3.5 Develop a Remediation Strategy

Developing the POA&M must be a collaborative effort between program officials, ISSOs, system owners, system administrators, and others, as needed. After weaknesses have been identified, documented and prioritized, a plan must be developed to resolve them. The process should include, but not be limited to, the following steps:

- Identify the root cause of the weakness. The goal of root cause analysis is to focus on finding the real cause of a problem, rather than merely dealing with or addressing the symptoms of the identified condition. Root cause analysis is an iterative process, and is frequently viewed as a tool of continuous improvement. There is usually more than one root cause for any given problem and often one root cause for multiple problems. In performing a root cause analysis, the policy, procedures, people, technology and resources relevant to the identified security weakness are reviewed because inadequacies in one or more of those areas are generally the root cause(s) of the weakness. Appendix E to this Guide provides additional guidance and steps to follow when performing a root cause analysis.

- Identify resources needed to resolve weaknesses and where those resources will come from. Resources can include staffing, funding, equipment (e.g., hardware and software), training, licenses, or a combination of each.
- Develop the steps needed to resolve the weakness. These should include specific actions that need to be taken, coordination that might be needed, obtaining and allocating resources, testing the corrections to ensure they effectively resolve the weakness, and updating documentation to reflect any changes. Key steps that are identified should be documented as milestones.
- Develop a realistic and achievable timeline and schedule for resolving the weaknesses.
- Record weaknesses and the remediation plan in the POA&M. Entering the plan into TAF is the last step in the process of developing a POA&M.
- If a weakness will take several months to resolve, multiple milestones should be used to show interim steps which can be used to track progress. In FY10 at lease one milestone is required for all POA&Ms that are open over 3 months.

Milestones in the following categories should be considered:

- Obtaining/allocating resources
- Implementation activities
- Testing and documentation

3.5.1 Financial Systems

- Financial systems POAMS require two milestones
  - Testing the design of a control
  - Testing the effective implementation of a control. and testing

- Testing Activities
- Each recommendation must have a POAM
- Requires a Test of Design (need milestone to implement the solution and Test of Effectiveness (need one milestone to ensure it is implemented properly.

For financial systems, and to some degree for all systems, it is important to include milestones for testing the design of a control and the effectiveness of a control. In this context, the design of a control relates to the documented process or procedure implementing a control. The test of the effectiveness of a control refers to the process of verifying that the control actually performs as intended and is consistent with the design. When financial systems are audited, it is important to show that the controls are effective over time, not just as a "snapshot in time".

Please note that a POA&M is a plan to resolve unacceptable risks. If, during the C&A process, the AO makes a decision to accept the risk posed by an identified weakness, there is no need to create a POA&M, as long as the risk acceptance is clearly documented. All such risk-based decisions must be documented in the C&A package in the Security Assessment Report. The only exception is financial audit findings, which must be documented as described in Section 3.1.

If the AO does not accept the risks, waivers or exceptions are options if a system cannot meet the minimum set of security controls required by DHS Policy. Waivers may be used for a maximum of 12 months (one 6-month waiver by the DHS CISO and one 6-mont waiver by the Component CISO.)

If non-compliance with DHS Policy is expected to last longer than 12 months, an Exception must be used. Lack of immediate funding to resolve a weakness may result in an Exception.

3.6 Take Corrective Actions

Once the plan has been developed, it must be implemented. Taking the corrective actions needed to resolve the weakness is the most important aspect of the POA&M because it is the only part of the process that actually reduces risk to the system or program.

3.7 Monitor and Update

POA&M data should be monitored on a continuous basis and updated as events occur. DHS requires that all information in the POA&M be updated at least monthly and be accurate on the first day of each month for Department tracking and reporting purposes.

As part of their review CISOs should:

- Validate that the weakness is properly identified and prioritized;
- Ensure appropriate resources have been made available to resolve the weakness;
- If these conditions are not met, fail the POA&M and provide comments regarding what needs to be don't to bring it into compliance with POA&M guidelines;
- Ensure that the schedule for resolving the weakness is both appropriate and achievable;

The annual DHS Information Security Performance Plan identifies the type of POA&M that must be reviewed and approved by CISOs. However, it is highly recommended that CISOs use the approval function in TAF to document their review of all POA&Ms as resources permit. The "Approval Status" feature is available on the weakness screen and is also available through the Weakness Search report. See Figure 14.

3.8 Completing a POA&M Weakness

When a weakness has been fully mitigated and all milestones have been completed, the POA&M weakness must be closed out by changing the status to "Completed" and entering the date in the "Actual Completion Date" field in the Weakness screen as described in Section 4.2.6. Note that TAF automatically assigns the current date in the "Actual Completion Date" field in TAF when the status is changed to "Completed." However, this date can be changed to reflect whatever date all actions were completed.

To substantiate OMB reporting that a weakness or audit finding is closed, an appropriate artifact should be uploaded in the "List of Weakness Artifacts" field in the weakness screen in TAF as evidence of completion. The artifact can be a document produced as a result of the remediation process, such as a contingency plan test report, a screenshot showing the correct setting for a control, a memo that describes the action taken or refers to other documentation, or an OIG memo attesting to the fact that the finding has been closed. While it is recommended that all completed POA&Ms have an appropriate artifact uploaded, it is required for all priority 4 and 5 POA&Ms.

POA&M items that have been completed should remain in the POA&M for a full year after the completion date for accounting and reporting purposes. TAF automatically archives all weaknesses that have a completion date that is more than one year old at the beginning of each fiscal year.

3.9 Report Status

OMB requires quarterly reports on the status of the Department's POA&Ms. These reports are extracted from TAF at the Department level so ISSOs should ensure, and CISOs/ISSMs should verify, that POA&Ms are maintained as current and accurate as possible.

4.0 POA&M ELEMENTS

Based on OMB guidance, DHS requires the following items to be included in POA&Ms:

- Weakness Number;
- Creation Date;
- Description of Weakness;
- Status;
- Criticality (Priority) Level;
- Point of Contact (POC);
- Risk Category;

- Resources Required;
- Severity;
- Type;
- Scheduled Completion Date;
- Is Material Weakness;
- Estimated Completion Date;
- Actual Completion Date;
- Link To Control Title;
- Source of Weakness;
- Milestones with Completion Dates;
- Milestone Changes;

Additionally, DHS requires that information regarding system identification and security costs be entered into TAF.

DHS has incorporated additional data, procedures and tools into its POA&M process to help Components and the Department manage the resolution of weaknesses. Section 4.1 describes support available for the DHS POA&M process. Section 4.2 describes the data fields DHS requires to be entered in the POA&M and provides guidance to help determine what data and level of detail should be documented.

4.1 TrustedAgent FISMA

TrustedAgent FISMA (TAF) is the Enterprise Compliance and Oversight tool that manages the collection and reporting of information associated with POA&Ms and the NIST 800-53 annual assessments. Components must use the TAF tool to identify, track, and manage all IT system weaknesses and associated POA&Ms to closure, for SBU systems. TAF is available on the Internet at (b) (7)(E) Users who need access to TAF may request an account and appropriate privileges through their CISO/ISSM. Help Desk Support for TAF is available via phone at (b)(6) (b)(7)(C) or via e-mail at (b)(6)

TAF/C, the version of TAF to be used for recording POA&Ms and other data for classified systems, is available through HSDN. Help Desk Support for TAF/C is available via phone at (b)(6) (b)(7)(C) or via e-mail at (b)(6)

4.2 Required POA&M Data

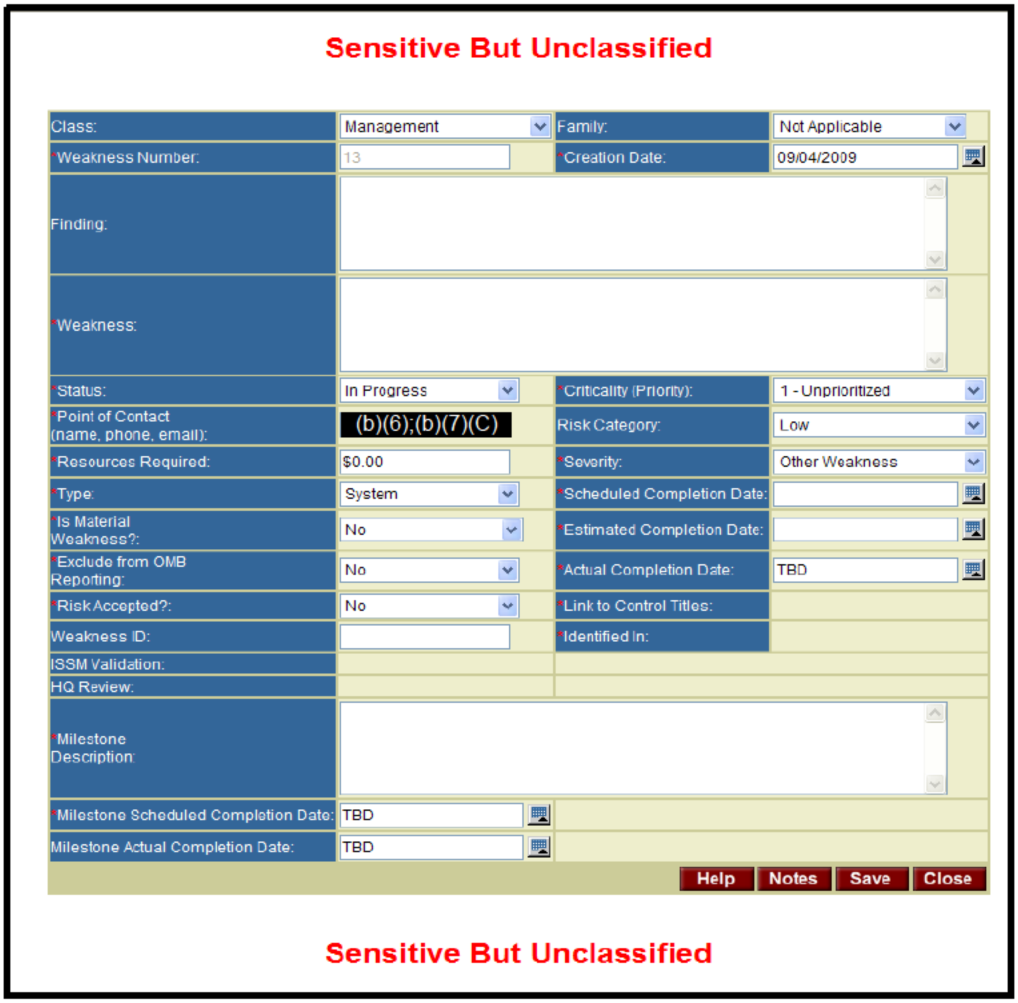
The following sections describe data that must be captured in the POA&M to meet OMB and DHS requirements. Figure 5 illustrates the main TAF screen used to build a POA&M item and is provided for reference. **Note that this figure represents the initial TAF Weakness Screen and some data (e.g., red ellipses boxes) are not available until the user hits save.** Detailed instructions for using TAF are provided in an on-line user's guide available by clicking the

"Technical Support" link at the bottom of the TAF homepage and selecting the Training materials tab. A number of other useful reference documents and training materials are also available through this link. Additionally, a worksheet for collecting POA&M data is located in Appendix C.

Below is a list of POA&M data elements in the TAF weakness window. The list identifies the fields that are required, optional, automatically filled in by TAF, and not applicable. Subsequent sections below describe data elements in detail.

- Class (Optional)
- Family (Optional)
- Weakness Number (Automatically filled in by TAF)
- Creation Date (Automatically filled in by TAF)
- Finding (Optional)
- Weakness Description (Required)
- Status (Required)
- Criticality (Priority) (Required)
- Point of Contact (POC) (Required)
- Risk Category (Required)
- Resources Required (Required)
- Severity (Required)
- Type (Automatically filled in by TAF)
- Scheduled Completion Date (Required)
- Is Material Weakness (Required)
- Estimated Completion Date (Required)
- Exclude from OMB Reporting (Not Applicable)
- Actual Completion Date (Automatically filled in by TAF)
- Risk Accepted (Not Applicable)
- Link to Control Titles (Required)
- Weakness ID (Not Applicable)
- Identified In (Required)
- ISSM Validation (Required)
- HQ Review (Required)
- Milestone Description (Required)

- Milestone Scheduled Completion Date (Required)
- Milestone Actual Completion Date (Required)



Sensitive But Unclassified

Class:	Management	Family:	Not Applicable
*Weakness Number:	13	*Creation Date:	09/04/2009
Finding:			
*Weakness:			
*Status:	In Progress	*Criticality (Priority):	1 - Unprioritized
*Point of Contact (name, phone, email):	(b)(6);(b)(7)(C)	Risk Category:	Low
*Resources Required:	$0.00	*Severity:	Other Weakness
*Type:	System	*Scheduled Completion Date:	
*Is Material Weakness?:	No	*Estimated Completion Date:	
*Exclude from OMB Reporting:	No	*Actual Completion Date:	TBD
*Risk Accepted?:	No	*Link to Control Titles:	
Weakness ID:		*Identified In:	
ISSM Validation:			
HQ Review:			
*Milestone Description:			
*Milestone Scheduled Completion Date:	TBD		
Milestone Actual Completion Date:	TBD		

Sensitive But Unclassified

Figure 5. Initial Weakness Screen in TAF

Class (Optional)

Select the NIST-800-53 class, Management, Operational, or Technical from the drop-down menu.

Family (Optional)

Select the NIST 800-53 control family from the drop-down menu.

Weakness Number (Automatically filled in by TAF)

The weakness number is a sequential number for each weakness when more than one weakness has been identified per system or program. TAF automatically assigns this number.

Creation Date (Automatically filled in by TAF)

The creation date of the POA&M is automatically filled in by TAF.

Finding (Optional)

The finding field is not required to be completed in a POA&M.

Weaknesses Description (Required)

Weaknesses are documented in detail by the source that identified them (e.g., C&A, annual assessments, audits). They must also be documented in the POA&M. Detailed descriptions are *not* necessary in the POA&M, but sufficient data is required to permit oversight and tracking, as well as to provide traceability back to the original source.

Weakness descriptions must include a weakness number, severity level, and description of the weakness, as described below. This data is entered in the "Weakness" field in TAF (see Figure 5). Only outstanding information security weaknesses that have not been accepted by the AO and audit findings must be entered.

Weaknesses should be described as a vulnerability that needs to be corrected and not simply listed as a corrective action that must be taken. For example, lack of a system security plan (SSP) should be entered as, "Inadequate planning" or "the system does not have an SSP" whereas a description such as, "Draft system security documentation" is a corrective action and should be reported as a milestone. The weakness description should not simply repeat the control that has not been met or cut and paste the weakness description from the source document. Instead, the real weakness should be determined and describe it appropriately. Each weakness must have at least one milestone if open for more than three months. Appendix H to this Guide contains examples of acceptable and unacceptable weakness descriptions.

For audit findings, each recommendation must be tied to a specific POA&M to comply with the FISMA requirement that all recommendations are addressed. To help identify and track audit findings for FISMA reporting purposes the recommendation number should be entered in the identified in screen in TAF. Figures 12 illustrates how this data should be entered.

