Unpacking the Authority to Operate (ATO) Process:
Implications for the DoD

Presenter:
Capt Grant Wilson, USAF Contracting Officer

Study Conducted By:
2024 NPS Air Force Element Cohort

Study Sponsored By:
SAF/CNDI (CIO Office)

Advisors:
Lt Col Daniel Finkenstadt, PhD
Lt Col Jamie Porchia, PhD

Background

SAF/CNDA (CIO Office) Presented

NPS with ATO Problem Statement

↓

ATO Process Required under FISMA

2014 and DODD 5144.02

↓

ATO Process Daunting and Complex

↓

Increased Timeline and Decreased

Interest in Business-Government

Actions

ATO
Authority-To-Operate

Research Questions

1. What is the current state of ATO processes, risk management, and authority delegation within the DAF?
2. What are the key decision points, pain points, and stakeholders in the ATO process?
3. How can applying process mapping techniques to visualize the ATO process assist with identifying areas for improvement?
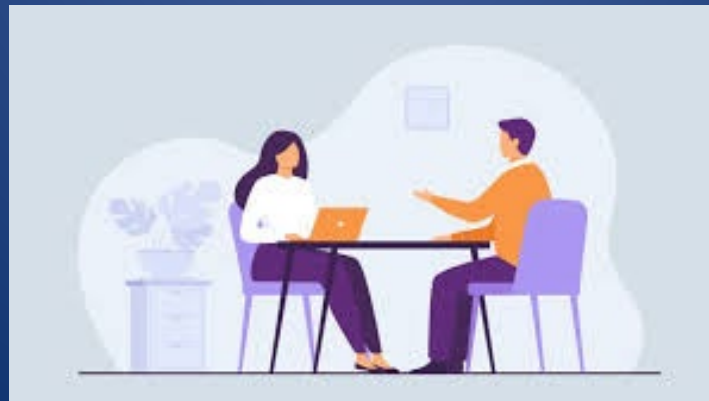
Methodology

- Two-Stage Interview Process

  - Stage 1: Fact Finding and Research Team Synthesis

  - Stage 2: Interviewee Validation

  - Final Report

- Interviewees:

  - 17 key stakeholders were interviewed

    - Military and civilian personnel

    - Cybersecurity experts

    - Program Executive Officers

    - Security Managers

- All opinions presented are those of the interviewees and do not reflect the views of the research team.

