# *Cyber Solutions*
# *Department of the Air Force (DAF)*
# *Risk Management Framework (RMF)*

DAU Cybersecurity Professor: Kelley Kiernan and

Department of the Air Force, Cybersecurity Risk Management Division:  Chief, Trevor Smith

May 23, 2024

DAU

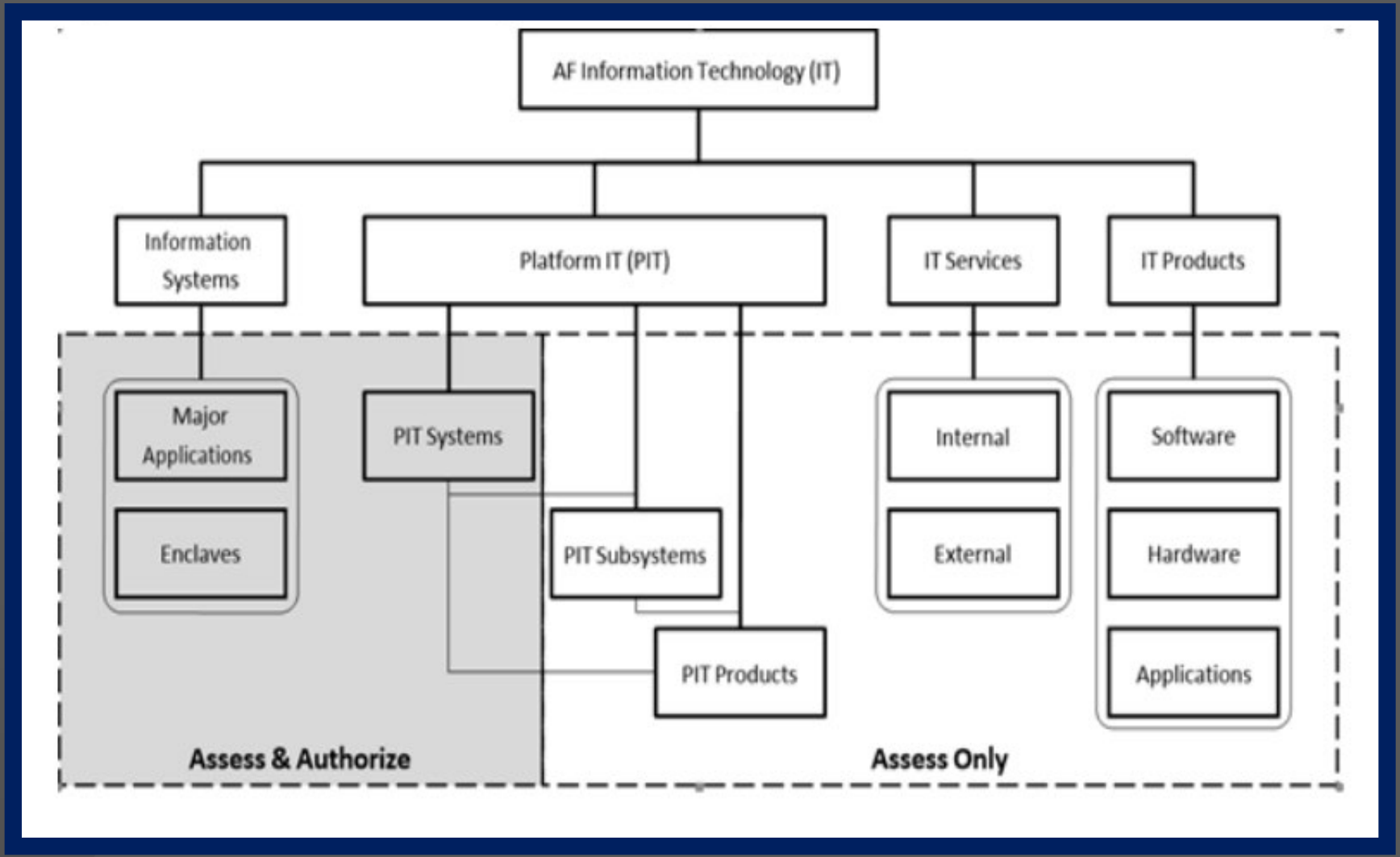
# DAF RMF: Agenda

- Bring: RMF Acumen/Qualified Staff to support your DAF RMF/Cybersecurity Journey
- How to Get Connected at DAF
  - Assess Only
  - Assess and Authorize
- Q&A
- Going Forward
  - Work with your COR/PM to approach your Program
  - COR/PM can email  proper email
  - RMF Training websites

