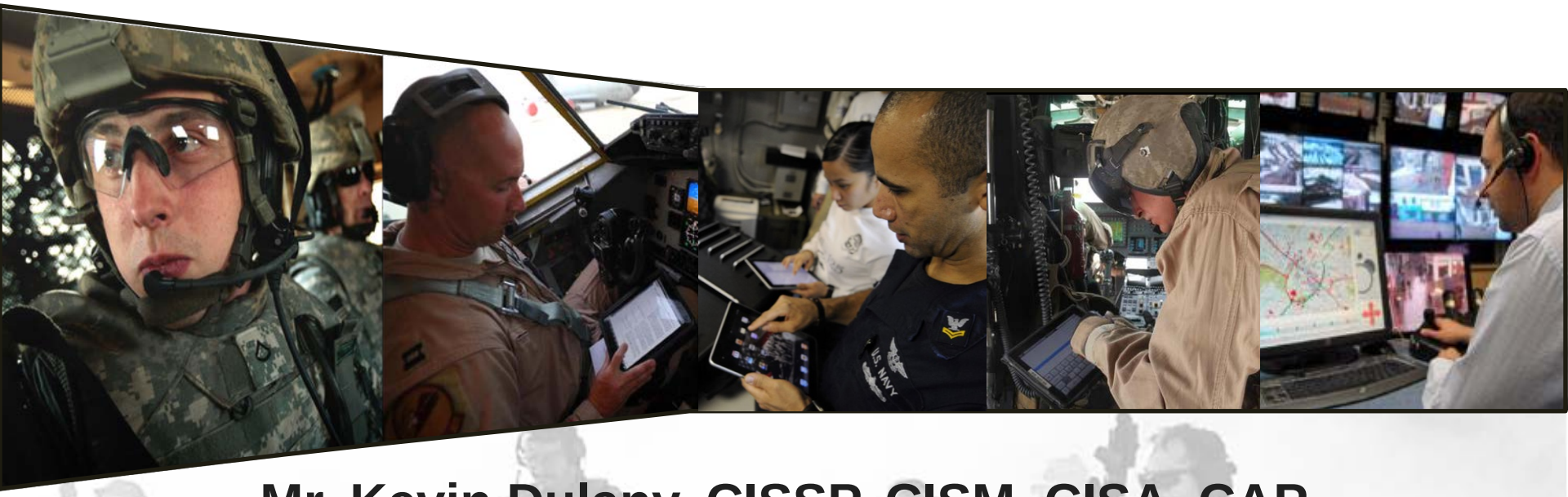
How to Apply the Risk Management Framework to Control Systems within DoD



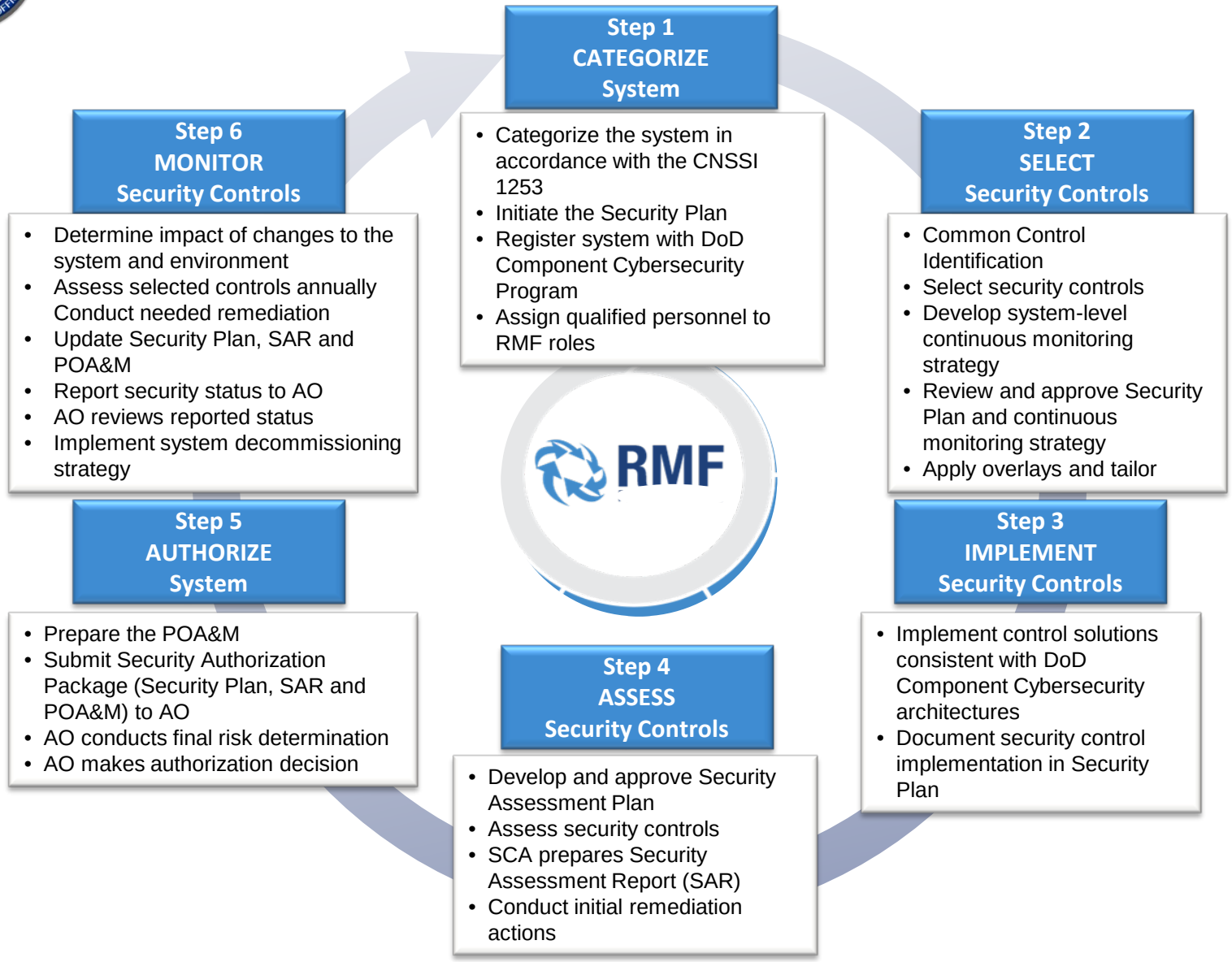
Mr. Kevin Dulany, CISSP, CISM, CISA, CAP

