United States Government Accountability Office

Report to Congressional Committees

April 2016

CIVIL SUPPORT

DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents

Accessible Version

GAO-16-332

April 2016

CIVIL SUPPORT

DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents

GAO Highlights

Highlights of GAO-16-332, a report to congressional committees

Why GAO Did This Study

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. DOD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* states that DOD must be prepared to support civil authorities in all domains—including cyberspace—and recognizes that the department plays a crucial role in supporting a national effort to confront cyber threats to critical infrastructure.

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. This report assesses the extent to which DOD has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to a cyber incident.

GAO reviewed DOD DSCA guidance, policies, and plans; and met with relevant DOD, National Guard Bureau, and Department of Homeland Security officials.

What GAO Recommends

GAO recommends that DOD issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with the recommendation and stated that the department will issue or update guidance.

View GAO-16-332. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

The Department of Defense (DOD) has developed overarching guidance about how it is to support civil authorities as part of its Defense Support of Civil Authorities (DSCA) mission, but DOD's guidance does not clearly define its roles and responsibilities for cyber incidents. Specifically, DOD has developed and issued key DSCA guidance—such as DOD Directive 3025.18, *Defense Support of Civil Authorities*—that provides guidance for the execution and oversight of DSCA. However, 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 called upon to support a cyber incident. Specifically:

- **DOD components:** DOD Directive 3025.18 identifies the specific responsibilities of DOD officials who oversee DOD components responsible for various elements of DSCA, such as the Assistant Secretary of Defense for Health Affairs for health or medical-related support, but does not specify the responsibilities of DOD components (such as the Assistant Secretary of Defense for Homeland Defense and Global Security) in supporting civil authorities for cyber incidents.
- **Supported command:** Various guidance documents are inconsistent on which combatant command would be designated the supported command and have primary responsibility for supporting civil authorities during a cyber incident. U.S. Northern Command's DSCA response concept plan states that U.S. Northern Command would be the supported command for a DSCA mission that may include cyber domain incidents and activities. However, other guidance directs and DOD officials stated that a different command, U.S. Cyber Command, would be responsible for supporting civil authorities in a cyber incident.
- **Dual-status commander:** Key DSCA guidance documents do not identify the role of the dual-status commander—that is, the commander who has authority over federal military and National Guard forces—in supporting civil authorities during a cyber incident. According to U.S. Northern Command officials, in a recent cyber exercise there was a lack of unity of effort among the DOD and National Guard forces that were responding to the emergency but were not under the control of the dual-status commander.

DOD officials acknowledged the limitations of current guidance to direct the department's efforts in supporting civil authorities in a cyber incident and discussed with GAO the need for clarified guidance on roles and responsibilities. DOD officials stated that the department had not yet determined the approach it would take to support a civil authority in a cyber incident and, as of January 2016, DOD had not begun efforts to issue or update guidance and did not have an estimate on when the guidance will be finalized. Until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, there would continue to be uncertainty about which DOD component or command should be providing support to civil authorities in the event of a major cyber incident.

Contents

Abbreviations

DOD	Department of Defense
DSCA	Defense Support of Civil Authorities
Stafford Act	Robert T. Stafford Disaster Relief and Emergency Assistance Act

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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

April 4, 2016

Congressional Committees

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.[1] The Department of Defense's (DOD) 2015 *Cyber Strategy* reports that threat actors are planning to conduct disruptive and destructive cyberattacks on the United States and that the government, military, and private sectors are vulnerable to this cyber threat.[2] DOD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* states that DOD must be prepared to defend the homeland and support civil authorities in all domains—including cyberspace—and recognizes that the department plays a crucial role in supporting a national effort to confront cyber threats to critical infrastructure.[3] Generally, DOD supports civil authorities through its Defense Support of Civil Authorities (DSCA) mission.[4]

We have previously reported on the progress DOD has made to address issues related to civil support. For example, in June 2015, we testified on the progress DOD had made in implementing our prior recommendations to support civil authorities including strengthening its strategy, plans, and guidance; interagency coordination; and capabilities.[5] We found that DOD had taken action to address some of our prior recommendations but had not fully addressed others. For example, we found that DOD had improved interagency coordination for support of civil authorities by

[1]James R. Clapper, Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Armed Services Committee (Feb. 26, 2015).

