EPRM
Enterprise Protection
Risk Management

DoD Counter Insider User Guide

EPRM v3.40, February 2021

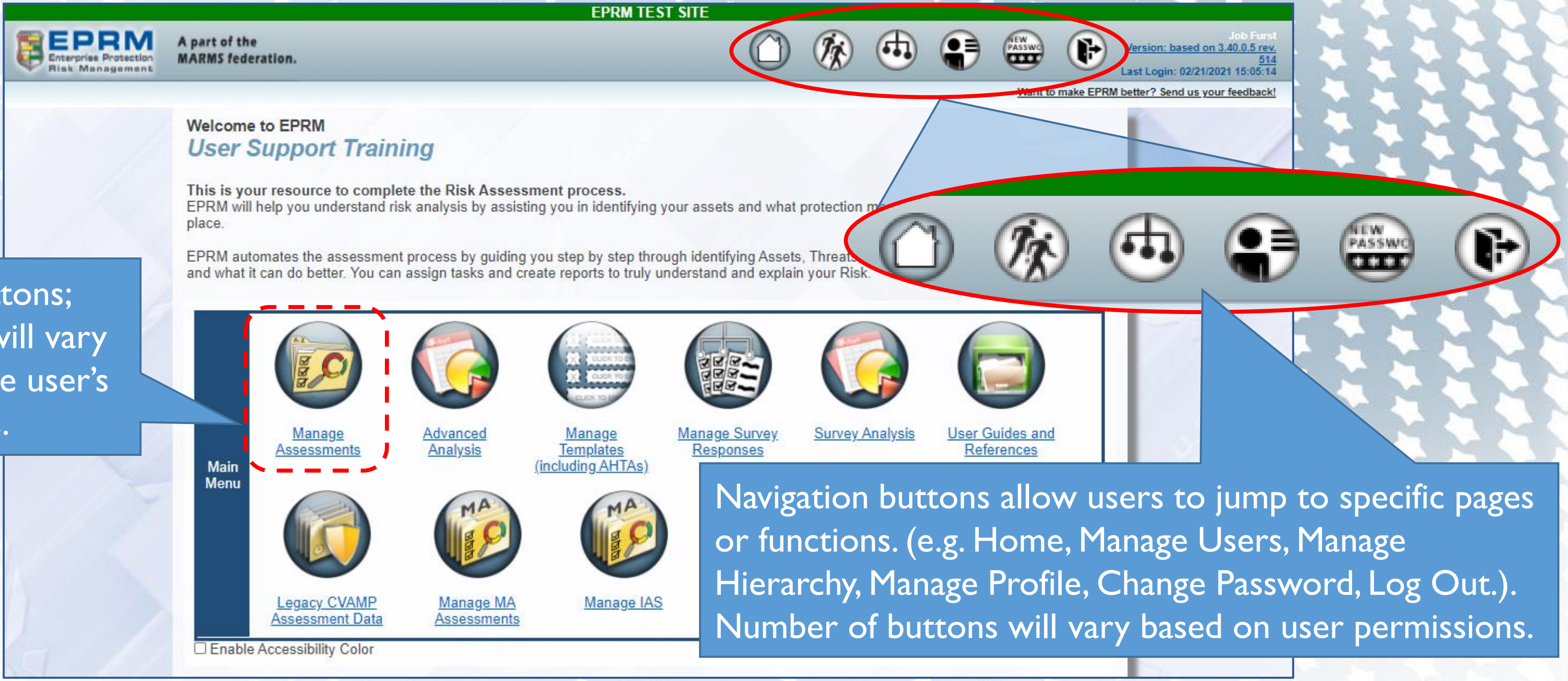
EPRM User Support: eprmhelp@alionscience.com
1.800.754.4204

Introduction

The DoD Component Counter Insider Threat module of EPRM is a quarterly requirement to evaluate the implementation and effectiveness of component insider threat programs. The assessment tool provides components the ability to assess gaps across multiple capabilities to help make informed decisions on where to best allocate resources. EPRM can also be used by each component to generate a variety of report documents, analysis spreadsheets, and presentations based on each individual assessment. Self-assessment data from all DoD Components, including those components that are at FOC, is summarized and reported annually to the Department's Senior Official and OUSD(I). It is our intent that the information can also be used to meet the component's internal requirement to report annually to their Senior Official.

User Home Screen

The user's home screen appears like the image below. The activity buttons compartmentalize various functions that are explained in greater detail in other user guides. Before beginning a new assessment, user's must first click on the **Manage Assessments** button to access the Manage Assessments Home page.



EPRM TEST SITE

EPRM Enterprise Protection Risk Management

A part of the MARMS federation.

Job Furst
Version: based on 3.40.0.5 rev. 514
Last Login: 02/21/2021 15:05:14

Want to make EPRM better? Send us your feedback!

Welcome to EPRM

User Support Training

This is your resource to complete the Risk Assessment process.
EPRM will help you understand risk analysis by assisting you in identifying your assets and what protection m
place.

EPRM automates the assessment process by guiding you step by step through identifying Assets, Threat
and what it can do better. You can assign tasks and create reports to truly understand and explain your Risk.

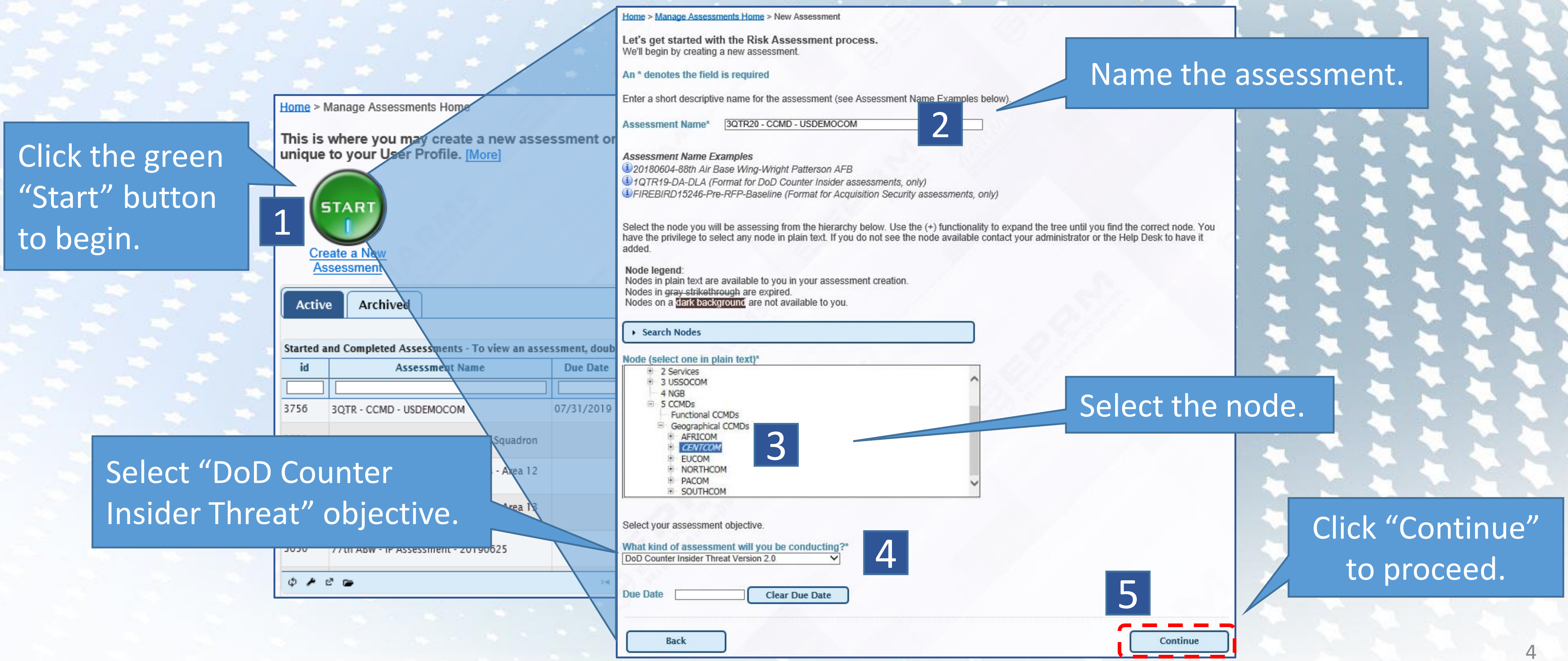
☐ Enable Accessibility Color

Activity Buttons; availability will vary based on the user's permissions.

