

UNCLASSIFIED



DoD Counter Insider User Guide

EPRM v3.64, March 2024

EPRM User Support: eprmhelp@hii-tsd.com
1.800.754.4204

UNCLASSIFIED

UNCLASSIFIED

Introduction

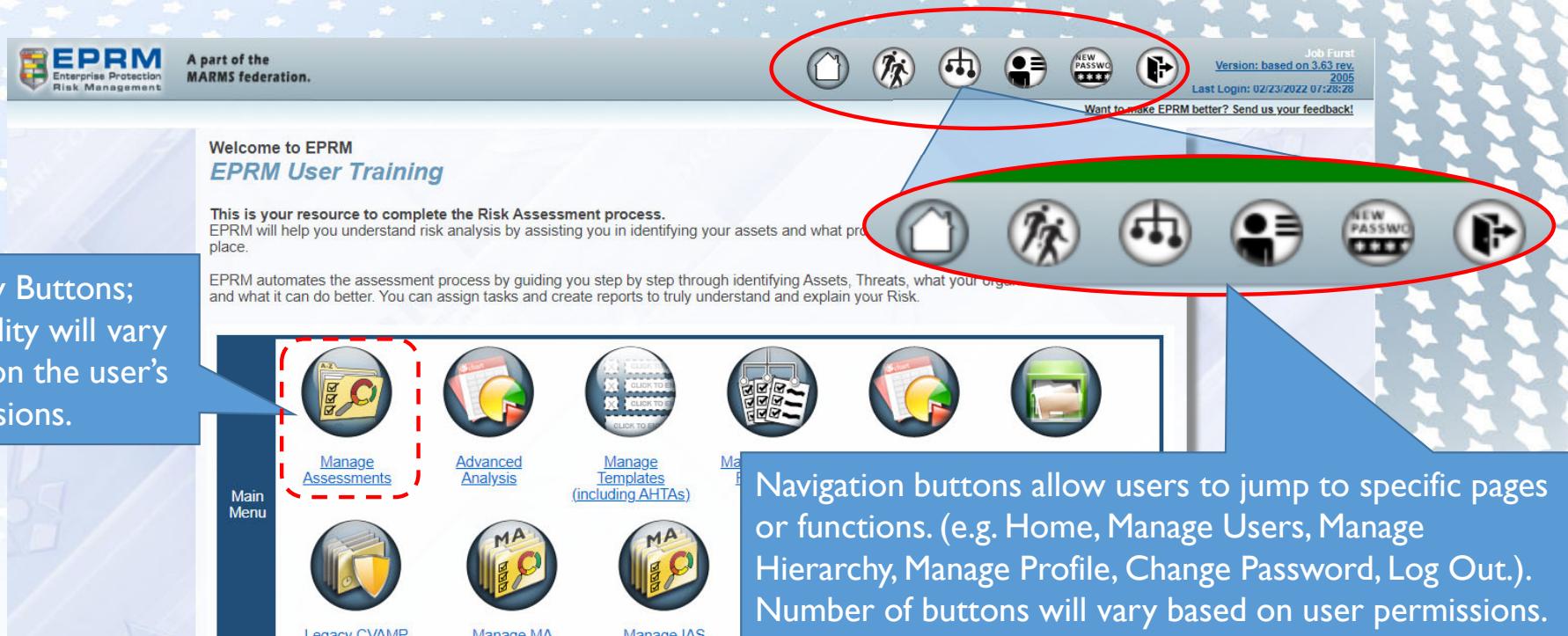
The DoD Component Counter Insider Threat module of EPRM is a semi-annual requirement to evaluate the implementation and effectiveness of component insider threat programs. The assessment tool provides components the ability to assess gaps across multiple capabilities to help make informed decisions on 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.

UNCLASSIFIED

UNCLASSIFIED

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.



UNCLASSIFIED

UNCLASSIFIED

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.

