United States Government Accountability Office

Report to Congressional Committees

September 2016

DEFENSE CIVIL SUPPORT

DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises

GAO-16-574

September 2016

DEFENSE CIVIL SUPPORT

DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises

GAO Highlights

Highlights of GAO-16-574, a report to congressional committees.

Why GAO Did This Study

The DOD 2015 Cyber Strategy reported that a cyber attack could present a significant risk to U.S. national security. House Report 114-102 included a provision that GAO assess DOD's plans for providing support to civil authorities for a domestic cyber incident.

This report assesses whether (1) the National Guard has developed and DOD has visibility over capabilities that could support civil authorities in a cyber incident; and (2) DOD has conducted and participated in exercises to support civil authorities in cyber incidents and any challenges it faced. To conduct this review, GAO examined DOD and National Guard reports, policies, and guidance and interviewed officials about the National Guard's capabilities in defense support to civil authorities. GAO also reviewed after-action reports and interviewed DOD officials about exercise planning.

What GAO Recommends

GAO recommends that DOD maintain a database that identifies National Guard cyber capabilities, conduct a tier 1 exercise to prepare its forces in the event of a disaster with cyber effects, and address challenges from prior exercises. DOD partially concurred with the recommendations, stating that current mechanisms and exercises are sufficient to address the issues highlighted in the report. GAO believes that the mechanisms and exercises, in their current formats, are not sufficient and continues to believe the recommendations are valid, as described in the report.

View GAO-16-574. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

National Guard units have developed capabilities that could be used, if requested and approved, to support civil authorities in a cyber incident; however, the Department of Defense (DOD) does not have visibility of all National Guard units' capabilities for this support. GAO found three types of cyber capabilities that exist in National Guard units:

- **Communications directorates**: These organizations operate and maintain the National Guard's information network.
- **Computer network defense teams**: These teams protect National Guard information systems, could serve as first responders for states' cyber emergencies, and provide surge capacity to national capabilities.
- **Cyber units**: These teams are to conduct cyberspace operations.

However, DOD does not have visibility of all National Guard units' cyber capabilities because the department has not maintained a database that identifies the National Guard units' cyber-related emergency response capabilities, as required by law. Without such a database to fully and quickly identify National Guard cyber capabilities, DOD may not have timely access to these capabilities when requested by civil authorities during a cyber incident.

DOD has conducted or participated in exercises to support civil authorities in a cyber incident or to test the responses to simulated attacks on cyber infrastructure owned by civil authorities, but has experienced several challenges that it has not addressed. These challenges include limited participant access because of a classified exercise environment, limited inclusion of other federal agencies and critical infrastructure owners, and inadequate incorporation of joint physical-cyber scenarios. In addition to these challenges, DOD has not identified and conducted a "tier 1" exercise—an exercise involving national-level organizations and combatant commanders and staff in highly complex environments. A DOD cyber strategy planning document states, and DOD officials agreed, that such an exercise is needed to help prepare forces in the event of a disaster with physical and cyber effects. Until DOD identifies and conducts a tier 1 exercise, DOD will miss an opportunity to fully test response plans, evaluate response capabilities, assess the clarity of established roles and responsibilities, and address the challenges DOD has experienced in prior exercises. The table below shows selected DOD-conducted exercises.

Selected DOD Exercises Designed to Support Civil Authorities During or After a Cyber Incident

Exercise title	Exercise host	Fiscal year	Cyber civil-support objective
Cyber Guard 15	U.S. Cyber Command	2015	Test DOD participation in a response to a cyberattack of significant consequence against U.S. critical infrastructure.
Cyber Shield 2015	Army National Guard	2015	Train and evaluate U.S. Army National Guard computer network defense teams in a civil-support scenario.
Vista Host II	North American Aerospace Defense Command and U.S. Northern Command	2015	Examine planning assumptions, potential resource requirements, and roles and responsibilities associated with cyber-related defense support to civil authorities operations.

Source: GAO analysis of DOD documentation | GAO-16-574

Contents

Abbreviations

DHS	Department of Homeland Security
DOD	Department of Defense
DSCA	Defense Support of Civil Authorities
ODASD	Office of the Deputy Assistant Secretary of Defense

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

September 6, 2016

Congressional Committees

The *Presidential Policy Directive on United States Cyber Incident Coordination* states that significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure in the United States.[1] DOD recognizes that a disruptive, manipulative, or destructive cyber attack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected[2] and that the department must be prepared to support civil authorities in all domains—including cyberspace.[3] DOD could support such an effort with capabilities from across the military—such as the National Security Agency, military services, U.S. Cyber Command, and the National Guard—through the department's Defense Support of Civil Authorities (DSCA) mission.

DOD has stated that the National Guard offers a unique capability for supporting the department's DSCA mission and represents a critical surge capacity for cyber responders.[4] According to the 2008 *National Response Framework*, exercises (i.e. training events) can play an instrumental role in preparing organizations to respond to an incident by providing opportunities to test response plans, evaluate response capabilities, assess the clarity of established roles and responsibilities, and improve proficiency in a simulated, risk-free environment.[5] Well-

[1]*Presidential Policy Directive—United States Cyber Incident Coordination/PPD-41* (July 26, 2016).

[2]See DOD, *The Department of Defense Cyber Strategy* (April 2015). (Hereinafter referred to as the *DOD Cyber Strategy*).

[3]See DOD, *Strategy for Homeland Defense and Defense Support of Civil Authorities* (February 2013).

[4]The *DOD Cyber Strategy* and DOD, *Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense* (Aug. 21, 2014).

[5]DHS, *National Response Framework* (Washington, D.C.: January 2008). The 2008 National Response Framework was revised and superseded by publication of the 2nd edition in 2013 and the 3rd edition in 2016. The National Response Framework is a component of the National Preparedness System mandated by *Presidential Policy Directive 8/PPD 8: National Preparedness.* The 2016 framework reiterates the principles and concepts of the 2008 and 2013 versions.

designed exercises can improve interagency coordination and communications, highlight capabilities gaps, and identify opportunities for improvement.

We have previously reported on progress DOD has made to address issues related to DSCA. In June 2015, we testified on the progress DOD had made in implementing our prior recommendations to support civil authorities including strengthening the department's strategy, plans, and guidance; interagency coordination; and capabilities.[6] We found that DOD had taken action to address some of our prior recommendations, but had not fully addressed others. For example, DOD had improved interagency coordination for support of civil authorities by defining interagency roles and responsibilities and had identified capabilities it could provide for DSCA. However, DOD had not issued implementation guidance on the use of dual-status commanders, as we had recommended.[7] According to DOD, as of May 2016, the Assistant Secretary of Defense for Homeland Defense and Global Security had drafted a DOD instruction that provides policy and guidance on dual-status commanders and the instruction was in the approval process. In April 2016, we reported on the extent to which DOD had developed guidance that clearly defines the department's DSCA roles and responsibilities in response to domestic cyber incidents.[8] We reported that DOD guidance does not clarify the roles and responsibilities of key DOD entities—such as DOD components, the supported command, and the dual-status commander—that may be

[6]GAO, *Civil Support: DOD Is Taking Action to Strengthen Support of Civil Authorities*, GAO-15-686T (Washington, D.C.: June 10, 2015).

[7]Dual-status commanders are commissioned officers (Army or Air Force or a federally recognized Army National Guard or Air National Guard officer) who serve as an intermediate link between the separate chains of command for state and federal forces and have authority over both National Guard forces under state control and active-duty forces under federal control during a civil-support incident or special event.

[8]GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

called upon to support a cyber incident.[9] We recommended that DOD issue or update guidance that clarifies roles and responsibilities for relevant entities and officials to support civil authorities as needed in a cyber incident. DOD concurred with our recommendation and stated that it will issue or update guidance, as appropriate, that will clarify these roles and responsibilities.

