April 2020

CYBERSECURITY

DOD Needs to Take Decisive Actions to Improve Cyber Hygiene

GAO Highlights

Highlights of GAO-20-241, a report to congressional committees

Why GAO Did This Study

DOD has become increasingly reliant on information technology (IT) and risks have increased as cybersecurity threats evolve. Cybersecurity experts estimate that 90 percent of cyberattacks could be defeated by implementing basic cyber hygiene and sharing best practices, according to DOD's Principal Cyber Advisor.

Senate Report 115-262 includes a provision that GAO review DOD cyber hygiene. This report evaluates the extent to which 1) DOD has implemented key cyber hygiene initiatives and practices to protect DOD networks from key cyberattack techniques and 2) senior DOD leaders received information on the department's efforts to address these initiatives and cyber hygiene practices.

GAO reviewed documentation of DOD actions taken to implement three cyber hygiene initiatives and reviewed recurring reports provided to senior DOD leaders.

What GAO Recommends

GAO is making seven recommendations to DOD, including that cyber hygiene initiatives be fully implemented, entities are designated to monitor component completion of tasks and cyber hygiene practices, and senior DOD leaders receive information on cyber hygiene initiatives and practices. Of the seven recommendations, DOD concurred with one, partially concurred with four, and did not concur with two. GAO continues to believe that all recommendations are warranted.

View GAO-20-241. For more information, contact Joe Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Department of Defense (DOD) has not fully implemented three of its key initiatives and practices aimed at improving cyber hygiene. Carnegie-Mellon University defines cyber hygiene as a set of practices for managing the most common and pervasive cybersecurity risks. In discussions with GAO, DOD officials identified three department-wide cyber hygiene initiatives: the 2015 DOD Cybersecurity Culture and Compliance Initiative, the 2015 DOD Cyber Discipline Implementation Plan, and DOD's Cyber Awareness Challenge training.

- The Culture and Compliance Initiative set forth 11 overall tasks expected to be completed in fiscal year 2016. It includes cyber education and training, integration of cyber into operational exercises, and needed recommendations on changes to cyber capabilities and authorities. However, seven of these tasks have not been fully implemented.
- The Cyber Discipline plan has 17 tasks focused on removing preventable vulnerabilities from DOD's networks that could otherwise enable adversaries to compromise information and systems. Of these 17, the DOD Chief Information Officer is responsible for overseeing implementation of 10 tasks. While the Deputy Secretary set a goal of achieving 90 percent implementation of the 10 CIO tasks by the end of fiscal year 2018, four of the tasks have not been implemented. Further, the completion of the other seven tasks was unknown because no DOD entity has been designated to report on the progress.
- The Cyber Awareness training is intended to help the DOD workforce maintain awareness of known and emerging cyber threats, and reinforce best practices to keep information and systems secure. However, selected components in the department do not know the extent to which users of its systems have completed this required training. GAO's review of 16 selected components identified six without information on system users that had not completed the required training, and eight without information on users whose network access had been revoked for not completing training.

Beyond the initiatives above, DOD has (1) developed lists of the techniques that adversaries use most frequently and pose significant risk to the department, and (2) identified practices to protect DOD networks and systems against these techniques. However, the department does not know the extent to which these practices have been implemented. The absence of this knowledge is due in part to no DOD component monitoring implementation, according to DOD officials. Overall, until DOD completes its cyber hygiene initiatives and ensures that cyber practices are implemented, the department will face an enhanced risk of successful attack.

While two recurring reports have provided updates to senior DOD leaders on cyber information on the Cyber Discipline plan implementation, department leadership has not regularly received information on the other two initiatives and on the extent to which cyber hygiene practices are being implemented. Such information would better position leaders to be aware of the cyber risks facing DOD and make more effective decisions to manage such risks.