NISP AUTHORIZATION OFFICE (NAO)

NSI IMPACT 2022

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NISP AUTHORIZATION OFFICE
CRITICAL TECHNOLOGY PROTECTION

Topics

- NISP Authorization Office Workforce
- National Metrics
- COVID-19 Operational Adjustments
- Security Review Assessor (SCA) Triage
- DCSA Assessment & Authorization Process Manual
- NISP Connection Process Guide (CPG)
- NISP Enterprise Mission Assurance Support Service
- eMASS Processing- CCPs
- NAO – What is Next

DCSA NAO Policy, Authority, & Stakeholders

ISOO, NISPPAC, NISA Working Group

USD I&S
(DoD 5220.32 Vol1)

DoD/GOV Partners

DoD CIO, NSA, USCC, JFHQ, DISA, NIST,

Cybersecurity Policy
CNSS 1253
NIST 800-37

NISP Authorization Office (NAO)

GCAs

Mid-Atlantic Region AO Team Leads/Cyber Lead ISSPs

RMF, CCRIs, Security Reviews, Violation Inquiries, ISA/FOCI/ECP, Outreach - Guidance

Mid-Atlantic Region AO Team Leads/Cyber Lead ISSPs

RMF, CCRIs, Security Reviews, Violation Inquiries,ISA, FOCI/ECP, Outreach - Guidance

Mid-Atlantic Region AO Team Leads/Cyber Lead ISSPs

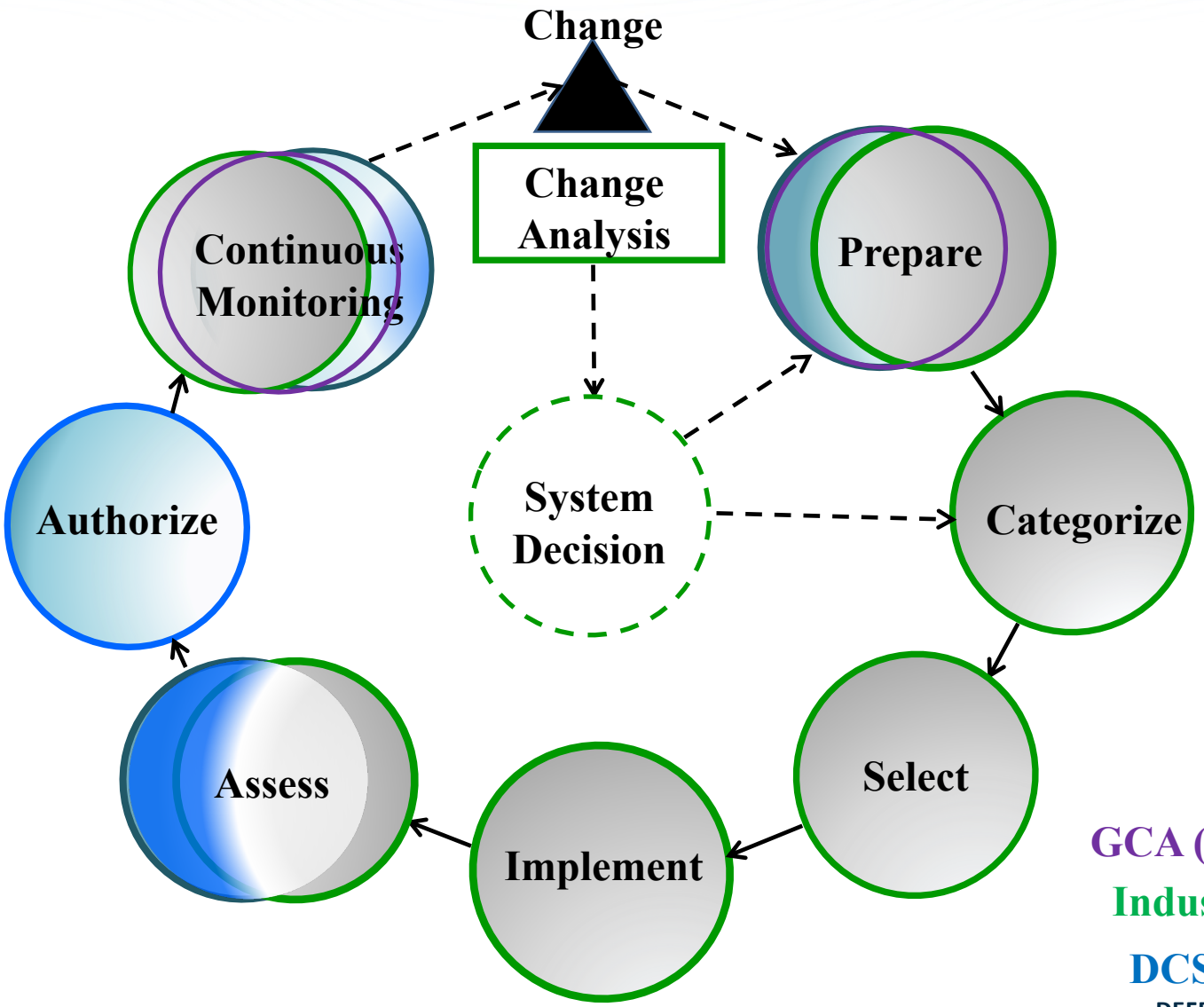
RMF, CCRIs, Security Reviews, Violation Inquiries, ISA,FOCI/ECP, Outreach - Guidance

