DCSA
NISP CYBERSECURITY OFFICE (NCSO)
NISA WG

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DAVID SCOTT
NISP CYBERSECURITY OFFICE
INDUSTRIAL SECURITY DIRECTORATE

NISP eMASS Updates

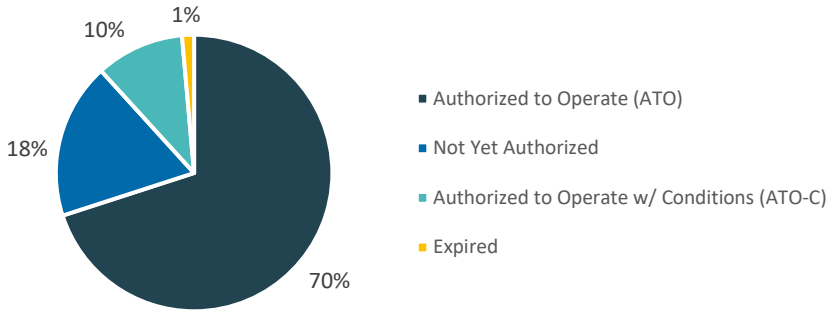
- The Defense Information Systems Agency released version 5.11 of the Enterprise Mission Assurance Support Service (eMASS) on March 2, 2024.
- The release introduced NISP specific enhancements and improved functionality. All enhancements are detailed in the NISP eMASS 5.11 Release Notes posted on the NISP eMASS Help page under “Organizational Artifact Templates, SOPs, and Guides”. The highlights of the NISP specific enhancements include:
  - System information customization
  - Removal of not applicable modules
  - User navigation tools
  - Custom auto-generated authorization letters
  - Enhanced metrics and reporting capability.
- The 5.11 release also introduced a migration capability that will allow organizations to migrate systems that have completed assessments against the NIST SP 800-53 Revision 4 controls to the Revision 5.
- Revision 4 remains the standard for the NISP eMASS. NCSO is conducting early planning phases. As we get closer to a target date, we will coordinate with the NISA WG and provide a transition plan.

National-Level Metrics

NCSO Baseline Stats:

- The NISP Cybersecurity Office oversees ~5,600 classified IT systems as a part of the of National Industrial Security Program (NISP).
- The Industrial Security (IS) instance of eMASS had over 3,600 users and processed over 2,100 authorizations by the end of FY23.
- ~35% of systems in the NISP have a Plan of Action & Milestone (POA&M) in process to address security controls and safeguarding efforts.

System Authorization Statuses Within the NISP



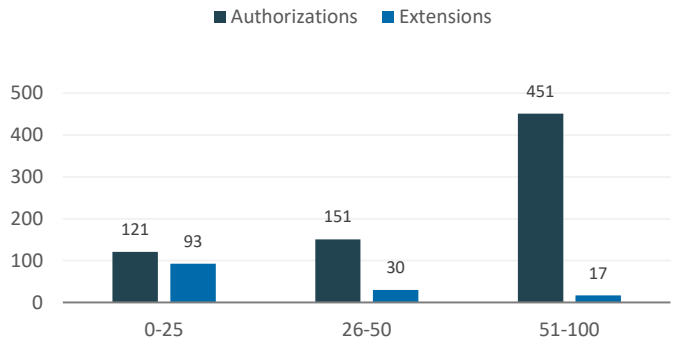
*Note: Denial of Authorization to Operate (DATO) & Interim Authorization to Test (IATT) omitted as combined total equals <1%

Median # of Days for NISP eMASS Authorization Decision:

IS Business Plan: < 90 Days

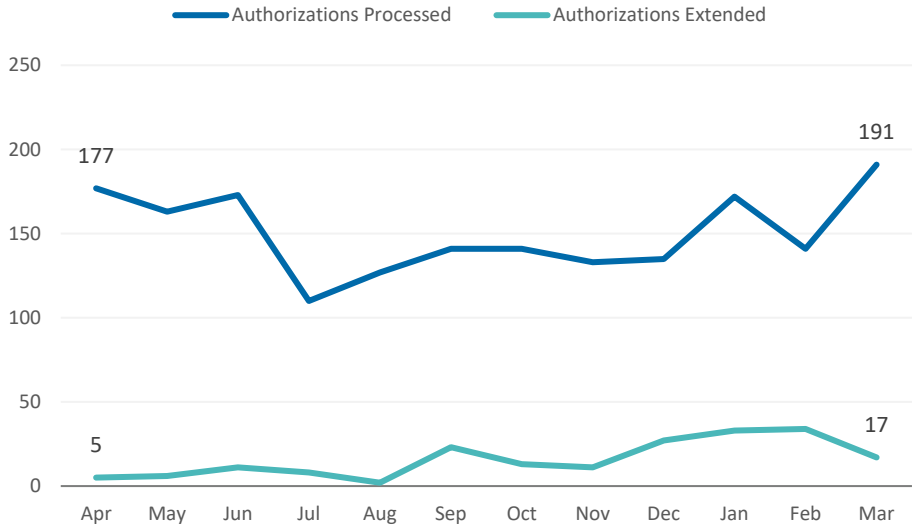
Med. Days for Authorizations:	Med. Days for Extensions:
78 Days	15 Days

Number of Completed Workflows by Days to Process:



Days for NISP eMASS Authorizations include both days in industry and days with DCSA

Number of Authorizations Processed and Extended



DAAPM v3.0 update

- Name change – TBD
- Internal Working Group led revision & updates to align with CNSS 1253 as appropriate
  - Updates to applicable references
- Provide clarity to areas identified by industry & internal work force since previous addition
- Coordination process
  - Internal coordination completed October 2023
  - Informal coordination with NISA Working Group completed March 2024
  - Next – formal coordination process
  - Transition & release – TBD

Industry Classified Cloud - ISL

- DCSA has issued Industrial Security Letter (ISL) 2024-01, Commercial Cloud Services (CCS).
  - Clarity on the process for DCSA to verify that a cleared contractor's contract includes an authorization by the Government Contracting Activity for the use of CSS in the performance of a classified contract as required by the Defense Federal Acquisition Regulation (DFARS).
- DCSA NISP AO may authorize Impact Level (IL) 6 CCS under one of the methods below to verify the contract requirement.
  1. On the DD Form 254, "Contract Security Classification Specification," block 11c ("Receive, Store, and Generate Classified Information or Material," is checked, and details on the use of IL6 CCS pursuant to contract-specific performance requirements are provided in item 13.
  2. If this information is not provided on the DD Form 254, the contractor may verify to DCSA that DFARS clause 252.239.7010, "Cloud Computing Services, is included in each contract for which IL6 CCS are required.
  3. If the contractor initially indicated in the solicitation that it did not anticipate using CCS in the performance of the contract, but later decides otherwise, DFARS clause 252.239-7010 states that the contractor "shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract." Proof of the contracting officer's approval may be accepted in a variety of forms, to include an email from the contracting officer or empowered official.

Industry Classified Cloud – Job Aid

- Industry is required to have customer/data owner approval to move their contract data into the Cloud in accordance with the Defense Federal Acquisition Regulation (DFAR)
- Industry must work directly with CSP and government sponsor on requirements to provision Industry purchased accounts/tenants.
- Cleared contractors and their government sponsors may review DISA approved IL6 Provisional Authorizations (PAs) at: https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/sitepages/CSOCatalog.aspx (PKI enabled).
  - DoD and Industry may have separate PAs for services. Recommend reading the PA to determine its applicability and services offered to Industry.
- After the contractual relationship is established with the CSP, the ISSM shall initiate and submit the applicable workflow within the NISP eMASS to request an Interim Authorization to Test (IATT).
  - Recommend Industry leadership focus on the RMF “Prepare” step
- The cleared contractor shall request a Cloud tenant kick-off meeting for DCSA support by sending an email to their assigned DCSA representatives and our NCSO mailbox at dcsa.quantico.hq.mbx.nao@mail.mil.

CORA (Formerly CCRI)

- Objective:
  - Resolve high risk vulnerabilities discovered during CORA to ensure mitigation of adversarial risk; provide situational awareness for Senior Leadership to facilitate improvements of DODIN Area of Operations' (DAO) Cybersecurity posture with a focus of reducing operational risk; Impart adversarial risk to DAO's and Mission owners accountable to shape cybersecurity posture ; Harden DoD Information Systems, reduce attack surface and strengthen defense.

- CORA aligns with a Risk-based methodology vs Compliance-based under legacy CCRI
  - CORA has officially transitioned to 3.0. JFHQ-DODIN Risk Based Metrics are derived from analyzing the MITRE ATT&CK Framework and through Key Indicators of Risk (KIORs) directly impact the risk rating

- DCSA CORA Team
  - FY24 utilizing a hybrid team of dedicated and volunteer personnel on track to conduct 30 assessments an increase from 16 in FY23
  - hiring actions ongoing to hire an additional 10 dedicated reviewers during this FY
  - Established leadership structure with 5 Cyber Team Leads, CORA Chief and Service Cyber Lead
  - FY25-27with a more dedicated workforce increase inspection frequency to every other year