

# Enterprise Mission Assurance Support Service (eMASS)



# 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).

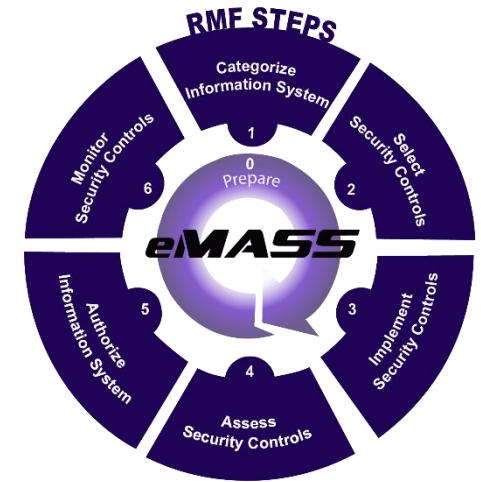


Generation of standardized RMF Reports, Digital Signatures on PDFs, Dashboards and metrics roll-ups, and automated reporting for Enterprise requirements (e.g. DoD CIO for RMF data calls).



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

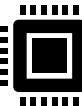
36,000+ (35 day active)

**60**



### Organizations

**22.8K**



### Systems

80,000+ (incl. decom)

**300K**

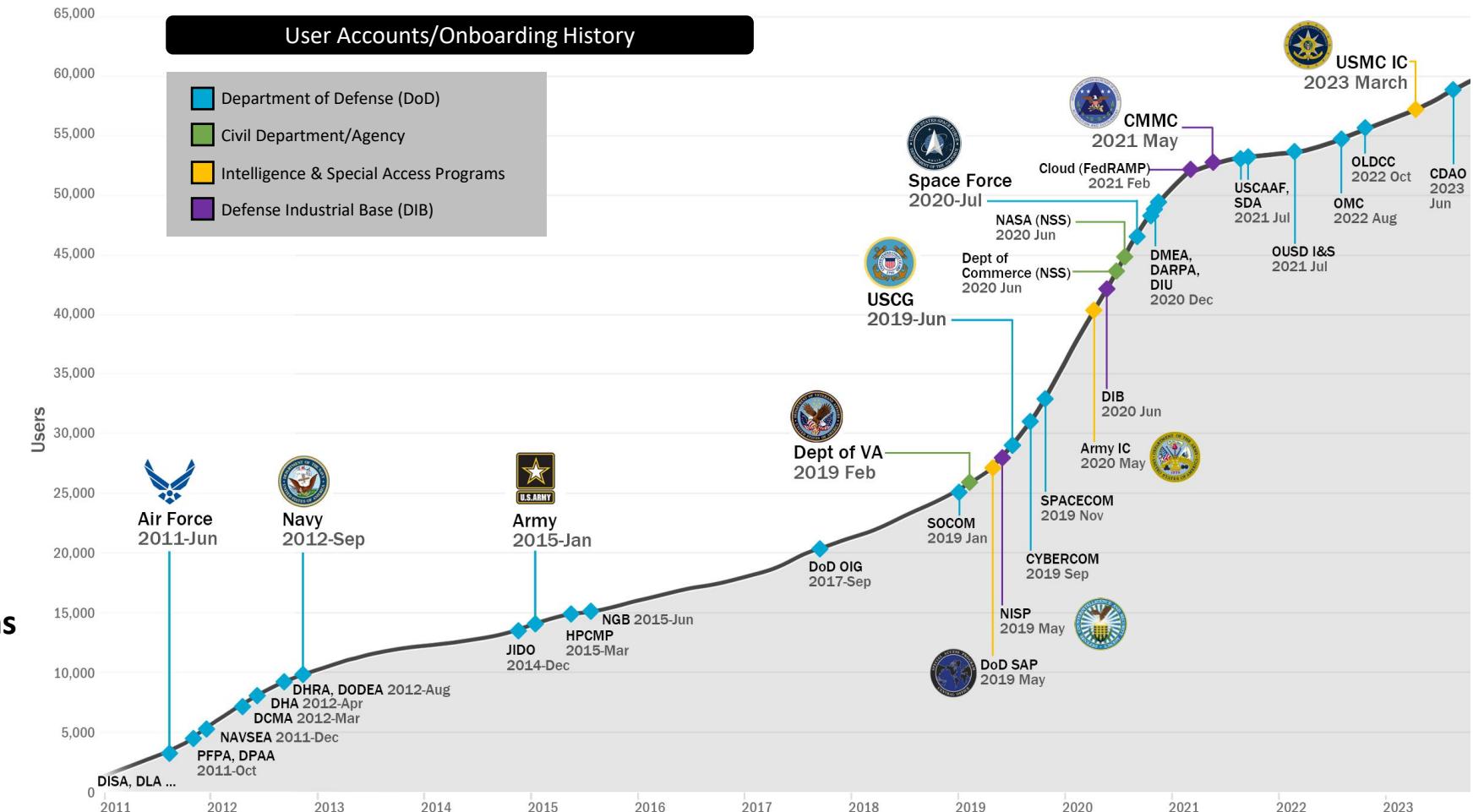


### Authorization Packages/Decisions

**200+**



### New Features Annually



Unclassified, Agency, NIPR

DoD, Veterans Affairs, CSPs & Industry Programs

SIPR

DoD and Civil Agencies with NSS

JWICS

Army IC, Marine Corps IC

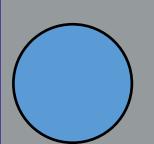
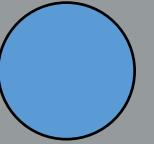
SAP

SAP CIO Community

# Mission Support

DoD RMF	Civil RMF	IC/SAP RMF	Other Risk Mgmt/Certifications
 <p>DoDI 8510.01 RMF</p>  <p>SP 800-53, SP 800-37, SP 800-30, SP 800-137, FIPS 199,...</p>  <p>CNSSI 1253</p> <ul style="list-style-type: none"> <li>Army, Air Force, Navy, Coast Guard, Space Force</li> <li>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&amp;S, OUSD P&amp;R, USD-P, OUSD I&amp;S), USCAF, IWTSD, OMC, SDA</li> </ul>	 <p>VA Directive 6500</p>  <p>SP 800-53B</p> <ul style="list-style-type: none"> <li>Veterans Affairs</li> <li>Dept. of Commerce (NSS)</li> <li>NASA (NSS)</li> </ul>	 <p>IC IT Systems Security Risk Mgmt</p>  <p>Joint SAP Implementation Guide (JSIG)</p> <ul style="list-style-type: none"> <li>DoD SAP CIO Community</li> <li>Army Intelligence Community</li> </ul>	 <p>NISP (DoD 5220.22-M)</p>  <p>CMMC</p>  <p>FedRAMP</p> <p>FISMA</p> <ul style="list-style-type: none"> <li>National Industrial Security Program (NISP)</li> <li>JFHQ-DoDIN's CSSP Evaluator Scoring Metrics</li> <li>Cloud (FedRAMP DoD Provisional Authorizations)</li> <li>Defense Industrial Base (NIST SP 800-171)</li> <li>Cybersecurity Maturity Model Certification (CMMC)</li> </ul>  <p>CSSP CSF ESM v10</p>

# Services Summary

Service Area	Description	Standard Model
