OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Continuous Authorization To Operate (cATO)

The Risk Management Framework (RMF) establishes the continuous management of system cybersecurity risk. Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached. Efforts in the Department are attempting to emphasize the continuous monitoring step of RMF to allow for continuous authorization (cATO). Real-time or near real-time data analytics for reporting security events is essential to achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces. The purpose of this memo is to provide specific guidance on the necessary steps to allow systems to operate under a cATO state.

cATO represents a challenging but necessary enhancement of our cyber risk approach in order to accelerate innovation while outpacing expanding cybersecurity threats. In order to achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies: On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of an approved DevSecOps reference design.

Continuous Monitoring (CONMON)

RMF requires a CONMON strategy for each system. This strategy describes how the System Owner, in coordination with Service Providers, will continuously monitor and assess all of the security controls within the information system's security baseline, including common controls. The specific plan will vary based on component monitoring infrastructure, the specific technologies used by the system, and the application of the system. Automated monitoring should be as near real time as feasible. Manual controls will have different timelines associated, but must be included in the overall monitoring strategy. It is critical that System Owners in coordination with Service Providers demonstrate the ability to effectively integrate the automation and monitoring of all security controls prior to entering into a cATO status.

Systems are rarely produced or deployed as a singular system; they operate as a system of systems. The goal of a cATO is to formalize and monitor the connections across these systems of systems to deliver cyber resilient capabilities to warfighters at the speed of relevance. CONMON requires the AO have the ability to monitor the cumulative set of security controls that span the AO's area of responsibility (AOR) in order to make real time risk decisions. The AO must approve, support and manage an organization's CONMON plan for all applications.

For cATO, all security controls will need to be fed into a system level dashboard view, providing a real time and robust mechanism for AOs to view the environment. Using this information, the AO will be better positioned to make real time and informed risk decisions as to

the threat level posed to the system. This view will also enable defensive cyber operations elements to conduct response actions based on current system posture.

Active Cyber Defense

Active cyber defense is the ability to respond to cyber threats in real, or near real time. As the Department adopts a data centric model, so too must our cyber defenses. The focus should be on using threat driven dashboards and metrics to establish patterns and discern threats before they are able to wreak havoc on DoD domains.

Simply conducting scans and patching does not meet the threshold for active cyber defense. Systems must be able to show a real, or near real time ability to deploy appropriate countermeasures to thwart cyber adversaries. AO's/AODR's must be in constant communications with the various cyber operational components, including Cybersecurity Service Providers (CSSP), component cyber operations forces, JFHQ-DoDIN, and United States Cyber Command. These communication channels are essential to ensuring operations within each system boundary rapidly ingest cyber threat intelligence and take appropriate actions. These communications will also serve to share indicators that may prevent intrusions in other DoD environments.

Secure Software Supply Chain

The number of components required to build, deploy, operate, and secure modern systems continues to expand rapidly, where underlying software architectures and deployment topologies have moved well beyond a single binary installed from physical media. These advancements are too often invisible to the end-user, where modern software applications are backed by an array of additional network services that include remote configuration updates, advanced analytics, artificial intelligence (AI)-powered rulesets that update cyber defense systems automatically, etc. As the Department's operations become increasingly dependent on software, we must ensure that this software is created in a secure, protected, and controlled environment that instills confidence in the user base that it will perform as designed. In order to prevent any combination of human errors, supply chain interdictions, unintended code, and support the creation of a software bill of materials (SBOM), the adoption of an approved software platform and development pipeline(s) are critical.

To achieve a cATO, a system must embrace the DoD Enterprise DevSecOps Strategy, aligning to an approved DevSecOps Reference Design. This strategy creates a cultural change that implements the full and open agile collaboration of what have traditionally been separate disciplines. Incorporating development, security, and operations together closes gaps with baked-in safeguards and monitoring functions that span the entire software supply chain. Specifics on the current DoD Enterprise DevSecOps Strategy and approved Reference Designs can be found here: https://DoDcio.defense.gov/Library/. The DevSecOps Strategy supports a "Pathway to a Reference Design" whereby new architectures can be submitted for evaluation.

cATO Issuance

If an AO determines their system provides the required real time risk posture to achieve a cATO, the AO will notify the component CISO of the intention to move that system to a cATO status. Together the AO and component CISO will present this request and the supporting body of evidence to the DoD CISO for consideration. Systems desiring to move from a traditional ATO model to a cATO model must demonstrate: complete understanding of activities inside of

their AO boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of a specific DoD Enterprise DevSecOps Reference Design.

DoD CISO approved cATOs do not have an expiration date and will remain in effect as long as the required real time risk posture is maintained. The cATO determination does not affect the underlying system ATO. Rather, it modifies requirements for re-authorizing that system's ATO. cATOs are a privilege and represent the gold standard for cybersecurity risk management for systems. They represent a raise the bar effort for system risk monitoring and management.

Shortly following this memo DoD CIO-CS will coordinate and publish guidance on the implementation and evaluation of reaching a cATO state. Published cATO guidance is intended to be agile as threats mature so cATO evaluation criteria will also be updated to outpace the threats we face. DoD CIO will iterate with the community to ensure that guidance is up to date and commensurate with cybersecurity best practices.

Maintenance

The approval of cATO does not guarantee a system will stay in that state, systems that have been granted permission to operate under a cATO may have this revoked for several reasons. This may include, but is not limited to: poor cybersecurity posture as identified through continuous monitoring or external assessments; changes in risk tolerance; or a cybersecurity incident resulting from poor adherence to cybersecurity practices. A system can temporarily lose its cATO privilege without any loss of existing ATO.

Evolving guidance and related resources will be published on the RMF Knowledge Service at https://rmfks.osd.mil. The DoD CIO point of contact is Tyler Gesling at tyler.d.gesling.civ@mail.mil or McKay Tolboe at mckay.r.tolboe.civ@mail.mil.

MCKEOWN.DAVID.W.1034948050

Digitally signed by MCKEOWN.DAVID.W.1034948050
Date: 2022.02.02 08:30:52 -05'00'

David W. McKeown
DoD Senior Information Security Officer (SISO)