(U) LOE 8: Sustain a Ready Cyber Workforce

LOE End State: (U//FOUO) The Department successfully identifies, recruits, and retains world-class military and civilian cyber talent. The Department provides ample opportunities—inside and outside the Department—to uniformed military personnel and civilians for development, training, and career progression. The Department uses realistic training environments, exercises, and peacetime activities to sustain highly-capable cyber personnel and resources postured for the rapid execution of tools against the highest-priority threats.

Objectives:

8-1: (U) Enhance cyber workforce capabilities to become a more agile, lethal, and effective force. [OPRs: DoD CIO; Services; USCYBERCOM; USD(I)]

8-1-1: (U) Employ a robust cyber workforce rationalization initiative across the Total Force military (Active, Reserve, Guard), personnel, government civilian employees, and contract support. [OPRs: Services; USCYBERCOM]

8-1-2: (U) Develop and implement the DoD Cyber Qualifications Program to enhance readiness. [OPRs: DoD CIO; USD(P)/PCA]

8-1-3: (U) Establish and formalize the process to manage and periodically update the DoD Cyber Workforce Framework to maintain relevancy. [OPRs: DoD CIO; USD(P)/PCA]

8-1-4: (U) Pursue authorities for the establishment of a dedicated fund for defense cyber workforce development. [OPRs: DoD CIO;USD(P)/PCA]

8-1-5: (U) Enhance the policies, authorities, and resourcing to improve the integration of Reserve and National Guard units into the Cyber Mission Forces. [OPRs: NGB; USCYBERCOM; Services]

8-1-6: (U) Explore and identify mechanisms to enhance and expand cyber red team capabilities in accordance with DoD initiatives. [OPRs: USD(P&R);USCYBERCOM; Services]

8-1-7: (U) Identify readiness issues/gaps that affect cyberspace operations, and capture and reported via appropriate feedback mechanisms. [OPRs: CCMDs; Services]

8-2: (U) Enhance and improve the identification and lifecycle management of military cyber workforce. [OPRs: USD(P&R); Services; DoD CIO]

8-2-1: (U) Mature the policies for the identification and coding of military manpower requirements and cyber work roles; and personnel skillsets and qualifications. [OPRs: DoD CIO; USD(P&R); USD(I)]

8-2-2: (U) Improve military accessions processes through development and implementation of enhanced cyber recruitment programs. [OPRs: Services]

8-2-3: (U) Identify personnel most likely to be successful in cyber work roles. [OPRs: USD(P)/PCA; Services; USCYBERCOM]

8-2-4: (U) Enhance military career broadening and exchange programs across federal government that have complementary cyber roles, functions, and/or missions. [OPRs: USD(P&R); Services]

8-2-5: (U) Improve military personnel retention through development and implementation of enhanced cyber retention programs. [OPRs: USD(P)/PCA; Services]

8-3: (U) Enhance and improve the identification and lifecycle management of the civilian cyber workforce. [OPRs: DoD CIO; Services; USD(P&R); USD(I)]

8-3-1: (U) Mature the implementation of the Cyber Excepted Service personnel system across the Department. [OPRs: DoD CIO;USD(P)/PCA]

8-3-2: (U) Mature the policies for the identification and coding of civilian manpower requirements and cyber work roles; and personnel skillsets and qualifications. [OPRs: DoD CIO; USD(P&R)]

8-3-3: (U) Execute the DoD Cyber Workforce Critical Needs Assessment Process. [OPRs: DoD CIO; Services; USD(I)]

8-3-4: (U) Explore and assess the need for a DoD cyber talent management program. [OPRs: DoD CIO; Services]

8-3-5: (U) Improve civilian recruitment and retention through the development and implementation of enhanced programs for the cyber workforce. [OPRs: DoD CIO; Services]

8-3-6: (U) Integrate and align the DoD Cyber Workforce Framework into the CES and other DoD civilian occupational structures. [OPRs: DoD CIO]

8-3-7: (U) In partnership with OPM, explore the establishment of a Federal cyber position classification standard and occupational series. (OPRs: USD(P&R); DoD CIO]