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

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

[4]DSCA is DOD's mission to provide support through the federal military force, 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."

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

defining interagency roles and responsibilities and had identified capabilities it could provide for DSCA; however, it had not issued implementation guidance on the use of dual-status commanders.[6]

House Report 114-102 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2016[7] included a provision that GAO assess DOD's plans for providing support to civil authorities related to a domestic cyber incident.[8] This report assesses the extent to which DOD has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to cyber incidents.

To assess the extent to which DOD has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to cyber incidents, we reviewed key DOD policies, guidance, strategies, and instructions such as Joint Publication 3-28, *Defense Support of Civil Authorities*;[9] *The DOD Cyber Strategy*;[10] Chairman of the Joint Chiefs of Staff Execute Order, *Defense Support to Civil Authorities (DSCA);*[11] and DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)*.[12] DOD officials identified these documents as the key documents the department uses to guide its DSCA efforts. We reviewed these documents to identify: (1) DOD's authority to respond to

[6]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.

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

[8]A cyber incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the nation; or both.

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

[10]DOD, *The DOD Cyber Strategy*.

[11]Chairman of the Joint Chiefs of Staff Standing Execute Order, *Defense Support of Civil Authorities (DSCA)* (June 2013). (Hereinafter cited as Chairman of the Joint Chiefs of Staff Standing Execute Order, *Defense Support of Civil Authorities*.)

[12]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.)

cyber incidents for civil authorities, (2) DOD's role in the Department of Homeland Security's National Response Framework, (3) DOD components' roles and responsibilities for providing support to civil authorities for a cyber incident,[13] (4) DOD's request for assistance procedures, (5) criteria DOD uses to support a request for assistance from civil authorities, and (6) the extent to which DOD has incorporated and provided specific information on responding to a cyber incident into its guidance on DSCA. We also reviewed the President of the United States' Unified Command Plan,[14] DOD's and the Department of Homeland Security's memorandum of agreement regarding cybersecurity,[15] and U.S. Northern Command's *Defense Support of Civil Authorities* concept plan[16] to determine the extent to which the documents identify the role of DOD components in supporting civil authorities in a cyber incident. We compared these documents to the standards and guidance for setting agency roles and responsibilities and command relationships identified in the *National Response Framework*,[17] *Standards for Internal Control in the Federal Government*,[18] the Office of Management and Budget's *Management Responsibility for Internal*

[13]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.

[14]The President of the United States, *Unified Command Plan* (Washington, D.C.: Apr. 6, 2011, with change 1, dated Sept. 12, 2011). (Hereinafter cited as *Unified Command Plan*.)

[15]Department of Homeland Security and Department of Defense, *Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity* (Sept. 27, 2010). (Hereinafter cited as *Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity*.)

[16]U.S. Northern Command, *Concept Plan 3500-14, Defense Support of Civil Authorities Response* (Colorado Springs, Colorado: July 2014). (Hereinafter cited as U.S. Northern Command*, Concept Plan 3500-14*.)

[17]Department of Homeland Security, *National Response Framework*, 2nd ed. (May 2013).The *National Response Framework* is a guide on how the United States responds to all types of disasters and emergencies.

