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

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Software Development, Security, and Operations for Software Agility

Reference: (a) DoD Enterprise DevSecOps Reference Design, August 12, 2019
(b) Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage, Defense Innovation Board, May 3, 2019

In the 2019 Digital Modernization Strategy, the Department outlined numerous goals and objectives to improve information technology (IT) to increase our military advantage across all spectrums. One of the goals identified was to pursue the use of Software Development (Dev), Security (Sec), and Operations (Ops) or DevSecOps, as a software development methodology. The use of this commercial best practice will support the Department's efforts to ensure better utilization of Artificial Intelligence and Cloud Environments. Reference (a) is the Department's approved DevSecOps Reference Design Document outlining the preferred software practice for all Department of Defense (DoD) components to rapidly provide software agility "at the speed of operations". The Reference Design Document provides implementation and operational guidance to IT capability providers, IT capability consumers, application teams, and Authorizing Officials.

The current approach to software development is less than optimal and is increasingly a long-term risk to the Department's competitive military advantage. Current software development takes too long, is expensive, and exposes warfighters to unacceptable risk by delaying access to tools needed to ensure mission success. That assessment is consistent with the DoD internal analysis and multiple external reviews conducted over the years including the Defense Innovation Board. Adoption of the DevSecOps approach can enable a more effective joint force, strengthen our ability to work with allies, and improve the business processes of the DoD enterprise (reference (b)).

To broaden the use of this DevSecOps Reference Design, the DoD Chief Information Officer (CIO) and the Under Secretary of Defense for Acquisition and Sustainment (USD (A&S)) are engaging Department Authorizing Officials (AO) and cyber assessment communities to establish a framework to accept authority to operate (ATO) inheritance from the cloud, reciprocity from shared hardened containers, and the output of the continuous monitoring tools. Mature DevSecOps practices will lead to "continuous ATOs" for software and the underlying infrastructure. The DevSecOps Reference Design v1.0 is currently available at: https://www.milsuite.mil/book/groups/dod-enterprise-devsecops/.

The DoD CIO point of contact (POC) is Mr. Tom Lam, (571) 372-4686, or ngoan.t.lam.civ@mail.mil. The OUSD (A&S) POC is Dr. Jeff Boleng, (703) 571-9029, or jeffrey.l.boleng.civ@mail.mil.

Dana Deasy
Department of Defense Chief Information Officer

Ellen Lord
Undersecretary of Defense
for Acquisition and Sustainment