Navigation buttons allow users to jump to specific pages or functions. (e.g. Home, Manage Users, Manage Hierarchy, Manage Profile, Change Password, Log Out.). Number of buttons will vary based on user permissions.

Creating a DoD Counter InT Assessment

From the Manage Assessments Home page, users should click the “Start” button to initiate a new assessment. On the New Assessment screen that opens, fields denoted by an asterisk (*) must be completed (numbered below). All new assessments must follow the naming convention detailed on **page 14** of this guide: Reporting Period-Component Category-Agency/Service abbreviation.



Click the green “Start” button to begin.

1

Home > Manage Assessments Home

This is where you may create a new assessment or unique to your User Profile. [More]

Create a New Assessment

Active | Archived

Started and Completed Assessments - To view an assessment, doub

id	Assessment Name	Due Date
3756	3QTR - CCMD - USDEMOCOM	07/31/2019
	Squadron	
	- Area 12	
	Area 13	
3030	77th ABW - IP Assessment - 20190625	

Home > Manage Assessments Home > New Assessment

Let's get started with the Risk Assessment process.
We'll begin by creating a new assessment.

An * denotes the field is required

Enter a short descriptive name for the assessment (see Assessment Name Examples below).

Name the assessment.

2

Assessment Name* 3QTR20 - CCMD - USDEMOCOM

Assessment Name Examples
20180604-88th Air Base Wing-Wright Patterson AFB
1QTR19-DA-DLA (Format for DoD Counter Insider assessments, only)
FIREBIRD15246-Pre-RFP-Baseline (Format for Acquisition Security assessments, only)

Select the node you will be assessing from the hierarchy below. Use the (+) functionality to expand the tree until you find the correct node. You have the privilege to select any node in plain text. If you do not see the node available contact your administrator or the Help Desk to have it added.

Node legend:
Nodes in plain text are available to you in your assessment creation.
Nodes in ~~gray strikethrough~~ are expired.
Nodes on a dark background are not available to you.

Node (select one in plain text)*

- 2 Services
- 3 USSOCOM
- 4 NGB
- 5 CCMDs
  - Functional CCMDs
  - Geographical CCMDs
    - AFRICOM
    - CENTCOM
    - EUCOM
    - NORTHCOM
    - PACOM
    - SOUTHCOM

Select the node.

3

Select your assessment objective.

What kind of assessment will you be conducting?* DoD Counter Insider Threat Version 2.0

Select “DoD Counter Insider Threat” objective.

4

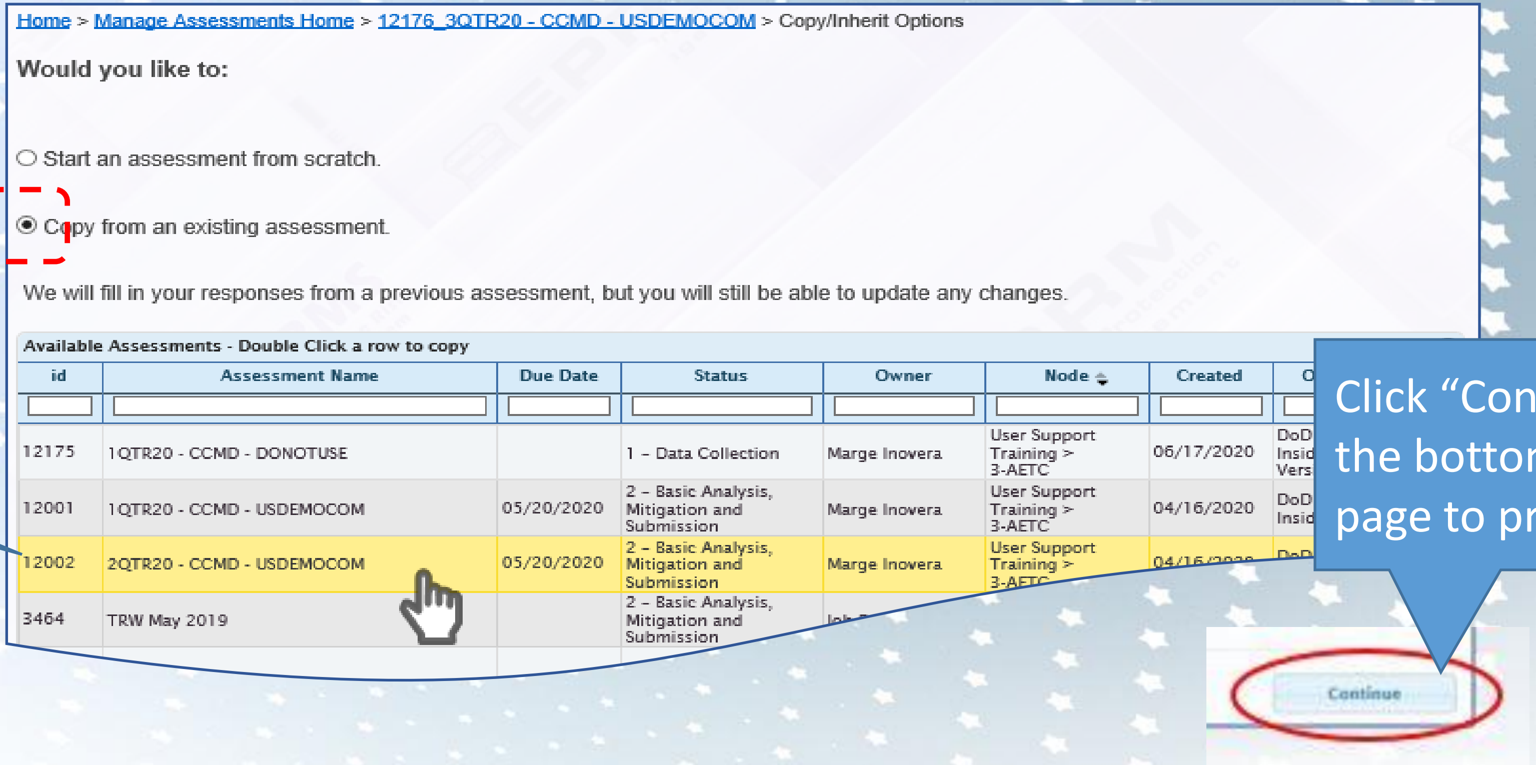
Due Date

5

Click “Continue” to proceed.

Creating a DoD Counter InT Assessment—cont’d

The next screen to appear is dependent on previous EPRM experience/contact. A first-time user will be taken directly to the “Describe the organization” page (***page 6***). Other users will see the option page shown below. This page will display if users have created at least one previous assessment; if they had an assessment shared with them, or ownership of an assessment was transferred to them. Copying from a previous assessment reduces the amount of data entry required for recurring assessments.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > Copy/Inherit Options

Would you like to:

○ Start an assessment from scratch.

● Copy from an existing assessment.

We will fill in your responses from a previous assessment, but you will still be able to update any changes.

