3:00 p.m. – 3:30 p.m.
Authentic Training for the Cyber Mission Forces: Achieving Crew Competency

Mr. Andrew Smallwood, CISSP, CCP, HCS
Lead Associate, Cyber Futures – Human Capital and Learning Team
Booz Allen Hamilton

Currently, the heart of combatant command cyber operations resides in the evolving Cyberspace Mission Force (CMF) and Cyberspace Mission Teams (CMTs), and in the Joint Cyber Centers (JCCs). Comprehensive training offerings for CMF, CMT and JCC mission areas exist, but with a rapidly evolving cyber threat landscape, more authentic, role-based training for these cyber warriors is critical. More importantly, the ability to validate that these training experiences truly affect performance, and to gather metrics which track progress for individuals and teams is essential. A comprehensive training repertoire, built upon the secure foundation of role and task analysis and mapped securely to the definitive frameworks which outline performance standards, would ensure the consistent development of the cyber workforce and allow for the evolution of the cyber crew competency identified by combatant commanders as so essential.
The CMFs serve on the front line of DoD s cybersecurity efforts, and their recruitment, training and retention present critical challenges: emergent requirements, rotating assignments, and mission and command specific dependencies all color the CMF training and performance landscape. Cyber CMTs may be assessed at Full Operational Capability (FOC) in the Defense Readiness Reporting System (DRRS) when they are fully staffed and have executed training, but they may still lack essential skills to deliver an effect needed by a Combatant Commander. US Pacific Command as an example, uses the ability to fight tonight as its readiness metric and does not consider these forces as mission ready , when evaluated by the traditional standards. Commanders at all levels must understand their cyber environments, to include vulnerabilities and threats, in order to assess operational risk. By the same token, they must have sound and reliable metrics to assess the readiness of their forces, both individual skill sets as applied to critical roles, and collectively, when applying crew competency assumptions to team missions. Authentic training must provide a holistic, innovative solution for the accurate assessment of cyber skill sets at all levels from basic to advanced, to the provision of just-in-time training

and practice capability for the individual, to collective full-scale exercises for mission teams. While there are any number of cybersecurity training providers serving the DoD, the Booz Allen CyberSim" Training Platform, with its ever growing repertoire of challenges supporting an infinite number of reliable assessments, targets essential performance skills and validates readiness in an authentic way. Outputs of the platform provide commanders with concrete metrics regarding the scope and depth of individual and team skill sets, making it possible to accurately funnel training resources, assign personnel appropriately to missions, and group personnel together in multi-disciplinary teams where skills complement one another to achieve true cyber mission readiness.