DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAY 2 2 2020

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
COMMANDANT OF THE UNITED STATES COAST GUARD
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
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: Designation of Enterprise Service Provider for DevSecOps

References: (a) DoD Chief Information Officer Memorandum, "Software Development, Security, and Operations for Software Agility," October 24, 2019
(b) Under Secretary of Defense for Acquisition and Sustainment Memorandum, "Software Acquisition Pathway Interim Policy and Procedures," January 3, 2020

Digital modernization is the cornerstone for advancing the Department's competitive advantage in a growing global threat and great power competition environment. Modernizing how we develop software to align with best commercial practices offers opportunities to speed the delivery of new capability to warfighters while simultaneously improving cybersecurity. Modernization of the Department's software development processes is a Department-wide effort encompassing both technical and non-technical factors. One critical technical component is the widespread adoption of a DevSecOps methodology for new software development. Per Reference (a), DevSecOps is an industry best practice for rapid, secure software development to unify software development, security, and operations. Likewise, the DoD Digital Modernization Strategy promotes DevSecOps as a key goal.

One limiting factor impacting the adoption of the DevSecOps methodology is lack of access to existing, accredited, and supported infrastructure. To accelerate progress and encourage a shared services model across the Department, the Office of the DoD Chief Information Officer (CIO) will begin to identify and endorse well-supported DevSecOps implementations that have existing security accreditations and are capable of supporting a broad user base. To that end, this memorandum recognizes the Air Force, Office of the Chief Software Officer, Platform One, as one of the DoD Enterprise Service Providers for DevSecOps. The initial portfolio of services is described in the attachment and is maintained at https://software.af.mil/dsop/services/.

Given the emerging nature of these technologies and the wide variety of requirements across DoD, the use of DoD Enterprise Service Providers for DevSecOps is not mandated. Per guidance in Reference (b), the Software Acquisition Pathway, these enterprise services should be leveraged "as a first choice, if available, before creating unique services."

To support DevSecOps technology and processes as they continue to mature, the Deputy CIO for the Information Enterprise will form a DevSecOps Senior Steering Group to oversee this portfolio in partnership with the Under Secretary of Defense for Acquisition & Sustainment. DoD Components interested in participating should contact OSD.DevSecOps@mail.mil to identify their representatives.

The DoD CIO point of contact for this effort is Dan Risacher at 571-402-5275 or daniel.r.risacher.civ@mail.mil, and the U.S. Air Force point of contact is Nicolas M. Chaillan at 703-693-4740 or usaf.cso@mail.mil.

for Dana Deasy

Attachments:
As stated

Attachment 1

Air Force-Provided DoD Enterprise Services for DevSecOps

To access the latest DoD Enterprise DevSecOps Services documentation provided by the Air Force, please visit: https://software.af.mil/dsop/services/.

DoD Centralized Container Source Code Repository (DCCSCR/Repo One)

The DCCSCR is the central repository for the source code to create hardened and evaluated containers for the Department of Defense. It also includes various open-source products and infrastructure-as-code used to harden Kubernetes distributions. DCCSCR is currently operated at https://repo1.dsop.io/dsop/.

All DoD activities that are creating containers that could benefit the DoD at an enterprise scale should publish their containers' source code in the DCCSCR by following the DoD Enterprise DevSecOps Ref Design, Container On-boarding guide, and Container Hardening guide requirements. These documents are available at https://software.af.mil/dsop/documents/.

All programs should evaluate any existing containers for reuse before creating a new container image.

DoD Centralized Artifacts Repository (DCAR/Iron Bank)

The DCAR is the DoD repository of digitally signed, binary container images that have been hardened according to the Container Hardening Guide coming from the DCCSCR. Containers accredited in the DCAR have DoD-wide reciprocity across classifications. DCAR is currently operated at https://dcar.dsop.io/.

Prior to creating a new container image, DoD programs should check if the container images already exists in DCAR and use the DoD signed containers whenever possible.

DevSecOps Platform (DSOP)

The DSOP is a collection of approved, hardened Cloud Native Computer Foundation (CNCF)-compliant Kubernetes distributions, infrastructure as code playbooks, and hardened containers that can be used to implement a DevSecOps platform compliant with the DoD Enterprise DevSecOps Reference Design, and its source code is hosted on the DCCSCR.

The DSOP includes the various containers included in the Reference Design including Elasticsearch, Fluentd, and Kibana (EFK), Sidecar Container Security Stack (SCSS), etc.

Teams should leverage the Infrastructure as Code (IaC) available on the DCCSCR whenever possible and contribute back their code improvements to the DCCSCR whenever applicable.

Platform One Enterprise Services

Platform One provides additional pay-per-use services and contract vehicles to facilitate teams' adoption and move to DevSecOps. The list of provided services is expected to continue to evolve and is located at https://software.af.mil/dsop/services/.

- Platform One Shared Enterprise Environments (for Development, Test and Production)
- Platform One Dedicated Continuous Integration / Continuous Delivery (CI/CD) Options
- Platform One Cybersecurity/Pen-testing Services:
- Platform One Custom Development Services
- Platform One DevSecOps Managed Tools
- Platform One Training/On-Boarding Options