All weaknesses that have been identified by any source and will be resolved must be entered in the POA&M for accounting purposes. Weaknesses that have been completely mitigated should remain in the POA&M for a full year beyond the "actual completion date" for accounting purposes. They will automatically be deleted by TAF after the appropriate period as part of the annual fiscal year data migration.

When a risk-based decision has been made by the AO to accept the risk posed by the weakness, no POA&M entry is required since no further action is planned. Audit findings are the only exception and must always be documented in a POA&M as required by OMB with appropriate disposition.

Status (Required)

All weaknesses must have an assigned status. Maintaining the POA&M to indicate the current status of a corrective action helps to demonstrate the POA&M is being used as a management tool and is part of an ongoing process.

To help Components manage their process and present a more understandable picture of the true status of remediation activities, TAF includes a number of status categories. The following guidelines are provided to help standardize use of these categories and provide Components more flexibility in managing their POA&Ms. TAF automatically converts DHS-unique categories to meet OMB reporting requirements (i.e., Not Started, Planned/Pending, Ongoing, In Progress, and Delayed are reported as “ongoing” while Completed and Cancelled are reported as “completed”). Figure 6 illustrates the TAF dropdown menu used to select the status of the weakness.

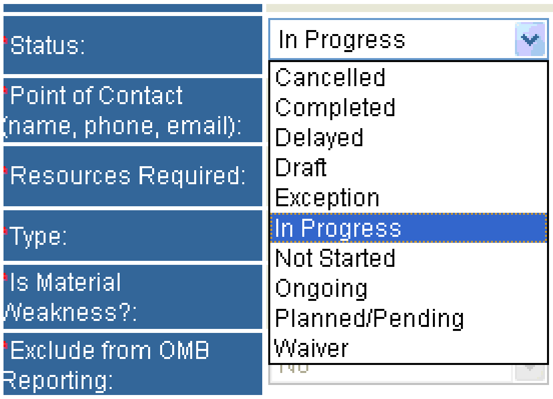
TAF allows the following status categories to be assigned:

- In Progress – should be used when any activities needed to resolve a weakness have begun. Such activities may include planning (e.g., creating a POA&M), procurement actions, coordination activities, or actual remediation actions. This category is the default in TAF and can be used properly in any case except completed, cancelled, waiver, exception or delayed. Note that there is no official distinction between In Progress, Ongoing, Not Started, and Planned Pending. In Progress is the preferred entry for all new POA&Ms but Components may use any of these others for internal tracking purposes, if desired.
- Ongoing – should be used when any activities needed to resolve a weakness have begun. This optional category can be used in lieu of or in addition to “In Progress” at Component discretion and may be used to make finer distinctions regarding the progress of individual activities.
- Not Started – can be used when no action has been taken to resolve the weakness. This optional category can be used in lieu of or in addition to “In Progress” at Component discretion and may be used to make finer distinctions regarding the progress of individual activities.
- Planned/Pending – can be used when planning has begun but no action has been taken to actually resolve the weakness. This optional category can be used in lieu of or in addition to “In Progress” at Component discretion and may be used to make finer distinctions regarding the progress of individual activities.
- Draft - should be used to indicate a POA&M has not been finalized (i.e., still a draft). POA&Ms with this status will not be included in the scorecard for 30 days after the POA&M creation date, but will automatically be changed to a status of “In progress” if not updated after 30 days. This status is not intended to change any requirements for entering POA&Ms in TAF but rather is intended to provide flexibility when entering and reviewing data.
- Waiver - should be used when a POA&M will take longer than six months to complete. When this status is used, an approved DHS waiver artifact must be uploaded in TAF. Use of

this status category must be approved by the Component CISO in TAF. Additionally, the DHS CFO must approve all requests for waivers and exceptions for CFO designated Systems prior to their submission to the DHS CISO. Approved waiver and exception requests must follow procedures in MD 4300A Attachment B.

- Exception – should be used when a POA&M will not resolve a weakness. When this status is used, an approved DHS exception artifact must be uploaded in TAF. Use of this status category must be approved by the Component CISO in TAF. Additionally, the DHS CFO must approve all requests for waivers and Approved waiver and exception requests must follow procedures in MD 4300A Attachment B exceptions for CFO designated systems prior to their submission to the DHS CISO.
- Completed – should be used only when a weakness has been fully resolved and the corrective action has been tested and approved. Therefore, corrective action testing should be incorporated into the weakness mitigation process and identified as a milestone. Completed items should remain in the POA&M for a full year after the completion date.
- Cancelled – should be used when the condition that was identified as a weakness is no longer an unacceptable risk, but has not otherwise been resolved. Examples of weaknesses that should be cancelled include: when a decision has been made by the AO to accept the risk after the weakness has been entered in the POA&M; when a system is retired; when responsibility for a system has been transferred to another Component. A “Cancelled” weakness is treated and counted as a completed weakness. When the status is cancelled, a reason for the cancellation must be selected from the dropdown menu in TAF after clicking the red ellipsis button. When “Other” is selected as a reason, an explanation must be entered in the box provided. Additionally, a POA&M with a status of “cancelled” requires approval from the Component CISO in TAF.
- Delayed – should be used if a weakness will be completed after the Scheduled Completion Date. TAF automatically changes the status to “Delayed” when the Scheduled Completion Date has passed. Use of this status category must be approved by the Component CISO in TAF. When the status is delayed, an estimated completion date must be entered in the appropriate field in TAF (see Section 4.2.5) and a reason for the delay must be selected from the dropdown menu in TAF after clicking the red ellipsis button. Examples of reasons for delay include:
  - Weakness priority changed
  - Original completion time underestimated
  - Funds not allocated/Insufficient funding
  - Assigned funds reallocated
  - Dependency on other task(s)
  - Contractor delay
  - Procurement delay
  - Personnel shortage
  - Technical dependency

- Other (describe in notes)



Status: In Progress

Point of Contact (name, phone, email):

Resources Required:

Type:

Is Material Weakness?:

Exclude from OMB Reporting: No

Figure 6. Status Dropdown Menu in TAF

Criticality (Priority) (Required)

See Section 3.0

Point of Contact (POC) (Required)

A point of contact (POC) must be listed in the POA&M for each weakness. The POC should be someone who is knowledgeable about the program or system and the weakness. The name and contact information (e.g., phone number and e-mail address) for the POC should be entered. This data is entered in the "Point of Contact" field in TAF. TAF automatically enters the contact data for the person who is logged in when the weakness is created but this may be changed if necessary by selecting the red ellipsis box next to this field in TAF. POCs for individual milestones may also be designated separately and may be different from the overall POC listed on the weakness screen as seen in Figure 15.

Risk Category (Required)

See Section 3.0

Resources Required (Required)

Every weakness identified in a POA&M must identify the resources required and source of funding to resolve it. Resources can include funding, staffing, equipment (e.g., hardware or software) or other items, such as training. The resources required will be based on the total amount of resources needed to fulfill all the milestones for resolution of a weakness.

Resources must be identified as a dollar amount and entered in the Resources Required field in TAF. The dollar amount can be determined in one of two ways:

- If a vendor is contracted to do the work, the value of the contract should be used.

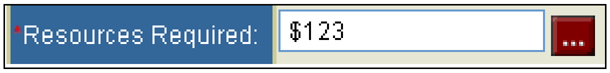
- If an existing asset (contractor or government employee) will do the work, the dollar amount can be determined by multiplying the time (i.e., number of hours) it will take to complete the work by the labor rate of the person(s) who will perform the task. Resources must include both government employees and contractors.

Any other costs (e.g., hardware, software, licenses, training, travel, support and maintenance fees, etc.) should also be included in this dollar amount.

The program manager, system owner, ISSO, system administrator, and/or others (as appropriate) should determine the time required. The program manager or system owner should be able to provide rate information for the weakness resources.

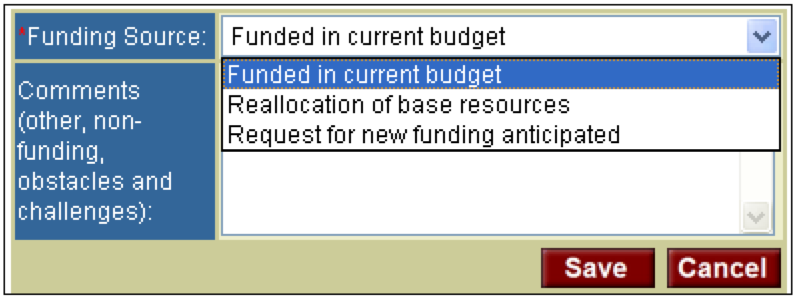
For example, if a service provider is already tasked to update patches as part of a contract, the resources required can be calculated by determining how many hours it will take to implement and test the patch, and multiplying that number by the rate for that labor category responsible for the work.

After the dollar figure has been entered in TAF, click on the **save** button on the bottom of the weakness screen and then click the ellipsis (see Figure 7) to enter the source of the funding, in the 'Funding Source' field (see Figure 8). Ensure that resources are identified as monetary values in whole numbers (e.g., $75,000) rather than $75k.



*Resources Required: $123

Figure 7. Resources Required Field in TAF



*Funding Source: Funded in current budget

Comments (other, non-funding, obstacles and challenges):

Funded in current budget
Reallocation of base resources
Request for new funding anticipated
Save
Cancel

Figure 8. Funding Source Dropdown Menu in TAF

Ensure that monetary funding is identified as "Funded in current budget," "Reallocation of base resources," or "Request for new funding anticipated."

"Funded in current budget" means that the required activities are already ongoing or are planned and funded and no action is needed to obtain additional resources. For example, a new firewall has been ordered and it will be installed and tested by existing staff when it arrives.

'Reallocation of base resources" means that resources planned for a different purpose will be used to remediate this weakness. For example, plans to upgrade servers have been postponed and the funds to obtain the servers will now be used to procure a firewall.

"Request for new funding anticipated" means that there are currently no resources available to remediate this weakness and new funding will be needed. This request for funding may be made within the organization (e.g., Program Office or Component) or through the budgetary process. Anytime "Request for new funding anticipated" is selected, a milestone must be included to show the actions needed to obtain the funding.

Resource data is entered in the "Resources Required" field in TAF with additional details provided in "Funding Source" fields in TAF. The reasonableness criteria provided in Appendix G provides a minimum level of resources that are considered appropriate for each NIST SP 800-53 control. However, the actual amount determined by management should be entered.

Severity (Required)

The severity level should be selected from the TAF Weakness screen 'Severity' field drop down menu and precedes the description of the weakness in the POA&M report. OMB defines three levels of severity for weaknesses:

- Significant deficiency,
- Reportable condition, and
- Other weakness.

Most weaknesses at the system level should be reported as a Reportable Condition or Other. In general, the significant deficiency category should be used rarely and only with senior management concurrence. Each of these severity levels is described below.

Significant Deficiency

In M-09-29, OMB defines a significant deficiency as:

> A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that **significantly restricts the capability of the agency to carry out its mission** or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

A significant deficiency under FISMA is to be reported as a **material weakness** under the Federal Managers Financial Integrity Act (FMFIA). As required in FISMA (section 3544(c)(3)), agencies are to report any significant deficiency in policy, procedure, or practice as a material weakness in reporting under FMFIA and if relating to financial management systems, as an instance of a lack of substantial compliance under FFMIA. Examples of significant deficiencies include lack of basic management control such as assignment of responsibility, a workable security plan, or a lack of substantial compliance under FMFIA.

Determining whether a security weakness is a significant deficiency must be a risk-based decision. Before designating a weakness as a significant deficiency, Component management and Inspectors General must carefully consider if weaknesses are systemic in nature and adversely affect other forms of management control as well as the gravity of the risk and magnitude or harm which may result should the weakness remain uncorrected. Additionally, any weakness that is to be designated as a significant deficiency/material weakness should be coordinated with the DHS CISO or Director of Compliance.

In general, the significant deficiency category should be used rarely and only with senior management concurrence. However, when a finding is identified as a material weakness by an auditor, it should be assigned a severity level of “significant deficiency.” In cases where an audit finding identifies a system or program as a material weakness, each POA&M that addresses a weakness (i.e., recommendation) identified in the audit report must be labeled a “significant deficiency.” When this categorization is used, the CISO must also select “yes” in the “Is Material Weakness” dropdown menu on the weakness screen and approve the weakness as described in section 4.4.

<u>Reportable Condition</u>

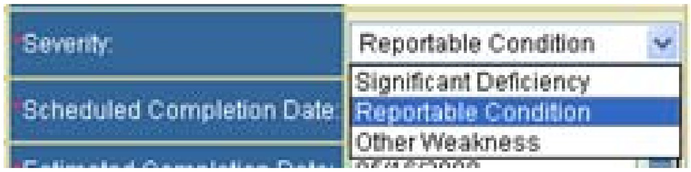
OMB defines a reportable condition in M-04-25 as follows:

> A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency, yet affecting the efficiency and effectiveness of operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. Reportable conditions are to be included in the POA&M. A reportable condition under FISMA is not reported as a material weakness under FMFIA. Most weaknesses identified in the DHS POA&M will be reportable conditions.

<u>Other Weakness</u> - Identified weaknesses that do not fall into either category above should be reported as an “other” weakness.

Simply put, not all security weaknesses introduce the same level of risk. For example, never having performed a certification and accreditation of a system is more problematic than having certification and accreditation expire simply due to passage of time. Similarly, failure to test and evaluate security controls within a high-risk national security system is starkly different than the same failure for a low-risk publicly accessible website. Additionally, a general failure to adequately train agency employees on their security responsibilities introduces different risks than not training systems administrators on their specialized security responsibilities. Whether any of the circumstances in the examples warrants designation as a significant deficiency or reportable condition, can only be determined after thoughtful consideration of the actual risk on a case-by-case basis.

Figure 9 illustrates the Severity Level drop down menu found in TAF.



*Severity: Reportable Condition

Figure 9. TAF Severity Level Dropdown Menu

Type (Autom atically filled in by TAF)

The type field is automatically filled in by TAF depending upon if the POA&M is a system or program level POA&M.

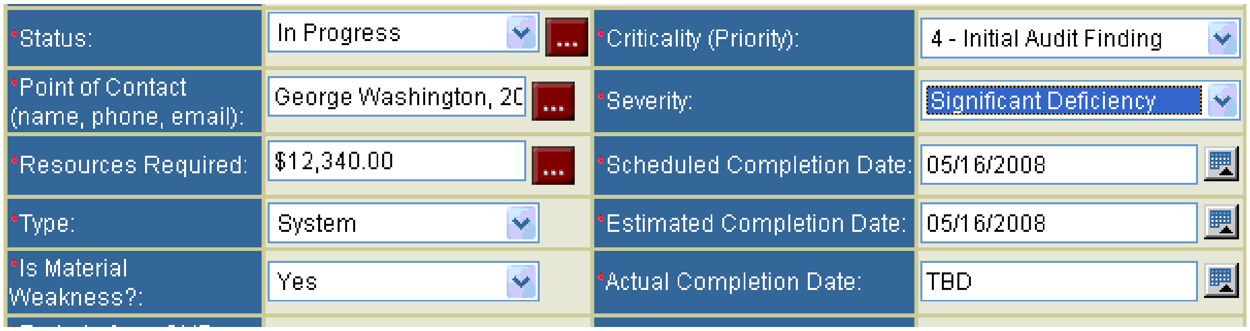
Scheduled Completion Date (Required)

The scheduled completion date should be determined based on a ***realistic*** estimate of the amount of time it will take to plan, allocate needed resources, and complete the corrective action. It is important to assign a scheduled completion date that is ***achievable*** because once entered and approved, **this date cannot be changed**. Draft documents do not receive credit for completion, so it is important to factor review and testing into the timeline. System POA&Ms that cannot be completed within timelines defined in the current FY DHS Information Security Performance Plan (currently six months), require a waiver or exception for non-compliance with DHS policy signed by the DHS CISO, or his designated official, (see DHS MD 4300A Attachment B for guidance on Waivers and Exceptions). Note that the Component CFO must approve any Waiver / Exception requests for CFO designated Financial Systems (before sending to the CISO).