[18]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1, 1999). These standards were in effect prior to fiscal year 2016 and cover the period of DOD's DSCA guidance. These standards were subsequently updated. The updates went into effect on October 1, 2015. See GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

Control,[19] the *Joint Action Plan for Developing Unity of Effort*,[20] *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity*,[21] and DOD's Joint Publication 3-12(R), *Cyberspace Operations*.[22] We did not review any state or local agency civil support–related documents because our review focused on DSCA provided by federal military and National Guard forces. Additionally, we interviewed officials from DOD involved in DSCA from the Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities and U.S. Northern Command to obtain further information regarding: the roles and responsibilities of DOD components in responding to cyber incidents; the cyber response framework; and the challenges in developing the framework, if any. We also interviewed officials from the Department of Homeland Security's National Cybersecurity and Communications Integration Center and the Federal Emergency Management Agency to obtain information regarding their efforts to coordinate with DOD components to support civil authorities in a cyber incident. A full list of the offices we contacted is in appendix I.

We conducted this performance audit from June 2015 to April 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.

[19]Office of Management and Budget, Circular A-123, *Management's Responsibility for Internal Control* (Washington, D.C.: Dec. 21, 2004).

[20]Department of Defense, Council of Governors, and Department of Homeland Security, *Joint Action Plan for Developing Unity of Effort* (Washington, D.C.: 2010). (Hereinafter cited as *Joint Action Plan for Developing Unity of Effort*.)

[21]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). (Hereinafter cited as *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity*.)

[22]Joint Chiefs of Staff, Joint Publication 3-12(R), *Cyberspace Operations* (Feb. 5, 2013). (Hereinafter cited as Joint Publication 3-12(R)).

Background

DOD Support to Major Disasters and Emergencies

Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), when state capabilities and resources are overwhelmed and the President declares an emergency or disaster, the Governor of an affected state can request assistance from the federal government for major disasters or emergencies.[23] Additionally under the Economy Act, a federal agency may request the support of another federal agency, including DOD, without a presidential declaration of an emergency.[24]

The federal government's response to major disasters and emergencies in the United States is guided by the Department of Homeland Security's *National Response Framework*, a national-level guide on how local, state, and federal governments respond to major disasters and emergencies.[25] The Department of Homeland Security's interim *National Cyber Incident Response Plan* outlines domestic cyber incident response coordination and execution among federal, state and territorial, and local governments,

[23]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.

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

[25]Department of Homeland Security, *National Response Framework*, 2nd ed. The National Response Framework is a component of the National Preparedness System mandated in Presidential Policy Directive 8, *National Preparedness.* The National Response Framework sets the doctrine for how the United States builds, sustains, and delivers the response core capabilities identified in the National Preparedness Goal. The National Preparedness Goal establishes the capabilities and outcomes the United States must accomplish in order to be secure and resilient. 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. The Department of Homeland Security is responsible for overseeing the preparedness activities of the communications emergency support functions, among others, which include cybersecurity.

and the private sector.[26] Various federal agencies can play a lead or supporting role in responding to major disasters and emergencies. 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.

Defense resources are committed after the lead agency submits a request for assistance and the President or Secretary of Defense directs DOD to provide support. DOD does not generally develop military forces specifically for the DSCA mission and the department does not provide funding to train, equip, or exercise specifically for DSCA unless directed to do so by Congress, the President, or the Secretary of Defense. Examples of DOD's DSCA missions include responding to major disasters and emergencies (both natural and man-made); support of civilian law enforcement agencies, including civil disturbance operations; restoring public health, medical services, and civil order, such as animal/plant disease eradication and counterdrug operations; and providing support for national special security events. Specifically, in its DSCA mission, DOD supports civil authorities by providing them with resources for responses to disasters like Hurricane Sandy and wildfires in the western United States as well as national special security events such as political-party national conventions.

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.[27] DOD components can also provide support to civil authorities under separate authority. For example, the DOD Cyber Crime Center can support digital and

[26]Department of Homeland Security, *National Cyber Incident Response Plan*, Interim Version (Washington, D.C.: September 2010). Department of Homeland Security 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 was finalized.

