SYM-AM-25-342

Excerpt from the Proceedings

of the

Twenty-Second Annual Acquisition Research Symposium and Innovation Summit

Thursday, May 8, 2025 Sessions
Volume II

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

Published: May 5, 2025

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

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

Jamie Porchia, Lt Col, PhD—is an Assistant Professor at the Naval Postgraduate School where she teaches enterprise innovation, strategic sourcing, and introductory contracting courses. She is an Air Force contracting officer with over 15 years of experience across a variety of contracting specialties. She has multiple publications in the International Journal of Physical Distribution & Logistics Management, Supply Chain Management an International Journal and the Journal of Contract Management. Her primary research interests are supply chain mapping, drone supply chains, supply chain design and procurement.

Daniel J. Finkenstadt, Lt Col, PhD—is a career field management staff officer for the Deputy Assistant Secretary (Contracting) Assistant Secretary of the Air Force (Acquisition, Technology, & Logistics) at the Pentagon specializing in applied artificial and business intelligence education and training. He is the former Assistant Professor of Defense Management at the Naval Postgraduate School Department of Defense Management. LtCol Finkenstadt has over 24 years of service with 20 of those in contracting and acquisition related work. He is the author of numerous peer-reviewed studies in journals such as the Milbank Quarterly, Journal of Purchasing and Supply Management and International Journal of Operations and Production Management. He has been published eight times by the Harvard Business Review, including two features that have been published in numerous languages. He is also co-author of the books Supply Chain Immunity (Springer 2023) and Bioinspired Strategic Design (Production Press 2024).

Contributing Authors—Capt Grant Wilson, SMSgt Anna Reyes; MSgt Philip Napier; Capt Luis Soto-Rodriguez, Capt Davin Johnson, Major Indigo Blakely, Capt James Blankenship, Capt Triston Halbert, Capt Ryan Koester, Capt Monet McNair, Capt Kevin Sheedy, Capt Ryan Weitgenant, and Capt Jonathan Woods

Abstract

Many of the novel technologies that the DoD seeks to leverage include software that needs to connect to the government's network. An important part of transitioning these novel technologies is ensuring that the technology can connect to the government's network in a timely and seamless manner. This is facilitated through the Authority to Operate (ATO) process. It is imperative that the DoD has a thorough understanding of the internal challenges and bottlenecks within the ATO process to identify opportunities for easing the navigation process for DoD members and new companies seeking to offer their novel technology to the Defense market. To this end, this study focuses on the Department of the Air Force's (DAF) ATO process and examines how the lessons learned from the DAF can be applied to the DoD. Through an analysis of the extant literature on the current state of the ATO process, semi-structured interviews with stakeholders inside and outside the DAF, and the creation of a detailed visualization of the ATO process, a set of recommendations for improving the ATO process are presented. Additionally, several research initiatives have emerged to enhance the DAF's understanding of the ATO process, its effectiveness, and security model evolution.

Introduction

Many of the novel technologies that the Department of Defense (DoD) is seeking to leverage include software that needs to connect to the government's network. An important part of transitioning these novel technologies is ensuring that the technology can connect to the government's network in a timely and seamless manner. This is facilitated through the Authority to Operate (ATO) process. The ATO ensures information systems meet an extensive list of security and risk management requirements before being authorized to oversee sensitive government information. The ATO process has become increasingly important as the DoD has become more reliant on a digital infrastructure where network security, data processing, and

communication are all vital to the mission's success. This complex and often daunting process can be a barrier to new companies who want to offer their novel technologies to the Defense market and to DoD members seeking to obtain these technologies. Therefore, it is imperative that the DoD has a thorough understanding of the internal challenges and bottlenecks within the ATO process to identify opportunities for easing the navigation process and streamlining the approval structure.

The Department of the Air Force (DAF) is seeking to better understand their internal ATO processes, recognizing that the integration of novel technologies, such as Generative AI, on its networks requires approvals by Authorizing Officials (AOs), Commanders, and several other people interwoven into the ATO process. The complexity of the ATO process is not widely understood across the DAF. Combining the complex approval process, with senior leader demand signals to rapidly integrate novel software, drives the need to better understand the bottlenecks in the process that can result in lengthy delays for approved ATOs. Within the process, there exist many additional reviews which the Authorizing Official (AO) is responsible for, and the program office/system owner is required to ensure it is up to date. While the DAF has utilized innovative methods to speed up the process such as the Fast Track ATO and the Continuous ATO (cATO), there remains an opportunity to understand when and how the complexities of this process are most susceptible to delays. As such, this sponsored research seeks to address these concerns by answering the following 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?

The approach to addressing these questions is multifaceted and provides an outline for how this paper is structured. The first research question is addressed through a literature review of publicly available information on the ATO process. The sources of the publicly available information include, but are not limited to, previous theses, GAO reports, RAND reports and scholarly articles. The second research question is addressed through semi-structured interviews with AOs, system owners, and cybersecurity personnel both inside and outside of the DAF. Lastly, the third research question is addressed though the development of a process map that is derived from the literature review and the semi-structured interviews. The culmination of this paper results in recommendations for how the DAF and DoD can improve the ATO process, provides an examination of emerging trends and offers future research initiatives. This research was conducted in support of the Department of Air Force Chief Data & AI Office (DAF CDAO) in partnership with DAF Contracting. The combined efforts of 13 NPS students, one faculty member and one DAF Contracting AI Education Lead enabled this research.

Literature Review

This literature review analyzes publicly available information resources which detail the ATO process, its uses, and challenges. This chapter is divided into three sections: regulations and guidance governing the ATO process, ATO execution options, and the findings of the Government Accountability Office (GAO). The literature review identifies that the ATO process has many working parts operating independently and requires immense documentation and task management to receive approval in a timely manner.

