United States Government Accountability Office

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

GAO-19-362

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.

Contents

Abbreviations

CMF	Cyber Mission Force
CYBERCOM	U.S. Cyber Command
DOD	Department of Defense
JCT&CS	Joint Cyberspace Training and Certification Standards

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 6, 2019

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

Developing a skilled cyber workforce is imperative to defending the Department of Defense's (DOD) information networks and achieving operational offensive and defensive cyber effects on the battlefield. According to the *DOD Cyber Strategy*, a crucial aspect of DOD's cyber workforce is to have a trained and ready Cyber Mission Force (CMF).[1]

In 2013, U.S. Cyber Command (CYBERCOM) and the military services began developing CMF teams.[2] The initial plan—which we will refer to as "the first wave"—consists of 133 teams and is comprised of active duty, civilian, and contract personnel from across the military services (Army, Navy, Air Force, and Marine Corps) as well as Air National Guard and Air Force Reserve personnel. These 133 teams were developed from 2013 through 2018. In 2017, the Commander of CYBERCOM endorsed the Army's proposal for a second wave of 21 Army reserve component (10 Army Reserve and 11 Army National Guard) Cyber Protection Teams to be assigned to CYBERCOM and integrated into the CMF. CYBERCOM announced that the first wave of 133 teams achieved full operational capability in May 2018, and it plans for the second wave of 21 teams to achieve that milestone by fiscal year 2024.[3]

[1]Department of Defense, *The Department of Defense Cyber Strategy* (April 2015) (hereinafter cited as the *DOD Cyber Strategy*). This strategy was recently superseded by the *2018 Department of Defense Cyber Strategy*.

[2]In 2009, DOD established U.S. Cyber Command (CYBERCOM) as a sub-unified command organized under U.S. Strategic Command. In 2010, the President tasked the director of the National Security Agency with the additional responsibility of leading CYBERCOM. In August 2017, the President directed that CYBERCOM be elevated to the status of a unified combatant command focused on cyberspace operations in compliance with the National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 923 (2016). CYBERCOM officially became a unified combatant command on May 4, 2018.

[3]According to DOD officials, full operational capability for CMF teams is an evaluation that the team can perform its mission as designed.

The CMF teams generally align with CYBERCOM's three central missions—(1) support military operations; (2) defend the United States against cyberattacks of serious consequence; and (3) defend DOD information networks. The three primary categories of teams are as follows:

- Combat Mission Teams and their associated Combat Support Teams support combatant commands by providing offensive cyberspace capabilities in support of operational plans and contingency operations.[4]
- National Mission Teams and their associated Mission Support Teams defend the United States and its interests against cyberattacks of significant consequence.
- Cyber Protection Teams augment traditional defensive measures and defend priority DOD networks and systems against priority threats.

House Report 115-200 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 includes a provision for us to assess the current and planned state of DOD's cyber training.[5] Our report examines the extent to which DOD (1) has developed trained CMF teams; (2) has plans to maintain a trained CMF; and (3) has leveraged other cyber experience to meet training requirements for CMF personnel—a process known as individual training equivalency. In November 2018, we issued a For Official Use Only version of this report. To prepare this unclassified version, we removed sensitive information about the number and organizational alignment of CMF teams. We also removed the sensitive information about the readiness levels of and training standards used by CMF teams. Although the information provided in this report is less specific, it addresses the same questions as the For Official Use Only report. Also, the overall methodology used for both reports is the same.

Our report focuses specifically on the training associated with DOD's CMF teams—the operational cyber forces organized under CYBERCOM. Our report does not address the cybersecurity awareness training that is

[4]The National Mission Teams and Combat Mission Teams have support teams that typically include linguists, analysts, and other specialists who provide more in-depth support to the teams' missions.

[5]See H.R. Rep. No. 115-200, at 254 (2017).

delivered to most DOD personnel, nor does it include personnel who have a mission within DOD's cyberspace but are not members of the CMF.[6] The objectives in this report focus on the cyber training standards, processes, and infrastructure used by CYBERCOM's CMF personnel. Wherever possible, we corroborated the results of our analyses with appropriate officials.

For our first objective, we reviewed DOD's cyber training standards and manuals, as confirmed by officials from CYBERCOM and the military service cyber components, including CYBERCOM's *CMF Training and Readiness Manual* and its cyberspace training and certification standards.[7] These documents contain tables that track the revisions made over time, allowing us to determine the extent to which substantive changes were made to the standards. In addition, we reviewed CYBERCOM's readiness reporting standard operating procedure, which describes the readiness reporting metrics, including training metrics that CMF teams must achieve. We also obtained and reviewed three recent versions of DOD's phase two foundational training progression—the specific sets of courses required for all CMF personnel to qualify for the various work roles in CMF teams. In order to understand how CYBERCOM and the military services have held CMF personnel to consistent standards, we compared the current phase two foundational training progression, updated in November 2017, against prior versions from June 2014 and December 2016 to document how it has changed.[8] We interviewed officials from CYBERCOM and its vendors who implemented the training and officials from the military services who received the training to understand how DOD ensures that the course content and progression are consistently applied to all CMF teams. We reviewed policies and interviewed DOD officials to obtain descriptions of and comparisons among the phase two foundational course training progressions from June 2014, December 2016, and November 2017.

[6]Cyber professionals outside of the CMF manage and secure networks and perform information assurance activities for the services. Service officials told us that there are also military cyber professionals who build and maintain information technology services at many bases and on ships, and that these professionals are not part of the CMF.

[7]Taken together, these documents serve as the procedures, guidelines, and standards for the individual and collective training of the CMF, including identifying core tasks each individual and team must be able to perform.

[8]As described later in this report, there are four phases of cyber training for CMF team personnel. Phase two foundational training is the first level of CMF-specific training provided to personnel.

Further, we examined DOD's reported progress toward its stated goal in the 2015 *DOD Cyber Strategy* to build a trained CMF workforce. Specifically, we reviewed implementation plans and Joint Staff quarterly status reports issued from September 2016 to December 2017 to summarize DOD's reported progress toward achieving full operational capability for the first wave of 133 CMF teams. To assess the quality of DOD's internal controls related to certifying CMF teams as operationally capable, we compared CYBERCOM's existing processes against the standards in the Office of Management and Budget's *Management's Responsibility for Enterprise Risk Management and Internal Control* and GAO's *Standards for Internal Control in the Federal Government*.[9] We also interviewed officials from CYBERCOM and the military services to obtain more insight into the services' training execution plans and use of existing training capabilities to build the CMF.

For our second objective, we reviewed DOD's associated implementation plans and status reports related to these goals from December 2017. To gain further insight into DOD's progress in maintaining a trained CMF, we reviewed the Joint Staff's quarterly readiness reports that characterize the various levels of resource readiness (personnel, training, equipment available, and condition of equipment available) reported by each of the 154 teams in the Defense Readiness Reporting System, a DOD-wide readiness tracking system. We also reviewed and analyzed any training plans developed by CYBERCOM and the military services to maintain readiness after achieving full operational capability. For example, we reviewed plans of actions and milestones produced by the services in response to a requirement from CYBERCOM to make plans regarding individual and course equivalency, training execution, and course validation.[10] We compared the contents of these plans against the requirements established by CYBERCOM's guidance.

