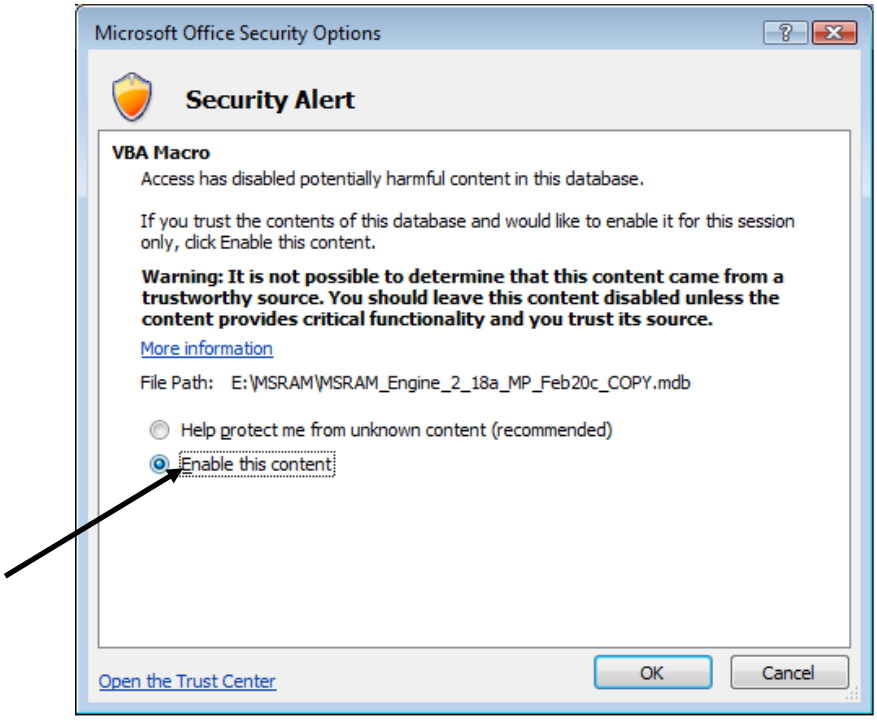


Figure 4 - Microsoft Access Security Options

Figure 5 – Initial Screen

3.3. Link Data File

To link the data file (*Barge)* you must push the button "Select Barge/Data File" on the top *Initial Screen* (Figure 5), revealing the pop-up box in Figure 6. Push the "Browse" button on the right side of the box to browse to the barge.mdb data file that you just renamed. Click "OK" when selected. You have now linked to your data file. Now click the "Proceed to Login" button (Figure 5).

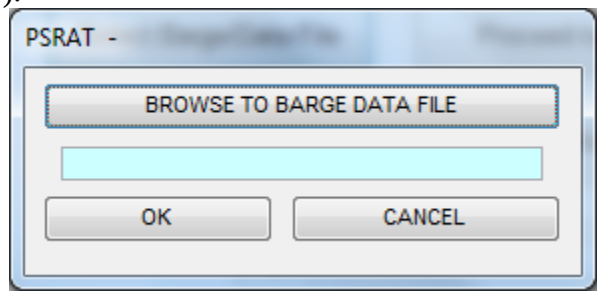


Figure 6 - Link to PSRAT Data File (*Barge)* Pop-Up Box

4. Login

After linking the *Barge* to the *Tug*, you will be required to login to PSRAT. Existing users' information is stored in a user list (Figure 7). New users can create a profile (Figure 8). Users can also edit their profile at any time via the Edit button. Once logged in, PSRAT stores the user's identification in the several audit functions that capture change history.

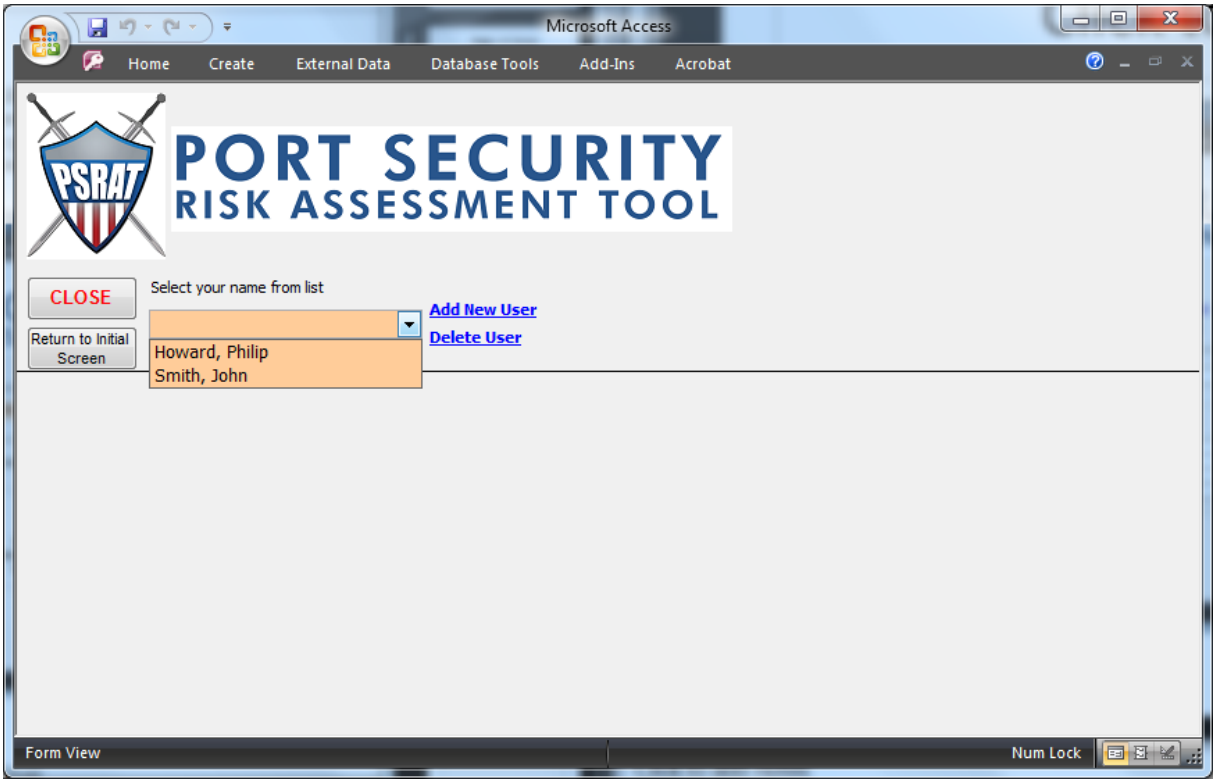


Figure 7 - Existing User Login List/Screen

4.1.Add User

To add a new user, click the "Add New User" blue hyperlink. This will expand the screen and load a blank user form to fill out (Figure 8). Enter all of your personal information within the boxes on the form.

When you have finished entering all of your information, click the "Proceed" button at the bottom right of the screen to continue. You only need to create your user profile one time. On subsequent PSRAT logins, you will be able to select your name from the existing users list.