ATO Regulations and Guidance

Federal Information Security Modernization Act and DoD Guidance

The Federal Information Security Modernization Act (FISMA) 2014 is currently the most recent public law established to govern security controls over information systems in the federal government. FISMA recognizes the inherent challenges of ensuring information systems are secure and seeks to codify mechanisms for improving oversight and management of information systems that house federal data. This public law delegates authority to the secretary of defense for oversight and development of guidance and policies that ensure standards are met and enforced in a timely manner (Federal Information Security Modernization Act, 2014). The secretary of defense further delegates these responsibilities to the DoD chief information officer (CIO) through Department of Defense Directive (DoDD) 5144.02, requiring the DoD CIO to establish policies and guidance on how the Department will manage the enterprise-wide information systems architecture (Deputy Secretary of Defense, 2014). Through key Department of Defense Instructions (DoDIs) such as DoDI 8310.01, DoDI 8500.01 and DoDI 8510.01, the DoD CIO has set forth the pathways for the services to establish and refine their processes to align with DoD objectives (Chief Information Officer Library, n.d.).

DAF Guidance

ATO is defined within AFI 17-101 as:

> The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (Secretary of the Air Force Chief Information [SAF/CN], 2024)

The Air Force and other government organizations structure the ATO process to evaluate information systems before they are allowed on the DoD network. This process ensures the system meets strict security and risk management requirements before becoming operational. Due to the continuous changes in cybersecurity and the increasing requirement for rapid system deployment, the process has evolved. In addition to the processes of reviewing the system, there are timelines that govern the length of the ATO approval. ATOs are standing until there are major changes to the system, risk or threat updates, or every 3 years (SAF/CN, 2024). The AO starts the process of ATOs with the Risk Management Framework (SAF/CN, 2024).

Risk Management Framework (RMF)

The Risk Management Framework (RMF) is comprised of six steps as shown in Figure 1. The RMF is a set of governing principles that outline the security, architectural, and monitoring process for DoD IT systems. Although the RMF began in the DoD, it became the federal standard for information systems in 2010. The RMF has been recognized by the National Institute of Standards and Technology (NIST) as the fundamental starting point for developing a strategy for securing all federal data. Overall, the main goal of RMF is to secure DoD IT systems and to encourage modeling potential threats to detect cyber-related risks and vulnerable areas (Blue Cyber Education Series, 2021).

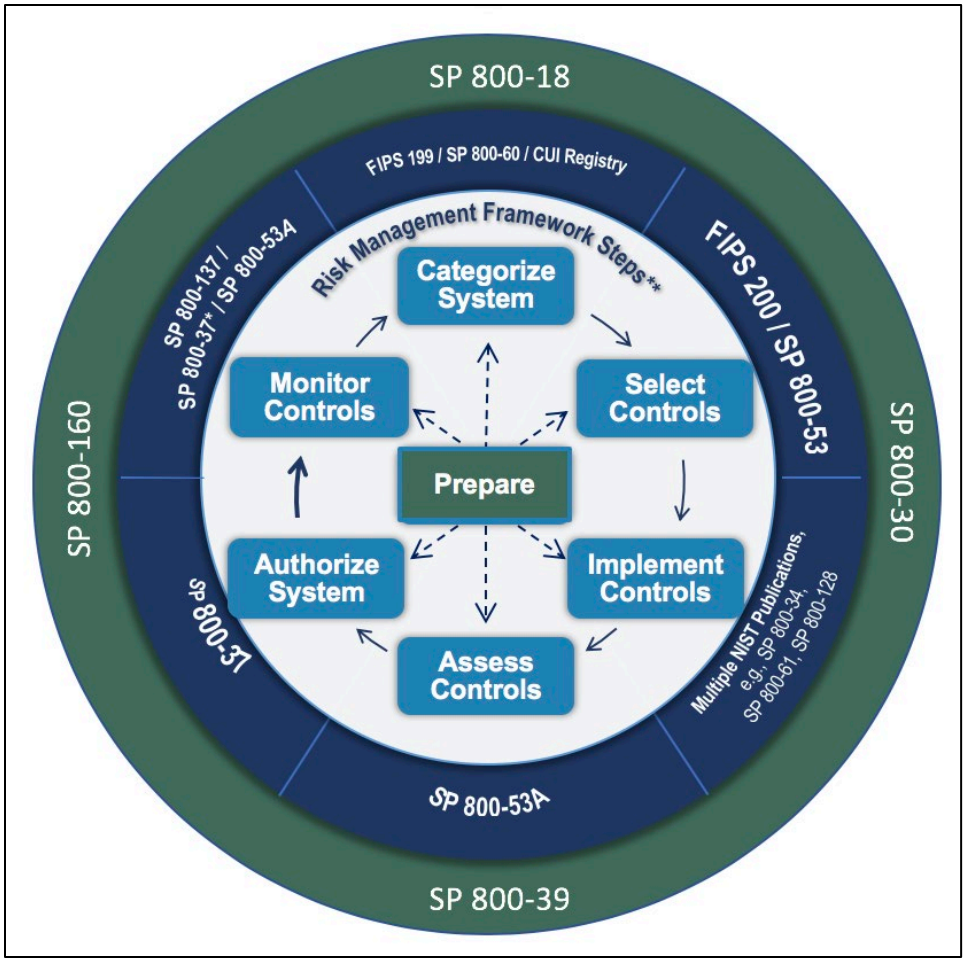

Figure 1. Risk Management Framework (OpenControl, n.d.).

Given the RMF's priority of securing IT systems, security considerations are embedded into each phase of the system's development following seven interlocking steps:

1. Prepare – This is the first step in the RMF framework and sets the priorities and context for the risk management process at the organizational level. This step includes 18 tasks that must be accomplished collectively by the "DoD Component CIO, DoD PAO, and JCA capability portfolio manager (CPM) to enable an effective risk-managed security authorization process" (DoD CIO, 2022, p. 13).
2. Categorize System – This step is where the security impact level of a system is determined. The AO will coordinate with the system's owner to determine whether to categorize a system as low, moderate, or high. The three objectives that influence how a system is categorized are confidentiality, integrity, and information availability, all outlined in the National Institute of Standards Federal Information Processing Standards (FIPS) 199 (NIST, 2002). Knowing what category level a system is helps ensure the right level of security controls are applied to a particular system (OpenControl, n.d.).

