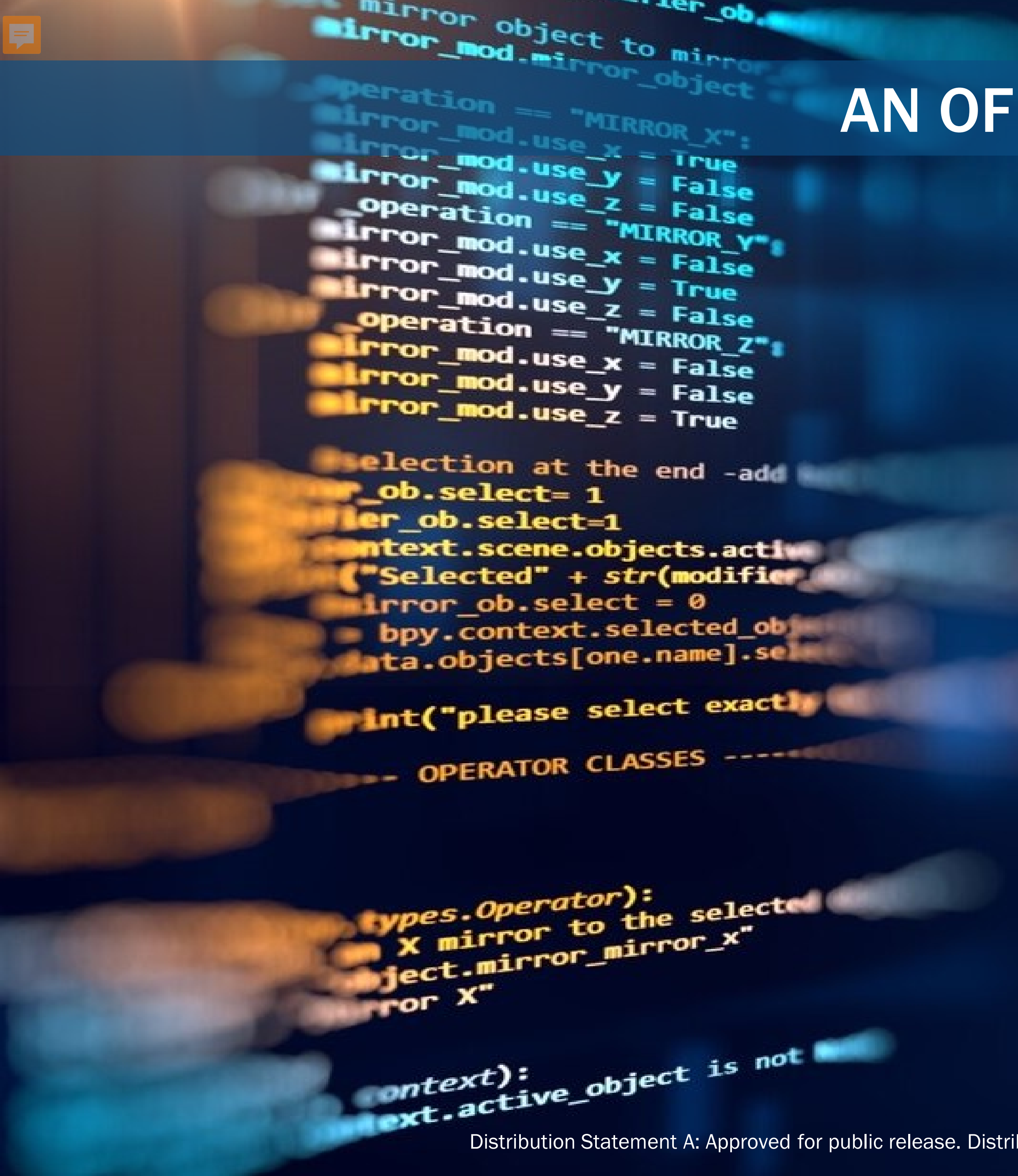
