Defense Security Service
SIPRNET CTO 10-133
Plan of Action and Milestone Template (POAM)

Company Name	DSS UID	ISSM	ISSM PHONE NUMBER

Item Number	Non-Compliance	Mitigation Plans and Adjustments	Milestone Date Based on Risk Level	ISSM/FSO Approval	Status (Open/Closed)	DSS Approval Date and Determination (Open/ Closed)	Risk Level Low/ Medium/ High
1	Disable all write capability.	**a.** Modify technical settings to disable write capabilities as needed. **b**. Confirm write capability is disabled through testing. **c.** Document how write capabilities have been disabled and tested in a "Classified Transfer Procedure" attachment to Security Documentation.					
2	Establish a program to appoint and account for authorized personnel responsible for conducting data transfers.	**a.** Obtain a RAL from sponsor allowing DSS approval of Authorized transfer personnel. **b.** Document authorized transfer individuals in a "Classified Transfer Procedure" attachment to Security Documentation.					

3	Create and maintain a logbook for any document transferred by the contractor.	**a**. Establish a log book that includes: • Date/time of transfer • Document subject • Document Type • Document Size • Transfer authorizing individual • Name of transferring authority • Computer Name/Unique ID used for Transfer • Confirmation of media scan after transfer. **b**. Document log book entries in a “Classified Transfer Procedure” attachment to Security Documentation.					
4	Scan all flash media transfers. (Applicable if flash media is used)	**a.** Install and Confirm ability to scan Flash media with NSA’s File Sanitization Tool (FiST) with Magik Eraser (ME). **b.** Document sanitization tool use in a “Classified Transfer Procedure” attachment to Security Documentation.					
5	Re-Accredit Information system.	Submit revised security documentation including Risk Acceptance Letter (RAL) and additional “Classified Transfer Procedure” along with any outstanding POAM items					

		to DSS for re-accreditation.					
6	Implement HBSS.	Coordinate with Sponsor and DSS to implement a Host Based Security System on all systems connected to SIPRNET.					
7	Report compliance to DISA.	Document compliance in Vulnerability Management System (VMS).					

* Milestone dates will be determined on a High/Medium/Low scale. High = 90 days, Medium = 180 days, Low = 365 days. The criteria for these elements are listed on the following page.

Plan of Action and Milestone Template (POAM) Guidance

- The POAM apply to initial SSP submissions, as well as existing accredited systems that require accreditation under the new DSS Configuration Baseline.

- *C/I – Enter C if non-compliance issue was identified during the C&A process. Enter I if non-compliance issue was identified during inspection. Milestone date for non-compliance issues should completed within **XX** days.

- Milestone dates will be determined on a High/Medium/Low scale. High = 90 days, Medium = 180 days, Low = 365 days. Risk level settings will be vetted against each configuration setting and the NIST risk-factor (action item).

  * High Impact Code. The absence or incorrect implementation of the IA control may have a severe or catastrophic effect on system operations, management, or information sharing. Exploitation of the weakness may result in the destruction of information resources and/or the complete loss of mission capability. High impact codes will be assessed on a case-by-case basis. If approved, system must be compliant within 90 days.

  *Medium Impact Code. The absence or incorrect implementation of the IA control may have a serious adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in loss of information resources and/or the significant degradation of mission capability. Must be compliant within 180 days

  *Low Impact Code. The absence or incorrect implementation of the IA control may have a limited adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in temporary loss of information resources and/or limit the effectiveness of mission capability. Must be compliant within 365 days

- Items under Status are considered closed when validated by DSS.

- Self-certified systems – All new systems will require a new master and will have to be compliant with the new settings. To add a new workstation to an existing system by self-cert, it must be configured IAW the enhanced requirements. They may either update the entire IS at that time, or this may push them into a POAM whereby they plan migration of the entire IS to the new settings

- GCA must approve non-compliant settings due to program compatibility or contract requirements. Non-compliance with baseline configuration settings resulting from operating system limitations or capabilities will not require GCA approval.

- Documentation must reflect which items cannot be met, as well as why it cannot be met.

- All non-compliant issues that come up during an inspection that are not corrected on the spot must be put in the POAM. This will make a formal, trackable date for resolution.