



OFFICE OF THE SECRETARY OF DEFENSE

1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000

**CLEARED**  
**For Open Publication**  
**NOV 14 2022**  
**Nov 15, 2022**

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Expanding Cybersecurity Workforce by Eliminating Educational Barriers and Leveraging Apprenticeship Programs

Department of Defense

OFFICE OF PREPUBLICATION AND SECURITY REVIEW

The Department of Defense (DoD) and the Defense Industrial Base (DIB) continue to identify, recruit, develop, and retain the cybersecurity workforce in order to support the Nation's ability to defend against and react to current and future cyber threats and attacks. However, attracting cybersecurity professionals continues to fall short of demand. To address this shortfall, DoD must consider qualified applicants who have obtained appropriate qualifications through training, industry certifications, on-the-job training, or apprenticeship programs. We will encourage the industrial base to adopt the same approach.

Removing formal education-rooted barriers, combined with the use of apprenticeship programs, provides a faster pipeline to acquire talent, increases talent pool, and enhances diversity by allowing applicants to enter the workforce through nontraditional pathways. The Federal Acquisition Regulations specify that solicitations and contracts for information technology services should not routinely describe any minimum experience or educational requirement (FAR 39.104).

Efforts including apprenticeship programs enhance our cybersecurity workforce and complement the Biden-Harris Administration's focus on diversity, equity, inclusion, and accessibility. Registered apprenticeship programs – high-quality training programs that are industry-vetted and approved and validated by the U.S. Department of Labor or a State Apprenticeship Agency – provide skills-based pathways for entry-level candidates into cybersecurity jobs, help fill skill gaps in the cybersecurity workforce, and increase opportunities for historically underserved communities. We request that you communicate to contractors supporting your components and programs that they consider developing a cybersecurity apprenticeship program. Information on this topic can be found at <https://www.apprenticeship.gov/cybersecurity-apprenticeship-sprint> or from the Department of Labor at <https://www.apprenticeship.gov/about-us/state-offices>.

Closing the talent gap in both DoD and the DIB is critical to strengthen and safeguard our Nation's cybersecurity. Moreover, removing formal education barriers and providing nontraditional skills-based pathways is a step that brings DoD closer to our goal of scaling up a workforce in other sectors that are critical to mission readiness and supporting the warfighter.

William A. LaPlante Jr.  
Under Secretary of Defense for  
Acquisition and Sustainment

John B. Sherman  
Department of Defense Chief  
Information Officer

**Distribution:**

**Secretaries of the Military Departments**  
**Chairman of the Joint Chiefs of Staff**  
**Under Secretaries of Defense**  
**Commanders of the Combatant Commands**  
**Chief, National Guard Bureau**  
**Director of Cost Assessment and Program Evaluation**  
**Inspector General of the Department of Defense**  
**Director of Operational Test and Evaluation**  
**Assistant Secretaries of Defense**  
**Assistants to the Secretary of Defense**  
**Director, Administration and Management**  
**Director, Net Assessment**  
**Directors of the Defense Agencies**  
**Directors of the DoD Field Activities**  
**Commander, United States Special Operations Command**  
**(attn: Acquisition Executive)**  
**Deputy Assistant Secretary of the Army (Procurement)**  
**Deputy Assistant Secretary of the Navy (Procurement)**  
**Deputy Assistant Secretary of the Air Force (Contracting)**  
**Chief Information Officers, Military Departments**