Enterprise Mission Assurance Support Service (eMASS)

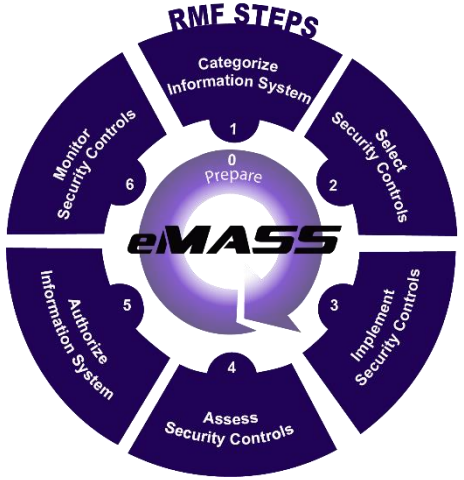
DISA

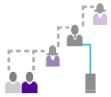
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

eMASS

SERVICE

- **Software as a Service (SaaS) or Deployed** for Organizations automating Cybersecurity Risk Management, Risk Management Framework (RMF), Assessment & Authorization (A&A), and Certification processes. *As a shared service, enhancements are engineered to be available for the entire community, contribution from one organization benefits all.*
- **Operational on NIPR, SIPR, SAP, Internet (approved-only), Agency-Network.** Centralized deployment per classification level, maintained and operated by DoD, scalable by multi-tenant instantiations for both data isolation and sharing. Supports CAC/PIV (PKI), Single Sign-On authentication (SSO SAML2).
- **Subject-Matter Expertise/Support Services.** Onboarding, Requirements/Customization & Tailoring, Enhancements & Integrations, Business Process, Hands-On Instructor-Led Training.





Workflows and Role-based access control for managing essential security functions from system registration through decommissioning.

Enabling execution for RMF Steps (automate NIST 800-53 and Committee on National Security Systems Instructions (CNSSI) 1253 System Categorization, PO&AM Management, Security Control Assessments, Risk Review).

Generation of standardized RMF Reports, Digital Signatures on PDFs, Dashboards and metrics roll-ups, and automated reporting for Enterprise requirements (e.g. DoD CIO for RMF data calls).

Advanced features such as Inheritance hierarchies, API enabling system-to-system integrations, Collaboration Boards for Workflows, and operational Continuous Monitoring support with sensor data.

- Customize Organizational Hierarchy, User Roles and Workflows
- Register and Track Information Systems
- Apply Data Types, Control Baselines, and Overlays
- Develop & Manage Plan of Action & Milestones (POA&M)
- Manage and Track Security Control Assessments
- Automate and Generate Policy-Required Documents
- Validate Data Based on Policy-Business Rules
- Provide Enterprise Visibility with Executive Dashboards
- Integrates with your Systems through an API
- Integrates with Sensor Data Repositories for Continuous Monitoring

User Community

METRICS

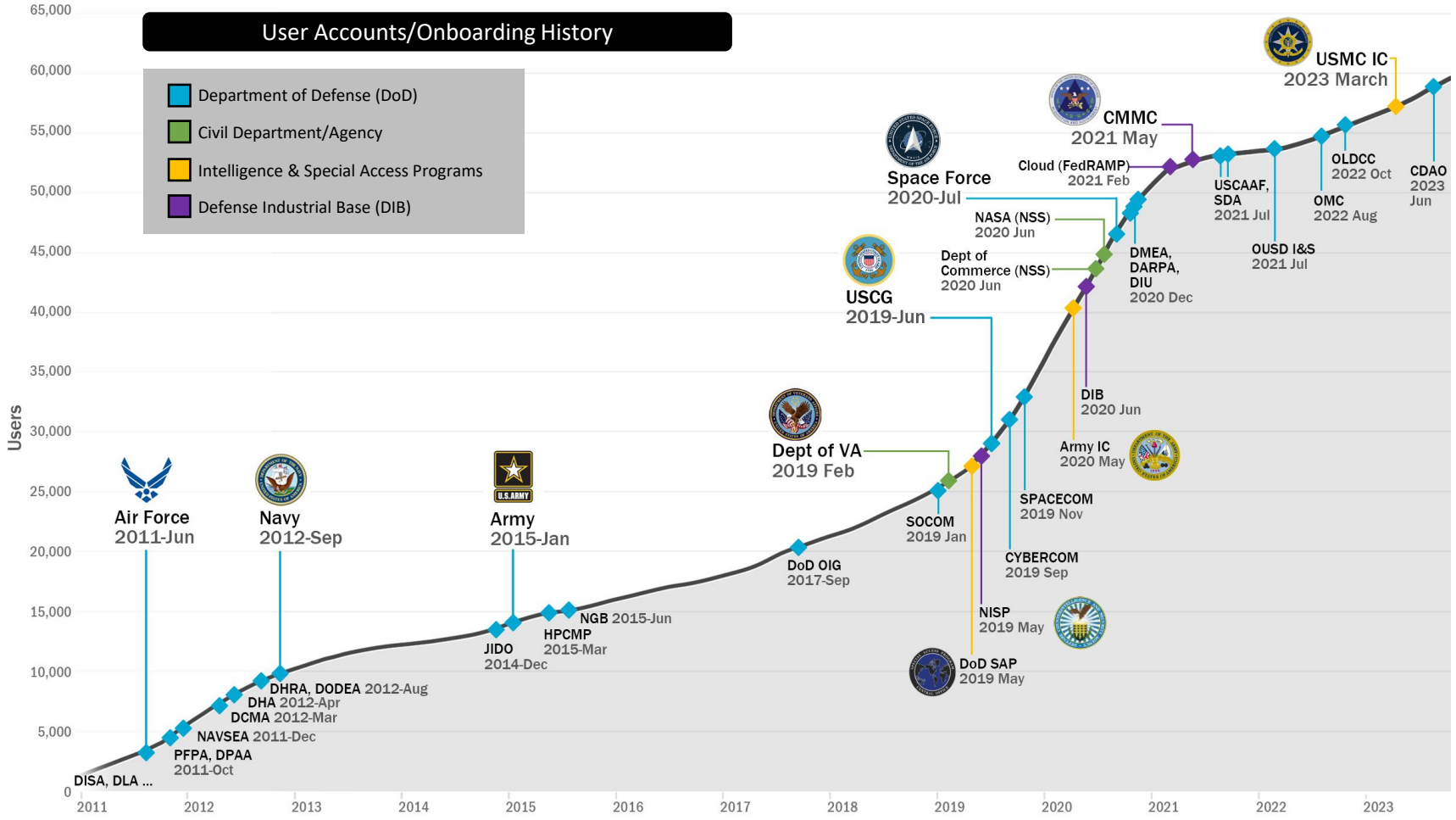
58K — **User Accounts**
36,000+ (35 day active)