Further, we interviewed officials from CYBERCOM's training and readiness directorates, the service cyber components, and CMF teams to learn their perspectives on whether personnel were prepared to perform their missions as a result of going through CMF training. We also

[9]Office of Management and Budget, Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Washington, D.C.: July 15, 2016); and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[10]U.S. Cyber Command Deputy Commander, *Memorandum for the Record* (Nov. 28, 2017).

reviewed DOD's internal readiness reports to determine whether there were any challenges being reported with regard to maintaining sufficient capability for CMF personnel.[11] Further, we reviewed DOD's plan to transition phase two foundational training for the CMF from CYBERCOM to the military services after the first wave of CMF teams had achieved full operational capability. In addition, we interviewed knowledgeable officials from CYBERCOM's training directorate, the Joint Staff directorate responsible for cyber capability requirements, and the service offices working on training transition with regard to the implementation of this plan.[12] We compared the standards related to defining objectives from the *Standards for Internal Control in the Federal Government*, which explains that management should clearly define goals to be achieved, how those goals will be achieved, and time frames for achievement, against the practices DOD used to implement its transition plan.[13]

For our third objective, we reviewed CYBERCOM's policies with regard to granting training exemptions for CMF staff based on their previous education and/or work experience, a process known as individual training equivalency. We also reviewed the milestones set in the *CMF Training Transition Plan*, which required CYBERCOM to establish a master individual training equivalency policy and master training task lists for phase two foundational courses by March 2018, and compared CYBERCOM's progress in promulgating the training tasks against that milestone. We collected and reviewed the 69 signed official memorandums from CYBERCOM's Individual Training Equivalency Board reporting the number of applications and individual training equivalencies the board granted, by course, from September 2017 through April 2018.

We interviewed and obtained information from individuals from selected DOD organizations and teams affected by the individual training exemption process to learn their perspectives on the strengths and challenges associated with it. We selected interview subjects such that we had representation from each of the four military services' cyber components, as well as at least one cyber organization from each of the

[11]Joint Staff, *Joint Force Readiness Review* (July 2017 and September 2017).

[12]Joint Staff and DOD Principal Cyber Advisor, *Cyber Force Model Training Transition Plan for 2000-Level Training* (Jan. 19, 2017) (hereinafter cited as the *CMF Training Transition Plan*) (S//NOFORN).

[13]GAO-14-704G.

four military services that can provide CMF team perspectives—including active duty, National Guard, and Reserve teams. To determine which courses are commonly bypassed due to individual training exemptions, we reviewed the content of the 69 Individual Training Equivalency Board memorandums issued as of May 2018. Specifically, we collated the equivalency board decisions, as reported in these memorandums, to obtain estimates of the number of equivalencies granted for each of the CMF courses during this period. Additionally, we obtained descriptions of the courses that were commonly bypassed to determine the nature and content of those courses.

The performance audit upon which this report is based was conducted from August 2017 to November 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from November 2018 to February 2019 to prepare this public version of the report. This version of the report was also prepared in accordance with generally accepted government auditing standards.

Background

CYBERCOM's Cyber Mission Force

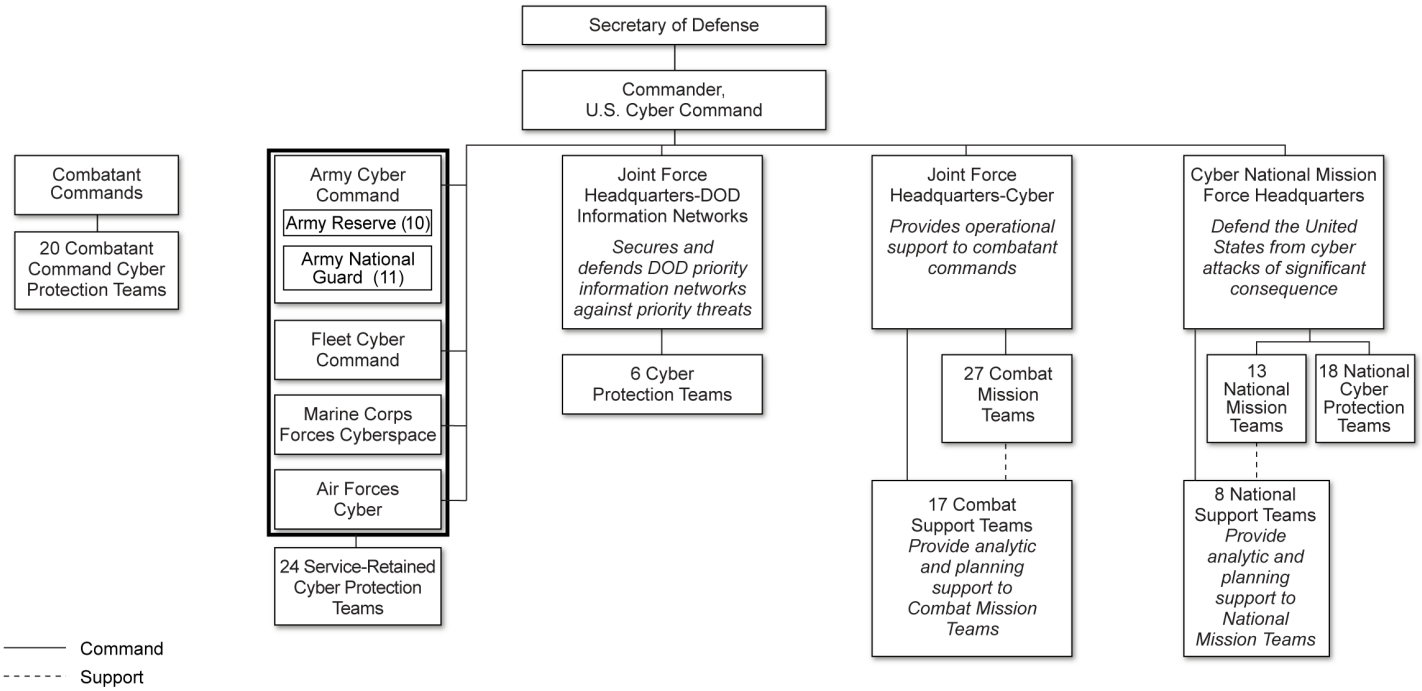
In 2012, DOD developed plans to establish 133 CMF teams focused on offensive operations, defensive operations, and DOD network protection. DOD provided budget resources for these teams beginning in fiscal year 2014. It subsequently set goals for reaching initial operational capability and full operational capability. Later in this report we describe how some of the methods used to facilitate these teams' achievement of full operational capability subsequently affected readiness.

Once each CMF team has achieved full operational capability, it is required to certify to its mission at least every 2 years. According to CYBERCOM's 2017 readiness guidance, in order for each CMF team to achieve the best readiness rating it must certify to its mission every 12 months. According to the *DOD Cyber Strategy* published in 2015, the first wave of CMF teams will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components, when they are fully staffed.

In February 2017, the commander of CYBERCOM endorsed an Army proposal to present its 21 Reserve component Cyber Protection Teams (11 Army National Guard and 10 Army Reserve) for assignment to U.S. Strategic Command to help address increased mission requirements. These 21 teams represent a second wave of teams, which CYBERCOM has scheduled to achieve full operational capability by September 30, 2024. The second wave of 21 Army Reserve component teams are to include more than 800 personnel once they are fully staffed.

The CMF teams are aligned with various DOD organizations, as shown in figure 1.[14] The military service cyber components—Army Cyber Command, Fleet Cyber Command, Marine Corps Forces Cyberspace, and Air Forces Cyber—are CYBERCOM's service elements and support CYBERCOM in achieving its missions.

