

# Capabilities

- Automated report generation, including all required DIACAP, RMF, and applicable Federal Information Security Management Act (FISMA) reports.
- Enterprise-level visibility of all authorization packages offering comprehensive organizational security postures.
- Management of all cybersecurity-compliance activities and automation of the workflow process from system registration through system decommissioning.
- Maintenance of an enterprise baseline for security controls, which is stored in the eMASS repository and updated with industry standards.
- Fully automated inheritance allows systems to inherit security-control statuses, artifacts, test results, and view system-security postures from other combatant commands, services, agencies, or systems.
- Asset Manager allows eMASS to consume outputs from external-vendor scanning tools and map results to information systems.
- Allows product teams, testers, and security-control assessors to effectively collaborate and execute security assessments from geographically dispersed locations with Integrated Project Teams.



## United States Army Europe

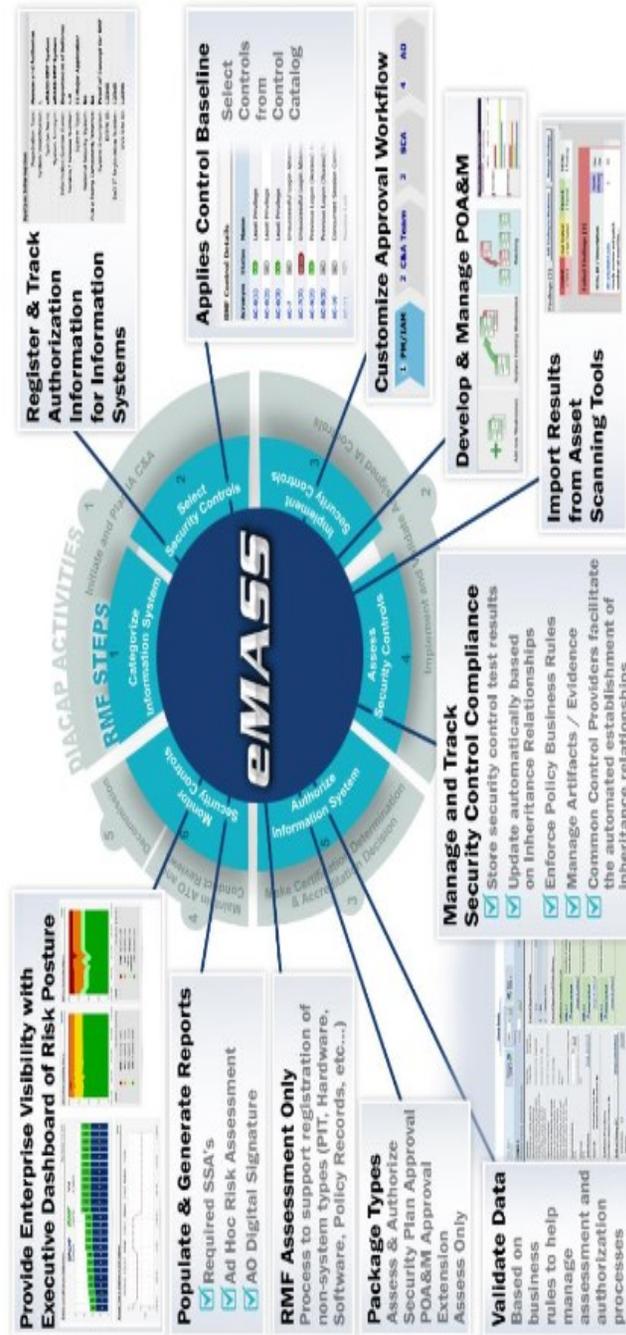
<http://www.eur.army.mil/>

### eMASS Program Managers:

Todd Black & Paul Scandrick  
Policy, Programs, and Training Branch  
USAREUR G6 Cybersecurity Division  
Military 314-537-6172

E-mail:

[todd.f.black.civ@mail.mil](mailto:todd.f.black.civ@mail.mil)  
[paul.e.scandrick.civ@mail.mil](mailto:paul.e.scandrick.civ@mail.mil)



This publication is available at  
<https://aepubs.army.mil>.

## Overview

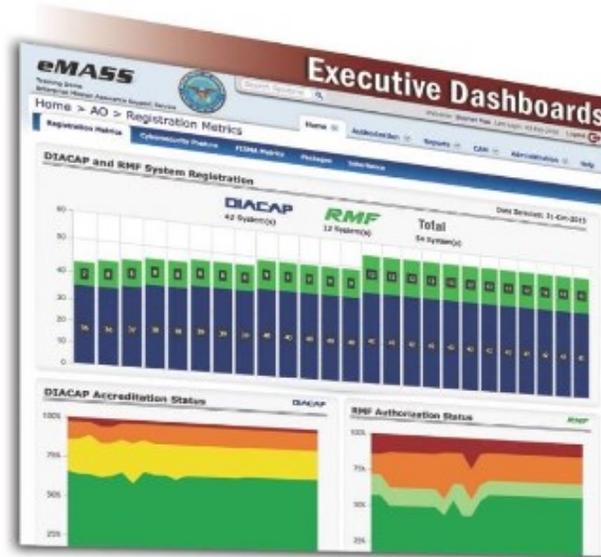
eMASS is a web-based Government off-the-shelf solution that automates a broad range of services for comprehensive, fully integrated cybersecurity management, including controls-scorecard measurement, dashboard reporting, and the generation of a risk-management framework (RMF) for Department of Defense (DOD) information technology (IT) and DOD Information Assurance Certification and Accreditation Process (DIACAP) package reports. eMASS provides an integrated suite of authorization capabilities and prevents cyber attacks by establishing strict process-control mechanisms for obtaining authority to connect information systems to DOD networks.

## Quick Facts

- Sponsors: DISA jointly with the DOD Chief Information Officer.
- Established at more than 35 combatant commands, services, and agencies.
- Supports more than 22,000 user accounts.
- Seamlessly integrates with enterprise web-enabled security assessment tools.

## eMASS

eMASS empowers the cybersecurity workforce through its control-requirements wizard, intuitive user interface, linear workflows, integrated computer-based training capability, and autogeneration of all security-compliance package reports so that more time can be spent on securing the network than on interpreting the policy. Through improved cyber situational awareness, eMASS enables managers to readily identify vulnerabilities and make decisions concerning cybersecurity resources and program needs. Through its central management and governance of an enterprise's cyber policy, eMASS promotes speedy delivery of policy changes and dramatically improves the cycle time to effect these changes directly down to individual teams.



## eMASS Provides Customers with Unmatched Benefits

- Automates customizable workflow for managing essential security functions at the enterprise level down to system-control activities.
- Supports reciprocity by providing a common operating picture and a simplified enterprise-architecture environment to facilitate information exchange and dynamic connection decisions.
- Speeds the delivery of systems supporting critical enterprise infrastructure, the warfighter, and other protective-service entities by streamlining the RMF assessment, authorization, and connection-approval processes.
- Enables enterprise reporting and efficiencies through automatic generation of all required security-compliance package reports, seamless integration with security scanning tools, and robust custom reporting capabilities.
- Eliminates variable costs such as vendor licensing fees, payments for software updates, and escalating operations and maintenance costs.
- Centralizes the management of cybersecurity activities and offers system-security practitioners the flexibility to manage artifacts, establish and monitor inheritance relationships, and collaborate on security-compliance development.
- Rapidly responds to requests for deployment of RMF policy enhancements (overlays and assess-only process).