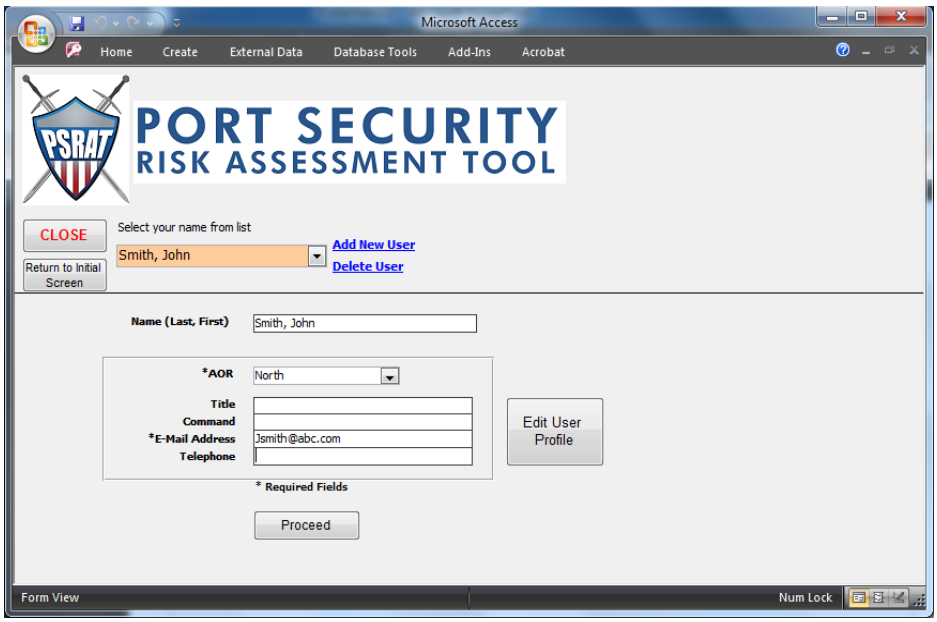


Figure 8 - New User Login Screen

4.2. Main Menu

The Main Menu screen (Figure 9) provides you with the opportunity to navigate to the primary analysis functions within the application: (1) List Targets and (2) Score Scenarios & Results and the Administrative Setup screen.

Figure 9 - Main Menu

5. List Targets

Before performing a risk analysis, and evaluating scenarios, you must first identify the targets that terrorist attacks will be evaluated against. During the *List Targets* phase, you should list all of the significant targets within your Area of Responsibility (AOR). This list of targets will serve as the foundation for the score scenarios process.

When adding targets, you will assign each a target class, this target class selection will determine the scenarios evaluated during the *Score Scenarios* step. The default PSRAT target classes are:

- Attraction vessels
- Barges
- Cargo/tank ships
- Cargo/tank terminals
- Commercial passenger vessels
- Fueling facilities
- Military vessels
- Military/government facilities
- Offshore
- Other
- Passenger terminals
- Public areas/buildings
- Transportation/distribution system
- Waterway
- Petroleum Refinery
- Offshore oil/gas facility
- Agricultural and Food
- Petroleum facility
- Maintenance dock
- Marine cargo terminal
- Fuel storage facility
- Oil Pipeline
- Waterway transportation system
- Rail/ Highway/ Road
- Bridges
- Energy gridline
- Power plants
- Commercial key assets
- Offside port storage
- Bulk/mineral/ general cargo
- Container Ships
- Cruise ships
- Industrail fishing boats
- Passenger vessels & Recreational boats
- Petroleum tank vessels
- Roll-on/Roll-off
- Chemical tank vessel
- Hazardous Material

In addition to Target Class, the following information is gathered for every target

- Target name
- Availability of Target / Sub-target
- Type of target
- Class
- Cargo Type
- Port area
- Port name
- Waterway
- Mile Marker
- Region and
- Latitude
- Longitude

All of the above information will be entered on the *1. List Targets* screen as seen in Figure 10.

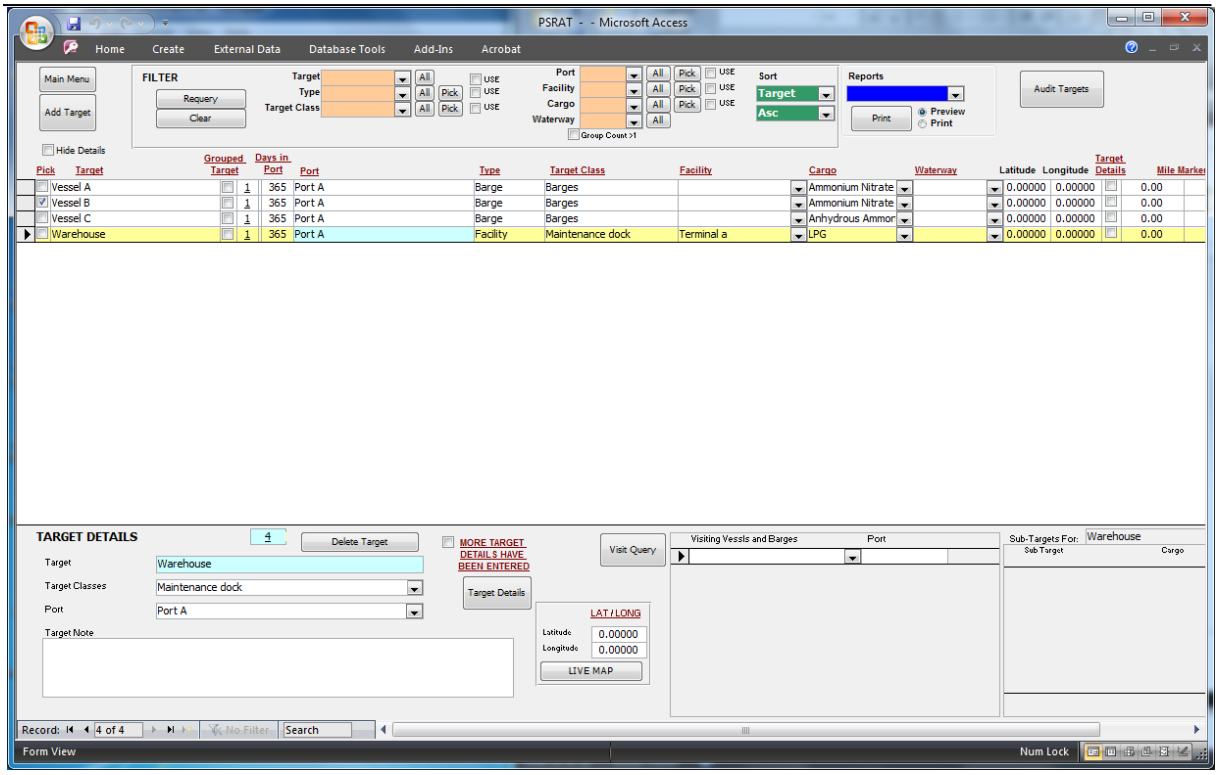


Figure 10 - List Targets

5.1. Add Target

At the beginning of the risk analysis process and as the operating environment changes in your AOR, you will have to add new targets to PSRAT. To add targets to the target list, click on the "Add Target" button (Figure 9), located on the top left of the *List Targets* screen. After clicking this button an Add Target Screen (Figure 11) will popup.

