United States Government Accountability Office

Report to Congressional Committees

November 2017

DEFENSE CIVIL SUPPORT

DOD Needs to Address Cyber Incident Training Requirements

Accessible Version

GAO-18-47

November 2017

DEFENSE CIVIL SUPPORT

DOD Needs to Address Cyber Incident Training Requirements

GAO Highlights

Highlights of GAO-18-47 a report to congressional committees.

Why GAO Did This Study

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. Section 1648 of the National Defense Authorization Act for Fiscal Year 2016 included a provision that DOD develop a comprehensive plan for CYBERCOM to support civil authorities in responding to cyberattacks by foreign powers against the United States. Section 1648 also included a provision that GAO review DOD's plan.

This review assesses the extent to which DOD's Section 1648 report addressed the statutorily required submission elements. To conduct this work, GAO assessed DOD's Section 1648 report against the elements outlined in the statute. GAO also discussed the Section 1648 report with DOD policy, Joint Chiefs of Staff, combatant commands, and military service officials.

What GAO Recommends

GAO has previously recommended that DOD take actions on elements of the Section 1648 report that were partially addressed. GAO is making two new recommendations that DOD update cyber incident coordination training and maintain a list of officials trained in the National Incident Management System. DOD concurred with maintaining a list of trained officials and partially concurred on updating cyber training. GAO continues to believe the updating recommendation is warranted.

View GAO-18-47. For more information-contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

The Department of Defense (DOD) did not develop a comprehensive plan for U.S. Cyber Command (CYBERCOM); instead, the department submitted a report consisting of a collection of documents that fully addressed two of the six statutorily required elements; partially addressed three elements; and did not address the sixth element on DOD training activities.

Table: Extent to Which the Department of Defense's (DOD) Section 1648 Report Addressed Required Elements

Required element	GAO assessment
Descriptions of the roles, responsibilities, and expectations of federal, state, and local authorities as the Secretary understands them.	Addressed
A description of such legislative and administrative action as may be necessary to carry out the plan.	Addressed
Descriptions of the roles, responsibilities, and expectations of the active and reserve components of the armed forces.	Partially addressed
Plans for coordination with heads of other federal agencies and state and local governments pursuant to the exercises required in the previous clause.[a]	Partially addressed
A list of any other exercises previously conducted that are used in the formulation of the plan.	Partially addressed
A plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments.	Not addressed

Legend:

● Addressed: Submission includes all aspects of the required element.

◐ Partially addressed: Submission includes some but not all aspects of the required element.

○ Did not address: Submission does not include required element.

Source: GAO analysis of DOD's Section 1648 report. | GAO-18-47

[a]The "previous clause" refers to the plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments. Since we listed the requirements in order of the extent to which DOD's Section 1648 report addresses the legislative requirement, we listed the "internal DOD collective training" requirement last.

GAO also found that, in addition to not addressing the training element in the report, DOD had not ensured that staff are trained as required by the *Presidential Policy Directive on United States Cyber Incident Coordination* or DOD's Significant Cyber Incident Coordination Procedures, which were included DOD's Section 1648 report. Taking action to improve these areas should help DOD sustain progress it has already made. With the President's decision to elevate CYBERCOM to a unified combatant command, such actions will also help as DOD continues to plan to support civil authorities in response to a cyber incident and where CYBERCOM has a significant role.

Contents

Letter 1

Background 3
DOD's Section 1648 Report Addressed Some of the Statutorily Required Elements 6
Conclusions 14
Recommendations for Executive Action 15
Agency Comments and Our Evaluation 15

Appendix I: Status of Three Recommendations from Our Recent Reports on Defense Cyber Civil Support 18

Appendix II: Section 1648 (a) of the National Defense Authorization Act for Fiscal Year 2016 20

Appendix III: Objective, Scope, and Methodology 22

Appendix IV: Comments from the Department of Defense 24

Appendix V: GAO Contact and Staff Acknowledgments 26

GAO Contact 26
Staff Acknowledgments 26

Appendix VI: Accessible Data 27

Agency Comment Letter 27

Related GAO Products 30

Tables

Table 1: Extent to Which the Department of Defense's (DOD) Section 1648 Report Addressed Required Elements 6
Table 2: Status of Three Recommendations from Our Recent Reports Related to Defense Cyber Civil Support 18

Abbreviations

CYBERCOM	US Cyber Command
DHS	Department of Homeland Security
DSCA	Defense Support of Civil Authorities
DRRS	Defense Readiness Reporting System
FEMA	Federal Emergency Management Agency
HDI	Homeland Defense Integration
NORTHCOM	US Northern Command
ODASD	Office of the Assistant Secretary of Defense
PACOM	US Pacific Command
PPD-41	Presidential Policy Directive on United States Cyber Incident Coordination

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

November 30, 2017

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] The Department of Defense (DOD) recognizes that a disruptive, manipulative, or destructive cyberattack 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 and that the department must be prepared to support civil authorities in all domains—including in cyberspace.[2] Generally, DOD supports civil authorities through its Defense Support of Civil Authorities (DSCA) mission.[3]

We previously reported on DOD's preparation efforts for providing support to civil authorities in response to cyber incidents. In April 2016, we reported that DOD's guidance—such as DOD Directive 3025.18, *Defense Support of Civil Authorities*—did not clearly define the roles and responsibilities of key DOD entities for domestic cyber incidents.[4] For example, U.S. Northern Command's (NORTHCOM) *Defense Support of Civil Authorities Response* concept plan states that NORTHCOM would be the supported command for a mission to support civil authorities in responding to a domestic cyber incident. However, we found that other

[1]*Presidential Policy Directive—United States Cyber Incident Coordination/PPD-41* (July 26, 2016). (Hereinafter cited as PPD-41) (July 26, 2016). A significant cyber incident is defined as a cyber incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[2]See Department of Defense, *The Department of Defense Cyber Strategy* (April 2015) and Department of Defense, *Strategy for Homeland Defense and Defense Support of Civil Authorities* (February 2013).