Figure 1: Alignment of U.S. Cyber Command's Cyber Mission Force Teams, as of June 2018

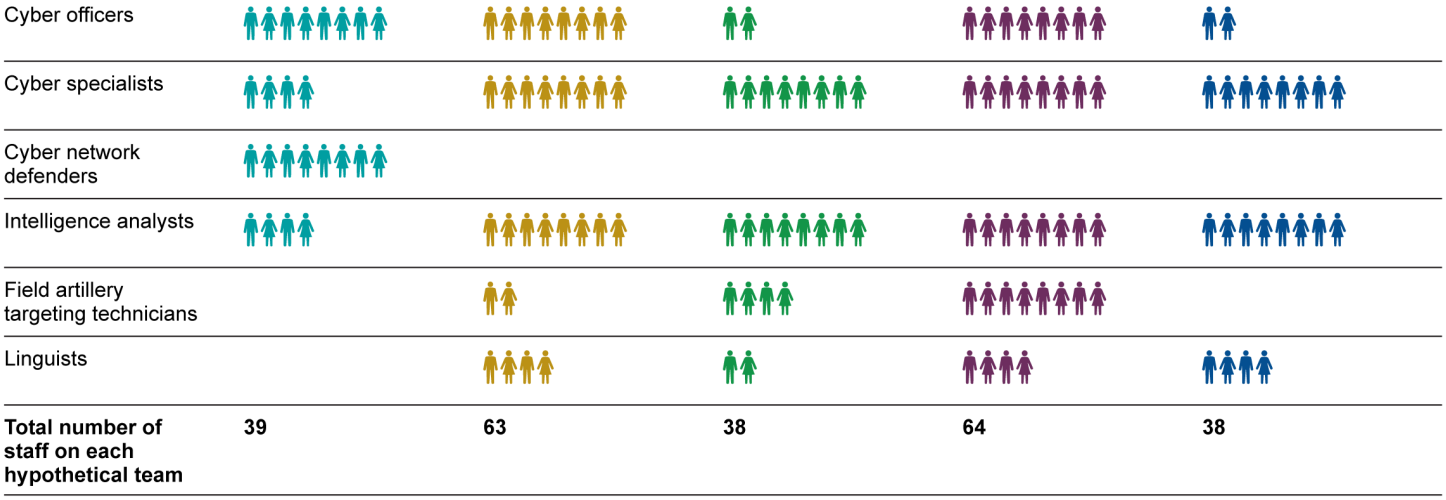


Source: GAO analysis of Department of Defense (DOD) information. | GAO-19-362

[14]For a broader perspective of DOD's cyber-related organization see GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened*, GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

The personnel on each team represent a variety of specialties, such as intelligence analysts, linguists, and cyber operators and specialists. Figure 2 provides a hypothetical example of how each team might combine personnel from different specialties to carry out its missions. This figure does not show the actual composition of any type of team, but rather provides notional examples of how each team consists of personnel from different specialties who unite to perform cyber missions as part of the CMF.

Figure 2: Hypothetical Mix of Staff Work Roles That Could Be Assigned to the Various Types of Cyber Mission Force Teams



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

Note: The number of figures depicted in each work role is hypothetical and they do not add to the total number of staff on each team.

The Four Phases of CMF Training

Training personnel for the CMF occurs in four phases and is administered by different entities, as shown in figure 3. Phase one basic training is the initial training performed by the military services that is delivered to any new recruit so that he or she may be assigned a military specialty. As shown in figure 2, CMF personnel draw from a number of different military specialties, including cyber, all-source intelligence, signals intelligence, information technology, and language specialists. Phase one basic training is not necessarily cyber-specific, as it is meant to provide military personnel with the basic skills needed to perform a particular occupation for the service. For example, CMF teams include intelligence

professionals who may be assigned to analyze intelligence information that comes from a variety of sources. Training in phases two (foundational), three (collective), and four (sustainment) are focused more directly on the specific skills required to function as a member of the various CMF teams.

Figure 3: Cyber Mission Force (CMF) Training Model Phases, as of June 2018

	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 depending upon occupation.[a]	U.S. Cyber Command	U.S. Cyber Command	U.S. Cyber Command
Training administered by	Services	U.S. Cyber Command vendors, including the National Security Agency and the Defense Cyber Investigations Training Academy.[b] The Army and the Air Force also deliver training for some CMF courses, as approved by U.S. Cyber Command.	Services at the unit level.	Services at the unit level and U.S. Cyber Command vendors.[b]
Description	Provides initial specialty occupation training—it is not necessarily cyber-oriented.	Consists of a specific pipeline of classes that differs by the position a person will fill in the CMF team to which they are assigned (e.g. intelligence analysts will complete different training than linguists).	Consists of activities at the unit level that will prepare personnel to pass U.S. Cyber Command's certification standards. Includes on-the-job training and exercises. Once a team passes the phase three certification event, they are recognized as operationally capable.	Refreshes team certifications continuously. Aims to keep training and skills current, and maintain readiness. Contains many of the same activities from phases two and three, and also includes mission rehearsal exercises.

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

[a]For example, signals intelligence and cryptologic-related training are conducted to the standards of the National Security Agency. However, standards for most of the occupations in the CMF are service-specific.

[b]Responsibility for administering phase two foundational and related phase four sustainment training activities is scheduled to transition from U.S. Cyber Command to the military services beginning in October 2018.

Key Roles and Responsibilities for Training the CMF

To establish and train the CMF teams, DOD has assigned components and senior officials with CMF training roles and responsibilities. The key responsibilities for training the CMF are summarized in table 1 below; a more inclusive list is presented in appendix I.

Table 1: Key Cyber Mission Force (CMF) Training Roles and Responsibilities in the Department of Defense (DOD), as of June 2018

DOD components	Key CMF training roles and responsibilities
U.S. Cyber Command (CYBERCOM)	The command under which the CMF teams are organized. Sets the training and certification standards for all CMF personnel as the joint training lead. For fiscal years 2014 through 2018 CYBERCOM managed funding for phase two foundational training for the CMF.
Secretaries of the Military Departments (Army, Navy, Air Force)	The Secretaries are to establish and conduct individual military training programs to qualify personnel for assignment within the force (training for particular jobs within the military). Establish and conduct individual and collective training programs that align training schedules and curriculums to support joint training for CMF personnel.
DOD Cyber Crime Center	The center administers the Defense Cyber Investigations Training Academy, which provides training to DOD elements that protect DOD information systems. This training includes some of the phase two foundational training for the CMF.
National Cryptologic School	The school serves as the training and education institution of the National Security Agency, which contributes to training a cryptologic workforce, including CMF personnel.

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

Note: These DOD components have a number of roles and responsibilities that are identified in DOD directives, instructions, memorandums, and guidance documents. For the purposes of this table we focused only on these components' CMF training roles and responsibilities.

DOD Has Taken Action to Develop a Trained Cyber Mission Force

As part of the department's efforts to develop and maintain trained CMF teams, CYBERCOM and the military services have implemented a number of initiatives. Specifically, CYBERCOM established consistent training standards, developed standard operating procedures for readiness reporting, and established and maintained a series of phase two foundational training courses. Further, CYBERCOM and the military services used existing training capabilities to build CMF teams. However, many of the teams that have been built are not yet fully trained and, according to agency officials, have "generally low" readiness levels.

CYBERCOM and the Military Services Have Taken Actions to Train CMF Teams

In 2012, CYBERCOM established consistent standards for CMF training phases within its responsibility, and the command has continuously updated those standards, as needed, to meet evolving requirements. Specifically, the command has established and updated the standards for phases two (foundational), three (collective), and four (sustainment) of

CMF training. These standards apply to all military personnel regardless of service affiliation or active/reserve status.

The standards are contained primarily in two documents. First, CYBERCOM issued and has regularly updated the Joint Cyberspace Training and Certification Standards (JCT&CS) to create standardized joint procedures, guidelines, and standards for individual staff and collective training, and to accurately assess CMF teams' ability to perform their missions. This document was most recently revised in February 2018, to update, among other things, the tasks and abilities associated with CMF work roles based on feedback from experts within the military services and CYBERCOM. Second, CYBERCOM published the *CMF Training and Readiness Manual* to serve as the primary training and evaluation guidance for DOD cyber professionals. The *CMF Training and Readiness Manual* has been updated 13 times since it was originally issued in 2013, and it is CYBERCOM's authoritative guide to building and maintaining cyber training and readiness for its personnel. It provides graduated levels of evaluated training that teams can use in preparing for certification and in being certified. Additionally, it identifies approved training events and the mission-essential tasks, associated standards, and key duties for members of CMF teams. The manual requires each team to recertify every 2 years, or upon recovery from a 50 percent or higher turnover of CMF team personnel.

CYBERCOM Developed Standard Operating Procedures for Readiness Reporting

In December 2017, CYBERCOM published standard operating procedures for readiness reporting that CMF teams are to use to assess whether they have the resources and capability to perform their missions.[15] The procedures define CMF readiness reporting guidelines related to personnel, equipment, and training. For example, the document identifies three training metrics that evaluate (1) whether personnel are trained to job qualification standards; (2) whether CMF teams have successfully completed supporting tasks during training exercises, events, or real world operations; and (3) the length of time between formal evaluations. Specifically, the standard operating procedures emphasize that in order to obtain the best training readiness rating, teams must perform an evaluated event or operation at least once every 12 months.