House Report 114-102 included a provision that GAO assess DOD's plans for providing support to civil authorities related to a domestic cyber incident.[10] This report assesses whether (1) the National Guard has developed cyber capabilities that could support civil authorities in response to a cyber incident and DOD has visibility over those capabilities and (2) DOD has conducted and participated in exercises to support civil authorities in cyber incidents, and any challenges it faced in doing so.

To assess the extent to which the National Guard has developed cyber capabilities that could support civil authorities in response to a cyber incident and DOD has visibility over those capabilities, we reviewed DOD policies and guidance to identify the National Guard's role in providing DSCA, National Guard cyber capabilities, and the mechanisms used to identify National Guard capabilities. Specifically, we reviewed Joint Publication 3-28, *Defense Support of Civil Authorities*; DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)*; DOD Instruction 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities*; and DOD Directive 7730.65, *Department of Defense*

[9]DOD defines "DOD components" to include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the DOD Office of Inspector General, the defense agencies, the DOD field activities, and all other entities within DOD. A supported combatant commander has primary responsibility for all aspects of an operation including capability requests, identifying tasks for DOD components, and developing a plan to achieve the common goal. Supporting combatant commanders provide the requested assistance, as available, to assist the supported combatant commander to accomplish missions.

[10]See H.R. Rep. No. 114-102 at 289-290 (2015).

Readiness Reporting System (DRRS).[11] We compared the DOD guidance documents listed above and the information we received in our interviews to the requirement for identifying National Guard emergency response capabilities listed in the United States Code.[12] Additionally, we discussed National Guard unit cyber capabilities and capability identification mechanisms with officials from DOD involved in DSCA, including from the National Guard Bureau, the Army National Guard, and the Air National Guard. After pre-testing our interview questions with officials from the Maryland National Guard and meeting with the Colorado National Guard, we interviewed officials from a non-generalizable sample of state National Guard cyber units from Georgia, Nevada, and Washington regarding their cyber civil-support roles and responsibilities, cyber capabilities, and capability identification mechanisms. We judgmentally selected these states based on factors such as the type and number of cybersecurity teams in the state, and the participation of teams in cyber civil-support exercises. Our findings regarding the capabilities identified during our interviews with these National Guard units are not generalizable to all state National Guard cyber units and do not reflect an exhaustive list of National Guard cyber capabilities. While some of the National Guard capabilities could be used to support their respective state missions, our focus was on National Guard capabilities that could be used in DOD's DSCA mission.

To assess the extent to which DOD has conducted and participated in exercises to support civil authorities in cyber incidents and any challenges it faced in doing so, we reviewed the *DOD Cyber Strategy*, the *Strategy for Homeland Defense and Defense Support of Civil Authorities*, and DOD's joint doctrine for DSCA. We also reviewed these documents to determine the types of exercises in which DOD should be conducting or participating. We then identified a non-generalizable sample of relevant exercises from fiscal years 2013 through 2015 by reviewing DOD

[11]Joint Chiefs of Staff, Joint Publication 3-28, *Defense Support of Civil Authorities* (July 31, 2013) (Hereinafter cited as Joint Publication 3-28); DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)* (Dec. 29, 2010) (incorporating change 1, Sept. 21, 2012) (Hereinafter cited as DOD Directive 3025.18); DOD Instruction 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities* (July 26, 2013); and DOD Directive 7730.65, *Department of Defense Readiness Reporting System* (*DRRS)* (May 11, 2015) (Hereinafter cited as DOD Directive 7730.65).

[12]See 10 U.S.C. § 113 (note).

exercise planning documentation and by interviewing knowledgeable officials from DOD and the Department of Homeland Security (DHS). We chose this timeframe because it allowed us to identify a range of exercises for review and to identify any trends over time. We selected exercises where DOD trained for its role in supporting civil authorities during a domestic cyber incident. To examine DOD planning for conducting future exercises related to civil support for cyber incidents, we compared DOD planning documentation to DOD guidance for exercises, such as the *DOD Cyber Strategy* and Joint Publication 3-28. We also interviewed officials from the Office of the Deputy Assistant Secretary of Defense (ODASD) for Cyber Policy, National Guard Bureau, U.S. Northern Command, and U.S. Cyber Command.

We conducted this performance audit from June 2015 to September 2016 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. See appendix I for a detailed description of the scope and methodology for this report.

Background

Defense Support of Civil Authorities

Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), when state capabilities and resources are overwhelmed and the President of the United States declares an emergency or disaster, the governor of an affected state can request assistance from the federal government for major disasters or emergencies.[13] Additionally, under the Economy Act, a federal agency

[13]See Pub. L. No. 100-707 (1988) (codified as amended at 42 U.S.C. § 5121, et seq.). The Stafford Act aims to provide a means of assistance by the federal government to state and local governments in responding to a presidentially declared major disaster or emergency. A governor's request for the President to declare a major disaster or emergency is required to be based on a finding that the situation is of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that federal assistance is necessary. 42 U.S.C. § 5191.

may request the support of another federal agency, including DOD, without a presidential declaration of a major disaster or an emergency.[14]

The federal government's response to major disasters and emergencies in the United States is guided by the *National Response Framework*, a national-level guide on how local, state, and federal governments respond to major disasters and emergencies.[15] The DHS interim *National Cyber Incident Response Plan* outlines domestic cyber-incident response coordination and execution among federal, state and territorial, and local governments, and the private sector.[16] Overall coordination of federal incident-management activities is generally the responsibility of DHS. DOD supports the lead federal agency in the federal response to a major disaster or emergency. When the appropriate DOD official approves a lead federal agency's request to provide support to civil authorities for domestic disasters or emergencies, DOD may provide capabilities and resources, including those drawn from the National Guard. Through DSCA, DOD provides these capabilities and resources, which the department defines as support provided by U.S. federal military forces, DOD civilians, DOD contract personnel, DOD component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32 status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

National Guard

The National Guard, which is comprised of Army and Air National Guard units, is located in the 50 states, three U.S. territories, and the District of Columbia.[17] The National Guard has both federal and state-level missions, making it unique among U.S. military organizations. Its federal

[14]See 31 U.S.C. § 1535(a), which permits one federal agency to request goods and services from another federal agency provided that, among other things, the service is available and cannot be obtained more cheaply or conveniently by contract. 31 U.S.C. § 1535(a)(1)-(4).

[15]DHS, *National Response Framework 3rd Edition*, (June 2016).

[16]DHS, *National Cyber Incident Response Plan,* Interim Version, (Washington, D.C.: September 2010). DHS officials told us that while the plan is identified as an "Interim Version," the officials have been told to treat this plan as if it were finalized.

[17]The three territories are Guam, Puerto Rico, and the U.S. Virgin Islands.

mission, which is executed under the control of the President of the United States and the Secretary of Defense, includes maintaining well-trained and well-equipped units that are ready to be mobilized and, when mobilized, to execute military missions in support of the full spectrum of DOD missions, including, but not limited to warfighting, contingency operations, defense security cooperation activities, and DSCA during national emergencies, major disasters, insurrections, and civil disturbances. Its state-level mission, which is executed under the control of state and territorial governors or by the President for the District of Columbia—is to protect life and property and preserve peace, order, and public safety. This mission involves providing emergency relief support during local or statewide emergencies, such as riots, earthquakes, floods, or terrorist attacks.

National Guard unit personnel may operate in a Title 10 status, a Title 32 status, or a state active-duty status. Personnel in a Title 10 status are federally funded and under the command and control of the President. Personnel in a Title 32 status are federally funded but under the command and control of the governor. National Guard personnel could support DOD's DSCA mission while in a Title 10 or Title 32 status. The Secretary of Defense, in coordination with respective state governors, determines the most appropriate duty status for National Guard personnel when providing federal support during disasters and emergencies, including cyber support. Separately, National Guard personnel could also support the state's civil authorities in a state active-duty status. Personnel in a state active-duty status are under the command and control of the governor and are state funded. Under state active duty status, the National Guard can be used for state purposes in accordance with the state constitution and statutes and the respective state is responsible for National Guard expenses.