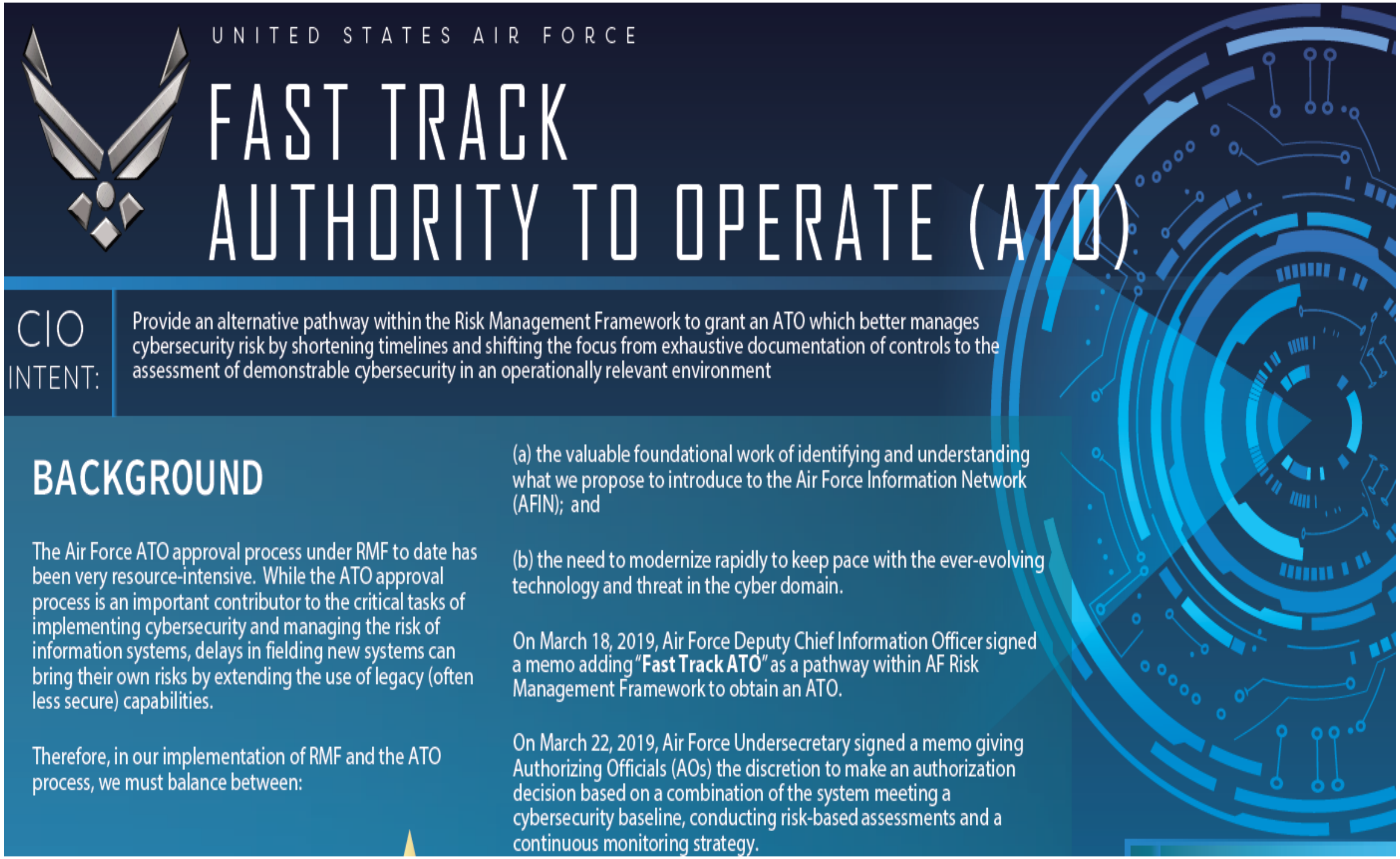