60 — **Organizations**

22.8K — **Systems**
80,000+ (incl. decom)

300K — **Authorization Packages/Decisions**

200+ — **New Features Annually**



Unclassified, Agency, NIPR	SIPR	JWICS	SAP
DoD, Veterans Affairs, CSPs & Industry Programs	DoD and Civil Agencies with NSS	Army IC, Marine Corps IC	SAP CIO Community

Mission Support

DoD RMF

DoDI 8510.01 RMF

SP 800-53, SP 800-37, SP 800-30, SP 800-137, FIPS 199,…

CNSSI 1253

- Army, Air Force, Navy, Coast Guard, Space Force
- DAU, DCAA, DCMA, DeCA, DFAS, DHA, DHRA, DISA, DLA, DMA, DoDEA, DoDIG, DPAA, DCSA, DTIC, DTRA, DTSA, HPCMP, JIDO, JSP, MDA, NGB, PFPA, SecDef, WHCA, Joint Staff, USSOCOM, USAFRICOM, USCENTCOM, USEUCOM, USPACOM, USNORTHCOM, USSOUTHCOM, USSTRATCOM, USTRANSCOM, USSPACECOM, DIU, DMEA, DARPA, OSD (OUSD A&S, OUSD P&R, USD-P, OUSD I&S), USCAAF, IWTSD, OMC, SDA

Civil RMF

VA Directive 6500

SP 800-53B

- Veterans Affairs
- Dept. of Commerce (NSS)
- NASA (NSS)

IC/SAP RMF

IC IT Systems Security Risk Mgmt

Joint SAP Implementation Guide (JSIG)

- DoD SAP CIO Community
- Army Intelligence Community

Other Risk Mgmt/Certifications

NISP (DoD 5220.22-M)

CMMC

FedRAMP
FISMA

CSSP CSF ESM v10

- National Industrial Security Program (NISP)
- JFHQ-DoDIN's CSSP Evaluator Scoring Metrics
- Cloud (FedRAMP DoD Provisional Authorizations)
- Defense Industrial Base (NIST SP 800-171)
- Cybersecurity Maturity Model Certification (CMMC)

Services Summary

Service Area	Description
Managed System	• System provided software-as-a-service (SaaS) including infrastructure hosting costs, software licenses, hosting operations & maintenance, A&A maintenance (ATO), etc; or managed Deployed. • Currently Unclassified/NIPR (DISA hosted), SIPR (DISA hosted), Special Access Programs (DoD/SAP CIO hosted), JWICS (Army hosted).
Instructor-Led Training	• Instructor-led training for 30-60 students per class (virtual, at your location, or DC Metro region). • DoD/generic flavor training curriculum (and workbook/hands-on modules designed). • Hands-on modules and training environment (brought to your location or online sandbox with virtual events).
Help Desk & Enterprise Support	• Help desk support to answer end-user questions related to eMASS usage, RMF policy, technical issue troubleshooting, etc. • Customer requests such as data analysis, metrics queries, subject matter expertise & recommendations. • Enterprise support for Continuous Monitoring implementations, API integrations, etc.
Enhancements, Customizations	• Engineering for implementation of enhancements, configurations, customizations (e.g. fields, roles/workflows, custom system integrations, tailoring of capability, new capability aligned to need/direction, etc.).
Community Collaboration	• Ensure enhancements/efficiencies funded/executed by one Component/Agency beneficial for the community is made available to all eMASS users. • Collaborate with RMF TAGs & eMASS Configuration Control Board (CCB) for Community-wide execution of major automation/implementation guidance. • (SaaS-only) Automation between eMASS-using Components/Agencies (Inheritance across all, Reciprocity, etc.) for those with a common Control Set.

Standard Model

DoD RMF Technical Advisory Group (TAG)

Agency TAG, Organization

Responds to RMF TAG/Enterprise & Organization/Agency changes in implementation guidance

eMASS Joint-Stakeholder Configuration Control Board

Organization/Agency (optionally) joins the eMASS CCB to drive methodology

eMASS workstream supports Agency's AO/RMF/Policy & Implementation organization for execution of *their own requirements per Agency's direction and priorities*.

Backup

Program Structure

EMASS CONTRACT STRUCTURE

- eMASS is supported by a Blanket Purchase Agreement (BPA) contract, with the ability to support both Federal agencies
- DoD Organizations (e.g. Service/Component/Agency) can use DoD (e.g., MIPR) or Interagency process for access to the BPA.
- Non-DoD Organizations (e.g. Department/Agency) can use 7600A/B process for access to the BPA.

EMASS PROGRAM STRUCTURE

- No Organization is required to use eMASS. All usage/adoption is voluntary. eMASS is operated centrally SaaS or deployed by DoD for Federal (DoD Components and Civil) Agencies.
- Central operations for the program are provided by DISA while Organization (Agency)-specific efforts as individual task orders for support on the eMASS BPA contract. Organizations can establish their own workstreams for ongoing support, customizations/development, integrations, training, etc.

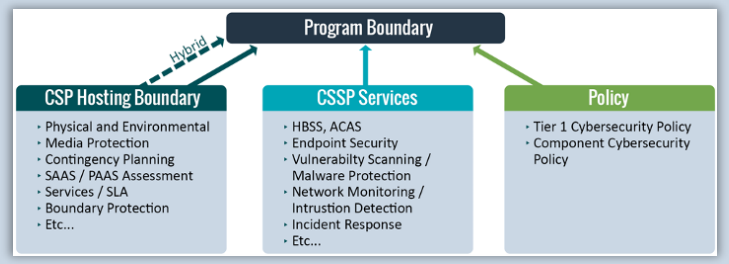
POCS

- **eMASS Tier III Support:** disa.meade.id.mbx.emass-tier-iii-support@mail.mil
- **DISA PM:** vonzell.o.bandy.civ@mail.mil
- **CTR Support:** stephen.j.mao.ctr@mail.mil, cameron.b.childs.ctr@mail.mil
- **DoD CIO:** jeffrey.a.eyink.civ@mail.mil

Major Features

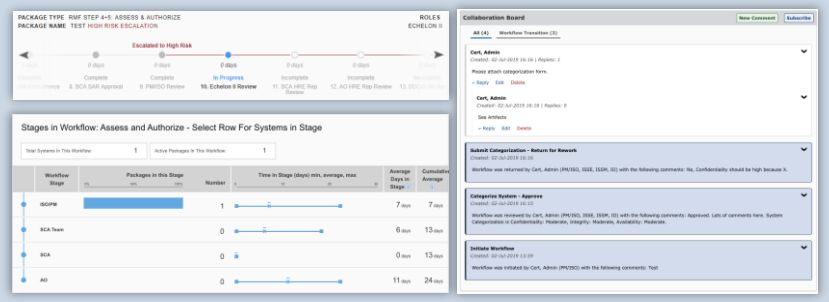
Inheritance Automation

Enables providers to propagate Control data across thousands of systems and establish CCPs, Cloud hosting systems, Cybersecurity Service Providers, etc.