The National Guard Bureau is a joint organization of DOD that, by law, is the channel of communications on all matters pertaining to the National Guard between (a) the Department of the Army and the Air Force, and (b) the states.[18] In addition, according to DOD Directive 5105.77, *National Guard Bureau (NGB)*, the bureau is the focal point at the strategic level for non-federalized National Guard matters that are not the responsibility

[18]See 10 U.S.C. § 10501.

in law or DOD policy of the Secretary of the Army, the Secretary of the Air Force, or the Chairman of the Joint Chiefs of Staff.[19] The directive also states that the bureau supports force employment matters pertaining to homeland defense and DSCA missions by advising the Chairman of the Joint Chiefs of Staff on the activities of the National Guard as they relate to those missions. Specifically, according to the directive, the bureau prescribes training requirements; plans, programs, and administers the budget; and implements guidance on the structure of the Army National Guard of the United States and the Air National Guard of the United States.

In its 2014 cyber mission analysis report, DOD reported that the National Guard is well-positioned to offer its expertise and support to states in traditional missions like natural disasters as well as less traditional missions in cyberspace.[20] Further, the Chief of the National Guard Bureau in his *2017 National Guard Bureau Posture Statement* reported that the National Guard is uniquely postured to provide cyber capabilities and that its cyber capacity will play an integral role in coordinating with state and federal cyber professionals.[21] In May 2016, DOD issued a Deputy Secretary of Defense policy memorandum that provides guidance on (a) coordinating, training, advising, and assisting cybersecurity support and services that DOD—including National Guard units—could provide to civil authorities incidental to military training, and (b) a state's use of DOD networks, hardware, and software for state cybersecurity activities.[22]

Exercises

Exercises are training events that, according to the 2008 *National Response Framework*, can play an instrumental role in preparing organizations to respond to an incident by providing opportunities to test response plans, evaluate response capabilities, assess the clarity of established roles and responsibilities, and improve proficiency in a

[19]DOD Directive 5105.77, *National Guard Bureau, (NGB),* (Oct. 30, 2015).

[20]DOD, *Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense* (Aug. 21, 2014).

[21]National Guard Bureau, *2017 National Guard Bureau Posture Statement.*

[22]Deputy Secretary of Defense, *Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DOD Information Networks, Software, and Hardware for State Cyberspace Activities*, May 24, 2016.

simulated, risk-free environment.[23] Short of performance in actual operations, exercises provide the best means to assess the effectiveness of organizations in achieving mission preparedness. Exercises provide an ideal opportunity to collect, develop, implement, and disseminate lessons learned and to verify corrective action taken to resolve previously identified issues.[24] Sharing positive experiences reinforces positive behaviors, doctrine, tactics, techniques, and procedures, while disseminating negative experiences highlights potential challenges in unique situations or environments or identifies issues that need to be resolved.[25] According to the 2008 *National Response Framework*, well-designed exercises improve interagency coordination and communications, highlight capability gaps, and identify opportunities for improvement. There are various types of exercises ranging from tabletop exercises that involve key personnel discussing simulated scenarios in informal settings to full-scale response exercises that include many agencies, jurisdictions, and disciplines. In addition to different types of exercises, there are different complexities or focus areas for exercises, such as tiers of exercises identified by numbers 1 through 4. For example, DOD units are to conduct tier 4 training to focus on unit policy and joint and service doctrine linked to unit mission-essential tasks. However, for more complex training situations, DOD is to conduct tier 1 exercises that are designed to prepare national-level organizations and combatant commanders and staffs at the strategic and operational level to integrate interagency, non-governmental, and multinational partners in highly complex environments. Also, the goal of tier 1 exercises is to integrate a diverse audience in a joint training environment and identify

[23]DHS, *National Response Framework* (Washington, D.C.: January 2008).

[24]North American Aerospace Defense Command and U.S. Northern Command, *Commander's Training Guidance (CTG) to the FY17-18 N-NC Joint Training Plans (JTPs),* (Dec. 10, 2015).

[25]North American Aerospace Defense Command and U.S. Northern Command, Instruction 16-166, *Lessons Learned Program and Corrective Action Program*. (Sept. 19, 2013).

core competencies, procedural disconnects, and common ground to achieve U.S. unity of effort.[26]

The National Guard Has Developed Cyber Capabilities That Could Support Civil Authorities, but DOD Does Not Have Full Visibility of National Guard Units' Capabilities

The National Guard Has Cyber Capabilities That Could Support Civil Authorities

The National Guard in the 50 states, three territories, and the District of Columbia have capabilities that could be used—if requested and approved—to perform DOD or state missions to support civil authorities in a cyber incident. National Guard cyber capabilities, according to DOD officials, vary among states, territories, and the District of Columbia based on their differences in funding and prioritization. National Guard officials told us that National Guard units are in a unique position to recruit and retain individuals who have significant cyber expertise based on their full-time positions outside of the military and can coordinate with state authorities and critical infrastructure owners within their respective states. Based on our review of DOD reports, National Guard guidance documents, and our interviews with National Guard officials, we found three types of cyber capabilities that exist within the National Guard:

[26]Chairman of the Joint Chiefs of Staff Instruction 3500.01H, *Joint Training Policy for the Armed Forces of the United States*, (Apr. 25, 2014). Tier 2 training is joint training designed to assist the Joint Task Force Commander in preparing for the conduct of complex military operations at the operational level of conflict. Tier 3 training is training for service component and other service headquarters that is designed to ensure the ability of systems, units, or forces to function within a joint, interagency, non-governmental, and multinational environment.

- **Communications directorates:** The National Guard has a communications directorate[27] within each state, territory, and the District of Columbia that operates and maintains that state's part of the National Guard information network called GuardNet.[28] In this capacity, the directorate conducts information assurance, information operations, and internal defensive activities. The size of each National Guard unit's communications directorate varies between state, territory, and federal district. For example, Nevada National Guard officials told us that there were 26 full-time Army National Guard personnel staffed to their communications directorate in fiscal year 2016. Also, Maryland National Guard officials told us that there were 30 full-time personnel staffed to their Army National Guard communications directorate in fiscal year 2016. According to National Guard officials, personnel who work within a communications directorate, if requested and approved, could support a DSCA mission in a cyber incident. For example, Washington National Guard officials told us that their communications directorate's cyber personnel can conduct vulnerability assessments, support cyber recovery efforts, provide cyber incident response support, and provide cyber and communication capabilities during cyber-related emergencies. Further, National Guard officials told us that the Georgia, Washington, and Maryland National Guard units have developed partnerships with state agencies and local governments to provide cybersecurity support.
- **Computer network defense teams:** The National Guard has computer network defense teams[29] in each state, three territories, and the District of Columbia with a mission to protect National Guard information systems against cyber threats within the respective state, territory, or federal district.[30] According to the 2015 *Concept of Operations Army National*

[27]These directorates are also known as the Command, Control, Communications and Computers directorate; J6 directorate; or G6 directorate.

[28]GuardNet is a network of interconnected federal and state military networks across the United States, its territories, and the District of Columbia that bridges military and civilian sectors.

[29]According to the Army National Guard computer network defense team concept of operations, computer network defense teams report to their respective states' communications directorate, unless otherwise directed. The communications directorate also provides guidance and technical oversight of the computer network defense teams. Army National Guard, *Concept of Operations Army National Guard Computer Network Defense Team (CND-T)* (May 30, 2015).

[30]According to National Guard Bureau officials, the name of computer network defense teams will change to defense cyber operation elements in 2017.