[27]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 Title 10 or Title 32. 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 statues, and the respective state is responsible for National Guard expenses.

multimedia forensic requests and provide training services to non-DOD government organizations.[28] Additionally, the National Security Agency, as an element of the Intelligence Community, is authorized to provide any other assistance and cooperation to law enforcement and other civil authorities not precluded by applicable law.[29]

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 U.S. Northern Command and U.S. Pacific Command commanders), and the chief of the National Guard Bureau, among others.[30] DOD's Assistant Secretary of Defense for Homeland Defense and Global Security is the principal civilian advisor responsible for homeland defense, DSCA, and cyber policy for the department.[31] 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.[32] The Chairman of the Joint Chiefs of Staff advises the Secretary of Defense on the effects of requests for

[28]DOD Directive 5505.13E, *DOD Executive Agent (EA) for the DOD Cyber Crime Center (DC3)* (Mar. 1, 2010).

[29]White House, Executive Order 12333, as amended, *United States Intelligence Activities*, paragraph 2.6(d).

[30]According to Joint Chiefs of Staff, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Nov. 8, 2010, as amended through Nov. 15, 2015), 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.

[31]In January 2015, the Office of the Under Secretary of Defense for Policy reorganized its missions and renamed the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs as the Assistant Secretary of Defense for Homeland Defense and Global Security. The Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities and the Deputy Assistant Secretary of Defense for Cyber Policy report to this official.

[32]According to Joint Publication 1-02, cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Joint Publication 1-02 defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

DSCA on national security and identifies available resources for support in response to DSCA requests. U.S. Northern Command and U.S. Pacific Command provide support to civil authorities at the federal, state, and local levels as directed. Further, U.S. Cyber Command synchronizes the planning for cyberspace operations in coordination with other combatant commands, the military services, and other appropriate federal agencies.[33] The National Guard Bureau is supposed to coordinate communications between DOD components and states for National Guard matters and conducts an annual assessment on the readiness of the National Guard to conduct DSCA activities.[34] 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.[35]

In military operations where multiple combatant commands have a role, the Secretary of Defense will establish support relationships and determine the supported and supporting combatant commanders. 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.

[33]U.S. Cyber Command is a subordinate unified command to U.S. Strategic Command. A subordinate unified command is established by a commander of a unified command to conduct operations on a continuing basis in accordance with the criteria set forth for unified commands. See Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.*

[34]The Army National Guard and Air National Guard of the United States perform federal missions under the command of the President, and the National Guard of each state performs state missions under the command of the state's governor.

[35]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 when the armed forces and National Guard are employed simultaneously in support of civil authorities, including missions involving major disasters and emergencies. In their technical comments to our draft report, DOD officials stated that 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.

DOD Cyber Reports to Congress

In response to a provision in the National Defense Authorization Act for Fiscal Year 2014,[36] DOD issued a cyber mission analysis report on the department's efforts to conduct cyberspace operations using its total cyber forces including its active and reserve components—the Army National Guard of the United States, Army Reserve, Air Force Reserve, Air National Guard of the United States, Marine Corps Reserve, and Navy Reserve.[37] In this analysis, DOD found advantages to using its reserve components for cyber missions such as load sharing and providing surge capabilities. The report recommends, among other things, that National Guard state active-duty policies and processes be clarified to ensure unity of effort between DOD and National Guard forces, and that the National Guard focus on support roles such as coordinate, train, advise, and assist with state or local agencies or private industry when directed by their respective governor or authorized by DOD. Additionally, section 933(e) of the National Defense Authorization Act for Fiscal Year 2014 mandated that the Chief of the National Guard Bureau assess DOD's description of the role of the National Guard in supporting DOD's cyber operations. In September 2014, the National Guard Bureau issued its report highlighting, among other things, that the bureau concurs with DOD's finding that the cyber reserve components can offer load sharing and surge capacity and supports DOD's plan to integrate reserve personnel into cyberspace forces.[38]

Additionally, a provision in the National Defense Authorization Act for Fiscal Year 2016 requires DOD to develop a comprehensive plan for U.S. Cyber Command to support civil authorities in response to a cyber attack by a foreign power. 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.[39] This plan is due to Congress in May 2016.

[36]Pub. L. No. 113-66, § 933 (2013).