Available Assessments - Double Click a row to copy

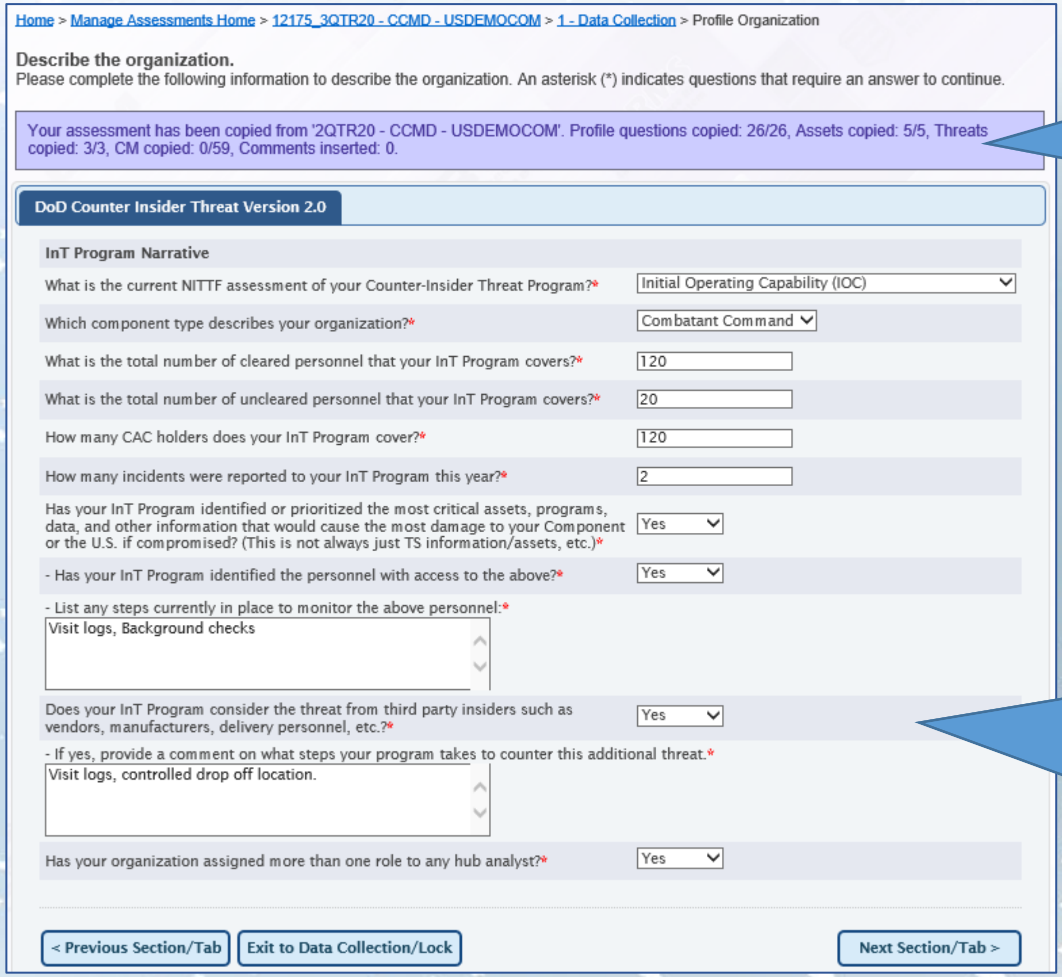
id	Assessment Name	Due Date	Status	Owner	Node	Created	O
12175	1QTR20 - CCMD - DONOTUSE		1 – Data Collection	Marge Inovera	User Support Training > 3-AETC	06/17/2020	DoD Insid Vers
12001	1QTR20 - CCMD - USDEMOCOM	05/20/2020	2 – Basic Analysis, Mitigation and Submission	Marge Inovera	User Support Training > 3-AETC	04/16/2020	DoD Insid
12002	2QTR20 - CCMD - USDEMOCOM	05/20/2020	2 – Basic Analysis, Mitigation and Submission	Marge Inovera	User Support Training > 3-AETC	04/16/2020	DoD
3464	TRW May 2019		2 – Basic Analysis, Mitigation and Submission	Joh			

Last quarter’s assessment.

Click “Continue” at the bottom of the page to proceed.

Creating a DoD Counter InT Assessment—cont’d

For new users with no previous assessments this page will automatically appear. For other users, it will appear after the Copy From option discussed above. This page is the first step in conducting the assessment and begins the question process to characterize the organization being assessed.



Home > Manage Assessments Home > 12175_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > Profile Organization

Describe the organization.
Please complete the following information to describe the organization. An asterisk (*) indicates questions that require an answer to continue.

Your assessment has been copied from '2QTR20 - CCMD - USDEMOCOM'. Profile questions copied: 26/26, Assets copied: 5/5, Threats copied: 3/3, CM copied: 0/59, Comments inserted: 0.

DoD Counter Insider Threat Version 2.0

InT Program Narrative

What is the current NITTF assessment of your Counter-Insider Threat Program?*	Initial Operating Capability (IOC)
Which component type describes your organization?*	Combatant Command
What is the total number of cleared personnel that your InT Program covers?*	120
What is the total number of uncleared personnel that your InT Program covers?*	20
How many CAC holders does your InT Program cover?*	120
How many incidents were reported to your InT Program this year?*	2
Has your InT Program identified or prioritized the most critical assets, programs, data, and other information that would cause the most damage to your Component or the U.S. if compromised? (This is not always just TS information/assets, etc.)*	Yes
- Has your InT Program identified the personnel with access to the above?*	Yes

- List any steps currently in place to monitor the above personnel:*
Visit logs, Background checks

Does your InT Program consider the threat from third party insiders such as vendors, manufacturers, delivery personnel, etc.?*	Yes

- If yes, provide a comment on what steps your program takes to counter this additional threat.*
Visit logs, controlled drop off location.

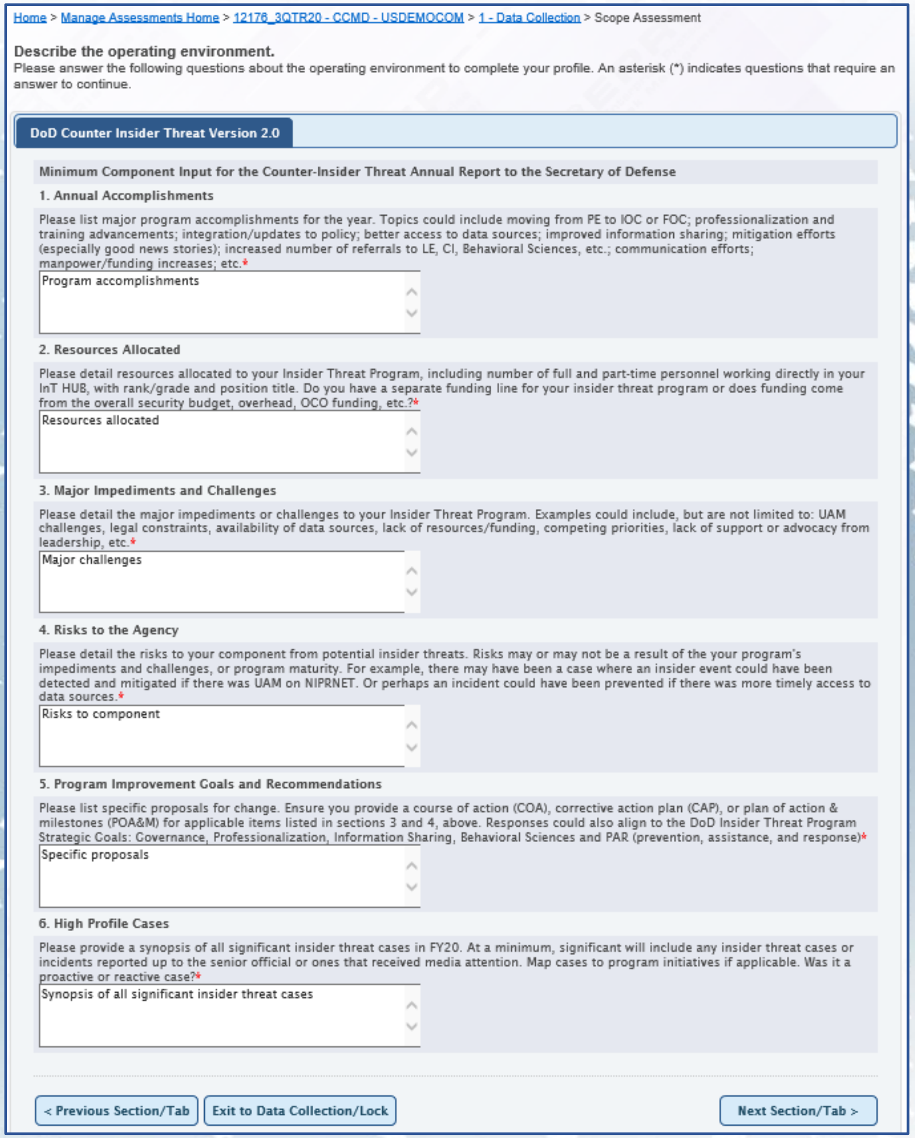
Has your organization assigned more than one role to any hub analyst?*	Yes

This banner confirms data was copied from previous assessment.

Note: The user is able to modify any prefilled answers copied from the previous assessment if conditions have changed.

Creating a DoD Counter InT Assessment—cont’d

The Scope Assessment page is used to describe the operating environment to complete the profile. Provide details of the organization’s Annual Accomplishments, Resources Allocated, Major Impediments and Challenges, Risks to the Agency, Program Improvement Goals and Recommendations, and High Profile Cases.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > Scope Assessment

Describe the operating environment.
Please answer the following questions about the operating environment to complete your profile. An asterisk (*) indicates questions that require an answer to continue.

