

Army Software Updates

The Army is overhauling how it buys software, shifting away from custom-built military products toward commercial solutions in an effort to speed up delivery to soldiers.

Army Secretary Dan Driscoll's directive, dated July 22 and published last week, rescinds Army Directive 2024-02 and replaces it with new guidance. The policy directs the Army to rely on commercial companies adapting their existing products rather than purchasing products custom-built for military needs. It follows Defense Secretary Pete Hegseth's push to reform Pentagon acquisition to deliver weapons and business systems "at speed and scale," and cites executive orders on modernizing defense acquisition and ensuring cost-effective commercial solutions.

The directive makes the Software Acquisition Pathway mandatory for all software development efforts, including mixed efforts that involve software development. Program managers currently using other pathways must transition at their next major decision point. Under the policy, program managers must consider commercial solutions first, then configured commercial solutions. Custom development, the memo states, "should be extremely rare and will be authorized only when no commercial solution can meet a significant portion of operational needs." When a product has applications beyond a single use case, contracting officers are to use Army enterprise software contracts.

Under the new approach, the Army will default to Commercial Solutions Openings (CSOs) and other transaction authorities (OTAs) as its standard solicitation and award methods. These have typically served as backup options. Traditional acquisitions set prescriptive requirements, vet proposals over months or years, and delay deployment until all features are ready. By contrast, CSOs begin with a five-page concept paper, followed by discussions with the bidder and a demonstration or pilot project.

The directive also instructs test organizations to use automated testing and, when feasible, accept vendor test data and conduct testing in parallel with development. Army cybersecurity organizations are directed to implement continuous authority to operate (cATO) processes and accept reciprocity across Army organizations.

The Assistant Secretary of the Army for Acquisition, Logistics and Technology is the proponent for the policy and will incorporate its provisions into a new Army regulation within two years. The directive remains in effect until that regulation is published.