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

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

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

DOD Has Developed Guidance for Supporting Civil Authorities, but the Guidance Does Not Clearly Define Roles and Responsibilities for Domestic Cyber Incidents

DOD Has Developed DSCA Guidance

DOD has developed and issued overarching policies and guidance for the department's activities to support civil authorities. DOD officials that we met with identified several key documents that guide their DSCA activities:

- DOD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)*, establishes DSCA policy and provides guidance for the execution and oversight of DSCA.[40] This directive also establishes the criteria to evaluate all requests for assistance from civil authorities.[41]
- DOD's Joint Publication 3-28, *Defense Support of Civil Authorities*, provides guidelines to assist in planning and governing the department's activities in DSCA operations and states that DOD may be requested to provide cyberspace support services during DSCA incidents.[42] Joint Publication 3-28 also explains how DOD will support

[40]DOD Directive 3025.18. In addition to this directive, DOD has issued other DOD directives and instructions to guide DOD components in supporting civil authorities for specific DSCA missions. For example, DOD Directive 3025.13 provides policy and guidance on DOD support to the U.S. Secret Service and DOD Instruction 3025.21 provides policy and guidance on DOD's support of civilian law enforcement agencies.

[41]DOD Directive 3025.18 states that all requests from civil authorities and qualifying entities for assistance shall be evaluated for: legality, lethality, risk, cost, readiness, and appropriateness.

[42]Joint Chiefs of Staff, Joint Publication 3-28.

a comprehensive all-hazards response to a catastrophic incident or event, law-enforcement activities and other domestic activities, and special events such as presidential inaugurations. The publication also establishes procedures, assigns responsibilities, and provides instructions for the designation, employment, and training of dual-status commanders for use in DSCA.

- DOD's *DSCA Standing Execute Order* provides the authority for supported combatant commanders to conduct DSCA operations for actual or potential domestic incidents within the commander's area of responsibility.[43]

In addition, U.S. Northern Command officials identified U.S. Northern Command's Concept Plan, *Defense Support of Civil Authorities Response*, as a key document to guide their DSCA efforts. Specifically, the plan provides the framework for a DSCA response within the domestic portions of U.S. Northern Command's area of responsibility.[44]

Further, in April 2015, DOD issued *The DOD Cyber Strategy* as a guide to develop DOD's cyber forces and strengthen DOD's cyber defense and deterrence posture.[45] The cyber strategy directs DOD to develop a framework and to conduct exercises on their capabilities to support civil authorities, the Department of Homeland Security, state and local authorities, and other agencies to help defend the federal government and the private sector in an emergency, if directed. DOD officials told us that the department is in the process of implementing and tracking the status of tasks as part of the framework, to include developing cyberspace operations policies, identified in the strategy.

[43]Chairman of the Joint Chiefs of Staff Standing Execute Order, *Defense Support to Civil Authorities.* This execute order directs DOD's DSCA in support of the Department of Homeland Security's National Response Framework and establishes the authorities to conduct DSCA operations through assigned and allocated forces, preidentified resources, internal resources, and large-scale response resources.

[44]U.S. Northern Command*, Concept Plan.* U.S. Northern Command's area of responsibility for civil support is comprised of the contiguous 48 states, Alaska, and the District of Columbia and the command may also support civil authorities' major disaster and emergency response operations in the Commonwealth of Puerto Rico and the U.S. Virgin Islands.

[45]DOD, *The DOD Cyber Strategy.*

DOD Guidance Does Not Clearly Define DSCA Roles and Responsibilities for Domestic Cyber Incidents