 <b>Managed System</b>	<ul style="list-style-type: none"> <li>System provided software-as-a-service (SaaS) including infrastructure hosting costs, software licenses, hosting operations &amp; maintenance, A&amp;A maintenance (ATO), etc; or managed Deployed.</li> <li>Currently Unclassified/NIPR (DISA hosted), SIPR (DISA hosted), Special Access Programs (DoD/SAP CIO hosted), JWICS (Army hosted).</li> </ul>	 <p>DoD RMF Technical Advisory Group (TAG)</p>  <p>Agency TAG, Organization</p>
 <b>Instructor-Led Training</b>	<ul style="list-style-type: none"> <li>Instructor-led training for 30-60 students per class (virtual, at your location, or DC Metro region).</li> <li>DoD/generic flavor training curriculum (and workbook/hands-on modules designed).</li> <li>Hands-on modules and training environment (brought to your location or online sandbox with virtual events).</li> </ul>	<p>↑</p> <p>Responds to RMF TAG/Enterprise &amp; Organization/Agency changes in implementation guidance</p>
 <b>Help Desk &amp; Enterprise Support</b>	<ul style="list-style-type: none"> <li>Help desk support to answer end-user questions related to eMASS usage, RMF policy, technical issue troubleshooting, etc.</li> <li>Customer requests such as data analysis, metrics queries, subject matter expertise &amp; recommendations.</li> <li>Enterprise support for Continuous Monitoring implementations, API integrations, etc.</li> </ul>	 <p>eMASS Joint-Stakeholder Configuration Control Board</p> 
 <b>Enhancements, Customizations</b>	<ul style="list-style-type: none"> <li>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.).</li> </ul>	<p>↑</p> <p>Organization/Agency (optionally) joins the eMASS CCB to drive methodology</p>
 <b>Community Collaboration</b>	<ul style="list-style-type: none"> <li>Ensure enhancements/efficiencies funded/executed by one Component/Agency beneficial for the community is made available to all eMASS users.</li> <li>Collaborate with RMF TAGs &amp; eMASS Configuration Control Board (CCB) for Community-wide execution of major automation/implementation guidance.</li> <li>(SaaS-only) Automation between eMASS-using Components/Agencies (Inheritance across all, Reciprocity, etc.) for those with a common Control Set.</li> </ul>	 <p>eMASS workstream supports Agency's AO/RMF/Policy &amp; Implementation organization for execution of <u>their own requirements per Agency's direction and priorities</u>.</p>

