Best Practices for Obtaining & Maintaining an Authorized Information System

Welcome to this presentation on best practices for achieving and maintaining authorized information systems under DCSA's Assessment and Authorization Process Manual (DAAPM) v2.2. This briefing is tailored for Information System Security Managers (ISSMs) and Facility Security Officers (FSOs) at cleared contractor facilities.

by Dr. Jose Neto

PC-WARRIORS

Following DAAPM and NISPOM Guidance

DAAPM v2.2

The DAAPM is your primary guide for Assessment and Authorization procedures. It provides detailed instructions for implementing the Risk Management Framework for classified systems.

When developing local procedures, cite the relevant DAAPM section to show auditors that your practices are grounded in official policy.

NISPOM (32 CFR Part 117)

The National Industrial Security Program Operating Manual provides overarching security requirements for cleared contractors.

The NISPOM establishes the baseline security requirements that must be met, while the DAAPM provides the specific implementation guidance for information systems.

ISSM & FSO Roles in the RMF Process

ISSM – RMF Implementation Lead

ISSM Responsibilities Highlights: Develop and maintain the System Security Plan (SSP) and policies, monitor system vulnerabilities and threats, conduct risk assessments (producing the Risk Assessment Report, RAR), develop and update POA&Ms for weaknesses, ensure user training and need-to-know, and enforce configuration management and continuous monitoring.

FSO – Integrating Security Program

FSO Responsibilities Highlights: Advise and brief cleared employees on safeguarding (NISPOM compliance), coordinate required security training (incl. cyber awareness), conduct periodic self-inspections (including for information systems), and ensure insider threat integration. The FSO also validates that all personnel accessing the system have the requisite clearance and need-to-know, in coordination with the ISSM.

Collaboration: The ISSM and FSO should work closely—e.g. during Prepare, the ISSM identifies security requirements while the FSO ensures facility clearance and senior management support; during Authorize, the ISSM submits the security package in eMASS while the FSO may brief the senior management official on residual risks. Both roles coordinate on continuous monitoring and incident response.

Collaboration Between ISSM and FSO

ISSM Responsibilities

- Implement and maintain RMF controls
- Manage system security posture
- Conduct technical assessments
- Maintain security documentation
- Monitor system vulnerabilities
- Implement security-relevant changes
- Manage user access (technical)

FSO Responsibilities

- Oversee facility security program
- Verify personnel clearances
- Conduct security briefings
- Lead self-inspections
- Interface with DCSA representatives
- Ensure NISPOM compliance
- Manage user access (administrative)

Collaborative Areas

- User onboarding and offboarding
- Security incident response
- Self-inspection activities
- Security awareness training
- DCSA assessment preparation
- Management briefings
- Contract/DD254 reviews

The ISSM and FSO roles complement each other. An ISSM who works in a silo, or an FSO who isn't engaged in the information systems side, can lead to gaps. Share information – e.g., the FSO should know about any significant system changes or issues (because they might affect facility security), and the ISSM should leverage the FSO's knowledge of NISPOM guidance and personnel security updates.

AIS Authorization Process

Pre-Kick-off — Set the Conditions for Success

Executive buy-in & staffing. Appoint an ISSM (must be a U.S. citizen) and confirm the FSO will be fully integrated in RMF activities. Have an alternate ISSM to avoid single-point failure.

eMASS access & training.

Timeline realism. DCSA "highly recommends" the complete security package reach them ≥ 90 days before the need date.

PREPARE (P-tasks)

Organizational prep – set risk tolerance, publish common controls, craft monitoring strategy.

Workshop the boundary diagram with IT, security, and program teams; unclear boundaries are the #1 cause of DCSA "Return Without Action."

CATEGORIZE (C-tasks)

Describe the system (C-1) and perform the FIPS 199 impact analysis for confidentiality, integrity, availability (default DCSA baseline = M-L-L).

Pull exact wording from DD 254s/SCGs into the SSP so reviewers see the lineage of every decision.

AIS Authorization Process (Continued)

SELECT (S-tasks)

Choose the baseline controls (DAAPM overlay, M-L-L) and tailor them (add/withdraw, designate common/hybrid/system-specific).

Document tailoring rationale inside eMASS.

IMPLEMENT (I-tasks)

Configure and deploy each control; build implementation descriptions, test results, and artifacts (screen-shots, SOPs, logs).

Update the SSP continuously; upload artifacts in eMASS (with "Implementation Guidance" or "Evidence" tags).

