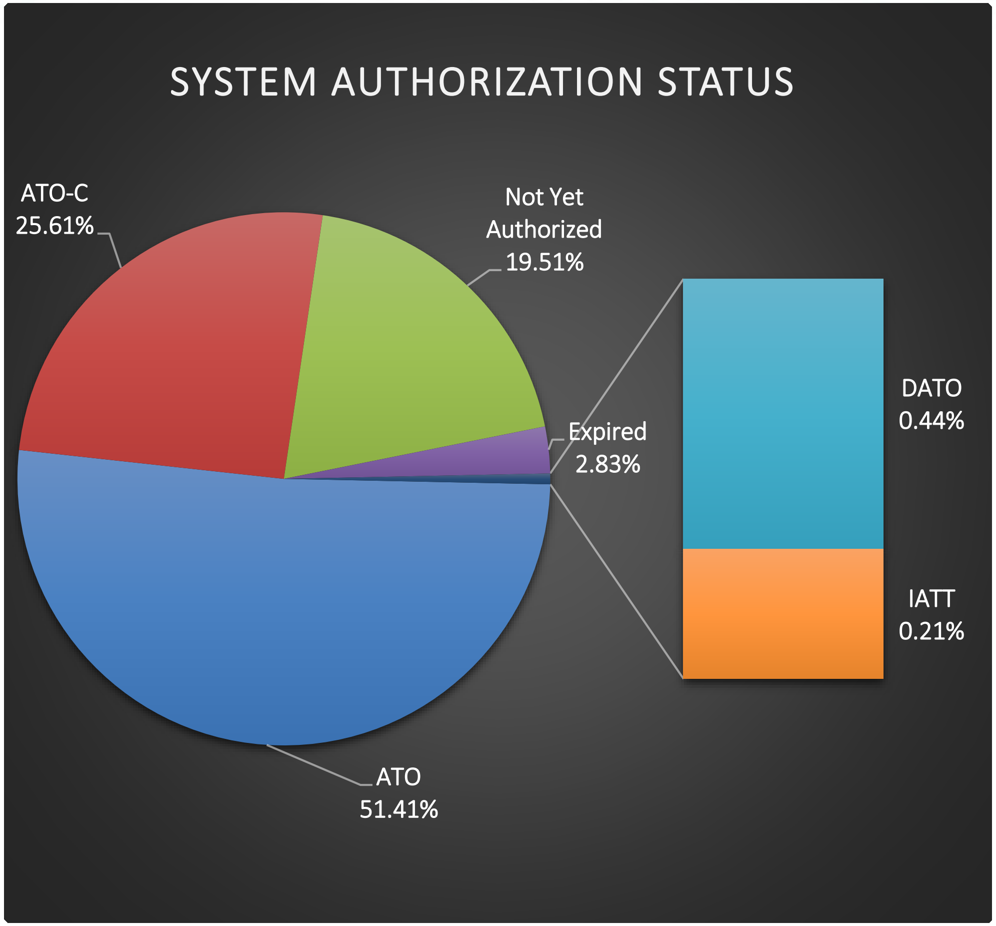
DCSA
NISA WORKING GROUP
UPDATE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DAVID SCOTT
NISP AUTHORIZATION OFFICE
CRITICAL TECHNOLOGY PROTECTION

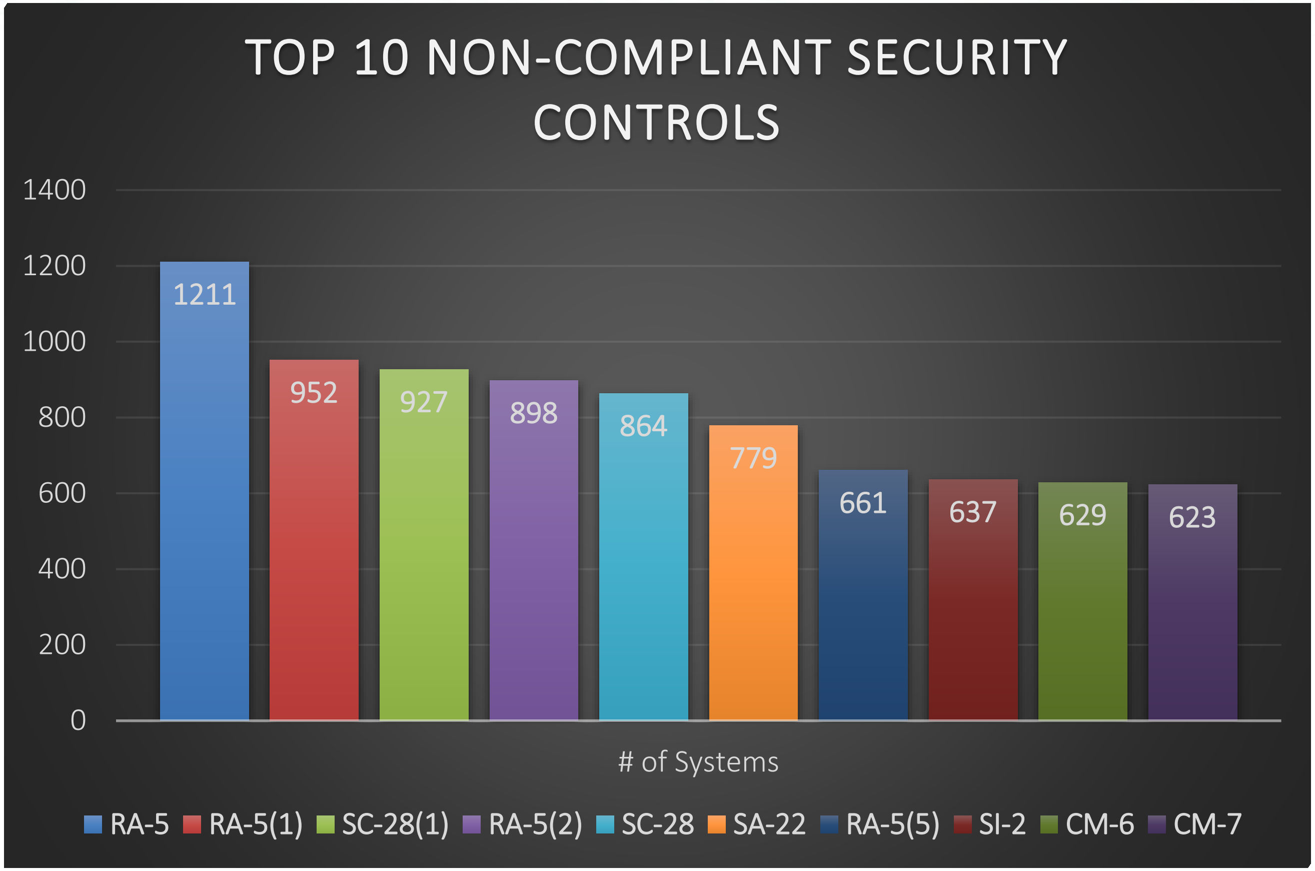
National Metrics



NISP eMASS Metric	Total
# Registered Systems in NISP eMASS	6,292
# of Authorizations Processed in FY21	2,995
# of NISP eMASS Users	3,649

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

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

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

SC-28: Protection of Information at Rest

SA-22: Unsupported System Components

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.

DAAPM Update

- 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.
  - An internal Working Group developing a Connection Process Guide (CPG) in order to assist all stakeholder with the establishment of interconnections. The CPG will provide process flows, templates, and guidance.

NISP eMASS Common Issues

1. Failing to follow the guidance in the NISP eMASS Industry Operation Guide
2. Incorrect System Name/System Acronym - *DCSA guidance for NISP eMASS system naming must be followed*
3. System details not fully populated
4. Incomplete System Description
5. Improper application of overlays
6. Artifacts needed to support authorization decision are not included in the security plan
7. Risk Assessment Reports (RAR) are not conducted at both the organization and system level. RARs must fully address: (1) relevant threats, (2) vulnerabilities (internal and external), (3) impacts to the organization, and (4) likelihood
8. Unsatisfactory inputs for Implementation Plan, SLCM, and Test Results (*All CCIs must be addressed*)
9. Plan of Action & Milestones (POA&M) is not accurate and/or does not address Non-Compliant security controls
10. Failing to submit security plan 90 days prior to Authorization Termination Date (ATD)

Questions

- Use 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/