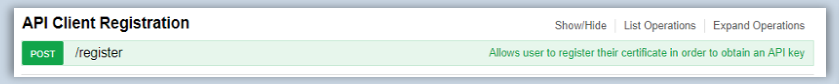
Workflows

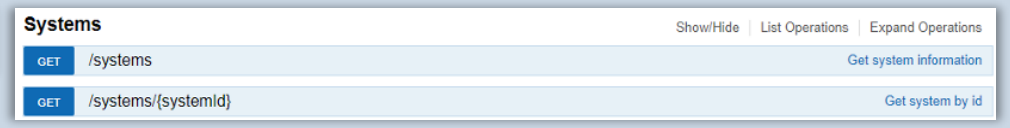
Workflows for process automation and approval processes alongside dashboard tracking and comments boards.



Web Service API

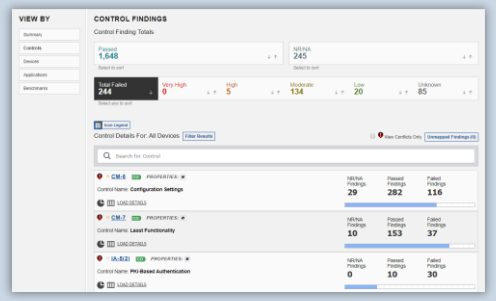
Web Service API (JSON, REST) for system-system integrations

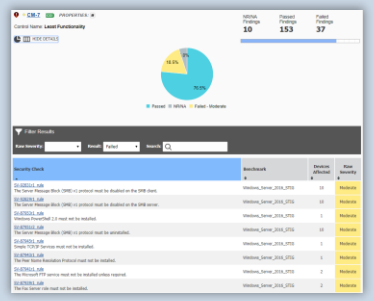


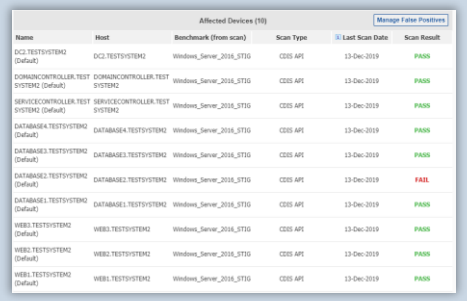


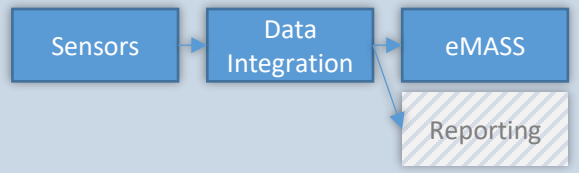
Assets w/ Continuous Monitoring

<u>Automated end-to-end</u> sensor data into system/authorization boundary for devices, scan results (vulnerabilities/configurations). For Civil Agencies, eMASS implements 2-way integration with CDM Data Integration (Layer B) – Executed on Layer B impl. used on Defend D and B.









Inheritance

INHERITANCE AUTOMATION

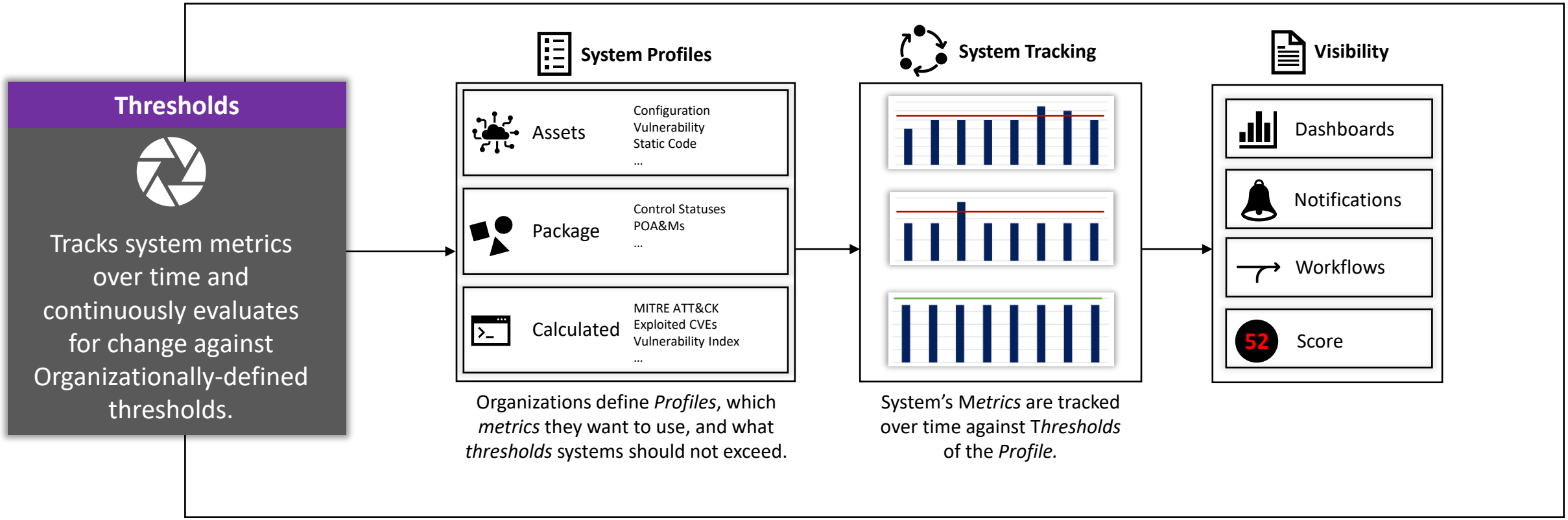
- Enables creation of Enterprise and Hosting common control provider System records/packages to automate Security Controls in receiving Systems.
- Enables establishment of relationships between System records and automated propagation of Control data.
- **Tired:** Enables multi-level Inheritance hierarchies.
- **Multi-Parent:** Enables multiple providers to single Controls (e.g., distributed hosting).
- **Hybrid:** Enables inherited Security Controls with shared responsibility.