Use automated STIG / SCC scripts early; store raw scan files for assessor review.

ASSESS (A-tasks)

(Industry): ISSM/ISSO conduct internal self-assessment with SCC/STIG tools; remediate; build first POA&M; verify all eMASS fields complete.

(ISSP): DCSA assessor performs desktop review, on-site technical test, produces Security Assessment Report (SAR) and residual-risk recommendation.

(Industry): ISSM updates POA&M with SAR findings and uploaded evidence.

AIS Authorization Process (Final Steps)

AUTHORIZE (R-tasks)

ISSP verifies the final package and submits it through the Package Approval Chain (PAC) in eMASS.

AO issues one of five decisions (ATO, ATO-C, IATT, DATO, Decommissioned). ATD ≤ 3 years.

MONITOR (Continuous)

Execute the System-Level Continuous Monitoring (SLCM) Strategy built in the Implement step.

Update POA&M monthly/quarterly; mitigate vulns within 15 days (tech) / 30 days (admin) per DCSA "Gold Standard".

Perform and certify annual AIS self-inspection—results and fixes go to senior management and DCSA.

Manage changes via the CCB and, for security-relevant changes, submit an eMASS maintenance package.

Common Industry Pain Points

Incomplete Security Plan: Use a master checklist (DAAPM App D/Q templates). Hold a "package freeze" review before submission.

Tool-driven STIG failures: Update SCC content monthly; for legacy gear, craft a documented risk-based hardening standard.

Under-resourced POA&M: Attach cost/schedule lines to each POA&M item; escalate unresolved Highs at quarterly risk council.

Most Common identified Findings/Vulnerabilities

Continuous Monitoring Matters

Continuous Monitoring transforms security from a point-in-time assessment into an ongoing risk management discipline.

DAAPM Reference	Requirement	Practical Implementation
§7.7 paragraph 1	Required monitoring strategy	Document CM strategy in SSP

Critical Benefits

Situational Awareness

Decision-makers always know current risk level rather than waiting for next assessment.

Real-Time Management

Immediate risk analysis when security conditions change.

Control Validation

Confirms defenses remain effective as threats and technologies evolve.

Authorization Support

AO can adjust authorization status based on monitoring data.

Documentation & Evidence Best Practices

Maintain Thorough Records

Keep comprehensive documentation for all security activities including training records, configuration changes, incident reports, and POA&Ms.

Organize Evidence Systematically

Tag artifacts with control IDs and dates, use consistent file naming conventions, and maintain a master index of documentation.

Preserve Historical Data

Maintain version history of key documents, don't overwrite original information when updating records, and keep an audit trail of changes.

Leverage eMASS Effectively

Upload evidence with appropriate tags, maintain current documentation in the system, and use eMASS workflows to document approvals and changes.

If it's not documented, it didn't happen in the eyes of an assessor. During audits or SVAs, being able to pull up the exact artifact (e.g., "Here's the memo where we got AO approval to add that new software") builds trust and demonstrates compliance.

Why a Robust Media Management Program Is Mission-Critical for DCSA-Authorized AISs

1 Protecting Classified Data at Its Most Vulnerable Point

Removable digital media (USBs, CDs/DVDs, backup tapes, SSDs, printer hard drives) can physically leave the system boundary. Unless every stage—creation, labeling, carriage, reuse, and disposal—is tightly controlled, a single device can carry terabytes of classified material outside approved spaces.

2 Explicit DAAPM Requirements Tied to the ATO

An ATO is contingent on demonstrating that media controls remain effective throughout the life cycle. Key DAAPM mandates include:

Failing any of these controls presents a "technical vulnerability" in DCSA terms and must be mitigated within 15 days or logged on the POA&M — persistent lapses jeopardize the authorization.

Media Management: Mitigating Insider Threats & Lifecycle Assurance

3 Mitigating Insider-Threat & Spillage RiskDAAPM folds media handling into the Insider-Threat minimum standards required by EO 13587 and CNSSD 504. Media logs, TPI, and DT...

Media Management: Continuous Monitoring & Best Practices

A disciplined media-management program prevents data spills, thwarts insider threats, and maintains your ATO. Documentation & Logs Media logs feed the Continuous-Monitori...

Media Management: Mitigating Insider Threats & Lifecycle Assurance

3 Mitigating Insider-Threat & Spillage Risk

DAAPM folds media handling into the Insider-Threat minimum standards required by EO 13587 and CNSSD 504. Media logs, TPI, and DTA peer reviews provide non-repudiation and early detection of malicious or negligent acts.