Guard Computer Network Defense Team (CND-T), the teams could serve as first responders for states for cyber emergencies and may provide surge capacity to national capabilities. For example, Colorado National Guard officials told us that their computer network defense team—if requested—could provide cyber capabilities to support civil authorities. In preparation for such a request, the team developed a planning document that identified specific cyber capabilities—such as cyber analysis, threat assessment, and incident response—that the team could provide to civil authorities for a cyber-related emergency or incident. Georgia National Guard officials also told us that their computer network defense team's primary mission is to provide direct cybersecurity support to the network enterprise center and the team also conducts cybersecurity assessments, incident response, network analysis, and forensic support.[31] As of October 2015, 50 states, three territories, and the District of Columbia had computer network defense teams that ranged from 1 to 23 personnel.

- **National Guard cyber units:** The Army and Air Force are in the process of setting up National Guard units with cyber capabilities to support U.S. Cyber Command's missions. For example, the Army and the Air Force are planning to establish National Guard cyber protection teams to conduct defensive cyberspace operations.[32] National Guard officials stated that while the Army National Guard and Air National Guard are approaching the organization of the teams differently, both sets of teams will have capabilities that could support civil authorities in a domestic cyber incident. Specifically, within the Army National Guard, the Army has 1 full-time cyber protection team in place and is developing 10 part-time cyber protection teams that would conduct defensive cyberspace operations, and could support DSCA missions if called upon. Also, within the Air National Guard, the Air Force plans to develop 2 full-time cyber protection teams that will be filled by 12 Air National Guard units on a rotational basis that would support U.S. Cyber Command to defend DOD networks and would be available as surge capacity in a cyber incident. According to the *2017 National Guard Bureau Posture Statement*, the National Guard will activate the cyber teams by the end of fiscal year

[31]According to Georgia National Guard officials, the network enterprise center is responsible for maintaining availability and delivering services on the Georgia National Guard's portion of GuardNet.

[32]DOD cyber protection teams perform cybersecurity functions such as assessments of network vulnerabilities, penetration testing, and remediation of vulnerabilities.

2019.[33] According to National Guard officials, the cyber protection teams are authorized to have 39 personnel each and Georgia National Guard officials told us that in fiscal year 2016 their cyber protection team had 34 assigned personnel. In addition to the cyber protection teams, the Air National Guard has 3 additional cyber units whose mission—as members of U.S. Cyber Command's national mission teams—is to stop cyber attacks and malicious cyber activity of significant consequence against the United States. The Air National Guard also has 7 cyber intelligence, surveillance, and reconnaissance units whose mission is to produce tailored all-source intelligence products that enable cyberspace operations.[34] In addition, according to DOD's cyber mission analysis report,[35] the Virginia National Guard Data Processing Unit, when activated, conducts cyberspace operations in support of U.S. Cyber Command and other organizations.[36]

DOD Does Not Have Full Visibility of All National Guard Cyber Capabilities

DOD has not identified and does not have full visibility into National Guard cyber capabilities that could support civil authorities during a cyber incident. As noted in DOD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities*, DOD is often expected to play a prominent supporting role in responding to a disaster and to rapidly and effectively harness resources to respond to civil-support requests in the homeland. According to the strategy, an effective response will require, among other things, better linking of established federal and state capabilities. DOD does not have visibility into all National Guard units' cyber capabilities because the department has not maintained a database that identifies National Guard cyber capabilities that could support civil authorities during a cyber incident. Section 1406 of the John Warner

[33]*2017 National Guard Bureau Posture Statement.*

[34]Intelligence, surveillance, and reconnaissance is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. Joint Chiefs of Staff, Joint Publication 2-01: *Joint and National Intelligence Support to Military Operations*, (Jan. 5, 2012).

[35]DOD, *Cyber Mission Analysis.*

[36]According to Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms* (Nov. 8, 2010, as amended through Feb. 15, 2016) cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

National Defense Authorization Act for Fiscal Year 2007 requires that DOD identify National Guard emergency response capabilities. Specifically, the section requires that the Secretary of Defense maintain a database of emergency response capabilities that includes the following: (1) the types of emergency response capabilities that each state's National Guard, as reported by the states, may be able to provide in response to a domestic natural or manmade disaster, both to their home states and under state-to-state mutual assistance agreements; and (2) the types of emergency response capabilities that DOD may be able to provide in support of the National Response Plan's emergency support functions, and identification of the units that provide these capabilities.[37]

Initially during our review, National Guard Bureau officials identified two systems that the bureau traditionally uses to identify some National Guard capabilities—the Defense Readiness Reporting System[38] and the Joint Information Exchange Environment.[39] However, National Guard officials acknowledged that neither of these systems fully or quickly identified National Guard cyber capabilities that could be used to support civil authorities in a cyber incident. For example, according to National Guard Bureau officials, the Defense Readiness Reporting System was designed to identify the capabilities associated with National Guard units' federal missions; however, since some National Guard capabilities, such as computer network defense teams, were established to support state and

[37]Pub. L. No. 109-364, §1406(1) (2006) and codified at 10 U.S.C. § 113 (note). The National Response Framework identifies 14 emergency support functions that serve as the federal government's primary coordinating structure for building, sustaining, and delivering response capabilities. DHS is responsible for overseeing the preparedness activities of the communications emergency support functions, among others, which include cybersecurity.

[38]According to DOD Directive 7730.65, the Defense Readiness Reporting System is a capabilities-based and near-real-time readiness reporting system and provides the means to manage and report the readiness of DOD and its components. DOD has used its readiness assessment system to assess the ability of units and joint forces to fight and meet the demands of the national security strategy and captures organizational capabilities to perform a wider variety of missions and mission-essential tasks.

[39]The Joint Information Exchange Environment is the National Guard's system of record for facilitating information sharing and collaboration for the National Guard. National Guard Bureau officials told us they use the Joint Information Exchange Environment to track National Guard missions, share critical event and mission information within the National Guard, coordinate requests for assistance, and identify specific National Guard capabilities to support a request for assistance.

local governments and do not have a federal mission, the Defense Readiness Reporting System will not report or identify these capabilities. Additionally, National Guard Bureau officials told us that they have used the Joint Information Exchange Environment system to query National Guard units for specific capabilities; however, the officials acknowledged that the query approach takes time that might not be available during a cyber incident. National Guard Bureau officials also told us that these systems were not designed to identify National Guard unit cyber capabilities and that neither of the systems were established or designed for the purposes described in section 1406. DOD officials, including National Guard Bureau officials and two state National Guard units we interviewed, acknowledged that DOD has not maintained a database that would allow the department to fully and quickly identify existing cyber capabilities of all National Guard cyber units. Without such a database, DOD may not have timely access to these capabilities when requested by civil authorities during a cyber incident.

DOD Has Conducted and Participated in Exercises to Support Civil Authorities in a Cyber Incident, but Has Not Addressed Challenges with the Exercises

DOD Has Conducted and Participated in Exercises to Prepare to Support Civil Authorities During or After a Cyber Incident

From fiscal years 2013 through 2015, DOD conducted or participated in 9 exercises that were designed to explore the application of policies for supporting civil authorities or to test the response to simulated attacks on cyber infrastructure owned by civil authorities. Of these 9 exercises, DOD conducted 7 exercises and participated in 2 non-DOD hosted exercises. Table 1 shows the 7 exercises that DOD components conducted during the time period of our review—fiscal years 2013 through 2015.

Table 1: Department of Defense (DOD) Exercises Designed to Support Civil Authorities During or After a Cyber Incident

Exercise title	Exercise host	Fiscal year	Cyber civil-support objective
Cyber Guard 13-1	U.S. Cyber Command	2013	Conduct defensive cyber operations and provide analysis assistance to private sector companies and municipalities during simulated cyber incidents.
Cyber Guard 14-1	U.S. Cyber Command	2014	Evaluate response of National Guard in a state active duty status, DOD, Department of Homeland Security and Federal Bureau of Investigation to a cyber incident against U.S. critical infrastructure.
Cyber Guard 15	U.S. Cyber Command	2015	Test DOD participation in a response to a cyberattack of significant consequence against U.S. critical infrastructure.
Cyber Shield 2015	Army National Guard	2015	Train and evaluate U.S. Army National Guard computer network defense teams on the detection, analysis, identification, reporting, and mitigation of cyber threats in a scenario supporting an electric utility.
Vista Host II	North American Aerospace Defense Command and U.S. Northern Command	2015	Examine planning assumptions, potential resource requirements, and roles and responsibilities associated with cyber-related defense support to civil authorities operations.
Vista Code I	North American Aerospace Defense Command and U.S. Northern Command	2015	Examine roles and responsibilities for cyber-related defense support to civil authorities.
Cyber Yankee 2015	New England-area U.S. Army National Guard units	2015	U.S. Army National Guard computer network defense teams and other National Guard cyber units train in cyber defense and share threat information with civil authorities in a regional cyber incident.