1 Click the green “Start” button to begin.

2 Name the assessment.

3 Select the node.

4 Select your assessment objective.

5 Click “Continue” to proceed.

UNCLASSIFIED

UNCLASSIFIED

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 > 12665_DoD InT 3.0 test > 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 | Objective(s) |
| 12664 | FY20 Q3/Q4 - CCMD - USCENTCOM | | 1 - Data Collection | Job Furst | HQDA User Support Training > 1- HQDA | 03/23/2021 | Version 3.0 DoD Counter Insider Threat Version 3.0 |
| 3464 | TRW May 2019 | | 2 - Basic Analysis, Mitigation and Submission | Job Furst | User Support Training > 2- USAF | 05/14/2019 | Information Protection Version 1.0 |
| 12175 | 1QTR20 - CCMD - DONOTUSE | | 1 - Data Collection | Marge Inovera | User Support Training > 3- AETC | 06/17/2020 | DoD Counter Insider Threat Version 2.0 |
| 12176 | 3QTR20 - CCMD - USDEMOCOM | | 2 - Basic Analysis, Mitigation and Submission | Marge Inovera | User Support Training > 3- AETC | 06/17/2020 | DoD Counter Insider Threat Version 2.0 |
| 12339 | AETC Test DoD InT 20200807 | | 1 - Data Collection | Marge Inovera | User Support Training > 3- AETC | 08/07/2020 | DoD Counter Insider Threat Version 2.0 |
| 12001 | 1QTR20 - CCMD - USDEMOCOM | 05/20/2020 | 2 - Basic Analysis, Mitigation and Submission | Marge Inovera | User Support Training > 3- AETC | 04/16/2020 | DoD Counter Insider Threat |
| 12002 | CCMD - USDEMOCOM | 05/20/2020 | 2 - Basic Analysis, | ... | User Support | 04/16/2020 | DoD Counter |

Rows 51 - 70 of 70

[Continue](#)

Last period's assessment.

Click “Continue” to proceed.

UNCLASSIFIED

UNCLASSIFIED

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 > 12666_FY21 1Q/2Q - CCMD - USCENTCOM > 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 created. 'FY20 Q3/Q4 - CCMD - USCENTCOM' copied successfully. Please use the workflow to continue.

DoD Counter Insider Threat Version 3.0

InT Program Narrative

What is the current NITTF assessment of your Counter-Insider Threat Program?*

Which component type describes your organization?*

What is the total number of cleared personnel that your InT Program covers?*

What is the total number of uncleared personnel that your InT Program covers?*

How many CAC holders does your InT Program cover?*

How many incidents were reported to your InT Program this year?*

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.)*

- Has your InT Program identified the personnel with access to the above?*

- List any steps currently in place to monitor the above personnel.*
Two factor ID, access logs, secured space security controls

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

- If yes, provide a comment on what steps your program takes to counter this additional threat.*
100 percent escort for vendors/delivery personnel.

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

< Previous Section/Tab Exit to Data Collection/Lock Next Section/Tab >

This banner confirms data was copied from previous assessment.

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

UNCLASSIFIED

UNCLASSIFIED

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](#) > [12000_FY21 1Q/2Q - CCMD - USCENTCOM](#) > [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.

DoD Counter Insider Threat Version 3.0

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.*

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.?*

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.*

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.*

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)*

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?*

[< Previous Section/Tab](#) [Exit to Data Collection/Lock](#) [Next Section/Tab >](#)

UNCLASSIFIED

UNCLASSIFIED

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 > 12868 FY21 1Q/2Q - CCMD - USCENTCOM > 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.