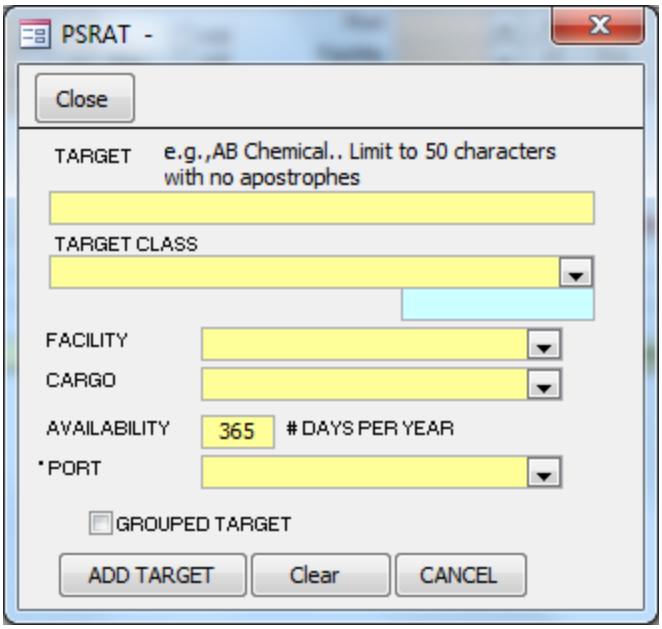


Figure 11 - Add New Target Popup

5.2. Delete Target

To delete a target in the target list, click into any field on the row of the target you wish to delete. Look to the "Target Details" area at bottom portion of the screen. Make sure the target you want to delete is listed in the target details then click the "Delete Target" button which is located in the "Target details" part of the screen.

5.3. Target Auditing

Changes to the target list can be viewed by accessing the target's audit log located in the top right of the *List Targets* screen. Click the Audit-Target button to see the: Target Name, Port, Target Class, User and Date Updated, and Type of change.

5.4. More Target Details

For targets that are not from the target class of *Vessel* or *Barge* more details about the target can be entered through the *More Target Details* button located at the bottom middle of the *List Targets* screen. This information does not directly feed into the risk equation, however it is qualitative information that should help inform your assessment of vulnerability and consequence factors in the *Score Scenarios* Screen. For *Vessel* or *Barge* class targets, more details can be added via the Target Memo field at the bottom of the *List Targets* screen.

6. Score Scenarios

This section of PSRAT is where you will perform a risk analysis of scenarios for each of the targets that have been created. PSRAT auromatically generates scenarios that are required to be assessed for each target, based on the target's class assigned in the *1. List Targets* process. If there are additional scenarios that you wish to assess, you may do so using the "Add Scenarios" button. Each scenario has an associated "Scenario Description" that will provide a synopsis of the attack mode.

You will be required to evaluate the Threat, Vulnerability, and Consequences for each scenario. The available optional scenarios for each target include those that are not mandatory, but still possible. All attack types are not available for all target classes.

The risk score is calculated based on the following main factors:

Threat – what is the likelihood that terrorists will attempt the scenario?
Consequence – what are the impacts if the attack is successful?
Vulnerability – what is the probability that the terrorists will be successful?

Threat is assessed as a single value quantifying the relative likelihood of an attempted attack similar to the scenario being assessed. Vulnerability and Consequence are assessed as the combination of several sub-factors. All factors and sub-factors are then combined to create a Risk Index Number (RIN) for a given scenario. All of the factors and sub-factors are shown in Figure 12:

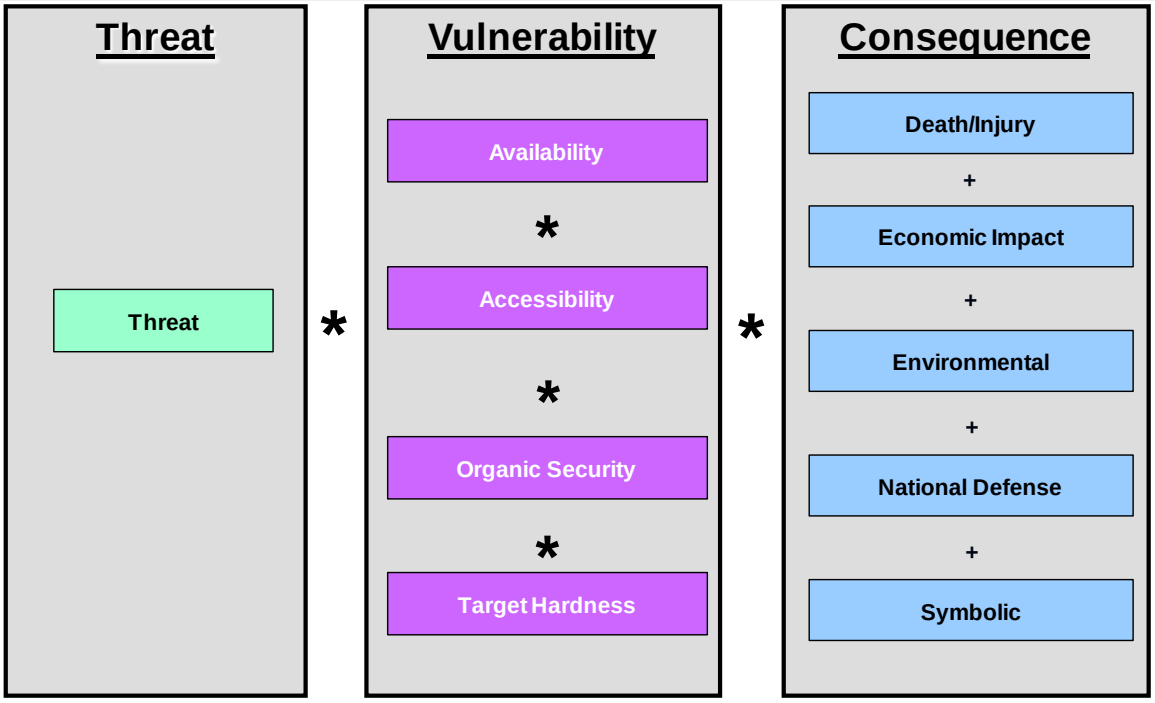


Figure 12 - PSRAT Risk Factors

Each risk factor is assessed on the *2. Score Scenarios* screen (Figure 13) based on a drop-down menu selection of established benchmarks and associated numberical values.