AN OFFERING IN THE BLUE CYBER SERIES:

Fast Track ATO

Version 14 March 2022

#5 in the Blue Cyber Education Series



UNITED STATES AIR FORCE

FAST TRACK AUTHORITY TO OPERATE (ATO)

CIO INTENT: Provide an alternative pathway within the Risk Management Framework to grant an ATO which better manages cybersecurity risk by shortening timelines and shifting the focus from exhaustive documentation of controls to the assessment of demonstrable cybersecurity in an operationally relevant environment

BACKGROUND

The Air Force ATO approval process under RMF to date has been very resource-intensive. While the ATO approval process is an important contributor to the critical tasks of implementing cybersecurity and managing the risk of information systems, delays in fielding new systems can bring their own risks by extending the use of legacy (often less secure) capabilities.

Therefore, in our implementation of RMF and the ATO process, we must balance between:

(a) the valuable foundational work of identifying and understanding what we propose to introduce to the Air Force Information Network (AFIN); and

(b) the need to modernize rapidly to keep pace with the ever-evolving technology and threat in the cyber domain.

On March 18, 2019, Air Force Deputy Chief Information Officer signed a memo adding "**Fast Track ATO**" as a pathway within AF Risk Management Framework to obtain an ATO.

On March 22, 2019, Air Force Undersecretary signed a memo giving Authorizing Officials (AOs) the discretion to make an authorization decision based on a combination of the system meeting a cybersecurity baseline, conducting risk-based assessments and a continuous monitoring strategy.

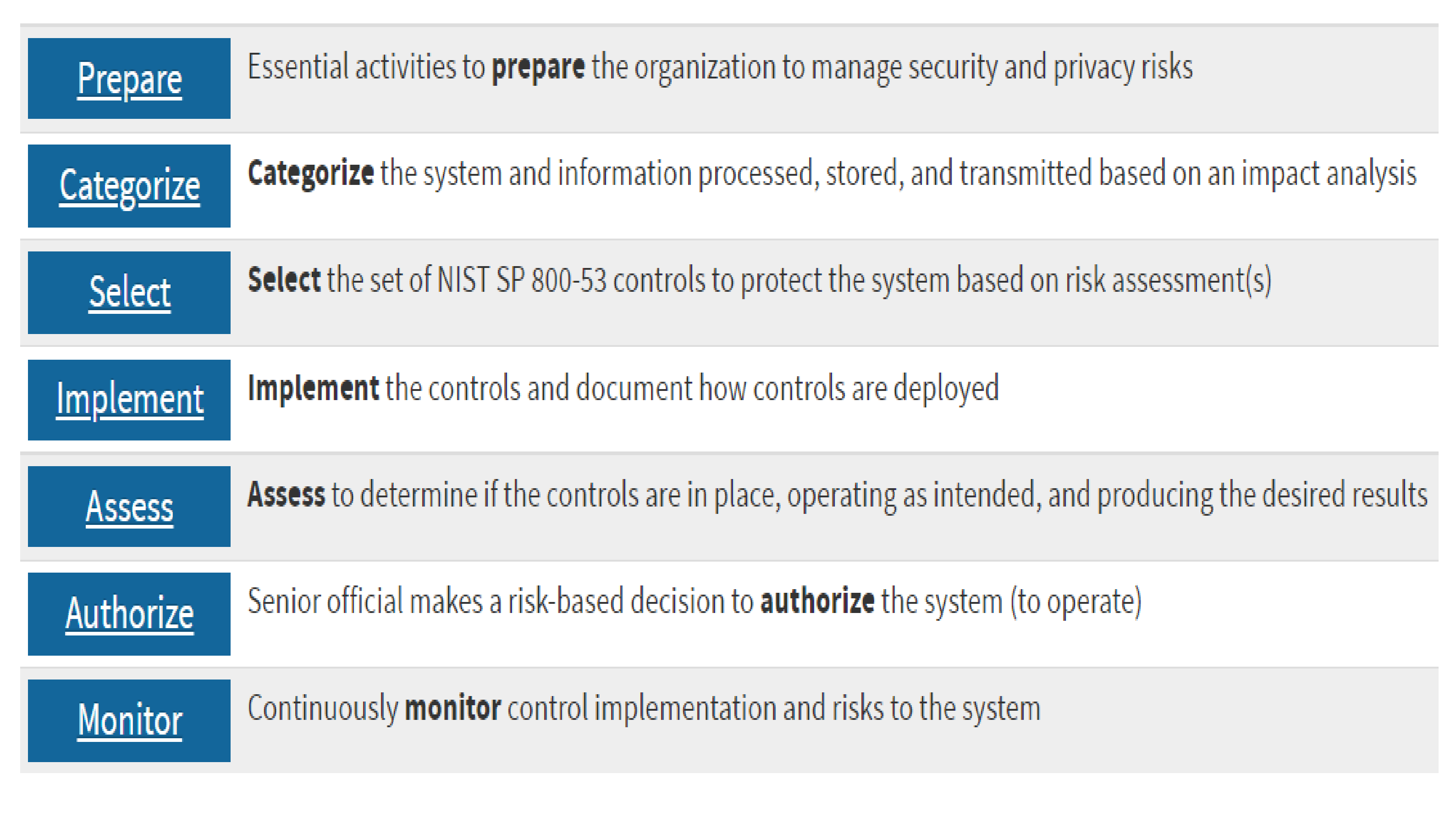
The Fast Track Authorization to Operate (ATO) allows the AO to make an authorization decision based on the review of