< Previous Section/Tab Exit to Data Collection/Lock Next Section/Tab >

Answer 'No' to All Unanswered Add/View Comment Duplicate Selected Asset Remove Duplicated Asset

Filter by Category (All Categories 10 / 10) Overall Progress: 10 Answered / 10 Required

Assets - Double click row for more information

| Category | Type | Name | Applicable? | Criticality | Score | Comment | Objective(s) |
|------------------------|--|------|---|-------------|-------|---------|--|
| Classified Information | Confidential Information | | <input checked="" type="button"/> Yes <input type="button"/> No | Medium-High | 78 | | DoD Counter Insider Threat Version 3.0 |
| Classified Information | Secret Information | | <input checked="" type="button"/> Yes <input type="button"/> No | Medium | 48 | | DoD Counter Insider Threat Version 3.0 |
| Classified Information | Special Access Program Information | | <input checked="" type="button"/> Yes <input type="button"/> No | Medium-Low | 18 | | DoD Counter Insider Threat Version 3.0 |
| Classified Information | Top Secret Information | | <input checked="" type="button"/> Yes <input type="button"/> No | Medium-High | 78 | | DoD Counter Insider Threat Version 3.0 |
| Classified Information | Top Secret/Sensitive Compartmented Information | | <input checked="" type="button"/> Yes <input type="button"/> No | Low | 0 | | DoD Counter Insider Threat Version 3.0 |
| Facilities | Facilities | | <input checked="" type="button"/> Yes <input type="button"/> No | Low | 5 | | DoD Counter Insider Threat Version 3.0 |

Rows 1 - 10 of 50

< Previous Section/Tab Exit to Data Collection/Lock Next Section/Tab >

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. |
| US | Adversary | Medium-Low | Medium | Medium-High | Medium-High |
| Medium-Low | Low | Medium | Medium-High | Medium-High | Medium-High |
| Medium | Low | Medium-Low | Medium | Medium | Medium-High |
| Medium-High | Medium-Low | Medium-Low | Medium-Low | Medium-Low | Medium |
| High | Medium-Low | Low | Low | Low | Medium-Low |

The asset is of **Critical** importance to the adversary. Destroying or acquiring the asset considerably contributes to meeting the adversary's objectives.

The asset is of **SIGNIFICANT** importance to the adversary. Destroying or acquiring the asset appreciably contributes to meeting the adversary's objectives.

The asset is of **Moderate** importance to the adversary. Destroying or acquiring the asset measurably contributes to meeting the adversary's objectives.

The asset is of **Low** importance to the adversary. Destroying or acquiring the asset may contribute to meeting the adversary's objectives.

The asset is of **Minimal** or no importance to the adversary.

Cancel

UNCLASSIFIED

UNCLASSIFIED

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.

The screenshot displays a web-based application interface for managing assets. At the top, there's a header with navigation links: Home > Manage Assessments Home > 12868 FY21 1Q/2Q - CCMC - USCENTCOM > 1 - Data Collection > All Assets. Below the header, a message asks for user input to identify protected assets, mentioning a dropdown for filtering by category and a note about saving individual responses.

Below the message is a table titled "Assets - Double click row for more information". The table has columns for Category, Type, Name, Applicable?, Criticality, Score, and Comment. There are 10 rows of data, each with a "Comment" column containing a small icon indicating text has been entered. Buttons at the top of the table include < Previous Section/Tab, Exit to Data Collection/Lock, Next Section/Tab >, Answer 'No' to All Unanswered, Add/View Comment, Duplicate Selected Asset, and Remove Duplicated Asset. A progress bar shows "Overall Progress: 10 Answered / 10 Required".

A callout box on the right says: "Highlight any row and click 'Add/View Comment' to leave additional information." It points to the "Add/View Comment" button and the "Comment" column in the table.

A callout box on the left says: "Double clicking in a row will open an info panel with a definition of the asset." It points to the table row for "Secret Information".

An info panel titled "Asset Details - Secret Information" is shown in a modal window. It contains a definition of "Secret" according to Executive Order 13526 and a "Close" button.

A callout box on the right says: "Each page allows the user to filter the questions by category and displays the overall progress toward completion." It points to the "Filter by Category" dropdown and the progress bar.

At the bottom of the page are buttons for < Previous Section/Tab, Exit to Data Collection/Lock, and Next Section/Tab >. A page number indicator shows "Page 1 of 1" and a dropdown for "Rows 1 - 10 of 10".

UNCLASSIFIED

UNCLASSIFIED

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.