The scheduled completion date for resolving the entire weakness should be entered in the "Scheduled Completion Date" field in TAF.

Is Material Weakness (Required)

If the severity level is listed as "Significant Deficiency," the Component CISO must also select "Yes" in the "Is Material Weakness?" dropdown menu on the weakness screen and approve the weakness as described below in the ISSM Validation section. Figure 10 illustrates the section of the weakness screen with the "Severity Level," "Is Material Weakness," windows.



*Status:	In Progress	*Criticality (Priority):	4 - Initial Audit Finding
*Point of Contact (name, phone, email):	George Washington, 20	*Severity:	Significant Deficiency
*Resources Required:	$12,340.00	*Scheduled Completion Date:	05/16/2008
*Type:	System	*Estimated Completion Date:	05/16/2008
*Is Material Weakness?:	Yes	*Actual Completion Date:	TBD

Figure 10. Material Weakness Data Screen

Estimated Completion Date (Required)

The "Estimated Completion Date" field in TAF is used to change the date that the weakness will be resolved if it exceeds the original in "Scheduled Completion Date." The Estimated Completion Date should be updated as often as necessary to ensure there is a current plan. Estimated completion dates that have passed are considered "overdue" and are reported to OMB by DHS. For new POA&Ms, the Estimated Completion Date should be the same as the Scheduled Completion Date.

Exclude from OMB Reporting (Not Applicable)

The exclude from OMB reporting field in TAF cannot be changed by users.

Actual Completion Date (Automatically filled in by TAF)

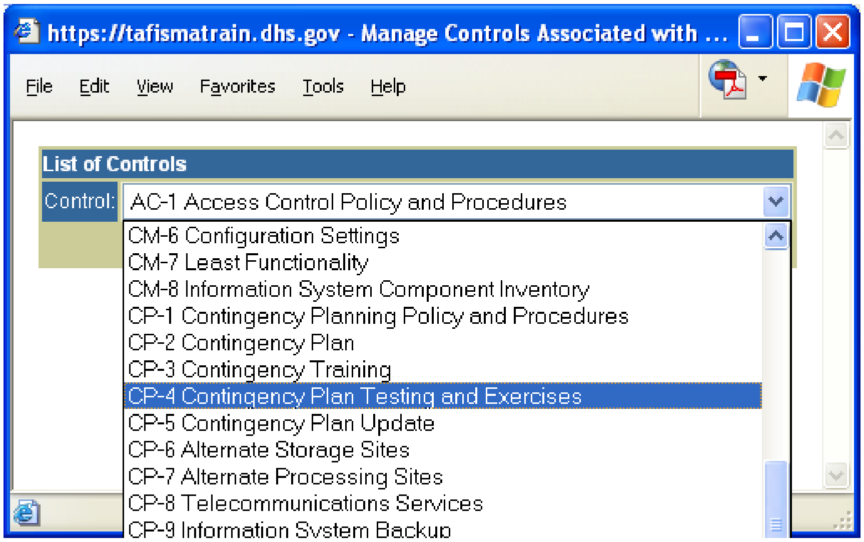
Once a weakness is resolved and all milestones are completed, the actual completion date should be entered in the "Actual Completion Date" field in TAF. When an actual completion date is entered, the status should also be changed to "Completed." Note that TAF automatically assigns the current date in the "Actual Completion Date" field in TAF when the status is changed to "Completed." However, this date can be changed to reflect the date all actions were completed. Future dates should not be entered and will result in failing POA&M validation when reported to senior management.

Risk Accepted (Not Applicable)

The risk accepted field in TAF cannot be changed by users.

Link to Control Title (Required)

All weaknesses must be linked to a Control Title in TAF to help identify trends in weaknesses across systems, Components and the Department and ensure metrics used for scorecards and other reporting are accurate. For weaknesses identified through the C&A process or the annual assessment process, 800-53 control titles are already identified through the Requirements Traceability Matrix (RTM). Weaknesses identified by other sources, such as audits or scans, and weaknesses involving 4300A controls must be mapped to the most appropriate 800-53 control. Multiple control titles can and should be used when POA&Ms are designed to resolve weaknesses across several different control titles. For scorecard purposes, reasonableness criteria are combined when more than one control title is identified. Figure 11 illustrates the dropdown menu used to select the control title. The window is activated by clicking the red ellipsis button next to the link to control title box. Note that the elipisis is only available after the page is saved. Multiple control titles can be added to a POA&M one at a time using the "link to control title" ellipsis.


https://tafismatrain.dhs.gov - Manage Controls Associated with ...
File Edit View Favorites Tools Help

List of Controls

Control: AC-1 Access Control Policy and Procedures

- CM-6 Configuration Settings
- CM-7 Least Functionality
- CM-8 Information System Component Inventory
- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- CP-5 Contingency Plan Update
- CP-6 Alternate Storage Sites
- CP-7 Alternate Processing Sites
- CP-8 Telecommunications Services
- CP-9 Information System Backup

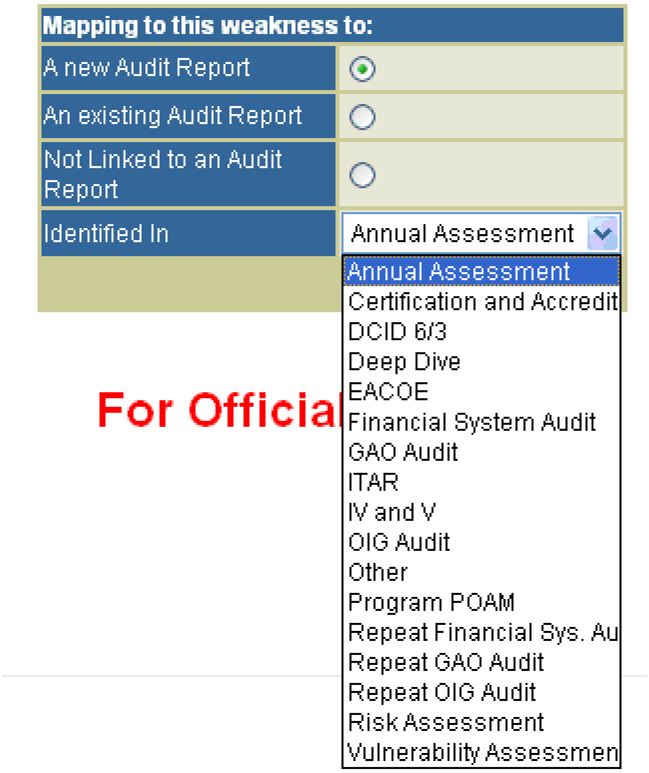
Figure 11. Control Title Dropdown Menu

Weakness ID (Not Applicable)

The weakness ID field in TAF cannot be changed by users.

Identified In (Required)

Each POA&M must have at least one weakness source identified. All weaknesses identified in any source must be captured in a POA&M and the source identified using the “Identified in” dropdown menu in TAF as illustrated in Figure 12. “Program POA&M” may be used to link a system POA&M to a program POA&M to ensure that a program level solution is actually implemented at the system level. This optional feature can be useful in tracking long term solutions that are implemented across multiple systems. If a weakness is identified in a source not included in the dropdown menu’ “other” should be used.



Mapping to this weakness to:	
A new Audit Report	●
An existing Audit Report	○
Not Linked to an Audit Report	○
Identified In	Annual Assessment

Figure 12. Weakness Sources (Identified in) Dropdown Menu in TAF

Details for weaknesses identified in the following sources must also be captured in the Report Identification screen as illustrated in Figure 12:

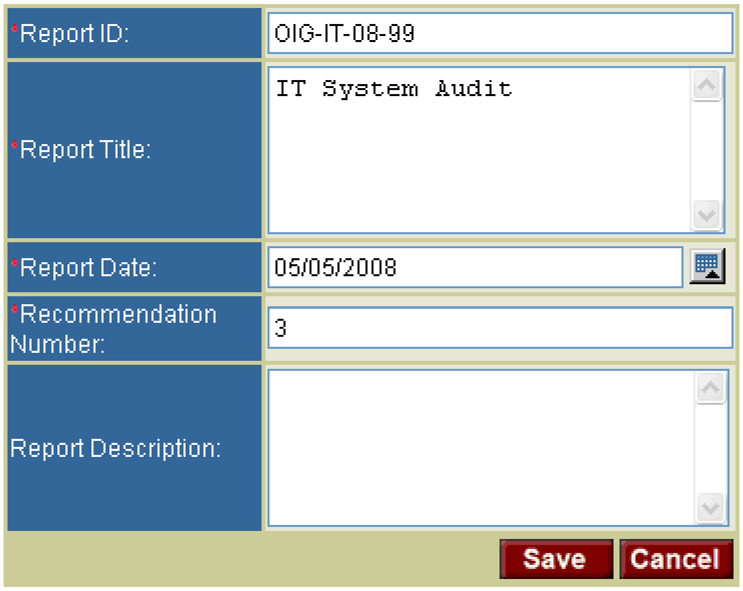
- C&A activities (SAR)
- Annual Assessments
- OIG audits
- GAO audits
- Financial audits (NFRs)
- ITAR Conditions

- EACOE Conditions
- Deep Dives
- CCRs
- FDCC
- OMB A-123 ITGC Assessment

For each of these sources, select the appropriate category (e.g., SAR, GAO audit, Repeat OIG audit, ITAR Condition, etc) then click the "A new audit report" radial button and fill in the report number, title and date and recommendation number. Note that the "new audit report" function should be used regardless of the source to allow appropriate data to be entered, even if the source is a repeat audit finding.

When OIG or GAO audit reports a source, the actual audit report number, not the finding number should be entered in the Report ID field. For financial audits, the Notice of Findings and Recommendations (NFR) number should be used. It is extremely important to enter the Report ID correctly for all audits to ensure you receive proper credit on the scorecard. Report IDs entered incorrectly will not receive credit on the scorecard. Additionally, if the source of the weakness is from an ITAR review, the ITAR Condition ID number must be included in the Report ID field. Likewise, if the source of the weakness is from an EACOE review, the EACOE log number and condition number must be included in the Report ID field. This information can be obtained from the program manager and/or system owner. For SARs or other documents that do not have a discrete report number, use the type of the report in this field.

Enter each recommendation number from the report for tracking purposes. If the source report does not have numbered recommendations, assign a sequential number for each bullet under the recommendation section. Note that there may be more than one recommendations section. In that case, continue the sequential numbering process throughout the entire report.



*Report ID:	OIG-IT-08-99
*Report Title:	IT System Audit
*Report Date:	05/05/2008
*Recommendation Number:	3
Report Description:	

Figure 13. TAF Screen Used to Enter Source Data

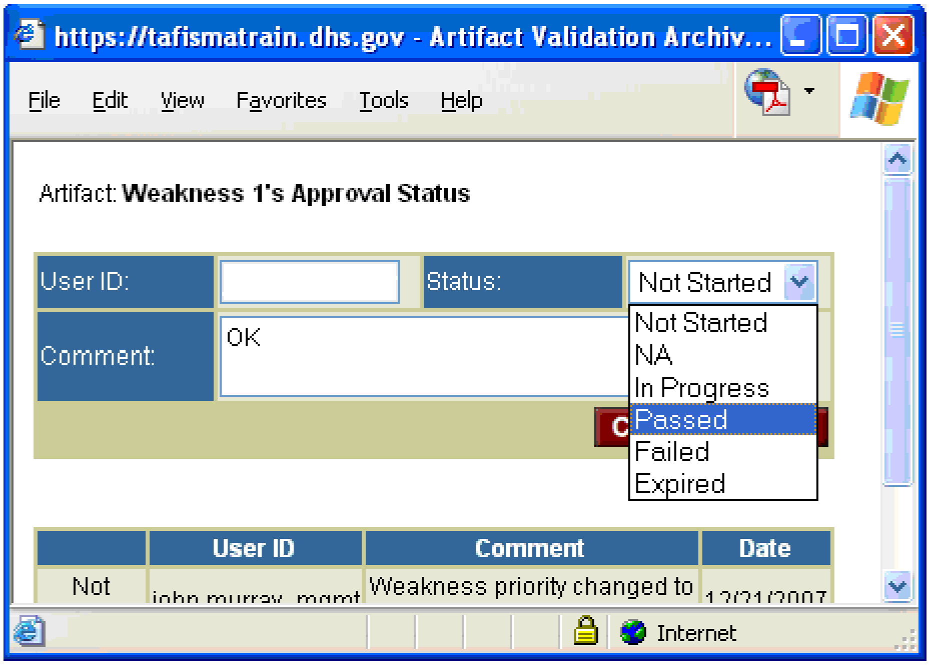
In the event that duplicate or multiple sources cite a specific weakness, all sources must be noted in the POA&M for accountability purposes. Multiple sources can be linked to the same weakness in TAF, thus eliminating multiple line items for the same weakness. The goal is to ensure that all weaknesses are addressed and to be able to identify a POA&M that will resolve every weakness identified. Note that new sources can only be added to open POA&Ms. Once a POA&M is marked as completed, additional findings or sources cannot be linked to it. For example, if a POA&M for an audit finding is closed and a repeat audit finding is issued in the following year, the new report number cannot be linked to the old POA&M, since the original plan obviously was not good enough to resolve the finding. If this occurs (i.e., a new weakness is identified in a report issued after the original POA&M is closed), Components must create a new POA&M in TAF.

When adding a new source to an existing weakness, be sure to check if there is any impact on the prioritization. For example, if a weakness originally identified in an annual assessment was subsequently identified in an audit, the priority should be changed from a 2 to a 4. If the original source was an audit and the new source is a C&A, the priority should remain a 4.

ISSM Validation (Required)

As part of their oversight responsibilities, Component CISOs are required to monitor the status of POA&Ms. Component CISOs must formally approve all Priority 4 and Priority 5 POA&Ms in TAF when they are new and when they are closed. The approval of closed POA&Ms should include a review of the artifact that has been uploaded to ensure it provides adequate evidence of closure. They must also formally approve all POA&Ms with a status of “Delayed”, “Cancelled”, “Waiver” and “Exception.” A comment must be entered as part of each review. The comment should include reason for failure if “failed” is selected. If the Component CISO passes the POA&M, a simple comment of “OK” is adequate. In addition to the above, Component CISO’s must also formally approve all Priority – 3 Program-Level POA&Ms.