- a Cybersecurity Baseline,
- a Threat-Risk Assessment (e.g. penetration test), and
- an Information System Continuous Monitoring Strategy.

Let’s start at the beginning:
Risk Management Framework (RMF)

- The Risk Management Framework (RMF) is criteria that describe processes for the architecture, security and monitoring of United States government IT systems.
- Created by the Department of Defense, the RMF was adopted by all US federal information systems in 2010. The RMF has been documented by the National Institute of Standards and Technology (NIST) and it serves as the foundation for federal data security strategy.
- RMF requires secure data governance systems and performance of threat modeling to identify cyber risk areas.

RMF Steps



Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

Fast Track accelerates RMF steps "Select" through "Authorize" by focusing on operationally relevant risk identification, and ensuring threat-informed risk assessments for DAF systems and missions. The objective being the integration of the Acquisition, Test, and Operations communities in assessing and determining system and mission risk to better inform mission owners.

Additionally, Fast Track ATO is for managing risk for the life-cycle of a system; not a one and done. **The job does not end when the ATO is issued, it only begins…**

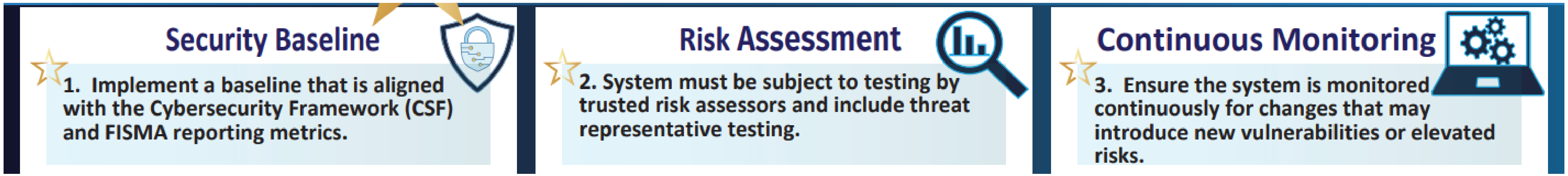
What is an Authorization to Operate?

An ATO is 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.

ATOs often have conditions and assumptions, which must be continuously monitored by the Program Office which applied for the ATO.

What is a Fast Track ATO?

Fast Track demonstrates the cyber risk management process can be based on solid foundational systems engineering, by treating cyber risks equal to other program risks.



Security Baseline

1. Implement a baseline that is aligned with the Cybersecurity Framework (CSF) and FISMA reporting metrics.

Risk Assessment

2. System must be subject to testing by trusted risk assessors and include threat representative testing.

Continuous Monitoring

3. Ensure the system is monitored continuously for changes that may introduce new vulnerabilities or elevated risks.

Fast Track outlines the requirements and testing methodology to move toward operationally informed risk management.

Do I need an ATO?