3. Select Controls – In this step, the NIST Special Publication 800-53 is used as a guideline to select security controls for a system based on its category. Security controls identify potential vulnerabilities and aid in mitigating any risks associated with the system. The AO makes this determination based on the system's impact level, controls already in place, the type of ATO requested, and if any tailoring is needed to the security controls (OpenControl, n.d.).
4. Implement Controls – The security controls selected in the previous step are implemented to ensure they function as intended, which is outlined in the System Security Plan (SSP) document (OpenControl, n.d.). Technical, operational, and management measures are all required in this step to help reduce risks to acceptable levels.
5. Assess Controls – After the controls are established, they are evaluated using testing and validation processes to ensure effective operation while meeting established security requirements. This assessment must be completed before the system can become operational. The type of assessment will depend on what form of ATO is requested. Regardless, the assessment will be conducted by a development and infrastructure team; all of which are in the SSP (NIST, n.d.). The Security Assessment Report (SAR) (NIST, n.d.) documents the assessment results and these results determine if the system needs to be changed before it can have an ATO.
6. Authorize System – Here, the AO reviews the risk assessment and residual risks and decides whether or not to authorize the system to be used in operation. If the AO approves the system, they will sign an ATO memo. The memo lists criteria such as allowing the ATO to stay valid, the expiration date of the ATO, and when the system in question can begin operations (OpenControl, n.d.).
7. Monitor Controls – After a system receives an ATO, it will be placed under continuous monitoring to ensure the security controls maintain their effectiveness. If any changes are made to the system, an assessment must be done to determine the impact the change(s) will make. This step is vital since it is where new vulnerabilities can be identified and promptly addressed to ensure system compliance. This can be completed by routinely performing scans of the systems and by keeping all documentation updated (OpenControl, n.d.).

Authority Delegation

Delegation authority for the ATO process is important in balancing security with operational agility. Being able to delegate decision-making authority allows an ATO to be processed faster while still ensuring the system's security is maintained. The ATO delegation authority must be managed closely to avoid any potential lapses in security while ensuring decision-makers have the appropriate resources and knowledge to make accurate risk assessments. While some decisions can be delegated, the NIST Special Publication 800-37 and DoDI 8510.01 offer top-level guidance on which decisions and tasks can be delegated and the resulting accountability that must still be maintained (DoD CIO, 2022; NIST, 2018).

ATO Execution Options

There are two ways in which the ATO process is traditionally executed, centralized and decentralized. Centralization is the process in which all responsibility resides with the AO. On the other hand, decentralization of responsibility occurs when the AO delegates portions of the process to cybersecurity teams or operational leaders.

Centralized ATO Process

Until recently, the Air Force ATO process was centralized with final authority residing with a high-ranking AO. These AOs are responsible for reviewing security assessments, evaluating risks, and deciding whether a system is safe to use within the Air Force's. This centralized authority has been criticized for being very inefficient as an AO must sign off on all major and minor decisions for a security system. Doing so bottlenecks the approval process as the AO must manage a large volume of systems going through authorization procedures. The result is a long delay in obtaining an ATO, which restricts the deployment of modern systems and limits the Air Force's ability to adapt to current and future operational needs. Additionally, with a centralized authority, the decisions about a system often occur several layers removed from the actual environment of the system being assessed. Some AOs are not directly involved with operational teams, which may lead to security evaluations that lack the awareness to fully comprehend how certain risks could impact real-world operations infrastructure (SAF/CN, 2024).

Decentralized ATO Process

After recognizing the need for change, the Air Force shifted to a decentralized authority delegation for the ATO process. This developed from the need to increase the speed of the system authorization process without sacrificing the level of security evaluation (SAF/CN, 2019). Using this strategy, the AO can delegate some of their responsibilities to lower-level officials, such as certain members of the cybersecurity team or some operational leaders, allowing these individuals to make important decisions at a more localized level. The following is a list of a few of the key benefits of decentralized execution:

1. Swifter Decision-Making: Delegating authority to lower levels allows the Air Force to streamline parts of the decision-making process (SAF/CN, 2019). This can reduce the time needed to issue an ATO for systems with lower risks or that already have partial authorization. Delegation helps the team address some security issues much sooner by not having to wait or route for approval from a higher-ranking official.
2. Operational Risk Evaluation: Having decentralized authority allows risk evaluations to be conducted closer to the operational environment. AOs with direct knowledge of a system and how it will be used in the field can make an informed decision about risk more than an official at a higher level who is not in the operational field (SAF/CN, 2019). This helps ensure that risk is evaluated by someone who better understands a system's mission-criticality.
3. Empower Cyber and Operational Teams: Delegating approval authority empowers cybersecurity members and operational leaders. This allows them to be more active during the ATO process (SAF/CN, 2019). This empowerment can bolster collaboration between the security team and the system owners by ensuring that security is part of the system development and deployment from the beginning. Integrating security into the operational workflow allows the Air Force to make a more agile and responsive cybersecurity environment.

GAO Findings

The GAO is responsible for analyzing how the government spends taxpayer's dollars and identifying ways that the government can save money and operate in a more efficient manner (GAO, n.d.). In this function, and as it pertains to the ATO process, the GAO has generated several reports and investigated protests related to the ATO process with the intention of providing unbiased assessments and recommendations on how to improve the process across the federal government. There are three key reports that highlight the internal government consternation with the ATO process and related functions, and there are two key protests that highlight the impact

of the ATO process on external parties, such as contractors, seeking to provide the government with a service where access to DAF and DoD networks are necessary. The subsequent paragraphs describe the pertinent reports and protests examined by the GAO.

