

DHS-VISAT-T PRA Screen Shots

Currently the OMB language is located on the third page, which is the fourth page of this document.

The screenshot shows a Windows Internet Explorer browser window displaying the DHS-VISAT-T PRA web application. The address bar shows the URL: <http://topweb.tsa.dhs.gov/risk/SSIRrequest.ser?forward=agree>. The page title is "Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer".

The application header features the "Homeland Security" logo and the title "Vulnerability Self-Assessment Tool". A navigation menu includes: "Vulnerability Assessments", "User Administration", "Profile Administration", "Administration Tool", and "Risk Assessment User Management".

The main content area is titled "Vulnerability Assessments" and includes a "Welcome to Vulnerability Assessments" message. It states: "The Vulnerability Assessment module allows authorized users to perform a detailed analysis of the security posture for a particular entity. Assessments focus on identifying the security issues that may exist for the entity and how to get these issues solved." A prominent warning reads: "Please note that the browser back button may cause problems while using this application. Please use the page navigation buttons instead of the browser's back button to avoid any potential issues." Below this, two instructions are provided:

- Add Assessment- To add a new Vulnerability Assessment, click "Add Assessment" on the left navigation bar.
- Edit or View - To edit or view an existing Vulnerability Assessment, click "Search Assessment" on the left navigation bar.

A left-hand navigation bar contains the following items:

- Vulnerability Assessments
- Add Assessment
- Search Assessments
- Inbox
 - 0 Unstarted
 - 37 Draft
 - 0 Submitted
 - 2 Unresolved
 - 0 Final
 - 0 Archived
 - 6 To Review

The footer of the application includes "U.S. Department of Homeland Security" and "Privacy Policy : Terms Of Use : DHS.gov". A warning at the bottom of the page states: "WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR PART 1520. NO PART OF THIS DOCUMENT MAY BE RELEASED WITHOUT THE WRITTEN PERMISSION OF THE UNDER SECRETARY OF TRANSPORTATION FOR SECURITY, WASHINGTON, DC 20591. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 U.S.C. 552."

The Windows taskbar at the bottom shows the Start button, several open applications (Warning: Sens..., 2 Microsoft..., PRA screen sh..., Microsoft Excel...), a search bar, and the system tray with the time 6:00 PM.

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updateassessment.do?evaluationId=23538821

File Edit View Favorites Tools Help

Share Warning: Sensitive Securi... X

Home : Sitemap

Homeland Security Vulnerability Self-Assessment Tool

Vulnerability Assessments | User Administration | Profile Administration | Administration Tool | Risk Assessment User Management

Vulnerability Assessments

▸ Add Assessment

▸ Search Assessments

Inbox

0	Unstarted
37	Draft
0	Submitted
2	Unresolved
0	Final
0	Archived
6	To Review

1. Select **2. Checklist** **3. Scenarios** **4. Summary**

Select Entity for Vulnerability Assessment

Use the controls below to select the entity for which you wish to perform an assessment. To continue to the next step click the continue button at the bottom of the page or select the second step in the path above.

Please select the entity for which you wish to perform an assessment

U.S. Department of Homeland Security Privacy Policy : Terms Of Use : DHS.gov

WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR PART 1520. NO PART OF THIS DOCUMENT MAY BE RELEASED WITHOUT THE WRITTEN PERMISSION OF THE UNDER SECRETARY OF TRANSPORTATION FOR SECURITY, WASHINGTON, DC 20591. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 U.S.C. 552.

Done Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:04 PM

DHS-VISAT-T PRA Screen Shots

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updateentitydata.do

Vulnerability Assessments | User Administration | Profile Administration | Administration Tool | Risk Assessment User Management

Vulnerability Assessments

1. Select 2. Checklist 3. Scenarios 4. Summary

Mode Instructions

The Department of Homeland Security Vulnerability Identification Self Assessment Tool (DHS-VISAT) is a multi-modal, no cost, web based, vulnerability self-assessment tool. Individual modules support the requirements of different transportation modes and their operations. This particular module addresses the specific requirements for the evaluation of vulnerabilities of the Highway Tunnel Systems.

Process:

- Users answer a list of checklist questions regarding specific security measures in place at the facility. Answer the questions with yes/no or "not applicable" and utilize the textbox to include further comments.
- Users rate the effectiveness of security measures in detecting and preventing a given threat scenario.
- Users list the specific security countermeasures that would be employed to guard against each threat scenario.