4 Lifecycle Assurance—Creation → Transport → Reuse/Destruction

1. **Creation & Labeling** – Every device produced on a classified AIS inherits the **highest classification** until an Assured File Transfer (AFT) proves otherwise.
2. **Controlled Storage & Transport** – MP-4/MP-5 demand locked containers, courier orders, and (for Secret +) encryption or dedicated custodians.
3. **Virus Scans & Write-Protect Tests** – Low-to-high and high-to-high transfers require dual malware scans and write-protect verification to prevent malware ingress or data bleed.
4. **Sanitization / Destruction** – Appendix S prescribes NIST SP 800-88-style clearing, purging, degaussing or physical destruction, tailored to magnetic, optical, or solid-state media (NSA EPL devices, shredders, smelting, etc.).
5. **Documentation & AO Concurrence** – Every wipe or destruction action is logged; bulk-wipe utilities must meet multi-pass, bad-sector, and printout criteria. AO approval is mandatory for sanitization SOPs and any exceptions.

Media Management: Continuous Monitoring & Best Practices

A disciplined media-management program prevents data spills, thwarts insider threats, and maintains your ATO.

Documentation & Logs

Media logs feed the Continuous-Monitoring strategy. Auditors sample disposal records, DTA transfer sheets, and security-seal logs to verify controls remain effective.

- **Publish a media-management SOP** covering marking, custody, transfer, sanitization, and destruction
- **Store sanitized/destruction evidence** with the CM log

Transfer Controls

Rigorous transfer procedures maintain separation between classification levels and prevent data spills.

- **Use AV scanning** both *before* and *after* transfer
- **Implement TPI** for all High-to-Low moves; log both DTA names
- **Enforce factory-fresh rule** for inbound media

Sanitization & Destruction

NIST SP 800-88 processes for clearing, purging, degaussing, or destroying different media types are essential.

- **Periodically test** sanitization equipment and record results (MP-6(2))
- Obtain AO approval for sanitization SOPs and exceptions

Audit Readiness

Clean, current records demonstrate the ISSM is executing MP-6(1)'s "review/track/verify" enhancement—a strong indicator the ATO should remain in force.

- **Train and document** DTAs annually
- **Minimize portable media**; use company-owned, serialized devices
- Include incident-handling drills in training

Bottom line: For a DCSA-authorized AIS, a disciplined media-management program is not merely a paperwork exercise—it is the operational safeguard that keeps the ATO alive.

Change Management & Configuration Control

Formal Change Control Board (CCB)

Establish a CCB or similar process for reviewing and approving changes to the accredited information system.

Include the ISSM and/or ISSO as key members to evaluate security impact.

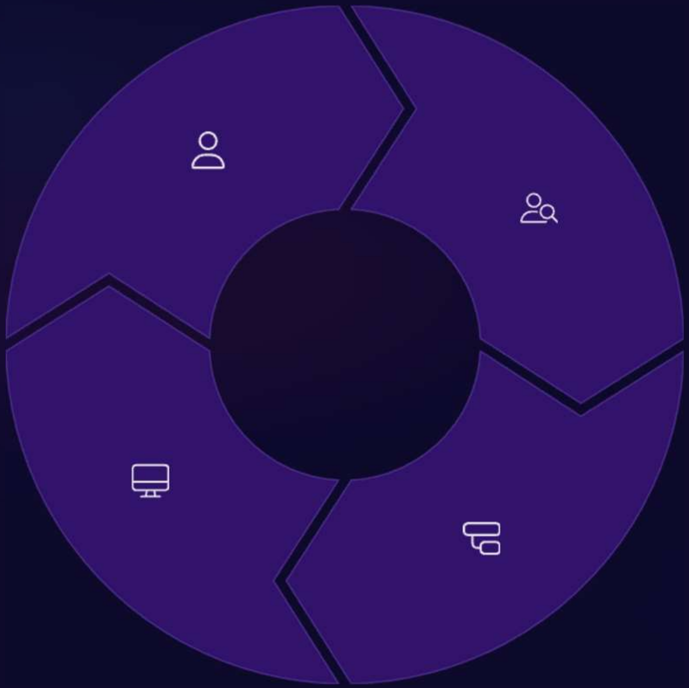
The CCB should also include system owners, IT support, and potentially the FSO for major changes.

Use of eMASS Workflows

Leverage the NISP eMASS system for change management with DCSA.