# 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.

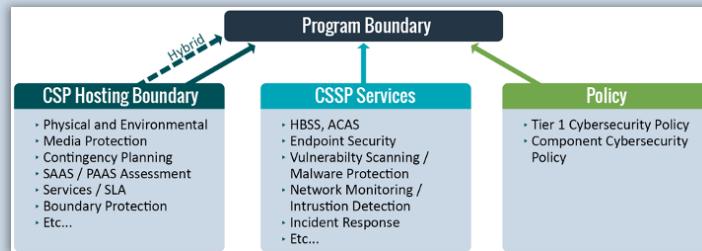
## POCS

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



## Web Service API

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

API Client Registration

POST /register

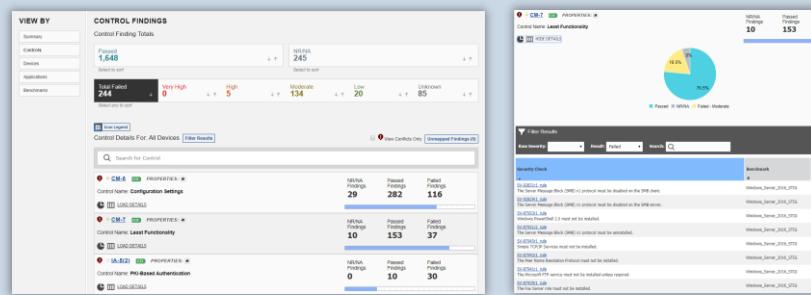
Allows user to register their certificate in order to obtain an API key

## Workflows

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

## Assets w/ Continuous Monitoring

Automated end-to-end 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.



Systems

GET /systems

Get system information

GET /systems/{systemId}

Get system by id

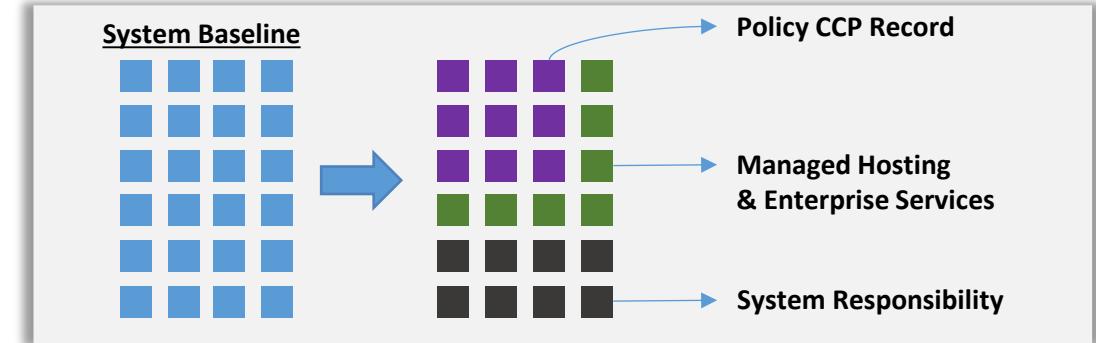


Name	Host	Benchmark (From scan)	Scan Type	Last Scan Date	Scan Result
CC TESTSYSTEM (Default)	DC1.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS
COMMANDCONTROLLER.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
SERVICECONTROLLER.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
DATABASE1.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
DATABASE2.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
DATABASE3.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
DATABASE4.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	FAIL	
WEB1.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
WEB2.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
WEB3.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	
WEB4.TESTSYSTEM2	Windows_Server_2016_STIG	CDSS API	13-Dec-2019	PASS	