The countermeasures are divided into seven, broad countermeasure groupings that represent different security layers; these categories are common for all DHS-VISAT modules developed for the different modes of transportation.

The tool assumes a baseline security posture at the "yellow" threat level, as defined by the Homeland Security Advisory System (HSAS). For each threat scenario, the assessor describes the baseline (yellow threat level) security countermeasures employed. After the user defines the baseline security practices, the tool captures any additional countermeasures deployed in response to increased threat warnings (Orange and Red).

DHS-VISAT also does not incorporate the "black" (under attack) and "purple" (recovering from attack) threat levels used by FTA in their security guidelines, but rather follows the HSAS threat levels. The additional FTA-defined threat levels concern measures taken after an attack has occurred, while the DHS-VISAT tool

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updateentitydata.do

File Edit View Favorites Tools Help

security layers; these categories are common for all DHS-VISAT modules developed for the different modes of transportation.

The tool assumes a baseline security posture at the "yellow" threat level, as defined by the Homeland Security Advisory System (HSAS). For each threat scenario, the assessor describes the baseline (yellow threat level) security countermeasures employed. After the user defines the baseline security practices, the tool captures any additional countermeasures deployed in response to increased threat warnings (Orange and Red).

DHS-VISAT also does not incorporate the "black" (under attack) and "purple" (recovering from attack) threat levels used by FTA in their security guidelines, but rather follows the HSAS threat levels. The additional FTA-defined threat levels concern measures taken after an attack has occurred, while the DHS-VISAT tool addresses pre-attack security preparedness. While the DHS-VISAT tool does not explicitly cover response and recovery planning efforts, all operators are encouraged to plan response and recovery efforts.

Upon completion of the DHS-VISAT tool, users receive a complete report of the assessment. This report will assist personnel in identifying security vulnerabilities and in developing strategies to mitigate these vulnerabilities.

Paperwork Reduction Act Statement of Burden:

Through this information collection, TSA is seeking to assist transportation asset owners/operators in developing a security plan and in performing a vulnerability assessment of their assets. The public burden for this collection of information is estimated to be approximately 8 hours. This is a voluntary collection of information. An agency may not conduct or sponsor, and persons are not required to respond to, a collection of information unless it displays a currently valid OMB control number. The OMB control number assigned to this collection is 1652-0037, which expires 02/28/2009.

[CONTINUE](#)

U.S. Department of Homeland Security Privacy Policy : Terms Of Use : DHS.gov

WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR PART 1520. NO PART OF THIS DOCUMENT MAY BE RELEASED WITHOUT THE WRITTEN PERMISSION OF THE UNDER SECRETARY OF TRANSPORTATION FOR SECURITY, WASHINGTON, DC 20591. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 U.S.C. 552.

Done Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:05 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updateentitydata.do

File Edit View Favorites Tools Help

Search Assessments

Inbox

- 0 Unstarted
- 37 Draft
- 0 Submitted
- 2 Unresolved
- 0 Final
- 0 Archived
- 6 To Review

1. Select **2. Checklist** **3. Scenarios** **4. Summary**

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 1 of 7 Next >

Plans, Policies, and Procedures

1: [Corporate Security Practice] Does the agency's alert system align with the National Homeland Security Alert System? --Select--

2: [Corporate Security Practice] Does the agency have a documented system for processing the flow of threat information? --Select--

3: [Corporate Security Practice] Is the threat information that the agency collects kept on file and assessed periodically? --Select--

4: [Corporate Security Practice] Does the agency conduct vulnerability assessments on its assets? --Select--

5: [Corporate Security Practice] Does the agency have a documented vulnerability assessment program? --Select--

Done

Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:06 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Share Warning: Sensitive Security Information X

0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 2 of 7 < Previous Next >

Training

1: [Corporate Security Practice] Is the training curriculum documented in the security plan? If yes, please elaborate using the comments field. --Select--

2: [Corporate Security Practice] Are drills and training exercises regularly conducted so that personnel can review and practice their security duties and responsibilities? If yes, please describe (using the comments field) how often such exercises occur. (FTA Top 20 -16; suggests that agencies conduct table top exercises at least once every six months and regional drills annually.) --Select--

3: [Corporate Security Practice] Does the agency conduct employee training on security awareness and security plan implementation? If yes, how many do you train each year? --Select--

4: [Corporate Security Practice] Does the agency conduct refresher training on security awareness and security plan implementation? If yes, please elaborate using the comments field. --Select--