Significant changes should be communicated to DCSA via eMASS workflows.

eMASS has an Approval Chain that involves the ISSM, ISSP (DCSA reviewer), and AO.



Security Impact Analysis (SIA)

For each proposed change, perform a documented Security Impact Analysis.

Determine if the change is **security-relevant** – i.e., could it affect the system's security posture or accreditation boundary.

DAAPM emphasizes that the ISSM must assess changes to see if they could affect the authorization status.

Configuration Management Procedures

Follow documented CM policies for all changes.

Maintain an audit trail: update the system's hardware/software inventory, update network diagrams if needed, and record the change in a change log.

Ensure **no changes are made unilaterally** – even emergency changes should be reviewed after the fact.

New Account Creation & User Management

Clearance Validation

For each new user account on a classified system, the ISSM/ISSO must **verify the individual's security clearance level** (and citizenship status) is appropriate for the system's classification.

Need-to-Know (NTK) & Authorization

The ISSM/FSO must ensure the user has a need-to-know for the specific information on the system.

Document the authorization (e.g., an account request signed by the user's manager or the FSO) that confirms the need-to-know.

Mandatory Training & Briefings

New users must complete required security training before receiving access.
The ISSM/ISSO should **brief users on their system security responsibilities and restrictions** and have them sign user agreements.

Account Management Documentation

Follow a formal account creation process. Use an account request form that captures all necessary information..

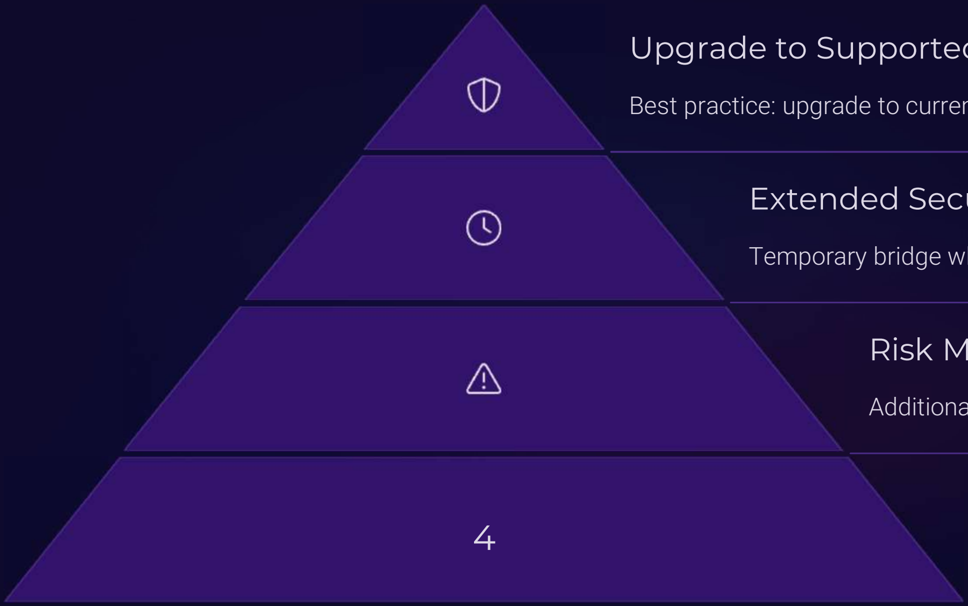
Enforce **least privilege** – assign the new user only the privileges/roles needed.

Compliance Checks for SA-22

Common DCSA Question	Proactive Response
"Are any systems running operating systems or software that are no longer vendor-supported?"	"We have a plan for Win10 EOL – all systems will be on Win11 by Q3 2025, and in the interim, we'll leverage Microsoft ESU for continued patching."
"How do you track end-of-life dates for your system components?"	"We maintain a software/hardware inventory with vendor support dates noted. We review this quarterly as part of our continuous monitoring process."
"What compensating controls do you have for legacy systems that cannot be upgraded?"	"For our specialized equipment running older OS versions, we've implemented network isolation, application whitelisting, enhanced monitoring, and received formal AO risk acceptance with a documented timeline for replacement."
"How do you budget and plan for technology refresh cycles?"	"We include technology lifecycle planning in our annual security and IT budgeting process, with specific line items for replacing EOL components before they reach end of support."

DCSA will scrutinize SA-22 compliance during assessments. It's far better to proactively address end-of-life issues than to be found non-compliant during an assessment. Not addressing EOL will likely result in a vulnerability finding.

