

# MOST COMMON INSTANCES OF NON-COMPLIANCE FOR INFORMATION SYSTEM SECURITY (AIS)


Practical Solutions and best practices

# TABLE OF CONTENTS

- Establishing an Insider Threat Program
  - Access Control
  - Configuration Management
  - Audit and Accountability
  - Senior Management Support
  - Documentation, Retention, and Verification
  - System Level Continuous Monitoring (SLCM)
  - After ATO Actions
- 

# 117.18(A) INFORMATION SYSTEM SECURITY: GENERAL

## Establishing an Insider Threat Program

- Develop a Clear Policy
    - Ensure top management level support
  - Create Cross-functional Insider Threat Management Team
    - Include individuals from different departments and areas of expertise
  - Conduct Risk Assessments
    - Annually in accordance with RA-3
  - User Activity Monitoring
  - Awareness Training
  - Confidential Reporting Mechanisms
- 


# 117.18(B) INFORMATION SYSTEM SECURITY: INFORMATION SYSTEM SECURITY PROGRAM

## Access Control

- Least Privilege
  - Limiting access to only the necessary functions an account needs
- Separation of Duties
  - Assigning privileged functions on the system to multiple key personnel instead of a few “multi-hatted” individuals.
- Maintaining and Auditing User Forms
  - User agreements should be protected to avoid loss or destruction
  - Maintain user documentation for required retention periods
- Configuring Group Policy Effectively
  - Ensuring policy settings on the system match the control requirements for your system to include password configuration, expiration times, and lockout settings.

# 117.18(B) INFORMATION SYSTEM SECURITY: INFORMATION SYSTEM SECURITY PROGRAM

## Configuration Management

- Configuration Management and Change Control Policy
    - Ensure a charter for the board is included
  - Ensure changes to the IS are tracked, approved, and noted by the change control board (CCB).
    - Proper documentation includes: CCB minutes, Security Impact Analysis, and evidence of AO approval for security relevant changes
  - Ensure hardware changes are tracked and updated in the FSO's Information Management System
- 

# 117.18(B) INFORMATION SYSTEM SECURITY: INFORMATION SYSTEM SECURITY PROGRAM

## Audit and Accountability

- Consider using audit reductions tools to both simplify auditing and capture more information.
  - Splunk is a great option for this but there are others out there.
- Develop ISSOs to have a better understanding of the audit process and not simply following a checklist.
- Ensure auditing is conducted by the ISSO and not the SA to avoid corrective actions occurring without following the CM process.
- Ensure networked systems all have the same time source and that the time is accurate.
  - Accurate system logs depend on a valid time source shared by all systems.

# 117.18(C) INFORMATION SYSTEM SECURITY: CONTRACTOR RESPONSIBILITIES

## Senior Management Support

- Senior management support will ensure the IS program has adequate resources available to support and execute the program mission.
  - Organizations should ensure the ISSM is placed the appropriate organizational level to have access to senior-management.
    - An ISSM that is not at the appropriate organizational level, has a greater chance of not being heard or given the opportunity to discuss the needs of the security program.
  - Hold regular meetings with senior management.
  - Discuss the importance of the security program to improve their understanding.
  - Discuss needs and where improvements can be made.
  - Provide metrics and evidence to support your cause.

# 117.18(C) INFORMATION SYSTEM SECURITY: CONTRACTOR RESPONSIBILITIES

## Documentation, Retention, and Verification

- ISSMs who are responsible for the overall IS security program need to ensure they have proper documentation for security activities that are maintained for the appropriate retention periods.
  - This includes system level documentation, access forms, training records, auditing actions, ConMon (Continuous Monitoring) activities, maintenance records, change management, self inspections and more.
    - Program management tools such as JIRA can be useful to centralize ConMon taskings and provide robust tracking metrics.
    - SharePoint can be useful in maintaining digital records for retention and securing them from unwanted destruction.
- ISSMs should ensure anyone requesting access to an information system has the appropriate training documented, need to know (NTK) and clearance to the level of the system they are requesting access to.
  - The verification of the information should be documented, typically on an access request form and maintained for the appropriate retention periods.
    - Consider making digital backups of any hard copy access requests and briefing agreements.



# 117.18(D) INFORMATION SYSTEM SECURITY: INFORMATION SYSTEM SECURITY LIFE-CYCLE

## System Level Continuous Monitoring (SLCM)

- Documenting SLCM per NISP eMASS Industry Operations Guide
  - Criticality: Indicate the criticality of monitoring the Control as Red, Yellow, or White (see NISP eMASS Industry Operations Guide for more details).
  - Frequency: Indicate the frequency with which the control is monitored.
    - The frequency of monitoring is based on the continuous monitoring strategy developed by the ISO/ISSM as part of the security plan, or provided by the CCP and approved by the AO. (DAAPM v2.2)
  - Method: Indicate the method of monitoring the control.
  - Reporting: Provide a short narrative explaining who reports what to whom by when;
  - Tracking: Provide a short narrative explaining how security controls found to be non-compliant or ineffective will be tracked.
  - SLCM Comments: Provide a short narrative further explaining any other details not appropriate for the other fields.

# 117.18(D) INFORMATION SYSTEM SECURITY: INFORMATION SYSTEM SECURITY LIFE-CYCLE

Following SLCM and A&A

- ISSMs should ensure they are following the established SLCM process documented in their eMASS system package.
- This includes:
  - Conducting and self assessing the SLCM plan.
  - Ensuring training requirements are being conducted and testing of Contingency and Incident Response plans are completed.
  - Reviewing POAM items, updating milestones, closing out completed items, and submitting risk acceptance requests for issues that cannot be fixed.
- It's important to note that some controls have time requirements that differ from the ConMon frequency. For example, RA-5 has a recommended ConMon frequency of quarterly, while the control has a monthly vulnerability scanning requirement.
- ISSM's should ensure that all reauthorization packages are submitted within 90 days of expiration to ensure a lapse does not occur.

# 117.18(E) INFORMATION SYSTEM SECURITY: RISK MANAGEMENT FRAMEWORK

## After ATO Actions

- Following the decision to authorize, the ISSM must ensure they continue their effort to remediate all outstanding issues addressed during the ATO review process.
  - ISSM should review the System Deficiency Summary Report (SDSR) issued following ATO decision.
  - ISSM should address all issues on the SDSR to include:
    - Updating POAM to add any items that were not on the initial POAM and still require remediation.
    - Closing out POAM items that have been remediated.
    - Update security controls and resubmit (related controls only) based on open or closing of control deficiencies.
  - Continue to monitor and assess controls and POAM.