Hello, friends and colleagues!

The Fiscal Year 2019 National Defense Authorization Act was signed by the President on Aug. 13, with many provisions reflecting the relevance of DISA's mission: DOD Information Network operations for the joint warfighter … and our workforce remains committed to making it happen, each and every day.

I appreciate your support as DISA continues to earn your trust, meet your specific mission needs, and ensure the readiness and lethality of the DOD as a whole.

This newsletter highlights just a few of the ways we are doing that. This month, I have updates regarding our unclassified mobility offerings and the work we are doing to migrate DOD 'fourth estate' organizations' applications to the milCloud 2.0 service. I am also pleased to invite those in the endpoint security community to participate in an upcoming event regarding the way forward for our services in that realm.

I encourage you to disseminate this information across your organization and to provide your feedback to the Mission Partner Engagement Team or the DISA field office or liaison officer in your area of responsibility.

DOD Mobility Unclassified Capability now available to organizations not using DOD Enterprise Email

- One of the most significant announcements we made over the course of the summer is that our unclassified mobile device management service is now available to all Department of Defense (DOD) mission partners, services, agencies, and field activities. Previously, only mission partners who purchased the agency's DOD Enterprise Email (DEE) service were able to utilize the DISA-managed DOD Mobility Unclassified Capability (DMUC).
- Why the change? As DISA strives to become the trusted provider to connect and protect the warfighter in cyberspace, we must ensure our enterprise services are enabling you, our mission partners, to focus your time and your financial and manpower resources on your core missions.
- Learn more about the DMUC service, which costs only $4.31 per device, per month, by visiting the DOD Mobility User Corner (Common Access Card required).

New Apple device enrollment program reduces provisioning time, increases security

- Another mobility update is the availability of our Apple device enrollment program, available to all mission partners using iOS devices with the DMUC service. This free service allows you to streamline DMUC enrollment, reducing device provisioning time by more than 40 percent and providing additional device management controls to improve the security of this critical capability.
- Using this service, administrators no longer need to physically prepare each device before distributing to users; everything is done through automation, and the device is configured to your organization's standards when the user activates it.
- Devices are inherently more secure because updates are performed or automated by an administrator rather than burdening the end user. The service also assists with the recovery of lost or stolen devices.
- This program is one of many ways DISA continues to expand and improve upon our mobility offerings.

DOD CIO, DISA assist 'fourth estate' with cloud migrations

- In compliance with the DOD chief information officer's May 3 directive, DISA is assisting DOD 'fourth estate' organizations with transitioning computing workloads hosted in their own data centers to DISA's milCloud 2.0 service offering.

- A workshop held this summer provided stakeholders with insight on the transition process, which begins with a visit by a DOD CIO "triage" team. That team helps each organization define their systems and assess which applications are ready to migrate to the cloud and which will require additional rationalization. DISA then helps mission partners with funding requirements and developing security plans and timelines for the move. The agency also provides a standard operating procedure for on-boarding and ongoing migration support.
- As the migrations progress, DISA will continuously share experiences, challenges, and best practices.

Participate in DISA's Endpoint Security Summit Oct. 2

- In recent years, there have been increasing efforts to address gaps in the cybersecurity of DOD endpoint devices. DISA has worked to integrate prevailing endpoint security capabilities and has begun laying the groundwork to modernize endpoint security. Within the last year, in support of DOD chief information officer initiatives, DISA has implemented application whitelisting, continued the evolution of the Windows 10 Secure Host Baseline, and initiated pilots to identify suitable application containment and endpoint detect and response technologies.

- I invite our mission partners to join us in shaping the endpoint security solutions of the future by participating in our Oct 2 Endpoint Security Summit at DISA Headquarters on Fort Meade, Maryland.

- The purpose of this event is to explore the issues, challenges, and considerations faced when protecting the endpoint from the latest threats. Practitioners and subject matter experts will review the current status of endpoint security modernization and secure configuration management, along with the way ahead.

- Register for the summit and join the endpoint security modernization online forum to be a part of the discussion before and after the event.