SA-22 Compliance – Managing End-of-Life (EOL) Systems



Upgrade to Supported Systems

Best practice: upgrade to current supported versions

Extended Security Updates

Temporary bridge while planning full upgrade

Risk Mitigation Controls

Additional safeguards for legacy systems

Formal Risk Acceptance

AO approval for unavoidable exceptions

SA-22 – Unsupported System Components: NIST control SA-22 (adopted in DAAPM) requires organizations to **identify and replace or mitigate unsupported components**. When a system component (like an OS or application) reaches vendor End-of-Life (meaning no more security patches), it becomes a security liability.

Windows 10 22H2 EOL Example: Windows 10 (22H2) is the final release of Win10 and will reach end of official support on **October 14, 2025**. In anticipation, **develop an upgrade plan now**. Best practice is to upgrade systems to Windows 11 (or the latest supported OS) before that date.

Extended Security Updates (ESU): If an immediate upgrade isn't feasible by the EOL date, Microsoft offers **Extended Security Updates for up to 3 years beyond EOL** for Windows 10 Enterprise/Education editions. ESU is a paid program that provides critical security patches even after 2025.

Managing the POA&M (Plan of Action & Milestones)

Purpose of POA&M

The POA&M is a living document that **itemizes all known security weaknesses or deficiencies** in the system and tracks the plan to resolve them.

It's an essential part of the RMF package – used during authorization (to document residual risks) and during continuous monitoring (to manage ongoing improvements).

Every finding from assessments, audits, continuous monitoring, or self-inspections that is not immediately fixed should be recorded in the POA&M.

Required Information

For each POA&M entry, include: a **description of the weakness/vulnerability**, the **reference** (which security control or requirement is not met), the **planned corrective actions**, **resources required**, and a **milestone timeline** with scheduled completion dates.

Also note the status (open, in-progress, or closed) and any interim risk mitigation in place.

Updating and Tracking

The ISSM is responsible for **maintaining and updating the POA&M** regularly.

As work is done on an item, update the milestone dates or add comments on progress.

Do not erase history – when updating critical info in the POA&M, you shouldn't overwrite or destroy the original details.

Closure and Risk Acceptance

Ensure that each POA&M item is either **closed out** (fixed and verified) or **accepted** by the AO.

Closing an item means you implemented the corrective action and the vulnerability no longer exists (document evidence of closure).

If an item cannot be fully resolved, then you seek a formal risk acceptance or use a compensatory measure – but that exception and mitigation must be documented in the POA&M and approved by the AO.

Adding a New Contract/DD254 to an Accredited System

Assess Compatibility

Verify that the system's accreditation parameters cover the contract's requirements.

Check the classification level, categories/special markings, and any handling caveats on the DD254/Security Classification Guide.

The system must be approved for those levels/types of information.

Update Documentation

Revise the System Security Plan and other accreditation artifacts to incorporate the new contract.

Add the contract number and description to the SSP's scope, update the list of information types/data, and append the new Security Classification Guide references.

The Information Owner for the new contract should provide any unique security requirements.

DCSA Notification

Inform your DCSA ISSP or ISR about the addition of a new contract to the system.

Update the system's profile in NISS (National Industrial Security System) to list the new contract.

Use eMASS to upload the updated SSP and potentially a memo detailing the contract addition.

Implementing NTK & Access Controls

Ensure that only personnel with the new contract's need-to-know are given access to that program's data on the system.

The FSO should validate that everyone being added for the new contract is cleared to the appropriate level and briefed to any special accesses.

Maintain need-to-know segregation as required by the DD254.

Example Scenario: Adding a New Contract

Original System

System originally supported Army Contract A (Secret collateral)

System is accredited for Secret level information

Current users all have Secret clearances and are assigned to Contract A

New Contract

Air Force Contract B, also Secret collateral

Ensure Caveats match the original ATO.

New users will need to be added who are assigned to Contract B

Required Actions

Verify the system can meet any unique Contract B requirements

Update the SSP to mention Contract B, its DD254, classification guidance, and any changes

Notify DCSA via email or eMASS note that Contract B info will reside on System X

Implement need-to-know controls between Contract A and Contract B users if required

According to DAAPM, one system can host multiple Information Owners' data, and each IO's rules must be applied. This approach allows contractors to maximize use of accredited systems when security requirements are compatible.

Annual Self-Inspections for AIS

Annual Requirement

Cleared contractors must perform a formal self-inspection of their security program **at least annually**, and this includes **Automated Information Systems (AIS)** (classified IS) elements.