In 2018, the GAO was requested by Congress to conduct a review and generate a report on the extent to which chief information officers (CIOs) were carrying out their responsibilities. Specifically, the GAO examined how effectively CIOs were operating in their roles as outlined in federal regulations and guidance and identifying critical factors that were helping or hindering CIOs in fulfilling their responsibilities. Through survey responses from 24 CIOs and interviews with current CIOs and members of the Office of Management and Budget (OMB), the GAO identified that most agency CIOs were not effectively operating in their roles and that they were hindered from operating in these roles for reasons such as limited financial and personnel resources. However, resources such as the NIST and OMB guidance's were major enablers for aiding CIOs in carrying out their responsibilities (Harris & Powner, 2018). Although not explicitly highlighted in the report, without having the appropriate CIO roles and empowerment in place, the ATO process would undoubtedly be hindered particularly since the CIO has an important role in guiding the ATO process.

The second report was published in 2023. In this report, the GAO was tasked with examining the status of the DoD's implementation of the Defense Innovation Board (DIB) and Defense Science Board's (DSB) recommendations for modernizing the software acquisition process. One of the key findings was that the DoD had only partially implemented the DIB's recommendation to create an ATO reciprocity process. An established process for ATO reciprocity would enable rapid sharing of software capabilities and platforms across the military branches and other DoD organizations (Oakley, 2023). Although the DoD issued DoDI 8510.01 in 2022, which provides some guidance on decision-making authority reciprocity, according to the GAO, further work was still needed to enable a DoD-wide ATO reciprocity process.

Shortly after the 2023 report, a third report was issued in 2024, which analyzed how well federal agencies were implementing cloud computing procurement requirements across their organizations. The report identified that most agencies had established the CIO as the responsible authority for modernization projects; however, "most agencies did not establish guidance related to service level agreements (SLA), which define the levels of service and performance that the agency expects its cloud providers to meet" (Harris, 2024, What GAO Found section, para. 1). The limited guidance on SLA requirements is challenging not only for government employees, but also for contractors trying to gain approval so they can compete for contracts.

In addition to the three key reports produced by the GAO, the GAO also examined two protests in 2019 that highlight the importance of clear ATO solicitation procedures. In both protests, the contractors disagreed with the source selection evaluation factors related to ATO requirements and Federal Risk and Authorization Management Program (FedRAMP). Although both protests were either denied or dismissed, there are valuable lessons that can be learned (Cho & Eyester, 2019; Magnell & Pereira, 2019).

The first protest was filed against the United States Marine Corps (USMC) who issued a request for quote (RFQ) for a web-based service. The Performance Work Statement (PWS) stated that the "Contractor shall provide the Government with proof of its hosting environment's interim ATO [authority to operate], ATO, or active FedRAMP accreditation" (Magnell & Pereira, 2019, p. 2). The protestor contended that the awarded contractor did not possess the appropriate accreditations and therefore did not meet the requirements of the PWS. However, the GAO asserted that the PWS requirement did not specify that a contractor was required to have the

appropriate accreditations specifically through the Marine Corps or the DoD. Thus, the awarded contractor did meet the requirements of the PWS (Magnell & Pereira, 2019).

The second protest was filed against the Department of Labor (DoL) who was seeking to establish a Blanket Purchase Agreement (BPA) utilizing the Federal Supply Schedule (FSS) for integration support, information assurance, and cybersecurity services. The protestor did not agree with the weaknesses assigned to their proposal, one of which was the government's decision to assess a weakness to their proposal for failing to adequately describe how they would support and manage the DoL's ATO process for the services being acquired. The solicitation requests that bidders "perform an in-depth analysis of current processes to determine the adequacy and shall prepare recommendations describing the technical approach, organizational resources, and management controls to be employed to meet the cost, performance and schedule requirements for the task; ensuring conformance with federal policies and guidelines" (Cho & Eyester, 2019, p. 5). However, the protestor did not provide sufficient depth to their response that adequately met the level of detail requested. Though the protests pertained to agencies inside and outside of the DoD, the NIST created a common procedure based on these rulings. The biggest lesson learned across these protests is that even when the prospective company follows compliance rules, the rules are often confusing and hard to follow. Some evaluators have difficulty following what compliance is and what it is not.

Overall, the literature on the regulations governing the ATO process, ATO centralization versus decentralization options, and the findings of the GAO offer insights into the prevailing guidelines that are shaping the ATO process. The literature sets the foundation for the subsequent sections of this research. The following section will delve into the data collection process and analysis.

Data and Analysis

This section synthesizes the findings from 17 interviews conducted with military and civilian personnel across the Navy and Air Force in the fall of 2024 by graduate students assigned to the Naval Postgraduate School's Enterprise Sourcing Program. Interviewees included cybersecurity experts and program executive officers, who shared detailed insights into their respective processes for achieving an Authority to Operate (ATO), challenges faced, and best practices. Figures referenced throughout provide visual representations of specific processes and trends.

Introduction to Data and Analysis

This study aimed to document ATO processes, identify challenges, and analyze trends across organizations. Data was collected to highlight how workflows vary between systems and to uncover recurring themes like delays, automation needs, and the shift to agile methodologies. The analysis section builds on this data to explore patterns, contradictions, and innovative practices.

ATO Processes Overview

42nd Communications Squadron

The ATO process at the 42nd Communications Squadron involves multiple steps, starting with a system owner submitting a Cyber Security Requirements Document (CSRD) to their Communications Squadron (CS):

1. Verify if the requested software, hardware, or network is on the base-level Approved Products List (APL).
    - If not, consult the Air Force's APL.

- If absent, escalate to the local Configuration Control Board (CCB).

2. The CCB evaluates the system's mission impact and approves or denies the request.
3. Approved packages are sent to the HQ Cyberspace Capabilities Center (CCC) at Scott, IL.
4. The Air Force Network Integration Center (AFNIC) reviews the code for vulnerabilities.
5. The Information Assurance Manager (IAM) communicates AFNIC's recommendation to the local Communications Squadron Commander.
6. Certification is sent to the base's HQ for final accreditation by the Authorizing Official (AO).
7. If accreditation is granted, the system is authorized for 3 years.

