June 2018

CYBERSECURITY WORKFORCE

Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions

GAO Highlights

Highlights of GAO-18-466, a report to congressional committees

Why GAO Did This Study

A key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce. The Federal Cybersecurity Workforce Assessment Act of 2015 requires OPM and federal agencies to take several actions related to cybersecurity workforce planning.

GAO is to monitor agencies' progress in implementing the act's requirements. For this report, GAO assessed whether: (1) OPM developed a coding structure and procedures for assigning codes to cybersecurity positions and submitted a progress report to Congress; (2) CFO Act agencies submitted complete, reliable baseline assessments of their cybersecurity workforces; and (3) CFO Act agencies established procedures to assign codes to cybersecurity positions. GAO examined OPM's coding procedures and progress report on the act's implementation, and baseline assessments and coding procedures from the 24 CFO Act agencies. GAO also interviewed relevant OPM and agency officials about efforts to address the act's requirements.

What GAO Recommends

GAO is making 30 recommendations to 13 agencies to fully implement two of the act's requirements on baseline assessments and coding procedures. Of the 12 agencies to which we made recommendations that provided comments on the report, 7 agreed with the recommendations made to them, 4 did not state whether they agreed or disagreed, and 1 did not agree with one of two recommendations made to it. GAO continues to believe that the recommendation is valid as discussed in this report.

View GAO-18-466. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

As required by the Federal Cybersecurity Workforce Assessment Act of 2015 (act), the Office of Personnel Management (OPM) developed a cybersecurity coding structure under the National Initiative for Cybersecurity Education (NICE) as well as procedures for assigning codes to federal civilian cybersecurity positions. However, OPM issued the coding structure and procedures 5 and 4 months later than the act's deadlines because OPM was working with the National Institute of Standards and Technology (NIST) to align the structure and procedures with the draft *NICE Cybersecurity Workforce Framework*, which NIST issued later than planned. OPM also submitted a progress report to Congress on the implementation of the act 1 month after it was due. The delays in issuing the coding structure and procedures have extended the expected time frames for implementing subsequent provisions of the act.

Most of the 24 agencies covered by the Chief Financial Officers (CFO) Act submitted baseline assessment reports to Congress but the results may not be reliable. As of March 2018, 21 of the 24 CFO Act agencies had conducted baseline assessments identifying the extent to which their cybersecurity employees held professional certifications and had submitted the assessment reports to Congress as required by the act. Three agencies had not conducted the assessments for various reasons, such as a lack of resources and tools to do so. Of the 21 agencies that did, 4 did not address all of the reportable information, such as the extent to which personnel without professional certifications were ready to obtain them or strategies for mitigating any gaps. Additionally, agencies were limited in their ability to obtain complete or consistent information about their cybersecurity employees and the certifications they held. This was because agencies had not yet fully identified all members of their cybersecurity workforces or did not have a consistent list of appropriate certifications for cybersecurity positions. As a result, the agencies had limited assurance that their assessment results accurately reflected all relevant employees or the extent to which those employees held appropriate certifications. This diminishes the usefulness of the assessments in determining the certification and training needs of these agencies' cybersecurity employees.

Most of the 24 CFO Act agencies established coding procedures, but 6 agencies only partially addressed certain activities required by OPM in their procedures. Of the 24 agencies reviewed, 23 had established procedures to identify their civilian cybersecurity positions and assign the appropriate employment codes to the positions as called for by the act. However, 6 of the 23 agencies did not address one or more of 7 activities required by OPM in their procedures, such as the activities to review all filled and vacant positions and annotate reviewed position descriptions with the appropriate employment code. These 6 agencies cited a variety of reasons for not addressing all of the required activities in their coding procedures. For example, these agencies stated that they addressed the activities in existing guidance or did not include activities that their components did not have the responsibility to perform. By not addressing all of the required activities in their coding procedures, the 6 agencies lack assurance that the activities will be performed or performed consistently throughout their agency.