[15]*USCYBERCOM Readiness Reporting Standard Operating Procedure*.

CYBERCOM Established and Maintained a Series of Courses for Individual Foundation Training

CYBERCOM maintains and coordinates a series of CMF courses for phase two foundational training. It develops and administers these course requirements for all of the CMF work roles and requires personnel to complete courses specific to their job responsibilities. All CMF personnel filling a specific mission and role complete the same foundational courses, regardless of military service, employment status—active duty or reserve—or type of CMF team to which they are assigned. For example, all intelligence analysts on CMF teams are to complete the same 14 courses that are specific to their role on the team.

CYBERCOM training directorate officials told us they had to make changes to the training progression over time to adapt to the changing threat environment. Accordingly, CYBERCOM has added, modified, or deleted phase two foundational training courses over the past 4 years. For example, in the past 4 years CYBERCOM consolidated four existing courses into a single introductory cyber course that is taken by all-source intelligence analysts who will be part of CMF teams. In November 2017, the command updated the phase two foundational training requirements by removing three courses that were required for a variety of Cyber Protection Team work roles. CYBERCOM also added a new networking course that is a pre-requisite to a course that comes later in the training progression for Cyber and National Mission Team mission commanders. The most recent update also emphasized that Cyber Protection Team personnel must complete the Intermediate Cyber Core Course, the Cyber Protection Team Core Course, and then their specific methodology courses, in that order.

According to officials from the service cyber components, the changes CYBERCOM has made to its phase two foundational training progression have been transparent and have addressed evolving threats. However, the changes have also negatively affected training time frames, particularly for the CMF teams composed of National Guard and Reserve personnel. Because National Guard and Reserve teams are scheduled to achieve full operational capability after the active duty teams, they are more likely to be subject to the newer training progressions, which in some cases require a few additional days of courses. Officials from the National Guard told us that this additional training time is more difficult to schedule for National Guard and Reserve personnel because—unlike the active duty personnel who are available to train full time—National Guard and reservist personnel are available to train only one weekend per month and generally for 2 weeks of annual training. Additionally, most of these personnel must coordinate time off from their full-time jobs to take the required phase two foundational training courses. To help address

these challenges, CYBERCOM officials told us they use mobile training teams. The Army Cyber School has also used mobile training teams to provide CMF training opportunities to Reserve personnel. The officials from CYBERCOM and the Army told us that the mobile training teams make training more accessible by avoiding the need for the National Guard and Reserve personnel to travel.

CYBERCOM and the Services Used Existing Training Capabilities

DOD has used existing training capabilities—including courses, instructors, and facilities—throughout all phases of CMF training. For example:

- *Joint Cyber Analysis Course*. The Navy's Center for Information Warfare Training is the host for the Joint Cyber Analysis Course—a phase one basic training course for personnel designated for cryptologic roles. CYBERCOM recommends this course for many CMF work roles.
- *Cyber and Cryptologic training institutions.* CYBERCOM has partnered with the Defense Cyber Investigation Training Academy, the Defense Information Systems Agency, the National Security Agency, and military service schoolhouses to deliver phase two foundational training for the CMF. The Defense Cyber Investigation Training Academy offers almost all of the training courses needed by Cyber Protection Teams, and Army officials said they used the expertise and course materials provided by the Defense Cyber Investigation Training Academy to develop Cyber Protection Team training courses that they offer at the Army Cyber School as well. National Security Agency's National Cryptologic School provides a majority of the other phase two foundational CMF training courses. According to officials from CYBERCOM and the National Cryptologic School, reliance on existing training capabilities and expertise from the National Security Agency enabled the command to quickly establish CMF capabilities.
- *Operational events.* CYBERCOM used both simulated and real-world operational events on networks to support the certification of CMF teams. For example, CYBERCOM officials told us that CYBER KNIGHT is a training event offered periodically by CYBERCOM for CMF teams to exercise national and non-national mission sets. CYBER FLAG and CYBER GUARD, also conducted by CYBERCOM on a periodic basis, utilize a dynamic joint cyber training environment and, according to CYBERCOM officials train all types of CMF teams. In addition to using simulated events through exercises, CYBERCOM and military service officials said that teams were allowed to use real-world operations to meet phase three collective training requirements.

The military services and CYBERCOM plan to continue to use existing resources, such as the service school houses, for new and continuous training into the future. For example, as part of their training transition plan, Marine Corps officials reported that they have a contract in place with Navy's Space and Naval Warfare Systems Command to provide additional training to Marine Corps CMF personnel after they complete the phase two foundational training progression. Additionally, the Army Cyber School, which provides CMF-specific training for the Army, currently trains Marine Corps personnel as well. The Army and Marine Corps have training agreements in place to continue this arrangement. Figure 4 below shows a member of the National Guard participating in a cyber training exercise.

Figure 4: A Member of the National Guard Participates in a Cyber Training Exercise, 2018

Source: Defense Visual Information Distribution Service photo by Staff Sgt. Jeremiah Runser. | GAO-19-362

Certified Teams Are Not Fully Trained, But CYBERCOM Is Taking Actions to Improve Training and Readiness

We found that many of the CMF teams for which DOD has reported achieving full operational capability actually require further training, for varying reasons. For example, officials from many key organizations across the DOD cyber enterprise told us that the services moved some personnel among teams, reducing the readiness for teams from which personnel were transferred. Officials from the Office of the Under Secretary of Defense for Personnel and Readiness, Joint Staff, and the

military services cited other challenges affecting CMF team readiness levels as well, including the long time frames needed to obtain the appropriate clearances for CMF personnel and the high pace of operations for the teams, leaving little time for training. The same officials from across DOD's cyber enterprise affirmed that, taken together, these actions and circumstances have had a negative effect on CMF team resource readiness levels.[16] In April 2018, the commander of CYBERCOM acknowledged in testimony that "much works remains to be done to make the personnel proficient at their duties and the whole team ready and able to perform whatever missions might be directed."[17]

The CMF teams were not fully trained and had lower readiness levels because CYBERCOM and the military services focused primarily on the teams' achieving full operational capability by October 1, 2018, rather than on building operational readiness. Building operational readiness requires the teams to simultaneously have the appropriate number of sufficiently trained personnel across the force. According to the *CMF Training Transition Plan*, CYBERCOM's senior leadership directed the command to achieve full operational capability, and it designated that effort as a higher priority than operational readiness.

CYBERCOM officials told us that they recognized the low readiness of the CMF teams and have identified two actions to address the training deficiencies—and associated effects on readiness—for the CMF teams. First, according to the officials, CYBERCOM has developed a system that assigns unique identifiers to each person in the CMF and allows CYBERCOM to easily track when personnel move from one team to another. Second, in December 2017, CYBERCOM issued its readiness reporting standard operating procedure that establishes new readiness reporting guidelines. CYBERCOM officials stated that these guidelines emphasize readiness over the achievement of interim milestones, such as full operational capability. Given that CYBERCOM recently

[16]The military services organize their forces into units (teams) for training and equipping purposes. Joint guidelines require that commanders assess their teams' abilities to perform their core competencies, or their ability to undertake the wartime or primary missions for which they are organized or designed. These classified assessments are based on four distinct resource indicators—personnel, equipment availability, equipment readiness, and how well the team is trained to conducts its missions. Chairman of the Joint Chiefs of Staff Instruction 3401.02B, *Force Readiness Reporting* (Washington, D.C.: May 31, 2011).

[17]Statement of Admiral Michael S. Rogers Before The House Committee on Armed Services Emerging Threats and Capabilities Subcommittee (Apr. 11, 2018).

implemented these efforts to improve the readiness of the CMF teams, and that the quarterly readiness reports indicate improved resource readiness for personnel and training metrics, we are not making recommendations related to this issue. Through our body of work on defense cyber issues, we will continue to monitor DOD's and CYBERCOM's efforts to maintain a ready CMF.