Source: GAO analysis of DOD documentation. | GAO-16-574

The exercises explored how the department would provide assistance to civil authorities during or after a cyber incident. For example,

- U.S. Cyber Command's Cyber Guard—The command conducted exercises in fiscal years 2013, 2014, and 2015 to explore the ability of DOD, other federal agencies, and the private sector to respond in cyberspace to a destructive or disruptive attack of significant consequence on U.S. critical infrastructure. In the 2015 Cyber Guard exercise, DOD participants supported DHS network defense as part of a simulated DSCA response. National Guard teams also conducted activities to coordinate, train, advise, and assist civil authorities in a state active duty status. The exercises also included legal and policy tabletop review sessions to explore legal and policy issues related to a national response to significant domestic cyberspace incidents.
- Army National Guard's Cyber Shield—The Army National Guard conducted Cyber Shield exercises in fiscal years 2013, 2014, and 2015 to train computer network defense teams on the detection, analysis,

identification, reporting, and mitigation of cyber threats. The Army National Guard focused the fiscal year 2013 and 2014 exercises on defense of the GuardNet, and in the fiscal year 2015 exercise, changed the focus to support for civil authorities. Specifically, the Cyber Shield 2015 exercise included a scenario where industrial-control systems for electric grid infrastructure and hydroelectric dams were under cyber threat. According to Army National Guard officials, this change to focus on civil support was in response to requests from states for an exercise that would involve National Guard support for information technology infrastructure in the states.

- Vista Host II—In this May 2015 tabletop exercise, North American Aerospace Defense Command and U.S. Northern Command focused on examining planning assumptions, potential resource requirements, and the roles and responsibilities for cyber-related defense support of civil authorities. Specifically, the exercise scenario involved civil support to an electric power generator in responding to a disaster caused by a cyber attack on the generator's industrial-control systems that controlled hydroelectric and nuclear power generation systems. According to U.S. Northern Command officials, the exercise showed that there was a lack of clarity on roles and responsibilities for supporting civil authorities during a cyber incident.

In addition to conducting the 7 exercises, from fiscal year 2013 through 2015, DOD components participated in 2 exercises conducted by non-DOD organizations.

- DHS's Cyber Storm IV—The department's Cyber Storm IV exercises, which consisted of a series of 15 exercises focused on cybersecurity preparedness and response capabilities, ran from fiscal year 2011 through fiscal year 2014. The exercise series was designed to, among other things, improve the processes, procedures, interactions, and information-sharing mechanisms that exist or should exist under the interim *National Cyber Incident Response Plan*. According to DHS officials involved in planning the exercise series, DOD officials assisted in designing the exercise scenarios and DOD officials also participated in multiple exercises that included a tabletop exercise component designed to examine policy issues. U.S. Cyber Command officials also noted that Cyber Storm IV helped participants better understand federal cyber capabilities.

- North American Electric Reliability Corporation's GridEx II—The not-for-profit international organization conducted the GridEx II exercise in fiscal year 2014 on responding to cyber attacks on electric grid components.[40] The exercise included both executive decision making in a tabletop exercise and a response to simulated cyber attacks on electric grid networks. According to a North American Electric Reliability Corporation official, DOD components such as U.S. Northern Command, U.S. Cyber Command, and two state National Guard units participated in GridEx II.

DOD Has Experienced Challenges in Its Civil-Support Exercises and Has Not Conducted a Tier 1 Exercise That Could Address Challenges

We identified three types of challenges with DOD's exercises that could limit the extent to which DOD is prepared to support civil authorities in a cyber incident; DOD has not addressed the challenges. The *DOD Cyber Strategy* states that DOD will exercise its DSCA capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector, if directed, in an emergency. Similarly, the *Strategy for Homeland Defense and Defense Support of Civil Authorities* states that DOD will deepen and facilitate rigorous federal, regional, and state-level planning, training, and exercises through coordination and liaison arrangements that support civil authorities at all levels. Although DOD has developed the two guidance documents, we found challenges that could limit the effectiveness of DOD's exercises. Specifically,

- **Limited access because of classified exercise environments:** According to documents we reviewed and officials we interviewed, DOD's tendency to exercise in a classified environment limited the ability of other federal agencies and critical infrastructure owners to participate in DSCA exercises. In one example, Washington National Guard officials told us that utility personnel who had flown across the country to participate in a civil support exercise that the National Guard unit had invited them to participate in were not admitted into the classified exercise environment. According to DHS's Cyber Guard 15 after-action report, DOD's requirement for the exercise environment to be closed and classified prohibited a more active participation by industry partners and

[40]The North American Electric Reliability Corporation is a not-for-profit international electric reliability organization whose mission is to ensure the reliability of the bulk power system in North America, including the continental United States, Canada, and the northern portion of Baja California, Mexico. In the United States, the corporation is subject to oversight by the Federal Energy Regulatory Commission.

DHS components, including the National Cybersecurity and Communications Integration Center. According to the DHS Cyber Guard 15 exercise after-action report, the exercise has experienced this challenge since 2013. Similarly, according to U.S. Cyber Command's after-action report for its February 2016 Cyber Guard 16 tabletop exercise, the exercise experienced issues because officials of state and local governments and the private sector did not have security clearances, which hindered information sharing.

- **Limited inclusion of other federal agencies and critical infrastructure owners:** Some of the exercises DOD conducted included key federal agencies such as DHS and critical infrastructure owners such as power providers. However, the exercises DOD conducted did not include other key federal agencies (e.g., State and Treasury departments), or other critical infrastructure owners (e.g., bank owners). According to an official from ODASD for Cyber Policy, DOD recognizes that such organizations potentially would be involved in a cyber incident. Similarly, according to the *DOD Cyber Strategy*, the private sector owns and operates over 90 percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense. In Vista Host II, DOD officials reportedly learned that the critical infrastructure owner would contact its security vendors first because of their familiarity with the critical infrastructure's industrial-control systems; however, none of the DOD exercises we reviewed included such vendors.

- **Inadequate incorporation of joint physical-cyber scenarios:** The 7 DOD-conducted exercises we reviewed did not fully explore a scenario in which multiple DOD components and commanders would be responding to a cyber incident that causes an emergency or disaster with physical effects or occurs during such an emergency. The *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity*, which was approved by DOD, recognizes the possibility of a cyber incident with physical effects as well as a physical incident with cyber implications.[41] DOD recognizes that a cyber incident could cause physical effects, including cascading failures of multiple, interdependent, critical, life-sustaining infrastructure

[41]Council of Governors, Department of Homeland Security, and Department of Defense, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (Washington, D.C.: July 2014).

sectors. Similarly, Washington National Guard officials told us that bad actors may take advantage of a disaster or emergency to conduct cyber attacks on information and communications systems in that geographic area. In its planning, DOD has recognized that this is an area that needs to be addressed. Specifically, a planning document that the ODASD for Cyber Policy, the National Guard Bureau, U.S. Northern Command, and U.S. Cyber Command developed to implement the DOD Cyber Strategy states that the department should conduct an exercise that will incorporate cybersecurity as part of broader exercise scenarios.[42] DOD officials acknowledged that DOD exercises to date, such as the Cyber Guard exercises, have not been ideal for a nationwide exercise that addresses multiple complexities of cyber incidents and physical consequences.

