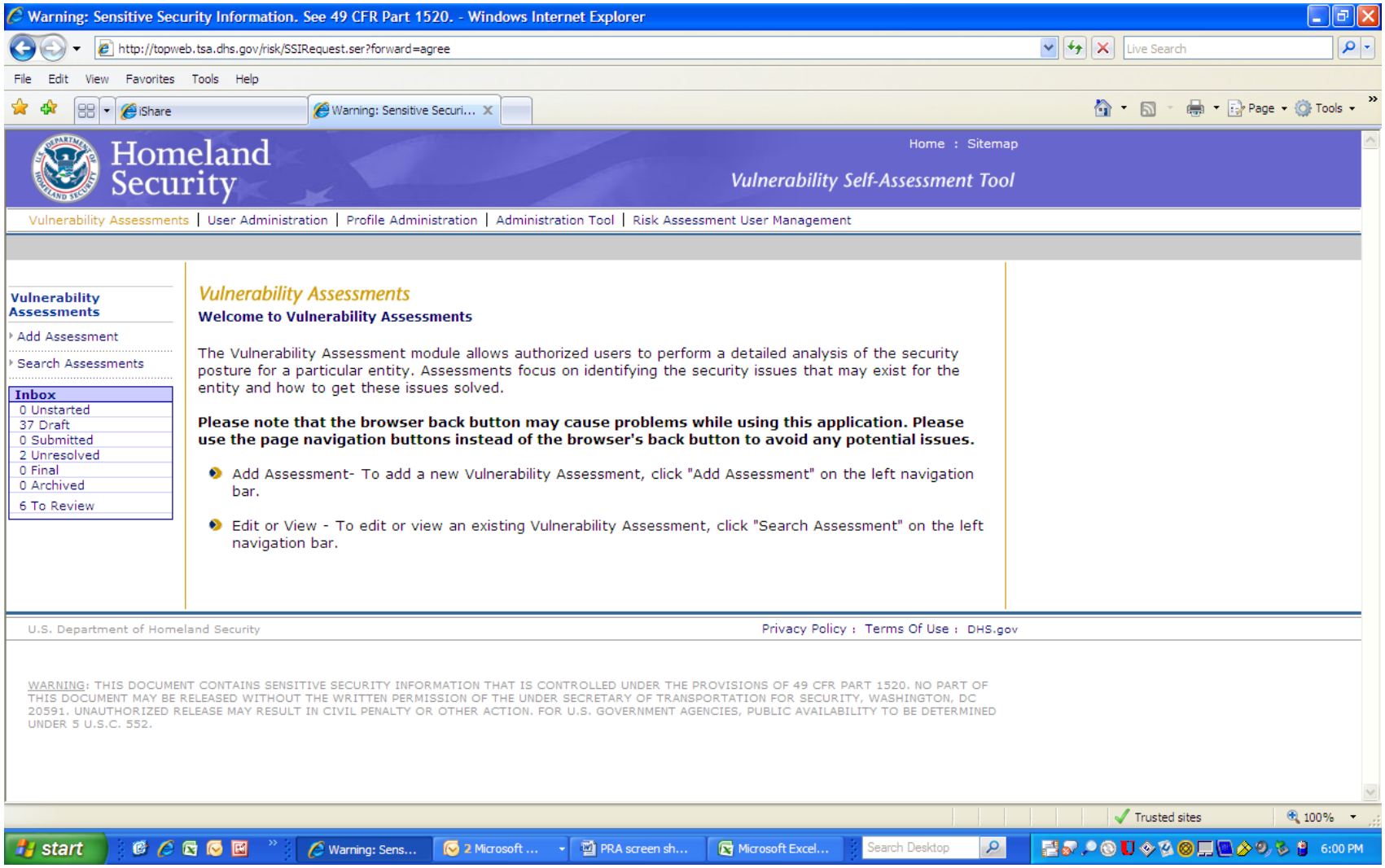
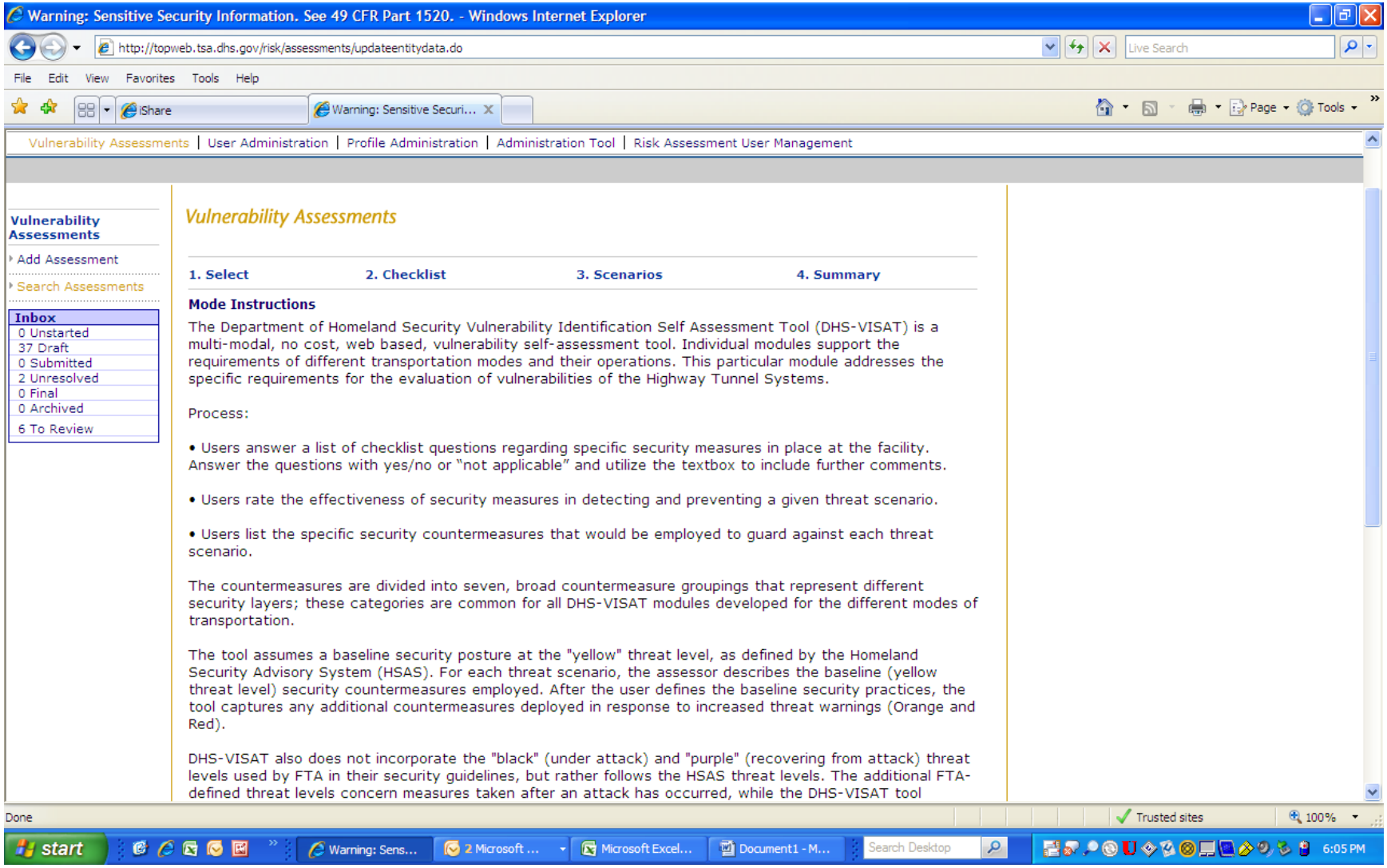
DHS-VISAT-T PRA Screen Shots