Minimum Component Input for the Counter-Insider Threat Annual Report to the Secretary of Defense

1. Annual Accomplishments

Please list major program accomplishments for the year. Topics could include moving from PE to IOC or FOC; professionalization and training advancements; integration/updates to policy; better access to data sources; improved information sharing; mitigation efforts (especially good news stories); increased number of referrals to LE, CI, Behavioral Sciences, etc.; communication efforts; manpower/funding increases; etc.*

Program accomplishments

2. Resources Allocated

Please detail resources allocated to your Insider Threat Program, including number of full and part-time personnel working directly in your InT HUB, with rank/grade and position title. Do you have a separate funding line for your insider threat program or does funding come from the overall security budget, overhead, OCO funding, etc.?*

Resources allocated

3. Major Impediments and Challenges

Please detail the major impediments or challenges to your Insider Threat Program. Examples could include, but are not limited to: UAM challenges, legal constraints, availability of data sources, lack of resources/funding, competing priorities, lack of support or advocacy from leadership, etc.*

Major challenges

4. Risks to the Agency

Please detail the risks to your component from potential insider threats. Risks may or may not be a result of the your program's impediments and challenges, or program maturity. For example, there may have been a case where an insider event could have been detected and mitigated if there was UAM on NIPRNET. Or perhaps an incident could have been prevented if there was more timely access to data sources.*

Risks to component

5. Program Improvement Goals and Recommendations

Please list specific proposals for change. Ensure you provide a course of action (COA), corrective action plan (CAP), or plan of action & milestones (POA&M) for applicable items listed in sections 3 and 4, above. Responses could also align to the DoD Insider Threat Program Strategic Goals: Governance, Professionalization, Information Sharing, Behavioral Sciences and PAR (prevention, assistance, and response)*

Specific proposals

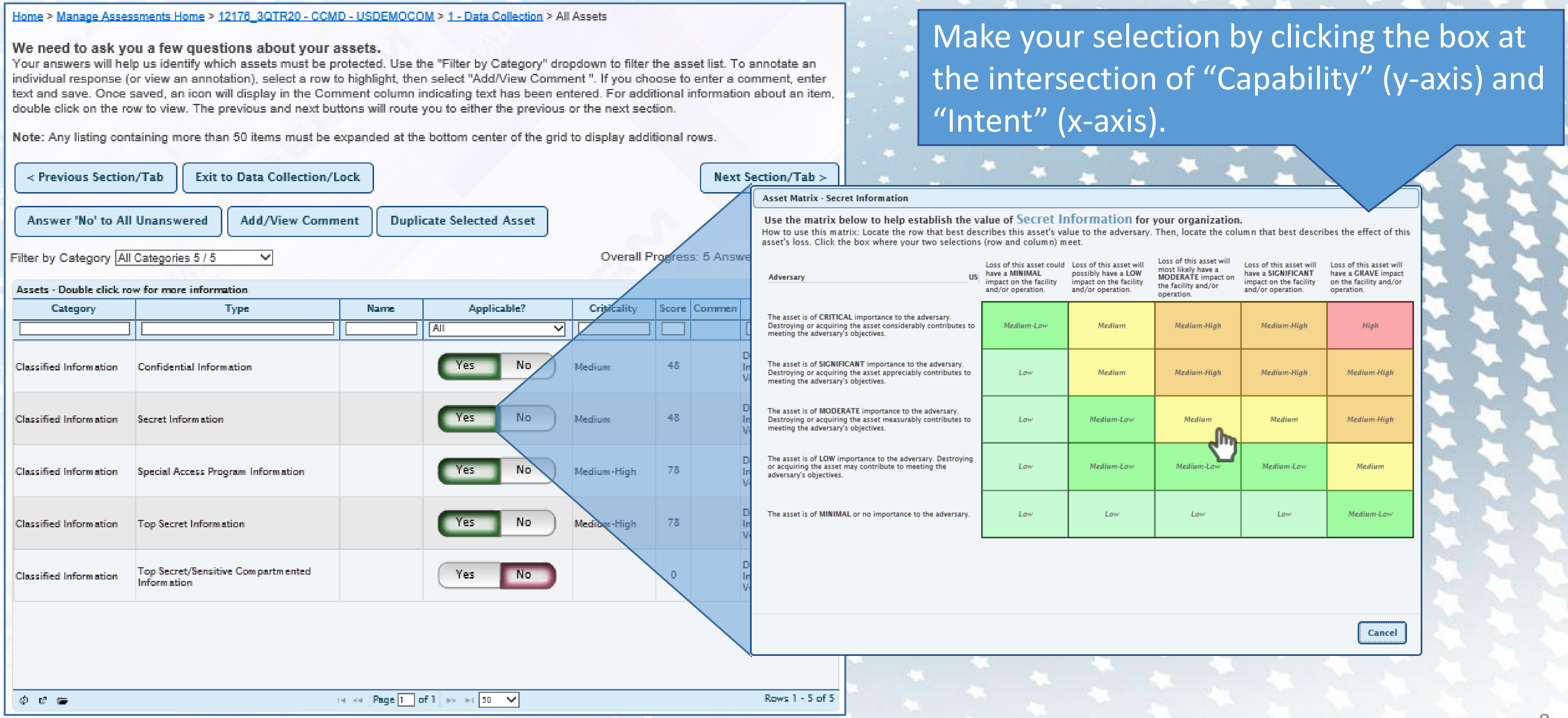
6. High Profile Cases

Please provide a synopsis of all significant insider threat cases in FY20. At a minimum, significant will include any insider threat cases or incidents reported up to the senior official or ones that received media attention. Map cases to program initiatives if applicable. Was it a proactive or reactive case?*

Synopsis of all significant insider threat cases

Creating a DoD Counter InT Assessment—cont’d

Confirm answers from a copied assessment are correct or make new selections. All “yes” answers require users to establish the asset’s value. Use the valuation matrix to assign the asset’s criticality.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > All Assets

We need to ask you a few questions about your assets.
Your answers will help us identify which assets must be protected. Use the "Filter by Category" dropdown to filter the asset list. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment ". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you to either the previous or the next section.

Note: Any listing containing more than 50 items must be expanded at the bottom center of the grid to display additional rows.

Filter by Category: All Categories 5 / 5

Overall Progress: 5 Answe

Assets - Double click row for more information

Category	Type	Name	Applicable?	Criticality	Score	Commen
			All			
Classified Information	Confidential Information		[✓ Yes] No	Medium	48	
Classified Information	Secret Information		[✓ Yes] No	Medium	48	
Classified Information	Special Access Program Information		[✓ Yes] No	Medium-High	78	
Classified Information	Top Secret Information		[✓ Yes] No	Medium-High	78	
Classified Information	Top Secret/Sensitive Compartmented Information		Yes [✓ No]		0	

Make your selection by clicking the box at the intersection of “Capability” (y-axis) and “Intent” (x-axis).