5: [Corporate Security Practice] Does the agency use a formal training curriculum? If yes, is it based on a standard, identify in the comments field. --Select--

Done Trusted sites 100%

start Warning: Sens... 2 Microsof... Microsoft Excel... Document1 - M... Search Desktop 6:06 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Search Assessments

Inbox

- 0 Unstarted
- 37 Draft
- 0 Submitted
- 2 Unresolved
- 0 Final
- 0 Archived
- 6 To Review

1. Select **2. Checklist** **3. Scenarios** **4. Summary**

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 3 of 7 < Previous Next >

Cargo, Personnel, and Vehicle Access Control

1: [Corporate Security Practice] Does the security plan identify or define secure areas? If yes, please describe using the comments field. --Select--

2: [Corporate Security Practice] Does the agency provide identification cards to employees? --Select--

3: [Corporate Security Practice] Does the agency provide identification cards to contractor personnel? --Select--

4: [Corporate Security Practice] Does the agency differentiate between levels of access for secure areas? If yes, please describe using the comments field. --Select--

5: [Corporate Security Practice] Does the agency use technology to verify identities when allowing access into secure areas (e.g., biometric identification)? If yes, please

Done

Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:06 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Share Warning: Sensitive Securi... X

0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 4 of 7 < Previous Next >

Physical Security Assets

1: [Corporate Security Practice] Does the agency use surveillance capabilities at its facilities? If yes, please describe in the comments field. --Select--

2: [Corporate Security Practice] Does the agency use guard services/patrols (armed/unarmed contract, LEO, National Guard, USCG)? If yes, please elaborate using the comments field. --Select--

3: [System-wide issue] Are transit agency police officers armed? --Select--

4: [System-wide issue] Does the agency hire contract employees to provide security? If yes, please describe (using the comments field) the force level (number of officers) of the contracted security force. (If no, please answer "n/a" to the next question.) (APTA Baseline Security Checklist) --Select--

5: [System-wide issue] Are private security officers armed? --Select--

Done Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:07 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Share Warning: Sensitive Security Information X

0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 5 of 7 < Previous Next >

Security Technologies and Equipment

1: [Corporate Security Practice] Does the agency use identification card technology to verify employee identities (e.g., photo, chips, biometrics)? If yes, please describe using the comments field. --Select--

2: [Corporate Security Practice] Is your system dependent upon cyber security to function? --Select--

3: [Corporate Security Practice] Does the agency use intrusion detection devices in its buildings? If yes, please describe in the comments field. --Select--

4: [System-wide issue] Does the agency conduct any screening of the station, vehicles, or passengers using scanning/detection equipment or other devices? --Select--

5: [Station-Specific Issue] Does the station have closed-circuit television (CCTV)? If yes, please describe (using the comments field) the technology and how it is used. (FTA Top 20; APTA Baseline Security Checklist) --Select--

6: [Station-Specific Issue] Does the station have --Select--

Done Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:07 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 6 of 7 < Previous Next >

Communications Security

1: [Corporate Security Practice] Does the agency use internal methods to monitor and transmit threat information (e.g. intranet, media, toll-free number)? If yes, please describe these methods in the text box. --Select--

2: [Corporate Security Practice] Does the agency use external resources to monitor and transmit threat information (e.g., state agency, ISAC, FBI, LEO)? If yes, please describe in the text box. --Select--

3: [Corporate Security Practice] Does the agency have a 24/7 emergency response center? --Select--

4: [Corporate Security Practice] Does the agency maintain an updated list of contact information for their personnel? --Select--

5: [Corporate Security Practice] Does the agency have designated personnel to be alerted when the alert-level changes or an incident occurs? If yes, please elaborate using the comments field. --Select--

6: [Corporate Security Practice] Does the agency have --Select--

Done

Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:07 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Share Warning: Sensitive Security Information X

0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

Entity Information

Entity: test4

Vulnerability Assessment Checklist

The completed vulnerability assessment checklist will provide the vulnerability assessor with a snapshot of the assessed entity's current security profile. Additionally, the checklist will provide the vulnerability assessor with useful information that will assist her or him in completing a security plan. The checklist consists of seven sections that contain security-related questions. The vulnerability assessor will answer every question with a 'Yes', 'No', or 'Not Applicable' answer. Additionally, the vulnerability assessor will expound on all answers in the corresponding textbox.