Component CISOs can access the approve window through the Weakness screen or through the Weakness Search Report. Figure 14 illustrates the TAF window where Component CISOs must select the proper approval status and enter a comment, which is a mandatory field.



https://tafismatrain.dhs.gov - Artifact Validation Archiv...
File Edit View Favorites Tools Help
Not Started
NA
In Progress
Passed
Failed
Expired
C
Internet

Artifact: **Weakness 1's Approval Status**

User ID:		Status:	Not Started
Comment:	OK		

	User ID	Comment	Date
Not	john murray_mgmt	Weakness priority changed to	12/21/2007

Figure 14. ISSM Validation Screen

HQ Review (Optional)

This field is completed by DHS HQ only.

Milestones

Each new weakness must have at least one (or more) milestone(s) if open greater than three months and scheduled completion date associated with it. Milestones should effectively communicate the major steps that will be performed to mitigate a weakness. The number of milestones articulated per weakness should reflect the number of major steps or corrective actions necessary to address the weakness. One milestone for each 3 months of schedule for the POA&M is recommended to be able to capture major activities needed and to be able to monitor progress over time.

In general, milestones should address root causes, resource allocation, activities to resolve weaknesses, updating documentation, and testing or approval of the change. Milestones should be developed not only to address the specific weakness that has been identified but also the underlying cause of that weakness to ensure the weakness does not recur. Depending on the individual weakness, some of these areas may not be appropriate or additional milestones may be included. POA&Ms that address a financial audit finding are required to include a milestone to test the remediation activity before it can be closed in addition to the milestone to resolve the weakness.

Milestones should not simply re-state that the weakness will be completed by repeating the weakness description but rather should describe an action needed to correct a weakness. For example, appropriate milestones for a weakness like, “patches are not current” could include:

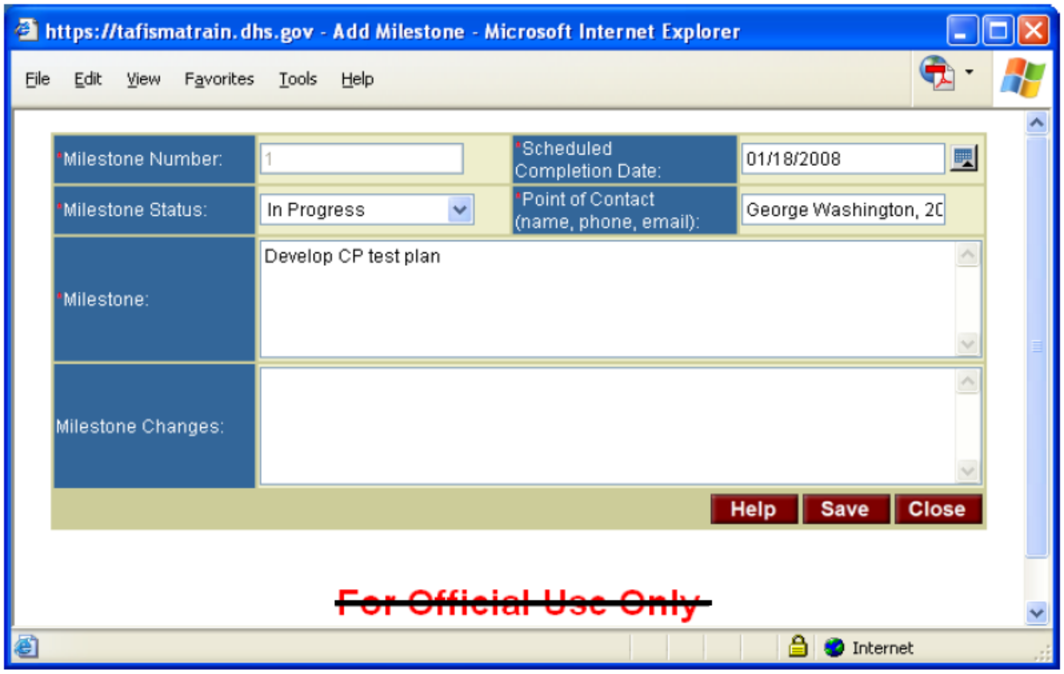
- Determine root causes

- Update patch policy;
- Develop procedures to standardize the patch update process;
- Establish a test environment for implementing patches before applying them to the production environment;
- Test the process; and
- Update system patches.

Appendix F to this Guide contains examples of acceptable and unacceptable milestone descriptions. The first milestone should be entered directly into the Weakness Screen in the Milestone Description box (see Figure 15). A Milestone Scheduled Completion Date must also be entered. To enter additional milestones, click save, and then click "new" under List of Milestones to bring up the appropriate page. Figure 15 illustrates the screen used to enter more than one milestone in TAF.

The scheduled completion date for each milestone should be entered in the "Scheduled Completion Date" field and the milestone description should be entered in the "Milestone" field. The status and POC for individual milestones is not required but provides a useful means for Components to track the progress of activities toward resolution of the weakness. As many additional milestones as needed may be added by selecting "new" on the Weakness Screen.

Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones or their schedule, they should be entered by clicking "edit" under List of Milestones and filling in appropriate fields.


https://tafismatrain.dhs.gov - Add Milestone - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Help
Save
Close
Internet

*Milestone Number:	1	*Scheduled Completion Date:	01/18/2008
*Milestone Status:	In Progress	*Point of Contact (name, phone, email):	George Washington, 2C
*Milestone:	Develop CP test plan		
Milestone Changes:			

~~For Official Use Only~~

Figure 15. TAF Milestone Window

Changes to Milestones

If a situation exists that prevents a milestone and/or overall corrective action from being completed on time, the new date and reason need to be recorded in the Milestones Changes column of the POA&M report. No changes should be made to the original estimate in either the 'Scheduled Completion Date' or the 'Milestones with Completion Date.'

If there are changes to any of the milestones or their schedule, that do not affect the overall completion date, they should be entered by clicking "edit" under List of Milestones and filling in appropriate fields. Milestone changes can be entered in the Milestone Window in TAF by clicking "edit" in the weakness screen.

4.3 Closing a POA&M

When all milestones have been completed, the POA&M may be closed. To close a POA&M, select the status "Completed" from the drop down menu (see Figure 6) and change the "Actual Completion Date" field to the date the final action was completed. TAF defaults to the date the change is made to the status field but the actual date should be entered if it is not the same.

For Priority 4 and 5 POA&Ms, an artifact must be uploaded into TAF with evidence that the weakness has been resolved and the Component CISO must approve the action (see section 4.4). Artifacts can include a letter from the auditor stating the weakness has been resolved or any other form of documentation that demonstrates that all corrective actions have been successfully completed. In cases where the artifact would be especially lengthy or contain specific details of a weakness (e.g., a scan report) only the cover page, table of contents and signature page (where applicable) need to be uploaded as long as the original document is available for inspection by the DHS compliance team or auditor.

POA&Ms for audit reports that are issued as repeat findings with a new audit or NFR number should not be closed, even if the prior year finding is closed by the auditor. As long as the original finding remains unresolved, the original POA&M should remain open and additional or repeat findings should be added to the "identified in" field (see section 4.2.9). Additional milestones may be added as needed using the milestone changes field (see section 4.2.8).

4.4 POA&Ms for Classified Systems

All National Security Systems **must** have a POA&M to document their plan for resolving weaknesses. POA&Ms for classified systems should be developed following the process described in Section 3 of this document and entered in TAF/C following the same process described in Section 4. No classified data should ever be entered into the SBU version of TAF

5.0 REPORTS

DHS produces a variety of daily, monthly, and quarterly reports to track the status of POA&M activity. These reports are described below.

5.1 Daily Reports

DHS produces a daily report indicating POA&Ms that do not meet performance plan standards. This report is automatically disseminated via Crystal Reports to CISOs/ISSMs and a select group of designated users at each Component. Requests for distribution of this report should be made to Component CISOs/ISSMs. Details on elements that are included in the scorecard and grading criteria can be found in the current year DHS Information Security Performance Plan. .

5.2 Monthly Reports

DHS produces a monthly scorecard which includes metrics on POA&M quality, management, completeness, reasonableness, and timeliness of POA&M closures. The scorecard is intended to monitor POA&M progress, identify potential problem areas and provide feedback to Department and Component managers. It is disseminated at CISO Council and CIO Council meetings each month. Details on elements that are included in the scorecard and grading criteria can be found in the current year DHS Information Security Performance Plan.

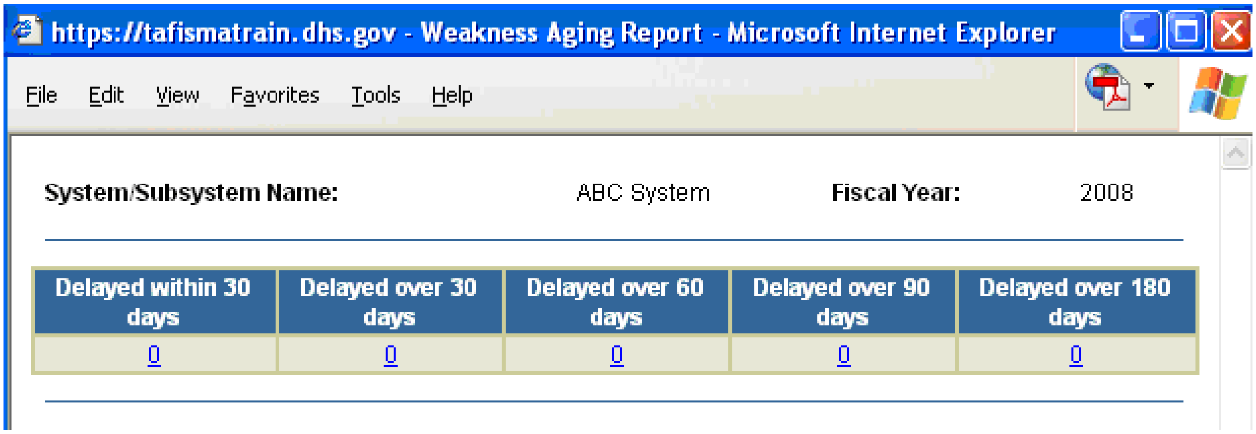
5.3 Quarterly Reports

DHS must provide summary information on the POA&M progress and an update on information security performance measures to OMB on a quarterly basis. The quarterly updates enable the Department and OMB to monitor Component remediation efforts and identify progress and problems. DHS extracts data for these reports from TAF. Thus, it is essential that data in TAF is current, complete and accurate.

5.4 TAF Reports

TAF has a number of reports available that support the POA&M monitoring and oversight function. A brief description of these reports is provided below. A full description of each report and input / output options can be found in the TAF Reports Manual, which is available on-line by clicking the Technical Support option on the bottom of the TAF page and selecting the Training Materials tab.

- **Plan of Actions and Milestones**
  This report displays all eight POA&M columns and identification data by system.
- **Weakness Aging Report**
  This report displays the number of weaknesses for systems within a Component that are delayed for more than 30, 60, 90, and 180 days. This report allows the user to drill down to the individual weakness screen. Figure 16 illustrates the weakness aging report output.

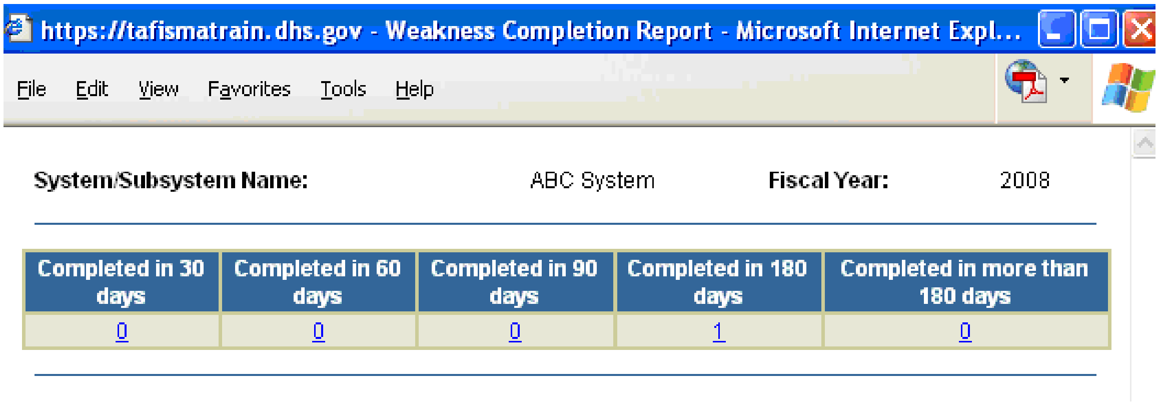

https://tafismatrain.dhs.gov - Weakness Aging Report - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help

System/Subsystem Name: ABC System Fiscal Year: 2008

Delayed within 30 days	Delayed over 30 days	Delayed over 60 days	Delayed over 90 days	Delayed over 180 days
0	0	0	0	0

Figure 16. Weakness Aging Report Output

- **Weakness Completion Report**
  This report displays the number of weaknesses for systems within a Component that are scheduled for completion within 30, 60, 90, and 180 days. This report allows the user to drill down to the individual weakness screen. Figure 17 illustrates the weakness completion report output.


https://tafismatrain.dhs.gov - Weakness Completion Report - Microsoft Internet Expl...
File
Edit
View
Favorites
Tools
Help

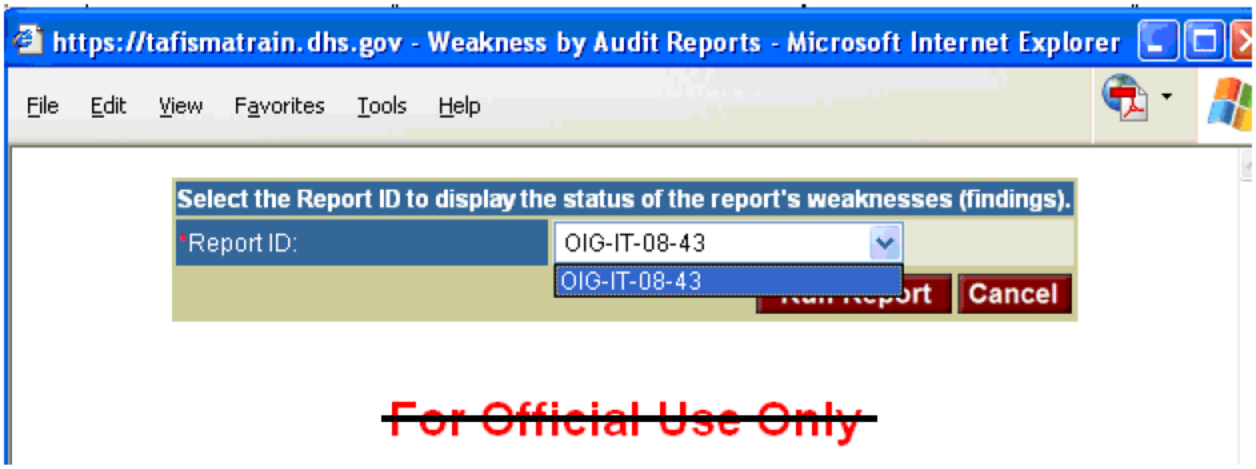
System/Subsystem Name: ABC System Fiscal Year: 2008

Completed in 30 days	Completed in 60 days	Completed in 90 days	Completed in 180 days	Completed in more than 180 days
0	0	0	1	0

Figure 17. Weakness Completion Report Output

Weakness by Audit Reports

This report displays the report numbers that have been entered in the "Report ID" field, as described in section 4.2.9, and allows the user to drill down to individual weaknesses identified in the report. Figure 18 illustrates the weakness by audit reports output.


https://tafismatrain.dhs.gov - Weakness by Audit Reports - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Run Report
Cancel

Select the Report ID to display the status of the report's weaknesses (findings).