[3]DSCA is DOD's mission to provide support through the federal military force, the National Guard, and other resources in response to requests for assistance from civil authorities for domestic emergencies (e.g., hurricanes and wildfires), special events (e.g., political party national conventions), designated law enforcement support, and other domestic activities. Throughout this report we also refer to DSCA as "civil support."

[4]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).

guidance directs and DOD officials confirmed that a different command, U.S. Cyber Command (CYBERCOM), would be responsible for supporting civil authorities in the event of a domestic cyber incident. Therefore, we recommended that DOD issue or update guidance that clarifies roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with this recommendation.

In September 2016, we reported that DOD did not have visibility over all National Guard units' cyber capabilities that could be used to support civil authorities in a cyber incident.[5] We also reported that DOD had not identified and conducted a "tier 1" exercise—an exercise involving national-level organizations, combatant commanders, and staff in highly complex environments. Therefore, we recommended that DOD maintain a database that identifies the National Guard units' cyber-related emergency response capabilities and conduct a tier 1 exercise to prepare its forces in the event of a disaster with cyber effects. DOD partially concurred with these recommendations and stated that its current mechanisms and exercises were sufficient to address the issues highlighted in the report. See appendix I for the status of DOD's implementation of these recommendations.

Section 1648 of the National Defense Authorization Act for Fiscal Year 2016 included a provision that DOD develop a comprehensive plan for CYBERCOM to support civil authorities in responding to cyberattacks by foreign powers against the United States.[6] Among the elements required in the plan is a description of the roles, responsibilities, and expectations of active and reserve components of the armed forces. See appendix II for the full text of the statutory reporting requirements. DOD was required to develop its plan by May 2016 (180 days after the National Defense Authorization Act was signed into law); however, the department did not complete its plan until April 2017.

Section 1648 also included a provision that we review DOD's plan. This review assesses the extent to which DOD's Section 1648 report submission addressed the statutorily required elements. We reviewed the required elements outlined in Section 1648 of the National Defense Authorization Act for Fiscal Year 2016 and analyzed DOD's submission to

[5]GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises.* GAO-16-574 (Washington, D.C.: Sept. 6 , 2016).

[6]Pub. L. No. 114-92, § 1648(a) (2015).

determine whether it addressed those elements. Additionally, we interviewed officials from the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security—specifically, the Office of the Deputy Assistant Secretary of Defense (ODASD) for Homeland Defense Integration and Defense Support of Civil Authorities (HDI/DSCA) and the ODASD for Cyber Policy, as well as other DOD components to obtain clarifying and supporting information from relevant DOD components on the process by which the department plans and prepares for a cyber incident requiring civil support. A more detailed description of our objective, scope, and methodology is provided in appendix III.

We conducted this performance audit from May 2017 to November 2017, 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.

Background

Defense Support of Civil Authorities

Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the 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.[7] 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. Additionally, under the Economy Act, a federal agency may request the support of another federal agency, including DOD, without a presidential

[7]See Pub. L. No. 100-707 (1988) (codified as amended at 42 U.S.C. § 5121, et seq.).

declaration of a major disaster or an emergency.[8] This act 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.

In July 2016, the White House issued the *Presidential Policy Directive on United States Cyber Incident Coordination* (hereafter referred to as PPD-41) to establish principles governing the federal government's response to cyber incidents involving government or private sector entities.[9] Subsequently, in December 2016, the Department of Homeland Security issued an updated *National Cyber Incident Response Plan* that outlines domestic cyber-incident response coordination and execution among federal; state, territorial, and local governments; and the private sector.[10] Overall coordination of federal incident-management activities is generally the responsibility of the Department of Homeland Security. DOD supports the lead federal agency in the federal response to a major disaster or emergency. When authorized to provide support to civil authorities for domestic emergencies, DOD may provide capabilities and resources—such as military forces (including the National Guard under Title 10 and Title 32, U.S. Code), DOD civilians, and DOD contractors—through DSCA.[11] DOD components can also provide support to civil authorities under separate authority. For example, under Executive Order 12333, the National Security Agency, as an element of the intelligence community, is authorized to provide technical assistance and cooperation to law enforcement and other civil authorities not precluded by applicable law.[12]

[8]See 31 U.S.C. § 1535(a),

[9]PPD-41 (July 26, 2016).

[10]DHS, *National Cyber Incident Response Plan,* (Washington, D.C.: December 2016).

[11]Title 10 and Title 32, U.S. Code, govern the operations of the Department of Defense and the National Guard respectively. Military forces, both active and reserve, may support domestic missions in a Title 10 status; however, the National Guard may provide support in a Title 10 or Title 32 status. Title 32 provides the authority for the National Guard to conduct activities in a federal pay status but subject to state control. The National Guard normally responds to domestic emergencies in a state active duty status. Under state active duty, 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.

[12]White House, Executive Order 12333, as amended, *United States Intelligence Activities*, paragraph 2.6(d). DOD Directive 3025.18, *Defense Support of Civil Authorities*, does not apply to technical assistance that the National Security Agency provides using this authority.

DOD Components with DSCA Responsibilities

In an effort to facilitate DSCA across the nation and at all organizational levels, DOD has assigned responsibilities within the Office of the Secretary of Defense (such as the Assistant Secretary of Defense for Homeland Defense and Global Security); the Chairman of the Joint Chiefs of Staff; various combatant commanders, such as the NORTHCOM and the U.S. Pacific Command (PACOM) Commanders; and the Chief of the National Guard Bureau, among others. A combatant command is a unified or specified command with a broad continuing mission under a single commander established and designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. DOD's Assistant Secretary of Defense for Homeland Defense and Global Security is the principal civilian advisor responsible for homeland defense, DSCA, and cyber for the department. This official is to develop policies, conduct analysis, provide advice, and make recommendations on homeland defense, DSCA, emergency preparedness, and cyberspace operations within the department.