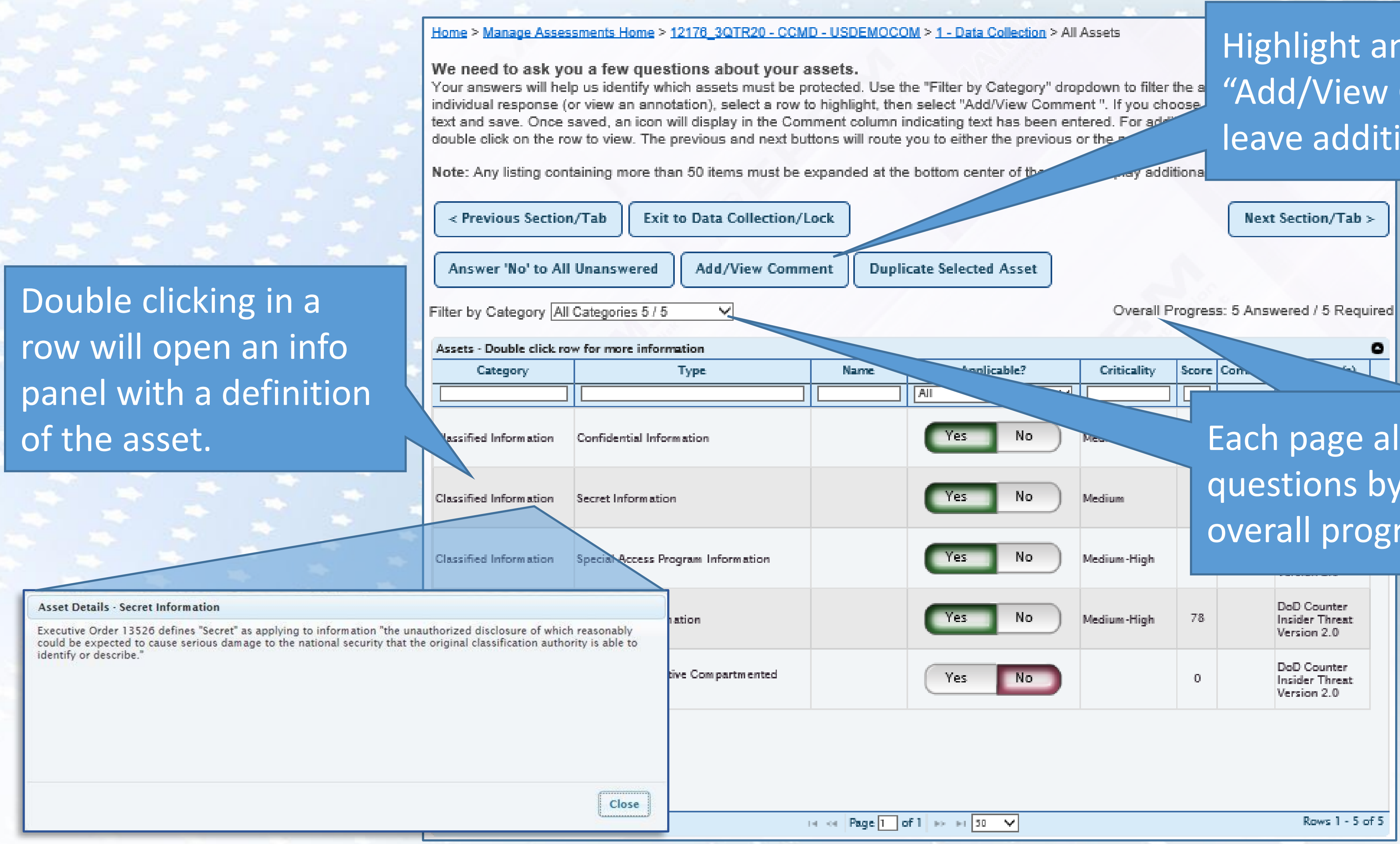
Asset Matrix - Secret Information

Use the matrix below to help establish the value of Secret Information for your organization.
How to use this matrix: Locate the row that best describes this asset's value to the adversary. Then, locate the column that best describes the effect of this asset's loss. Click the box where your two selections (row and column) meet.

Adversary US	Loss of this asset could have a **MINIMAL** impact on the facility and/or operation.	Loss of this asset will possibly have a **LOW** impact on the facility and/or operation.	Loss of this asset will most likely have a **MODERATE** impact on the facility and/or operation.	Loss of this asset will have a **SIGNIFICANT** impact on the facility and/or operation.	Loss of this asset will have a **GRAVE** impact on the facility and/or operation.
The asset is of **CRITICAL** importance to the adversary. Destroying or acquiring the asset considerably contributes to meeting the adversary's objectives.	*Medium-Low*	*Medium*	*Medium-High*	*Medium-High*	*High*
The asset is of **SIGNIFICANT** importance to the adversary. Destroying or acquiring the asset appreciably contributes to meeting the adversary's objectives.	*Low*	*Medium*	*Medium-High*	*Medium-High*	*Medium-High*
The asset is of **MODERATE** importance to the adversary. Destroying or acquiring the asset measurably contributes to meeting the adversary's objectives.	*Low*	*Medium-Low*	*Medium*	*Medium*	*Medium-High*
The asset is of **LOW** importance to the adversary. Destroying or acquiring the asset may contribute to meeting the adversary's objectives.	*Low*	*Medium-Low*	*Medium-Low*	*Medium-Low*	*Medium*
The asset is of **MINIMAL** or no importance to the adversary.	*Low*	*Low*	*Low*	*Low*	*Medium-Low*

Additional Features

Shown here are additional functions, including an information panel on each asset row to help the user determine if an asset should be selected.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > All Assets

We need to ask you a few questions about your assets.
Your answers will help us identify which assets must be protected. Use the "Filter by Category" dropdown to filter the a individual response (or view an annotation), select a row to highlight, then select "Add/View Comment ". If you choose text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For ad double click on the row to view. The previous and next buttons will route you to either the previous or the

Note: Any listing containing more than 50 items must be expanded at the bottom center of th additiona

Filter by Category: All Categories 5 / 5

Overall Progress: 5 Answered / 5 Required

Assets - Double click row for more information

Category	Type	Name	Applicable?	Criticality	Score	Com	
			All				
lassified Information	Confidential Information		Yes No	Me			
Classified Information	Secret Information		Yes No	Medium			
Classified Information	Special Access Program Information		Yes No	Medium-High			
	ation		Yes No	Medium-High	78		DoD Counter Insider Threat Version 2.0
	tive Compartmented		Yes [✓ No]		0		DoD Counter Insider Threat Version 2.0

Page 1 of 1 | 50 | Rows 1 - 5 of 5

Asset Details - Secret Information

Executive Order 13526 defines "Secret" as applying to information "the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."

Highlight any row and click "Add/View Comment" to leave additional information.

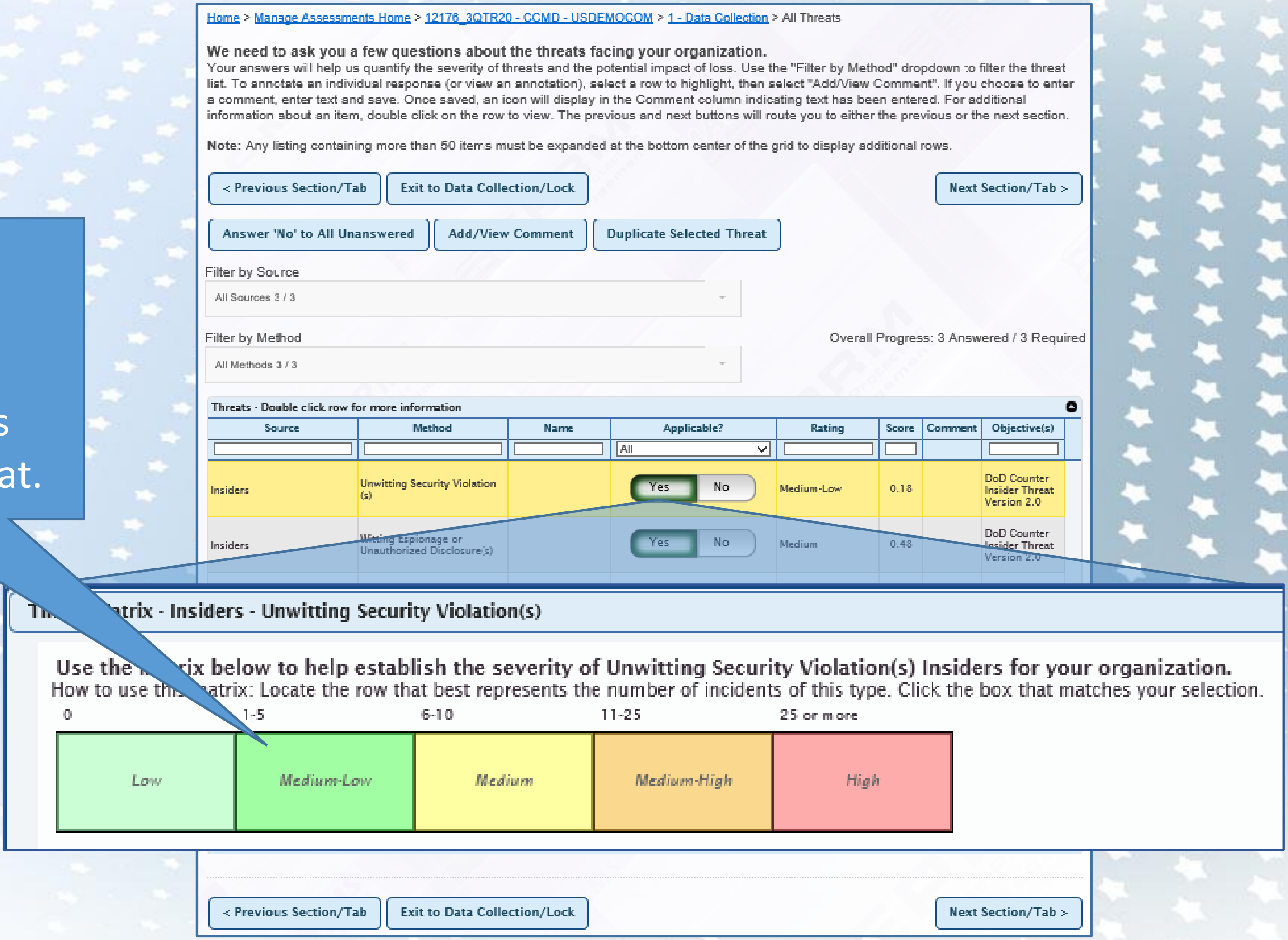
Double clicking in a row will open an info panel with a definition of the asset.