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

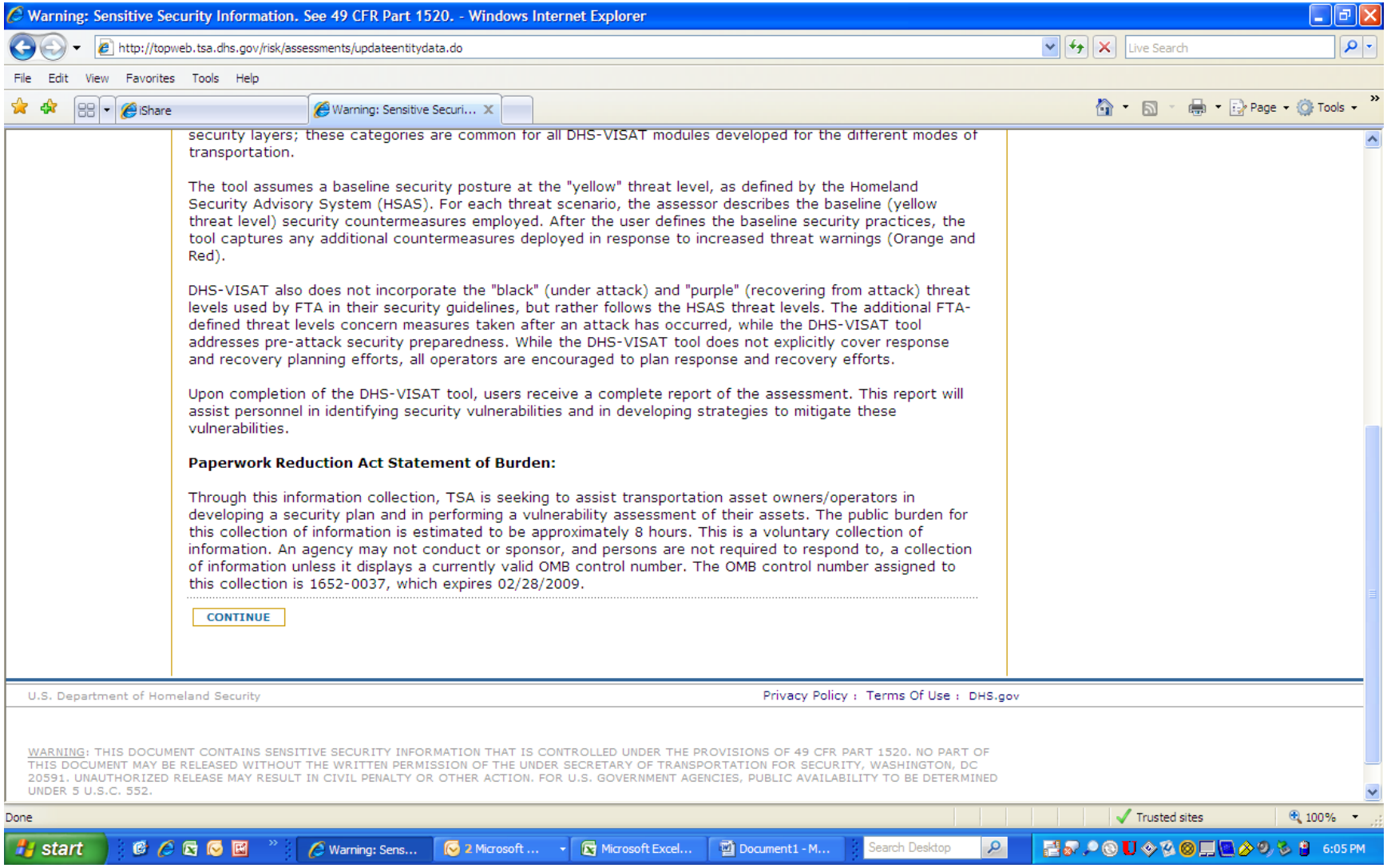


DHS-VISAT-T PRA Screen Shots

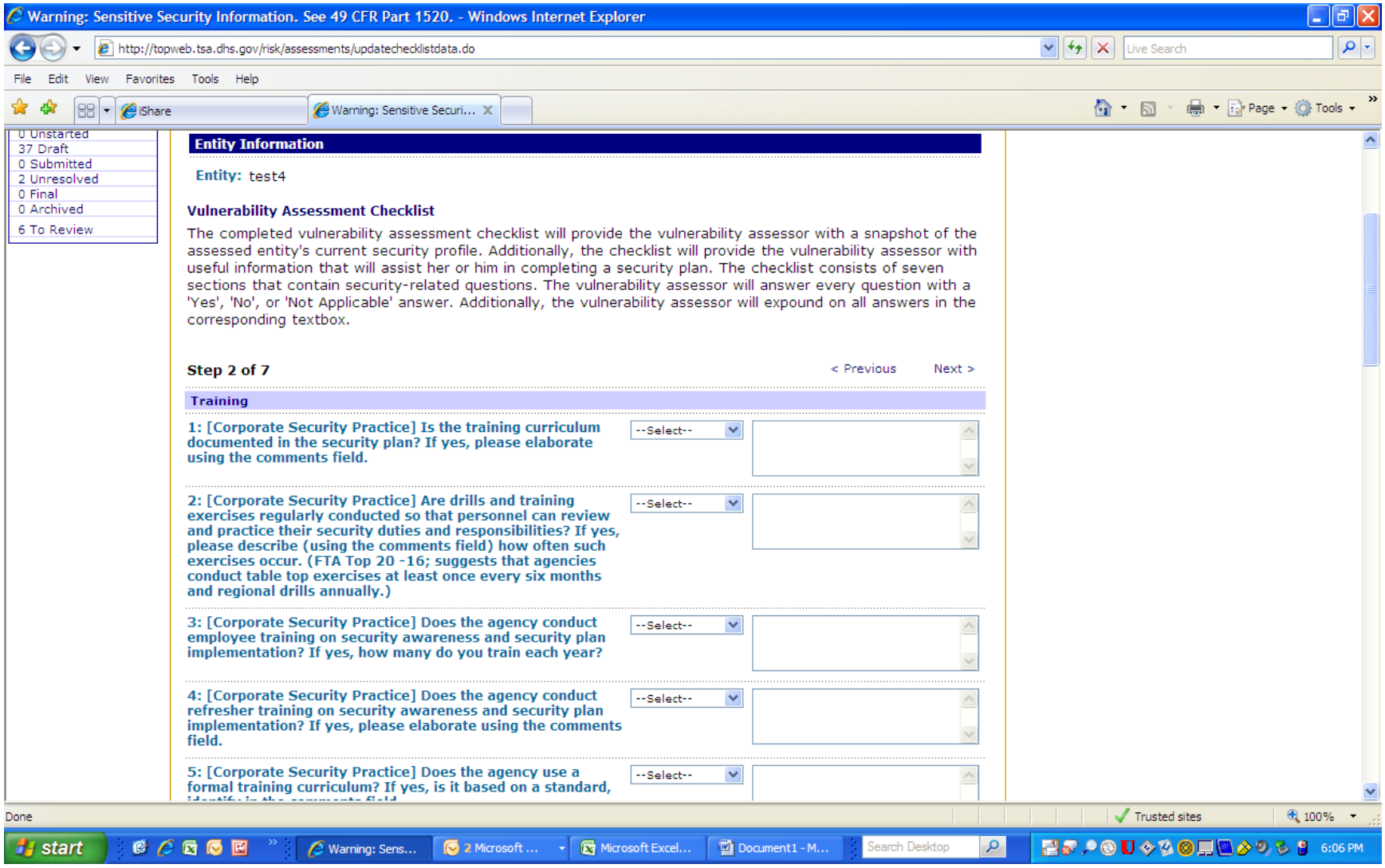
DHS-VISAT-T PRA Screen Shots

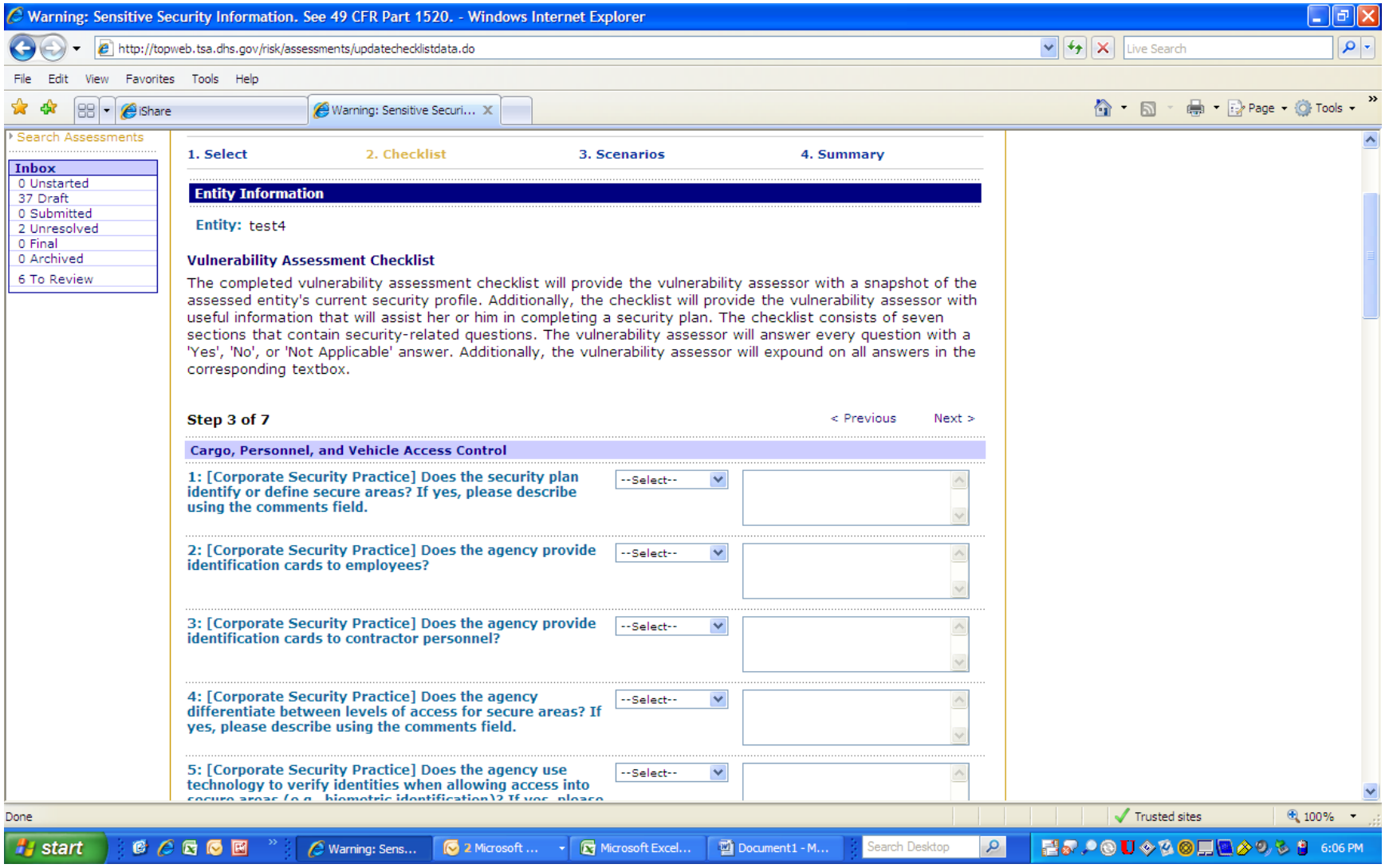


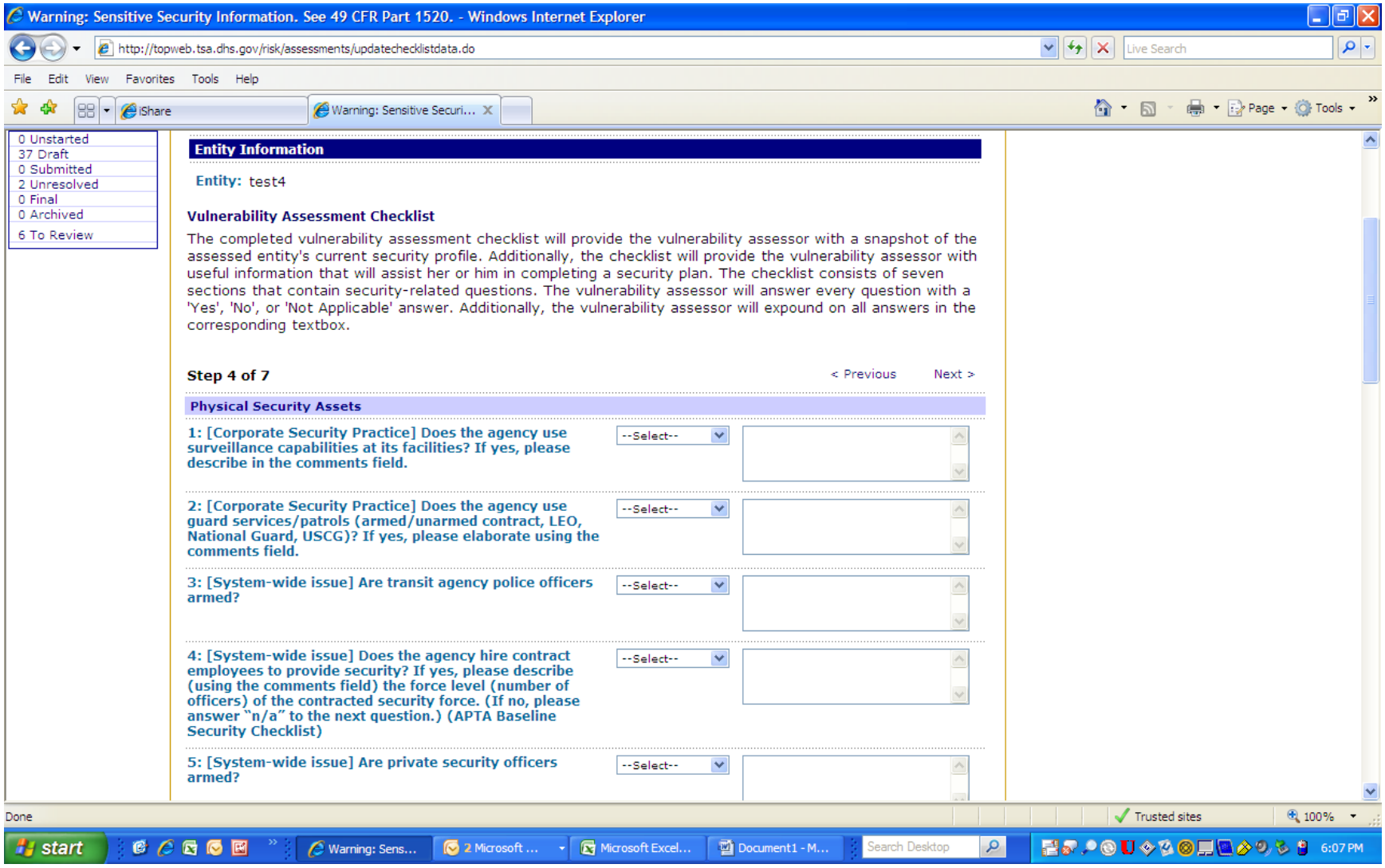
DHS-VISAT-T PRA Screen Shots

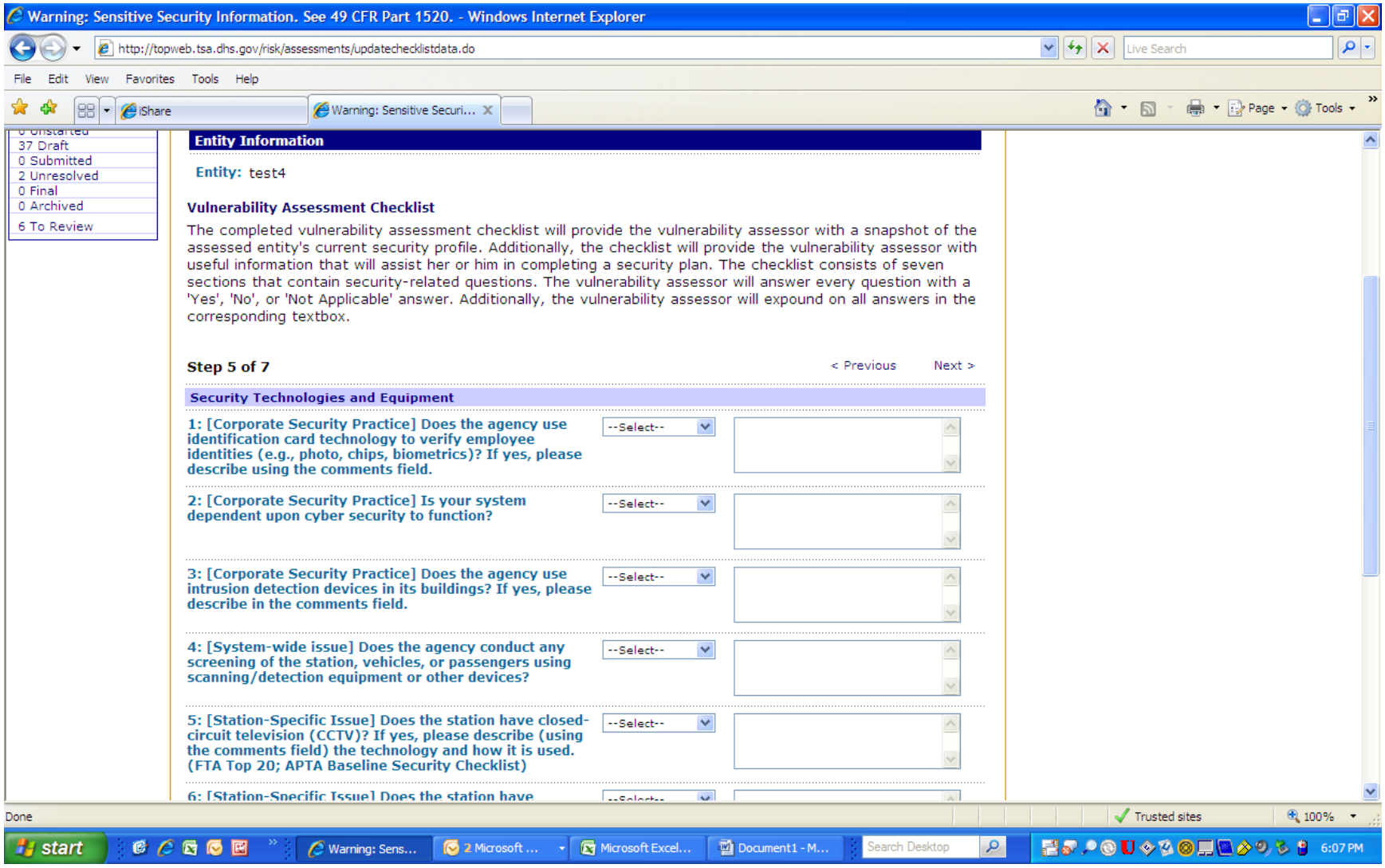



Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updateentitydata.do
File Edit View Favorites Tools Help
Search Assessments
Inbox
0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review
1. Select
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?
2: [Corporate Security Practice] Does the agency have a documented system for processing the flow of threat information?
3: [Corporate Security Practice] Is the threat information that the agency collects kept on file and assessed periodically?
4: [Corporate Security Practice] Does the agency conduct vulnerability assessments on its assets?
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

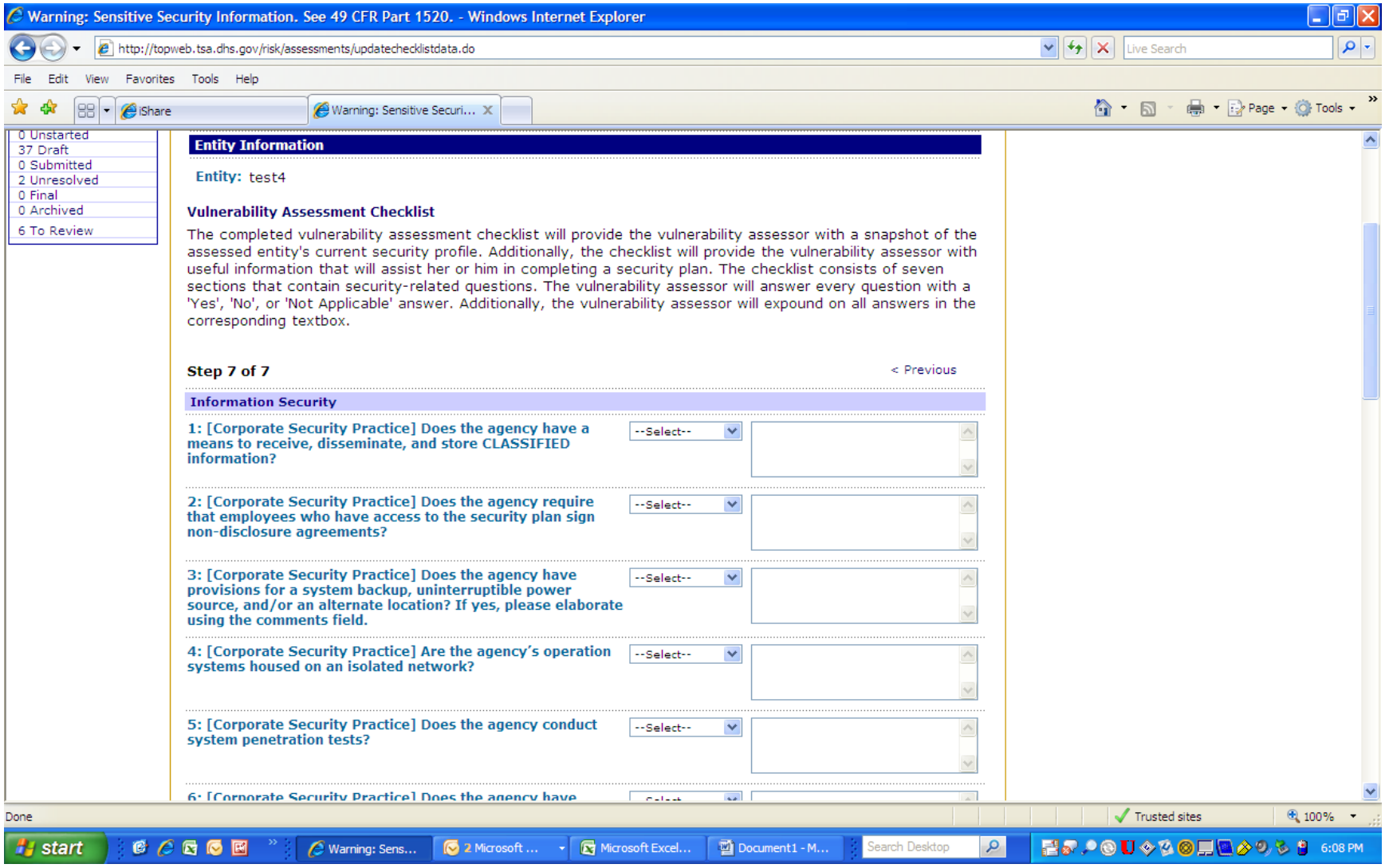

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do
File Edit View Favorites Tools Help
0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review
Entity Information
Entity: test4
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,
--Select--
Done
Trusted sites
100%
start
Warning: Sens...
2 Microsoft ...
Microsoft Excel...
Document1 - M...
Search Desktop
6:06 PM