# Inheritance

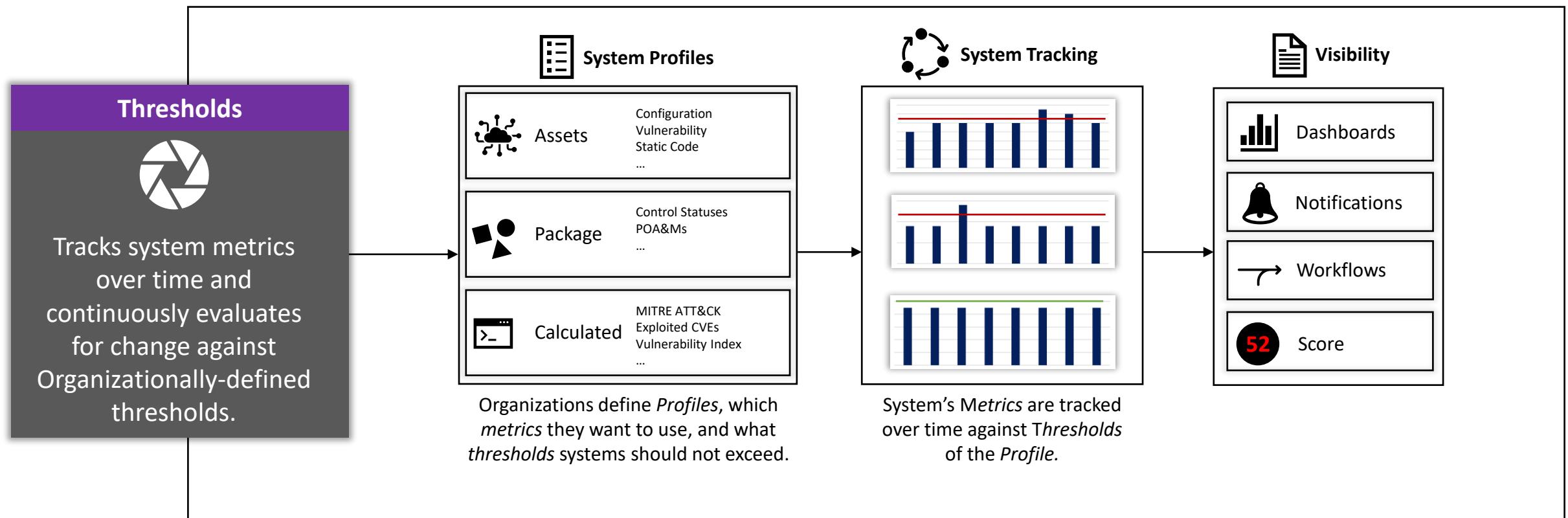
## INHERITANCE AUTOMATION

- 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.
- **Tiered:** 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.



# 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](mailto:disa.meade.id.mbx.emass-tier-iii-support@mail.mil) for additional information.

**eMASS** <https://localhost:9091/api/developer/docs/v1>  [Explore](#)

### eMASS API Version 1.0

Created by Defense Information Systems Agency (DISA)  
See more at <http://www.disa.mil/Cybersecurity/Assessments-and-Inspections/EMASS>