Each page allows the user to filter the questions by category, and displays the overall progress toward completion.

Creating a DoD Counter InT Assessment—cont’d

In the threat valuation section the user is asked to select the frequency range that best describes the rate of occurrence for the given threat.

Select the threat severity rating that best represents the number of incidents for this type of threat.


Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > All Threats
< Previous Section/Tab
Exit to Data Collection/Lock
Next Section/Tab >
Answer 'No' to All Unanswered
Add/View Comment
Duplicate Selected Threat

We need to ask you a few questions about the threats facing your organization.
Your answers will help us quantify the severity of threats and the potential impact of loss. Use the "Filter by Method" dropdown to filter the threat list. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you to either the previous or the next section.

Note: Any listing containing more than 50 items must be expanded at the bottom center of the grid to display additional rows.

Filter by Source: All Sources 3 / 3

Filter by Method: All Methods 3 / 3

Overall Progress: 3 Answered / 3 Required

Threats - Double click row for more information

Source	Method	Name	Applicable?	Rating	Score	Comment	Objective(s)
			All				
Insiders	Unwitting Security Violation (s)		Yes No	Medium-Low	0.18		DoD Counter Insider Threat Version 2.0
Insiders	Witting Espionage or Unauthorized Disclosure(s)		Yes No	Medium	0.48		DoD Counter Insider Threat Version 2.0

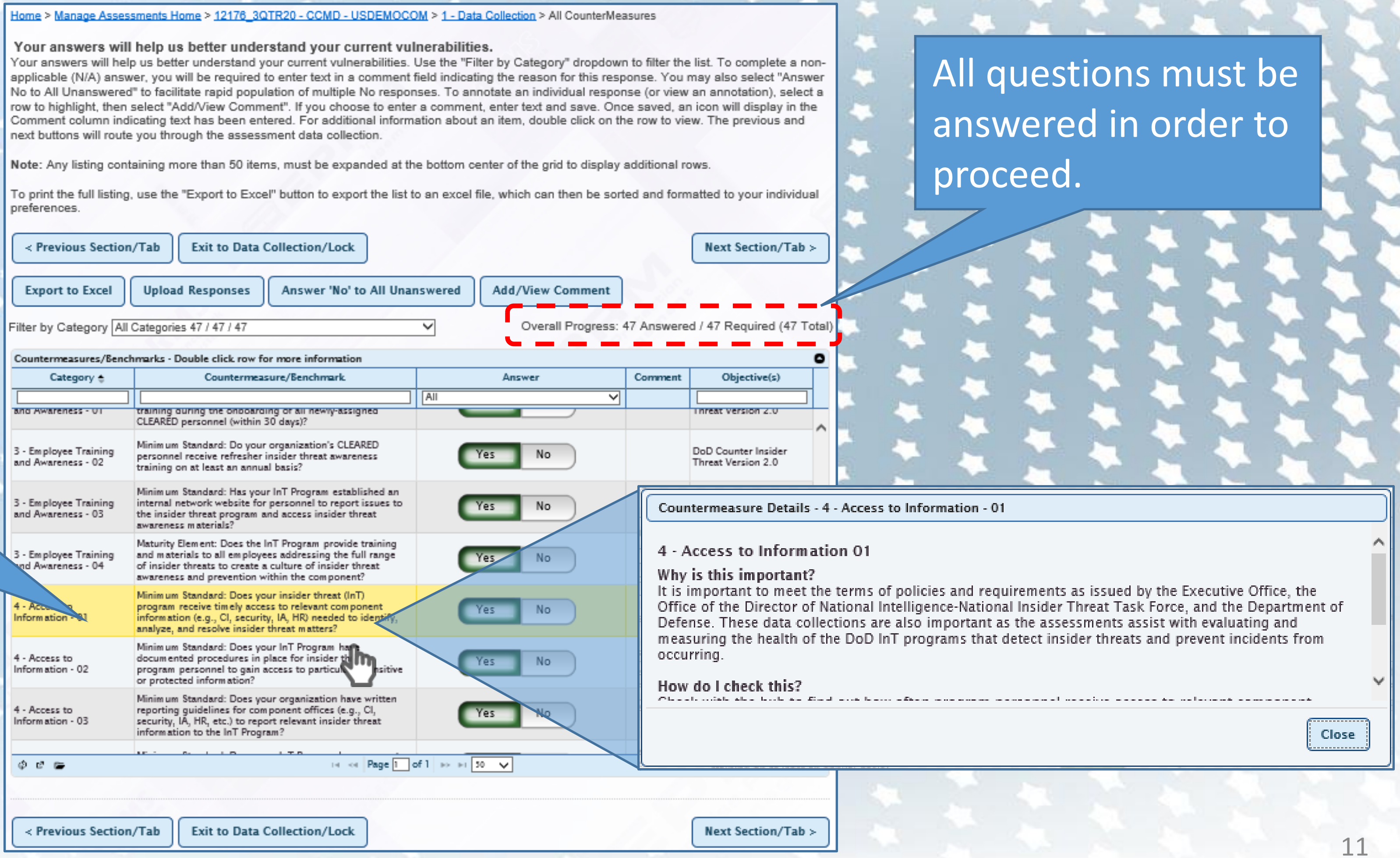
Th atrix - Insiders - Unwitting Security Violation(s)

Use the rix below to help establish the severity of Unwitting Security Violation(s) Insiders for your organization.
How to use th atrix: Locate the row that best represents the number of incidents of this type. Click the box that matches your selection.

0	1-5	6-10	11-25	25 or more
Low	Medium-Low	Medium	Medium-High	High

Creating a DoD Counter InT Assessment—cont’d

The last section is to characterize vulnerabilities (countermeasures). It follows the same grid format as the two previous sections. If you’ve copied answers from a previous assessment be sure to verify all questions have been answered.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > All CounterMeasures

Your answers will help us better understand your current vulnerabilities.

Your answers will help us better understand your current vulnerabilities. Use the "Filter by Category" dropdown to filter the list. To complete a non-applicable (N/A) answer, you will be required to enter text in a comment field indicating the reason for this response. You may also select "Answer No to All Unanswered" to facilitate rapid population of multiple No responses. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you through the assessment data collection.

Note: Any listing containing more than 50 items, must be expanded at the bottom center of the grid to display additional rows.

To print the full listing, use the "Export to Excel" button to export the list to an excel file, which can then be sorted and formatted to your individual preferences.

Filter by Category: All Categories 47 / 47 / 47

Overall Progress: 47 Answered / 47 Required (47 Total)

Countermeasures/Benchmarks - Double click row for more information

Category	Countermeasure/Benchmark	Answer	Comment	Objective(s)
		All		
and Awareness - 01	training during the onboarding of all newly-assigned CLEARED personnel (within 30 days)?			Threat Version 2.0
3 - Employee Training and Awareness - 02	Minimum Standard: Do your organization's CLEARED personnel receive refresher insider threat awareness training on at least an annual basis?	Yes No		DoD Counter Insider Threat Version 2.0
3 - Employee Training and Awareness - 03	Minimum Standard: Has your InT Program established an internal network website for personnel to report issues to the insider threat program and access insider threat awareness materials?	Yes No		
3 - Employee Training and Awareness - 04	Maturity Element: Does the InT Program provide training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the component?	Yes No		
4 - Access to Information - 01	Minimum Standard: Does your insider threat (InT) program receive timely access to relevant component information (e.g., CI, security, IA, HR) needed to identify, analyze, and resolve insider threat matters?	Yes No		
4 - Access to Information - 02	Minimum Standard: Does your InT Program have documented procedures in place for insider threat program personnel to gain access to particular sensitive or protected information?	Yes No		
4 - Access to Information - 03	Minimum Standard: Does your organization have written reporting guidelines for component offices (e.g., CI, security, IA, HR, etc.) to report relevant insider threat information to the InT Program?	Yes No		

Page 1 of 1 | 50

Countermeasure Details - 4 - Access to Information - 01

4 - Access to Information 01

Why is this important?

It is important to meet the terms of policies and requirements as issued by the Executive Office, the Office of the Director of National Intelligence-National Insider Threat Task Force, and the Department of Defense. These data collections are also important as the assessments assist with evaluating and measuring the health of the DoD InT programs that detect insider threats and prevent incidents from occurring.