Maybe not…

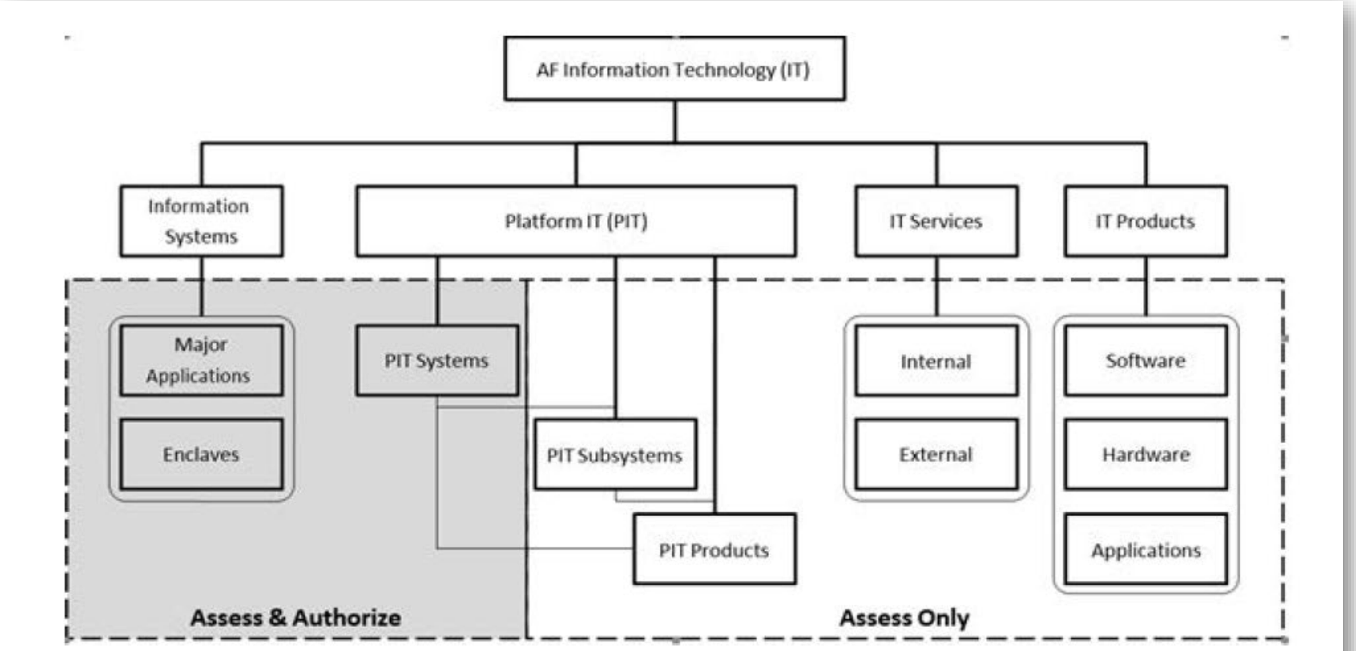


Figure 1: DAF Information Technology (IT)

Reference: AFI 17-101, Fig.1.1. DAF IT Categories

If the Program is proposing an internal or external IS service, such as a web-based application or SaaS, the AO will decide

IT below the system level (Single Purpose IT Products or Devices, PIT Subsystems, PIT Products, IT Products, and IT Services) **or** if the IS in an internal or external IS service, the AO has discretion to simply approve for use.