The screenshot shows a web-based application for threat assessment. At the top, there's a header with navigation links: Home > Manage Assessments Home > 12066_FY21 1Q/Q2 - CCMD - USCENTCOM > 1 - Data Collection > All Threats. Below the header, a message asks users to answer questions about threats facing their organization, mentioning a filter by method dropdown, annotation feature, and comment history. It also notes that listing more than 50 items must be expanded at the bottom. There are buttons for 'Answer No' to All Unanswered, 'Add/View Comment', 'Duplicate Selected Threat', and 'Remove Duplicated Threat'. Below these are two filter dropdowns: 'Filter by Source' (All Sources 7 / 7) and 'Filter by Method' (All Methods 7 / 7). An overall progress bar shows 7 Answered / 7 Required. The main content area is titled 'Threats - Double click row for more information' and contains a table with columns: Source, Method, Name, Applicable?, Rating, Score, Comment, and Objective(s). Two rows are visible: one for 'Insiders Fraud' with a 'Yes' button, 'Medium' rating, and score 0.46, and another for 'Insiders Sabotage' with a 'Yes' button, 'Medium-Low' rating, and score 0.18. Both rows have a 'DoD Counter Insider Threat Version 3.0' comment. A callout bubble from the text above points to the 'Fraud' row. Below the table is a 'Threat Matrix - Insiders - Fraud' section with instructions to use a matrix to establish severity. The matrix has columns for 0, 1-5, 6-10, 11-25, and 25 or more, with rows for Low, Medium-Low, Medium, Medium-High, and High. The 'Medium-Low' cell is highlighted in green. Navigation buttons at the bottom include '< Previous Section/Tab', 'Exit to Data Collection/Lock', and 'Next Section/Tab'.

UNCLASSIFIED

UNCLASSIFIED

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.

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.

The screenshot shows a web-based application for managing assessments. At the top, there's a header with navigation links: Home > Manage Assessments Home > 12868 FY21 1Q/2Q - CCMD - USCENTCOM > 1 - Data Collection > All CounterMeasures. Below the header is a detailed instruction box:

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.

Below these instructions is a toolbar with buttons: < Previous Section/Tab, Exit to Data Collection/Lock, Next Section/Tab >, Export to Excel, Upload Responses, Answer 'No' to All Unanswered, Add/View Comment, File/Image Upload. A progress bar indicates "Overall Progress: 19 Answered / 19 Required (19 Total)".

The main area is a grid titled "Countermeasures/Benchmarks - Double click row for more information". The columns are: Category, Countermeasure/Benchmark, Answer, Comment, and Objectives(s). The grid contains several rows of data, each with a "Details" button. A specific row (row 5, Monitoring User Activity on Networks - 05) is highlighted with a yellow background and has a hand cursor pointing at its "Details" button. A large blue callout box points to this row with the text: "All questions must be answered in order to proceed."

A modal window titled "Countermeasure Details - 5 - Monitoring User Activity on Networks - 05" is open over the grid. It contains the question "5 - Monitoring User Activity on Networks 05" and the sub-question "Why is this important?". The text in the modal describes the legal framework for monitoring user activity on organization networks, mentioning the U.S. Government's ownership, user consent, and privacy expectations. It also states that it is important to meet terms of policies and requirements issued by the Executive Office, the Office of the Director of National Intelligence-National Insider Threat Task Force, and the Department of Defense.

At the bottom of the grid, there are buttons for < Previous Section/Tab, Exit to Data Collection/Lock, and Next Section/Tab >. The page footer shows "Page 1 of 1" and "Rows 1 - 19 of 19".

UNCLASSIFIED

UNCLASSIFIED

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 center of the page.
To print the full listing, use the "Export to Excel" button to export the list to an excel file based on your preferences.

