Hello, and happy spring!

The past few months have been a whirlwind, but I wouldn't trade it. It has been a pleasure to speak with so many of you: to better understand your needs, and to hear valuable feedback about the services and capabilities we provide. In addition, the DISA team continues to impress me with their passion for and commitment to our enduring mission in service to our warfighters.

This edition of the newsletter will tell you about a new application that enables the automated completion of DD Form 2875: System Authorization Access Requests and the upgrade of the Defense Information Systems Network (DISN) optical transport system from its current 10 GB per second operational status to a 100 GB per second packet-optical transport system. I also provide an explanation of our Secure Cloud Computing Architecture service offering and invite you to engage with members of the DISA team this month.

I encourage you to disseminate this information within 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.

Automated system authorization access requests

- The DISA Ecosystem Cyber Services Line of Business created an application called System Access Management (SAM), which automates the completion and approval of DD Form 2875: System Authorization Access Requests. SAM enables the request to move through the approval process — requestor, supervisor, security manager, and account creator — within a single day, or even minutes, and eliminates the time-consuming process of completing and routing paper forms.

- We piloted the tool within DISA last month. Approximately 6,000 employees created accounts and requested access to a specific system. The entire process, which included making employees across the globe aware of the requirement to request access, completing access requests, and obtaining all required approvals, and granting access, was completed in only four weeks.

- Mission partners will be able to request access to SAM for both NIPRNet and SIPRNet-based DISA-managed systems this summer. This is one of the many ways we are trying to streamline processes.

- For more information, please read this article.

Defense Information Systems Network upgrade underway

- The ongoing Next Generation Optical Transport project, targeted for completion in fiscal year 2019, will upgrade the Defense Information Systems Network (DISN) optical transport system from its current 10 GB per second operational status to a 100 GB per second packet-optical transport system.

- The result will be a more robust and survivable network infrastructure that supports the ever-growing demand for bandwidth by increasing efficiency, reliability, and capacity. Benefits include improved infrastructure resiliency, service delivery node resiliency, and improved encryption. In addition, legacy components of the DISN will be transitioned to an internet protocol-based Ethernet infrastructure.

An explanation of the Secure Cloud Computing Architecture

- One of the most frequent questions we are asked about our cloud services portfolio is "What is the Secure Cloud Computing Architecture (SCCA)?" Essentially, SCCA is a set of services for the cloud environment that provides the same level of security mission partners typically receive when hosted in one of DISA's physical data centers.
- SCCA has four components: Cloud Access Points, a Virtual Data Center Security Stack, Virtual Data Center Managed Services, and a Trusted Cloud Credential Manager. These components, and their functions, are explained in this article.

- The key takeaways are:

    - All Impact Level 4 and 5 data hosted in commercial cloud environments must use the Cloud Access Point component of the SCCA to connect to the Defense Information Systems Network (DISN).

    - Impact Level 4 and 5 data and must also be secured according to criteria defined in the DOD Cloud Computing Security Requirements Guide. A suite of services that meet the defined security requirements can be provided through the SCCA, or may be acquired from other service providers.

Will I see you in Baltimore May 15-17?

- I will provide a keynote address regarding DISA's priorities and initiatives at the AFCEA Defensive Cyber Operations Symposium May 15-17 at the Baltimore Convention Center. My senior leaders and I will be available throughout the event, including during "Meet the Program Managers" and "Meet the DISA Seniors" networking events.

- Agency subject matter experts will provide content for 15 breakout sessions, covering topics such as the future of unified capabilities, mission-focused mobility, innovations in identity management, Joint Regional Security Stacks, Risk Management Framework, and migrating applications to the cloud. The DISA exhibit pavilion will also feature more than a dozen exhibits staffed by subject matter experts.

- If you are unable to attend in person, be sure to watch a live stream of the keynote speakers and panels at https://www.disa.mil/NewsandEvents/Events/Baltimore-2018.

- The DISA Cloud Symposium will also take place at the Baltimore Convention Center May 15-16. Although registration for this event has reached capacity, I encourage you to join the waitlist to ensure you receive notification when briefings and supporting materials from the event are made available online.