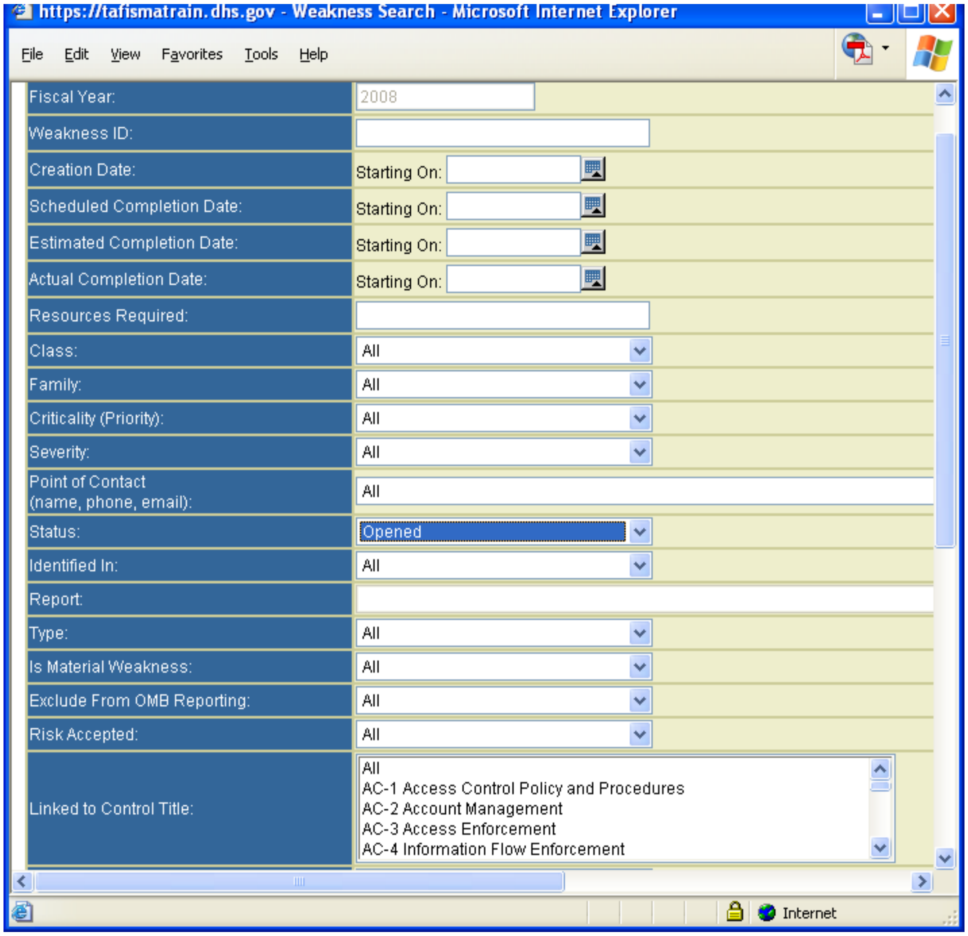
*Report ID: OIG-IT-08-43

OIG-IT-08-43

~~For Official Use Only~~

Figure 18. Weakness by Audit Reports Output

- **<u>Weakness Search Report</u>**
  This report displays all POA&M related data for a system or program and allows the user to drill down to individual weaknesses. This is one of the most useful reports because of the large number of filters or sort options that are available. The report also allows the user to select data elements to be displayed as output. Some columns of this report can be sorted to help with usability. The report can also be exported to an Excel spreadsheet which also allows the user to manipulate data for analysis purposes. Figure 19 illustrates the search filters and a sample of the report. Appendix H to this Guide provides Weakness Search Report queries that can be run to verify compliance with scorecard criteria.


https://tafismatrain.dhs.gov - Weakness Search - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Internet

Fiscal Year:	2008
Weakness ID:	
Creation Date:	Starting On:
Scheduled Completion Date:	Starting On:
Estimated Completion Date:	Starting On:
Actual Completion Date:	Starting On:
Resources Required:	
Class:	All
Family:	All
Criticality (Priority):	All
Severity:	All
Point of Contact (name, phone, email):	All
Status:	Opened
Identified In:	All
Report:	
Type:	All
Is Material Weakness:	All
Exclude From OMB Reporting:	All
Risk Accepted:	All
Linked to Control Title:	All AC-1 Access Control Policy and Procedures AC-2 Account Management AC-3 Access Enforcement AC-4 Information Flow Enforcement

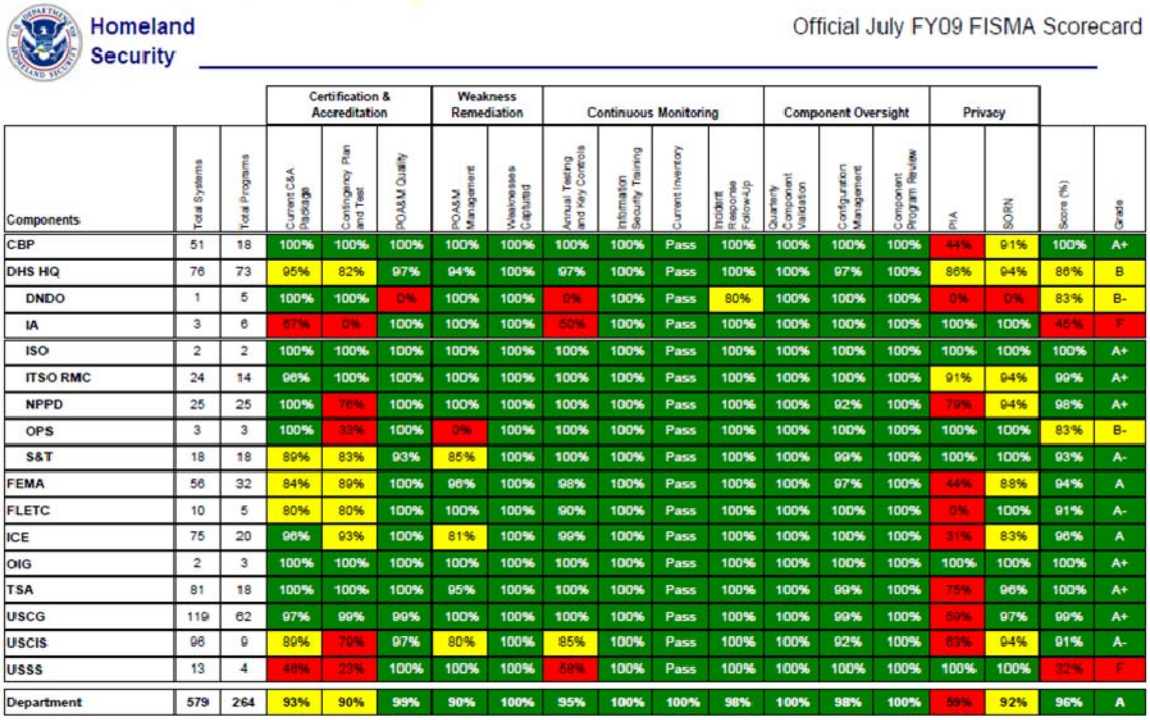
Figure 19. Weakness Search Report Options

6.0 ENSURING A COMPREHENSIVE POA&M PROCESS

To help ensure the POA&M process is comprehensive and applied consistently, DHS provides a variety of support options. Available support is described in following sections.

6.1 Scorecard

DHS produces a monthly scorecard which includes metrics on POA&M quality, management, completeness, reasonableness, and timeliness of POA&M closures. The scorecard is intended to monitor POA&M progress, identify potential problem areas and provide feedback to Department and Component managers. It is disseminated at CISO Council and CIO Council meetings each month. Details on elements that are included in the scorecard and grading criteria can be found in the current year DHS Information Security Performance Plan. A sample summary sheet of the scorecard is provided in Figure 20. In addition to summary sheets, each Component also receives a number of feeder reports which describe in detail data elements that contribute to each section of the scorecard.



Homeland Security

Official July FY09 FISMA Scorecard

			Certification & Accreditation			Weakness Remediation		Continuous Monitoring				Component Oversight			Privacy			
Components	Total Systems	Total Programs	Current C&A Package	Contingency Plan and Test	POA&M Quality	POA&M Management	Weaknesses Captured	Annual Testing and Key Controls	Information Security Training	Current Inventory	Incident Response Follow-Up	Quarterly Component Validation	Configuration Management	Component Program Review	PIA	SORN	Score (%)	Grade
CBP	51	18	100%	100%	100%	100%	100%	100%	100%	Pass	100%	100%	100%	100%	44%	91%	100%	A+
DHS HQ	76	73	95%	82%	97%	94%	100%	97%	100%	Pass	100%	100%	97%	100%	86%	94%	86%	B
DNDO	1	5	100%	100%	0%	100%	100%	0%	100%	Pass	80%	100%	100%	100%	0%	0%	83%	B-
IA	3	6	67%	0%	100%	100%	100%	50%	100%	Pass	100%	100%	100%	100%	100%	100%	45%	F
ISO	2	2	100%	100%	100%	100%	100%	100%	100%	Pass	100%	100%	100%	100%	100%	100%	100%	A+
ITSO RMC	24	14	96%	100%	100%	100%	100%	100%	100%	Pass	100%	100%	100%	100%	91%	94%	99%	A+
NPPD	25	25	100%	76%	100%	100%	100%	100%	100%	Pass	100%	100%	92%	100%	79%	94%	98%	A+
OPS	3	3	100%	33%	100%	0%	100%	100%	100%	Pass	100%	100%	100%	100%	100%	100%	83%	B-
S&T	18	18	89%	83%	93%	85%	100%	100%	100%	Pass	100%	100%	99%	100%	100%	100%	93%	A-
FEMA	56	32	84%	89%	100%	96%	100%	98%	100%	Pass	100%	100%	97%	100%	44%	88%	94%	A
FLETC	10	5	80%	80%	100%	100%	100%	90%	100%	Pass	100%	100%	100%	100%	0%	100%	91%	A-
ICE	75	20	96%	93%	100%	81%	100%	99%	100%	Pass	100%	100%	100%	100%	31%	83%	96%	A
OIG	2	3	100%	100%	100%	100%	100%	100%	100%	Pass	100%	100%	100%	100%	100%	100%	100%	A+
TSA	81	18	100%	100%	100%	95%	100%	100%	100%	Pass	100%	100%	99%	100%	75%	96%	100%	A+
USCG	119	62	97%	99%	99%	100%	100%	100%	100%	Pass	100%	100%	99%	100%	59%	97%	99%	A+
USCIS	96	9	89%	79%	97%	80%	100%	85%	100%	Pass	100%	100%	92%	100%	83%	94%	91%	A-
USSS	13	4	48%	23%	100%	100%	100%	59%	100%	Pass	100%	100%	100%	100%	100%	100%	32%	F
Department	579	264	93%	90%	99%	90%	100%	95%	100%	100%	98%	100%	98%	100%	59%	92%	96%	A

Figure 20. Sample Scorecard

6.2 POA&M Support

POA&M support is available from several sources. The TAF Help Desk representative is an excellent source for questions regarding both TAF and the POA&M process and may be reached at (b)(6) (b)(7)(C) or via e-mail at (b)(6) POA&M Subject Matter Experts (SMEs) are available by phone through the helpdesk to answer questions or provide "how to" help. Additionally, Review and Assist Visits are available through the DHS Compliance office. These visits are tailored to meet the specific requirements of the requesting organization and can range from formal training sessions for ISSOs through a one-on-one hands-on practicum using real system data.

Appendix A

Acronyms

Acronym	Meaning
AO	Authorizing Official (formerly DAA)
ATO	Authorization to Operate
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAA	Designated Accrediting Authority (Replaced by AO)
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FITSAF	Federal Information Technology Security Assessment Framework
FMFIA	Federal Managers Financial Integrity Act
FOUO	For Official Use Only
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HQ	Headquarters
IG	Inspector General
INFOSEC	Information Security
IPSO	Information Processing Service Organization
ISO	Information Security Office (formerly OIS)
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
NFR	Notice of Findings and Recommendations

Acronym	Meaning
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OIG	Office of Inspector General
OIS	Office of Information Security (Replaced by ISO)
POC	Point of Contact
PDD	Presidential Decision Directive
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RMS	Risk Management System
SP	Special Publication
TAF	TrustedAgent FISMA
TBD	To Be Determined
USC	United States Code

Appendix B

References

References

1. Public Law 107-347 [H.R. 2458], The E-Government Act of 2002 Title III, of this Act is the Federal Information Security Management Act of 2002 (FISMA), December 17, 2002.
2. Federal Information Processing Standards Publications (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
3. OMB Circular A-130, Management of Federal Information Resources, November 28, 2000.
4. OMB Memoranda titled Guidance for Preparing and Submitting Security Plans of Action and Milestones. Memos are produced annually and can be found at http://www.whitehouse.gov/omb/memoranda/index.html. Memos issued to date include 02-01, 03-19, 04-25, 05-15, 06-20, 07-19, 08-20, and 09-29.
5. National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series (e.g., NIST SP 800-53 Recommended Security Controls for Federal Information Systems) http://csrc.nist.gov/publications/nistpubs/index.html
6. DHS MD 4300A Sensitive Systems Handbook.
7. Fiscal Year 2010 DHS Information Security Performance Plan

Appendix C

POA&M Data Collection Worksheet

POA&M Data Collection Worksheet

Recording weaknesses and the remediation plan in TAF is the last step in developing a POA&M. The following worksheet can be used to guide POA&M development and collect the data that will be entered into TAF.

POC

Who will be responsible for ensuring this weakness is resolved (i.e., POC)?

Name ____

Phone ____

e-mail ____

Who will be responsible for resolving this weakness? __________________________________

Who needs to be involved in planning and implementation activities?

____

____

Weakness

What is the weakness? ____

____

What is the root cause of the weakness? ____

_________________________________ ____

What is the NIST SP 800-53 control?

____

Is it a:

- ( ) Significant deficiency (material weakness)
- ( ) Reportable condition
- ( ) Other (control deficiency)

What is the risk level of the weakness? High ___ Medium ___ Low ___

Weakness source

What is the source of the weakness?

____

Audit report number _______________________

NFR number _____________________________

Was this weakness previously identified by another source?

____

____

Priority

What priority should the weakness be? _____________________________________

( ) Repeat audit finding (Level 5)

( ) Initial audit finding (Level 4)

( ) IT acquisition review condition (Level 4)

( ) Enterprise architecture board condition (EAB/EACOE) (Level 4)

( ) A-123 Review (Level 4)

( ) FDCC (Level 4)

( ) C&A (Level 3 or higher)

( ) Critical Control Review (CCR) / Deep Dive finding (Level 3)

( ) Annual assessment (Level 2 or higher)

( ) Management decision (may raise any category above)

Resources

Who will do the work? How many hours will it take? What is their hourly rate?