Process Flow Chart
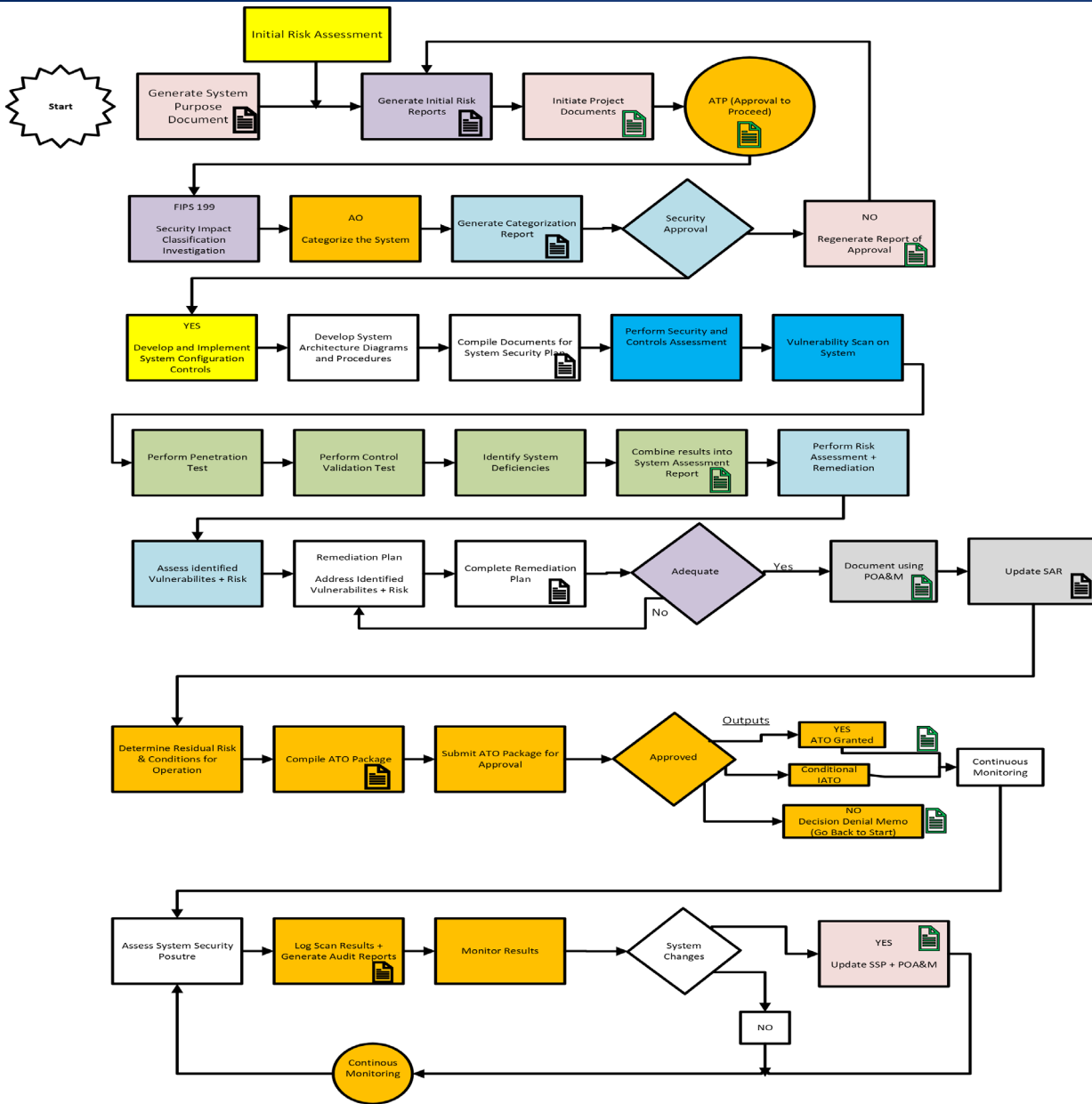
Legend:

Document was Created or Reviewed
Green Icon - Decision and Routing Documents
Black Icon - Documents Generated for Approval

Process or Step in the overall Approvals

Decision Point

Conclusion Point

Flowchart steps:

- Initial Risk Assessment
- Start
- Generate System Purpose Document
- Generate Initial Risk Reports
- Initiate Project Documents
- ATP (Approval to Proceed)
- FIPS 199 Security Impact Classification Investigation
- AO Categorize the System
- Generate Categorization Report
- Security Approval
- NO Regenerate Report of Approval
- YES Develop and Implement System Configuration Controls
- Develop System Architecture Diagrams and Procedures
- Compile Documents for System Security Plan
- Perform Security and Controls Assessment
- Vulnerability Scan on System
- Perform Penetration Test
- Perform Control Validation Test
- Identify System Deficiencies
- Combine results into System Assessment Report
- Perform Risk Assessment + Remediation
- Assess identified Vulnerabilites + Risk
- Remediation Plan / Address Identified Vulnerabilites + Risk
- Complete Remediation Plan
- Adequate
- Yes
- No
- Document using POA&M
- Update SAR
- Determine Residual Risk & Conditions for Operation
- Compile ATO Package
- Submit ATO Package for Approval
- Approved
- Outputs
- YES ATO Granted
- Conditional IATO
- Continuous Monitoring
- NO Decision Denial Memo (Go Back to Start)
- Assess System Security Posutre
- Log Scan Results + Generate Audit Reports
- Monitor Results
- System Changes
- YES Update SSP + POA&M
- NO
- Continous Monitoring

Organization legend:

Peach - System Owner
Orange - Authorizing Official
Blue - Security Managers
Green - Cybersecurity Teams
Yellow - Communications Squadron
No Color - Multiple Organizations
Purple - Configuration Control Boards
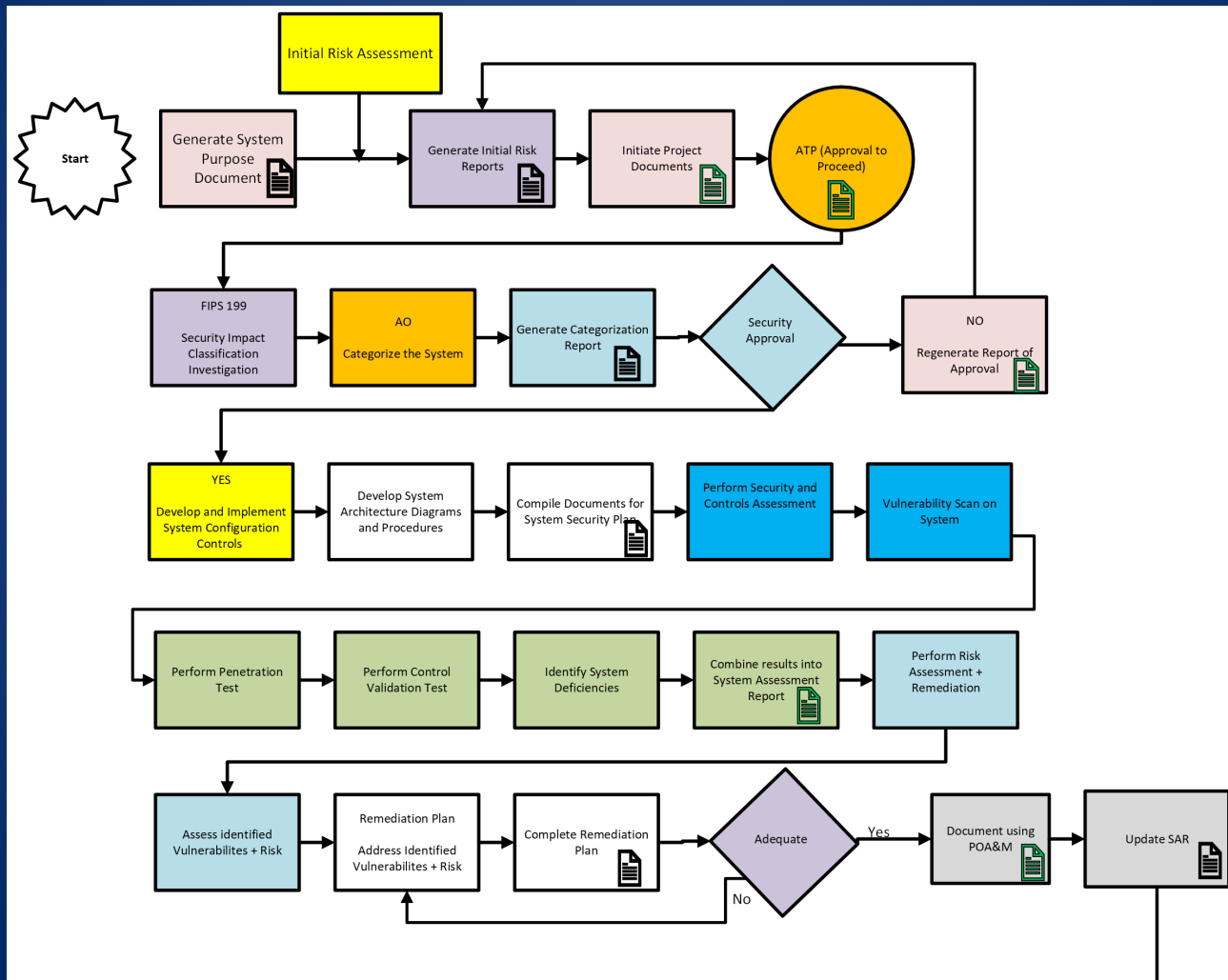**Teal** - Air Force Network Integration Center
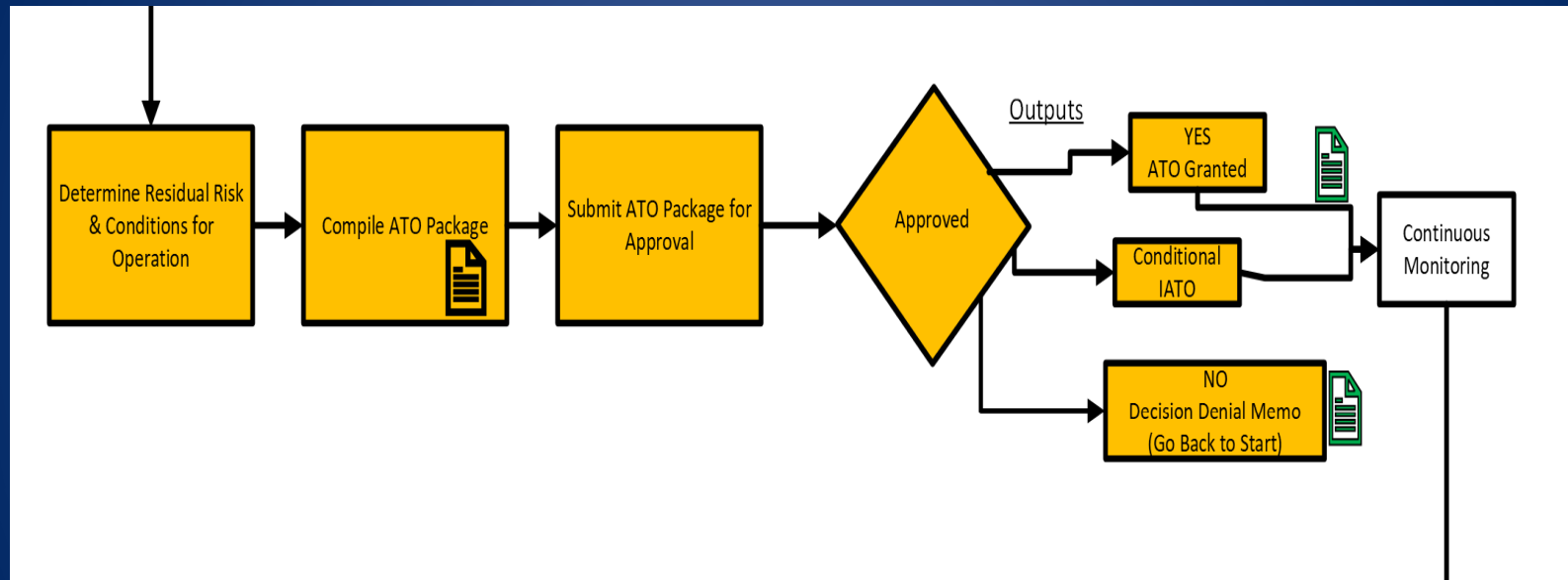**Light Gray** - Program Executive Officers