Test Connection		
<a href="#">Show/Hide</a>   <a href="#">List Operations</a>   <a href="#">Expand Operations</a>		
<b>API Client Registration</b>	<a href="#">POST</a> <a href="#">/register</a>	Allows user to register their certificate in order to obtain an API key
<b>Artifacts</b>	<a href="#">DELETE</a> <a href="#">/systems/{systemId}/artifacts</a>	Remove one or many artifacts in a system
	<a href="#">GET</a> <a href="#">/systems/{systemId}/artifacts</a>	Get one or many artifacts in a system
	<a href="#">POST</a> <a href="#">/systems/{systemId}/artifacts</a>	Add one or many artifacts in a system
	<a href="#">PUT</a> <a href="#">/systems/{systemId}/artifacts</a>	Update one or many artifacts in system
	<a href="#">GET</a> <a href="#">/systems/{systemId}/artifactexport</a>	Get the file of an artifact in system
<b>Controls</b>	<a href="#">GET</a> <a href="#">/systems/{systemId}/controls</a>	Get control information in a system for one or many controls
	<a href="#">PUT</a> <a href="#">/systems/{systemId}/controls</a>	Update control information in a system for one or many controls
<b>Plan of Action and Milestones</b>	<a href="#">Show/Hide</a>   <a href="#">List Operations</a>   <a href="#">Expand Operations</a>	
<b>Systems</b>	<a href="#">GET</a> <a href="#">/systems</a>	Get system information
	<a href="#">GET</a> <a href="#">/systems/{systemId}</a>	Get system by id
<b>Test Results</b>	<a href="#">Show/Hide</a>   <a href="#">List Operations</a>   <a href="#">Expand Operations</a>	
<b>Workflow Approval</b>	<a href="#">Show/Hide</a>   <a href="#">List Operations</a>   <a href="#">Expand Operations</a>	