Step 7 of 7 < Previous

Information Security

1: [Corporate Security Practice] Does the agency have a means to receive, disseminate, and store CLASSIFIED information? --Select--

2: [Corporate Security Practice] Does the agency require that employees who have access to the security plan sign non-disclosure agreements? --Select--

3: [Corporate Security Practice] Does the agency have provisions for a system backup, uninterruptible power source, and/or an alternate location? If yes, please elaborate using the comments field. --Select--

4: [Corporate Security Practice] Are the agency's operation systems housed on an isolated network? --Select--

5: [Corporate Security Practice] Does the agency conduct system penetration tests? --Select--

6: [Corporate Security Practice] Does the agency have ...

Done Trusted sites 100%

start Warning: Sens... 2 Microsoft ... Microsoft Excel... Document1 - M... Search Desktop 6:08 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do

File Edit View Favorites Tools Help

Search Assessments

Inbox

- 0 Unstarted
- 37 Draft
- 0 Submitted
- 2 Unresolved
- 0 Final
- 0 Archived
- 6 To Review

1. Select **2. Checklist** **3. Scenarios** **4. Summary**

Entity Information

Entity: test4

Vulnerability Assessment Scenarios

DHS has developed a base set of threat scenarios for each entity category. The base threat scenarios for this category are listed in the box below. In general, threat scenarios represent the starting point for VSAT applications. The user should select a scenario, and then click the 'Work Scenario' button to move to the first VSAT tool application screen. When VSAT has been completely applied against a given threat scenario, the tool will bring the user back to this vulnerability assessment scenario screen. Once a scenario is complete, it will appear in the 'Completed Scenarios' box. At that point, the user should select a different scenario. Users should follow this general procedure until VSAT has been applied against each of the below listed threat scenarios.

Scenarios:

WORK SCENARIO

Completed Scenarios:

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatescenarios.do

File Edit View Favorites Tools Help

Warning: Sensitive Security... X

1. Select 2. Checklist 3. Scenarios 4. Summary

Entity Information

Entity: test4

Vulnerability Assessment Scenario Attractiveness

First, select how attractive the entity is as a target for the scenario. Use the help text link beneath the drop down box for the attractiveness ratings to assist in determining the proper attractiveness rating for the entity. Next, select the consequences rating for each of the five categories listed below that determines how high the consequences are for the scenario occurring at the entity. Again, use the help text link beneath the consequences ratings drop down box to assist in determining the proper consequence ratings for the entity.

Scenario: Passengers leave multiple explosives concealed in backpacks on the transit vehicle(s) entering the station.

Relative Attractiveness

Target --Select--

This category determines the level of destruction, devastation, or disruption caused by a terrorist's successful completion of this threat scenario. For definitions of the ratings, please click [here](#).

Consequences Rating Criteria

Health and Well Being --Select--

This category determines the level of deaths, injuries, illnesses and environmental impact assuming a successful completion of this threat scenario. For definitions of the ratings, please click [here](#).

Economic Impact --Select--

This category assesses the monetary loss resulting from a successful completion of this threat scenario. Determine if the impact expands your immediate geographic area. For definitions of the ratings, please click [here](#).

Loss of Function --Select--

This category determines the impact of losing the function(s) housed at your transportation asset. Determine the volume of traffic flow that would be impeded along with the potential impact on other transportation modes. For definitions of the ratings, please click [here](#).

Reconstitution --Select--

This category assesses the availability of alternatives assuming a successful attack impacts your asset's functionality. Consider the

Done Trusted sites 100%

start Warning... 2 Micro... Microsoft... Documen... untitled - ... Search Desktop 6:12 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatescenarios.do

File Edit View Favorites Tools Help

Inbox
0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review

1. Select 2. Checklist 3. Scenarios 4. Summary

Entity Information

Entity: test4

Vulnerability Assessment Scenario Attractiveness

First, select how attractive the entity is as a target for the scenario. Use the help text link beneath the drop down box for the attractiveness ratings to assist in determining the proper attractiveness rating for the entity. Next, select the consequences rating for each of the five categories listed below that determines how high the consequences are for the scenario occurring at the entity. Again, use the help text link beneath the consequences ratings drop down box to assist in determining the proper consequence ratings for the entity.

Scenario station.

Relative Attractiveness

Target --Select--

This category determines the level of destruction, devastation, or disruption caused by a terrorist's successful completion of this threat scenario. For definitions of the ratings, please click [here](#).

Consequences Rating Criteria

Health and Well Being --Select--

This category determines the level of deaths, injuries, illnesses and environmental impact assuming a successful completion of this threat scenario. For definitions of the ratings, please click [here](#).