DATA SUPPORTED

- Control Status, Implementation Narrative, Assessment Procedure Test Results, Artifacts POA&Ms, etc.) update from providers to receiving Systems in near real-time.
- Provider contact information (e.g., Provider PM/ISSM/System Owner POC information).

Thresholds

- A minimally required amount of data can provide an automated means of deviation over time available to the ISSO/ISSM, SCA, and AO (with an ongoing refinement of accuracy of a risk-based automated measure).



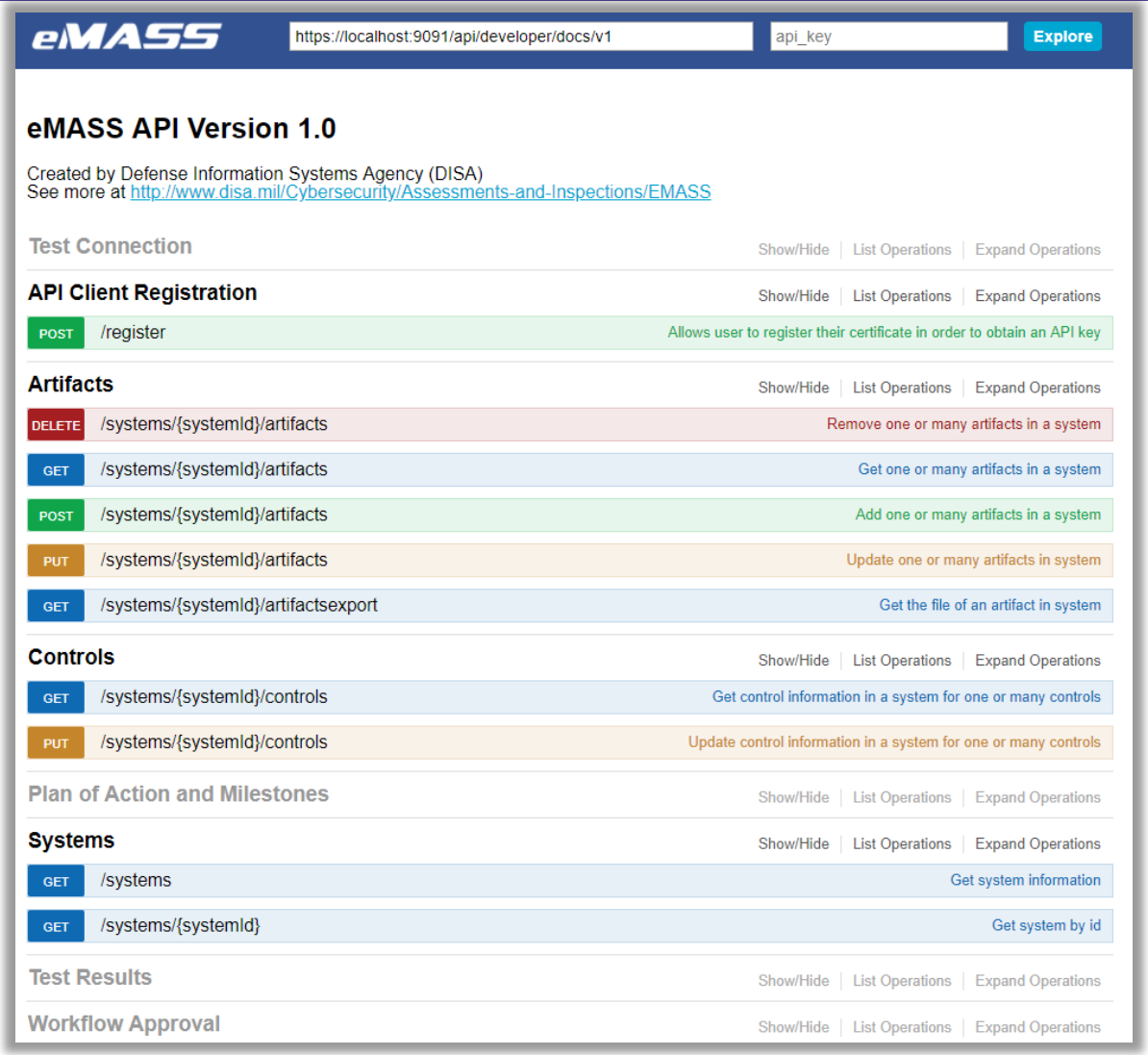
Web Service API

WEB SERVICE API

- JSON RESTful Web Service API with endpoints for two-way access of core eMASS data elements supporting system-to-system interfaces.
- Granular permissions provides control of the client application to specific sub-organizations, read/write, etc.
- **Available Networks:** DoD NIPRNet, SIPRNet, JWICS, and Agency Network (e.g., VA) with PKI/Client Certificate authentication.
- **Internet Availability:** Limited capability on Internet is in-progress for Early Summer, 2024 (approved by Agency, Component, Service)

CURRENT USAGE

- 40+ active integrations using the eMASS API to Enterprise Reporting & Automation use cases
- Multiple integration efforts are currently in-progress. New requests are queued based on priority order, please contact the eMASS Tier III support team at disa.meade.id.mbx.emass-tier-iii-support@mail.mil for additional information.