We found that DOD guidance that we reviewed—identified by DOD officials as the key documents that guide DOD's DSCA activities—does not clearly define the roles and responsibilities of key DOD entities, such as DOD components, the supported command, or the dual-status commander, if they are requested to support civil authorities in a cyber incident. Further, we found that, in some cases, DOD guidance provides specific details on other types of DSCA-related responses, such as assigning roles and responsibilities for fire or emergency services support and medical support, but does not provide the same level of detail or assign roles and responsibilities for cyber support. In other cases, the designation of cyber roles and responsibilities in DOD guidance is inconsistent. National and DOD guidance documents highlight the importance of clearly established roles, responsibilities, and command relationships. For example, the Department of Homeland Security's *National Response Framework* highlights that incident response structures should be based on clearly established roles, responsibilities, and reporting protocols.[46] Also, the 2010 *Joint Action Plan for Developing Unity of Effort* emphasizes the importance of properly configured command and control arrangements for designated planned events or in response to emergencies or natural disasters within the United States.[47] The 2014 *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* also emphasizes that agencies should develop, enhance, and clarify policies, roles, and responsibilities that promote a national approach to preventing, responding to, and recovering from cyber incidents.[48] Further, DOD's Joint Publication 3-12(R), *Cyberspace Operations*, states that clearly established command relationships are

[46]Department of Homeland Security, *National Response Framework*, 2nd ed.

[47]Department of Defense, Council of Governors, and Department of Homeland Security, *Joint Action Plan for Developing Unity of Effort*. In 2010, DOD worked with the Department of Homeland Security, the Federal Emergency Management Agency, and the Council of Governors to develop the Joint Action Plan for Developing Unity of Effort, which provides a framework for state and federal agencies to coordinate their response to domestic incidents and describes the general arrangement of the dual-status commander construct.

[48]Council of Governors, Department of Homeland Security, and Department of Defense, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity*. According to DOD's 2014 Cyber Mission Analysis Report—which DOD provided to Congress in response to a reporting requirement identified in the National Defense Authorization Act for Fiscal Year 2014—this joint action plan is a commitment by the states, Department of Homeland Security, and DOD to improve the nation's cybersecurity posture and it establishes a framework to guide state-federal discussions in areas such as information sharing, operational coordination, and incident response.

crucial for ensuring timely and effective employment of forces.[49] Additionally, defining roles and responsibilities is a leading management practice cited in *Standards for Internal Control in the Federal Government* and the Office of Management and Budget Circular A-123.[50] The standards and the circular state that management within an organization structure must clearly define key areas of authority and responsibilities and establish appropriate lines of reporting.

In reviewing DOD DSCA documents that DOD officials identified as key guidance to determine whether they address roles and responsibilities in cyber incidents, we found examples of lack of clarity on key roles and responsibilities—specifically for DOD components, the supported command, and the dual-status commander—to support civil authorities in a cyber incident.[51]

- **DOD components:** We found that the key DSCA guidance documents do not identify roles and responsibilities of DOD components that may be called upon to support civil authorities in a cyber incident. For example, Joint Publication 3-28 states that DOD forces may be required to provide cyberspace support services during a DSCA incident and provide assistance to state and local government's networks to remediate a disrupted or degraded environment. Joint Publication 3-28 provides joint doctrine to govern the activities and performance of military forces in DSCA operations, the doctrinal basis for interagency coordination during DSCA operations.[52] The publication states that the federal government

[49]Joint Chiefs of Staff, Joint Publication 3-12(R).

[50]GAO/AIMD-00-21.3.1 and OMB Circular A-123. *Standards for Internal Control in the Federal Government* were in effect prior to fiscal year 2016 and cover the period of DOD's DSCA guidance. These standards were subsequently updated and state that management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. The updates went into effect on October 1, 2015. See GAO-14-704G.

[51]DOD officials identified the following key documents that guide their DSCA efforts: Joint Publication 3-28; Chairman of the Joint Chiefs of Staff Standing Execute Order, *Defense Support of Civil Authorities*; and DOD Directive 3025.18. In addition, U.S. Northern Command officials identified the command's Concept Plan 3500-14, *Defense Support of Civil Authorities*, as a key document that guides their DSCA efforts within the command's area of responsibility.