# Major Features: Assets

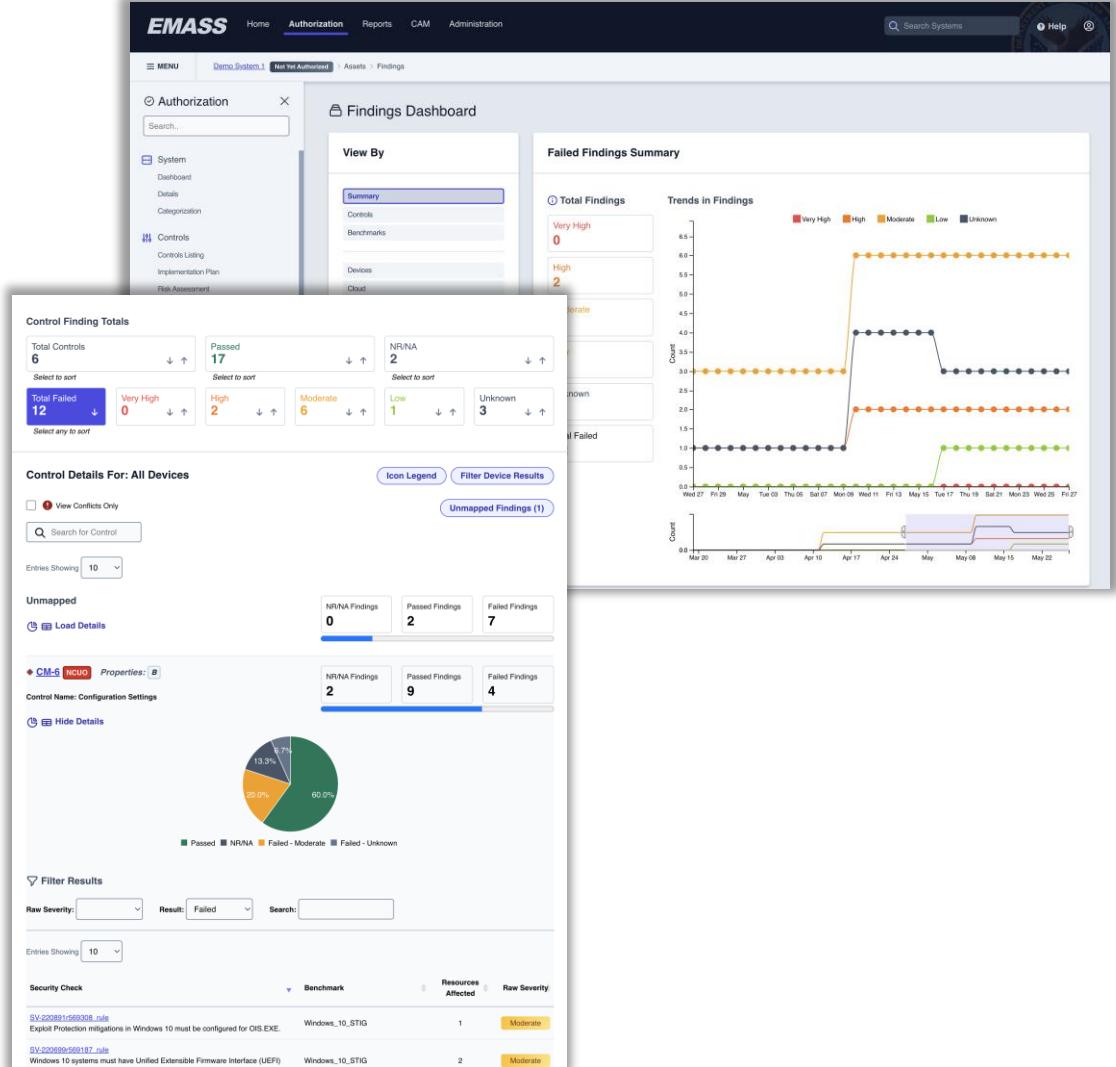
## CORE CAPABILITY

- 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.

Package Type RMF Step 4-5: Assess & Authorize  
Package Name Sample High Risk Escalation  
Roles PM/ISO

Start RMF Step 4  
0 days  
Complete 1. Security Control Assessment - CAC Step 1  
0 days  
Complete 2. Assess - CAC Step 2 - Review and Submit  
0 days  
Complete 3. SCAL Concurrence  
0 days  
End RMF Step 4  
31 days  
Escalated to High Risk  
In Progress  
5. PM/ISO Review (HRE)  
6. Echelon II Review (HRE)  
7. SCA Review (HRE)  
0 days  
0 days  
Incomplete  
Incomplete

\* Select Action: Approve  
\* Required Tasks: Review and select the appropriate action.  
Optional Tasks: Add Recommendation  
\* Comments:  
Updates to System  
Approve

Collaboration Board  
All (6) Workflow Transition (5) Files (1)  
New Comment Subscribe

Smith, John  
Created: 27-May-2022 16:56 | Replies: 1  
Sample collaboration board post with associated artifact.  
Sample\_PDF\_1.pdf  
Reply Edit Delete

Doe, Jane  
Created: 27-May-2022 16:57 | Replies: 0  
Sample reply.  
Reply

# 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.

Package Type RMF Step 1: Security Categorization  
Package Name Test

Start RMF Step 1  
49 days

Complete System Details  
0 days

**In Progress**

2. Categorize System  
3. Categorization Review (Information System Owner)  
4. Categorization Approval (ISSO)

Roles  
System Steward

Select Action:  
Approve

Comments:

Required Tasks

- Determine the [security categorization](#) of the information system. Identify the applicable NIST SP 800-60 Information Types that are representative of input, stored, processed, and/or output data from the system. Select the appropriate Confidentiality, Integrity, and Availability values and provide justification for the categorization decision.

Optional Tasks

- [Add Recommendation](#)

Categorization Information

Primary Security Control Set: NIST SP 800-53 Revision 4

Confidentiality: Moderate (Recommended: Low)

Integrity: Moderate (Recommended: Low)

Availability: Moderate (Recommended: Low)

Impact: Moderate (Recommended: Moderate)

