Fast Facts and Future Initiatives of the DoD and IC

From Officials:

- William Burns, Director of the CIA, declared the pivot of the IC and DoD from counterterrorism to great power competition which requires increased technology investment and all aspects of strategy, technology, etc. to be both offensive and defensive for the IC.

- Vice Admiral Frank Whitworth, Director of the NGA, highlighted the necessity of defense readiness through utilizing defense intelligence. The DoD must remain ahead of its strategic competitors by quickly adapting and integrating emerging technologies. For operations and missions, this shift includes an acceptance of relying on remote capabilities and unmanned systems.

- John Sherman, the DoD CIO, stated that a Cyber Workforce Strategy will be released early 2023. He compared the cyber challenge to that of the Space Race and asserted it should have the "same motivating influence as our parents and grandparents to push STEM and other areas."

Challenges and Future Initiatives:

- The military faces the challenge of shifting to a peer competition or crisis mode, which requires modernizing processes and adopting digital age technologies. To stay ahead, the IC needs to move faster. Speed and scale of innovation is essential to take full advantage of capabilities, and it requires not just technological change, but organizational and cultural adjustments as well. Infrastructure technology must be adopted to obtain cyber capabilities at the speed of relevance. The overall goals for DIA's Desktop of the Future are reducing operating costs, reducing the amount of hardware, and maintaining a secure baseline by moving away from manual patching. To enable their vision, the DIA is looking for solutions to the Desktop of the Future's challenges including high costs, latency issues and keeping legacy systems online while modernizing.

- One of the three objectives the Center for Cybersecurity Standards (CCSS) outlined for the futured include promoting US leadership in international standards stage. The US has stepped back from leading the creation of standards which has led to two major issues. When adversaries create the technology standards and own that intellectual property, US companies must pay licensing fees and navigate around the national security risks that it presents. The CCSS encourages US industry to push back in the key markets & CCSS focus areas which include 5G cellular networks, secure network protocols, cloud security automation, AI/machine learning, and IoT.

- The up and coming As-a-Service model will allow the rapid acquisition and sustainment of new capabilities without the need for recurrent tech refreshes. The DIA Platform-as-a-Service (DPaaS) enables developers to build to a single standard that provides advanced and commonly used technical enterprise services necessary to decrease development time while achieving strategic competition goals. This enhances a developer's ability to focus on functionality, enabling mission applications to be rapidly prototyped and move at the speed of mission by reducing technical overhead. The As-a-Service model also allows budgets to shift from a procurement-heavy focus and use funds from Operations & Maintenance (O&M) and Research, Development, Test, and Evaluation (RDT&E) more often than in the past.

- JWICS Modernization through the JWICS Cyber Inspection Program (JCIP) is another priority for the DIA. Through JCIP assessments, the DIA will strive to shift programs toward the mission enablement goal and revise or remove programs that do not. The assessments will last 120 days and will undergo four phases: Scoping & Mission Mapping, On-Site Inspection/Vulnerability Synthesis, CTX, and Analysis and Final Report.

- The DIA is reforming their Capability Pipeline Delivery through a new program called ATO@Hello aimed at increasing agility within ATOs as technology improves. The Authority to Operate (ATO) @ Hello process will allow for the approval to deploy a capability onto DoDIIS upon first meeting, even if the capability is not built yet, as long as the office and vendor follow security regulations. Continuous monitoring will provide oversight of these capabilities and automatically quarantine programs that fail to meet standards. (There are currently no programs running off ATO@Hello.)