< Previous Section/Tab Exit to Data Collection/Lock

Export to Excel **Upload Responses** Answer No to All Unanswered

Filter by Category: All Categories 59 / 59 759

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

Countermeasures/Benchmarks - Double click row for more information

| Category | Countermeasure/Benchmark | Answer | Comment | Objective(s) |
|---------------------------------|--|--------|---------|--------------|
| Access to Information - 01 | Does your insider threat (InT) program receive access to relevant component information (e.g., security, IA, HR) needed to identify, analyze, and mitigate insider threat matters? | | | |
| Access to Information - 01.a | Does your InT Program receive counterintelligence information? If yes, do you also receive external information (i.e., FBI, etc.) | | | |
| Access to Information - 01.b | Does your InT Program have access to 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 Evaluations, is the information vetted before it is received? | | | |
| Access to Information - 01.d | Does your InT Program receive Information about your organization? If yes, add a comment on what information you receive. | | | |
| Access to Information - 01.e | Does your InT Program have access to Human Resources (HR) information? If yes, provide a list of relevant information received from HR, such as performance and | | | |

Instructions: 1. Use the checkbox for choosing Yes, No/N/A in Column D. Answer: 2. A red highlighted cell indicates that an answer is missing in Column D. Answer: 3. A blue highlighted cell indicates that a comment has been added in Column F. Comment: this field is optional. 4. Click the sheet to continue to the next cell. Save the file and close the computer. 5. Upload the document to the SharePoint library and then click the Update Progress button on the page where the question appears.

Category Question Answer Answer Response Comment Comment Response

Access to Information - 01 Does your InT Program receive access to relevant component information (e.g., security, IA, HR) needed to identify, analyze, and mitigate insider threat matters? **Red Cell**

Access to Information - 01.a Does your InT Program receive counterintelligence (CI) information? If yes, do you also receive external information (i.e., FBI, etc.)

Access to Information - 01.b Does your InT Program have access to 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 Evaluations, is the information vetted before it is received?

Access to Information - 01.d Does your InT Program receive Information about your organization? If yes, add a comment on what information you receive.

Access to Information - 01.e Does your InT Program have access to Human Resources (HR) information? If yes, provide a list of relevant information received from HR, such as performance and

UNCLASSIFIED

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.

UNCLASSIFIED

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 > 12686 FY21 1Q/2Q - CCMD - USCENTCOM > 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.

< Previous Section/Tab Exit to Data Collection/Lock

Export to Excel Upload Responses Answer ‘No’ to All Unanswered Add/View Comment File/Image Upload

Filter by Category: All Categories 19 / 19 Overall Progress: 19 Answered / 19 Required (19 Total)

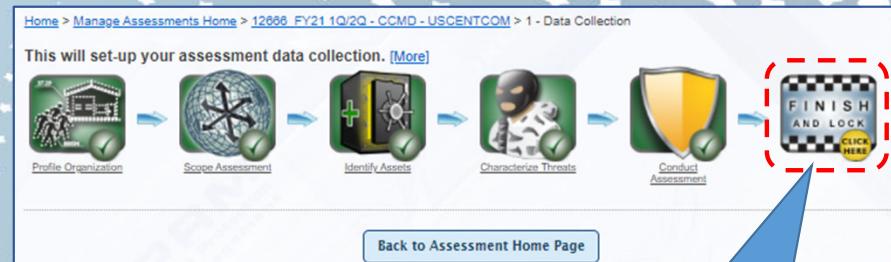
Countermeasures/Benchmarks - Double click row for more information