DOD Has Shifted Focus from Building to Maintaining a Trained CMF, but Has Not Taken Key Actions to Maintain Future Training

DOD has taken steps to shift its focus from *building* a trained CMF to *maintaining* this force, but it has not taken key actions to ensure that the department is poised to maintain CMF training following this transition. Specifically, the military services have not developed plans that include time frames for validating all phase two foundational training courses, or that comprehensively assess their training requirements. Further, as of June 2018, CYBERCOM had not provided a plan for establishing independent assessors to evaluate and certify the completion of phase three collective training for CMF teams.

DOD Is Shifting from Building to Maintaining a Trained CMF

DOD officials told us that the department is shifting its focus away from building and toward maintaining a trained CMF. For example, the Army is leading the development of a Persistent Cyber Training Environment. The goal of that training environment is to provide on-demand access to scenarios that Army officials told us will enhance the quality, quantity, and standardization of phase three (collective) and phase four (sustainment) training and exercise events. The Persistent Cyber Training Environment is scheduled to provide some operational capability by 2019, and it is expected to continue to evolve to meet training needs.

In addition to building a Persistent Cyber Training Environment, the department has developed the *CMF Training Transition Plan*, which will transfer administration of phase two foundational training from CYBERCOM to the services. Specifically, beginning in October 2018, the military services will assume responsibility for phase two foundational training of CMF personnel, which CYBERCOM has centrally managed since CMF training began in 2013. Officials from the services and CYBERCOM have held quarterly meetings to help guide the implementation of this plan. According to the *CMF Training Transition Plan*, the transfer is being made in response to a direction in Senate Report 114-49 accompanying a bill for the National Defense Authorization

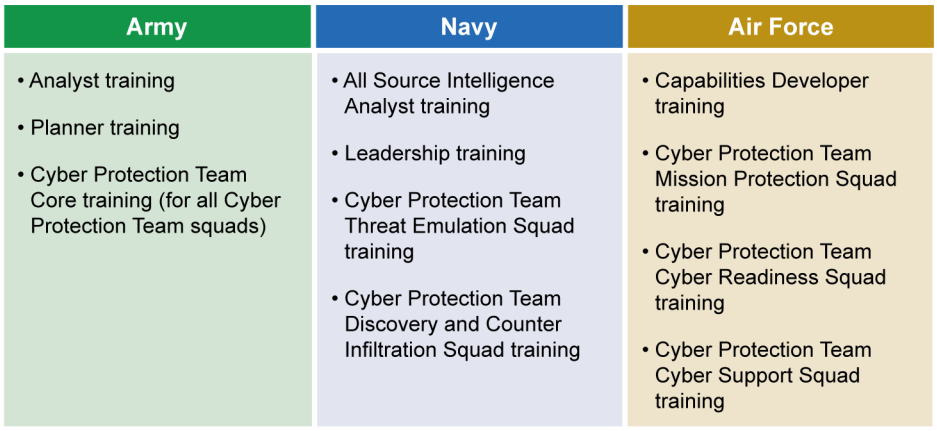
Act for Fiscal Year 2016.[18] The report directed the DOD Principal Cyber Advisor, the Commander, CYBERCOM, and the service secretaries to develop a plan for the military services to complete all required training for the second wave of CMF teams and to maintain individual training capabilities for the existing teams.

In January 2017 the Joint Staff and Principal Cyber Advisor published the *CMF Training Transition Plan*, to transition CMF training to a model that complied with congressional committee direction. The principal goal of this approach is to drive efficiencies and reduce training development and delivery costs. According to the plan, CYBERCOM maintains control of the standards for phase two foundational training, while the Army, Navy, and Air Force are to assume specific joint curriculum lead roles. These roles entail developing joint training plans for the courses under the work roles they are assigned.[19] In addition, the joint curriculum leads (i.e., Army, Navy, and Air Force) are responsible for identifying training gaps and developing learning objectives and courseware based on the CYBERCOM training task list requirements for each of the work roles. For example, under its curriculum lead role, the Army has accepted responsibility for the cyber planner courses. In carrying out this role, the Army developed the Cyber Operations Planners Course and submitted it to CYBERCOM to establish as an approved course for all cyber planners—regardless of service affiliation and of active or reserve duty status—in the CMF. Figure 5 shows the work role categories and responsibilities for which each military service has agreed to be curriculum lead.

[18]See S. Rep. No. 114-49, at 286-287 (2015).

[19]The Marine Corps was not assigned a joint curriculum lead role, and officials from the Marine Corps and CYBERCOM indicated that this was the Marine Corps' choice.

Figure 5: Designated Military Service Curriculum Lead Roles for the Cyber Mission Force, as of May 2018



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

Note: CYBERCOM will continue to be the curriculum lead for operator training but plans to transition operator training curriculum lead responsibility over to a service in the future.

Military Services' CMF Training Transition Implementation Plans Do Not Include Time Frames for Validating Courses or Comprehensive Assessments of Training Requirements

In November 2017, CYBERCOM directed the military services to develop plans to implement their responsibilities in support of the *CMF Training Transition Plan*.[20] In accordance with the training transition plan, the military services will assume responsibility for phase two foundational course validation as part of their joint curriculum lead duties. In February 2018, each of the four services provided a plan to CYBERCOM that, at a minimum, highlighted the efforts each service was taking to prepare for its new training transformation responsibilities, including phase two foundational course validation.

The purpose of course validation is to determine whether a course adheres to CYBERCOM's joint training standards as published in the *Joint Cyberspace Training and Certification Standards* (JCT&CS). CYBERCOM's draft course validation guidance states that validation involves an examination of both the content of the courses, as well as the instructional methods. The manual states that the content should align with the knowledge, skills, and abilities for the appropriate CYBERCOM

[20]The military services on October 1, 2018, are to assume phase two foundational training responsibilities for course validation, training requirements and execution, and individual training equivalency.

work roles and should meet the joint training standard. Further, the manual states that the validation of instructional methods examines how the course is taught and determines whether the methods are appropriate to support desired course outcomes.

CYBERCOM's draft course validation guidance lays out a series of requirements for the validation process, among which are the following:

- The military service that is submitting the course for validation is responsible for assembling course information, providing back-up data about the course, and securing subject matter experts to review the submission.
- The military service that is the joint curriculum lead for the course is responsible for reviewing the submissions and offering recommendations for modifications to courses to reflect joint standards.
- CYBERCOM is responsible for making final determinations of course validity. In this final review, CYBERCOM may hold discussions with key stakeholders, audit the course, review student feedback on the course, or review evaluation data from the course to inform its final validation determination.

Our review of the services' training transition plans found that the Army's and Air Force's plans address course validation to some degree, but they do not identify specific time frames for completing course validation. Specifically, the Army's plan identifies the milestones, dates, and resources for the submission of two of its analyst and planner courses to CYBERCOM for validation, but it does not indicate when the service will submit its Cyber Protection Team Core Training Course for validation. The Air Force's plan establishes a timeline for developing, finalizing, and distributing course validation guidance, but it does not have time frames or milestones indicating a time for beginning the process of submitting courses to CYBERCOM for validation.

Standards for Internal Control in the Federal Government highlights the need to define objectives in specific terms, to include how objectives are to be achieved and time frames for their achievement.[21] For example, the Navy's plan indicates that the four courses for which it is responsible will

[21]GAO-14-704G.

be iteratively validated between fiscal years 2019 and 2021. While a 24-month time frame is broad and it may be challenging for CYBERCOM and the other services to know with precision when the Navy will complete its course validation efforts, the plan includes a time frame that CYBERCOM and the services can use for further discussion and planning purposes.

The plans submitted by the Army and the Air Force indicate that the course validation time frames for phase two foundational courses are unknown because course validation is still dependent upon CYBERCOM's review. The Army's plan includes time frames for submitting to CYBERCOM two of the three courses it is responsible for developing, but one of the courses does not have any time frames. Further, the Air Force plan includes time frames for developing guidance on how to perform course validation that only carry it through September 2018; it does not have time frames for actually carrying out its course validation processes.