Rationale for Categorization: Test Rationale

National Security System: No

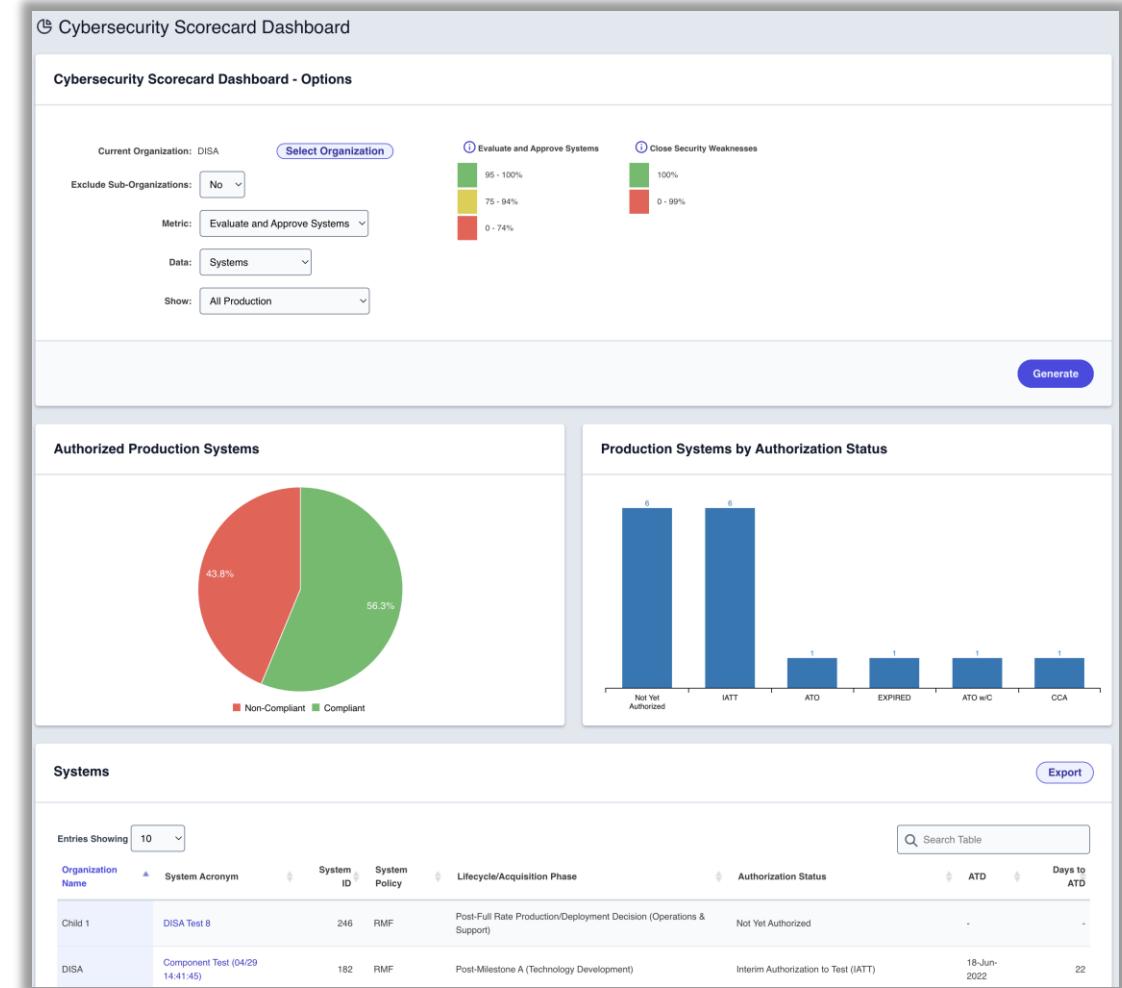
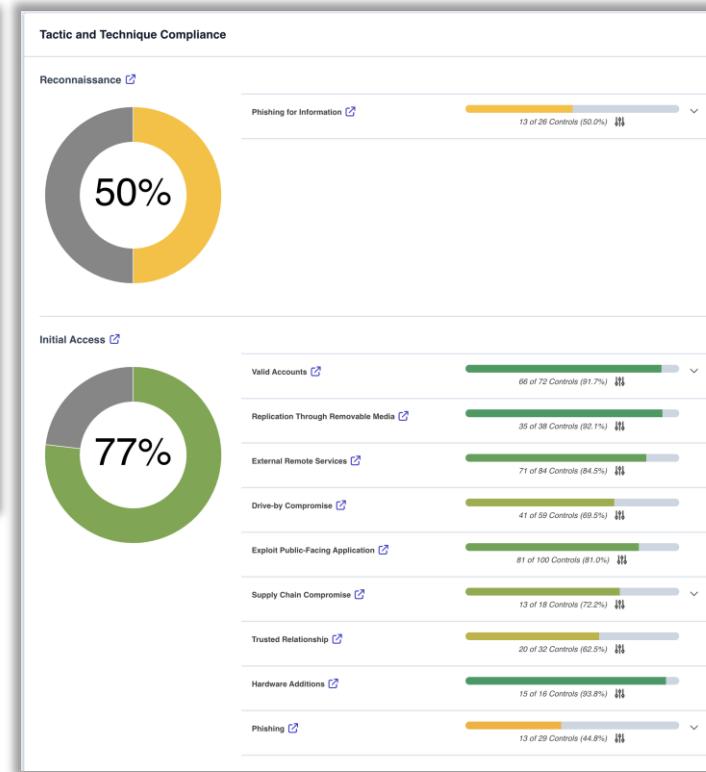
View Additional Categorization Information

Approve

# 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.

The image shows the eMASS (Enterprise Management and Administration System) interface. The top navigation bar includes 'Home', 'Authorization', 'Reports', 'ATC', 'CAM', and 'Administration'. A search bar and help links are also present. The main content area is divided into two main sections: 'MITRE ATT&CK © Tactics' and 'MITRE ATT&CK Dashboard'.