The Chairman of the Joint Chiefs of Staff advises the Secretary of Defense on the effects of requests for DSCA on national security and identifies available resources for support in response to DSCA requests. NORTHCOM and PACOM provide support to civil authorities at the federal, state, and local levels, as directed. Further, CYBERCOM synchronizes the planning for cyberspace operations in coordination with other combatant commands, the military services, and other appropriate federal agencies. In August 2017, DOD initiated the process to elevate CYBERCOM from a subunified command to a unified combatant command. According to DOD, this elevation "will help to streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of those operations and will ensure that critical cyberspace operations are adequately funded." Additionally, a dual-status commander could serve as an intermediate link between the separate chains of command for state and federal forces and is intended

to promote unity of effort between federal and state forces to facilitate a rapid response during major disasters and emergencies.[13]

DOD's Section 1648 Report Addressed Some of the Statutorily Required Elements

DOD did not develop a comprehensive plan; instead, the department submitted a collection of separate documents that addressed some, but not all six statutorily required elements (hereafter referred to as DOD's Section 1648 report). Table 1 lists each of the required elements and shows our determination of the extent to which the elements were addressed in DOD's Section 1648 report.

Table 1: Extent to Which the Department of Defense's (DOD) Section 1648 Report Addressed Required Elements

Required element	Our assessment
1. Descriptions of the roles, responsibilities, and expectations of federal, state, and local authorities as the Secretary understands them.	Addressed
2. A description of such legislative and administrative action as may be necessary to carry out the plan.	Addressed
3. Descriptions of the roles, responsibilities, and expectations of the active and reserve components of the armed forces.	Partially addressed
4. Plans for coordination with heads of other federal agencies and state and local governments pursuant to the exercises required in the previous clause.[a]	Partially addressed
5. A list of any other exercises previously conducted that are used in the formulation of the plan.	Partially addressed
6. A plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments.	Not address

Legend:
● Addressed : Submission addresses all aspects of the required element.
◐ Partially addressed: Submission addresses some but not all aspects of the required element.
○ Did not address: Submission does not address the required element.
Source: GAO analysis of DOD's Section 1648 report. | GAO-18-47

[13]The National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 515 (2011) provided that a dual-status commander should be the usual and customary command and control arrangement in situations in which the armed forces and National Guard are employed simultaneously in support of civil authorities, including in support of missions involving major disasters and emergencies. As mentioned in our April 2016 report, additional DOD components may also promote DOD unity of effort and support DSCA missions to include defense coordinating officers and elements, liaisons, and other coordinating mechanisms. See GAO-16-332.

[a]The "previous clause" refers to the "plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments" that is currently listed below this element. Since we listed the elements in order of the extent to which DOD's Section 1648 report addresses the legislative requirement—and not in the order listed in the legislation—we listed the "internal DOD collective training" requirement last.

DOD officials agreed that their submission was not a comprehensive plan. These officials told us they developed a report that they believed would address the required elements of the legislation and articulate the department's comprehensive work to prepare for supporting civil authorities in response to a cyber incident with plans, policies, guidance, among other things. Specifically, DOD's Section 1648 report is a collection of separate documents that, according to DOD, outline core federal, state, local, and private sector roles and responsibilities; summarize plans for coordination at all levels of government and across sectors in the event of a cyber incident; and prescribe the roles and responsibilities of the active and reserve components.

DOD's Report Fully Addressed Two of the Six Elements Required by the Statute

As noted in the table above, DOD's Section 1648 report addressed two of the six elements required by the statute–to provide (1) descriptions of the roles, responsibilities, and expectations of federal, state, and local authorities and (2) a description of legislative and administrative actions necessary to carry out its plan to support domestic cyber incident response efforts. Specifically, DOD's Section 1648 included copies of the PPD-41 and the Department of Homeland Security's *National Cyber Incident Response Plan*.[14] Both of these documents provide general descriptions of the roles, responsibilities, and expectations of federal, state, and local authorities. For example, the *National Cyber Incident Response Plan* was developed to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure.

DOD's Section 1648 report also included a description of administrative actions that the department believed were necessary to carry out its plan to support domestic cyber incident response efforts. Specifically, according to the report, DOD had drafted a directive type memorandum to

[14]PPD-41 and DHS, *National Cyber Incident Response Plan,* (Washington, D.C.: December 2016).

provide supplementary policy guidance, assign responsibilities, and detailed procedures for providing defense support for cyber incident response. This memorandum was signed and issued by DOD subsequent to the department submitting its Section 1648 report to Congress.[15] DOD officials also acknowledged that there were incorporating cyber into all aspects of policy, doctrine, and guidance. In the report, DOD stated that the department believed current authorities were sufficient and did not recommend any legislative actions.

DOD's Report Partially Addressed Three of Six Elements Required by the Statute but the Information Provided Was Incomplete

DOD partially addressed three of the six elements required by the statute—to provide (1) descriptions of the roles, responsibilities, and expectations of the active and reserve components of the armed forces; (2) the department's plans for coordination with heads of other federal agencies and state and local governments; and (3) a list of exercises previously conducted that are used in the formulation of the plan.

DOD's Section 1648 report includes a copy of DOD Directive 3025.18, *Defense Support of Civil Authorities*, which establishes DSCA policy and provides guidance for the execution and oversight of DSCA, as an appendix. This directive includes a section that identifies roles and responsibilities of DOD components such as the Joint Staff, the combatant commands, and the military departments, among others.

However, we have previously reported that DOD's guidance does not clearly define the department's roles and responsibilities.[16] For example, we found inconsistency on which combatant command would be designated the supported command and have the primary responsibility for providing support to civil authorities during a cyber incident. Consequently, as noted in appendix I, we recommended that DOD issue or update guidance that clarifies roles and responsibilities for relevant entities and officials to support civil authorities in a domestic cyber incident. However, key DOD documents such as DOD Directive 3025.18,

[15]See DOD, Directive Type Memorandum (DTM) 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response* (June 21, 2017). This memorandum will expire on June 21, 2018, and will be converted to a new issuance.

[16]GAO-16-332.