Mid-Atlantic Region AO Team Leads/Cyber Lead ISSPs

RMF, CCRIs, Security Reviews, Violation Inquiries, ISA,FOCI/ECP, Outreach - Guidance

Cleared Industry (>6000 classified systems)
32CFR 117 (NISPOM)

NISP RMF Implementation

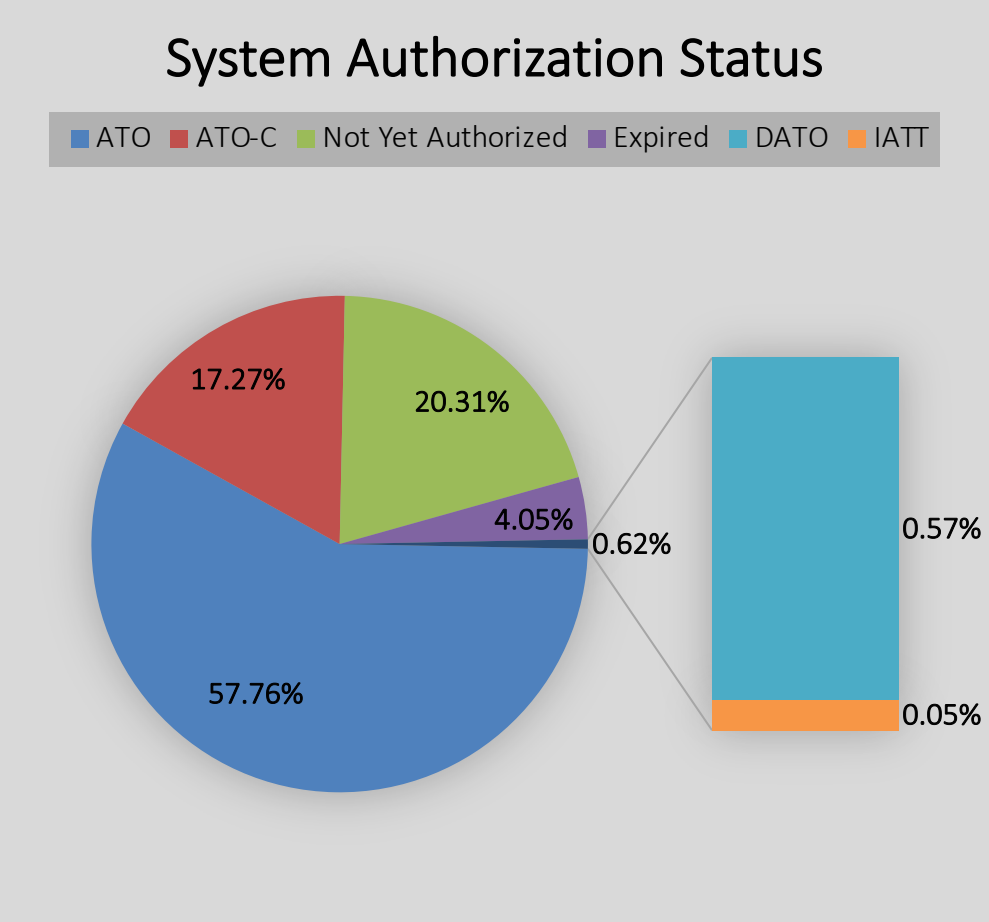


GCA (i.e. dd254)