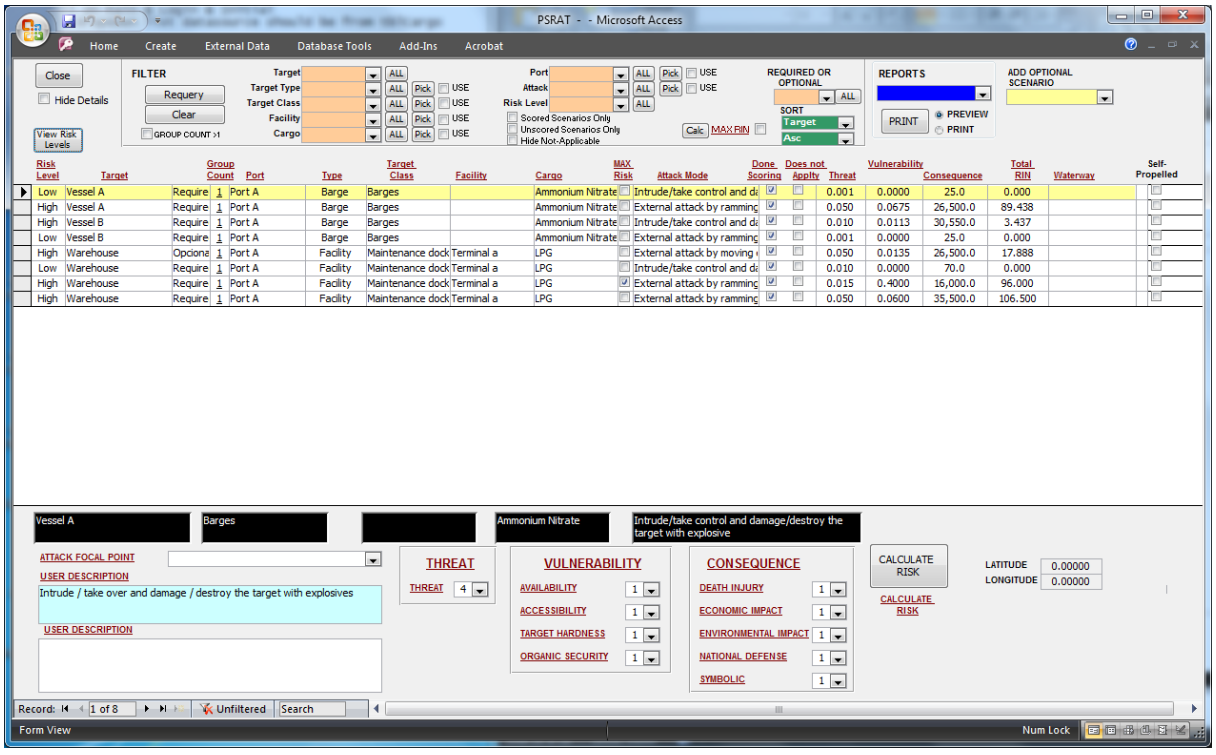


Figure 13 - Score Scenarios Screen

Figure 13 shows the Scenario Scoring screen. In the middle is a listing of all of the scenarios. You can filter the listing of scenarios based on any of the parameters in the orange boxes at

the top of the screen. There are also additional filtering checkboxes located just underneath the orange filter fields, and through Micrsoft Access.

When a scenario is selected in the middle of the screen by clicking anywhere in the row, the bottom of the screen will update with the details (scenario scoring) associated with the attack mode.

6.1. Threat

Threat is defined as the likelihood of an attempted terrorist attack. When assessing threat, consider the likelihood of an attack being attempted similar to that of the specific scenario being scored (attack mode/target class combination).

Threat is assessed by selecting the appropriate category (1-5) based on the Category Description. The categories, descriptions, and weights are shown below in Table 1.

Table 1 - Threat Categories, Descriptions, and Weights

Category	Factor Category Description	Value
1	No credible intelligence indicating the presence/activity of terrorist cells	0.001
2	Credible intelligence indicates that terrorist cells are operating with unknown targets and methods of attack	0.01
3	A terrorist attack on the same class of target has recently occurred AND/OR Possible precursor/sentinel events that may indicate specific types of attacks on specific targets have been observed	0.05
4	Credible intelligence indicates that a specific type of attack is imminent against a class of targets	0.015
5	Credible intelligence or operational information indicates that a specific type of attack will occur against a specific target at a specific time	0.6

For every target and attack mode combination, select the threat score that best describes the specific scenario. Simply use the drop down box under threat to select the value.

6.2. Vulnerability

Vulnerability is the probability that an attack will be successful that the attack is successful at achieving the assessed consequences, given that an attack is attempted. PSRAT consideres Availability, Accessibility, Target Harndness, and Organic Security as part of vulnerability, or layers to prevent a successful attack. Remember, when scoring vulnerability, it is the success at creating the consequences assessed for the scenario. Each of these sub-factors are defined below:

Availability: Probability that the target is present for the attack to proceed
Accessibility: Probability that the target is accessible from some physical path
Organic Security: Probability that security measures at the target defeat the attack
Target Hardness: Probability that the target withstands the attack

Tables 2 through 5 show the Vulnerability sub-factors,with the associated categories, descriptions, and values:

6.2.1. Availability

In order for an attack to be successful, the target must be present at the time of the attack. While the terrorist may deide to go forward with an attack, it will likely cause significantly lower consequences than have been assessed for the given scenario. Note: The value (Table 2) corresponds to the probability that the target will be available.

Table 2 - Availability Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Rarely available (e.g., no set schedule and on any given day presence highly unlikely and unpredictable; arrives once a year or less for a few hours and arrival is not publicly known)	0.001
2	Limited availability (e.g., present several times a year or unpredictable arrival times/departure times with < 1 week advanced notice of schedule)	0.01
3	Often available (e.g., present several times a month; arrival times predictable 1week to 2 months in advance; predictable departure times)	0.1
4	Usually available (e.g., present several times a week or on a relatively set schedule)	0.5
5	Always available (e.g., continually present or present daily on a set schedule)	1

6.2.2. Accessibility

In order to successfully carry out an attack the terrorist must be able to navigate the threat to the target. Accessibility considers the geographic or other physical impediments to delivering the threat to the target. This does not consider security measures that are scored under Organic Security. Note: The value (Table 3) corresponds to the probability of terrorist success in accessing the target.

Table 3 - Accessibility Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Excellent deterrence (expected to deter attack; access restricted to within 500yds of target; multiple physical/geographical barriers)	0.01
2	Substantial deterrence (e.g., multiple barriers that are difficult to defeat; unrestricted access to within 200yds of target)	0.1
3	Good deterrence (e.g., single substantial barrier; unrestricted access to within 100yds of target)	0.3
4	Limited deterrence (easily defeated access barrier; unrestricted access up to perimeter of the target itself)	0.75
5	No deterrence (e.g., unrestricted access to target and unrestricted internal movement)	1

6.2.3. Organic Security

The terrorist must also be defeat an target-based security. This includes that ability of security measures to both detect and interdict the threat. Note: The value (Table 4) corresponds to the probability of terrorist success defeating security.

Table 4 - Organic Security Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Excellent deterrence capability expected to deter attack (e.g., all of #2 and covert security elements that represent additional elements not visible or apparent)	0.01
2	Substantial deterrence capability (e.g., detailed security plan, effective emergency communications, well trained and equipped guard force; multiple detection systems [camera, x-ray, etc.], timely outside L.E. for prevention)	0.05
3	Good deterrence capability (e.g., minimal security plan, some communications, armed guard force of limited size relative to the target; outside L. E. not timely for prevention, limited detection systems)	0.5
4	Limited deterrence capability (e.g., no plan, limited communications, outside L. E. not timely for prevention, unarmed minimal guard force)	0.9
5	No deterrence capability (e.g., no plan, no guard force, no emergency communication, outside L. E. [law enforcement] not timely for prevention, no detection capability	1

6.2.4. Target Hardness

Assuming the terrorist is able to successfully access the target and defeat target security, the target focal point must then fail to withstand the attack in order for the assessed consequences to occur. The ability of a target to withstand an attack is called Target Hardness. Note: The value (Table 5) corresponds to the probability of terrorist success in accessing the target.

