

Memorandum

Accelerating Secure Software

April 24, 2025

Overview

On April 24, 2025, Acting Chief Information Officer for the DoW Katie Arrington signed the [memo](#) titled “Accelerating Secure Software” which established the Software Fast Track (SWFT) initiative for the department. This initiative will reform the way the DoD acquires, tests, and authorizes secure software as well as further the goals of the memo “Directing Modern Software Acquisition to Maximize Lethality”. SWFT will utilize AI to replace the legacy Authority to Operate (ATO) and Risk Management Framework (RMF) processes when buying new software.

The initiative directs the OCIO to undertake a **90-day sprint** to define clear and specific:

- Cybersecurity and SCRM requirements
- Rigorous software security verification processes
- Secure information sharing mechanisms
- Federal government-led risk determinations to expedite cybersecurity authorizations

Software Fast Track (SWFT)

Three RFIs were posted to gather market information and capabilities in accelerating secure software delivery for the Federal Government. These RFIs encompass the following capabilities:

- [Software Fast Track \(SWFT\) Tools](#)
- [Software Fast Track \(SWFT\) External Assessment Methodologies](#)
- [Software Fast Track \(SWFT\) Automation & Artificial Intelligence](#)

These RFI’s gathered information from industry regarding:

- External assessment methodologies and streamlined risk assessment and authorization processes for software-enabled products and services
- Software supply chain security tools have already been developed and are in use
- How automation and artificial intelligence can support the government’s objective to accelerate secure software adoption

Implications for Industry

For vendors working with the Department of War, new security standards and processes will take place. With the SWFT program initiated, vendors need to:

- Be aware of new security authorizations outside of the traditional ATO and RMF framework
- Respond and understand information developed from the three RFI’s released with this memo
- Adapt and update their security postures to align with the new goals of SWFT

Vendors should be aware of new developments regarding SWFT as the associated implementation plan as well as understand the FY25-26 Software Modernization Implementation Plan as many of the goals pursued by this order can be found there.

Implications for Government

This new pathway provides new avenues for government. Defense departments looking to procure secure technologies will no longer follow the ATO and RMF process and follow this streamlined SWFT pathway.

Defense departments will also need to work with vendors on updating their security postures and aligning with this framework as well as understanding how AI will be used to maintain and streamline their security standards.

Timeline

Policy	Key Dates	Focus & Key Provisions
Federal Information Security Modernization Act	December 18, 2014	Established the ATO process which requires a Designated Approving Authority (DAA) that grants permission for an IT system or product to operate with other existing systems or networks after testing.
NIST SP 800-37 Rev. 2	December, 2018	Established the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations
DoD Instruction 5000.87	October 2, 2020	Establishes policy, assigns responsibilities, and prescribes procedures for the establishment of software acquisition pathways to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software.
Memo: Directing Modern Software Acquisition to Maximize Lethality	March 6, 2025	Directs DoW services and agencies to adopt the Software Acquisition Pathway (SWP) as the preferred pathway for software development components.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:

To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.