As the military services assume phase two foundational training responsibilities from CYBERCOM, it is important that they coordinate with CYBERCOM to establish a timeline for course validation, as appropriate. With a clearer idea of which information can appropriately be removed from training courses, the services will be able to make informed decisions to balance the cost-effectiveness of the training with delivering trained cyber personnel to CMF teams more quickly. However, without an established time frame to assess and validate the efficiency and effectiveness of all phase two individual foundational training against established expectations, DOD will not be well positioned to reasonably assure that the phase two foundational training meets the needs of the CMF and its mission.

The Military Services' Plans Do Not Comprehensively Assess Personnel Training Requirements

Training plans should be detailed enough to provide insight into the number of people needed to fill specific positions to sustain an organization. As part of the training transition process, CYBERCOM required the military services to submit implementation plans that identify, among other things, training requirements and execution. Also, according to our prior work published in *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, training plans should be designed to determine the skills and competencies a workforce needs to prepare for current, emerging, and future agency needs in pursuit of its missions. These needs include the size of the workforce; its deployment across the organization; and the knowledge, skills, and abilities needed for the agency to pursue its current and future missions. To ensure a strategic workforce planning approach,

it is important that agencies consider how hiring, training, and other human capital strategies can be aligned to support mission success.[22]

The Army, Navy, and Air Force developed training transition implementation plans to address training requirements and execution to some degree, but the plans do not identify the number of personnel or teams and the specific training activities needed across all phases of training to maintain the CMF. For example, neither the Army nor the Air Force plan identifies the number (average or total) of personnel for each of the work roles described in figure 2 (for example, cyber operators, intelligence analysts, linguists) that the military services need to complete phase two foundational training courses to maintain the appropriate sizing and deployment of personnel across CMF teams. Additionally, the Army and Air Force plans do not identify the number of personnel or teams needed to conduct phase three (collective) and phase four (sustainment) training in future years. In contrast, the Navy's plan identifies the average number of personnel who would need to take specific phase two foundational courses—including those being developed by other services and CYBERCOM—to maintain its CMF teams. However, the Navy's plan does not include this same information for phases three and four of training. The Marine Corps did not address training requirements and execution within its implementation plan.

According to officials from the Army and the Air Force, the February 2018 documents they provided in response to CYBERCOM's requirement do not include plans that identify training requirements because submission of that information was not required by CYBERCOM. However, a November 2017 CYBERCOM memorandum clearly directed the military services with joint curriculum lead responsibilities to submit plans that support implementation of the department's *CMF Training Transition Plan*, including training requirements execution data.[23]

Having a comprehensive plan that identifies the number of personnel or teams needed to accomplish specific training activities would help the services to better manage the number of personnel who need to be rotated into the CMF teams. It would also help the military services coordinate with each other on course offerings by providing situational awareness of the number of personnel from other services who could

[22]GAO-04-546G.

[23]U.S. Cyber Command Memorandum, Nov. 28, 2017.

attend their courses in any given year. For example, the Air Force would know how many Army, Navy, and Marine Corps personnel would attend the courses being offered by the Air Force. Without a plan that comprehensively assesses and identifies the services' training needs for each type of personnel, DOD cannot reasonably ensure that its training plan will support the transition to a joint training model or be aligned with its stated goal to maintain a trained and ready force.

CYBERCOM Was Unable to Provide a Plan for Establishing Independent Assessors for Phase Three Collective Training

As of June 2018, CYBERCOM had not provided a plan for establishing independent assessors to evaluate and certify the completion of phase three collective training for CMF teams. CYBERCOM's *CMF Training and Readiness Manual* explains that evaluations are necessary to assess readiness and provide commanders with a process to determine a team's proficiency in the tasks it must perform during a mission. Assessors play an important role in this evaluation process by judging the performance of CMF teams using CYBERCOM's evaluation forms, which establish common evaluation criteria to determine whether the team being evaluated has met the certification standards. CYBERCOM officials told us that to evaluate teams completing phase three certification through CYBERCOM events (approximately 50 percent, according to agency officials), the command provided a joint team of assessors. CYBERCOM and service officials told us that the services provided their own assessors for teams that completed phase three training through their respective service-hosted exercises.

In discussions with Army and Air Force officials, they identified two challenges they have experienced with the services providing assessors to evaluate their own teams, which could lead to subjectivity in CMF team evaluations. First, in some instances the assessors have come from within the same chain of command as the CMF team and thus are not truly independent. *Standards for Internal Control in the Federal Government* discusses the importance of segregation of duties in designing control activities so that incompatible duties are segregated in order to mitigate the risk of management override of internal control. In this case, having an assessor from the same chain of command evaluate a CMF team's performance in a certification event presents an increased risk of fraud through management override.

Second, while the *CMF Training and Readiness Manual* includes checklists that assessors can use to evaluate team performance, according to service officials, the manual does not provide clear guidance on how to evaluate whether the tasks and performance standards have

been sufficiently met by the team. The absence of such information could lead to subjective evaluations as to whether a team met the desired performance standard. According to one service official, these challenges could be addressed if CYBERCOM were to provide an expert who evaluates the training tasks and performance standards—an action that could lead to a more consistent application of evaluation criteria.

When we asked officials from CYBERCOM's training directorate about whether the command could provide more oversight for certification events, the officials acknowledged that, among other tasks, the command is responsible for ensuring that assigned joint cyber forces are trained, certified, and interoperable with other forces. The officials said that to do this, the command will use established training standards and develop a plan to train and certify CMF team evaluators to a set of standardized criteria. Command officials said they believe this will enable the services and CMF teams to have qualified assessors who are trained and certified by CYBERCOM to consistently evaluate the performance of the CMF teams based on joint standards. With this capability, for example, a Navy Cyber Protection Team assessor can be used by an Army Cyber Protection Team to evaluate that team in an operation, exercise, or training event. This training capacity should enhance the interoperability between the services and allow for consistent evaluation of a team's performance.

However, as of June 2018, CYBERCOM had not provided a plan to train and certify assessors from across the services; as such a plan had not yet been developed. *Standards for Internal Control in the Federal Government* explains that in defining objectives, management should clearly define what is to be achieved, how it will be achieved, and the time frames for achievement.[24] Documenting these objectives in a plan also will help formalize the new process and ensure that the appropriate managerial emphasis is given to the effort. DOD has used similar mechanisms to implement changes to cyber training in the past, such as developing the *CMF Training Transition Plan* in response to moving phase two foundational training responsibility from CYBERCOM to the military services. Since phase three certification events act as a quality control mechanism for CMF teams, it is important that the events be independently evaluated to ensure that CMF teams are trained to a consistent standard. Without a documented plan to train and certify

[24]GAO-14-704G.

assessors to evaluate CMF phase three collective training certification events, the CMF teams will not be consistently evaluated as they are operationally certified.

CYBERCOM Has Leveraged Other Cyber Experience to Meet Training Requirements, but It Has Not Established Master Training Task Lists for Courses

CYBERCOM Has Established a Training Exemption Process for CMF Personnel Who Have Relevant Prior Experience

CYBERCOM assesses the prior experience of CMF personnel to meet training requirements through a process known as individual training equivalency. This process allows personnel to be exempted from specific training courses by showing that they have already met the learning objectives of the course through their prior experience. CYBERCOM established an Individual Training Equivalency Board consisting of subject matter experts and representatives from CYBERCOM, the National Security Agency, and service cyber components who review the applications and recommend whether equivalency should be granted. The Individual Training Equivalency Board reviewed approximately 700 applications for equivalency from September 2013 through April 2018, and more than three-quarters of those applicants had at least one course exemption approved.

According to officials from CYBERCOM's training directorate, which is responsible for administering the individual equivalency process, there are a number of reasons why requests for course exemptions are not approved. For example, some applicants are denied for administrative reasons, such as not filling out the paperwork correctly. Also, applicants are not eligible to receive exemptions for courses that are not part of their work role requirements, but some personnel try to do so. Officials also said that board members do not deem some applicants' reported experiences as comparable to the knowledge and skills they would obtain from taking courses for which they seek exemptions.