____

____

What other resources are needed? (Hardware, software, licenses, training, etc) Are they available or will they have to be purchased?

____

____

____

Where will resources come from?

- ( ) Are resources available? (Funded in current budget)
- ( ) Will resources be diverted from another area? (Reallocation of base resources)
- ( ) Will new funding be requested? (Request for new funding anticipated)

Milestones

What is the root cause of the weakness? (consider policy, procedures, people, technology and resources)

____

____

____

What steps are needed to resolve the weakness?

Identify steps needed to resolve the weakness

____

____

____

Testing/documentation activities

____

____

Schedule

When will each of the steps needed to resolve the weakness be completed?

____

____

Is this schedule realistic and achievable?

Are there any steps that could be delayed by circumstances beyond your control?

____

____

Appendix D

POA&M Creation Checklist

POA&M Creation Checklist

The following checklist is intended to walk the user through the New Weakness screen in TAF to help ensure all fields are filled in properly. It assumes that data has already been assembled and properly coordinated and that the user has a basic understanding of the steps needed.

Directions to “select” refer to selecting an item from a drop down menu. Directions to “enter” refer to a text field that must have data typed in. Directions to “click” refer to a button or box that will bring up another window where data must be entered.

SAVE and CLOSE refer to the buttons at the bottom of the page.

Creating a POA&M:

On the System POA&M tab, select **New** under **List of Weaknesses**. The **Add Weakness** window will pop up.

- Select the **Class** of the weakness (Management, Operational, Technical)
- Select the appropriate **Family;** choices are derived from the 17 families identified in NIST 800-53
- The **Weakness Number** is automatically filled in by TAF.
- The **Creation Date** defaults to today’s date.
- Leave the **Finding** field blank; this can be used to record comments if desired.
- Enter the appropriate text into the **Weakness** field – This text can not be changed after saving, so ensure accuracy prior to saving.
- The **Status** field defaults to **In Progress;** select another entry if desired. .
- Enter **POC** data as necessary (TAF automatically assigns the user)
- Enter **Resource** amount in whole dollars
- The **Type** field defaults to the **System;** change if the POA&M is for a Program.
- The **Is Material Weakness** field defaults to **No**.
- The **Exclude from OMB Reporting** field defaults to **No**.
- The **Risk Accepted** field defaults to **No**. (If the risk was accepted, no POA&M is necessary)
- The **Weakness ID** field is not used. Leave blank.
- The **ISSM Validation** field defaults to **NA**; no further action required at this point. The CISO/ISSM will use this field to approve the POA&M.
- The **HQ Review** field defaults to **NA**; no further action required at this point. The DHS POA&M team will use this field to review the POA&M.
-
- Select the **Criticality / Priority** – corresponding to source of weakness or management decision (do not use priority 1)
- Select the **Severity** – select “reportable condition” or “other”
    - (CISO/ISSM approval required for significant deficiency)
- Select the **Scheduled completion date** – must be realistic and achievable, but less than 6 months for a system POA&M and less than 5 years for a program POA&M. – **cannot be changed**

- Select the **Estimated completion date** - use same date as Scheduled completion date
- The **Actual Completion Date** defaults to **TBD.** This field is only used when the POA&M is completed.

Click SAVE - Once the POA&M is saved, it will refresh with additional button selections.

- Click the red box next to Resources Required and select the **source of funding**
- Click the red box next to Link to Control Title and select the control title that applies to the weakness. Use multiple control titles if applicable. Control titles can only be selected one at a time but the process may be repeated as often as needed.
- Click the red box next to Identified in and select **New**
    - Select the appropriate **Source**, select **Save**. Multiple **Sources** may be identified.
    - Click the "A new audit report" radial button
    - Fill in report data
- The **List of Weakness Artifacts** is used to upload artifacts as evidence of completion or other related documents. It is not used at this point.
- To create the initial Milestone, enter the first milestone in the **Milestone Description** field. To enter additional milestones select **New** under **List of Milestones**. When the **Add Milestone** window pops up:
    - The **Milestone Number** defaults to the next value.
    - Enter the **Scheduled Completion Date** up to the date of the POA&M **Scheduled Completion Date**.
    - The **Milestone Status** defaults to **In Progress;** select another entry if desired.
    - The **POC** defaults to the POA&M **POC**; include a name and phone or e-mail information separated by commas if another POC is desired.
    - Enter the appropriate text in the **Milestone** field, select **Save**, and select **Close**.

Click SAVE

Click CLOSE

Delaying a POA&M

To Delay a POA&M:

- The **Status** is automatically changed to **Delayed** once the Scheduled Completion Date passes.
- Update the **Estimated Completion Date** to the new date.
- **Save** the POA&M.
- Select the red ellipsis box next to the **Status** field.
- Select a **Delay Reason** and do not select **Delayed/Unassigned.**
- Select **Save** and **Close.**
- Select **Edit** for any associated open **Milestones** (any Delayed POA&M should have at least one open **Milestone**).
- Set the Milestone Status to **Delayed**.
- Enter text in the **Milestone Change** field if any changes are needed.
- Select **Save** and select **Close**.

Completing a POA&M

To Complete a POA&M:

- Change the **Status** to **Completed**.
- Enter the **Actual Completion Date** if different than the current date.
- **Save** the POA&M.
- Select **Edit** for any associated open **Milestones.**
- Set the Milestone Status to **Completed**.
- Select **Save** and select **Close**.
- For Priority 4 and 5 POA&Ms, click on "New" in the List of Weakness Artifacts box and upload artifacts that provide evidence that all actions have been completed.

Canceling a POA&M

To Cancel a POA&M:

- Change the **Status** to **Cancelled**.
- **Save** the POA&M.
- Select the red ellipsis box next to the **Status** field.
- Select a **Cancelled Reason. If Other, enter the reason** in the text box**.**
- Select **Save** and **Close.**
- Select **Edit** for any associated open **Milestones.**
- Set the Milestone Status to **Cancelled**.
- Select **Save** and select **Close**.
- On the POA&M **Edit Weakness** window, select **Save**, select **OK**, and select **Close**.

Appendix E

Root Cause Analysis

Root Cause Analysis

Root cause analysis is a structured systems analysis methodology whose purpose is to identify the underlying causes of problems, issues, and/or events. The goal of root cause analysis is to identify the underlying problem(s) and solution(s) to problems by attempting to bound, correct, or eliminate underlying causes, as opposed to merely addressing the immediately obvious symptoms. This is important because correcting the underlying root cause may eliminate more than one seemingly unrelated symptom or address a prevalent issue across an entire organization.

The reasons for conducting a root cause analysis include:

- Help system owners and stakeholders understand information security impact to mission and operations
- Assist system owners, CISO and ISSOs with the assignment of risk and subsequent prioritization for remediation
- Identify underlying causes for control weaknesses in order to strengthen issues which are preventing the control from working as designed and/or implemented.
- Documenting root causes provide broader understanding of control gaps
- Reduce the likelihood of control recurrence by focusing corrective actions on the cause versus the systematic conditions which are more frequently reported.

There is usually more than one root cause for any given problem. Likewise, a root cause may be reflected in more than one symptom. To be most effective, the analysis should try to address all known causal relationships between the root cause(s) and the identified problem(s). When performing root cause analysis, always consider **Policies, Procedures, Process, People, and Systems Technology and Resources** in the investigation. For example, technical symptoms often have procedural or people-oriented root causes such as a poorly implemented internal control. Root cause analysis should be performed in an iterative manner, building upon the work of the previous iteration, and brain storming with multiple people with varying backgrounds and expertise should be encouraged to develop the most robust solutions.

Root cause analysis worksheets are provided at the end of this section to help the analyst identify, categorize, and document the root cause of a security control weakness or vulnerability. The form may also be used to assist in documenting the root cause of a weakness identified from multiple types of sources (*e.g.*, Audit, C&A, ST&E, annual assessment, etc.)

At a minimum, the following steps are recommended when conducting a root cause analysis:

1. Understand the impact of the identified problem (*i.e.*, a security control weakness) on business or mission needs; do not focus on the symptoms or technology issues. Try to first understand the problem, the context for the problem, and the stakeholders of the problem. Do not start investigating possible solutions until the problem is bound and defined from the people, process, and technology perspectives; otherwise the solution may bias the root cause analysis.

2. Consider the known threats and vulnerabilities associated with the security control weakness and understand the risk to and impact on the organization, location, program / project, a system, and/or the data and information.

3. Work with the system owners, CISO, ISSM, ISSOs, and audit liaisons to help **prioritize** the order in which control weaknesses should be addressed. For example, is the control weakness identified as a material weakness? Is it a significant deficiency or a reportable condition? Does it impact more than one Component system or site?

4. Identify and walk through the following potential root causes associated with the security control weakness:

   - Review the applicable **Policies** to determine if they provide clear requirements. Determine if the DHS guidance (*e.g.*, DHS MD 4300A Sensitive System Policy or Handbook as well as Component Policy or Handbooks) are being appropriately and consistently applied. Contact the policy staff at your Component or DHS headquarters if clarifications are needed.

   - Review the latest applicable control **Procedures** (*e.g.*, as referenced in NIST SP 800-53) to determine if the procedures are understood, and the expected control design and implementation is documented in the System Security Plan (SSP). Evaluate and document if the control is considered a critical "key control". Review the underlying security requirement (independent of the solution) and consider functional control requirements for quantity, quality, coverage, timelines, and availability.

   - Review existing Business **Processes** or Standard Operating Procedures (SOP). Consider business process descriptions and compensating controls. Are they part of the documented security control design and implementation requirements?

   - Review the **Systems Technology**, including security architecture and security services being used to implement and support the control. Determine whether the hardware platform, Operating System and application software are adequate to meet the internal control design and implementation requirements.

   - Identify the **People** who are responsible for developing, implementing, documenting, testing and continuously monitoring the security control (*e.g.*, ISSO, system administrators, supervisors, etc.) Determine if they are aware of and understand the procedures they are responsible for supporting. Has the staff been sufficiently trained and do they follow the procedures?

   - Identify the **Resources** needed to properly implement and monitor the internal control (*e.g.*, people, hardware, software licenses, software development time, implementation, test, documentation, training, and continual monitoring of effectiveness, etc.). Is the solution achievable with current resources (staff, funding, and systems) within the next 6 to 12 months or does the system owner and/or other principal stakeholder (*e.g.*, Component CIO, CFO) want to consider a waiver or exemption request? Is the remediation / mitigation activity (i.e., the solution) cost justifiable? Root cause analysis should determine if current resources can address the control weakness or if additional longer range funding for resources will need to be requested (*e.g.*, OMB Exhibit 300 funding requests, etc.).

- **Identify the Resources** (staff, funding, systems) needed to properly implement and monitor the internal control (*e.g.*, people, hardware, software licenses, software development time, implementation, test, documentation, training, and continual monitoring of effectiveness, etc.). Is the solution achievable with current resources? Is the remediation / mitigation activity cost justifiable? Is additional longer range funding required? Will the System Owner request additional funding (e.g. OMB Exhibit 300)?

Common Root Causes

Each control weakness will generally be a unique combination of factors. The following is a partial list of some suggested examples of root cause considerations:

Policy / Procedures

- Component policies have not implemented a recently required DHS update
- NIST control procedure requirements are missing or the control design is inadequately documented to reflect the implementation requirement

Processes

- Standard Operating Procedures are not being followed, i.e. Emergency Fixes applied without record of change management approvals.
- Are notification of critical security patches being received by the Operations Staff and tracked for implementation

People / Staff

- Poor or inconsistent communication between the System Owner, ISSO, and System Administrators, System Operator.
- Assigned ISSO supporting higher priority collateral duties
- The operational staff is not properly trained to performing control functions (*e.g.* which alerts are critical for identification when reviewing Security Log Files)

Systems Technology

- The hardware platform has reached end of life and is no longer being upgraded and only basic hardware maintenance activities are supported.
- Does the operating system include configuration management for hardening? Do insecure services or default accounts need to be removed?
- Control can not be implemented on the current platform, i.e. only weak passwords are supported.
- Security Log Files not turned on or being overwritten.

Appendix F

Sample Weakness Descriptions and Milestones

Sample Weakness Descriptions and Milestones

This Appendix provides examples of weakness descriptions and milestones to illustrate what is considered compliant with OMB and DHS guidance and what is not. Examples of non-complaint weaknesses and milestones provide a rationale regarding why they are non compliant with suggestions for improving them. All samples are actual weaknesses and milestones taken directly from TAF. Only system names or other identifying information have been changed.

Weakness Descriptions

The following two sections provide samples of compliant and non-compliant weakness descriptions. Accurately defining the weakness is the first step toward developing a remediation plan. If you can't accurately describe the real weakness, even at a high level, you probably can't develop an effective plan to resolve it.

Compliant Sample Weakness Descriptions

Below are examples of actual weaknesses extracted from TAF that illustrate descriptions that are compliant with DHS and OMB guidance. They are stated as weaknesses that need to be resolved and identify the core issue. They can easily be mapped to a control title.

- Privileged accounts are not secured by authentication technology stronger than that based only on a UserID and password (IA-2)
- Terminated and/or separated user accounts are not removed on a timely basis
- Backup tapes are stored in the same building as the production server
- There is not adequate procedures for documenting and correcting vulnerabilities found in quarterly vulnerability scans
- No ISA exists
- Application does not initiate a session lock after a period of inactivity.
- Password protected screen savers are not set to activate within 5 minutes of inactivity
- Inadequate system documentation
- Humidity controls are not deployed in the server rooms that house servers. Humidity levels are not consistently maintained / monitored in the server rooms. No redundant systems are available in the event of an outage of the temperature control systems

Non-compliant Sample Weakness Descriptions

The following table provides a sample of actual weaknesses extracted from TAF and provides a rationale for why they are non compliant with DHS POA&M guidance and thus why they would fail a HQ review.

Weakness Description	Comments
High system weaknesses	Does not identify any specific weakness. Cannot be mapped to a control title. Difficult to identify a remediation strategy or define milestones.
CISOs/ISSMs shall ensure that their IT systems comply with the DHS Enterprise Architecture (EA) and Security Architecture (SA) or maintain a waiver approved by the DHS CIO/CISO.	Not stated as a weakness. Could be improved if stated as, "System does not comply with DHS Enterprise Architecture (EA) and Security Architecture (SA) guidance." Or "The CISO does not ensure…" Note that each of these weakness descriptions requires a different solution. The first requires action by the system technical team while the second is focused on the CISO's oversight responsibility.
PL-5 Privacy Impact Assessment	Merely states the control title with no indication regarding what the actual weakness is (e.g., there is no PIA, the PIA is not completed properly, or the PIA is out of date).
Requirement: SI-2 The organization identifies, reports, and corrects information system flaws. The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.	States the requirement. Does not identify which part of the requirement is not met or the weakness that needs to be resolved.
Password History	Does not identify any weakness. It is unclear what aspect of password history needs to be resolved.
Batchup Exec Patch	Does not identify any weakness. It is unclear what weakness is posed by the Batchup Exec Patch or what needs to be resolved.
The system must eliminate or disable unnecessary ports from the servers, router, and switches. This will help prevent unauthorized entry into this information system.	This merely restates the control. It implies that unnecessary ports are open but it is unclear what the real weakness is. It could be written as, "Unnecessary ports from the servers, router, and switches are open." Or "Servers, router, and switches do not meet hardening guidelines."
Review and update the system FIPS 199 category.	This is stated as an action that needs to be completed. It would be a suitable milestone but does not describe a weakness. A better description might be, "The FIPS 199 category is incorrect." Or "The system has

	undergone significant changes and the FIPS 199 category may no longer be accurate."