Economic Impact --Select--

This category assesses the monetary loss resulting from a successful completion of this threat scenario. Determine if the impact expands your immediate geographic area. For definitions of the ratings, please click [here](#).

Loss of Function --Select--

This category determines the impact of losing the function(s) housed at your transportation asset. Determine the volume of traffic flow that would be impeded along with the potential impact on other transportation modes. For definitions of the ratings, please click [here](#).

Reconstitution --Select--

This category assesses the availability of alternatives assuming a successful attack imparts your asset's functionality. Consider the

Done Trusted sites 100%

start Warning:... 2 Micro... Microsoft... Documen... untitled - ... Search Desktop 6:12 PM

DHS-VISAT-T PRA Screen Shots

The screenshot shows a Windows Internet Explorer browser window with the address bar displaying <http://topweb.tsa.dhs.gov/risk/assessments/updateattractiveness.do>. The page title is "Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer".

The main content area is titled "Vulnerability Assessment Scenario Countermeasures". It contains the following text:

Security countermeasures are grouped into seven distinct categories. Each category represents a distinct layer of security, and is comprised of unique sets of possible countermeasures. Because different countermeasure sets are used to thwart the different threat scenarios, the users are instructed to list the existing countermeasures, per category, within the context of the threat scenario that appears on the "current" screen. The sum of the listed countermeasures listed for each of the threat scenarios defines the entity's baseline security system. Users should rate the baseline effectiveness, per countermeasure category, based on the existing countermeasures and using the descriptive guidance provided when clicking the guidance box.

Below the text is a form with the following elements:

- A "Scenario:" label followed by a text input field containing "station".
- A yellow highlighted section header: "Elevated-Code Yellow".
- A sub-section header: "1. Security Plans, Policies, and Procedures".
- Text: "Rate this countermeasure category within the context of this threat scenario and how effective the facility security plans, policies and procedural countermeasures are in preventing this scenario from happening. Consider each of the plans, policies and procedural countermeasures that you list as comprising your baseline vulnerability. For definitions of the ratings, please click [here](#)."
- A yellow highlighted section header: "Elevated-Code Yellow Security System Effectiveness".
- A "Rating" dropdown menu currently set to "--Select--".
- A section header: "Pre-defined Countermeasures".
- Text: "Please check all pre-defined countermeasures that apply to the countermeasure from the list below."
- A list of 14 checkboxes for pre-defined countermeasures:
 - Pre-Employment Background Checks on Employees
 - Policy/Procedure for Reporting and keeping Record of Security Incidents
 - Policy to Investigate and Manage Threats made against Assets
 - Established Threat and Vulnerability Assessment Process
 - Homeland Security Threat Advisory Levels Integrated into Security Plans
 - Regular Coordination with Outside Security Stakeholders on Implementation of Security Measures (Local and State Police, Fire/Emergency, FBI, ETC.)
 - Continuity of Operations Plan (COOP)
 - Annual Review and Revision of Security Plans
 - Approved Security Plans (Kept In A Secure Location)
 - Approved Security Vulnerability Assessments (Kept In A Secure Location)
 - Designated Facility Security Officer
 - Other Security Policies and Procedures Countermeasures (Describe)
 - Periodic Security Audits
- A section header: "User-defined Countermeasures".
- Text: "Please enter any additional countermeasures that are not listed above in the textbox below."
- A text input field for user-defined countermeasures.

The browser's taskbar at the bottom shows the Start button, several open applications (Warning..., 2 Micro..., Microsoft..., Documen..., untitled - ...), a search bar, and the system tray with the time 6:12 PM.

DHS-VISAT-T PRA Screen Shots

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatecountermeasures.do

File Edit View Favorites Tools Help

Warning: Sensitive Security Information

Severe Alert Level 2 - Code Red

1. Security Plans, Policies, and Procedures

Rate this countermeasure category within the context of this threat scenario and how effective the facility security plans, policies and procedural countermeasures are in preventing this scenario from happening. Consider each of the plans, policies and procedural countermeasures that you list as comprising your response to changing Department of Homeland Security Advisory Levels. For definitions of the ratings, please click [here](#).

Severe Alert Level 2 - Code Red Security System Effectiveness

Rating --Select--

High - Code Orange Security System Effectiveness

Rating --Select--

Elevated-Code Yellow Security System Effectiveness

Rating --Select--

Pre-defined Countermeasures

Please check all pre-defined countermeasures that apply to the countermeasure from the list below.