Table 5 - Target Hardness Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Target expected to withstand attack (e.g., complex design and substantial construction of target minimizes consequences)	0.01
2	Substantial ability to withstand attack (e.g., good design and construction of target)	0.1
3	Good ability to withstand attack (e.g., simple design and relatively strong construction)	0.3
4	Limited capability to withstand attack (e.g., simple design and construction)	0.8
5	Intent of attack easily accomplished (e.g., readily damaged or destroyed)	1

6.3. Consequence

Assuming a successful attack, what are the reasonable worse case consequences? The consequences are quantified using five (5) factors:

Deaths/Injuries – The number of expected deaths as a result of an attack. Suggested equivalence of 10 life threaning injuries to 1 death.
Economic Impact – The impact on the economy including target damage, and loss of product.
Environmental Impact – Impact of persitant pollutants on the environment including the cost of cleanup.
National Defense – Impact or disruption of military actions or national defense
Symbolic Impacts – Damage or destruction of important local, regional, national or international symbols

Tables 6 – 10 display the Categories, Category Descriptions and associated values for each consequence sub-factor are displayed

6.3.1. Deaths/Injuries

The number of expected deaths as a result of an attack. Suggested equivalence of 10 life threaning injuries to 1 death. See Table 6.

Table 6 - Death/Injury Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	No deaths or serious injuries; relatively only minor injuries	1.65
2	1 to 10 deaths or serious injuries	16.5
3	10 to 100 deaths or serious injuries	165
4	100 to 1,000 deaths or serious injuries	1,650
5	>1,000 deaths or serious injuries	16,500

6.3.2. Economic Impact

The impact on the economy including target damage, and loss of product. See Table 7.

Table 7 - Economic Impact Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	< $1 million	0.5
2	$1 million to $10 million	5
3	$10 million to $100 million	50
4	$100 million to $1 billion	500
5	>$1 billion	2000

6.3.3. Environmental Impact

Impact of persitant pollutants on the environment including the cost of cleanup. See Table 8.

Table 8 - Environmental Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Small spills with minimal, localized individual impact on the eco-system	0.5
2	Short-term serious damage to the eco-system (e.g., large spills)	5
3	Long-term damage to a portion of the eco-system	50
4	Complete destruction of multiple aspects of the eco-system over a small area	500
5	Complete destruction of multiple aspects of the eco-system over a large area	2000

6.3.4. National Defense

Impact or disruption of military actions or national defense. See Table 9.

Table 9 - National Defense Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	No serious military/defense impact	0.5
2	Short-term disruptions in military actions	5
3	Long-term disruptions in military actions	50
4	Creates critical short-term vulnerabilities in national defense	500
5	Creates critical long-term vulnerabilities in national defense	2000

6.3.5. Symbolic Impacts

Damage or destruction of important local, regional, national or international symbols. See Table 10.

Table 10 - Symbolic Impact Categories, Category Descriptions, and Values

Category	Factor Category Description	Value
1	Major damage or destruction of locally important symbols, or minor/no damage to an important symbol	0.5
2	Major damage or destruction of regionally important symbols	5
3	Major damage, but not destruction of, nationally important symbols that are internationally recognized	50
4	Destruction of other important symbols that are recognized internationally	500
5	Destruction of a unique national icon	2000

Table 11 shows the PSRAT consequence equivalency matrix describing the categories you will use to evaluate the five consequence factors. The matix is based on the default PSRAT values of $3 Million per Death and $1M to clean-up 50 barrels of oil. This equivalency is very important in that it

Table 11 - PSRAT Consequence Equivalency Based on $1M per Death

Category	Value	Death/Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Impact
5	2000	>1,000 deaths or serious injuries	>$1 billion	Complete destruction of multiple aspects of the eco-system over a large area	Creates critical long-term vulnerabilities in national defense	Destruction of a unique national icon
4	500	100 to 1,000 deaths or serious injuries	$100 million to $1 billion	Complete destruction of multiple aspects of the eco-system over a small area	Creates critical short-term vulnerabilities in national defense	Destruction of other important symbols that are recognized internationally
3	50	10 to 100 deaths or serious injuries	$10 million to $100 million	Long-term damage to a portion of the eco-system	Long-term disruptions in military actions	Major damage, but not destruction of, nationally important symbols that are internationally recognized
2	5	1 to 10 deaths or serious injuries	$1 million to $10 million	Short-term serious damage to the eco-system (e.g., large spills)	Short-term disruptions in military actions	Major damage or destruction of regionally important symbols
1	0.5	No deaths or serious injuries; relatively only minor injuries	< $1 million	Small spills with minimal, localized individual impact on the eco-system	No serious military/defense impact	Major damage or destruction of locally important symbols, or minor/no damage to an important symbol

Like the scoring for threat, score every target and attack mode combination, select the consequence value scores that best describe the specific scenario. Simply use the drop down box as shown in Tables 6-9 and select the value.

6.4. Calculate Risk

Once you have scored all of the consequence and vulnerability factors for a scenario, click the "Calc Risk" button on the bottom right of the *1. Score Scenarios* Screen to calculate the risk for the scenario. Risk is expressed in units of Risk Index Number (RIN). The RIN for a scenario is based on the threat, vulnerability, and consequence scores you chose during your analysis. If you go back and change any of your evaluations, you must press the "Calc Risk" button to update the RIN for a scenario.

$$Risk\ (RIN) = Threat\ x\ Vulnerability\ x\ Consequence$$

Where:

$$Vulnerabiliy\ (Probability\ of\ Terrorist\ Success) = Availability\ x\ Accessibility\ x\ Organic\ Security\ x\ Target\ Hardness$$

$$Consequence\ (Consequence\ Points) = Deaths + Economic + Envinron. + National\ Defense + Symbolic$$

6.4.1. Mark Scenario as Not Applicable

For scenarios where the attack mode may not be feasible against the target, the scenarios can be marked as "Does Not Apply". Typically these scenarios are not included in scenario reports.

6.4.2. Calculated Maximum Risk

For a comparison of the risk between scenarios, it is recommended that a comparison of the maximum risk scenario for each target be compared. Click the "Calc" Max Risk Button in the Top right of the *1. Score Scenarios* Screen to perform the calculation and filter on the maximum consequence scenarios for each target.

6.4.3. Create Scenario Reports

To review reports, click the drop down boxes on the Target and Score Scenarios screens in the section of the window labeled "Reports." Review the items in the drop down boxes to see the various reports that you can run.

7. Appendix A – Administrative Setup of PSRAT

To access the Administrative setup functions in PSRAT, on the *Main Menu* screen, click the *Administrative Setup* button. This will bring you to the screen as shown below in Figure A.1.

There are 10 steps in the PSRAT Administrative Setup process Figure A-1:

Figure A - 1 - Administrative Setup Process

The administrative setup screen is shown in Figure A-2. Each setup step has an associated checkbox in order to track setup progress

Figure A - 2 - Administrative Setup Menu

The Define Ports screen, on the Admin Setup Menu, allows the user to add, edit, and delete ports (Figure A-3).

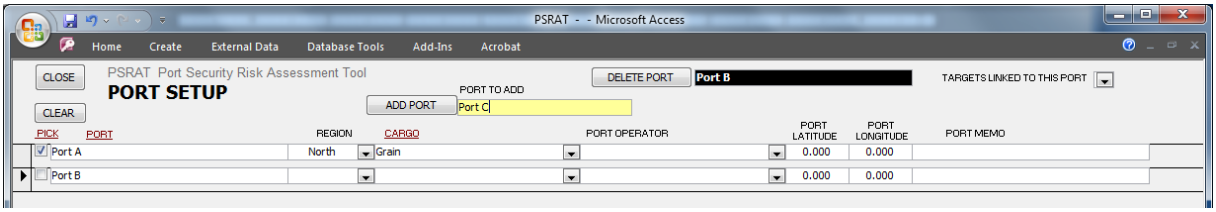


Figure A - 3 - Define Ports

The Facilities screen, on the Admin Setup Menu, allows the user to add, edit, and delete facilities and facility details in PSRAT (Figure A-4).