The FSO is typically responsible for running the self-inspection, with the ISSM focusing on the information systems portion.

Scope of AIS Self-Inspection

Verify that the system is being operated securely in accordance with the approved SSP and DAAPM controls.

Check user account management, review audit logs for anomalies, verify virus definitions and patches are up to date, validate security controls remain effective, and ensure documentation is current.

Use the same rigor DCSA uses – many contractors utilize the DCSA Self-Inspection Handbook and internal checklists mirroring NISPOM/DAAPM requirements.

Timely Mitigation of Issues

Treat self-identified issues with the same seriousness as DCSA findings.

Mitigate vulnerabilities within 15 days, and correct administrative issues within 30 days.

If something cannot be immediately fixed, enter it into the POA&M and plan out corrective measures with deadlines.

Documentation & Certification

Document the results of the self-inspection in a report – include what was checked, any findings, and corrective actions taken.

Per NISPOM requirements, **annually the Senior Manager must certify to DCSA in writing that a self-inspection was conducted**, that all issues were addressed, and that management has been briefed.

Retain all self-inspection records and be prepared to show them at the next DCSA review.

Preparing for a DCSA Audit

Review all SSP documentation for accuracy/changes

Validate all technical settings through automated and manual checks

Update eMASS with any undocumented changes.

Re-assess all Security Controls and CCIs

Leverage the Annual-Self Assessment to remediate any deficiency.

Host a pre-assessment meeting with the security team and stakeholders

Responding to DCSA Findings (Letters to Management)

Administrative Findings

Minor NISPOM/DAAPM non-compliance issues that **do not pose an immediate risk of** compromise (e.g. outdated documentation, training records incomplete).

Mitigation Timeline: Typically must be corrected within *30 days* of identification.

Document the corrective action (e.g. update the procedure or retrain staff) and be prepared to show evidence of closure.

Technical Vulnerabilities

Security weaknesses that **could lead to loss or compromise of classified info** if unaddressed. These can range from missing patches to misconfigured controls.

Mitigation Timeline: Aim to remediate within *15* days for most vulnerabilities, or even sooner for serious ones.

If a vulnerability is deemed *"Serious" or "Critical"* (imminent danger to classified data), notify your DCSA rep immediately and take prompt action.

Letters to Management & Follow-Up

After a Security Review/SVA, DCSA will issue a formal Letter to Management listing any findings. **Respond in Writing** by the required suspense (often 30 business days).

Enter all findings and corrective actions into your POA&M and/or tracking system. The ISSM should update the POA&M with status changes.

The FSO and ISSM should brief senior management on significant findings and the planned remedies.

Key Takeaways & Best Practices

1 Be Proactive, Not Reactive

Don't wait for DCSA to find problems – use the RMF continuous monitoring approach to self-identify and fix issues. Regular self-inspections, user training refreshers, and POA&M updates keep you ahead of the curve.

2 Documentation & Evidence Matter

Keep thorough documentation for everything – training records, configuration changes, incident reports, POA&Ms, etc. If it's not documented, it didn't happen in the eyes of an assessor.

3 Collaboration between ISSM and FSO

The ISSM and FSO roles complement each other. An ISSM who works in a silo, or an FSO who isn't engaged in the information systems side, can lead to gaps.

4 Follow the DAAPM and NISPOM Guidance

Whenever in doubt, refer to the DAAPM v2.2 for the correct procedures and the NISPOM/32 CFR Part 117 for overarching security requirements.

5 Maintain a Compliance Mindset

In the end, obtaining an ATO is not a one-time checkbox but an ongoing commitment. Embrace a culture of security: ensure every user, administrator, and manager understands that security is part of their job.

Proactive Security Approach

1 Regular Self-Assessment

Conduct frequent vulnerability scans and security checks

Don't wait for DCSA to find issues

2 Prompt Remediation

Address vulnerabilities within 15 days

Fix administrative issues within 30 days

3 Continuous Monitoring/Documentation

Update security artifacts in real-time

Maintain current POA&M status

4 Security Culture

Train all users regularly

Promote security awareness

Don't wait for DCSA to find problems – use the RMF continuous monitoring approach to self-identify and fix issues. Regular self-inspections, user training refreshers, and POA&M updates keep you ahead of the curve. A well-maintained security posture makes the authorization and re-authorization processes much smoother.

PC-WARRIORS

Dr. Jose Neto

PC-Warriors LLC
JNeto@PC-Warriors.com
407-715-7392

Expert Cyber Solutions and Services provider for RMF & CUI/CMMC