Milestones

The following three sections provide samples of non-compliant, adequate and fully compliant milestones.

Non-compliant Sample Milestones

The following table provides a sample of actual milestones extracted from TAF and provides a rationale for why they are non compliant with DHS POA&M guidance and thus why they would fail a HQ review. Defining good milestones is the most critical element of the POA&M process. Without clearly defined milestones, it is difficult to determine what actions need to be taken, who should take them or when the weakness has been resolved.

Milestone	Rationale for Failure
Mitigate all high level weaknesses	The milestone does not provide a plan for mitigating any specific weakness
Take the required preparatory steps to resolve all issues found at this site	The milestone does not provide a plan for mitigating the weakness
Create plan of action to mitigate the finding or provide a Risk Acceptance letter to the AO	The POA&M **IS** the plan to mitigate the finding. A POA&M to develop a POA&M is not sufficient.
Ensure the policy is followed	This was the only milestone and does not provide a plan for how to ensure the policy is followed.
Action required - Requirement: AU-2.4 Determine if the organization periodically reviews and updates the list of organization-defined auditable events.	Restates the requirement. Does not provide a plan for resolving the issue once a determination has been made.
CR#1234 addresses this issue.	Does not state what the plan is to resolve the weakness. Submit a CR is a good first milestone but there should be additional milestones to implement and test the solution.
Multifactor authenticators are required for Privileged Accounts	Restates the requirement. Does not provide a plan for resolving the issue. Appropriate milestones may include: • Identify authenticators that satisfy the

	requirement - Obtain/procure authenticators - Install required hardware/software - Test implementation of authenticators - Distribute authenticators to privileged account holders - Update SSP and other system documents
The new System, including PTA, RTM, SSP, and Contingency Plan have addressed all of the issues associated with this C&A package. Any weaknesses have been identified therein, and comprised in the Trusted Agent FISMA application through POA&Ms.	Past tense. Does not present a plan for resolving a weakness. A better approach would be for milestones to review and update C&A documents and create POA&Ms where appropriate.
There is a CM process with a SOP. - The CM process repeatedly fails to develop or use test plans, test-procedures or test results. - CM board rarely uses a defined topology map to outline where the changes occur. - The organization fails to document audit activities associated with configuration changes to the information system	Identifies several weaknesses but does not provide a plan to resolve any of them. This milestone would be more effective if it included steps like: - Update the CM Plan to address identifying impact to the topology of proposed changes - Update the CM SOP to include testing procedures and documentation - Develop a process to document changes and retain records
Identify all systems not using SSL 3.1 or TLS and SSHv2	Does not state what the plan is to resolve the weakness. Identifying systems is a good first milestone but there should be additional milestones to implement and test the solution.
System Security Plan (SSP) draft was finalized	Past tense. Milestone should read something like, "Draft and publish an SSP" or "Update SSP"

<u>Sample Milestones That Would Pass HQ Review but could be improved</u>

The following table provides a sample of actual milestones extracted from TAF that meets basic criteria but could be improved.

Milestone	How it could be improved
Create process to review mobile code.	Once the process is created, it needs to be documented, tested and implemented. Additional

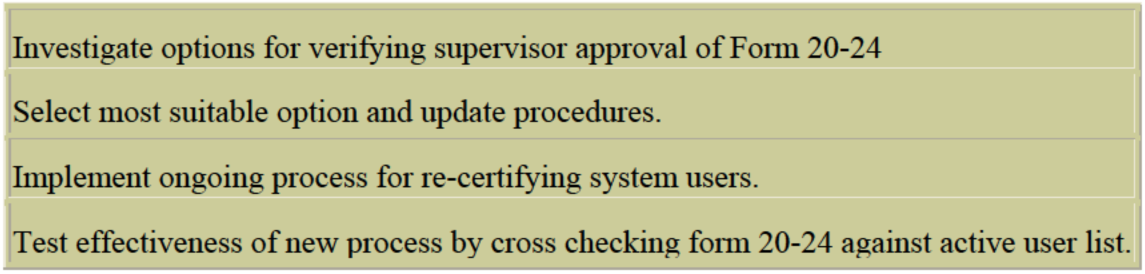
	milestones should be added for each of these steps.
Work with the Business Continuity Planning team to update accessibility requirements for the alternate storage site.	This is a good start but once the requirements are updated, there needs to be a milestone to develop a process for ensuring they are met.
Update telecommunications room	This milestone does state what needs to be done but provides no details regarding how the telecommunications room must be updated. Supporting milestones would including things like obtaining resources, installing equipment and updating documentation.

Compliant Sample Milestones

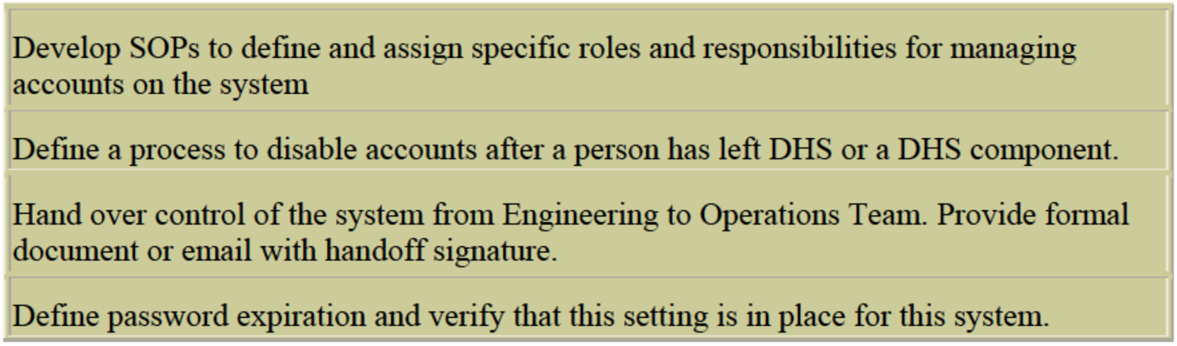
Below are sample milestones extracted directly from TAF that properly capture the actions that are needed to resolve the weakness. There may be root causes that need to be addressed but, as stated, these milestones are fully compliant.

- Update CPT documentation to reflect DHS comments listed in CPT Checklist.
- Set all passwords to expire per DHS policy
- Turn off Telnet and implement SSH on all switches

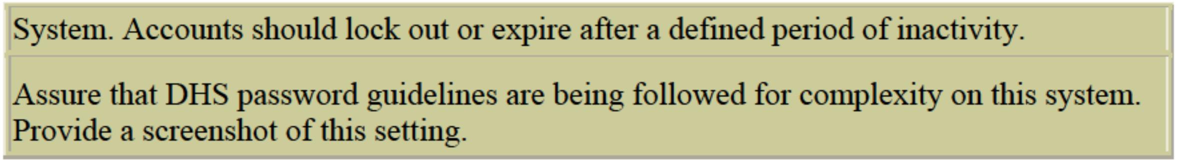
Below are examples of actual milestones extracted from TAF that illustrate a series of steps to address and resolve the weakness. They include steps for planning, testing, implementing and documenting the proposed solution. In some cases, the root cause is also clearly being addressed. These are examples of how milestones should be written.



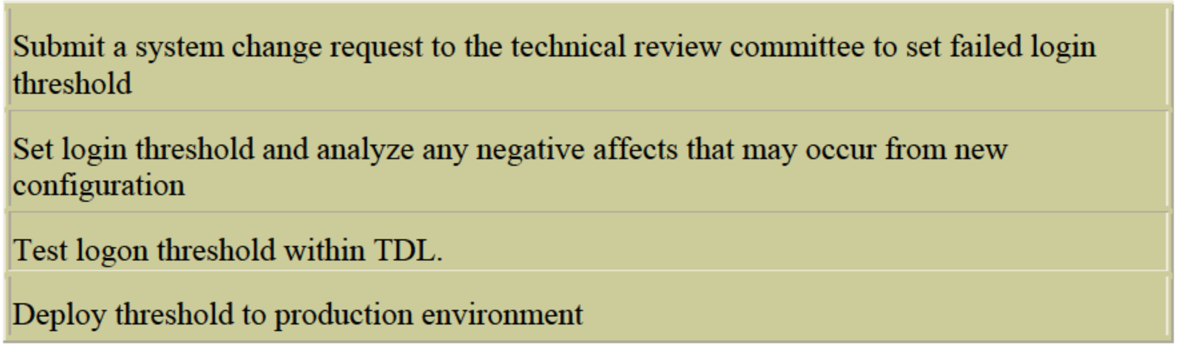
Investigate options for verifying supervisor approval of Form 20-24
Select most suitable option and update procedures.
Implement ongoing process for re-certifying system users.
Test effectiveness of new process by cross checking form 20-24 against active user list.



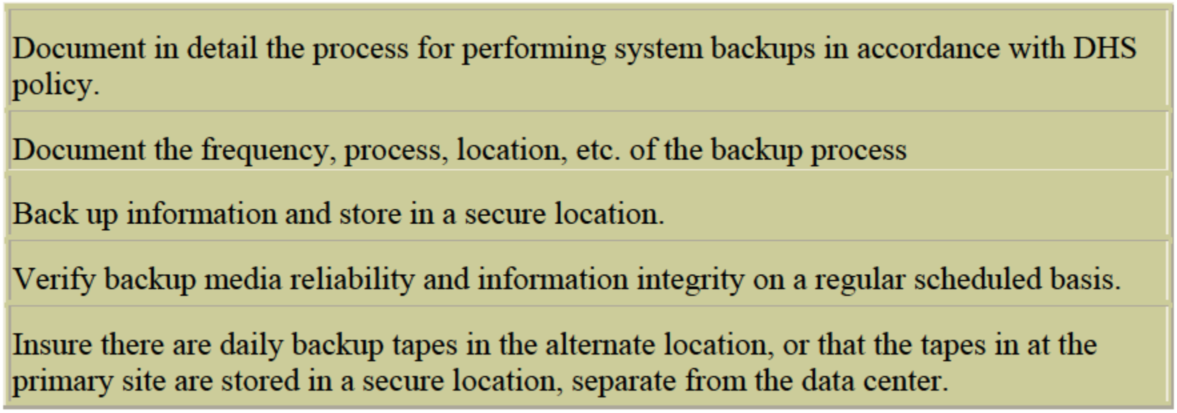
Develop SOPs to define and assign specific roles and responsibilities for managing accounts on the system
Define a process to disable accounts after a person has left DHS or a DHS component.
Hand over control of the system from Engineering to Operations Team. Provide formal document or email with handoff signature.
Define password expiration and verify that this setting is in place for this system.



System. Accounts should lock out or expire after a defined period of inactivity.
Assure that DHS password guidelines are being followed for complexity on this system. Provide a screenshot of this setting.



Submit a system change request to the technical review committee to set failed login threshold
Set login threshold and analyze any negative affects that may occur from new configuration
Test logon threshold within TDL.
Deploy threshold to production environment



Document in detail the process for performing system backups in accordance with DHS policy.
Document the frequency, process, location, etc. of the backup process
Back up information and store in a secure location.
Verify backup media reliability and information integrity on a regular scheduled basis.
Insure there are daily backup tapes in the alternate location, or that the tapes in at the primary site are stored in a secure location, separate from the data center.

Appendix G

POA&M Reasonableness Criteria

POA&M Reasonableness Criteria

The POA&M reasonableness metric in FY10 includes a check for remediation costs (i.e. resources). This metric was prepared to address OIG FISMA recommendations that DHS check POA&Ms for reasonableness. The metric is included under the POA&M Quality metric. Like other quality issues, POA&M reasonableness will be scored on a pass / fail basis at the system level (aggregating the POA&Ms under a system).

The POA&M reasonableness criteria is not intended to replace the planning process as described in the DHS POA&M Process Guide. Nor is it intended to provide an expected cost. Rather, it is designed as a check to ensure that ISSOs do not enter data that is clearly not obtained as part of a valid planning process.

The resource estimates provided below have been developed to address a range of data that is considered to be the minimum resources "reasonable" for developing POA&Ms. **They are not intended and should not be used as a guideline for what it should cost to correct a weakness.**

The resources metric is intended to preclude Components from using $1, $2, or another placeholder when developing their POA&Ms. It seeks to identify the minimum level of effort (LOE) needed to resolve a weakness. It is based on a nominal labor rate of $100 per hour and does not include other direct expenses (e.g., hardware or software). Because of the wide range of potential circumstances affecting any specific control, the "best possible case" was used to determine LOE. Below are rules of thumb used in computing LOE.

- All documents (policies, procedures, etc.) require a minimum of 4 hours or $400 to complete. The best case would be a Component or system policy that simply cites DHS 4300A or NIST guidance.
- All configuration hardening weaknesses require a minimum of ½ hour or $50. In some cases, only one part of a control may not be implemented. The best case could require a system administrator to close a single port or configure a setting on a server, which would take a minimal amount of time.
- All resources needed to prepare C&A documentation were based on estimated times required in the *Certification and Accreditation Guidance for SBU Systems User's Manual*, Appendix B.
- All weaknesses where a cost could not be estimated due to the complexity of the task or unknown factors (e.g., installing a fire suppression system) have been consistently listed at a nominal $50.