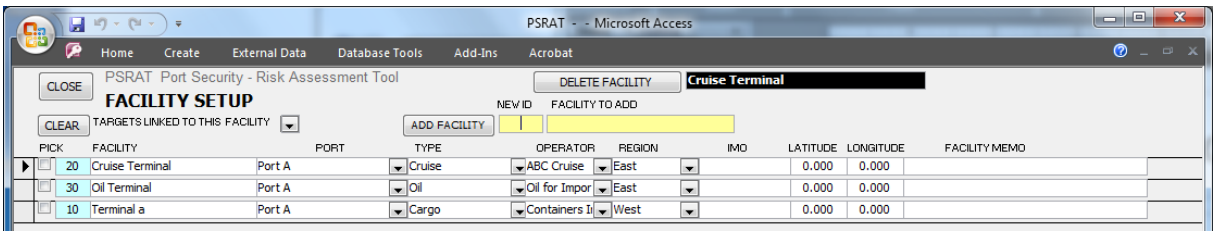


Figure A - 4 - Define Facilities

The Define Cargo screen, on the Admin Setup Menu, allows the user to add, edit, and delete cargo (Figure A-5).

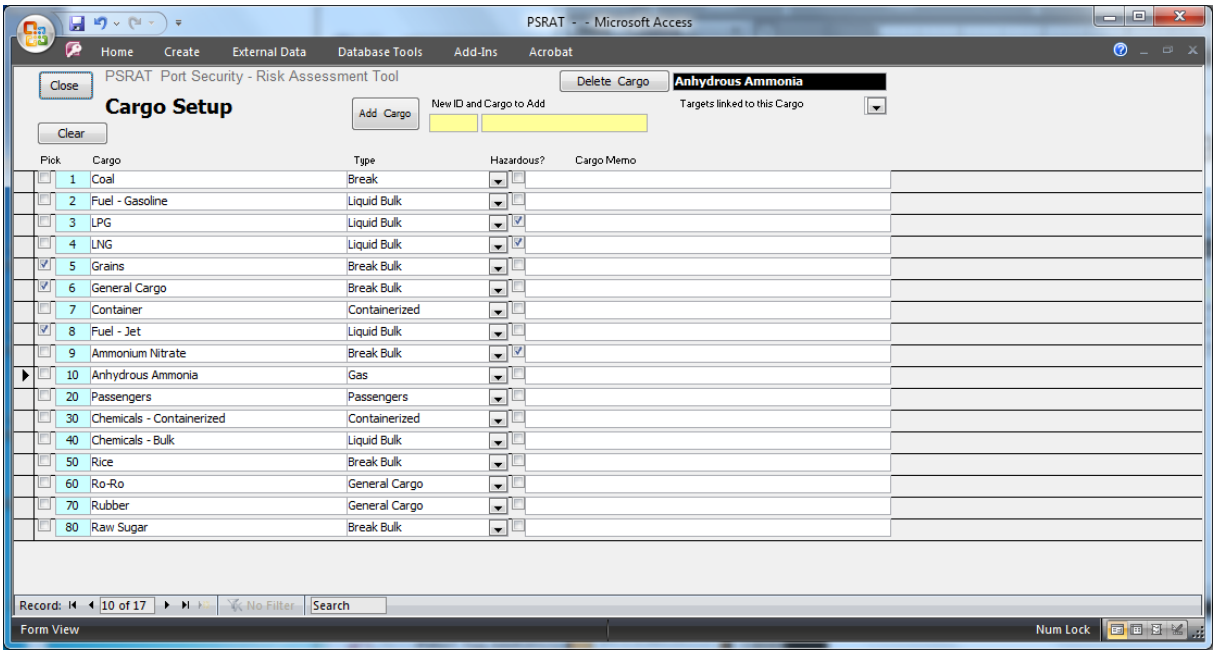


Figure A - 5 - Define Cargo

The Target Classes screen, on the Admin Setup Menu, allows the user to define the target classes to which targets will be assigned (Figure A-6).

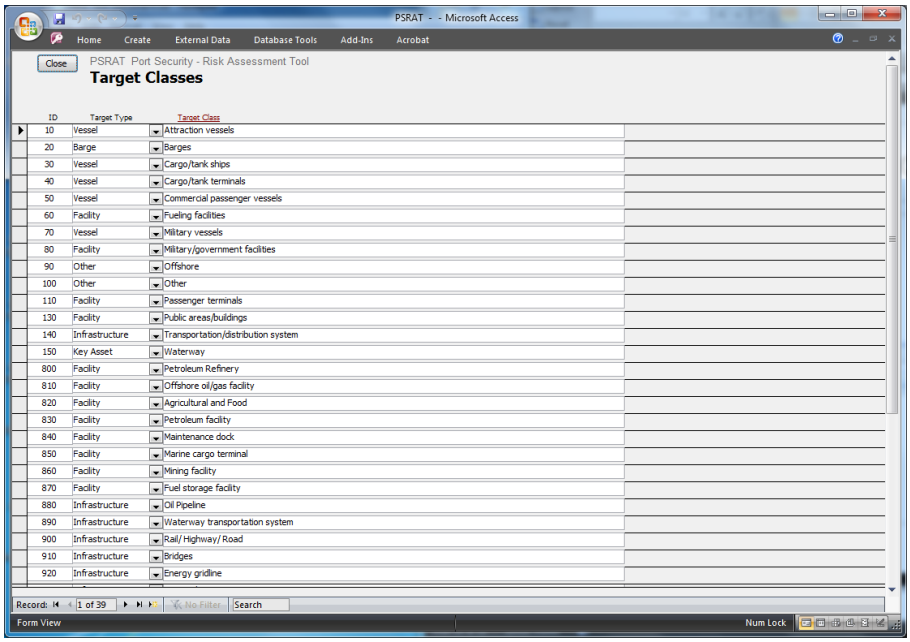


Figure A - 6 - Target Classes

The Attack Modes screen on the Admin Setup Menu, allows the user to review and/or edit the current Attack Modes defined in PSRAT. (**Error! Reference source not found.**A-7).