Navy Information System Security Manager (ISSM)

The Navy's ATO process consists of four distinct phases, based on NIST SP800 guidelines:

1. **Interim Authority to Test (IATT):** Grants temporary testing approval for systems on the Department of Defense Information Networks (DoDIN) for up to 6 months.
2. **Certification:** Includes System Operation and Verification Testing (SOVT) to ensure compliance with network requirements.
3. **Accreditation:** Involves documentation review and approval, often the lengthiest phase.
4. **Reaccreditation:** Conducted every 18–36 months to confirm ongoing compliance by revisiting key Risk Management Framework (RMF) steps.

Communications AFSC Program Coordinator

The Risk Management Framework (RMF) Process is a primary method used to:

1. Categorize the system based on CNSSI 1253.
2. Select security controls, reviewed and approved by the security manager.
3. Implement controls during the program's ATO phase.
4. Conduct continuous monitoring, including security updates and vulnerability management.

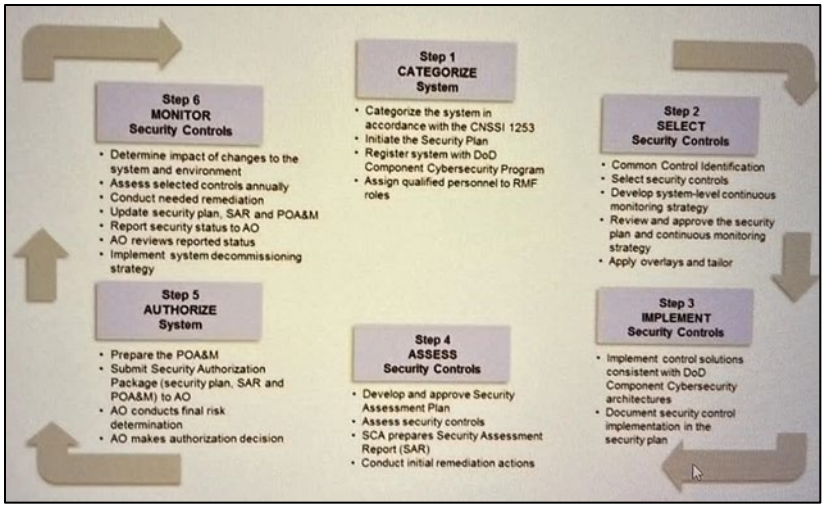

Figure 2: The RMF Process. Source: Communications AFSC Program Coordinator

TRANSCOM ATO Approach

At TRANSCOM, the J6, designated by the TRANSCOM commander, serves as the Authorizing Official (AO), with some delegation to the deputy J6 for efficiency. While major authorizations require AO-level approval, interim software releases or minor modifications follow a streamlined process where approval is handled at lower levels, such as the J6 side or program leadership.

For the DevSecOps platform, the traditional Risk Management Framework (RMF) process is used for initial authorization. This includes a comprehensive package and security assessment that goes to the AO. Tenant applications on the platform inherit approximately 80% of security controls from the platform, simplifying their requirements. These tenants perform a smaller subset of controls (the "assess-only" portion), which still requires AO sign-off but benefits from automation. Automated control gates further streamline authorization, ensuring repeatable and efficient processes for moving applications live.

The traditional step-by-step ATO process, where all documentation is submitted for periodic review, is being replaced by a more agile and efficient approach centered on continuous monitoring. This shift enables Authorizing Officials (AOs) to view real-time vulnerability and risk data through dashboards, ensuring transparency and ongoing oversight. The goal is to transition to a continuous ATO process, enhancing efficiency and risk management compared to the outdated annual or multi-year review cycles. This agile approach aligns with modern development practices and operational demands.

The focus is shifting from approving individual software releases to approving the process for software deployment. Once the process meets all predefined criteria, software releases that adhere to it are automatically authorized, eliminating the need for repeated reapproval for each deployment. This streamlines operations and enhances efficiency.

Key Issues and Considerations

Need for Automatic Data Collection

Efficient and automated data collection has been consistently identified by interviewees as a critical requirement to streamline the ATO process. A recurring challenge is the inefficiency of manual systems, which are outdated and slow. One program executive officer (PEO) highlighted managing legacy programs with code from as early as 1995. Developers accustomed to traditional waterfall methods often resist transitioning to modern workflows, further exacerbating delays.

To address this, transitioning to continuous integration for tenant applications is essential. Continuous integration embeds automated checks into the development pipeline, ensuring security standards are met throughout the deployment process. Tools like Fortify, SonarQube, and Twistlock enable developers to receive immediate feedback on vulnerabilities as code is uploaded to a centralized repository. Automated technical controls replace error-prone administrative tasks, enforcing consistent compliance with security baselines and supporting robust auditing mechanisms. This approach aligns with DevSecOps and agile methodologies, enhancing overall system integrity and efficiency.

The extensive documentation requirements of the ATO process also contribute to significant delays. Security control assessments, vulnerability management plans, and continuous monitoring protocols must be maintained as technologies and threats evolve. However, real-time updates to documentation are resource-intensive, especially across diverse projects. Automating these updates can alleviate bottlenecks by prioritizing accurate, up-to-date information.

Recommendations include better defining and documenting specific requirements from the outset of the ATO process. Standardizing compliance frameworks and tools across organizations would ensure greater efficiency and consistency. Additionally, agencies should establish clear guidelines and role definitions to align contractor efforts with government standards, particularly for ongoing compliance monitoring. Automated processes and standardized tools can significantly reduce reliance on contractors while maintaining alignment with security and operational goals.

Overall, automating data collection and approval processes offers transformative potential for the ATO framework. These advancements would streamline operations, reduce delays, and enhance the agility required to adapt to emerging technologies and threats.

Agile Methods

Adapting contracts to agile methodologies presents significant challenges, as highlighted by interviewees. A primary shift in agile development is emphasizing "working software" as the Key Performance Parameter (KPP) rather than traditional metrics. Many contracting officers, while skilled and diligent, have limited exposure to agile training and struggle to apply agile principles to requirements and deliveries. This reflects a broader need to modernize how contracts are structured.