Major Features: Assets

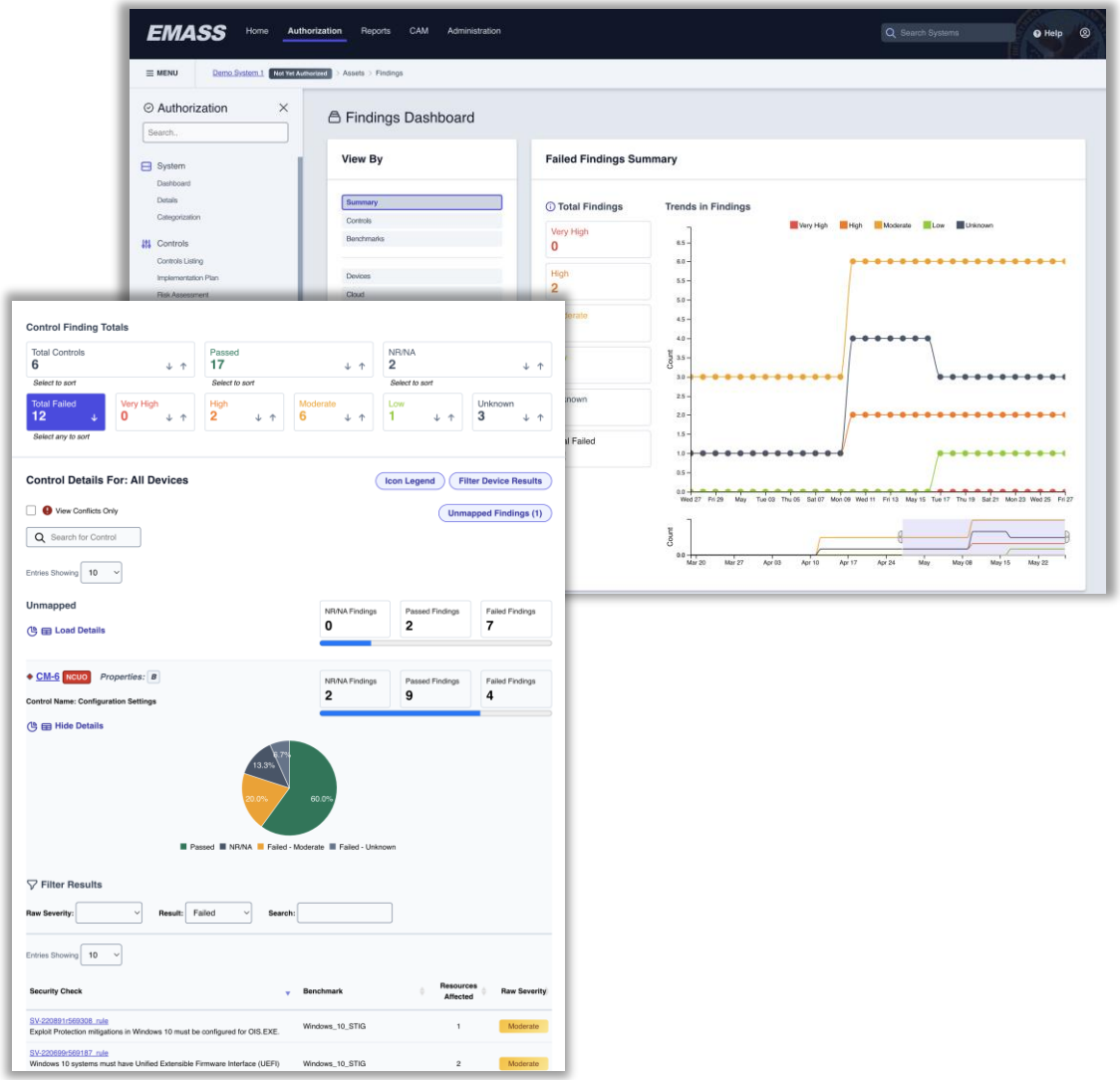
CORE CAPABILITY

- Cyber Content (STIGs, IAVM notices, Plugins, NVD/CVE, COAMS/device tags) is ingested to provide definitions, vulnerability information, and correlation to Security Controls.
- Automated and manual uploads for Devices, Vulnerabilities/Patch Compliance, Configuration/STIG Compliance (STIG Viewer, SCC, ACAS, HBSS, etc.); Management of hardware/software inventory baseline.
- Automated roll-up/visibility to Security Controls using Enterprise definitions, Community sourced mappings.

EMASS ASSETS INTEGRATION

Integrated with CMRS or other repositories (containing publishes of device and scan data endpoint/vulnerability sensors) and Civil CDM Layer B/Data Integration Layer.

- Cyber Content (STIGs, IAVM notices, Plugins, NVD/CVE, COAMS/device tags) is ingested to provide definitions, vulnerability information, and correlation to Security Controls.



Major Feature: Workflows

SUPPORTS A&A PROCESSES

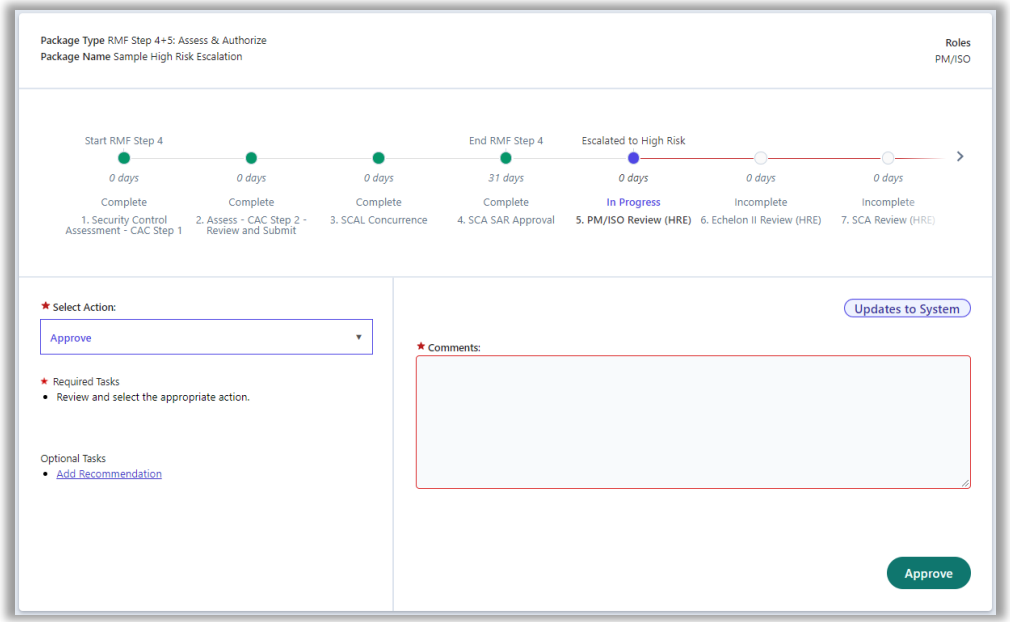
- Organizations can define complex workflows (multiple, simultaneous, branched, conditional, etc.) for A&A processes.
- Workflows support eMASS' **package approval chain roles** assigned to Stages to perform actions during the stage.
- Shows **hyperlinked required tasks** for the assigned personnel to complete or to show information for the reviewer.
- Supports **multiple-active workflows** simultaneously (e.g. POA&M approval while waiting for RMF ATO package approval).
- Supports workflow **branches** based on decisions/tasks at specific stages.