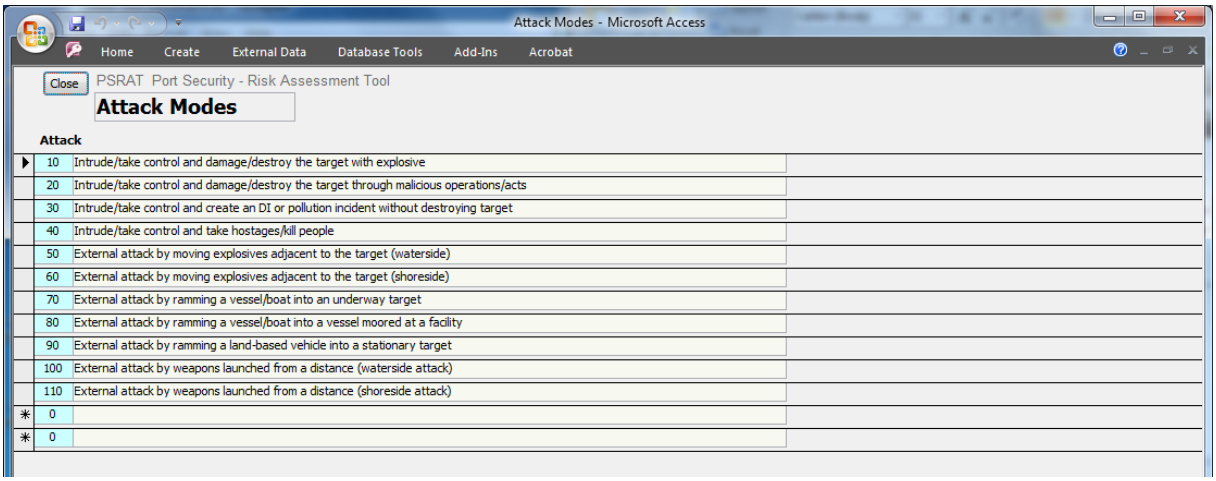


Figure A - 7 - Attack Modes

The Scenario Matrix screen, on the Admin Setup Menu, allows the user to give best guesses to scenarios they deem most appropriate for the threat in their Ports and attack modes (Figure A-8).

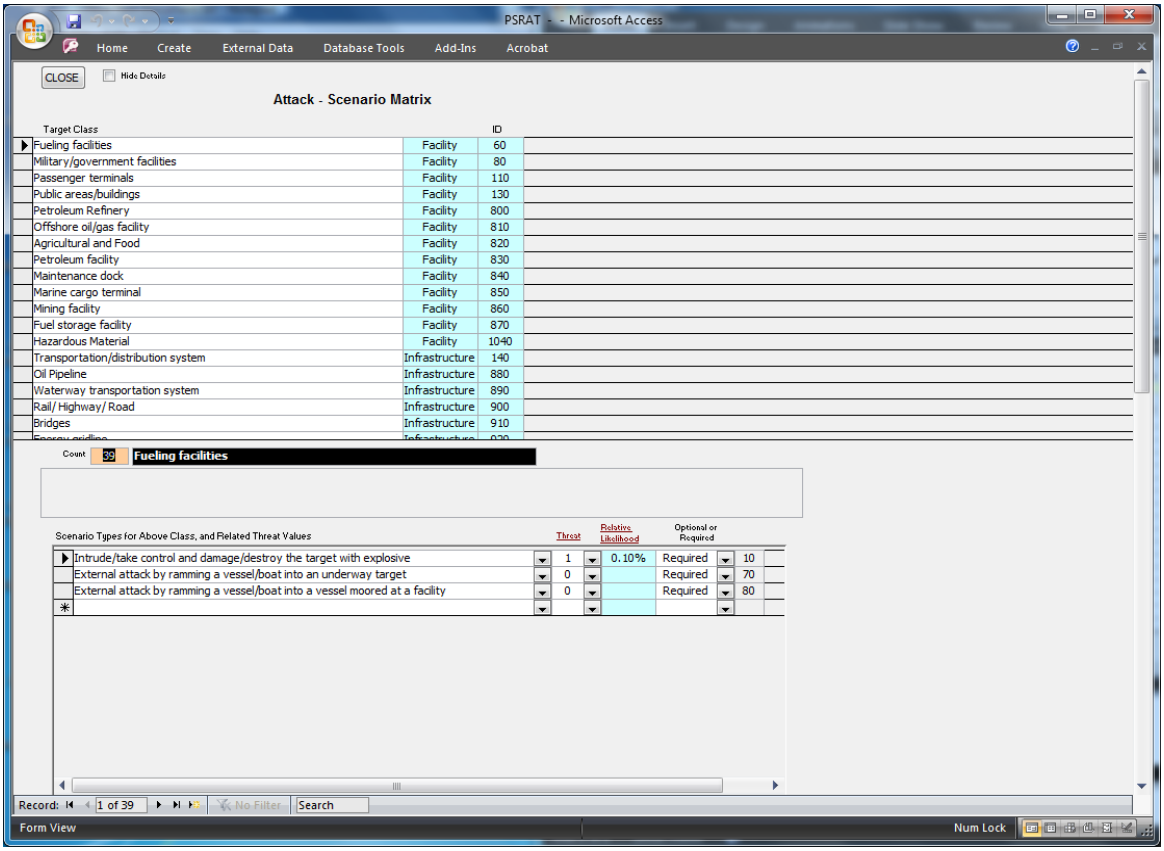
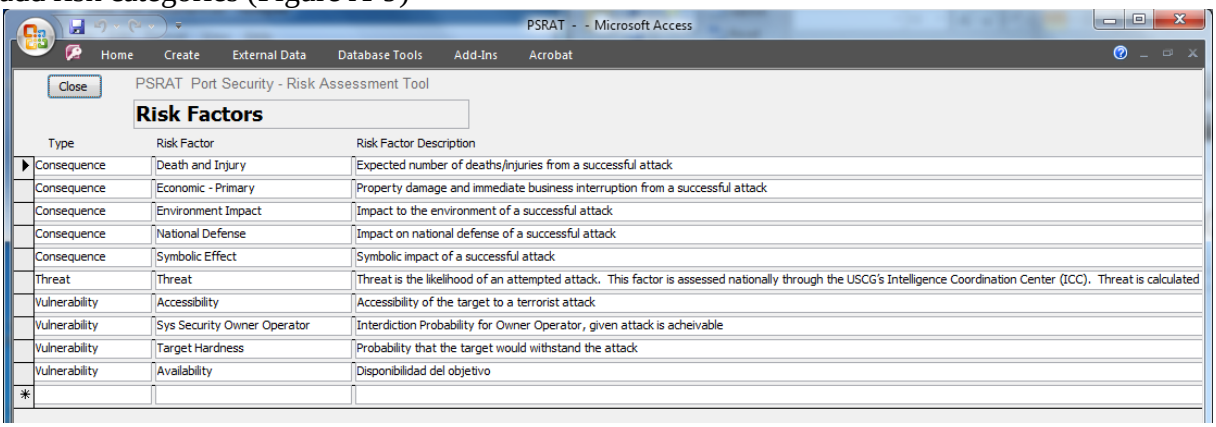