The cultural shift required for agile delivery is particularly challenging within the functional community. Historically, this community has adhered to waterfall methods, characterized by long delivery cycles, static requirements, and extensive post-development testing. In contrast, agile methodologies prioritize rapid delivery, automated testing, and iterative releases. Agile models fix cost and schedule while allowing feature sets to evolve, focusing on incremental capability delivery. Functional teams must embrace the concept of a Minimum Viable Product (MVP) and redefine requirements into smaller, actionable increments. This cultural change demands new approaches to defining both requirements and delivery timelines.

An example of these challenges is evident within the cybersecurity service provider (CSSP) community. Tasked with securing modern cloud-based platforms, the CSSP community—accustomed to physical server monitoring—discovered that existing policies failed to address cloud cybersecurity requirements. It took 6 months to identify and begin addressing these gaps. Although the DoD is actively updating cybersecurity and acquisition policies, current efforts have yet to reach the agility required for rapid program development, including ATO processes.

Lack of Training

A recurring concern among interviewees was the limited formal training available for the ATO process. Most personnel only realized mistakes during final approval, often due to inconsistent ATO processes across offices. This reactive approach—focusing on rejection with feedback—results in frustration and inefficiencies.

Improved collaboration with experienced professionals such as ISSMs, ISSOs, and Cyber Leads is essential. Encouraging Authorizing Officials (AOs) to actively participate in all stages of the ATO process is particularly crucial for new program managers. Formalized training programs and workshops would foster a proactive culture, equipping personnel with the knowledge and tools to navigate ATO complexities effectively.

Detailed Process Analysis

Students at the Naval Postgraduate School conducted a detailed process analysis based on a combination of literature review research and interview data. The result is a robust process mapping of a typical ATO (Figures 3–7 below).

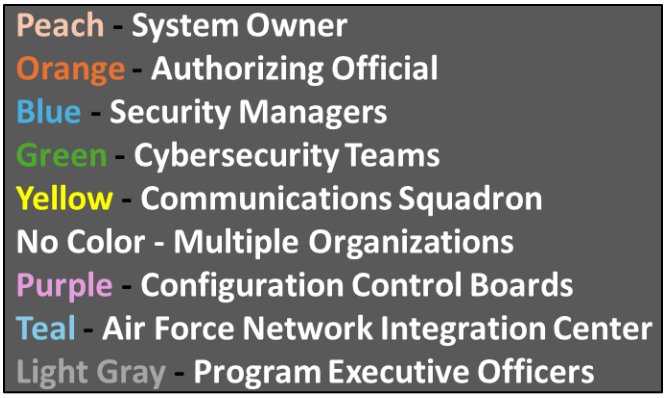

Figure 3: ATO Process Map Legend

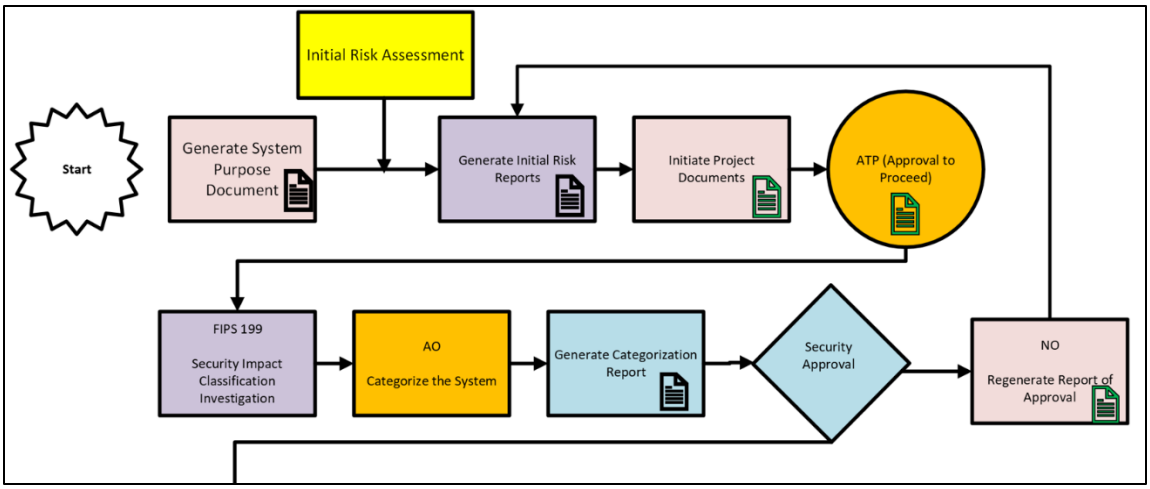

Figure 4: ATO Process Map (Phase 1, Steps 1–8)