Chair, RMF TAG, Department of Defense (DOD) Chief Information Officer (CIO)
Deputy CIO for Cybersecurity
Cybersecurity Policy & Strategy Directorate

DoDI 8510.01 "RMF for DoD IT"

- Incorporates cybersecurity early and robustly in the acquisition and system development lifecycle
- Implements a three-tiered approach to risk management that addresses risk-related concerns at the enterprise level, the mission and business process level, and the information system level
- Focuses on risk to the mission and buying down cybersecurity risks through the right mitigations
- Provides a risk management methodology that gives organizations a true picture of vulnerabilities caused by non-compliant controls as it relates to other risk factors (i.e. likelihood, threat, and impact)
- Codifies system authorization reciprocity, enabling organizations to accept approvals by other organizations for interconnection or reuse of IT without retesting
- Emphasizes information security continuous monitoring and timely correction of deficiencies, including active management of vulnerability and incidents
- Applies to all IT which reduces exploitation of vulnerabilities in PIT, Services, or Products previously not secured or assessed

RMF Lifecycle for DoD Information Systems and Platform Information Technology (PIT) Systems



Challenges and Solutions

- **Challenges**:
  - How to assess non-traditional IT
  - Integrating current security requirements and performing a gap analysis

- **Solutions:**
  - Establishment of guidance through the RMF KS (e.g., EI&E PIT Control Systems page)
  - Establishment of focus groups to address: defining the process for DoD IT that is designated as "Assess Only" and cybersecurity of DoD PIT systems

Mr. Kevin M. Dulany
Chief, Risk Management Framework Division
DOD CIO, DCIO(CS), CSPS
Kevin.M.Dulany.civ@mail.mil

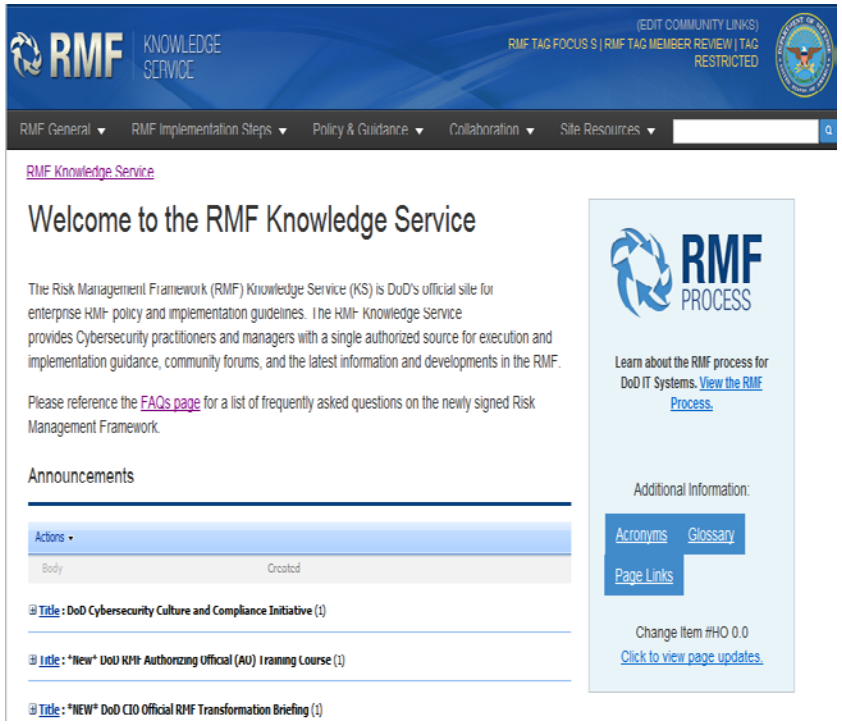
Email RMF Implementation Questions to:

RMF TAG Secretariat (OSD.RMFTAG-Secretariat@mail.mil) or
via the RMF KS Help and Feedback Form (https://rmfks.osd.mil)

BACK-UP

DIACAP / RMF Knowledge Service

The authoritative source for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework



https://rmfks.osd.mil

RMF Technical Advisory Group (RMF TAG)

- Mission: Strengthen and evolve the ability for DoD to rapidly deploy secure IT systems that enable information sharing between the Department, the IC, and other entities.
- Duties:
  - Provide implementation guidance for the RMF
  - Provide detailed analysis and authoring support for the enterprise portion of the Knowledge Service (KS)
  - Recommend changes to security controls, baselines, and RMF policy
  - Advise DoD forums established to resolve RMF priorities and cross-cutting issues
  - Develop and manage RMF automation requirements
- Chair: DoD SISO appointed
- Members: All DoD Components are authorized to be represented by one primary and one alternate cybersecurity SME.