DOD's Section 1648 report, and the Directive Type Memorandum issued in June 2017 do not clarify roles and responsibilities of DOD components, liaisons, and personnel who DOD had previously assigned coordination roles and responsibilities for supporting civil authorities.[17] As a result, there is still uncertainty about these roles and responsibilities within the department. For example, disagreement still exists among officials in the department regarding whether NORTHCOM and PACOM (as the geographic combatant commands) or CYBERCOM, which according to command officials maintains the department's existing inventory of cyberspace command and control capabilities, is the supported command in a cyber incident requiring civil support.[18] DOD officials acknowledged to us that there are a number of planning and guidance documents that need to be updated to clarify roles and responsibilities. Until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, as we recommended, department leaders and components will continue to experience uncertainty about the roles and responsibilities of different components and commands in providing support to civil authorities in the event of a significant cyber incident.

In an effort to describe the department's plans for coordination with heads of other federal agencies and state and local governments, DOD's Section 1648 report provided information on the department's role in supporting a whole-of-government approach during a significant cyber incident. Specifically, DOD included copies of PPD-41, the Department of Homeland Security's *National Cyber Incident Response Plan*, and DOD's *Department of Defense (DOD) Significant Cyber Incident Coordination Procedures*. These documents recognize that the department coordinates with other federal agencies (and state and local governments, as appropriate) through the Cyber Response Group and the Cyber Unified

[17]DOD, Directive Type Memorandum (DTM) 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response* (June 21, 2017).

[18]In August 2017, DOD initiated the process to elevate the U.S. Cyber Command from a subunified command to a unified combatant command. According to DOD, this elevation "will help to streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of those operations and will ensure that critical cyberspace operations are adequately funded."

Coordination Group that were consistent with PPD-41.[19] According to PPD-41, the Cyber Unified Coordination Group is the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating private sector partners into incident response efforts.

While DOD's Section 1648 report recognizes the role and value of these two groups, these groups have limited coordination opportunities with state and local governments. For example, the Cyber Response Group is a national-level policy coordination group composed of federal department and agencies (i.e., does not include state and local governments). Also, the Cyber Unified Coordination Group is an ad-hoc group that is convened in response to a significant cyber incident and will not include state and local governments unless it is required by the scope, nature, and facts of a particular significant cyber incident.

In addition, the report did not identify any plans for coordinating with heads of other federal agencies and state and local governments, as required by the statute. DOD guidance and joint doctrine state that, among the defense coordinating officers' multiple responsibilities, they are supposed to develop and promote relationships with federal, state, tribal, and local governmental and non-governmental organizations, and with private sector entities in the assigned Federal Emergency Management Agency (FEMA) region.[20] However, DOD's Section 1648 report did not identify how the defense coordinating officers, their supporting elements, or other DOD components that coordinate with civil

[19]According to PPD-41, a Cyber Unified Coordination Group may be formed and activated in the event of a significant cyber incident, will be incident specific, and will be formed (1) at the direction of the National Security Council Principals Committee (Secretary level), Deputies Committee (Deputy Secretary level), or the Cyber Response Group; (2) when two or more federal agencies that generally participate in the Cyber Response Group, including relevant sector specific agencies, request its formation; or (3) when a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. A Cyber Unified Coordination Group will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one federal agency are no longer required to manage the remaining facets of the federal response to an incident.

[20]DOD Instruction 3025.23, *Domestic Defense Liaison with Civil Authorities,* Enclosure 3 2.b.(8) (May 25, 2016) and Joint Publication 3-28, *Defense Support of Civil Authorities* (July 31, 2013).

authorities—including state and local governments—plan to coordinate in preparation to provide support of DSCA activities.[21]

We are not making a recommendation on this issue because we previously recommended that DOD issue or update guidance that clarifies roles and responsibilities for DOD components—such as for the defense coordinating officers and their supporting elements—to support civil authorities in response to a domestic cyber incident.[22]

DOD's Section 1648 report also includes a list of cyber civil support exercises that DOD conducted over the last 3 years. However, this list was incomplete because DOD did not include all exercises where DOD components provided support to civil authorities in a cyber incident. For example, the report did not include NORTHCOM's 2015 exercises—Vista Host and Vista Code. These two exercises examined planning assumptions, potential resource requirements, and roles and responsibilities associated with cyber-related defense support to civil authorities operations. By not including this information in this one-time report, DOD missed an opportunity to provide Congress more complete information about exercises that the department is conducting to prepare itself and commands to support civil authorities for a cyber incident within the United States.

During our review of DOD's Section 1648 report, we also found that the department had yet to conduct a command and control (i.e., operational-level) exercise focused on providing support to civil authorities in a cyber incident—a gap acknowledged by officials from NORTHCOM, PACOM, and CYBERCOM. According to these officials, the exercises identified in the Section 1648 report focused on strategic–level decisions (e.g., Cyber Guard 16 Legal and Policy table top exercises) or tactical-level actions (e.g., Cyber Guard 16). CYBERCOM officials told us that they believe that

[21]A defense coordinating officer is a senior-level military officer or civilian equivalent who serves as DOD's single point of contact for domestic emergencies in a joint field office. Among other things, the defense coordinating officer processes requirements for military support and forwards mission assignments through proper channels to the appropriate military organizations. A defense coordinating element is a staff and military liaison officers who assist the defense coordinating officer in facilitating coordination and support to activated emergency support functions.

[22]In our prior report, DOD officials from a defense coordinating element told us that, given their role in facilitating coordination between DOD and civil authorities, they would benefit from additional guidance about the element's roles in supporting civil authorities for a cyber incident. See GAO-16-332.

Cyber Guard is a tier 1 exercise. However, a 2015 DOD Cyber Strategy implementation document stated that while Cyber Guard is a valuable "whole-of-nation" scenario, its focus is much more tactical in nature and that the department needed another tier 1-level exercise.[23] Similarly, officials from both DHS and DOD acknowledged that Cyber Guard was a tactical-level exercise.