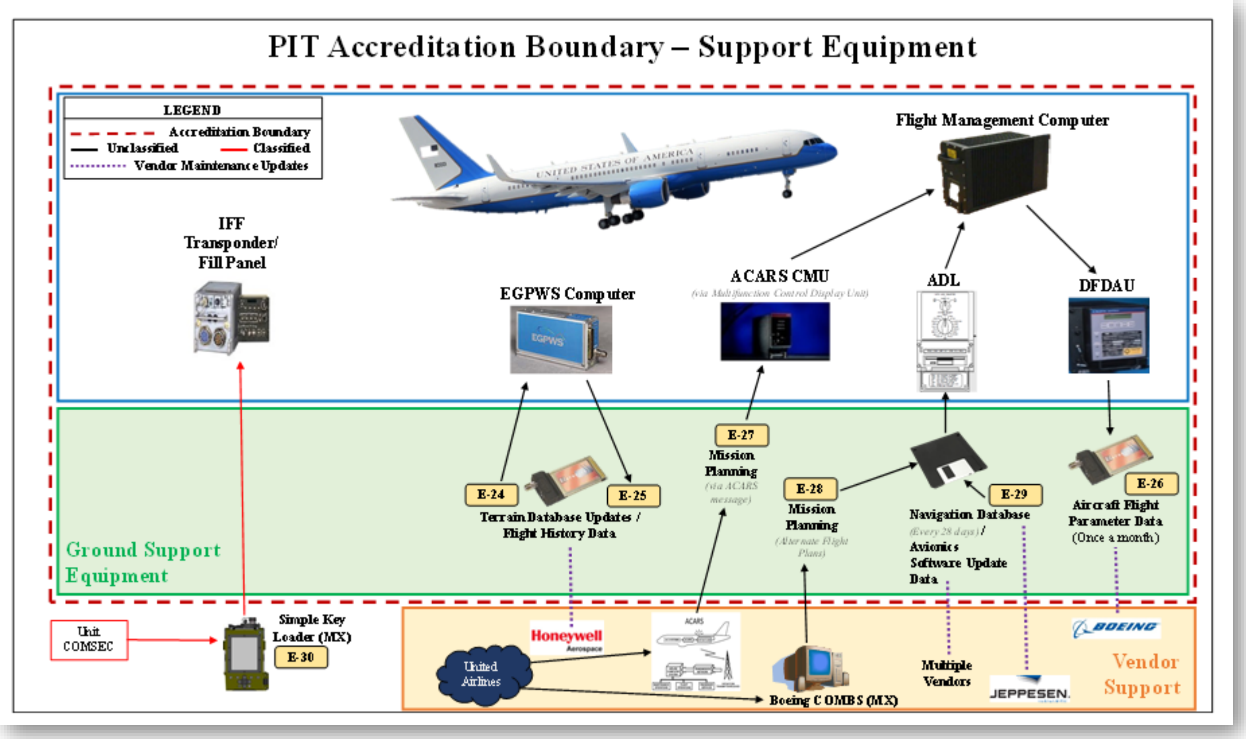
How do I get an ATO?

An ATO is a relationship between a DAF Program Office and the Authorizing Official (AO).

The Program Office is an DAF program of record, which has leadership and resources, such as cybersecurity resources, which can accept and manage the risk outlined to operations within the ATO. Fast Track relies upon AOs, Program Information System Owners (ISOs), Program Managers (PMs), Program Information System Security Managers (ISSMs), and Wing Information Assurance staffs. **The ATO process carries a cost of time and contracts ($) for Penetration Testing, when appropriate; the Program Office will decide if the cost is warranted.**

The AO is a very senior DAF cyber leader. After reviewing the security authorization documentation, the AO formally accepts or rejects risk by authorizing the IT through an interim authority to test, authorization to operate, authorization to operate with conditions, or a denial of authorization to operate.

Where does the vendor come in? AO Determination Brief



- What is the System? What does it do? CONOPS? Missions?
- What is the System Architecture?
- List of Hardware (LRU), Software and providence of each (e.g., supply chain); identification of Critical Program Information (CPI), Critical Components (CC); Technical Orders, Operational Procedures.
- Identification of technologies being used.
- Identification of all external communications access points.
- How does data flow into, through, and out of the system? What type of data is it? How is it protected? Where does it come from? Where does it go? What is it used for?
- What threat/intel information is available?

Where do Airmen/Guardians go to Start the Fast Track ATO Process?

Start with your Program Office

Visit your Program Office FOG to speak to your Program Information System Owner or Program Manager

Not Sure of Your Program Office...

Ask for your Wing Cyber Security Advisor at your IT HELP DESK

What is about a continuous ATO?

Platform One is an accredited, approved, and authorized DoD Enterprise DevSecOps baseline. This authorization includes managed services hosted within Cloud One, approved on-premise environments, and various classified cloud service environments.

Additionally, Platform One has satisfied the Continuous Authority to Operate (cATO) requirements of its Designated DAF AO and the DAF DCIO. The team has undergone intense scrutiny to achieve a cATO, as defined by the Office of the DAF DCIO, and is able to onboard new development teams that can deliver accredited applications to warfighters within weeks. We need this kind of agility to underpin our future competitive advantage and accelerated change.

More info at https://software.af.mil/

References

- DAF Risk Management Framework: https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf
- Fast Track ATO: https://www.fedscoop.com/fast-track-ato-air-force-wanda-jones-heath/

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions at https://www.safcn.af.mil/Contact-Us/
  - Daily Office Hours for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!
  - **Every Tuesday,** 1pm Eastern dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything.