DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE UNDER SECRETARY

MAR 1 8 2019

MEMORANDUM FOR AUTHORIZING OFFICIALS

FROM: SAF/CN
       1800 Air Force Pentagon
       Washington, DC 20330-1800

SUBJECT: Fast-Track Authorization to Operate (ATO)

1. The ATO approval process under Risk Management Framework in the Air Force to date is very resource-intensive and does not keep pace with cyber threats. While the Authorization to Operate 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. To improve our ability to support the warfighter with rapid and innovative capabilities, I am adding *"Fast-Track ATO"* as a pathway within AF Risk Management Framework to obtain an Authorization to Operate.

2. The *Fast-Track ATO* process (aka *Fast Track*) allows Authorizing Officials the discretion to make an authorization decision based on review of the combination of a Cybersecurity Baseline, an Assessment (e.g. Penetration Test), and an Information Systems Continuous Monitoring Strategy. A fundamental tenet of this *Fast-Track ATO* process is the Authorizing Official will make operationally informed risk management decisions. Authorizing Officials are expected to make these decisions by working closely with Information Systems Owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment. Use cases for *Fast Track* include applications developed for deployment to secured cloud infrastructure, and Authorizing Officials may consider other applicability as well; systems that have not "baked security in" to the system design and are not prepared to endure a strong penetration test, are not good candidates for *Fast-Track*.

3. The *Fast-Track ATO Process Overview* (Attachment 1) outlines additional implementation guidance. As required by AFI 17-110, systems pursuing *Fast Track ATO* must still register in the Information Technology Investment Portfolio System (ITIPS). Systems will also be registered in the Authorizing Official's system of record, usually Enterprise Mission Assurance Support Service, to maintain cybersecurity documentation. As an example, if an Authorizing Official used a Decision Brief like the sample in Attachment 2, the brief would be uploaded in Enterprise Mission Assurance Support Service to historically document the decision. Systems following the *Fast Track* process for which the Authorizing Official's team assesses an overall as high or very high risk will still require SAF/CN approval for an Authorization to Operate.

4. *Fast Track ATO* process is now one of the three current pathways to an Authorization to Operate in the Air Force, and it is available for Authorization Officials and Information System Owners who jointly wish to use it. For system, process, or skillset that do not indicate *Fast Track ATO* as the best pathway, the original Risk Management Framework (RMF) pathway remains

available. The *Operational Risk Tolerance Baseline* is an authorized, <u>phased approach</u> of the original pathway. The combination of original RMF and phased Operational Risk Tolerance Baseline are known as *RMF Now*. The third authorized pathway is "*Ongoing Authorization.*" Also known as "*Continuous ATO,*" *Ongoing Authorization* is for organizations building software by agile software Development Secure Operations processes, and it allows the Authorizing Official to authorize the Development Secure Operations <u>process</u> instead of each release of the <u>product</u>.

RMF NOW

(1) The process and procedures to implement the <u>AF Organizational Risk Tolerance Baseline (ORTB)</u>
(2) <u>Collaboration</u> with AF Stake Holders with the focus on:

- Governance
- Documentation
- Culture & Communication
- Control Standards
- Automation
- Prepare Activities IAW NIST SP 800-37 Rev 2

FAST TRACK ATO

(1) Shifts focus from the historically front end compliance/documentation generation to the validation of cyber resiliency

(2) Leverages threat representative adversarial assessments to replicate real-world threats to the system or device

(3) Provides Authorizing Officials the ability to accept risk based on mission performance in an operationally relevant environment

Ongoing Authorization

(1) Process combining software security into the agile software development methodology so that the ATO assessment process is done alongside development

(2) Leverages NIST 800-37 Rev 2 and NIST Supplemental Guidance on Ongoing Authorization

(3) Initial assessment performed on agile development software development process with follow-on risk determinations and risk acceptance decisions based on assessment plan results

Figure 1: Pathways to Authorization to Operate (ATO) in AF's RMF

5. We look forward to feedback on the *Fast Track ATO* or other processes in support of continuing to improve cybersecurity and its risk management. Per AFI 17-101, *Risk Management Framework for Air Force Information Technology*, policy updates (including this and future versions) are posted to the AF Component Workspace in the DoD Knowledge Service (KS) at https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce.

6. If you have questions or concerns, please contact the AF CISO Risk Management Division at usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil.

WILLIAM E. MARION II, SES, SAF
Deputy Chief Information Officer

2 Attachments:
1. Fast Track ATO Process Overview
2. Sample AO Decision Brief-Fast Track ATO