8-4: (U) Leverage the existing DoD background investigation prioritization program to optimize the timely availability of qualified military, civilian, and contractor cyber personnel. [OPRs: USD(I); DoD CIO]

8-4-1: (U) Validate and reconcile security background investigation requirements for cyber workforce (military, civilian, and contractor) positions. [OPRs: USD(I); DoD CIO]

8-4-2: (U) Leverage mechanisms to enhance screening and vetting to accommodate mission critical skillsets for DoD cyber professionals. [OPRs: USD(I); DoD CIO]

8-5: (U) Enhance the quality of the cyber training and education continuum across the Department. [OPRs: USD (P&R), Services;]

8-5-1: (U) Develop DoD enterprise baseline training standards and joint training standards, aligned to the DoD Cyber Workforce Framework and augmented by the Joint Cyberspace Training and Certification Standards (JCT&CS). [OPRs: DoD CIO; USCYBERCOM]

8-5-2: (U) Enhance the cyberspace curriculum at Joint Professional Military Education (JPME) schools by incorporating realistic and relevant case studies. [OPRs: USCYBERCOM;JS]

8-5-3: (U) Develop the concept for establishing a leadership-level cyber strategy development and planning framework into course curriculum at Joint and Service-sponsored function courses. [OPRs: JS; USCYBERCOM]

8-5-4: (U) Incorporate cyber mission, roles, and responsibilities into required leadership training plans and curriculum. [OPRs: USCYBERCOM; Services]

8-5-5: (U) Enhance cyberspace operations and planning through participation in the Chairman's Joint Exercise Program. [OPRs: JS; CCMDs; USCYBERCOM]

8-5-6: (U) Ensure training issues/gaps for cyberspace operations are captured and reported via appropriate feedback mechanisms (i.e, JLLIS, JTIMS). [OPRs: JS; CCMDs; USCYBERCOM]

8-6: (U) Mature, sustain, and resource cyber training infrastructure. [OPRs: Army (DoD EA CTR); USCYBERCOM]

8-6-1: (U) Mature the cyber training environment to meet current and future operational requirements. [OPRs: Army (DoD EA CTR); USCYBERCOM]

8-6-2: (U) Based on prioritization by USD(P), increase accessibility, interoperability with select partners of cyber ranges in order to support training DoD personnel. [OPRs: Army (DoD EA CTR); USCYBERCOM; USD(P)]

8-7: (U) Strengthen relationships with academic and private institutions to increase cyber education opportunities. [OPRs: DoD CIO; Services; NSA]

8-7-1: (U) Enhance existing partnerships with the Department to advance the mission of the Centers of Academic Excellence (CAE) in cyber education. [OPRs: DoD CIO; NSA; Services]

8-7-2: (U) Infuse cyber into Science, Technology, Engineering, and Math (STEM) recruitment and outreach programs. [OPRs: DoD CIO; Services]

8-7-3: (U) Integrate community colleges into the DoD Cybersecurity Scholarship Program (CySP). [OPRs: DoD CIO; NSA]

8-8: (U) Increase cyber workforce interoperability with internal and external partners. [OPRs: DoD CIO; USCYBERCOM]

8-8-1: (U) Increase opportunities for the integration of cyber operations into Joint/Service training (including exercises and mission rehearsals), experimentation, and validation. [OPRs: USCYBERCOM; Joint Staff J7; CCMDs]

8-8-2: (U) Enhance exchange and exercise opportunities with Federal government and international partners. [OPRs: USCYBERCOM; USD(P); CCMDs]

8-8-3: (U) Enhance exchange opportunities with Industry partners (e.g. Cyber Information Technology Exchange Program (CITEP) and others). [OPRs: DoD CIO]

8-8-4: (U) Develop a Federal-wide cyber exchange program with agency partners that share similar cyberspace tasks, roles, functions, and/or missions. [OPRs: DoD CIO]

8-9: (U) Instill cybersecurity culture across the Department. [OPRs: DoD CIO; Services]

8-9-1: (U) Enhance annual cybersecurity training. [OPRs: DoD CIO; USD(I);DISA]

8-9-2: (U) Integrate cybersecurity content into DoD military and civilian leadership development programs and executive-level or equivalent qualification frameworks. [OPRs: DoD CIO]