In addition to these challenges, we also observed that DOD has not addressed its goals by conducting a tier 1 exercise involving various partners in highly complex environments. Specifically, while DOD conducted 7 exercises that evaluated in some part civil support for a cyber incident, these exercises varied from tabletop exercises to other exercises that do not meet Joint Staff's' tier 1 exercise criteria.[43] DOD's Cyber Strategy exercise planning document states that DOD needs to conduct a tier 1 exercise to achieve the *DOD Cyber Strategy* goal of exercising its DSCA capabilities in support of DHS and other agencies, including state and local authorities, to help defend the federal government and the private sector, if directed, in an emergency. Similarly, U.S. Northern Command and ODASD for Cyber Policy officials told us that the department needs to conduct a tier 1 exercise to explore a disaster with physical and cyber effects. DOD's Cyber Strategy planning document states and officials agree that the department needs to conduct such an exercise to prepare its forces to support civil authorities during or after a cyber incident. However, DOD has not conducted a tier 1 exercise that would prepare DOD forces and enable the department to achieve one of the goals in the *DOD Cyber Strategy* because the department has not identified an exercise to do so. According to U.S. Northern Command

[42]ODASD for Cyber Policy, U.S. Northern Command, U.S. Cyber Command, and the National Guard Bureau, *6-6 DTN Exercise Defense Support of Civil Authorities,* 2015.

[43]DOD is to conduct tier 1 exercises that are designed to prepare national-level organizations and combatant commanders and staffs at the strategic and operational level to integrate interagency, non-governmental, and multinational partners in highly complex environments.

officials, the command wanted to incorporate a cyber civil-support scenario in its 2016 Ardent Sentry exercise, which is a tier 1 exercise.[44] However, the command cancelled its plans after U.S. Cyber Command—a DOD component that would potentially provide critical capabilities in supporting civil authorities—stated that the command had to focus its exercise resources on the Cyber Guard exercise to certify DOD's cyber protection teams. Until DOD identifies and conducts a tier 1 exercise, DOD will miss an opportunity to fully test response plans, evaluate response capabilities, assess the clarity of established roles and responsibilities, and improve proficiency in supporting DHS, other federal agencies, and state and local authorities, if directed, in an emergency. In addition, identifying and conducting a tier 1 exercise would provide DOD an opportunity to address the challenges the department has experienced in previous exercises. For example, the tier 1 exercise could be conducted in part on an open network, include additional federal agencies and other critical infrastructure owners that would be involved in a response, and incorporate scenarios where both cyber threats and physical effects were involved.

Conclusions

DOD has a key role to prepare to defend the homeland and support civil authorities in all domains—including cyberspace—and plays a crucial role in supporting a national effort to confront cyber threats to critical infrastructure. The National Guard has cyber capabilities that could be used—if requested and approved—to support civil authorities in a cyber incident. During an emergency, it is necessary for decision makers to have visibility into the full capabilities that National Guard units possess to support civil authorities. Unless DOD develops or specifies a database to provide full and quick identification of all National Guard units' cyber capabilities, DOD may not have timely visibility and access for needed capabilities when requested by civil authorities during a cyber incident. Similarly, DOD has conducted and participated in exercises to prepare the department to support civil authorities in a cyber incident. Unless DOD conducts a tier 1 exercise that involves various partners in highly complex environments, DOD risks having unprepared forces to call upon to support civil authorities during or after a disaster with physical and

[44]Ardent Sentry is a DSCA exercise based on the interaction of federal, state, local, and tribal governments, private and non-profit organizations and their response to natural and man-made disasters.

cyber effects, and will miss a key opportunity to address the challenges we have identified with its previous exercises.

Recommendations for Executive Action

To ensure that decision makers have immediate visibility into all capabilities of the National Guard that could support civil authorities in a cyber incident, we recommend that the Secretary of Defense maintain a database that can fully and quickly identify the cyber capabilities that the National Guard in the 50 states, three territories, and the District of Columbia have and could be used—if requested and approved—to support civil authorities in a cyber incident.

To better prepare DOD to support civil authorities in a cyber incident, we recommend that the Secretary of Defense direct the Deputy Assistant Secretary of Defense for Cyber Policy, the Chief of the National Guard Bureau, the Commander of U.S. Northern Command, and the Commander of U.S. Cyber Command to conduct a tier 1 exercise that will improve DOD's planning efforts to support civil authorities in a cyber incident. Such an exercise should also address challenges from prior exercises, such as limited participant access to exercise environment, inclusion of other federal agencies and private-sector cybersecurity vendors, and incorporation of emergency or disaster scenarios concurrent to cyber incidents.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and DHS for their review and comment. In its written comments, DOD partially concurred with our two recommendations. DOD's comments are summarized below and are reprinted in entirety in appendix II. DOD also provided technical comments, which we incorporated into the report as appropriate. DHS provided technical comments which we incorporated as appropriate.

DOD partially concurred with our recommendation that the Secretary of Defense maintain a database that can fully and quickly identify the cyber capabilities that the National Guard in the 50 states, three territories, and the District of Columbia have and could be used—if requested and approved—to support civil authorities in a cyber incident. In its response, DOD stated that it already tracks capability and readiness across the entire force. Specifically, DOD stated that National Guard units assigned to and performing Title 10, U.S. Code, missions report readiness through the Defense Readiness Reporting System, and that units assigned to perform Title 32, U.S. Code, missions report to their state's adjutant general. However, as we reported—and DOD's comments reflect—the Defense Readiness Reporting System does not identify National Guard

capabilities that could provide cyber support in a cyber incident. While this system could track some National Guard capabilities, such as cyber protection teams assigned to U.S. Cyber Command, this system alone will not provide DOD leaders complete information about capabilities they could employ to assist civil authorities. For example, while National Guard computer network defense teams could serve as first responders for states for cyber emergencies and may provide surge capacity to national capabilities, the readiness system will not include these teams.

In its comments, DOD also made reference to an annual report that state adjutants general are to provide to the Chief of the National Guard Bureau regarding the readiness of their respective state National Guards. During our engagement, we reviewed the National Guard Bureau's submission to the July-September 2015 *Quarterly Readiness Report to the Congress*, which the bureau uses to meet its requirement to provide DOD leaders a status on the readiness of the National Guard to conduct DSCA activities. We found that the report identifies the readiness of state National Guard units to conduct certain DSCA missions—such as hurricane response. However, the National Guard has not incorporated other DSCA missions—including cyber civil support—in the *Quarterly Readiness Report to the Congress*. Consequently, as prepared now, this report does not help DOD leaders identify assets that could be used in a cyber crisis scenario. However, if the National Guard Bureau modifies the report to include the readiness level of National Guard units to provide civil support in a cyber incident, DOD leaders will potentially have more visibility into cyber capabilities that exist within the National Guard across each state. Because the Defense Readiness Reporting System and the National Guard report do not currently enable DOD leaders to identify National Guard cyber capabilities that could facilitate a quick response in a cyber incident, we continue to believe that DOD should maintain a database—as required by law—that can fully and quickly identify the cyber capabilities that the National Guard possesses.

In response to DOD's comments, we clarified the recommendation that was initially in the report. Specifically, we modified the recommendation from stating that the database should include cyber capabilities that "all National Guard units possess" to cyber capabilities that "the National Guard in the 50 states, three territories, and the District of Columbia have and could be used." This modification is consistent with the requirement identified in Section 1406 of the John Warner National Defense Authorization Act for Fiscal Year 2007, which states that the database should include emergency response capabilities that each state's National Guard may be able to provide in response to a natural or

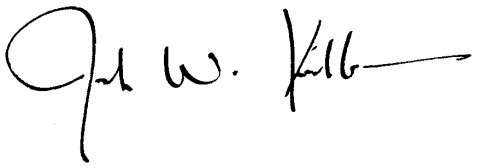
manmade domestic disaster. We discussed this modification with DOD officials and they agreed that the modified recommendation provided them the necessary flexibility to address the report's finding and recommendation.

