Job Aid: Plan of Action and Milestones (POA&M)

Using this job aid

This job aid is a tool to help information system security professionals understand how to create and use the Plan of Action and Milestones (POA&M).

Overview of POA&M

This section provides a general overview of the POA&M:

- *Purpose of the POA&M*
- *When a POA&M is required*
- *Who prepares/uses a POA&M and how*
- *How to create/update a POA&M*

Purpose of the POA&M	The purpose of the POA&M is to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses/deficiencies/vulnerabilities found in programs and systems. The POA&M— • Facilitates a disciplined and structured approach to mitigating risks in accordance with the priorities of the Information System Owner (ISO) • Includes the findings and recommendations of the security assessment report and the continual security assessments • Is maintained throughout the system life cycle
When a POA&M is required	The POA&M is created as part of Step 5 (Authorize System) in the 6-step Risk Management Framework (RMF) process and when common controls have been determined, through independent assessments, to be less than effective. The POA&M is maintained as part of the Security Authorization Package (formerly known as the Certification and Accreditation, or C&A, package).

Who prepares/uses the POA&M and how	• The ISO or the project manager/system manager (PM/SM) lists the following in the POA&M:
	  ○ Non-compliant (NC) security controls
	  ○ Security controls that are not applicable (N/A)
	  ○ Remediation or mitigation tasks for non-compliant security controls
	  ○ Required resources
	  ○ Milestones and completion dates
	  ○ Inherited vulnerabilities
	• The ISO or PM/SM initiates the corrective actions identified in the POA&M
	• With the support and assistance of the information system security manager (ISSM), the ISO or PM/SM provides visibility and status of the POA&M to the:
	  ○ Authorizing official (AO)
	  ○ Senior information security officer (SISO)
	• The DoD Component SISOs monitor and track the overall execution of system-level POA&Ms across the entire Component until identified security vulnerabilities have been remediated and the RMF documentation (Security Authorization Package) is appropriately adjusted

How to create/update a POA&M	• Download and open the POA&M template. • Follow the instructions in the next section to complete the POA&M.

Plan of Action and Milestones (POA&M)

System Name	DoD Network	**Date of this POA&M**	10/1/2016
Company/ Organization Name	CDSE	**Date of last update**	2/15/2016
Sponsoring Service/Agency	Defense Security Service	**Date of original POA&M**	10/1/2015
ISSM Name	John Doe	**IS Type**	Enclave
ISSM Phone	410-xxx-xxxx	**UID**	009-1111-2222
ISSM Email Address	john.doe1000.civ@mail.mil		

SAMPLE POA&M
For Training Purposes Only

Item Identifier	Weakness or Deficiency	Security Control	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Weakness/ Deficiency Identified by	Risk Level (Low/Med/ High)	Estimated Cost	Status	Comments
FY16_001	Users are able to connect remotely	AC-17	John Doe	Network Administrator	3/15/2016	Disable remote access 3/15/16	N/A	Annual Audit	Medium	500.00	Completed	

Information Required to be in the POA&M

This section describes the information required in each column on the POA&M. Refer to the sample POA&M above as you review each of these items.

Column Header	Description	What You Should Do
Item Identifier	A unique weakness identifier used to track and correlate weaknesses that are ongoing throughout quarterly submissions within the organization	• Use the numbering schema that has been determined by your organization.
Weakness or Deficiency	Represents any program or system-level information security vulnerability that poses an unacceptable risk of compromising confidentiality, integrity, or availability of information	• Describe weakness or deficiency identified by certification/validation testing, annual program review, IG independent evaluation, or any other work done by or on behalf of the organization. • Sensitive descriptions are not necessary, but provide sufficient detail to permit oversight and tracking.

Column Header	Description	What You Should Do
Security Control	The Security Controls are listed in the NIST SP 800-53 and directly relate to the weakness identified in 'Weakness or Deficiency' column.	• Enter security control that correlates to the weakness or deficiency. • For a security weakness found by means other than a security controls assessment (e.g., vulnerability test), map the deficient function into the applicable security control.
Point of Contact (POC)	The organization or title of the position within the organization that is responsible for mitigating the weakness	• Enter the name, title and organization of the assigned responsible individual(s).
Resources Required	Estimated funding and/or manpower resources required for mitigating a weakness	• Note the source and type of funding (current, new, or reallocated) and any funding obstacles • Include the total funding requirements in the Security Costs column

Scheduled Completion Date	Completion date based on a realistic estimate of the amount of time it will take to procure/allocate the resources required for the corrective action and implement/test the corrective action	• Always enter either the estimated completion date or 'N/A' if the risk is accepted
		  ○ Never change this date
		  ○ If a security weakness is resolved before or after the originally scheduled completion date, put the actual completion date in the Status field.

Column Header	Description	What You Should Do
Milestones with Completion Date	Specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step	• List the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step ○ Enter changes to milestones and completion dates in the Changes to Milestones column
Changes to Milestones	New estimated completion date for a milestone and the reason for the change	• Indicate the new estimated date for a milestone's completion, if the original date is not met • Include the reason for the change

Weakness or Deficiency Identified By	The source of the weakness, the reviewing agency/organization, and the date that the weakness was identified	• Enter the source of the weakness, for example:
		  ○ Security controls assessment
		  ○ Penetration test
		  ○ IG audit
		  ○ Certification testing
		• Enter the reviewing agency/organization and the date that the weakness was identified

Column Header	Description	What You Should Do
Status	The stage or state of the weakness in the corrective process cycle	• Enter one of these stages or states of the weakness in the corrective process cycle: ○ **Completed** – when a weakness has been fully resolved and the corrective action has been tested; include date of completion ○ **Ongoing** – when a deficiency/weakness is in the process of being mitigated and it has not yet exceeded the original scheduled completion date ○ **Delayed** – when a deficiency/weakness continues to be mitigated after the original scheduled completion date has passed ○ **Planned** – when corrective actions are planned to mitigate the deficiency/weakness, but the actions have not yet been applied/implemented ○ **Accepted** – when AO decides to accept the risk – Include date AO decided to accept the risk of an identified weakness (after AO received a recommendation from the PM office along with a "Mitigation Strategy Report" addressing all implemented/ inherited countermeasures and mitigating factors) – Periodically review solutions to address the risk to eventually close out the finding when possible

Column Header	Description	What You Should Do
Comments	Any amplifying or explanatory remarks that will assist in understanding other entries relative to the identified weakness(es)	• Include any amplifying or explanatory remarks that will assist in understanding other entries relative to the identified weakness(es) such as ○ Mitigating factors that will lessen the risks to the system and the network ○ Recommendations to downgrade a finding based on implemented/inherited mitigations ○ Explanation for a delay or change in a Milestone or Scheduled Completion Date ○ Identification of other obstacles or challenges (non-funding-related) to resolving the weakness (e.g., lack of personnel or expertise, or developing new system to replace insecure legacy system)
Risk Level	A ranking that determines the impact of a vulnerability, if exploited, to the system, data, and/or program	• Enter the risk level of the weakness or deficiency: ○ High ○ Medium ○ Low
Estimated Cost	The total estimated cost of correcting the weakness or deficiency	• Enter the total estimated cost by adding up the individual estimated costs of correcting each weakness or deficiency