<input type="checkbox"/> Pre-Employment Background Checks on Employees	<input type="checkbox"/> Annual Review and Revision of Security Plans
<input type="checkbox"/> Policy/Procedure for Reporting and keeping Record of Security Incidents	<input type="checkbox"/> Approved Security Plans (Kept In A Secure Location)
<input type="checkbox"/> Policy to Investigate and Manage Threats made against Assets	<input type="checkbox"/> Approved Security Vulnerability Assessments (Kept In A Secure Location)
<input type="checkbox"/> Established Threat and Vulnerability Assessment Process	<input type="checkbox"/> Designated Facility Security Officer
<input type="checkbox"/> Homeland Security Threat Advisory Levels Integrated into Security Plans	<input type="checkbox"/> Other Security Policies and Procedures Countermeasures (Describe)
<input type="checkbox"/> Regular Coordination with Outside Security Stakeholders on Implementation of Security Measures (Local and State Police, Fire/Emergency, FBI, ETC.)	<input type="checkbox"/> Periodic Security Audits
<input type="checkbox"/> Continuity of Operations Plan (COOP)	

User-defined Countermeasures

Please enter any additional countermeasures that are not listed above in the textbox below.

2. Security Force and Security Awareness Training

Rate this countermeasure category within the context of this threat scenario and how effective the facility training security countermeasures are in preventing this scenario from happening. Consider each of the training countermeasures that you list as comprising your response to changing Department of Homeland Security Advisory Levels. For definitions of the ratings, please click [here](#).

Done Trusted sites 100%

start Warning... 2 Micro... Microsoft... Documen... untitled - ... Search Desktop 6:13 PM

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatescenarios.do

File Edit View Favorites Tools Help

iShare Warning: Sensitive Securi... X

1. Security Plans, Policies, and Procedures
2. Security Force and Security Awareness Training
3. Cargo, Personnel, and Vehicle Access Control
4. Physical Security Assets
5. Security Technologies and Equipment
6. Communications Security
7. Information Security

Elevated-Code Yellow High - Code Orange Severe Alert Level 2 - Code Red

1. Security Plans, Policies, and Procedures
2. Security Force and Security Awareness Training
3. Cargo, Personnel, and Vehicle Access Control
4. Physical Security Assets
5. Security Technologies and Equipment
6. Communications Security
7. Information Security

SAVE SUBMIT FOR REVIEW CANCEL

[Full Summary of Assessment](#)

DHS-VISAT-T PRA Screen Shots

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer

http://topweb.tsa.dhs.gov/risk/assessments/updatescenarios.do

File Edit View Favorites Tools Help

Inbox

- 0 Unstarted
- 37 Draft
- 0 Submitted
- 2 Unresolved
- 0 Final
- 0 Archived
- 6 To Review

1. Select 2. Checklist 3. Scenarios 4. Summary

Vulnerability Assessment Summary

Thank you for entering the vulnerability assessment. The grid below shows a summary of your responses to the scenarios for your assessment. You may either save the assessment without submitting it to the DHS so that it may be further modified, or you may submit the assessment to the DHS by clicking on the buttons on the bottom of the page. The buttons are defined as follows:

Save - The assessment can be saved multiple times and modified based upon additional or new information. The draft version of the checklist and vulnerability assessment will not be accessible by anyone. Once you are satisfied with your assessment, select the "Submit for Review" button for final distribution to DHS.

Submit for Review - Only select this button when you are completely finished with your assessment. The results will be sent to DHS. Any changes you make after this submission will not be reflected in the information maintained by DHS.

	Elevated-Code Yellow	High - Code Orange	Severe Alert Level 2 - Code Red
1. Security Plans, Policies, and Procedures			
2. Security Force and Security Awareness Training			
3. Cargo, Personnel, and Vehicle Access Control			
4. Physical Security Assets			
5. Security Technologies and Equipment			
6. Communications Security			
7. Information Security			

	Elevated-Code Yellow	High - Code Orange	Severe Alert Level 2 - Code Red
1. Security Plans, Policies, and Procedures			
2. Security Force and Security Awareness Training			
3. Cargo, Personnel, and Vehicle Access			

Done

Trusted sites 100%

start Warning:... 2 Micro... Microsoft... Documen... untitled - ... Search Desktop 6:16 PM

DHS-VISAT-T PRA Screen Shots