DOD partially concurred with our recommendation that the Secretary of Defense direct the Deputy Assistant Secretary of Defense for Cyber Policy, the Chief of the National Guard Bureau, the Commander of U.S. Northern Command, and the Commander of U.S. Cyber Command to conduct a tier 1 exercise that will improve DOD's planning efforts to support civil authorities in a cyber incident. DOD concurred in the need to exercise a whole range of challenges associated with responding to a cyber incident but stated that it believes that the Cyber Guard exercise meets the intent of the recommendation. DOD stated that Cyber Guard is designed to address a whole-of-government, whole-of-nation response to a significant cyber attack and included participants from across DOD, the National Guard, DHS, the Federal Bureau of Investigation, the intelligence community, and the private sector. Based on our review of after-action reports and discussions with DOD officials, we believe that the Cyber Guard exercise provides DOD components with an opportunity to evaluate aspects of the department's DSCA mission—such as Cyber Guard 15's test of DOD participation in a response to a cyber attack of significant consequence against U.S. critical infrastructure. However, these after-action reports and DOD officials at various levels also identified a number of issues that keep Cyber Guard in its current form from being a tier 1 exercise that would enable the department to achieve its *DOD Cyber Strategy* goal of exercising its DSCA capabilities in support of DHS and other agencies, including state and local authorities. Specifically, officials from the ODASD for Cyber Policy, U.S. Northern Command, U.S. Cyber Command, and National Guard units told us that Cyber Guard, in its current form, does not meet the intentions of a tier 1 exercise. For example, according to DOD officials, one of the primary purposes of Cyber Guard is to use the exercise as a forum to certify cyber protection teams as being operationally ready. Consequently, according to DOD officials, this does not provide DOD flexibility to address training requirements that are not part of the certification requirements. DOD has also conducted the exercise in a classified forum, which consistently limits public and private sector participation. DOD stated that it strives for greater inclusion of public and private entities in its exercises to increase realism and enhance its understanding of domestic response requirements; however, the exercises are typically classified because they can reveal capabilities, readiness, or plans for military forces that must be protected.

DOD's approach does not recognize that while some DOD components may support civil authorities using classified means, other DOD components—including the National Guard—may be coordinating, training, advising, or assisting civil authorities on unclassified networks. Other cyber civil support exercises, such as the Army National Guard's Cyber Shield exercise and the North American Electric Reliability Corporation's GridEx exercise, demonstrate that training in unclassified forums is both possible and beneficial. If DOD modifies Cyber Guard to address the challenges we have highlighted—such as limited participant access to exercise environment, inclusion of other federal agencies and private-sector cybersecurity vendors, and incorporation of emergency or disaster scenarios concurrent to cyber incidents—it could improve DOD's planning efforts to support civil authorities in a cyber incident. Otherwise, we still believe that DOD should conduct a tier 1 exercise such as a modified Ardent Sentry that includes a DOD response to civil authorities for a cyber incident.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Secretary of Homeland Security. 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

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

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

Appendix I: Scope and Methodology

To examine the extent to which the National Guard has developed cyber capabilities that could support civil authorities in response to a cyber incident and the Department of Defense (DOD) has visibility over those capabilities, we reviewed DOD policies and guidance to identify the National Guard's role in providing Defense Support of Civil Authorities, National Guard cyber capabilities, and the mechanisms used to identify National Guard capabilities. Specifically, we reviewed Joint Publication 3-28, *Defense Support of Civil Authorities*;[1] DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)*;[2] DOD Instruction 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities*;[3] and DOD Directive 7730.65 *Department of Defense Readiness Reporting System (DRRS)*.[4] To identify National Guard cyber capabilities, we reviewed DOD's[5] and the National Guard's[6] cyber mission analysis reports.[7] Additionally, we discussed National Guard unit cyber capabilities and capability identification mechanisms with officials from DOD involved in DSCA from the National Guard Bureau, the Army National Guard, the Air National Guard, and the Office of the Deputy Assistant Secretary of Defense (ODASD) for Cyber Policy. We also spoke with Timothy Lowenberg, a recognized expert on the National Guard's role in cyber incidents who is a retired U.S. Air Force Major General; he also has served as an advisor to the Council of Governors and the National Governors Association. We compared the DOD guidance documents

[1]Joint Chiefs of Staff, Joint Publication 3-28, *Defense Support of Civil Authorities* (July 31, 2013).

[2]DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)* (Dec. 29, 2010) (incorporating change 1, Sept. 21, 2012).

[3]DOD Instruction 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities* (July 26, 2013).

[4]DOD Directive 7730.65, *Department of Defense Readiness Reporting System* (*DRRS)* (May 11, 2015).

[5]DOD, *Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense* (Washington, D.C.: Aug. 21, 2014).

[6]Chief, National Guard Bureau, *National Guard Bureau Cyber Mission Analysis Assessment* (Sept. 29, 2014).

[7]A provision in the National Defense Authorization Act for Fiscal Year 2014 mandated DOD to report on the department's efforts to conduct cyberspace operations and for the Chief of the National Guard Bureau to issue an assessment of the DOD report. Pub. L. No. 113-66, § 933 (2013).

listed above and the information we received in our interviews to the requirement for identifying National Guard emergency response capabilities listed in the United States Code.[8] Based on these discussions and relevant DOD documentation, we categorized National Guard units with cyber capabilities. After pre-testing our interview questions with officials from the Maryland National Guard and meeting with the Colorado National Guard, we conducted structured interviews with a non-generalizable sample of officials from state National Guard cyber units from Georgia, Nevada, and Washington to discuss their cyber civil-support roles and responsibilities, cyber capabilities, and capability tracking mechanisms. We judgmentally selected these states based on the type and number of cybersecurity teams in the state, participation of teams in cyber civil-support exercises, and the relative level of information sector employment in the state based on 2014 Bureau of Labor Statistics sector-level data.[9] We found the Bureau of Labor Statistics information-sector activity data sufficiently reliable for the purpose of this selection. Our findings regarding the capabilities identified during our three sets of interviews with these National Guard units are not generalizable to all state National Guard cyber units and do not reflect an exhaustive list of National Guard cyber capabilities. While some of the National Guard capabilities could be used to support their respective state missions, our focus was on National Guard capabilities that could be used in DOD's DSCA mission.

To assess the extent to which DOD has conducted and participated in exercises to support civil authorities in cyber incidents and any challenges it faced in doing so, we reviewed the *DOD Cyber Str*ategy, *Strategy for Homeland Defense and Defense Support of Civil Authorities*, and Joint Publication 3-28 for DSCA. We also reviewed these documents to determine the types of exercises in which DOD should be conducting or

[8]See 10 U.S.C. § 113 (note).

[9]The Bureau of Labor Statistics reports the total size of the information sector in each state and the District of Columbia. According to the North American Industry Classification System, the information sector comprises establishments engaged in producing and distributing information and cultural products, providing the means to transmit or distribute these products as well as data or communications, and processing data.

participating.[10] We identified a non-generalizable sample of relevant exercises by reviewing exercise planning documentation and through interviews with knowledgeable officials. Specifically, we reviewed an exercise planning document that DOD developed in response to the *DOD Cyber Strategy*[11] and interviewed DOD and DHS officials to identify exercises that DOD components conducted or participated in from fiscal years 2013 through 2015. We chose this timeframe because it allowed us to identify a range of exercises for review and to identify any trends over time. We selected exercises—to include tabletop or simulated network defense exercises—that addressed computer network defense and involved support to civil authorities. We excluded exercises that focused solely on defense of DOD networks. We confirmed these exercises met our selection criteria through reviewing exercise after-action reports. To examine DOD planning for conducting future exercises related to civil support for cyber incidents, we reviewed the DOD Cyber Strategy exercise planning document. We also reviewed DOD guidance for such exercises, such as the *DOD Cyber Strategy*; Joint Publication 3-28; DOD Directive 3025.18, and Chairman of the Joint Chiefs of Staff Instruction 3500.01H *Joint Training Policy for the Armed Forces of the United States*.[12] We compared DOD plans for exercises for supporting civil authorities in cyber incidents to these documents. We observed the Cyber Guard 2016 Legal/Policy Tabletop Exercise held in February 2016 in Laurel, Maryland. To learn about DOD challenges in conducting exercises and planning for exercises of civil support in cyber incidents over the next few years, we interviewed officials from ODASD for Cyber Policy, National Guard Bureau, U.S. Northern Command, and U.S. Cyber Command.