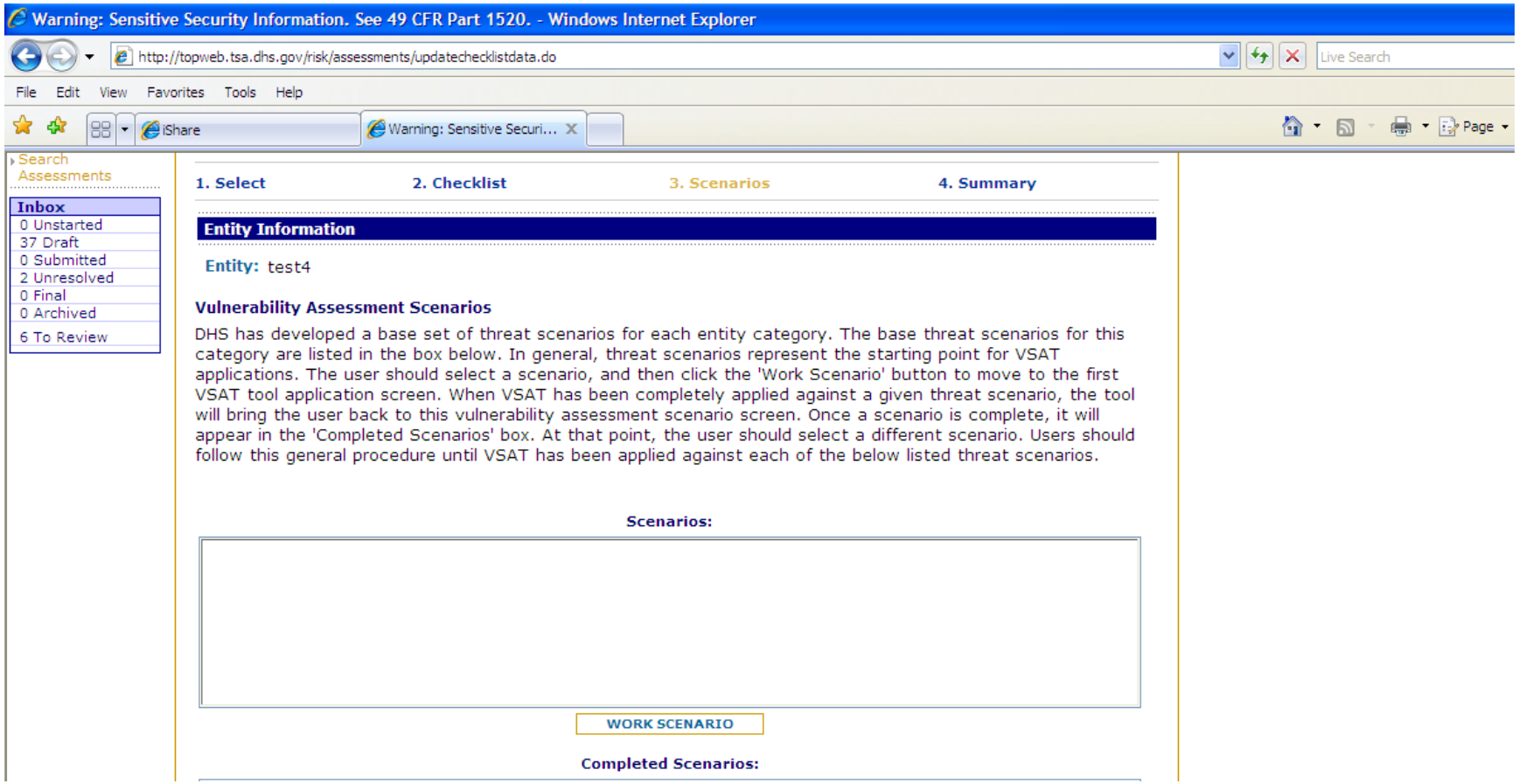

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do
Live Search
File Edit View Favorites Tools Help
iShare
Warning: Sensitive Securi...
Page
Tools
Search Assessments
Inbox
0 Unstarted
37 Draft
0 Submitted
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
--Select--
Done
Trusted sites
100%
start
Warning: Sens...
2 Microsoft ...
Microsoft Excel...
Document1 - M...
Search Desktop
6:06 PM


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
iShare
Warning: Sensitive Securi...
Page Tools
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


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 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--
Done
Trusted sites
100%
start
6:07 PM

