GAO

Highlights

Highlights of GAO-19-362, a report to the Committee on Armed Services, House of Representatives

March 2019

DOD TRAINING

U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force

Why GAO Did This Study

Developing a skilled cyber workforce is imperative to DOD achieving its offensive and defensive missions, and in 2013 it began developing CMF teams to fulfill these missions. CYBERCOM announced that the first wave of 133 such teams achieved full operational capability in May 2018. House Report 115-200 includes a provision for GAO to assess DOD's current and planned state of cyber training.

GAO's report examines the extent to which DOD has (1) developed a trained CMF, (2) made plans to maintain a trained CMF, and (3) leveraged other cyber experience to meet training requirements for CMF personnel. To address these objectives, GAO reviewed DOD's cyber training standards, planning documents, and reports on CMF training; and interviewed DOD officials. This is an unclassified version of a For Official Use Only report that GAO previously issued.

What GAO Recommends

GAO is making eight recommendations, including that the Army and Air Force identify time frames for validating foundational CMF courses; the military services develop CMF training plans with specific personnel requirements; CYBERCOM develop and document a plan establishing independent assessors to evaluate training; and CYBERCOM establish the training tasks covered by foundational training courses and convey them to the services. DOD concurred with the recommendations.

View GAO-19-362. For more information, contact Joe Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

U.S. Cyber Command (CYBERCOM) has taken a number of steps—such as establishing consistent training standards—to develop its Cyber Mission Force (CMF) teams (see figure). To train CMF teams rapidly, CYBERCOM used existing resources where possible, such as the Navy's Joint Cyber Analysis Course and the National Security Agency's National Cryptologic School. As of November 2018, many of the 133 CMF teams that initially reported achieving full operational capability no longer had the full complement of trained personnel, and therefore did not meet CYBERCOM's readiness standards. This was caused by a number of factors, but CYBERCOM has since implemented new readiness procedures that emphasize readiness rather than achieving interim milestones, such as full operational capability.

Figure: Cyber Mission Force (CMF) Training Model Phases

	Phase one *Basic individual training*	Phase two *Individual foundation training*	Phase three *Collective training*	Phase four *Sustainment training*
Training standards established by	Services or by a joint organization (e.g. signals intelligence training standards are set by the National Security Agency).	U.S. Cyber Command	U.S. Cyber Command	U.S. Cyber Command
Training administered by	Services	U.S. Cyber Command vendors, such as the Defense Cyber Investigations Training Academy. Some services also have the U.S. Cyber Command's approval to deliver training.	Services at the unit level.	Services at the unit level and U.S. Cyber Command vendors.
Description	Provides initial specialty occupation training.	Prepares personnel for the specific position they will fill in the CMF team to which they are assigned using a particular progression of courses.	Prepares personnel to pass U.S. Cyber Command's certification standards through on-the- job training and exercises.	Refreshes team skills and certifications using activities from phases two and three. Also includes mission rehearsal exercises.

Source: GAO analysis of Department of Defense information. | GAO-19-362

DOD has begun to shift focus from *building* to *maintaining* a trained CMF. The department developed a transition plan for the CMF that transfers foundational (phase two) training responsibility to the services. However, the Army and Air Force do not have time frames for required validation of foundational courses to CYBERCOM standards. Further, services' plans do not include all CMF training requirements, such as the numbers of personnel that need to be trained. Also, CYBERCOM does not have a plan to establish required independent assessors to ensure the consistency of collective (phase three) CMF training.

Between 2013 and 2018, CMF personnel made approximately 700 requests for exemptions from training based on their experience, and about 85 percent of those applicants had at least one course exemption approved. However, GAO found that CYBERCOM has not established training task lists for foundational training courses. The services need these task lists to prepare appropriate course equivalency standards.