As previously discussed and identified in appendix I, we previously recommended that DOD conduct a tier 1 exercise to prepare its forces in the event of a disaster with cyber effects. CYBERCOM officials told us the command is currently planning an internal staff exercise to address our recommendation to exercise its forces at the operational-level of leadership. However, an internal staff exercise (i.e., an exercise that does not exercise command-and-control relationships with other combatant commanders) will not be consistent with DOD guidance that states tier 1 exercises are designed to prepare national-level organizations and combatant commanders and staff at the *strategic* and *operational* levels to integrate a diverse audience in highly complex environments. We maintain our position that Cyber Guard in its current form is not a tier 1 exercise that would enable the department to achieve its DOD Cyber Strategy goal of exercising its DSCA capabilities in support of the Department of Homeland Security (DHS) and other agencies, including state and local authorities. We continue to believe that DOD should conduct a tier 1 exercise to improve the department's planning efforts to support civil authorities in a cyber incident.

DOD's Report Did Not Address One of the Elements Required by the Statute and DOD Has Not Ensured That Staff Are Trained

DOD's Section 1648 report did not address one of the six required elements—to provide a plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments. Instead, the department provided a classified list of planned exercises for 2017 that, according to officials,

[23]According to the Chairman of the Joint Chiefs of Staff Instruction 3500.01H, *Joint Training Policy for the Armed Forces of the United States*, (Apr. 25, 2014), the goal of tier 1 exercises is to integrate a diverse audience in a joint training environment and identify core competencies, procedural disconnects, and common ground to achieve a U.S. unity of effort.

have training value for cyber incident response. Officials from ODASD (HDI/ DSCA) and ODASD (Cyber Policy) told us that DOD does not train for DSCA. Rather, the department trains and exercises its forces to conduct military missions and can apply the knowledge and experience from these activities to support civil authorities when requested and approved. The officials emphasized that, while exercises generally test whether DOD forces have learned training, in the case of DSCA exercises are a key training tool.

While exercises may have training value, DOD did not provide information on existing DSCA-related training efforts within the department—such as on NORTHCOM's DSCA course offered to officials from DOD and other federal agencies.[24] Specifically, according to NORTHCOM officials, the command's DSCA course focuses on training senior military officers, DOD civilians, and their staff to ensure DOD's readiness to support its homeland defense and civil support missions. The officials explained that this course introduces participants to national, state, local, and DOD statutes, directives, plans, command and control relationships, and capabilities with regard to disaster and emergency response. By not including this information in this one-time report, DOD missed an opportunity to provide Congress more complete information about training that the department is conducting to prepare itself and commands to support civil authorities for a cyber incident within the United States.

In addition, during our review, we found that DOD had not met the training requirements outlined in PPD-41, which was included in DOD's Section 1648 report. Specifically, the policy directive requires federal agencies, including DOD, to update cyber incident coordination training to incorporate the tenets of PPD-41 by December 2016 and to identify and maintain a cadre of personnel qualified and trained in the National Incident Management System and unified coordination to manage and respond to a significant cyber incident. According to the PPD-41, the overarching document guiding DOD's Section 1648 report, these personnel would provide necessary expertise to support tasking and decision making by a Cyber Unified Coordination Group.

[24]According to NORTHCOM, the command also offers this course to civilians from the Department of Homeland Security, the Federal Emergency Management Agency, the Department of Justice, other federal emergency support function agencies, state emergency response agencies, and non-governmental and volunteer agencies.

In addition, DOD's Significant Cyber Incident Coordination Procedures require the Chairman of the Joint Chiefs of Staff, through the National Military Command Center, to maintain a list of senior DOD officials from specified organizations that could represent DOD during a Cyber Unified Coordination Group and who are trained in the National Incident Management System.

As of August 2017, DOD officials acknowledged the department had not updated its cyber incident coordination training to incorporate the tenets of PPD-41. Joint Staff officials told us they have staff qualified and trained in the National Incident Management System; however, the officials were unable to provide us a list of senior officials from DOD organizations that could participate in a Cyber Unified Coordination Group that had been trained in the National Incident Management System.

An official from the Office of DOD Principal Cyber Advisor acknowledged the Joint Staff is not tracking personnel who have been qualified and trained in the National Incident Management System, as required by the DOD Significant Cyber Incident Coordination Procedures. Consequently, it is unclear whether senior DOD officials who may be asked to participate in a Cyber Unified Coordination Group will be trained in the National Incident Management System. Until DOD updates its cyber incident response training and maintains a list of senior DOD officials from organizations who could represent DOD during a Cyber Unified Coordination Group and who are trained in the National Incident Management System, the department will not be in compliance with PPD-41 and may not have the personnel with expertise to manage and respond to a significant cyber incident.

Conclusions

DOD recognizes that a disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security and that the department must be prepared to support civil authorities in all domains—including in cyberspace. While DOD addressed some of the required elements set forth in Section 1648, the report submitted does not highlight the full scope of the department's planning and preparation efforts to support civil authorities in response to a cyber incident. We are not making recommendations on these issues because we have previously made recommendations in areas where the Section 1648 report did not contain complete information. However, without complying with the training requirements outlined in PPD-41 and

the *DOD Significant Cyber Incident Coordination Procedures*, the department cannot reasonably ensure it has the personnel with expertise to manage and respond to a significant cyber incident. Taking action to improve the areas we have highlighted should help DOD sustain the progress it has already made. With the President's decision to elevate CYBERCOM to a unified combatant command, such actions will also help as DOD continues to plan to support civil authorities in response to a cyber incident and where CYBERCOM has a significant role.

Recommendations for Executive Action

We are making the following two recommendations to DOD:

The Assistant Secretary of Defense for Homeland Defense and Global Security, in coordination with the Chairman of the Joint Chiefs of Staff and other appropriate DOD components, should update the department's cyber incident coordination training to incorporate the tenets of PPD-41.

The Chairman of the Joint Chiefs of Staff should maintain a list of senior DOD officials from organizations that could represent DOD during a Cyber Unified Coordination Group and that are trained in the National Incident Management System.

Agency Comments and Our Evaluation

We provided a draft of our report to DOD for review and comment. In its written comments, DOD partially concurred with our first recommendation and concurred with the second. DOD's written comments are reprinted in their entirety in appendix IV.