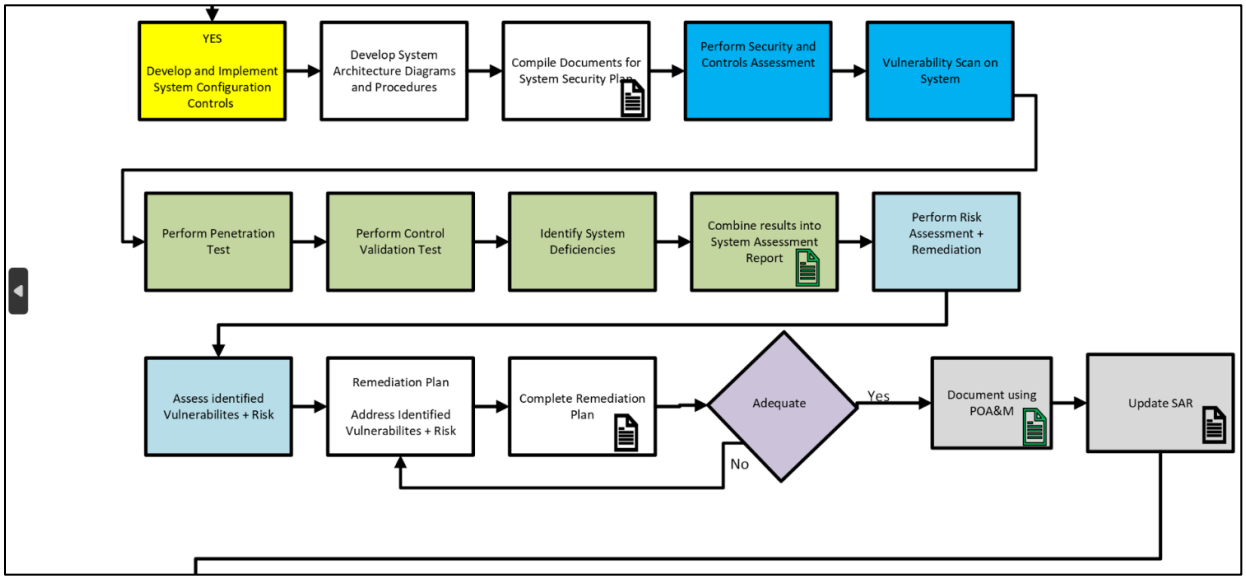

Figure 5: ATO Process Map (Phase 1, Steps 9–24)

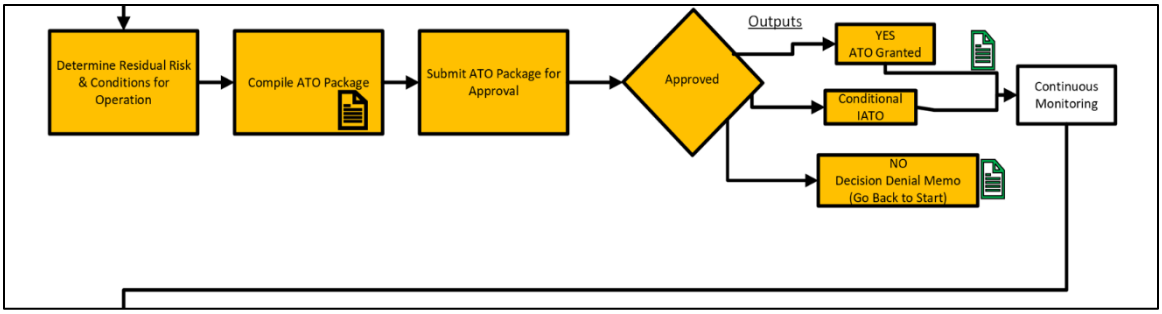

Figure 6: ATO Process Map (Phase 2)

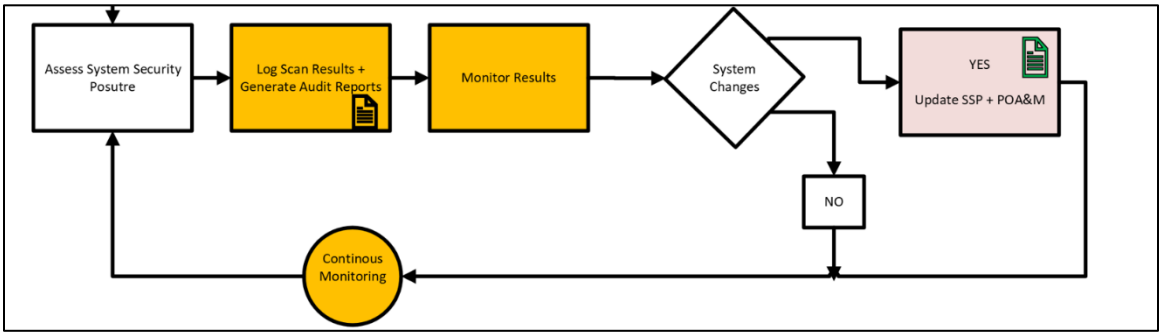

Figure 7: ATO Process Map (Phase 3)

The ATO process begins when the system owner and AO draft the System Purpose Document, which includes an initial risk assessment using the RMF. One of the most time-consuming ongoing tasks involves collecting project documents and completing tasks in eMASS. Once sufficient eMASS tasks are finished, the AO provides Approval to Proceed and categorizes the program using NIST Special Publication 800-53 guidelines. The security manager then evaluates the program by considering its necessity, integration costs, and risk assessment.

The next phase includes 17 sequential eMASS tasks, which can take anywhere from weeks to over 6 months depending on documentation quality and previous approval accuracy. These steps lead to the AO's final ATO review. Programs typically receive conditional approval with specific criteria for continuous monitoring. The expected timeline ranges from 6 to 18 months, though some cases extend to 24 months.

During the program's life cycle, ATO recertification occurs every 3 years or after major changes (SAF/CN, 2024). Updates reflect system performance changes and operating doctrine modifications listed in the Security Assessment Report. While recertification is generally simpler than initial approval, it can become challenging if documentation isn't maintained or if ATO expiration dates aren't tracked.

The traditional ATO process faces several implementation challenges. It requires extensive manual assessments and documentation, demanding significant time, personnel, and funding resources. As cyber threats grow more sophisticated, resource demands increase. While automation could streamline repetitive tasks and improve efficiency, it requires substantial initial investment. Future research should focus on developing cost-effective automation solutions that maintain security standards.

The increasing complexity of connected DoD systems has elevated technical requirements in the ATO process. Security focus has shifted from individual systems to ecosystem-level protection, requiring new approaches to handle interconnected systems within the Air Force's information infrastructure.

Emerging and Future Concepts

Recent developments include Zero Trust Architecture (ZTA) as a foundational element in modern ATO frameworks. ZTA requires all entities, internal or external, to be authenticated and authorized, with continuous validation of access requests. This approach aligns with continuous monitoring requirements and supports real-time authorization processes.

AI and machine learning are becoming integral to risk assessment and threat detection in the ATO process. However, these technologies present unique challenges, particularly regarding model transparency and adaptability, necessitating dedicated research for effective integration.

The Air Force has developed innovative approaches to address these challenges, including Fast Track ATO. This streamlined process focuses on operationally relevant risk assessments rather than pure compliance (Kiernan, 2021). It employs focused sprints where developers, cyber experts, and assessors collaborate intensively, reducing approval times to as little as 5 weeks (Feldman, 2018). Fast Track ATO reduces documentation requirements by emphasizing real-world testing and enables better integration of modern technologies like AI and cloud computing.