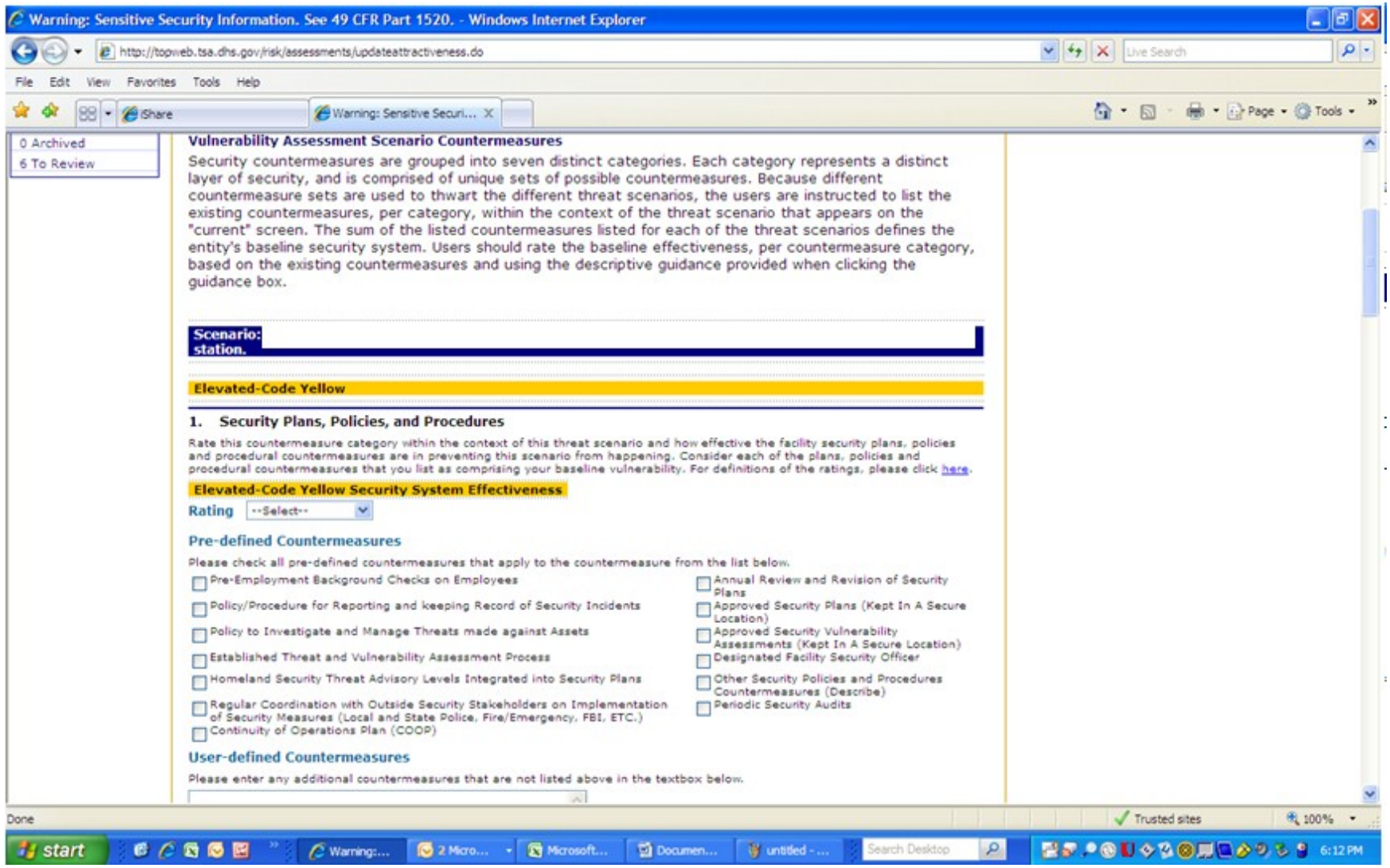

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updatechecklistdata.do
File Edit View Favorites Tools Help
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 To Review
Entity: test4
Vulnerability Assessment Checklist
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.
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.
3: [Corporate Security Practice] Does the agency have a 24/7 emergency response center?
4: [Corporate Security Practice] Does the agency maintain an updated list of contact information for their personnel?
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.
6: [Corporate Security Practice] Does the agency have
--Select--
Done
Trusted sites
100%
start
6:07 PM


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
iShare
Warning: Sensitive Securi...
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--
Done
Trusted sites
100%
start
Warning: Sens...
2 Microsoft ...
Microsoft Excel...
Document1 - M...
Search Desktop
6:08 PM


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
iShare
Warning: Sensitive Securi...
Page
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:

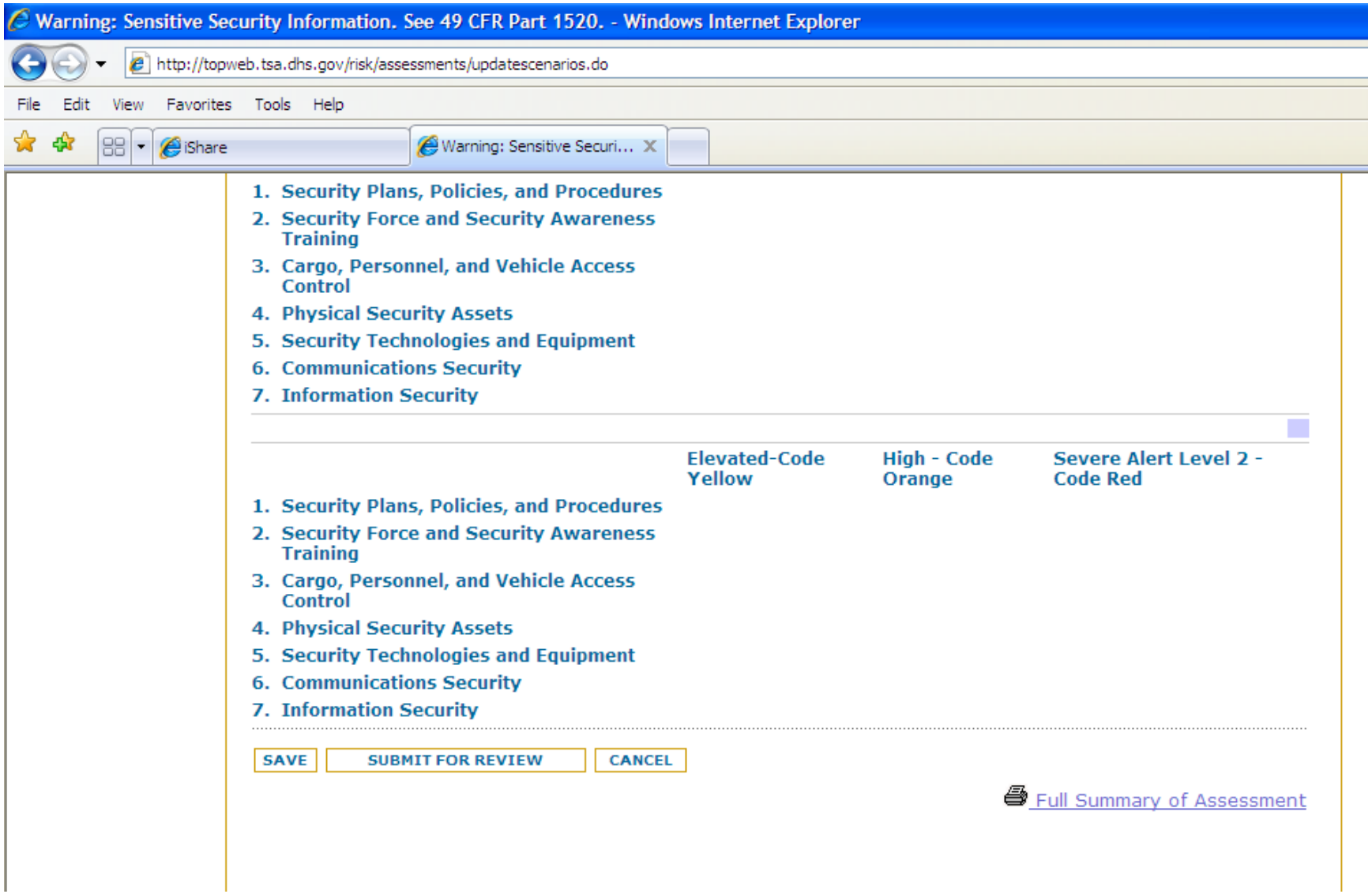
DHS-VISAT-T PRA Screen Shots

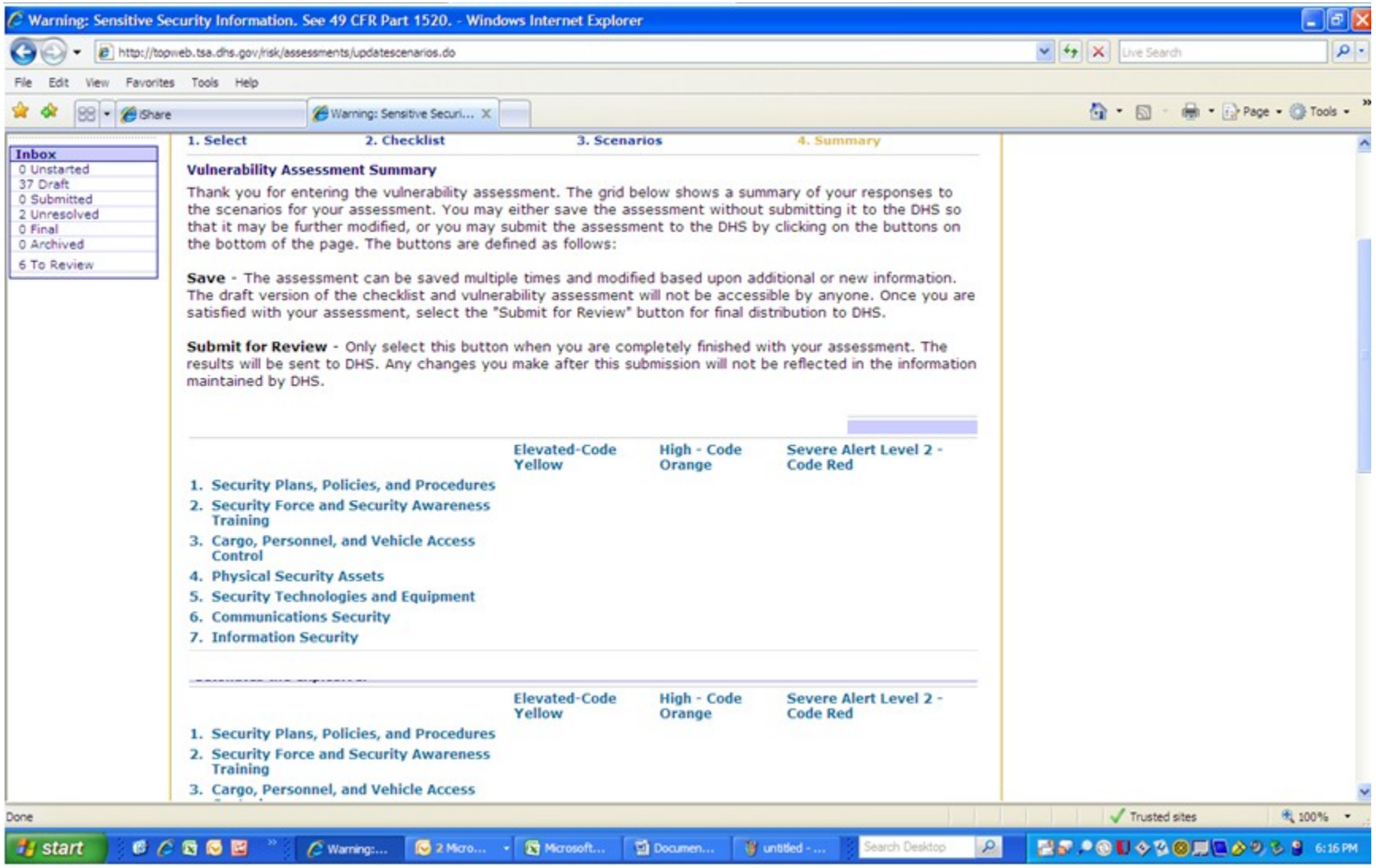

Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updatescenarios.do
File Edit View Favorites Tools Help
Warning: Sensitive Securi...
Page Tools
Inbox
0 Unstarted
37 Draft
0 Submitted
2 Unresolved
0 Final
0 Archived
6 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--
Done
Trusted sites
100%
start
Search Desktop
6:12 PM


Warning: Sensitive Security Information. See 49 CFR Part 1520. - Windows Internet Explorer
http://topweb.tsa.dhs.gov/risk/assessments/updateattractiveness.do
File Edit View Favorites Tools Help
0 Archived
6 To Review
Vulnerability Assessment Scenario Countermeasures
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.
Scenario:
station.
Elevated-Code Yellow
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 baseline vulnerability. For definitions of the ratings, please click here.
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.
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
User-defined Countermeasures
Please enter any additional countermeasures that are not listed above in the textbox below.
Done
Trusted sites
100%
start
6:12 PM


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
0 Final
0 Archived
6 To Review
Vulnerability Assessment Scenario Countermeasures
Users are required to re-visit each of the threat scenarios and list additional countermeasures or enhancements to existing countermeasures that can be applied in the case of a general increase in the national threat level. It is intended that the listed enhanced countermeasures will increase the security effectiveness rating compared to the baseline effectiveness ratings. These countermeasures should be included in a security plan along with estimated resource requirements and timeframes for implementation.
Scenario:
station.
High - Code Orange
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.
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.
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
User-defined Countermeasures
Please enter any additional countermeasures that are not listed above in the textbox below.
Done
Trusted sites
100%
start
6:13 PM


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
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.
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
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


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...
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


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
6:16 PM