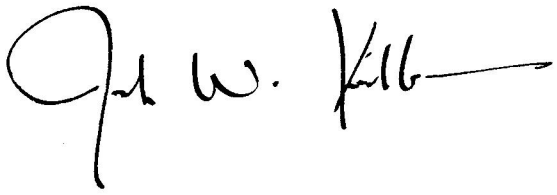
DOD partially concurred with our recommendation to update the department's cyber incident coordination training to incorporate the tenets of PPD-41. In its response, DOD acknowledged the need to continue its emphasis on cyber incident coordination training and states that the department is wholly committed to updating the appropriate training as part of its formal after action reviews during each exercise and training event. DOD stated that it prepares for cyber incidents by exercising interagency roles and responsibilities, and command and control within a cyber threat scenario. While these exercises emphasize the development of comprehensive cyber incident response plans and seek to foster cyber incident coordination, DOD did not identify any specific exercise or training event in which the department will incorporate the tenets of PPD-

41. Accordingly, we continue to believe that our recommendation is warranted. As we reported and DOD acknowledged, Cyber Guard is a tactical-level exercise that would not fully incorporate all DOD components that would participate in a unified cyber response consistent with PPD-41. DOD would meet the intent of our recommendation by conducting one or more cyber incident exercises that incorporate the tenets of PPD-41 into command and control (i.e., operational-level) relationships across all relevant commands and not just across CYBERCOM.

DOD concurred with our recommendation that the Joint Staff maintain a list of senior DOD officials from organizations who could represent DOD during a Cyber Unified Coordination Group and who are trained in the National Incident Management System. DOD stated that the Joint Staff will ensure that senior DOD personnel are familiar with the National Incident Management System, or advised by personnel that are, prior to representing the department during a Cyber Unified Coordination Group. The department also plans to re-emphasize these efforts as part of its onboarding process for newly assigned senior leaders, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Assistant Secretary of Defense for Homeland Defense and Global Security, the Chairman of the Joint Chiefs of Staff, 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. Key contributors to this report are listed in appendix V.



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: Status of Three Recommendations from Our Recent Reports on Defense Cyber Civil Support

During our review of the Department of Defense's (DOD) Section 1648 report, we followed up on three recommendations from our recent reports that could improve the department's planning and processes for supporting civil authorities in a cyber incident. Table 2 summarizes the status of these recommendations.

Table 2: Status of Three Recommendations from Our Recent Reports Related to Defense Cyber Civil Support

	Our recommendation	Status of recommendation
Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercise, GAO-16-574, September 6, 2016	Recommendation: 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 use—if requested and approved—to support civil authorities in a cyber incident.	Status: Open DOD response: Partially concurred Our assessment: As of July 2017, the department has not implemented this recommendation and indicated that the National Guard unit's cyber capabilities, when fully established, will be tracked in the Defense Readiness Reporting System (DRRS). We maintain our position that this system alone will not provide DOD leaders complete information about National Guard cyber capabilities that could facilitate a quick response in a cyber incident and that they could employ to assist civil authorities. 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. 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.

	Our recommendation	Status of recommendation
	Recommendation: Conduct a tier 1 exercise that will improve DOD's planning efforts to support civil authorities in a cyber incident.	Status: Open DOD response: Partially concurred Our assessment: As of July 2017, the department had not implemented this recommendation. U.S. Cyber Command officials told us the command is currently planning an internal staff exercise to address our recommendation to exercise its forces at the operational echelon of leadership. 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.
Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents, GAO-16-332, April 4, 2016	Recommendation: Issue or update guidance that clarifies roles and responsibilities for relevant entities and officials—including the DOD components, supported and supporting commands, and dual-status commander—to support civil authorities as needed in a cyber incident.	Status: Open DOD response: Concurred Our assessment: In June 2017, DOD issued supplementary policy guidance that assigns responsibilities and details procedures for providing defense support to cyber incident response.[a] Although DOD took part of the recommended action, our review of DOD's updated guidance shows that the supported and supporting commands have not been identified and the role of the dual-status commander is still not clearly defined. Until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, as we recommended, DOD will continue to experience uncertainty about the roles and responsibilities of different DOD components and commands with regard to providing support to civil authorities in the event of a significant cyber incident.

Source: GAO analysis of DOD information. | GAO-18-47

[a]See Directive-Type Memorandum 17-007, Interim Policy and Guidance for Defense Support to Cyber Incident Response (June 21, 2017).

Appendix II: Section 1648 (a) of the National Defense Authorization Act for Fiscal Year 2016

SEC. 1648. COMPREHENSIVE PLAN AND BIENNIAL EXERCISES ON RESPONDING TO CYBER ATTACKS.

(a) COMPREHENSIVE PLAN OF DEPARTMENT OF DEFENSE TO SUPPORT CIVIL AUTHORITIES IN RESPONSE TO CYBER ATTACKS BY FOREIGN POWERS.—

(1) PLAN REQUIRED.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall develop a comprehensive plan for the United States Cyber Command to support civil authorities in responding to cyber attacks by foreign powers (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)) against the United States or a United States person.

(B) ELEMENTS.—The plan required by subparagraph (A) shall include the following:

(i) A plan for internal Department of Defense collective training activities that are integrated with exercises conducted with other agencies and State and local governments.

(ii) Plans for coordination with the heads of other Federal agencies and State and local governments pursuant to the exercises required under clause (i).

(iii) A list of any other exercises previously conducted that are used in the formulation of the plan required by subparagraph (A), such as Operation Noble Eagle.

(iv) Descriptions of the roles, responsibilities, and expectations of Federal, State, and local authorities as the Secretary understands them.

(v) Descriptions of the roles, responsibilities, and expectations of the active components and reserve components of the Armed Forces.

(vi) A description of such legislative and administrative action as may be necessary to carry out the plan required by subparagraph (A).

(2) COMPTROLLER GENERAL OF THE UNITED STATES REVIEW OF PLAN.—The Comptroller General of the United States shall review the plan developed under paragraph (1)(A).