# BRING: RMF Acumen/Qualified Staff

- RMF is the means that the federal government and the DAF use to manage the profound risk of bringing new IT and software into the U.S. Air Force and U.S. Space Force networks.
- When a vendor wants to bring Information Technology (IT ) or Software to the DAF on contract,
  - Organize from your company: fully qualified, RMF practitioner partners for the DAF Authorizing Official's Team to work
  - Engage a cybersecurity professional to support the design and implementation of a cybersecurity program which will:
    - Meet and be responsive to the sophisticated NIST SP 800-53 security controls,
    - Implement a comprehensive architecture compliant with NIST SP 800-53 and
    - Provide a peer interface for the Authorizing Official’s team for the tasks of assessing security and privacy controls as well as establishing control baselines via a discussion of cyber risk.
- If you are the Contracting Officer Representative, or Technical Point of Contact for a SBIR/STTR contract; you should seek advice on the path forward for your contract from your Program Cybersecurity Team or MAJCOM A6.  The RMF is a long, comprehensive process and you should create awareness around your contract ASAP!

# RMF IT Categories



# *Assess Only: PIT Subsystems, PIT Product, IT Services, and IT Products (Hardware, Software, Applications)*

- IT below the system level must be security configured, documented in an assessment package, and reviewed by the appropriate RMF personnel for acceptance/connection
  - IT products, software, and applications must be assessed for supportability, operability, compatibility, and security accomplished via one of the following:
    - Software assessment and evaluation using the DOD RMF KS template
    - Air Force Software and Application Certification Assessment (SACA), testing may be accomplished by the Cyberspace Capabilities Center or by the organization sponsoring the software product. Software products are certified for use on computers running the Standard Desktop Configuration or DoD Server Core Configuration, applications, and approved mobile devices on the AFIN.
    - RMF KS - https://rmfks.osd.mil/rmf/Pages/default.aspx
    - SACA website - https://usaf.dps.mil/teams/ccc/fpu/CZZE_TE_SACA.aspx

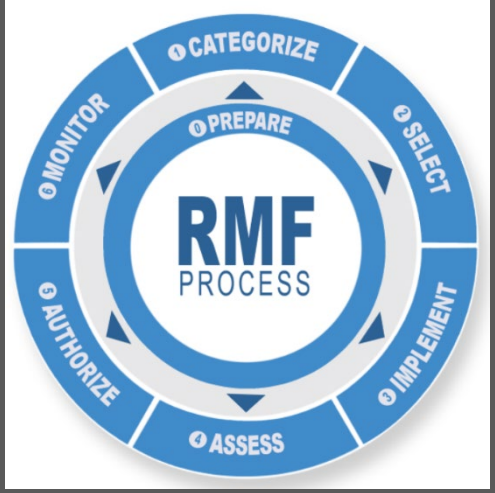
# Assess and Authorize

| Role | Appointed/ Identified By | Rank Minimum | Reference(s) |
|---|---|---|---|
| DAF CIO+ | SecAF (established) | O-9/SES | HAF MD1-26, *Chief Information Officer* |
| DAF CISO | DAF CIO | O-7 / SES | Title 40 United States Code Section 3554; DoDI 8510.01 |
| Mission Area Owner | Identified | O-7 / SES | AFPD 16-14, *Security Enterprise Governance*; DoDI 8510.01 |
| Senior AO*+ | DAF CIO | O-7 / SES | 40 USC §3506; DoDI 8510.01 |
| Subordinate AO*+ | DAF CIO | O-6/GS-15 | 40 USC §3506; DoDI 8510.01 |
| AODR | AO | O-5 / GS-14 | DoDI 8510.01 |
| SCA*+ | DAF CISO | O-4 / GS-13 | 40 USC §3554; DoDI 8510.01 |
| SCAR | SCA | Any | AFI 17-101 |
| PM+ | For programs of record, Service Acquisition Executive (SAE) (as applicable); otherwise, ISO performs duties. | Any government official | DoDI 5000.02 |
| ISO*+ | For programs of record, Service Acquisition Executive (SAE) (as applicable); otherwise, HAF/SAF 3-letter or MAJCOM 2-letter (as applicable) | Any | CNSSI No. 4009 |