Figure A - 8 - Scenario Matrix Definition

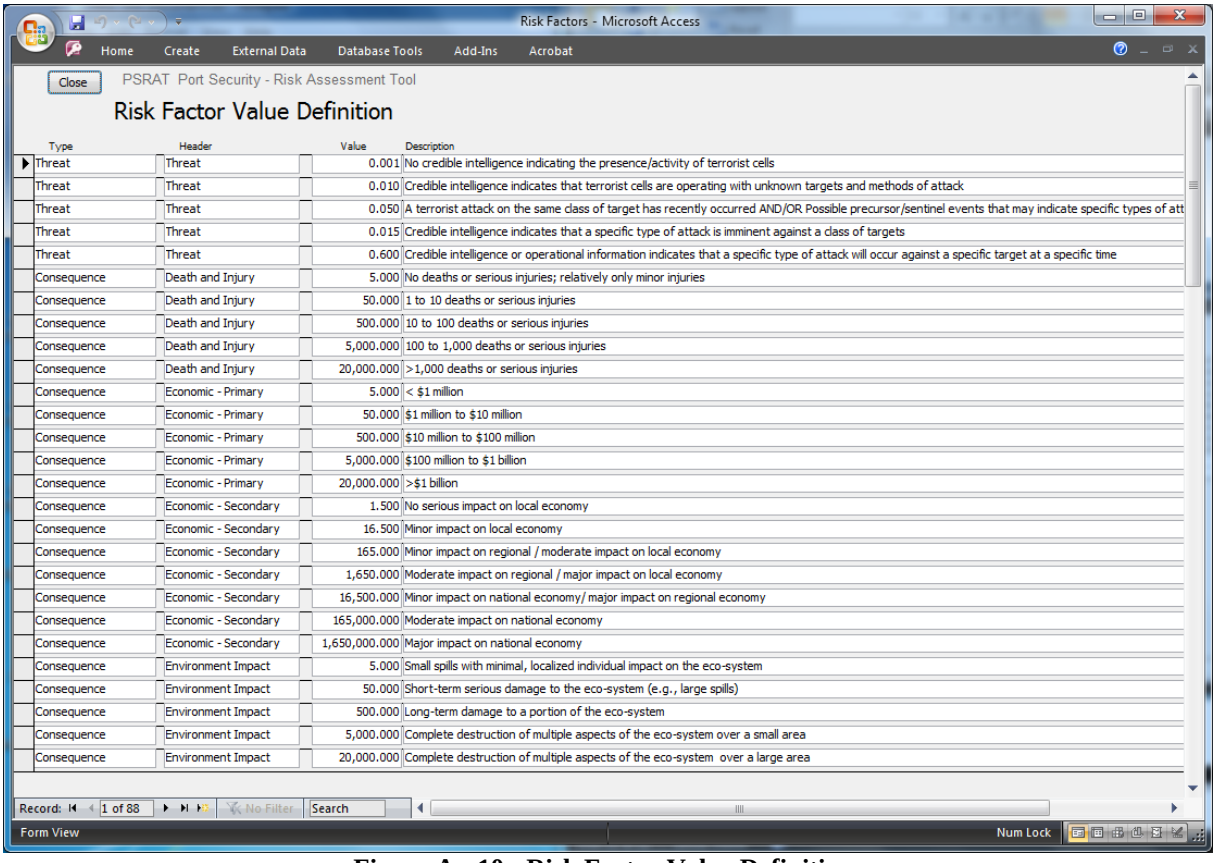
The Risk Categories screen, on the Admin Setup Menu, allows the user to edit, delete, and add risk categories (Figure A-9)



Type	Risk Factor	Risk Factor Description
Consequence	Death and Injury	Expected number of deaths/injuries from a successful attack
Consequence	Economic - Primary	Property damage and immediate business interruption from a successful attack
Consequence	Environment Impact	Impact to the environment of a successful attack
Consequence	National Defense	Impact on national defense of a successful attack
Consequence	Symbolic Effect	Symbolic impact of a successful attack
Threat	Threat	Threat is the likelihood of an attempted attack. This factor is assessed nationally through the USCG's Intelligence Coordination Center (ICC). Threat is calculated
Vulnerability	Accessibility	Accessibility of the target to a terrorist attack
Vulnerability	Sys Security Owner Operator	Interdiction Probability for Owner Operator, given attack is acheivable
Vulnerability	Target Hardness	Probability that the target would withstand the attack
Vulnerability	Availability	Disponibilidad del objetivo

Figure A - 9 - Risk Factors

The Risk Factor and Valuations screen, on the Admin Setup Menu, allows the user to review, edit, and update the valuations of the various risk factors (**Error! Reference source not found.**A-10).



Type	Header	Value	Description
Threat	Threat	0.001	No credible intelligence indicating the presence/activity of terrorist cells
Threat	Threat	0.010	Credible intelligence indicates that terrorist cells are operating with unknown targets and methods of attack
Threat	Threat	0.050	A terrorist attack on the same class of target has recently occurred AND/OR Possible precursor/sentinel events that may indicate specific types of att
Threat	Threat	0.015	Credible intelligence indicates that a specific type of attack is imminent against a class of targets
Threat	Threat	0.600	Credible intelligence or operational information indicates that a specific type of attack will occur against a specific target at a specific time
Consequence	Death and Injury	5.000	No deaths or serious injuries; relatively only minor injuries
Consequence	Death and Injury	50.000	1 to 10 deaths or serious injuries
Consequence	Death and Injury	500.000	10 to 100 deaths or serious injuries
Consequence	Death and Injury	5,000.000	100 to 1,000 deaths or serious injuries
Consequence	Death and Injury	20,000.000	>1,000 deaths or serious injuries
Consequence	Economic - Primary	5.000	< $1 million
Consequence	Economic - Primary	50.000	$1 million to $10 million
Consequence	Economic - Primary	500.000	$10 million to $100 million
Consequence	Economic - Primary	5,000.000	$100 million to $1 billion
Consequence	Economic - Primary	20,000.000	>$1 billion
Consequence	Economic - Secondary	1.500	No serious impact on local economy
Consequence	Economic - Secondary	16.500	Minor impact on local economy
Consequence	Economic - Secondary	165.000	Minor impact on regional / moderate impact on local economy
Consequence	Economic - Secondary	1,650.000	Moderate impact on regional / major impact on local economy
Consequence	Economic - Secondary	16,500.000	Minor impact on national economy/ major impact on regional economy
Consequence	Economic - Secondary	165,000.000	Moderate impact on national economy
Consequence	Economic - Secondary	1,650,000.000	Major impact on national economy
Consequence	Environment Impact	5.000	Small spills with minimal, localized individual impact on the eco-system
Consequence	Environment Impact	50.000	Short-term serious damage to the eco-system (e.g., large spills)
Consequence	Environment Impact	500.000	Long-term damage to a portion of the eco-system
Consequence	Environment Impact	5,000.000	Complete destruction of multiple aspects of the eco-system over a small area
Consequence	Environment Impact	20,000.000	Complete destruction of multiple aspects of the eco-system over a large area

Figure A - 10 - Risk Factor Value Definition

The Risk Categories screen, on the Admin Setup Menu, allows the user to view and adjust the boundaries for risk values and the corresponding action (**Error! Reference source not found.**A-11).

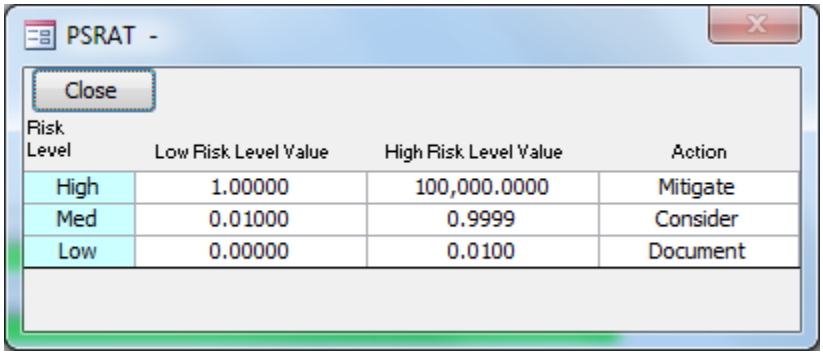


Figure A - 11 - Risk Level Review and Update