800-53 Control	Control Name	Minimum Resources
AC-1	Access Control Policy And Procedures	≥ $400
AC-2	Account Management	≥ $50
AC-3	Access Enforcement	≥ $50
AC-4	Information Flow Enforcement	≥ $200
AC-5	Separation of Duties	≥ $200
AC-6	Least Privilege	≥ $250

800-53 Control	Control Name	Minimum Resources
AC-7	Unsuccessful Login Attempts	≥ $50
AC-8	System Use Notification	≥ $50
AC-9	Previous Logon (Access) Notification	≥ $50
AC-10	Concurrent Session Control	≥ $50
AC-11	Session Lock	≥ $50
AC-12	Session Termination (Withdrawn)	≥ $50
AC-13	Supervision and Review—Access Control (Withdrawn)	≥ $400
AC-14	Actions Permitted Without Identification or Authentication	≥ $200
AC-15	Automated Marking (Withdrawn)	≥ $50
AC-16	Security Attributes	≥ $50
AC-17	Remote Access	≥ $2000
AC-18	Wireless Access	≥ $2000
AC-19	Access Control for Mobile Devices	≥ $4000
AC-20	Use of External Information Systems	≥ $400
AC-21	User-Based Collaboration and Information sharing	≥ $400
AC-22	Publicly Accessible Content	≥ $400
AT-1	Security Awareness and Training Policy and Procedures	≥ $400
AT-2	Security Awareness	≥ $2000
AT-3	Security Training	≥ $4000
AT-4	Security Training Records	≥ $4000
AT-5	Contacts with Security Groups and Associations	≥ $400
AU-1	Audit and Accountability Policy and Procedures	≥ $400
AU-2	Auditable Events	≥ $400
AU-3	Content of Audit Records	≥ $400
AU-4	Audit Storage Capacity	≥ $400
AU-5	Response to Audit Processing Failures	≥ $800
AU-6	Audit Review, Analysis, and Reporting	≥ $400
AU-7	Audit Reduction and Report Generation	≥ $1000
AU-8	Time Stamps	≥ $50
AU-9	Protection of Audit Information	≥ $50
AU-10	Non-Repudiation	≥ $50
AU-11	Audit Record Retention	≥ $400
AU-12	Audit Generation	≥ $100
AU-13	Monitoring for Information Disclosure	≥ $100
AU-14	Session Audit	≥ $100
CA-1	Security Assessment and Authorization Policies and Procedures	≥ $400
CA-2	Security Assessments	≥ $5000
CA-3	Information System Connections	≥ $2000
CA-4	Security Certification (Withdrawn)	≥ $92000

800-53 Control	Control Name	Minimum Resources
CA-5	Plan of Action and Milestones	≥ $1800
CA-6	Security Authorization	≥ $500
CA-7	Continuous Monitoring	≥ $100
CM-1	Configuration Management Policy and Procedures	≥ $400
CM-2	Baseline Configuration	≥ $4000
CM-3	Configuration Change Control	≥ $4000
CM-4	Security Impact Analysis	≥ $2400
CM-5	Access Restrictions for Change	≥ $50
CM-6	Configuration Settings	≥ $50
CM-7	Least Functionality	≥ $50
CM-8	Information System Component Inventory	≥ $400
CM-9	Configuration Management Plan	≥ $100
CP-1	Contingency Planning Policy and Procedures	≥ $400
CP-2	Contingency Plan	≥ $5200
CP-3	Contingency Training	≥ $2500
CP-4	Contingency Plan Testing and Exercises	≥ $10000
CP-5	Contingency Plan Update (Withdrawn)	≥ $1200
CP-6	Alternate Storage Sites	≥ $4000
CP-7	Alternate Processing Sites	≥ $4000
CP-8	Telecommunications Services	≥ $4000
CP-9	Information System Backup	≥ $200
CP-10	Information System Recovery and Reconstitution	≥ $400
IA-1	Identification and Authentication Policy and Procedures	≥ $400
IA-2	Identification and Authentication (Organizational Users)	≥ $50
IA-3	Device Identification and Authentication	≥ $50
IA-4	Identifier Management	≥ $400
IA-5	Authenticator Management	≥ $50
IA-6	Authenticator Feedback	≥ $400
IA-7	Cryptographic Module Authentication	≥ $100
IA-8	Identification and Authentication (Non-Organizational Users)	≥ $400
IR-1	Incident Response Policy and Procedures	≥ $400
IR-2	Incident Response Training	≥ $400
IR-3	Incident Response Testing and Exercises	≥ $1200
IR-4	Incident Handling	≥ $1200
IR-5	Incident Monitoring	≥ $400
IR-6	Incident Reporting	≥ $400
IR-7	Incident Response Assistance	≥ $100
IR-8	Incident Response Plan	≥ $400
MA-1	System Maintenance Policy and Procedures	≥ $400
MA-2	Controlled Maintenance	≥ $800

800-53 Control	Control Name	Minimum Resources
MA-3	Maintenance Tools	≥ $400
MA-4	Non-Local Maintenance	≥ $400
MA-5	Maintenance Personnel	≥ $50
MA-6	Timely Maintenance	≥ $2000
MP-1	Media Protection Policy and Procedures	≥ $400
MP-2	Media Access	≥ $400
MP-3	Media Marking	≥ $400
MP-4	Media Storage	≥ $400
MP-5	Media Transport	≥ $400
MP-6	Media Sanitization	≥ $400
PE-1	Physical and Environmental Protection Policy and Procedures	≥ $400
PE-2	Physical Access Authorizations	≥ $50
PE-3	Physical Access Control	≥ $50
PE-4	Access Control for Transmission Medium	≥ $50
PE-5	Access Control for Output Devices	≥ $50
PE-6	Monitoring Physical Access	≥ $800
PE-7	Visitor Control	≥ $400
PE-8	Access Records	≥ $400
PE-9	Power Equipment and Power Cabling	≥ $100
PE-10	Emergency Shutoff	≥ $50
PE-11	Emergency Power	≥ $50
PE-12	Emergency Lighting	≥ $50
PE-13	Fire Protection	≥ $50
PE-14	Temperature and Humidity Controls	≥ $50
PE-15	Water Damage Protection	≥ $50
PE-16	Delivery and Removal	≥ $400
PE-17	Alternate Work Site	≥ $50
PE-18	Location of Information System Components	≥ $1000
PE-19	Information Leakage	≥ $1000
PL-1	Security Planning Policy and Procedures	≥ $400
PL-2	System Security Plan	≥ $4000
PL-3	System Security Plan Update (withdrawn)	≥ $2000
PL-4	Rules of Behavior	≥ $400
PL-5	Privacy Impact Assessment	≥ $200
PL-6	Security-Related Activity Planning	≥ $50
PS-1	Personnel Security Policy and Procedures	≥ $400
PS-2	Position Categorization	≥ $50
PS-3	Personnel Screening	≥ $50
PS-4	Personnel Termination	≥ $50
PS-5	Personnel Transfer	≥ $50

800-53 Control	Control Name	Minimum Resources
PS-6	Access Agreements	≥ $50
PS-7	Third-Party Personnel Security	≥ $400
PS-8	Personnel Sanctions	≥ $50
RA-1	Risk Assessment Policy and Procedures	≥ $400
RA-2	Security Categorization	≥ $200
RA-3	Risk Assessment	≥ $4000
RA-4	Risk Assessment Update (Withdrawn)	≥ $2000
RA-5	Vulnerability Scanning	≥ $400
SA-1	System and Services Acquisition Policy and Procedures	≥ $400
SA-2	Allocation of Resources	≥ $400
SA-3	Life Cycle Support	≥ $400
SA-4	Acquisitions	≥ $400
SA-5	Information System Documentation	≥ $400
SA-6	Software Usage Restrictions	≥ $50
SA-7	User Installed Software	≥ $400
SA-8	Security Engineering Principles	≥ $400
SA-9	External Information System Services	≥ $400
SA-10	Developer Configuration Management	≥ $400
SA-11	Developer Security Testing	≥ $4000
SA-12	Supply Chain Protection	≥ $400
SA-13	Trustworthiness	≥ $400
SA-14	Critical Information System Components	≥ $400
SC-1	System and Communications Protection Policy and Procedures	≥ $400
SC-2	Application Partitioning	≥ $50
SC-3	Security Function Isolation	≥ $50
SC-4	Information in Shared Resources	≥ $50
SC-5	Denial of Service Protection	≥ $50
SC-6	Resource Priority	≥ $ 50
SC-7	Boundary Protection	≥ $50
SC-8	Transmission Integrity	≥ $100
SC-9	Transmission Confidentiality	≥ $100
SC-10	Network Disconnect	≥ $50
SC-11	Trusted Path	≥ $50
SC-12	Cryptographic Key Establishment And Management	≥ $50
SC-13	Use of Cryptography	≥ $50
SC-14	Public Access Protections	≥ $50
SC-15	Collaborative Computing Devices	≥ $50
SC-16	Transmission of Security Attributes	≥ $50
SC-17	Public Key Infrastructure Certificates	≥ $400

800-53 Control	Control Name	Minimum Resources
SC-18	Mobile Code	≥ $400
SC-19	Voice Over Internet Protocol	≥ $400
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	≥ $100
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	≥ $100
SC-22	Architecture and Provisioning for Name/Address Resolution Service	≥ $100
SC-23	Session Authenticity	≥ $100
SC-24	Fail in Known State	≥ $50
SC-25	Thin Nodes	≥ $50
SC-26	Honeypots	≥ $50
SC-27	Operating System-Independent Applications	≥ $50
SC-28	Protection of Information at Rest	≥ $50
SC-29	Heterogeneity	≥ $50
SC-30	Virtualization Techniques	≥ $50
SC-31	Covert Channel Analysis	≥ $50
SC-31	Information System Partitioning	≥ $50
SC-33	Transmission Preparation Integrity	≥ $50
SC-34	Non-Modifiable Executable Programs	≥ $50
SI-1	System and Information Integrity Policy and Procedures	≥ $400
SI-2	Flaw Remediation	≥ $50
SI-3	Malicious Code Protection	≥ $50
SI-4	Information System Monitoring	≥ $50
SI-5	Security Alerts, Advisories, and Directives	≥ $50
SI-6	Security Functionality Verification	≥ $50
SI-7	Software and Information Integrity	≥ $50
SI-8	Spam Protection	≥ $50
SI-9	Information Input Restrictions	≥ $50
SI-10	Information Input Validation	≥ $50
SI-11	Error Handling	≥ $50
SI-12	Information Output Handling and Retention	≥ $50
SI-13	Predictable Failure Prevention	≥ $50

Appendix H

Weakness Search Report Guide

Weakness Search Report Guide

for

DHS Summary Scorecard

The following step-by-step guide has been developed to help CISOs, ISSOs and other Compliance staff use TAF to monitor and update POA&M data to improve compliance and raise scores on the DHS scorecard. It is organized to correspond to the columns on the summary scorecard for ease of reference. While these steps capture the majority of POA&M related items that are graded, they are not all inclusive (e.g., reasonableness criteria cannot be monitored using this guide).

A. POA&M Quality Checks

See the FY2010 DHS Information Security Performance Plan for an explanation of the grading criteria for each of the Quality Checks.

<u>POA&M Status</u>

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Closed.

   Filter on Criticality (Priority) = 4.

   Filter on ISSM Validation = All Unapproved.
3. Run report.
4. All output needs to be updated. Weakness approvals and/or weakness artifacts

   are needed.

5. Re-run Weakness Search by returning to Filter.
6. Filter on Status = Closed.

   Filter on Criticality (Priority) = 5.

   Filter on ISSM Validation = All Unapproved.
7. Run report.
8. All output needs to be updated. Weakness approvals and/or weakness artifacts are needed.

9. Re-run Weakness Search by returning to Filter.
10. Filter on Status = Cancelled.

    Filter on Reason = Other.
11. Run report.

12. If there are any results, update the Reason for Cancellation by clicking on the weakness item and clicking the Ellipsis button dropdown menu or type in a reason in the box to explain why the weakness was cancelled.

13. Re-run Weakness Search by returning to Filter.
14. Filter on Status = Delayed.

    Filter on Reason = Unassigned.
15. Run report.
16. If there are any results, click on weakness and update the Reason for Delay with the Ellipsis button dropdown menu.

17. Re-run Weakness Search by returning to Filter.
18. Filter on Status = Waiver.
19. Run report.
20. If there are any results, click on the weakness and check to see if a Waiver artifact is uploaded and weakness is Approved.

21. Re-run Weakness Search by returning to Filter.
22. Filter on Status = Exception.
23. Run report.
24. If there are any results, click into the weakness and check to see if an Exception artifact is uploaded and weakness is Approved.

Point of Contact: Must include a name and either phone or email address

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Click on the POC Heading column to sort column. Any blank or missing data needs to be filled in.

Program-level POA&Ms

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Type = Program.

   Filter on Status = Opened.
3. Run report.
4. Manually review that the Scheduled Completion Date and Estimated Completion Date are less than 5 years from the Creation Date of the weakness.

Link to Control Title

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Run report.
4. Manually review the Linked To Control Title column. Weakness items without linkages to Control Titles need to establish that linkage by clicking on the weakness and updating the Link to Control Title field.

Identified In

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Run report.
4. Manually review the Identified In column. Update all information that has not established at least one Identified In source by clicking on the weakness and selecting an Identified In source.

Criticality (Priority) Level 1

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.

   Filter on Criticality (Priority) = 1.
3. Run report.
4. Update the results by clicking on the weakness and changing the Criticality (Priority) fields to a selection that is not Unassigned.

See the FY2010 DHS Information Security Performance Plan an explanation of the grading criteria for each of the checks listed below.

B. Open System POA&Ms <6 Months

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Filter on Creation Date Ending On and enter 6 months prior to current date. (NOTE: If the current date is 1 January 2008, then select the calendar icon date of 1 July 2007.)
4. Run report.
5. Address all weakness items produced in this report. Their status needs to be changed to Closed, Cancelled, Waiver, or Exception as appropriate. Update any other data required by these changes.

C. Audit Recommend. Captured

1. Contact the DHS Audit Manager to request a list of current audits.
2. Select the Weakness Search report at Component, Program or System level.
3. Run report.
   a. If a valid Audit Number does not appear in the dropdown window, the audit has not been entered or it not been properly linked in the Identified In field. Check to ensure which is the case and make corrections accordingly.
   b. If the Audit Number does appear in the dropdown window, select it, run the report, and check to ensure that all recommendations have been included in a POA&M as a weakness.

D. POA&Ms >=30 days overdue

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Estimated Completion Date Ending On and select the date 31 days before the current date from the calendar icon. (NOTE: If the current date is 1 January 2008, then select the calendar icon date of 30 November 2007.)
3. Filter on Status = Delayed.
4. Run report.
5. If there are any results, update the Estimated Completion Date by clicking into the weakness and updating the Estimated Completion Date.
6. Check to ensure that the new Estimated Completion Date is not more than 6 months after the Creation Date. If so, request a Waiver or Exception.

E. POA&M Approvals

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.

   Filter on ISSM Validation = Not Started.
3. Run report.
4. All results are non-compliant. All weaknesses need to be Approved.

5. Re-run Weakness Search by returning to Filter.
6. Filter on Status = Delayed.
7. Run report.
8. If any results except a green check mark are displayed in the ISSM Validation column, then weakness items are non-compliant and need updating.

9. Re-run Weakness Search by returning to Filter.
10. Filter on Status = Waiver.

11. Run report.
12. If any results except a green check mark are displayed in the ISSM Validation column, then weakness items are non-compliant and need updating.

13. Re-run Weakness Search by returning to Filter.
14. Filter on Status = Exception.
15. If any results except a green check mark are displayed in the ISSM Validation column, then weakness items are non-compliant and need updating.

16. Re-run Weakness Search by returning to Filter.
17. Filter on Status = Cancelled.
18. If any results except a green check mark are displayed in the ISSM Validation Column, then weakness items are non-compliant and need updating.

F. **Security Resource**

Funding Source

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Run report.
4. Manually review the Resources Required column to see if there is text associated with the Funding Source in the Resources Required column. If not, click the weakness and use the Ellipsis button dropdown menu to select a funding source.

Resources Required

1. Select the Weakness Search report at Component, Program or System level.
2. Filter on Status = Opened.
3. Run report.
4. Click on the Resources Required Heading column to sort column. Then, click on the weakness and update all zero (0) or one (1) dollar amounts to a reasonable dollar figure. (See the FY2010 DHS Information Security Performance Plan for Reasonableness Guidelines.)