Appendix III: Objective, Scope, and Methodology

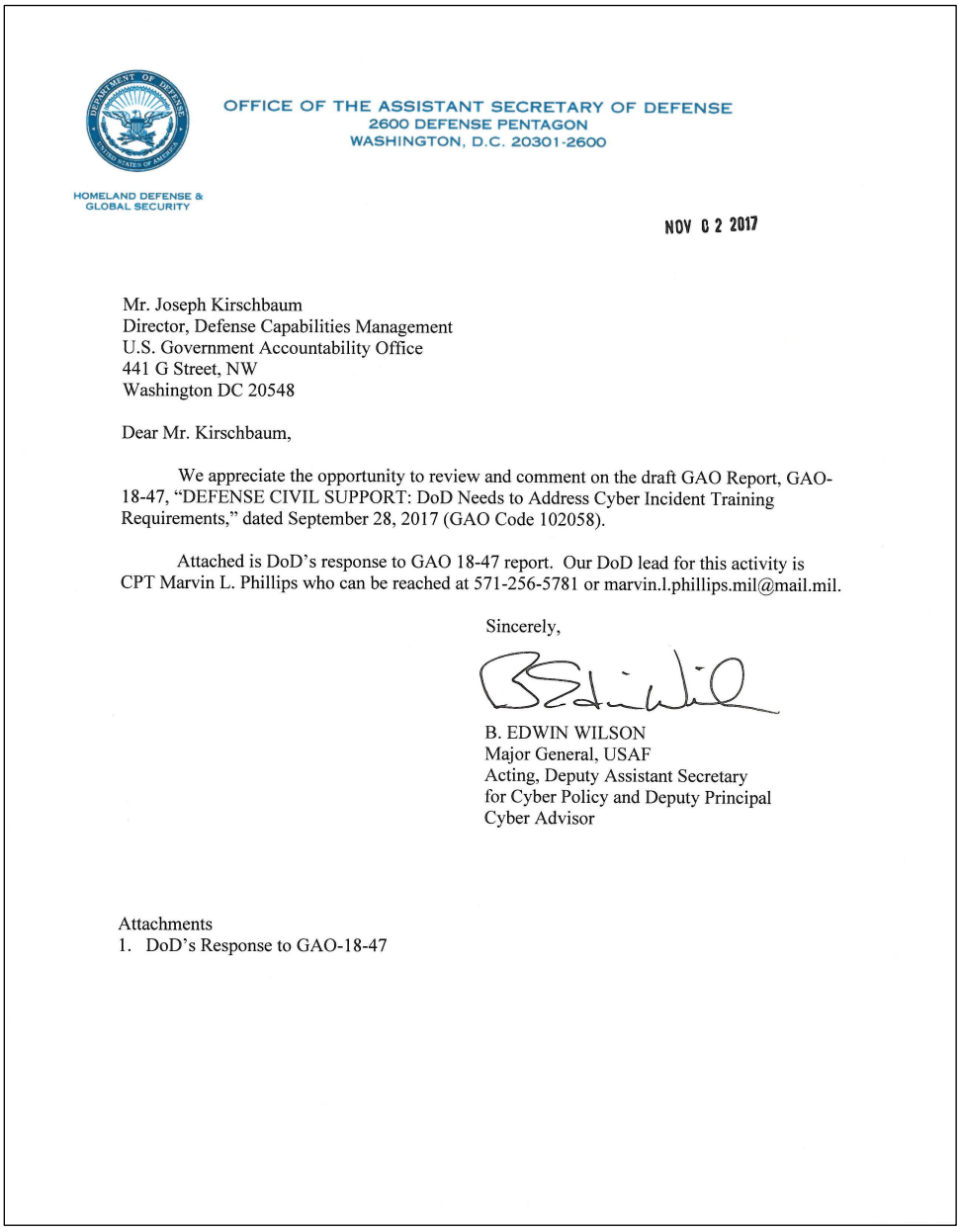
Our objective was to determine the extent to which the Department of Defense's (DOD) Section 1648 report submission addressed the statutorily required elements.

To determine the extent to which DOD's Section 1648 report addressed the statutorily required elements, we analyzed the text of DOD's Section 1648 report. To conduct our analysis of DOD's Section 1648 report, two of our analysts analyzed the text of the Section 1648 report and assessed the extent to which the report addressed the six elements required by the statute. The analysts assessed each element in the report as "fully addressed," "partially addressed," or "not addressed." If the Section 1648 report addressed all aspects of the required element, the analysts determined that DOD had "fully addressed" the element. If the report addressed some aspects of a required element, but not all, the analysts determined that DOD had "partially addressed" the element. If the report did not address any aspects of a required element, the analysts determined that DOD "did not address" the element. A third independent analyst reviewed the initial determinations and assessed whether they were accurate.

For further information, we met with relevant officials from DOD components—such as from the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, including the Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities and the Office of the Deputy Assistant Secretary of Defense for Cyber Policy; the Joint Staff; U.S. Northern Command (NORTHCOM); U.S. Pacific Command (PACOM); U.S. Cyber Command (CYBERCOM); and the National Guard Bureau. We also interviewed Department of Homeland Security officials to obtain clarifying and supporting information on the process by which the department plans and prepares for a cyber incident requiring civil support. In the cases in which the analysts determined that the plan did not address some aspects of a required element, they discussed their preliminary analyses with officials from the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security to seek additional information. Additionally, DOD officials offered clarification regarding the Defense Support of Civil Authorities process, DOD roles and responsibilities in civil support, and information on ongoing initiatives.

We conducted this performance audit from May 2017 to November 2017 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.

Appendix IV: 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

NOV 0 2 2017

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

Dear Mr. Kirschbaum,

We appreciate the opportunity to review and comment on the draft GAO Report, GAO-18-47, "DEFENSE CIVIL SUPPORT: DoD Needs to Address Cyber Incident Training Requirements," dated September 28, 2017 (GAO Code 102058).

Attached is DoD's response to GAO 18-47 report. Our DoD lead for this activity is CPT Marvin L. Phillips who can be reached at 571-256-5781 or marvin.l.phillips.mil@mail.mil.