Industry Action

DCSA Action

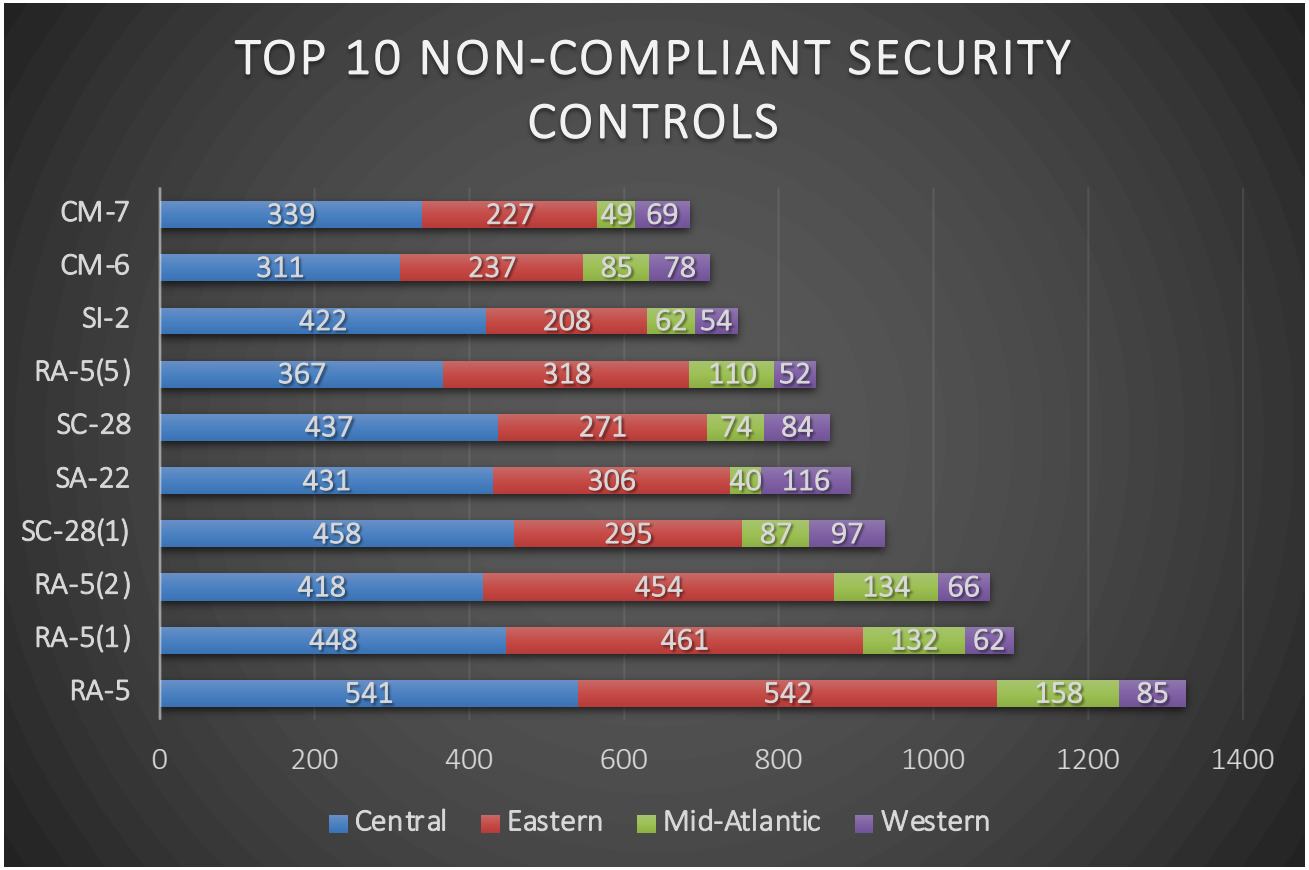
National Metrics



NISP eMASS Metric	Total
# Registered Systems in NISP eMASS	6,006
# of Authorizations Processed in FY21	3,473
# of NISP eMASS Users	4,079

Overview: The chart shows the percentage of all the systems within the NISP by authorization status. The following are the statuses: (1) Authorization To Operate (ATO), (2) ATO with Conditions, (3) Not Yet Authorized, (4) Expired, (5) Denial of Authorization to Operate (DATO), and (6) Interim Authorization to Test (IATT).

National Metrics



Security Control Information

RA-5: Vulnerability Scanning

RA-5(1): Vulnerability Scanning | Update Tool Capability

RA-5(2): Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified

SC-28(1): Protection of Information at Rest | Cryptographic Protection

SA-22: Unsupported System Components

SC-28: Protection of Information at Rest

RA-5(5): Vulnerability Scanning | Privileged Access

SI-2: Flaw Remediation

CM-6: Configuration Settings

CM-7: Least Functionality

Overview: This slide provides the top 10 non-compliant security controls within the NISP. In addition, the number of systems with the identified non-compliant security control is listed. A security control is deemed non-compliant when it is not properly implemented, operating as intended, and/or producing the desired outcome with respect to meeting established security requirements.