Based on our review CYBERCOM's memorandums that document the approval or disapproval of approximately 700 individual requests for training exemptions, we observed that applicants typically requested exemptions for multiple courses, with some seeking exemptions for up to 16 courses. Altogether during this period, we found that CYBERCOM granted more than 1,400 equivalencies for approximately 90 different phase two foundational training courses. Certain courses were exempted more often than others. For example, the course for which CYBERCOM most frequently granted individual exemptions was the Joint Advanced Cyber Warfare Course. This 4-week course provides an orientation to CYBERCOM, the global cryptologic platform, the intelligence community, and allies and major partners in the conduct of cyber warfare operations, planning, and analysis of effects.

Other courses that were commonly granted training exemptions included 1-week courses related to computer network exploitation, cyber offensive and defensive operations, and understanding network and operating system fundamentals. These courses teach the basic skills associated with performing CMF operations. Additionally, we found that CYBERCOM's Individual Training Equivalency Board approved approximately 50 exemptions for Intermediate Cyber Core, which is an 8-week course that CYBERCOM training officials described as providing the background and proficiency needed to identify, understand, and navigate the digital environment. The officials said that the course also provides an understanding of network operational methods and offensive and defensive cyber operation principles.

CYBERCOM Has Not Established Master Training Task Lists for Courses

CYBERCOM has not established master training task lists for phase two foundational training, a key set of standards the services are to use in preparing course equivalency standards. The task lists correlate to the knowledge, skills, and abilities that the services will use to develop learning objectives and course materials for training. They are also important in informing the services' ability to make equivalency application determinations because they form the learning objectives of the courses that may be bypassed. To determine whether an applicant's experience is equivalent to what would be taught in a course; the entity making the decision must know the learning objectives of the course. However, as of May 2018, CYBERCOM officials were unable to provide

evidence that the command had developed master training task lists for phase two foundational CMF training courses, as required.[25]

The January 2017 *CMF Training Transition Plan* required CYBERCOM to provide all mission and support team master training task lists for the phase two foundational training courses to the military services no later than March of 2018. Service and CYBERCOM officials said that they are holding monthly meetings to provide updates related to the training standards and other training transition-related information, but as of May 2018, CYBERCOM officials had not confirmed that they had provided the master training task lists to the services. Officials from the services told us that they need these master training task lists to develop clear decision rules as they assume responsibility for making equivalency decisions for phase two foundational training courses.

When we interviewed CYBERCOM in February of 2018, officials told us that they were not aware of the requirement established in the *CMF Training Transition Plan*, but said they would start developing the master training task lists. Establishing clear standards is particularly important at this time, because the services are scheduled to assume responsibility for administration of the individual training equivalency process for Cyber Protection Team phase two foundational training courses in October 2018.

Until CYBERCOM establishes and disseminates the master training task lists for phase two foundational CMF courses, the military services are at risk of developing inconsistent decision rules for their training equivalency processes, and the development of such processes could be delayed, resulting in the funding of training that is unnecessary.

Conclusions

Developing and maintaining a trained cyber mission force is imperative to DOD's ability to achieve its missions in the connected world within which it operates. DOD has made progress toward its goals of building and maintaining a trained cyber mission force. As DOD starts to focus on maintaining a ready CMF, addressing gaps in its training plans and structure will help it reach those goals. The Army's and Air Force's lack of time frames, like those established by the Navy in its implementation

[25]Master training task lists describe each task that must be performed in the operation and maintenance of a system. They also include the successful performance criteria for those tasks in the context of a mission.

plan, for validating phase two foundational training could contribute to training inefficiency and unnecessarily long time frames for training personnel. Further, the military services, by not clearly identifying the number of personnel they need to train, hinder planning and coordination efforts to ensure that the training infrastructure is sufficient and is used efficiently. In addition, the absence of a plan for CYBERCOM to establish independent assessors for phase three collective training certification events may lead to teams being certified to different standards. Also, not having the master training task lists necessary to establish clear decision rules for granting individual training exemptions for phase two foundational training courses may contribute to inconsistent personnel skill levels and inefficient use of training resources. Focusing on maintaining sustainable readiness, as DOD has already begun to do, and addressing these weaknesses can lead to long-term improvements in the capability and capacity of its CMF.

Recommendations for Executive Action

We are making eight recommendations to DOD.

The Secretary of Defense should ensure that the Army, in coordination with CYBERCOM and the National Cryptologic School, where appropriate, establish a time frame to validate all of the phase two foundational training courses for which it is responsible. (Recommendation 1)

The Secretary of Defense should ensure that the Air Force, in coordination with CYBERCOM and the National Cryptologic School, where appropriate, establish a time frame to validate all of the phase two foundational training courses for which it is responsible. (Recommendation 2)

The Secretary of the Army should ensure that Army Cyber Command coordinate with CYBERCOM to develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment), in order to maintain the appropriate sizing and deployment of personnel across the Army's CMF teams. (Recommendation 3)

The Secretary of the Navy should ensure that Fleet Cyber Command coordinate with CYBERCOM to develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases three (collective) and four (sustainment) in order to maintain the

appropriate sizing and deployment of personnel across the Navy's CMF teams. (Recommendation 4)

The Secretary of the Air Force should ensure that Air Forces Cyber coordinate with CYBERCOM to develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment), in order to maintain the appropriate sizing and deployment of personnel across the Air Force's CMF teams. (Recommendation 5)

The Commandant of the Marine Corps should ensure that Marine Corps Forces Cyberspace coordinate with CYBERCOM to develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment), in order to maintain the appropriate sizing and deployment of personnel across the Marine Corps' CMF teams. (Recommendation 6)

The Secretary of Defense should ensure that the commander of CYBERCOM develops and documents a plan for establishing independent assessors to evaluate CMF phase three collective training certification events. (Recommendation 7)

The Secretary of Defense should ensure that the commander of CYBERCOM establishes and disseminates the master training task lists covered by each phase two foundational training course and convey them to the military services, in accordance with the *CMF Training Transition Plan*. (Recommendation 8)

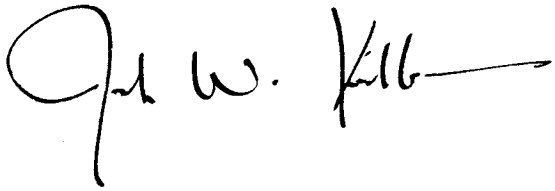
Agency Comments

We provided a draft of the FOUO version of this product to DOD for review and comment and worked with the department to develop this unclassified product. In its comments on the FOUO version of this, reproduced in appendix II, DOD concurred with our recommendations. DOD also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to appropriate congressional committees; the Secretary of Defense, the office of the Principal Cyber Advisor, the Office of the Under Secretary of Defense for Personnel and Readiness, the Office of the Deputy Assistant Secretary of Defense for Cyber Policy, the Commander of CYBERCOM, the leadership of each of the service cyber components, and the director of the National Security

Agency's National Cryptologic School. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Joseph W. Kirschbaum
Director
Defense Capabilities and Management

Appendix I: Roles and Responsibilities for Cyber Mission Force Training

Based on our review of related statutes, Department of Defense (DOD) instructions and directives, and other guidance, we found that various DOD officials have been assigned a variety of CMF training roles and responsibilities, summarized in table 1 below.