Sincerely,

B. EDWIN WILSON
Major General, USAF
Acting, Deputy Assistant Secretary
for Cyber Policy and Deputy Principal
Cyber Advisor

Attachments
1. DoD's Response to GAO-18-47

GAO DRAFT REPORT DATED SEPTEMBER 28, 2017
GAO-18-47 (GAO CODE 102058)

"DEFENSE CIVIL SUPPORT: DOD NEEDS TO ADDRESS CYBER INCIDENT TRAINING REQUIREMENTS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Assistant Secretary of Defense for Homeland Defense and Global Security, in coordination with the Chairman of the Joint Chiefs of Staff and other appropriate DoD components, should update the Department's cyber incident coordination training to incorporate the tenets of PPD-41.

DoD RESPONSE:

The Department of Defense (DoD) partially concurs with the GAO recommendation. DoD prepares for cyber incidents by conducting exercises to test preparedness, process, and command and control in responding to cyber incidents. This includes exercising coordination with interagency partners. For example, several recent and upcoming multi-combatant command joint events exercise interagency roles and responsibilities, and command and control within a cyber threat scenario. The objective is to emphasize the development of comprehensive cyber incident response plans that leverage interagency cyber capabilities and legal authorities. These exercises also seek to foster cyber incident coordination by promoting and developing greater understanding of individual and collective capabilities, to include refining whole-of-government tactics, techniques, and procedures. There is broad support of these exercises by the Department of Homeland Security, the Federal Bureau of Investigation, the Federal Aviation Administration, the National Security Agency, the National Guard Bureau, U. S. Cyber Command and U. S. Northern Command. The Department acknowledges the need to continue its emphasis on cyber incident coordination training and is wholly committed to updating the appropriate training as part of its formal after action reviews during each exercise and training event.

RECOMMENDATION 2: The GAO recommends that the Chairman of the Joint Chiefs of Staff should maintain a list of senior DoD officials from organizations that could represent DoD during a Cyber Unified Coordination Group and who are trained in the National Incident Management System (NIMS).

DoD RESPONSE:

The Department of Defense concurs with comment to the GAO recommendation. Efforts are underway to identify key personnel to complete the Federal Emergency Management Agency NIMS training. Consistent with DoD guidance, the Joint Staff will ensure that senior DoD personnel are familiar with NIMS, or advised by personnel that are, prior to representing the Department during a Cyber Unified Coordination Group. The Department is also re-emphasizing these efforts as part of its onboarding process for newly assigned senior leaders as appropriate.

Appendix V: 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, David Beardwood, Pamela Davidson, Ashley Houston, Gabrielle Matuzsan, and Spencer Tacktill made key contributions to this report.

Appendix VI: Accessible Data

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Defense

Page 1

NOV 2, 2017

Mr. Joseph Kirschbaum

Director, Defense Capabilities Management

U.S. Government Accountability Office 441 G Street, NW

Washington DC 20548

Dear Mr. Kirschbaum,

We appreciate the opportunity to review and comment on the draft GAO Report, GAO- 18-47, "DEFENSE CIVIL SUPPORT: DoD Needs to Address Cyber Incident Training Requirements," dated September 28, 2017 (GAO Code 102058).

Attached is DoD's response to GAO 18-47 report. Our DoD lead for this activity is CPT Marvin L. Phillips who can be reached at 571-256-5781 or marvin.l.phillips.mil@mail.mil.

Sincerely,

B. EDWIN WILSON Major General, USAF

Acting, Deputy Assistant Secretary for Cyber Policy and Deputy Principal Cyber Advisor

Attachments

1. DoD's Response to GAO-18-47

Page 2

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1:

The GAO recommends that the Assistant Secretary of Defense for Homeland Defense and Global Security, in coordination with the Chairman of the Joint Chiefs of Staff and other appropriate DoD components, should update the Department's cyber incident coordination training to incorporate the tenets of PPD-41.

DoD RESPONS**E**:

The Department of Defense (DoD) partially concurs with the GAO recommendation. DoD prepares for cyber incidents by conducting exercises to test preparedness, process, and command and control in responding to cyber incidents. This includes exercising coordination with interagency partners. For example, several recent and upcoming multi-combatant command joint events exercise interagency roles and responsibilities, and command and control within a cyber threat scenario. The objective is to emphasize the development of comprehensive cyber incident response plans that leverage interagency cyber capabilities and legal authorities. These exercises also seek to foster cyber incident coordination by promoting and developing greater understanding of individual and collective capabilities, to include refining whole-of-government tactics, techniques, and procedures. There is broad support of these exercises by the Department of Homeland Security, the Federal Bureau oflnvestigation, the Federal Aviation Administration, the National Security Agency, the National Guard Bureau, U.S. Cyber Command and U.S. Northern Command. The Department acknowledges the need to continue its emphasis on cyber incident coordination training and is wholly committed to updating the appropriate training as part of its formal after action reviews during each exercise and training event.

RECOMMENDATION 2:

The GAO recommends that the Chairman of the Joint Chiefs of Staff should maintain a list of senior DoD officials from organizations that could represent DoD during a Cyber Unified Coordination Group and who are trained in the National Incident Management System (NIMS).

DoD RESPONSE:

The Department of Defense concurs with comment to the GAO recommendation. Efforts are underway to identify key personnel to complete the Federal Emergency Management Agency NIMS training. Consistent with DoD guidance, the Joint Staff will ensure that senior DoD personnel are familiar with NIMS, or advised by personnel that are, prior to representing the Department during a Cyber Unified Coordination Group. The Department is also re- emphasizing these efforts as part of its onboarding process for newly assigned senior leaders as appropriate.

Related GAO Products

Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises. GAO-16-574. Washington, D.C.: September 6, 2016.

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.

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

Homeland Defense: DOD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters. GAO-10-386. Washington, D.C.: March 30, 2010.

Homeland Defense: DOD Needs to Take Actions to Enhance Interagency Coordination for Its Homeland Defense and Civil Support Missions. GAO-10-364. Washington, D.C.: March 30, 2010.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548