Security Review Assessor (SCA) Triage

- RMF SCA Triage - initial plan review for completeness prior to complete ISSP risk assessment
  - Initial cursory review enables immediate corrections as necessary from industry
- Common errors: Artifacts, Risk Assessment and Test Results (common issue with test results, controls do not reflect they were retested to support A&A reauthorizations and controls do not explain the how)

DCSA Assessment & Authorization Process Manual

- The Risk Management Framework (RMF) can only be successfully executed when the available resources are utilized.
  - Read the DAAPM to understand the RMF Assessment and Authorization (A&A) process and complete the required components of an RMF security plan.
  - Reference DAAPM Appendix A and B when addressing security controls.
- Security plan submissions, initial or a reauthorization, should be submitted at least 90 days before the need date.
- A timely assessment and authorization decision is contingent upon Industry submitting a complete and accurate security plan (Reference DAAPM Task A-7).
  1. Required System Details Populated;
  2. Implementation Plan & System Level Continuous Monitoring (SLCM) is completed for all security controls;
  3. Risk Assessment is addressed for all Non-Compliant security controls;
  4. Assessment Procedures (APs)/Control Correlation Identifiers (CCIs) assigned to a security control are tested and the test results applied;
  5. All Artifacts needed to support authorization activities are added; and
  6. Plan of Action and Milestones (POA&M) addresses all non-compliant controls.

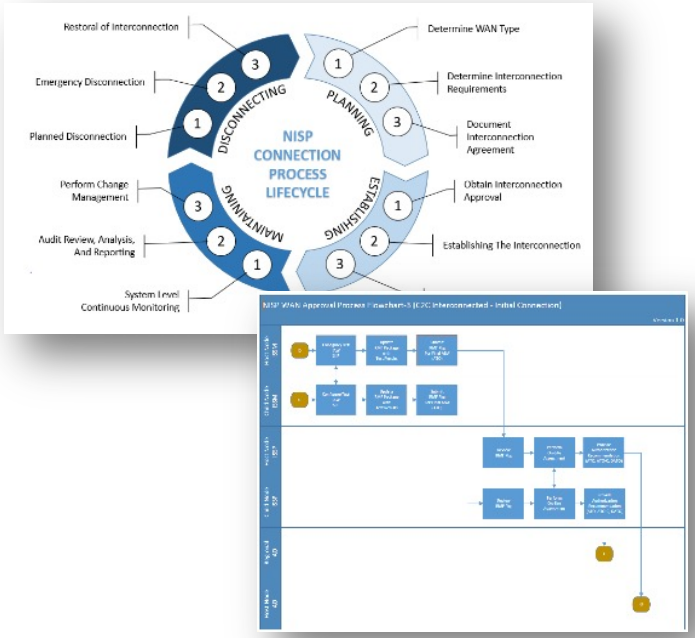
DAAPM Updates

- DAAPM Version 2.2 – Released August 31, 2020
  - Federal Information Systems (Section 9.8)
    - Amended guidance aligning with policy Department of Defense (DoD) Manual 5220.22, Volume 2, Industrial Security Procedures for Government Activities
  - Type Authorization (Section 13)
    - Provided clarification on the applicability of type authorization.

- Future DAAPM Revision (TBD - 2022)
  - NIST SP 800-53 Revision 5
    - NAO is tracking the transition from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 to Rev. 5.
    - Prior to updating the DAAPM, the updated Committee on National Security Systems Instruction (CNSSI) 1253 must be released.
  - 32 CFR 117 documentation updates
    - A tool is available to assist Industry in cross referencing Manual 5220.22, "NISPOM Manual," and 32 CFR Part 117, "NISPOM Rule," is available at https://www.cdse.edu/documents/toolkits-fsos/32CFR_Part117_NISPOM_Rule_Cross_Reference_Tool.xls