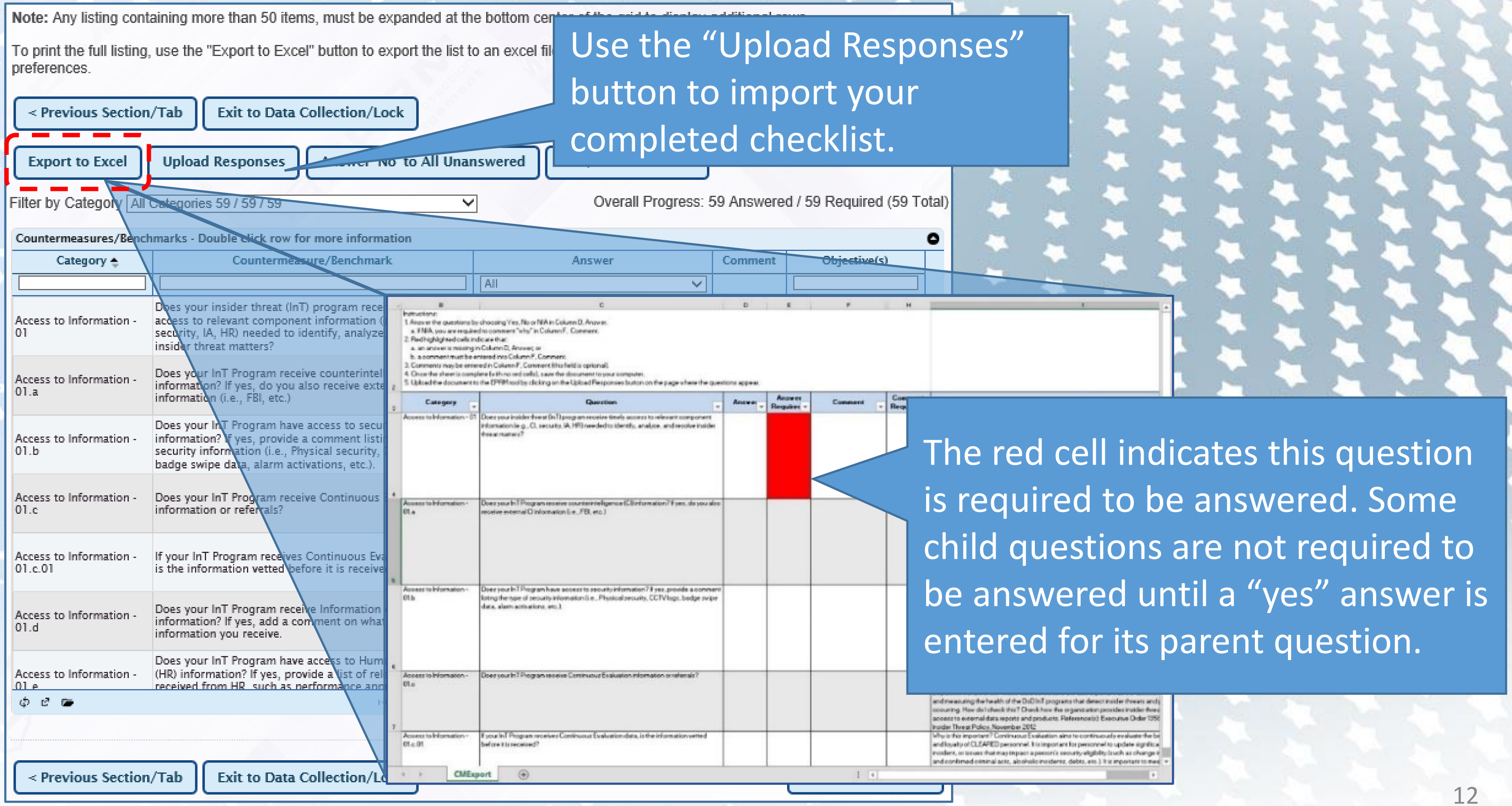
How do I check this?

All questions must be answered in order to proceed.

Double click any row to see the CMs importance, how the user can verify the presence of the CM, and policy references for more info.

Creating a DoD Counter InT Assessment—cont'd

Another method for answering countermeasure questions is by the "Export to Excel" button. Selecting this option will generate all CM questions in an Excel document for the user to answer. Once answered the user can upload the completed spreadsheet back to the assessment via the "Upload Responses" button.



Note: Any listing containing more than 50 items, must be expanded at the bottom cen

To print the full listing, use the "Export to Excel" button to export the list to an excel fil
preferences.

Filter by Category: All Categories 59 / 59 / 59

Overall Progress: 59 Answered / 59 Required (59 Total)

Countermeasures/Benchmarks - Double click row for more information

Category	Countermeasure/Benchmark	Answer	Comment	Objective(s)
		All		
Access to Information - 01	Does your insider threat (InT) program rece access to relevant component information (security, IA, HR) needed to identify, analyze insider threat matters?			
Access to Information - 01.a	Does your InT Program receive counterintel information? If yes, do you also receive exte information (i.e., FBI, etc.)			
Access to Information - 01.b	Does your InT Program have access to secu information? If yes, provide a comment listi security information (i.e., Physical security, badge swipe data, alarm activations, etc.).			
Access to Information - 01.c	Does your InT Program receive Continuous information or referrals?			
Access to Information - 01.c.01	If your InT Program receives Continuous Eva is the information vetted before it is receive			
Access to Information - 01.d	Does your InT Program receive Information information? If yes, add a comment on what information you receive.			
Access to Information - 01.e	Does your InT Program have access to Hum (HR) information? If yes, provide a list of rel received from HR, such as performance and			

Instructions:
1. Answer the questions by choosing Yes, No or N/A in Column D, Answer.
   a. If N/A, you are required to comment "why" in Column F, Comment.
2. Red highlighted cells indicate that:
   a. an answer is missing in Column D, Answer; or
   b. a comment must be entered into Column F, Comment.
3. Comments may be entered in Column F, Comment (this field is optional).
4. Once the sheet is complete (with no red cells), save the document to your computer.
5. Upload the document to the EPRM tool by clicking on the Upload Responses button on the page where the questions appear.

Category	Question	Answer	Answer Required	Comment	Comment Required
Access to Information - 01	Does your insider threat (InT) program receive timely access to relevant component information (e.g., CI, security, IA, HR) needed to identify, analyze, and resolve insider threat matters?		🟥		
Access to Information - 01.a	Does your InT Program receive counterintelligence (CI) information? If yes, do you also receive external CI information (i.e., FBI, etc.)				
Access to Information - 01.b	Does your InT Program have access to security information? If yes, provide a comment listing the type of security information (i.e., Physical security, CCTV logs, badge swipe data, alarm activations, etc.)				
Access to Information - 01.c	Does your InT Program receive Continuous Evaluation information or referrals?				
Access to Information - 01.c.01	If your InT Program receives Continuous Evaluation data, is the information vetted before it is received?				

and measuring the health of the DoD InT programs that detect insider threats and occurring. How do I check this? Check how the organization provides insider thre access to external data reports and products. Reference(s): Executive Order 1358 Insider Threat Policy, November 2012