We conducted this performance audit from June 2015 to September 2016 in accordance with generally accepted government auditing standards.

[10]DOD, *The Department of Defense Cyber Strategy* (April 2015), DOD, *Strategy for Homeland Defense and Defense Support of Civil Authorities* (February 2013, and Joint Chiefs of Staff, Joint Publication 3-28, *Defense Support of Civil Authorities* (July 31, 2013).

[11]ODASD for Cyber Policy, U.S. Northern Command, U.S. Cyber Command, and the National Guard Bureau, *6-6 Defend the Nation Exercise Defense Support of Civil Authorities,* 2015.

[12]Chairman of the Joint Chiefs of Staff Instruction 3500.01H *Joint Training Policy for the Armed Forces of the United States,* (April 25, 2014).

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.

Appendix II: Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

HOMELAND DEFENSE &
GLOBAL SECURITY

June 29, 2016

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

Dear Mr. Kirschbaum,

This is the Department of Defense (DoD) response to the GAO Draft Report GA0-16-574, "DEFENSE CIVIL SUPPORT: DoD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises," dated May 18, 2016 (GAO Code 100479).

Attached is DoD's proposed response to the subject report. My point of contact is Mr. Scott Mann at 703-692-3148 or via email at scott.f.mann.civ@mail.mil.

Sincerely,

Aaron Hughes
Deputy, Assistant Secretary of Defense
Cyber Policy

GAO DRAFT REPORT DATED MAY 18, 2016
GA0-16-574 (GAO CODE 100479)

"DEFENSE CIVIL SUPPORT: DOD NEEDS TO IDENTIFY NATIONAL GUARD'S CYBER CAPABILITIES AND ADDRESS CHALLENGES IN ITS EXERCISES"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: To ensure that decision makers have immediate visibility into all capabilities of the National Guard that could support civil authorities in a cyber incident, GAO recommends that the Secretary of Defense maintain a database that can fully and quickly identify the cyber capabilities that all National Guard units possess. Such a database should, at a minimum, track the cyber capabilities of National Guard communications directorates, computer network defense teams, and cyber units.

DoD RESPONSE: The Department of Defense (DoD) partially concurs in draft GAO Report 16-574 recommendation one. Although DoD agrees that it is important to track the capability and readiness of the Reserve and National Guard Components, DoD already tracks capability and readiness across the entire force. Currently, National Guard units that are assigned and perform Title 10, U.S. Code, missions report readiness through the Defense Readiness Reporting System (DRRS). Units that are assigned to perform Title 32, U.S. Code, missions report to their respective State's Adjutant General. In accordance with DoD Directive 5105.83, States' Adjutants General shall "provide detailed reports on the state of readiness of their respective State NGs on an annual basis to the Chief NGB, to satisfy the Chief, NGB, statutory reporting requirements to Congress." These reports will help us identify assets that can be used in a crisis scenario, and we will assess steps that can further streamline our ability to access this information quickly.

As the Cyber Mission Force (CMF) approaches full operating capability (FOC), DoD is working to include all forces, Active Duty, Reserve, and National Guard, into the appropriate databases so their readiness can be tracked and they can be called up for service in a contingency, including for Defense Support of Civil Authorities.

DoD tracks capabilities and readiness at the unit level. This requires standards for organizing, training, and equipping the unit. DoD does not set standards for National Guard communications directorates or computer network defense teams (CND-Ts); the requirements are set at the State level. Although the National Guard authorizes up to 10 positions for CND-T units, it does not require States to fill these positions. The manning and capabilities of CND-T units varies from State to State based on the needs of the State, and accurately tracking those capabilities would require either tracking down to the individual level or it would require setting an organize, train, and equip standard that would apply to State National Guard Force capabilities. Additionally, not all components listed in the report are operational units. Communications Directorates are staff elements; they do not have collective training tasks that produce readiness levels and should not be subject to "unit-like" reporting requirements.

RECOMMENDATION 2: To better prepare DoD to support civil authorities in a cyber incident, GAO recommends that the Secretary of Defense direct the Deputy Assistant Secretary of Defense for Cyber Policy, the director of the National Guard Bureau, the commander of U.S. Northern Command, and the commander of U.S. Cyber Command to conduct a tier 1 exercise that will improve DOD's planning efforts to support civil authorities in a cyber incident. Such an exercise should also address challenges from prior exercises, such as limited participant access to exercise environment, inclusion of other federal agencies and private sector cybersecurity vendors, and incorporation of emergency or disaster scenarios concurrent to cyber incidents.

DoD RESPONSE: The Department of Defense partially concurs in draft GAO report 16-574 recommendation two. DoD concurs in the need to exercise the whole range of challenges associated with responding to a cyber incident. DoD believes that its annual CYBER GUARD exercise meets the intent of the recommendation. CYBER GUARD is designed to address a whole-of-government, whole-of-nation response to a significant cyberattack. The exercise includes participants from across DoD, the National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the intelligence community, and the private sector. CYBER GUARD 16, which was conducted in June 2016, was co-sponsored by DHS and the FBI and had National Guard participants from 13 States, representatives from critical infrastructure sectors, the Federal Aviation Administration, Congress, and others. DoD continues to refine the exercise format for CYBER GUARD based on lessons learned during previous exercises and has worked to increase the complexity of scenarios, broaden participation both within and outside the Federal Government, and find ways to integrate private sector elements into a classified environment appropriately.

DoD also concurs in the need for an exercise that tests both the cyber and physical responses and is working to incorporate cyber elements into DoD exercises as appropriate. DoD, however, believes that the greatest value would be in a truly whole-of-nation exercise that should be organized and led by the departments and agencies with the responsibility for coordinating a domestic emergency response.

Finally, DoD understands the need for, and strives for, greater inclusion of public and private entities in its exercises to increase realism and enhance DoD's understanding of domestic response requirements. DoD exercises are typically classified because they can reveal capabilities, readiness, or plans for military forces that must be protected. Understanding how and under what circumstances DoD can employ its capabilities in a domestic response scenario is important for DoD readiness and must be balanced with the need to include outside entities. Many of these entities, as seen in this year's CYBER GUARD, are able to participate in a classified forum.

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 contact above, key contributors to this report included Tommy Baril (Assistant Director), Tracy Barnes, David Beardwood, Kevin Copping, Patricia Farrell Donahue, Jamilah Moon, and Richard Powelson.

Related GAO Products

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. GAO-16-332. Washington, D.C.: April 4, 2016.

Civil Support: DOD is Taking Action to Strengthen Support of Civil Authorities. GAO-15-686T. Washington, D.C.: June 10, 2015.

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems. GAO-15-573T. Washington, D.C.: April 22, 2015.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. GAO-14-354. Washington, D.C.: April 30, 2014.

Information Security: Federal Agencies Need to Enhance Responses to Data Breaches. GAO-14-487T. Washington, D.C.: April 2, 2014.

Civil Support: Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe, GAO-13-763. Washington, D.C.: September 30, 2013.

Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance. GAO-13-128. Washington, D.C.: October 24, 2012.

Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats. GAO-12-762SU. Washington, D.C.: August 3, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T. Washington, D.C.: June 28, 2012.

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012.