**MITRE ATT&CK © Tactics** (Left Panel):

- Authorization (Search bar, New System Registration, Pending System Registration, System Import, Cybersecurity Content, Security Checks, Import, Reports, Search Reciprocity System).
- System Reports (POA&M, Artifacts, Reports, Workflows, Relationships, Management).

**MITRE ATT&CK © Tactics** (Right Panel):

Table of MITRE ATT&CK © Tactics:

ID	Name	Description
T00043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations. Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

**MITRE ATT&CK Dashboard** (Left Panel):

- Authorization (Search bar, HW Baseline, SW Baseline, Ports/Protocols, Import/Export, POA&M, Artifacts, Reports, Workflows, Relationships, Management).

**MITRE ATT&CK Dashboard** (Right Panel):

**Compliance by Tactics** (Donut Chart): 79%

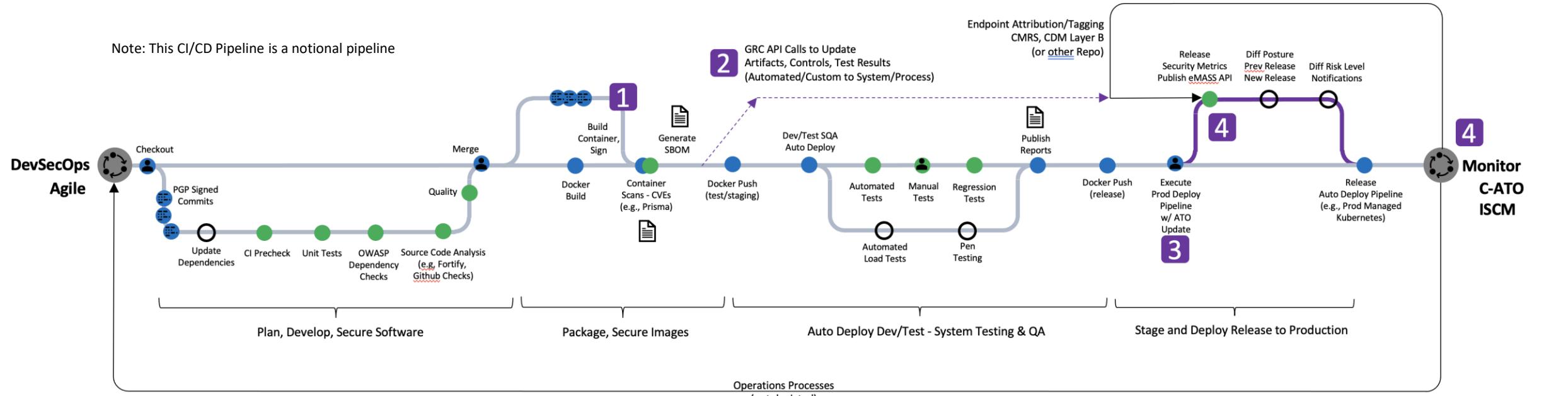
**Tactic and Technique Compliance** (Donut Charts and Bar Charts):

- Reconnaissance: 50%
- Initial Access: 77%
- Execution: 81%
- Persistence: 91.7%
- Privilege Escalation: 92.1%
- Defense Evasion: 84.5%
- Drive-by Compromise: 69.3%
- Exploit Public-Facing Application: 81.0%

Legend for Compliance by Tactics:

- Impact: Red
- Reconnaissance: Orange
- Initial Access: Green
- Execution: Blue
- Persistence: Purple
- Privilege Escalation: Yellow

# Pipeline for Integrated DevSecOps and RMF





 [www.disa.mil](http://www.disa.mil)  [@USDISA](https://www.facebook.com/USDISA)  [@USDISA](https://twitter.com/USDISA)

A large, semi-transparent globe is positioned on the right side of the slide. The globe is rendered in a light gray color and is overlaid with a complex network of thin gray lines and small circular nodes, representing a global communication or data network. The continents of Africa, Europe, and Asia are visible through the network.

Trust in DISA:  
Mission first, people always