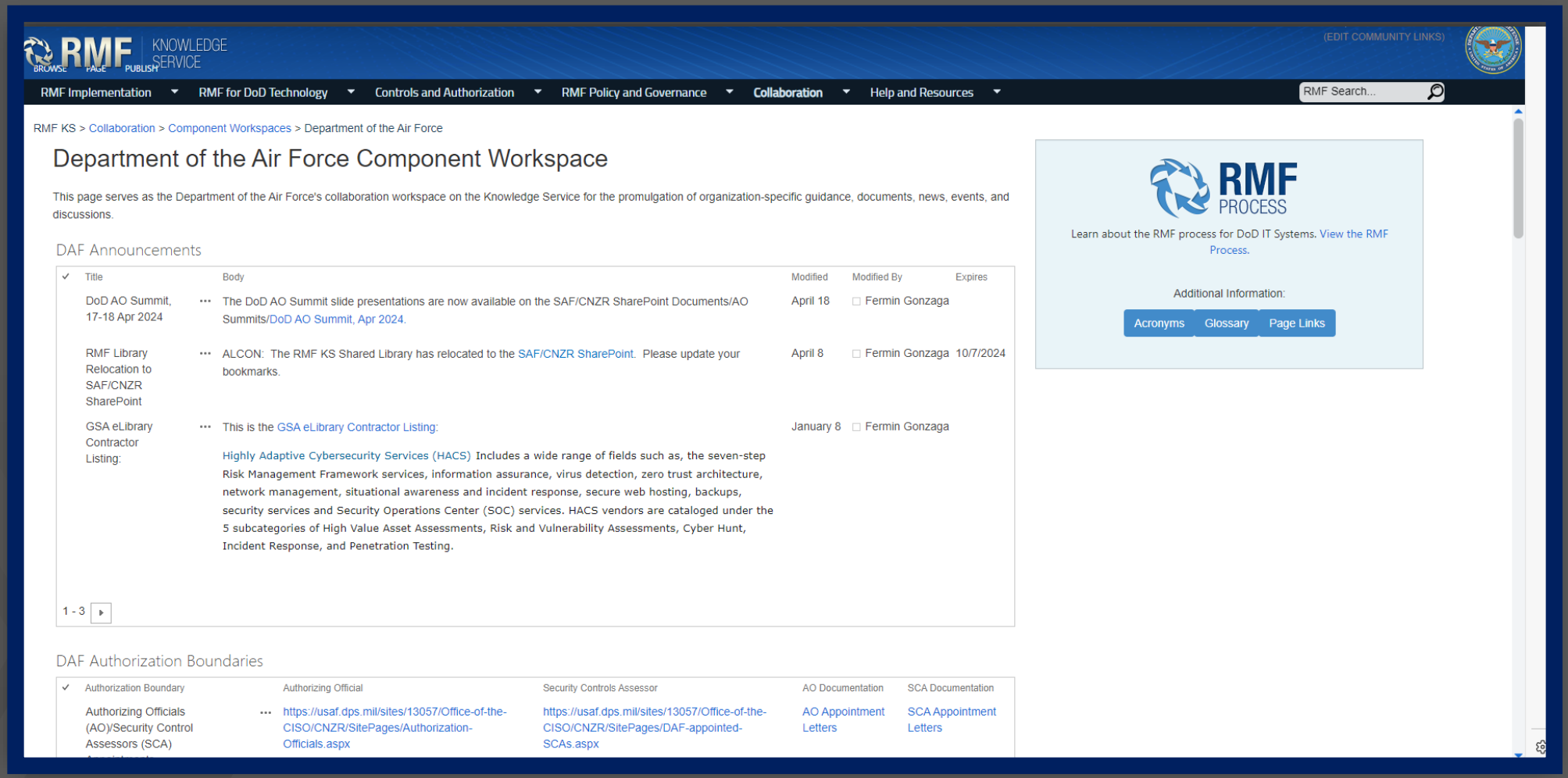
| Role | Appointed/ Identified By | Rank Minimum | Reference(s) |
|---|---|---|---|
| IO/Steward | Identified by the ISSM | Any | DoDI 8500.01, NIST SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* |
| ISSE+ | PM | Any | DoDI 8510.01 |
| ISSM*+ | PM or ISO | Any | DoDI 8510.01 |
| ISSO+ | ISSM | Any | DoDI 8510.01 |
| UR | ISO | Any | DoDI 8510.01 |

**1. * Denotes minimum system-level RMF positions**

**2. + Denotes additional responsibilities and authorities assigned in Attachments**



# For Contractors and COR / COTR / TPOC / PM



# Going Forward

- Going Forward
  - Work with your COR/PM to approach your Program
  - COR/PM can email Kelley.Kiernan@dau.edu

- Cyber Security/Risk Management Framework (RMF) Training
  - DAU - Cyber Security/Risk Mgmt. Framework (RMF)
    - VideoURL https://media.dau.edu/media/0_k1b5q0y9
    - LINK https://www.dau.edu/courses/isa-220
    - LINK https://www.dau.edu/courses/wss-003
  - NIST Four RMF Classes https://csrc.nist.gov/projects/risk-management
  - Center for Development of Security Excellence (CDSE)
    - CDSE Seven RMF Classes https://www.cdse.edu/Training/eLearning/
  - RMF Knowledge Service, RFM Implementation, CAC required, RMF KS portal at: https://rmfks.osd.mil/rmf/Pages/default.aspx