



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Employee Services

Wednesday, December 6, 2017

MEMORANDUM FOR: HUMAN RESOURCES DIRECTORS

FROM: MARK D. REINHOLD, ASSOCIATE DIRECTOR, EMPLOYEE SERVICES

Subject: Next Steps in Implementing the Federal Cybersecurity Workforce Assessment Act

The [Federal Cybersecurity Workforce Assessment Act of 2015](#) (Act) requires the U.S. Office of Personnel Management (OPM) to establish procedures to implement the National Initiative for Cybersecurity Education (NICE) coding structure and to identify all Federal civilian positions performing information technology, cybersecurity, or other cyber-related functions. OPM published this [guidance](#) on January 4, 2017.

The next steps, as mandated by the Act, are for agencies to complete the coding of their workforce by April 2018. After the completion of the position coding, agencies are required to identify information technology, cybersecurity, and other cyber-related work roles of critical need among their civilian workforce. Once the work roles of critical need are identified, agencies must submit a report to OPM indicating the roles and substantiating the designation of critical need. This will be due in April 2019 and annually thereafter. OPM is currently developing guidance for agencies to use in determining work roles of critical need and reporting this information.

The attachments below provide an overview of the Act's requirements, timelines, and key milestones. We will continue to keep you apprised as we develop the guidance to assist in the forthcoming requirements in the Act. If you have questions, please contact Erika Viola at Erika.Viola@opm.gov.

Attachments (see 508-compliant PDF below)

cc: Chief Human Capital Officers (CHCOs), Dep. CHCOs, Chief Information Officers, and Chief Information Security Officers