| Category # | Countermeasure/Benchmark | Answer | Comment | Objective(s) |
|--|--|-----------|---------|---|
| 1 - Senior Official and Policies/Procedures - 09 | Maturity Element: Does a dedicated effort exist to ensure access to leadership to build support, identify resources, and integrate insider threat objectives within the component's mission and functions? | Yes No | | Integrate Insider Threat Objectives 3.0 |
| 1 - Senior Official and Policies/Procedures - 10 | Maturity Element: Are metrics employed to determine progress in achieving program objectives and to identify areas requiring improvement? | Yes No | | Integrate Insider Threat Objectives 0 |
| 1 - Senior Official and Policies/Procedures - 11 | Maturity Element: Can the InT Program quickly adapt to changes in law, policy, organizational structure, and information technology (IT) architecture? | Yes No | | Integrate Insider Threat Objectives 1 |
| 1 - Senior Official and Policies/Procedures - 12 | Maturity Element: Does the InT Program employ risk management principles tailored to address the evolving threat environment and mission needs? | Yes No | | Integrate Insider Threat Objectives 2 |
| 2 - Insider Threat Program Personnel - 06 | Maturity Element: Does the InT Program include stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen InT Program processes? | Yes No | | Integrate Insider Threat Objectives 3 |
| 2 - Insider Threat Program Personnel - 07 | Maturity Element: Does the InT Program provide continuing education and training in appropriate fields and disciplines to help professionalize the insider threat career field? | Yes No | | Integrate Insider Threat Objectives 4 |
| | Maturity Element: Does the InT Program provide training | | | |

< Previous Section/Tab Exit to Data Collection/Lock

Next Section/Tab >

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



Click “Finish and Lock” to complete the assessment.

UNCLASSIFIED

UNCLASSIFIED

Assessment Naming Convention

The following naming convention should be used with all DoD Counter Insider assessments:

[Fiscal Year]-[Quarters]-[Your Component category]-[Your Agency Abbreviation/Service]

| Combatant Commands | Defense Agencies | Field Activities | Services | Other |
|----------------------------|-------------------------|-------------------------|--------------------------------|------------------------|
| FY21-Q1/Q2-CCMD-USAFRICOM | FY21-Q1/Q2-DA-DARPA | FY21-Q1/Q2-FA-DHRA | FY21-Q1/Q2-Service-Air Force | FY21-Q1/Q2-Other-DoDIG |
| FY21-Q1/Q2-CCMD-USCENTCOM | FY21-Q1/Q2-DA-DCAA | FY21-Q1/Q2-FA-DMA | FY21-Q1/Q2-Service-Army | FY21-Q1/Q2-Other-NGB |
| FY21-Q1/Q2-CCMD-USCYBERCOM | FY21-Q1/Q2-DA-DCMA | FY21-Q1/Q2-FA-DODEA | FY21-Q1/Q2-Service-Joint Staff | |
| FY21-Q1/Q2-CCMD-USEUCOM | FY21-Q1/Q2-DA-DeCA | FY21-Q1/Q2-FA-DTIC | FY21-Q1/Q2-Service-OPNAV | |
| FY21-Q1/Q2-CCMD-USNORTHCOM | FY21-Q1/Q2-DA-DFAS | FY21-Q1/Q2-FA-DTSA | FY21-Q1/Q2-Service-USMC | |
| FY21-Q1/Q2-CCMD-USPACOM | FY21-Q1/Q2-DA-DHA | FY21-Q1/Q2-FA-TRMC | | |
| FY21-Q1/Q2-CCMD-USSOCOM | FY21-Q1/Q2-DA-DIA | | | |
| FY21-Q1/Q2-CCMD-USSOUTHCOM | FY21-Q1/Q2-DA-DISA | | | |
| FY21-Q1/Q2-CCMD-USSTRATCOM | FY21-Q1/Q2-DA-DLA | | | |
| FY21-Q1/Q2-CCMD-USTRANSCOM | FY21-Q1/Q2-DA-DPAA | | | |
| | FY21-Q1/Q2-DA-DSCA | | | |
| | FY21-Q1/Q2-DA-DSS | | | |
| | FY21-Q1/Q2-DA-DTRA | | | |
| | FY21-Q1/Q2-DA-MDA | | | |
| | FY21-Q1/Q2-DA-NGA | | | |
| | FY21-Q1/Q2-DA-NRO | | | |
| | FY21-Q1/Q2-DA-NSA | | | |
| | FY21-Q1/Q2-DA-PFPA-WHS | | | |

DoD Counter Insider assessments
are now conducted semi-annually.
Naming convention has changed to
include either "Q1/Q2" or "Q3/Q4".

UNCLASSIFIED

UNCLASSIFIED

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@hii-tsd.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>



UNCLASSIFIED