Delivering DoD's Cyber Security Workforce of the Future

Stephanie Hammond
Solution Sales Executive – Department of Defense and Intelligence Community
ServiceNow

Emily Kourey
Solutions Consultant – Employee Workflow
ServiceNow

The Department of Defense's most valuable asset – its people – will be a critical component to achieve its cybersecurity workforce objectives in a complex global environment. To combat current and future cyber threats, DoD must empower and develop a highly-skilled cyber workforce. Employing the latest technologies, such as artificial intelligence and machine learning, as well as more effectively recruiting, retaining, upskilling, and reskilling will allow DoD to have a mission ready workforce of the future.

The DoD Cyber Workforce (CWF) Strategy will enable the DoD to close workforce development gaps, resource workforce management and development initiatives, stay at the forefront of technological advances, securely and rapidly deliver resilient systems, and transform into a data-centric enterprise with optimized workforce analytics.

The DoD is aligning strategic efforts to four human capital pillars:
1. Identification
2. Recruitment
3. Development
4. Retention

These pillars provide the foundation and set unified direction to accomplish the goals outlined in the CWF Strategy. These goals are to execute consistent capability assessment and analysis processes to stay ahead of force needs; establish an enterprise-wide talent management program to better align force capabilities with current and future requirements; facilitate a cultural shift to optimize Department-wide personnel management activities; and foster collaboration and partnerships to enhance capability development, operational effectiveness, and career-broadening experience.

Understand how DoD can accomplish its CWF strategy by employing technology that leverages artificial intelligence, machine learning, data analytics, and integration with defense business systems and USAStaffing to rapidly address the race for cyber talent.