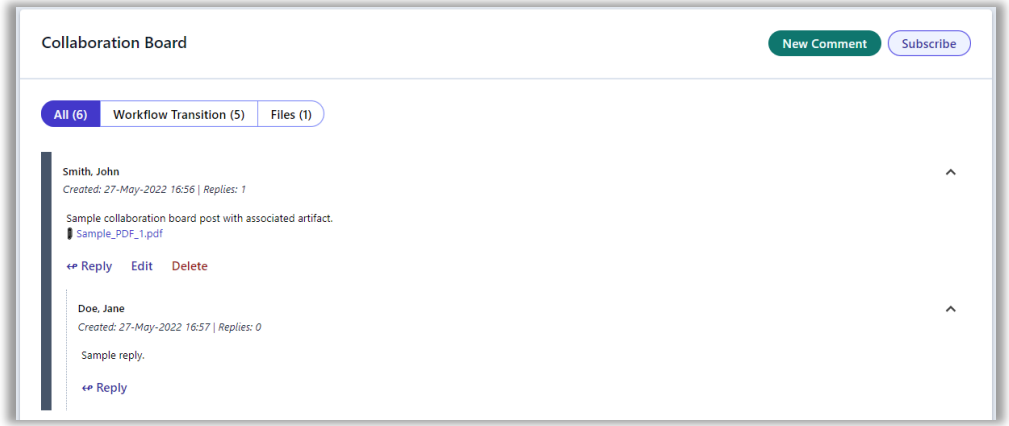
COLLABORATION BOARDS

- Users can post comments, reply, request and attach files throughout the workflows, and subscribe to email updates about posts.

WORKFLOWS DASHBOARD

- All Organizations are provided a workflows dashboard to provide leadership situational awareness of active workflows.
- Dashboard includes drill-down capability to view system information for each system record.





Major Feature: Workflows

ROLES

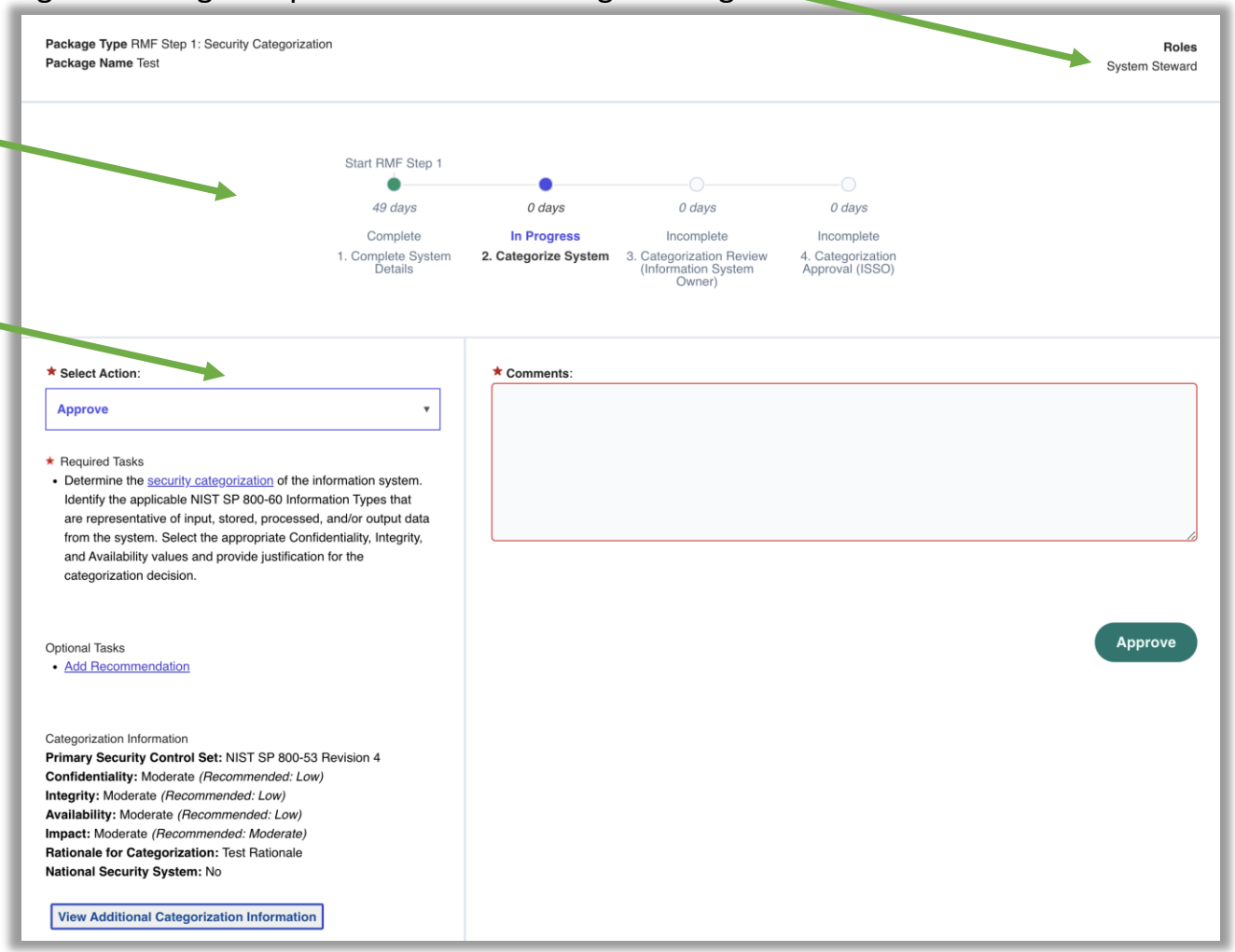
- Workflows support eMASS' package approval chain roles assigned to Stages to perform actions during the stage.

STAGES

- Steps for Workflows can be defined by organizations

TASKS

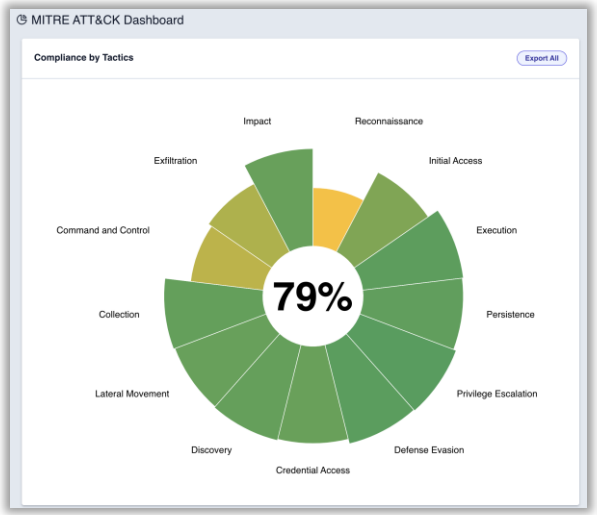
- Ability to show required actions for the assigned personnel to complete or to show information for the reviewer.
- Tasks can link directly to the page in eMASS to perform the action.