Continuous Authorization to Operate (cATO) represents another advancement in Air Force cybersecurity. Unlike traditional ATOs requiring periodic reauthorization, cATO enables ongoing monitoring and assessment of changes. This approach works particularly well in development, security, and operations (DevSecOps) environments, where security integration occurs throughout the system life cycle (Department of Defense Chief Information [DoD/CN], 2024). The continuous monitoring approach allows systems to remain operational while avoiding repeated ATO submissions.

cATO effectively supports DevSecOps and agile development methods, enabling faster updates and testing cycles. This capability proves especially valuable for military applications where rapid technological adaptation is crucial. By implementing cATO, the Air Force has reduced administrative barriers that previously delayed system deployments, improving operational readiness and security responsiveness.

Research Initiatives and Gaps

The following research initiatives and gaps were identified by the student research team during the fall of 2024 while studying this process.

Several research initiatives have emerged to enhance the Air Force's understanding of the ATO process, its effectiveness, and security model evolution in a dynamic operational environment. A key focus area involves developing comprehensive frameworks for securing AI and ML systems. Future research needs to address risks like data poisoning, model drift, and adversarial manipulation while incorporating real-time model validation and anomaly detection. Follow-on research should examine how continuous learning models affect ATO maintenance by analyzing recertification requirements for evolving AI models without compromising mission readiness. Studies should also explore incremental certification methods allowing partial AI model updates without full system recertification, enabling agile deployment while maintaining security standards. In addition to these broad research areas, the ensuing paragraphs establish a future research agenda that is organized around six main areas.

Process Analysis and Optimization

Research comparing traditional, Fast Track, and cATO models would help identify which approach best suits different operational scenarios. Using standardized metrics such as approval timelines, compliance ratings, and resource utilization would enable better assessment and improvement of each process. The exploration of automated tools for risk assessments and compliance checks could streamline the ATO process and reduce bottlenecks.

Organizational Impact Studies

Organizational studies should examine the effects of decentralized ATO authority on decision-making and accountability while identifying challenges in maintaining consistent security postures. These studies need to investigate cultural changes required for effective cATO adoption, including ways to promote security-first mindsets across operational and technical teams. Research should also focus on developing training methods that equip ATO stakeholders with skills for risk-based assessments, continuous monitoring, and adaptive security practices.

Risk Management Framework Development

Risk management research should develop assessment models specifically tailored for cloud, AI, and ML systems to address their unique security challenges. Studies must evaluate the impact of continuous monitoring in mission-critical environments by measuring early threat detection, resilience, and response times.

Policy Implementation and Development

Current policies may need amendments, and new policies must be created to accommodate AI, ML, and cloud-based systems, particularly regarding continuous learning and adaptability. Control measures for AI and ML systems should address model accuracy, data integrity, and vulnerability resilience. New policies must enable rapid integration of modern technologies while maintaining security standards.

Training and Education Requirements

Training programs need development to support modernized ATO frameworks, providing personnel with skills for managing risk in evolving security environments. Certification courses for AI and ML system assessment would ensure teams possess necessary expertise in AI security. Cybersecurity personnel require continuous learning programs to stay current with technological advances and emerging threats.

Operational Implementation Strategy

Implementation requires investment in automated tools for vulnerability scanning, compliance monitoring, and data collection to reduce manual labor and improve efficiency. Standardized templates for assessing emerging technologies would ensure consistent security evaluations. Deployment of monitoring systems would support continuous authorizations by enabling real-time threat response. Critically, the Force must be informed about and trained to use these tools effectively—without proper knowledge transfer, tool development becomes ineffective.

This comprehensive approach to research, policy development, and implementation provides a framework for evolving the ATO process to meet current and future security challenges while maintaining operational effectiveness.

Conclusion

Understanding and improving any complex system begins with acknowledging its challenges and thoroughly mapping its processes. Throughout this research, we have documented the current state of the ATO process, identified its pain points, and analyzed the environment in which these challenges occur. Our conversations with other defense services

reveal that these challenges extend far beyond the Air Force, representing a systemic issue across the entire federal government's cybersecurity infrastructure. The evolution of the ATO process within the Air Force represents a critical junction between security requirements and operational agility, and its solutions may provide a blueprint for other federal agencies facing similar challenges. As technology advances and threats become more sophisticated, the traditional approach to authorization must adapt through research-driven improvements, policy refinement, and enhanced training programs. The successful implementation of Fast Track and continuous ATO frameworks demonstrates the Air Force's commitment to modernization, while the focus on AI integration and automated tools points toward a future of more efficient, responsive security protocols. By addressing the identified research gaps, investing in personnel development, and maintaining a balance between security and operational flexibility, the Air Force can continue to strengthen its cybersecurity posture while supporting rapid technological advancement. This holistic approach ensures that the ATO process remains both rigorous and responsive to the dynamic challenges of modern warfare and defense operations, potentially serving as a model for federal-wide cybersecurity authorization reform.

References

Blue Cyber Education Series. (2021). *Fast Track ATO*. 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

Chief Information Officer Library. (n.d.). *Dodcio.defense.gov*. https://dodcio.defense.gov/library/

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 Officer. (2022). *Risk management framework for DoD systems* (DOD Instruction 8510.01). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

Department of Defense Chief Information Officer. (2024). *Continuous authorization to operate (cATO) evaluation criteria: DevSecOps use case*. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/Library/cATO-EvaluationCriteria.pdf

Deputy Secretary of Defense. (2014). *The DoD chief information officer (DoD CIO)* (DOD Directive 5144.02). https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/514402p.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/

Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3074, 3075, 3076, 3077, 3078, 3079, 3080, 3081, 3082, 3083, 3084, 3085, 3086, 3087 and 3088 (2014).

GAO. (n.d.). *About*. https://www.gao.gov/about

Harris, C. C., & Powner, D. A. (2018). *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). *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

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). *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

Oakley, S. S. (2023). *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). *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). *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

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net