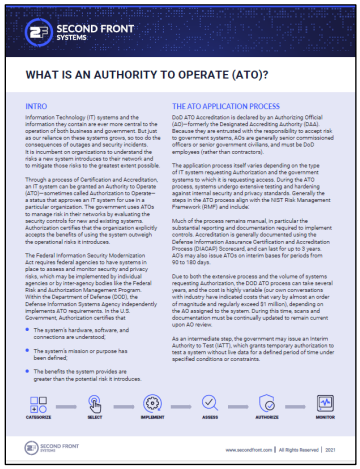

What is an Authority to Operate?

Thank you for downloading this SecondFront Solutions Brief. Carahsoft is the distributor for SecondFront DevSecOps solutions available via NASA SEWP V, and other contract vehicles.

To learn how to take the next step toward acquiring SecondFront's solutions, please check out the following resources and information:

For additional resources:
carah.io/SecondFrontResources

For upcoming events:
carah.io/xxxx (This microsite is created yet)

For additional SecondFront solutions:
carah.io/SecondFront

For additional DevSecOps solutions:
carah.io/DevSecOpSolutions

To set up a meeting:
SecondFront@carahsoft.com
703-230-7425

To purchase, check out the contract vehicles available for procurement:
carah.io/SecondFrontContracts

For more information, contact Carahsoft or our reseller partners:
secondfront@carahsoft.com | 703-230-7425

SECOND FRONT SYSTEMS

WHAT IS AN AUTHORITY TO OPERATE (ATO)?

INTRO

Information Technology (IT) systems and the information they contain are ever more central to the operation of both business and government. But just as our reliance on these systems grows, so too do the consequences of outages and security incidents. It is incumbent on organizations to understand the risks a new system introduces to their network and to mitigate those risks to the greatest extent possible.

Through a process of Certification and Accreditation, an IT system can be granted an Authority to Operate (ATO)—sometimes called Authorization to Operate—a status that approves an IT system for use in a particular organization. The government uses ATOs to manage risk in their networks by evaluating the security controls for new and existing systems. Authorization certifies that the organization explicitly accepts the benefits of using the system outweigh the operational risks it introduces.

The Federal Information Security Modernization Act requires federal agencies to have systems in place to assess and monitor security and privacy risks, which may be implemented by individual agencies or by inter-agency bodies like the Federal Risk and Authorization Management Program. Within the Department of Defense (DOD), the Defense Information Systems Agency independently implements ATO requirements. In the U.S. Government, Authorization certifies that

- The system's hardware, software, and connections are understood;
- The system's mission or purpose has been defined;
- The benefits the system provides are greater than the potential risk it introduces.

THE ATO APPLICATION PROCESS

DoD ATO Accreditation is declared by an Authorizing Official (AO)—formerly the Designated Accrediting Authority (DAA). Because they are entrusted with the responsibility to accept risk to government systems, AOs are generally senior commissioned officers or senior government civilians, and must be DoD employees (rather than contractors).

The application process itself varies depending on the type of IT system requesting Authorization and the government systems to which it is requesting access. During the ATO process, systems undergo extensive testing and hardening against internal security and privacy standards. Generally the steps in the ATO process align with the NIST Risk Management Framework (RMF) and include:

Much of the process remains manual, in particular the substantial reporting and documentation required to implement controls. Accreditation is generally documented using the Defense Information Assurance Certification and Accreditation Process (DIACAP) Scorecard, and can last for up to 3 years. AO's may also issue ATOs on interim bases for periods from 90 to 180 days.

Due to both the extensive process and the volume of systems requesting Authorization, the DOD ATO process can take several years, and the cost is highly variable (our own conversations with industry have indicated costs that vary by almost an order of magnitude and regularly exceed $1 million), depending on the AO assigned to the system. During this time, scans and documentation must be continually updated to remain current upon AO review.

As an intermediate step, the government may issue an Interim Authority to Test (IATT), which grants temporary authorization to test a system without live data for a defined period of time under specified conditions or constraints.

WHAT HAPPENS AFTER ACCREDITATION?

Accreditation is not the finish line for an IT system. Once the risks have been assessed and the system authorized, careful and continuous monitoring is key to maintaining confidence in a system and its controls. This includes incident response and management, as well as change management, all governed by documentation submitted as part of the ATO package. When a current ATO nears its expiration—usually after 3 years—it requires renewal.

As an intermediate step, the government may issue an Interim Authority to Test (IATT), which grants temporary authorization to test a system without live data for a defined period of time under specified conditions or constraints.

SOFTWARE RISK MANAGEMENT AND ASSURANCE IN INDUSTRY

Private companies and organizations must also concern themselves with their suppliers' software assurance practices. There are multiple sets of standards and certifications organizations can require their vendors implement prior to introducing software into their networks.

However, some such certifications—such as the Common Criteria [ISO 15408]—are subject to similar critiques as ATOs, specifically that they involve a large upfront investment from vendors that does not necessarily result in a more secure product. The Common Criteria also focuses on product security features rather than the development process.

Despite the absence of universal standards, there are emerging best practices for review during a supplier assessment by an organization with a mature assurance process. These practices, which tend to be most mature within large organizations in certain fields such as medical equipment and finance, include review of:

- Secure development and integration practices
- Product security governance
- Vulnerability response processes.

Secure development and integration practices include frameworks such as DevSecOps, a "secure by design" approach that introduces security as a foundational principle rather than an afterthought. In response to the practice of "shifting left," or moving security upstream in the development process, the government has begun offering continuous ATOs (cATOs), which involve the continuous authorization of software by building security into the development lifecycle, ensuring that all application elements meet or exceed ATO security requirements

THE BOTTOM LINE

For companies with dual-use software products—those with both civilian and military applications—an ATO can be a significant barrier to entry to the government market. The variable cost and extended timeline often prove fatal to startups targeting DOD customers, which has implications far beyond those companies. By limiting the ecosystem of software available to the government to only products from companies that can accept high initial costs and long time horizons, the government misses out on innovative solutions from non-traditional players, like startups. Fast Track ATOs—which use a streamlined approach to achieve accreditation more quickly—can help mitigate these challenges, but this option is not always available as it depends on branch leadership and different AO's preferred procedures.

While the ATO process is imperfect, it currently provides the most systematic way for the government to manage risk within its information systems—an essential function in this increasingly complex cyber risk environment.