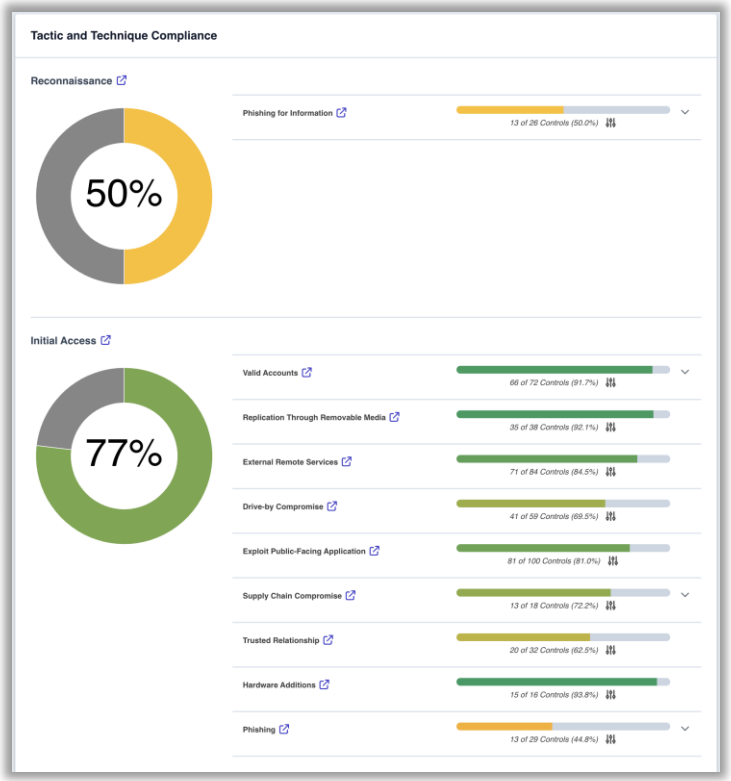


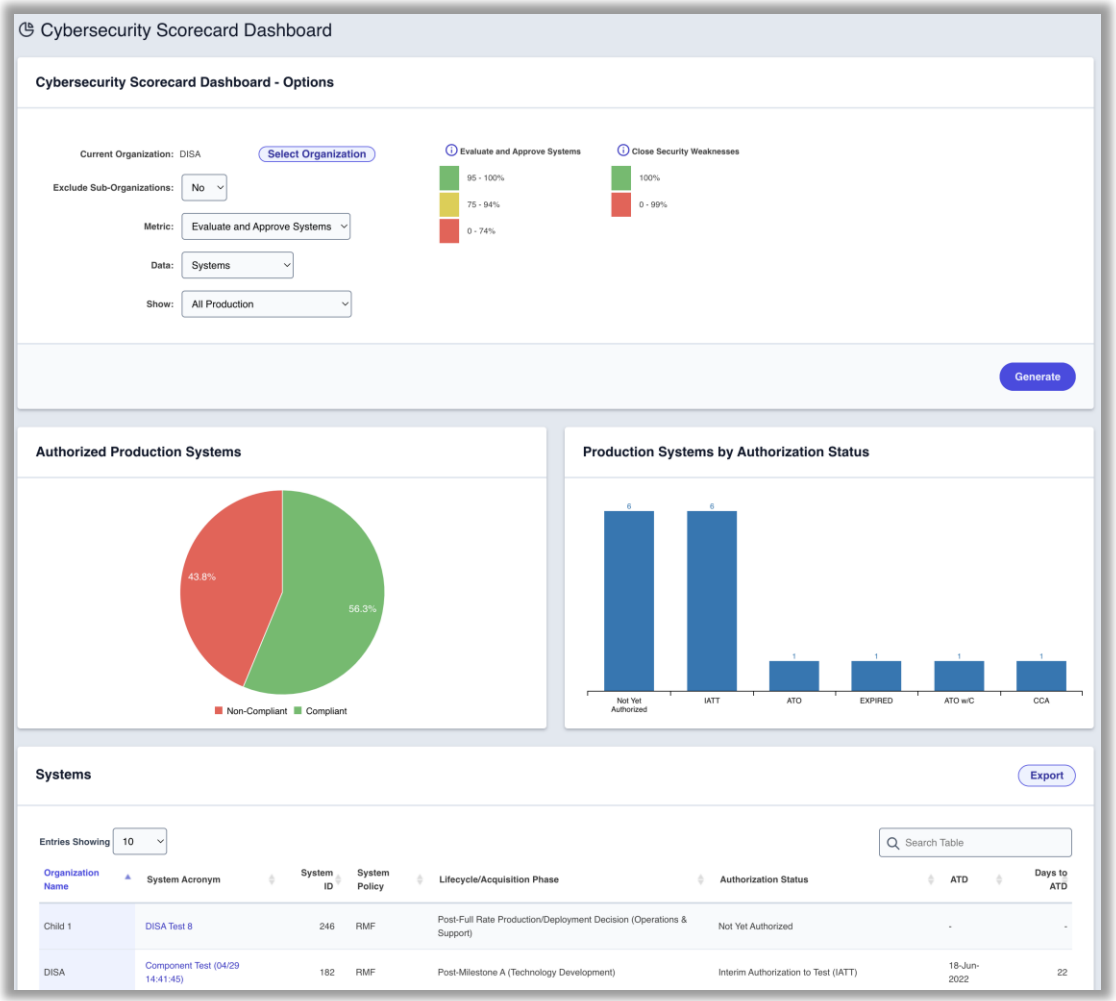
Major Features: Dashboards

DASHBOARDS

- Ability to build and deploy Dashboards, including visualizations, metrics, drilldowns, tabular displays/exports.
- Ability for data sets maintained in eMASS and calculated/roll-ups made available through API or export to an organization's reporting tools.



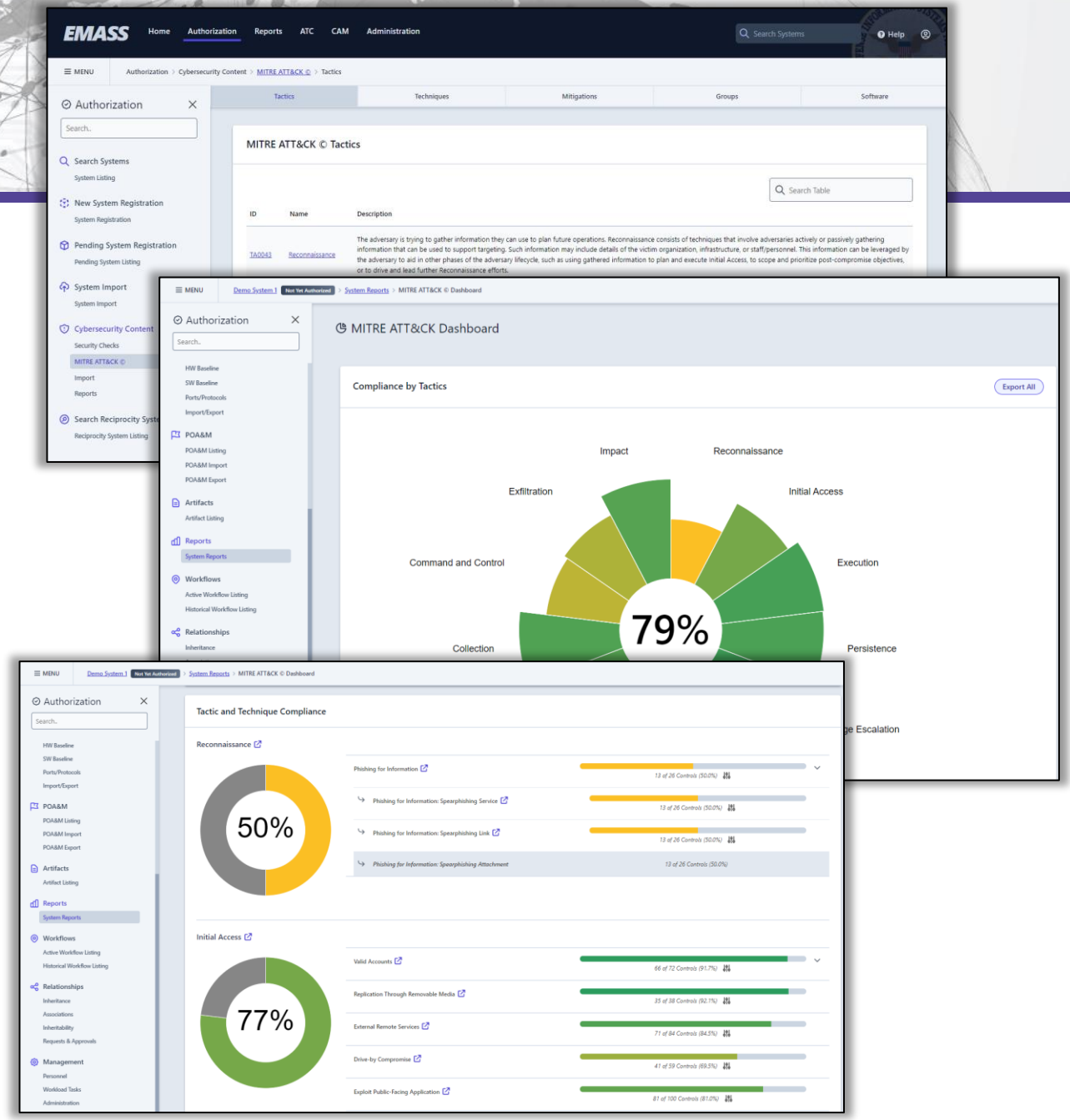




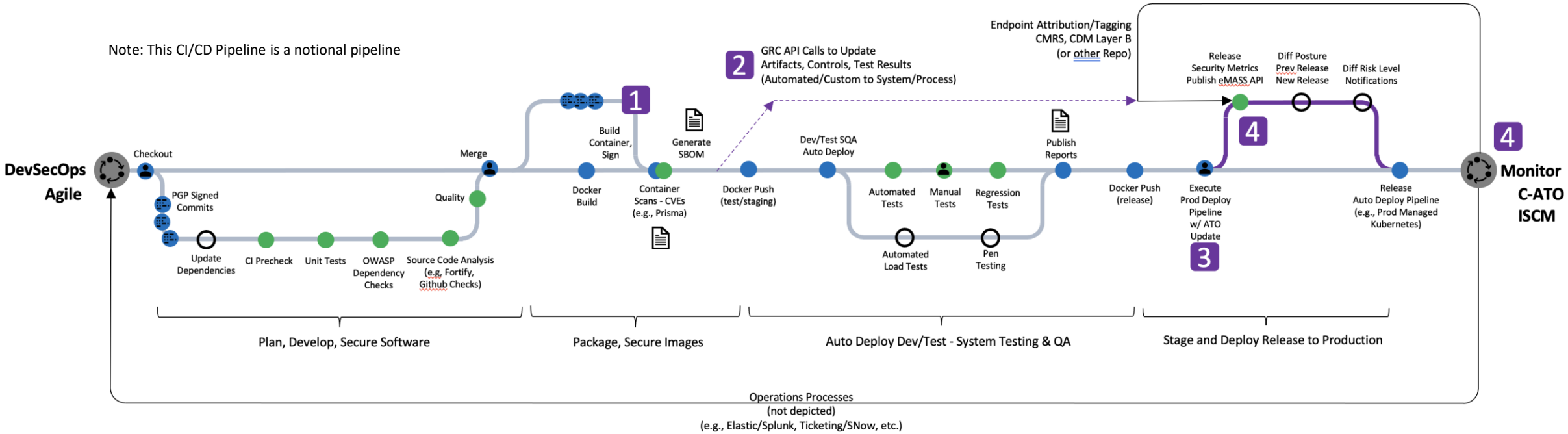
MITRE ATT&CK® FRAMEWORK

- eMASS launched MITRE ATT&CK framework library in Cybersecurity Content in v5.10. Requires System Profile creation/publish by eMASS System Admin with selected MITRE ATT&CK techniques and tactics followed by selection of profile by System Owners.

- Capability provides familiarity with external threat actor techniques and tactics against which Security Controls mitigate, real-world ATPs, visibility within Control Details.



Pipeline for Integrated DevSecOps and RMF



1 Pipeline leverages automated source code analysis & vulnerability scanning
(e.g., Fortify & Github Checks; Prisma Cloud/Container image scanning for CVEs, etc.).

2 Pipeline [optionally] pushes and update RMF Artifacts, Test Results, and change Controls to eMASS Web Service API
(providing flexibility/choice on what that System's CI/CD uses).

3 Deployment Pipeline provides a automatic "Release" checkpoint to eMASS Web Service API with standardized set of metrics and required scan results.
(e.g., from minimally required top level metrics (or to source code & container CVE results)).

4 eMASS provides metrics, data trends to the SCA/AO enabling high level difference between production deployment of components (e.g., releases).

5 "Ops" Continues with automation, monitoring, and Enterprise required endpoint & vulnerability scanning tools in production environments.

eMASS & CMRS, CDM Layer B (or other repo) using tagging maintain System's sensor visibility and metrics trends for the ISSM/ISSO, SCA, AO.

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil /USDISA @USDISA

Trust in DISA:
Mission first, people always