Draft NISP CPG

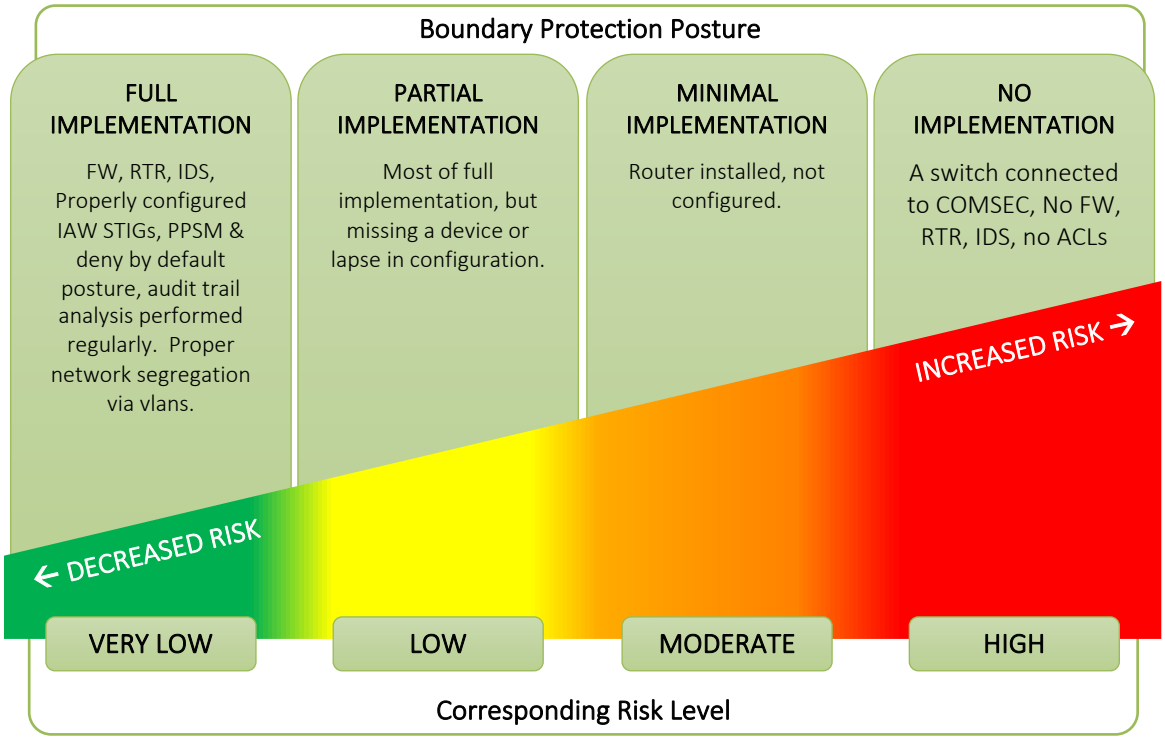
- NISP CPG Goal:
  - Provides guidelines for interconnecting systems processing classified information within the NISP
  - Easy to read guide format for government and industry stakeholders
    - Step by Step process, templates & enhanced guidance
    - RMF control mappings
  - Creates efficiencies for all NISP stakeholders & enhances security
  - New concepts such as:
    - Ports, Protocols, & Services Management (PPSM)
    - Corresponding Risk Levels with security posture guidance



- NISP CPG Status
  - Internal Working Group completing internal coordination June 2021
  - External Coordination to begin July-Aug 2021
  - Publication date – TBD

Draft NISP CPG - Boundary Protection Concept

- Example Only - Interconnection Guidance for improved security posture
  - Boundary, Training, & Auditing



eMASS Processing- CCPs

- Common Control Plans can't realistically include all 388 controls.
- CCPs will not be approved with "planned" controls.
- If a system with an inherited control is found to be NC, it will impact the CCP as well as ALL systems inheriting that control.
- Relevant controls must be marked as "common" or "hybrid and the applicable inheritability applied within NISP eMASS.
- Subsequent systems that inherit the controls have to identify the common control provider.
- Reference the recently released Common Security Controls and Inheritance Guidance (available on the NISP eMASS HELP page).

NAO – What is Next?

- Fiscal Year 2022 and Beyond
  - eMASS
    - Package Workflow enhancements (PAC).
    - Job Aids & additional guidance.
  - DAAPM 3.0
    - Provide enhanced guidance & clarity for industry.
    - Process improvements, identifying and addressing any gaps.
  - NISP Connection Process Guide (CPG).
  - Command Cyber Readiness Inspections (CCRI).
  - eWANs – Enterprise WANs.
  - Continued collaboration with NISP stakeholders.

Questions

- Utilize available resources (DAAPM, eMASS [HELP], NISP eMASS Internal and Industry Operation Guide, and DISA RMF Functionality Guide).
- Visit the DCSA website: https://www.dcsa.mil/mc/ctp/