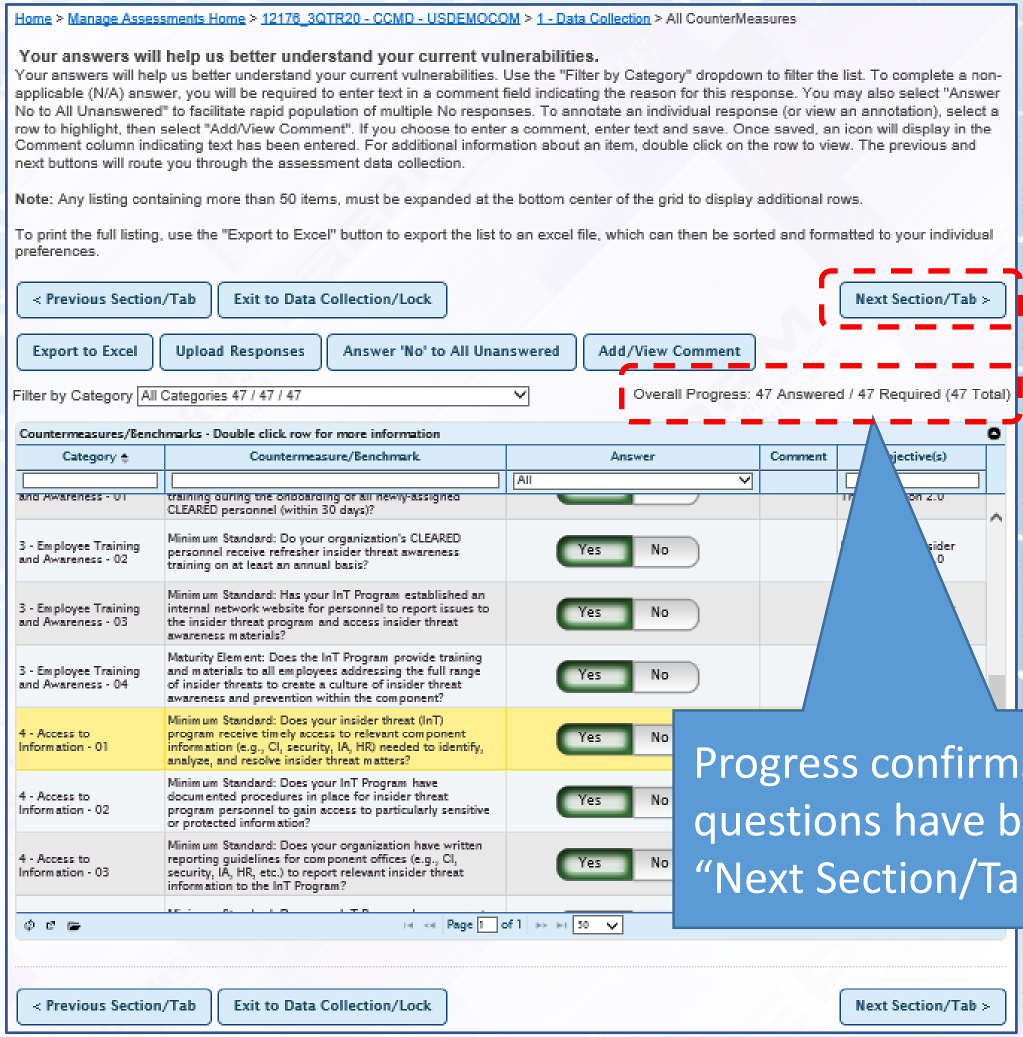
Why is this important? Continuous Evaluation aims to continuously evaluate the be and loyalty of CLEARED personnel. It is important for personnel to update significa incident, or issues that may impact a person's security eligibility (such as change i and confirmed criminal acts, alcohol incidents, debts, etc.). It is important to med

Use the "Upload Responses" button to import your completed checklist.

The red cell indicates this question is required to be answered. Some child questions are not required to be answered until a "yes" answer is entered for its parent question.

Concluding a DoD Counter InT Assessment

Once the user has confirmed their answers from a copied assessment and/or made necessary changes they are done with their assessment. Click “Next Section/Tab”, then “Finish and Lock” on the following page.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection > All CounterMeasures

Your answers will help us better understand your current vulnerabilities.

Your answers will help us better understand your current vulnerabilities. Use the "Filter by Category" dropdown to filter the list. To complete a non-applicable (N/A) answer, you will be required to enter text in a comment field indicating the reason for this response. You may also select "Answer No to All Unanswered" to facilitate rapid population of multiple No responses. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you through the assessment data collection.

Note: Any listing containing more than 50 items, must be expanded at the bottom center of the grid to display additional rows.

To print the full listing, use the "Export to Excel" button to export the list to an excel file, which can then be sorted and formatted to your individual preferences.

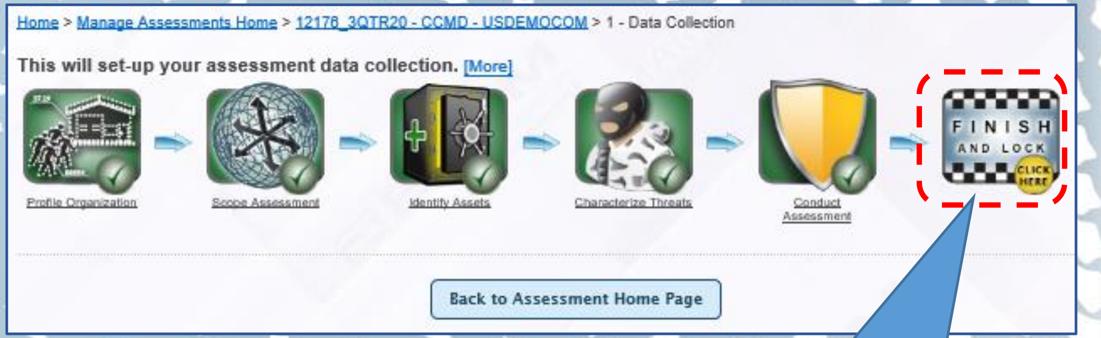
Filter by Category: All Categories 47 / 47 / 47

Overall Progress: 47 Answered / 47 Required (47 Total)

Countermeasures/Benchmarks - Double click row for more information

Category	Countermeasure/Benchmark	Answer	Comment	jective(s)
		All		
and Awareness - 01	training during the onboarding of all newly-assigned CLEARED personnel (within 30 days)?			Tr on 2.0
3 - Employee Training and Awareness - 02	Minimum Standard: Do your organization's CLEARED personnel receive refresher insider threat awareness training on at least an annual basis?	[✓ Yes] No		sider 0
3 - Employee Training and Awareness - 03	Minimum Standard: Has your InT Program established an internal network website for personnel to report issues to the insider threat program and access insider threat awareness materials?	[✓ Yes] No		
3 - Employee Training and Awareness - 04	Maturity Element: Does the InT Program provide training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the component?	[✓ Yes] No		
4 - Access to Information - 01	Minimum Standard: Does your insider threat (InT) program receive timely access to relevant component information (e.g., CI, security, IA, HR) needed to identify, analyze, and resolve insider threat matters?	[✓ Yes] No		
4 - Access to Information - 02	Minimum Standard: Does your InT Program have documented procedures in place for insider threat program personnel to gain access to particularly sensitive or protected information?	[✓ Yes] No		
4 - Access to Information - 03	Minimum Standard: Does your organization have written reporting guidelines for component offices (e.g., CI, security, IA, HR, etc.) to report relevant insider threat information to the InT Program?	[✓ Yes] No		

Progress confirms all required questions have been answered. Click “Next Section/Tab” to proceed.



Home > Manage Assessments Home > 12176_3QTR20 - CCMD - USDEMOCOM > 1 - Data Collection

This will set-up your assessment data collection. [More]

Click “Finish and Lock” to complete the assessment.

Assessment Naming Convention

The following naming convention should be used with all DoD Counter Insider assessments:
[Quarter & Year]-[Your Component category]-[Your Agency Abbreviation/Service]

Combatant Commands	Defense Agencies	Field Activities	Services	Other
1QTR20-CCMD-USAFRICOM	1QTR20-DA-DARPA	1QTR20-FA-DHRA	1QTR20-Service-Air Force	1QTR20-Other-DoDIG
1QTR20-CCMD-USCENTCOM	1QTR20-DA-DCAA	1QTR20-FA-DMA	1QTR20-Service-Army	1QTR20-Other-NGB
1QTR20-CCMD-USCYBERCOM	1QTR20-DA-DCMA	1QTR20-FA-DODEA	1QTR20-Service-Joint Staff	
1QTR20-CCMD-USEUCOM	1QTR20-DA-DeCA	1QTR20-FA-DTIC	1QTR20-Service-OPNAV	
1QTR20-CCMD-USNORTHCOM	1QTR20-DA-DFAS	1QTR20-FA-DTSA	1QTR20-Service-USMC	
1QTR20-CCMD-USPACOM	1QTR20-DA-DHA	1QTR20-FA-TRMC		
1QTR20-CCMD-USSOCOM	1QTR20-DA-DIA			
1QTR20-CCMD-USSOUTHCOM	1QTR20-DA-DISA			
1QTR20-CCMD-USSTRATCOM	1QTR20-DA-DLA			
1QTR20-CCMD-USTRANSCOM	1QTR20-DA-DPAA			
	1QTR20-DA-DSCA			
	1QTR20-DA-DSS			
	1QTR20-DA-DTRA			
	1QTR20-DA-MDA			
	1QTR20-DA-NGA			
	1QTR20-DA-NRO			
	1QTR20-DA-NSA			
	1QTR20-DA-PFPA-WHS			

Final Note: User Assistance

For additional user assistance, please utilize the following references and POCs:

- **Accessing system**: (SIPRNET) https://eprm.csd.disa.smil.mil
- **Help**: For assistance and for any questions, please email EPRMhelp@alionscience.com or call 1-800-754-4204. 0700-1700 Eastern time
- **Resources**:
  - On SIPR, check the User Guides and References section.
  - On NIPR, User guides, videos & other materials are available on the EPRMHelp page: http://eprmhelp.countermeasures.com