Greetings!

I was reminded this month that it has been a year since I assumed command of DISA and the Joint Force Headquarters – DOD Information Network (JFHQ-DODIN). It is hard to believe so much time has already passed! I am so proud of our joint accomplishments to support the warfighters and remain passionate to continue the same level of effort going forward. Thank you so much for a great team effort.

In this edition of the newsletter, I will update you on our efforts related to the Joint Regional Security Stacks and endpoint security. Additionally, I will share information regarding the impending transfer of DISA's National Background Investigation Service resources to the Defense Security Service, and invite warrant officers in the signal, communications, and cyber fields to attend a knowledge transfer session this spring.

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.

Joint Regional Security Stacks: We're addressing your concerns -

- The Joint Regional Security Stack (JRSS) program management office (PMO) has been hard at work to remedy mission partner issues identified during operational assessment conducted by the DOD Director of Test and Evaluation in March 2018. Over the past 10 months, the JRSS PMO, in partnership with our Mission Partner Engagement Office, has focused on systematic, active contact with all JRSS mission partners, at strategic and operational levels. These engagements surfaced five primary concerns and challenges related to JRSS: latency, cost, multi-tenancy, performance reliability, and synchronization with base infrastructure.

- This article addresses what DISA is doing to address and mitigate each of those issues. I want to emphasize we are actively listening to and incorporating your feedback. DISA is committed to improving the JRSS operator experience, refining standard operating procedures, and helping the department realize cost savings by eliminating duplication of effort / decommissioning of legacy systems.

Endpoint Security Summit focuses on enterprise modernization

- Earlier this month, DISA hosted an Endpoint Security Summit, which brought together more than 250 subject matter experts, system administrators, analysts, and users to discuss endpoint modernization efforts. The three-day event gave endpoint practitioners and subject matter experts the opportunity to hear from DISA, the DOD Chief Information Officer (CIO), U.S. Cyber Command, and JFHQ-DODIN about policy and operational strategies that will drive change in 2019 and beyond.

- Efforts to modernize endpoint security aim to achieve a more standardized, interoperable, and secure set of capabilities that strengthen integrated threat analysis, defensive actions, and command and control across the DODIN – from boundary to endpoints. You can learn more about the DOD CIO's strategic policy direction, combatant command operational requirements, and service and agency pilot efforts in progress in this article.

National Background Investigation Service to transfer to Defense Security Service

- DISA's National Background Investigation Service (NBIS) will soon fall under the authority, direction, and control of the Director of Defense Security Service (DSS), according to a Jan. 28 memorandum issued by David L. Norquist, who is performing the duties of the Deputy Secretary of Defense. The memorandum directs the move of the NBIS Program Executive Office and subordinate elements, the DoD Consolidated Adjudications Facility (DOD CAF), as well as Joint Service Provider (JSP) personnel providing direct support to the DOD CAF.

- The new alignment supports the transfer of DOD CAF functions, personnel, and associated resources to the DSS, which was mandated by Subsection 925(c) of the National Defense Authorization Act for fiscal year 2018. I am extremely proud of the members of the NBIS and JSP teams and the work they have done to advance the security clearance program for the DOD. I have great confidence they will continue to provide superior support to the department and this critical mission as DSS employees.

Signal, communications, and cyber warrant officers invited to participate in knowledge transfer event April 10-11

- DISA and JFHQ-DODIN will host a knowledge transfer event for signal, communications, and cyber warrant officers (WO1-CW5) from all services at our joint headquarters on Fort George G. Meade, Maryland, April 10-11.

- Attendees will learn about the services DISA provides (e.g., DOD Mobility, milCloud 2.0, Joint Regional Security Stacks, and many more), how JFHQ-DODIN protects the DODIN with support from DOD cyber elements, and what the future holds for both organizations. Registration is required and visit authorization requests must be submitted through the Joint Personnel Adjudication System. Units that send personnel will pay all travel costs and individuals must arrange for lodging and transportation. Additional details are included on the registration site.

We have increased the frequency of our Customer Engagement Forum

- In a continuing effort to enhance collaboration and forge trusted partnerships, DISA's Mission Partner Engagement Office increased the frequency of its customer engagement forum from once per quarter to bi-monthly. The next DCEF will take place Thursday, March 21 from 10:30 to noon EDT. Topics will include: a briefing from the DISN Infrastructure Services Working Group, and Defense Enterprise Office Solutions update, a DISA Storefront and Service Catalog Update, and an overview of DISA's storage as a service offering. To request an invitation and the Defense Collaboration Services URL for the meeting, mission partners should contact disa.meade.bd.mbx.disa-customer-engagement-forum@mail.mil.

I hope to see you at AFCEA TechNet Cyber May 14-16

- DISA will host a number of briefing sessions and an exhibit at AFCEA's TechNet Cyber conference in Baltimore, May 14-16. Topics we will explore in-depth include: the next generation of JRSS, unified capabilities, cloud migration initiatives and cloud storage, multifactor authentication, and big data solutions.