Phase 1: Categorization
Approx 3wks – 6mos

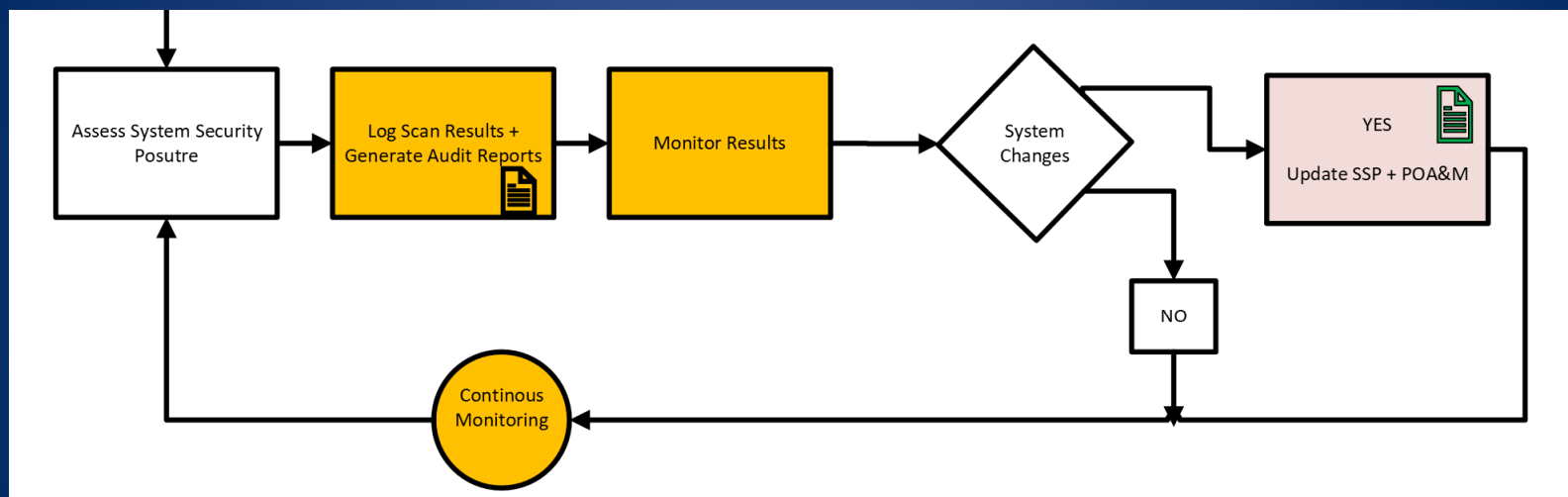# Phase 2: ATO Approval
Approx 1-5 days

Phase 3: Continuous Monitoring
Up to 3 Years

Recommendations

- Implement automation

- Shift to continuous integration for tenant application

- Integrate current security scanning tools

- Shift from administrative controls to technical controls

- Encourage collaboration

- Apply agile methods

- Broader adoption of emerging trends and advancements
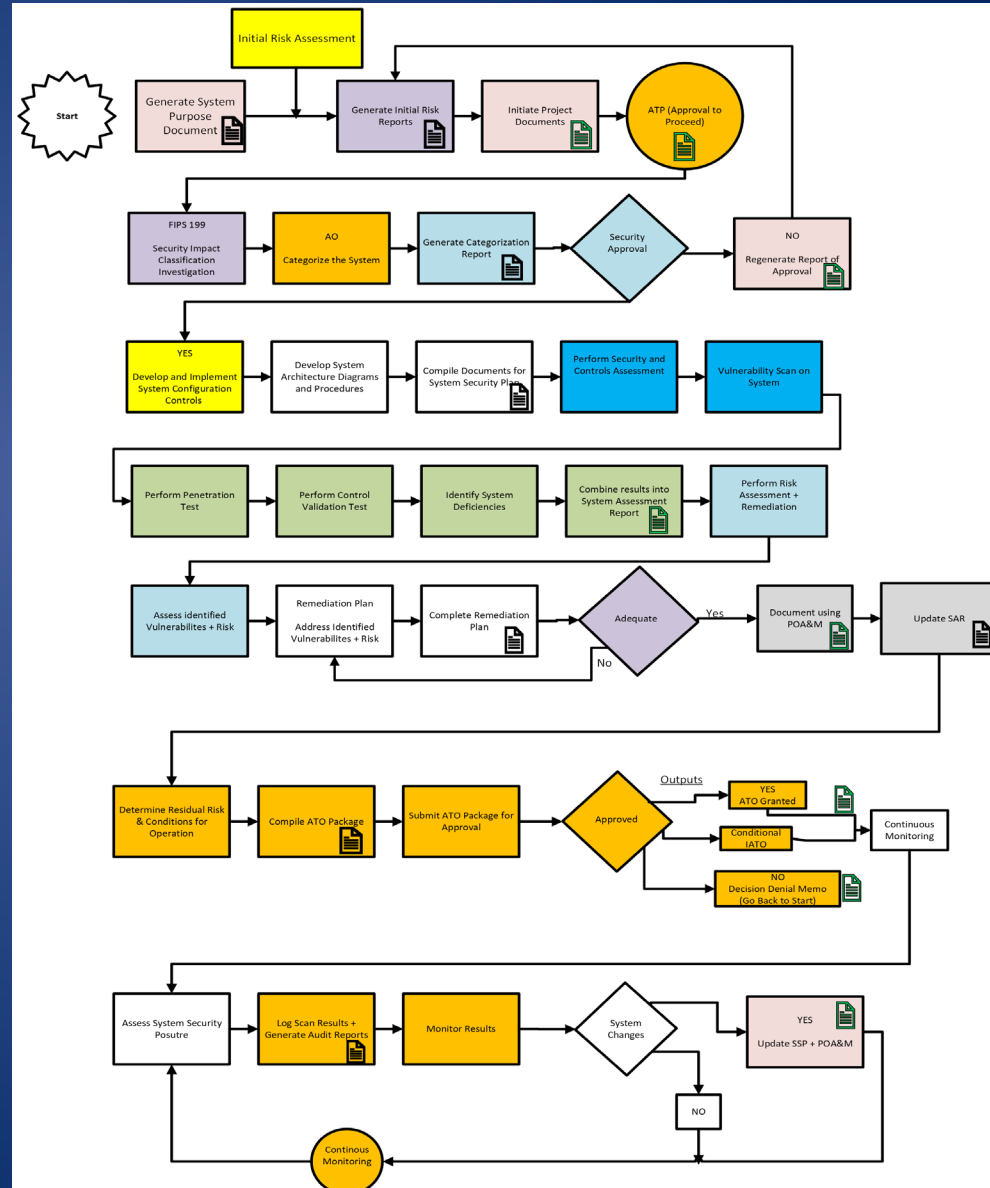
Questions