Table 2: Cyber Mission Force (CMF) Training Roles and Responsibilities in the Department of Defense (DOD), as of May 2018

DOD senior officials and components	CMF training roles and responsibilities
Under Secretary of Defense for Personnel and Readiness	Serves as the principal staff assistant and advisor for total force management, including readiness and training, and military and civilian personnel requirements. Supports implementation of cybersecurity requirements for effective manning, management, and readiness assessment of the cybersecurity workforce.
Under Secretary of Defense for Policy	Serves as the principal staff assistant and advisor to the Secretary of Defense for all matters on the formulation of national security and defense policy and the integration and oversight of DOD policy and plans to achieve national security objectives. Coordinates with DOD's Chief Information Officer to ensure that cybersecurity strategies, policies, and capabilities are aligned with overarching DOD cyberspace policy.
Under Secretary of Defense for Acquisitions, Technology, and Logistics[a]	Oversees all DOD cyber-capability acquisitions; establishes the architecture for a DOD enterprise-wide interoperable test capability; and ensures information assurance training of the DOD acquisition workforce.
Under Secretary of Defense for Intelligence	Serves as principal staff assistant and advisor to the Secretary of Defense regarding intelligence, counterintelligence, and intelligence-related matters. Has primary responsibility for management and program review of individual, collective, and staff training programs for intelligence skills and intelligence-related foreign language skills, which feed into the CMF.
DOD Chief Information Officer	Oversees management of DOD cyberspace information technology and cybersecurity workforce. Coordinates with the National Institute of Standards and Technology in development of cybersecurity-related standards and guidelines. Responsible for policy, oversight, and guidance for the architecture and programs related to DOD's networking and cyber defense.
Principal Cyber Advisor	Principal advisor to the Secretary of Defense on cyber-related activities, including policy and operational considerations, resources, personnel, acquisition, and technology. Oversees implementation of the DOD Cyber Strategy and other relevant policy and planning documents to help achieve DOD's cyber mission, goals, and objectives, including tasks on building and maintaining the CMF and operationalizing a persistent cyber training environment.
Chairman of the Joint Chiefs of Staff	Establishes training policy guidelines for various training systems, validates training capability requirements, and addresses joint training program and joint training support deficiencies and trends. Manages joint force training in coordination with combatant command and military department leaders. Provides staff for the Cyber Force Model Implementation Tiger Team, which supports the establishment and sustainment of the CMF by working to resolve challenges that span combatant command and military service equities.
U.S. Cyber Command (CYBERCOM)	The organization under which the CMF teams are organized. Sets the training and certification standards for all CMF personnel as the Joint Training Lead. For fiscal years 2014 through 2018 managed funding for phase two foundational training for the CMF.
Secretaries of the Military Departments (Army, Navy, Air Force)	Establish and conduct individual military training programs to qualify personnel for assignment within the force (training for particular jobs within the military). Establish and conduct individual and collective training programs, align training schedules, and align curricula to support joint training for CMF personnel.

DOD senior officials and components	CMF training roles and responsibilities
Secretary of the Army	The DOD Executive Agent for cyber training ranges, responsible for developing, coordinating, and integrating plans to synchronize activities across the designated cyber training ranges and establishing appropriate training infrastructure and standards in order to provide a realistic, scalable, and persistent training range architecture.
Army Cyber Center of Excellence	The Army organization primarily responsible for managing doctrine, organization, training, materiel, leadership and education, personnel, and facilities for cyberspace operations. A major aspect of the Cyber Center of Excellence's mission is the training and education of cyber professionals through the Army Cyber School.
DOD Cyber Crime Center	An entity within the Department of the Air Force that develops and provides specialized cyber investigative training for DOD and non-DOD personnel. Operates the Defense Cyber Investigations Training Academy, which provides training to DOD elements that protect DOD information systems. This training includes some of the phase two foundational training for the CMF.
National Cryptologic School	The training and education institution of the National Security Agency, which is also a component of the Cryptologic Training System, a system established to train a competent military and civilian cryptologic workforce. CMF personnel receive training from the National Cryptologic School and other Cryptologic Training System members.
Defense Information Systems Agency	Provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. Provided some phase two foundational training courses for CMF personnel.[b]

Source: GAO analysis of DOD information. | GAO-19-362

Note: These DOD components and senior officials have a number of roles and responsibilities that are identified in DOD directives, instructions, memorandums, and guidance documents. For the purposes of this table we focused on these components' CMF training roles and responsibilities.

[a]Section 901 of the National Defense Authorization Act for Fiscal Year 2017 directs the reorganization of the position of Under Secretary of Defense for Acquisition, Technology, and Logistics by February 2018 into two separate Under Secretaries of Defense: an Under Secretary of Defense for Research and Engineering and an Under Secretary of Defense for Acquisition and Sustainment. As of June 1, 2018, this organizational change was still being implemented.

[b]Officials from the military services reported and representatives from the Defense Information Systems Agency confirmed that, as of March 2018, the classes that the Defense Information Systems Agency provided to CMF personnel would be provided by the Defense Cyber Investigations Training Academy.

Appendix II: Comments from the Department of Defense

Note: Since the recommendations in this unclassified report are the same as the For Official Use Only (FOUO), which the Department of Defense (DOD) commented on in the letter included in this appendix, we did not seek additional DOD comments on this unclassified version of the report. The report GAO-18-551SU that DOD reviewed was renumbered to GAO-19-142SU to reflect that it was issued in Fiscal Year 2019.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

READINESS

SEP 2 6 2018

Mr. Joseph Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Kirschbaum:

Thank you for the opportunity to review and provide the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-18-551SU, *DOD TRAINING: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, dated July 27, 2018 (GAO Code 102226). The DoD concurs with the attached GAO recommendations.

The point of contact for this effort is Mr. Fred Engle, and he can be reached at (703) 693-3478 or frederick.c.engle.civ@mail.mil. Thank you again for the opportunity to review this report.

for: C. F. Drummond
Deputy Assistant Secretary of Defense
for Force Education and Training

Attachments:
As stated

GAO DRAFT REPORT DATED JULY 27, 2018
GAO-18-551SU (GAO CODE 102226)

"DOD TRAINING: U.S. CYBER COMMAND AND SERVICES SHOULD TAKE ACTIONS TO MAINTAIN A TRAINED CYBER MISSION FORCE"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense ensure that the Army, in coordination with USCYBERCOM and the National Cryptologic School, where appropriate, establish a timeframe to validate all of the phase two foundation training courses for which it is responsible.

DoD RESPONSE: Concur.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense ensure that Secretary of the Air Force, in coordination with USCYBERCOM and the National Cryptologic School, where appropriate, establish a timeframe to validate all of the phase two foundation training courses for which it is responsible.

DoD RESPONSE: Concur.

RECOMMENDATION 3: The GAO recommends that the Secretary of the Army ensure that Army Cyber Command develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment) to maintain the appropriate sizing and deployment of personnel across the Army's CMF teams.

DoD RESPONSE: Concur.

RECOMMENDATION 4: The GAO recommends that the Secretary of the Navy ensure that Fleet Cyber Command develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases three (collective) and four (sustainment) to maintain the appropriate sizing and deployment of personnel across the Navy's CMF teams.

DoD RESPONSE: Concur.

RECOMMENDATION 5: The GAO recommends that the Secretary of the Air Force ensure that Air Forces Cyber develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment) to maintain the appropriate sizing and deployment of personnel across the Air Force's CMF teams.

DoD RESPONSE: Concur.

RECOMMENDATION 6: The GAO recommends that the Commandant of the Marine Corps ensure that Marine Corps Forces Cyberspace develop a plan that comprehensively assesses and identifies specific CMF training requirements for phases two (foundational), three (collective), and four (sustainment) to maintain the appropriate sizing and deployment of personnel across the Marine Corps' CMF teams.

DoD RESPONSE: Concur.

RECOMMENDATION 7: The GAO recommends that the Secretary of Defense ensure that the commander of USCYBERCOM develops and documents a plan for establishing independent assessors to evaluate CMF phase three collective training certification events.

DoD RESPONSE: Concur.

RECOMMENDATION 8: The GAO recommends that the Secretary of Defense ensure that the commander of CYBERCOM establishes and disseminates the master training task lists covered by each phase two foundational training course and convey them to the military services, in accordance with the *CMF Training Transition Plan*.

DoD RESPONSE: Concur.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or KirschbaumJ@gao.gov

Staff Acknowledgments

In addition to the individual named above, Tommy Baril, Assistant Director; Tracy Barnes; Patricia Farrell Donahue; Ashley Houston; Amie Lesser; Randy Neice; Geo Venegas; and Cheryl Weissman made key contributions to this report.