References

Cho, Y. H., & Eyester, L. (2019). *Decision matter of: 22nd century technologies, inc.* U.S. Government Accountability Office. B-418029; B-418029.2; B-418029.3. https://www.gao.gov/products/b-418029%2Cb-418029.2%2Cb-418029.3

Department of Defense Chief Information. (2024, May 29). *Continuous Authorization to Operate (cATO) Evaluation Criteria: DevSecOps use case*. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/Library/cATO-EvaluationCriteria.pdf

Feldman, A. (2018). *Taking the ATO process from 6 months to 30 days*. GSA Technology Transformation Services. https://18f.gsa.gov/2018/07/19/taking-the-ato-process-from-6-months-to-30-days/

Harris, C. C., & Powner, D. A. (2018, August 2). *Federal chief information officers: Critical actions needed to address shortcomings and challenges in implementing responsibilities.* (GAO-18-93). U.S. Government Accountability Office. https://www.gao.gov/products/gao-18-93

Harris, C. C. (2024, September 10). *Cloud computing: Agencies need to address key OMB procurement requirements*. (GAO-24-106137). U.S. Government Accountability Office. https://www.gao.gov/products/gao-24-106137

References Cont.

Kiernan, K. (2021). *An offering in the blue cyber series: Fast track ATO.* AFWERX SIBR/STTR. https://www.safcn.af.mil/Portals/64/DAF%20Fast%20Track%20%20ATO%20072021%20Cleared%20for%20Public%20Release%20AFR-2021-2421%2C%2026%20Jul%202021.pdf

Magnell, S. B, & Pereira, A. B. (2019). *Decision matter of: Applied sciences & information systems, inc.* U.S. Government Accountability Office. B-418068; B-418068.2. https://www.gao.gov/products/b-418068%2Cb-418068.2

Mitchell, B. (2019). Cybersecurity ATOs, faster: Air Force sets up new Fast Track. In *FedScoop* (pp. 1–9). https://fedscoop.com/fast-track-ato-air-force-wanda-jones-heath/

National Institute of Standards and Technology. (n.d.). *NIST risk management framework.* https://csrc.nist.gov/projects/risk-management/about-rmf

National Institute of Standards and Technology. (2002). *Standards for security categorization of federal information and information systems*. (FIPS PUB 199). https://csrc.nist.gov/files/pubs/fips/199/final/docs/fips-pub-199-final.pdf

National Institute of Standards and Technology. (2018, December). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*. (SP.800-37 r2). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

References Cont.

Oakley, S. S. (2023, April 5). *Software acquisition: Additional actions needed to help DOD implement future modernization efforts.* (GAO-23-105611). U.S. Government Accountability Office. https://www.gao.gov/products/gao-23-105611

OpenControl. (n.d.). *OpenControl's introduction to ATOs: Steps of the ATO process.* https://atos.open-control.org/steps/

Secretary of the Air Force Chief Information. (2019, March 18). *Fast-track authorization to operate (ATO).* Department of the Air Force. https://federalnewsnetwork.com/wp-content/uploads/2019/04/AF-fast-track-ATO-memo-march-2019.pdf

Secretary of the Air Force Chief Information. (2024, September 5). *Risk management framework (RMF) for department of the air force information technology (IT).* (AFI17-101_DAFGM2024-01). Department of the Air Force. https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf

2024 NPS Air Force Element Cohort

Maj Blakely, Indigo

Capt Blankenship, James

Capt Halbert, Triston

Capt Johnson, Davin

Capt Koester, Ryan

Capt McNair, Monet

2d Lt(s) Napier, Philip

SMSgt Reyes, Anna

Capt Sheedy, Kevin

Capt Soto, Luis

Capt Weitgenant, Ryan

Capt Wilson, Grant

1st Lt Woods, Jonathan