[52]Joint Chiefs of Staff, Joint Publication 3-28.

should be prepared to fill potential gaps to ensure continuity of government and public- and private-sector operations during a catastrophic event.[53] Although the publication provides specific details on other types of DOD support to civil authorities such as meteorological, engineering, health services, and logistics—in some cases, the publication identifies the DOD component responsible for providing the support—it does not provide specific details on how DOD will provide cyber support to civil authorities or identify the DOD component responsible for providing the support.[54] DOD Directive 3025.18 identifies the specific responsibilities of DOD officials who oversee DOD components responsible for various elements of DSCA, such as the Assistant Secretary of Defense for Health Affairs for health or medical support and the Under Secretary of Defense for Acquisitions, Technology and Logistics for the DOD fire and emergency services program, but does not address cyber incidents or specify the responsibilities of DOD components (such as the Assistant Secretary of Defense for Homeland Defense and Global Security) in supporting civil authorities for cyber incidents. Further, DOD's DSCA Execute Order directs DSCA operations and identifies force packages and capabilities—such as search and rescue, transportation, and medical—to support DOD's DSCA efforts, but does not identify cyber-related force packages to support civil authorities.[55]

- **Supported command:** We found that although the key DSCA documents do provide guidance 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, there is a lack of clarity and understanding on this role and inconsistency in DOD guidance. For example, the 2011 Unified Command Plan identified U.S. Northern Command and U.S. Pacific Command as the commands to provide support to civil authorities, to include DSCA at U.S. federal, tribal, state, and local levels, as

[53]DOD defines a catastrophic event as the same as a catastrophic incident. A catastrophic incident is any natural or man-made incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions.

[54]Joint Chiefs of Staff, Joint Publication 3-28.

[55]A force package is a list of forces required to conduct an operation.

directed.[56] U.S. Northern Command's *Defense Support of Civil Authorities Response* concept plan, which is the Secretary of Defense–approved plan on how DOD would provide DSCA within the domestic portions of the U.S. Northern Command's area of responsibility, states that the U.S. Northern Command commander would be the supported commander for a DSCA mission, which may include cyber domain incidents or activities, within the command's area of responsibility—with other DOD components supporting in conducting the missions.[57]

However, other guidance directs and DOD officials stated that a different command, U.S. Cyber Command would be responsible for supporting civil authorities in a cyber incident. Specifically, in 2010, the Secretary of Defense and the Secretary of Homeland Security cosigned a memorandum of agreement that identified U.S. Cyber Command as the DOD component that would receive requests for cybersecurity support from the Department of Homeland Security.[58] Additionally, in June 2015, the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities testified that U.S. Cyber Command would oversee the support that DOD would provide to civil authorities in response to a cyber incident.[59]

Combatant commands had different understandings of which combatant command would be designated the supported command in supporting civil authorities in a cyber incident. For example, U.S. Cyber Command officials told us that if a DSCA incident involved a

[56]*Unified Command Plan.* U.S. Northern Command's domestic area of responsibility includes North America, Puerto Rico, and the U.S. Virgin Islands, and U.S. Pacific Command's area of responsibility includes Hawaii and territories in the Pacific Ocean.

[57]U.S. Northern Command*, Concept Plan 3500-14*. According to U.S. Northern Command officials, U.S. Northern Command would be the supported command for DSCA missions, which may include cyber incidents within U.S. Northern Command's area of responsibility.

[58]Department of Homeland Security and Department of Defense, *Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity.* The memorandum outlines how the two agencies collaborate and coordinate cyberspace activities including those related to a domestic cyber incident.

[59]Robert Salesses, Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities, testimony before the House Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, 114th Cong., 1st sess. (June 10, 2015), 20–24.

cyber response, the Secretary of Defense would likely assign U.S. Cyber Command, a different command than U.S. Northern Command, as the command responsible for providing support to civil authorities in the cyber domain. However, U.S. Northern Command officials stated as of September 2015 that their command had not delegated this responsibility to another command. Additionally, U.S. Pacific Command officials told us that they would be the supported command for a DSCA mission that included a cyber incident within their area of responsibility, with U.S. Cyber Command as the supporting command.

- **Dual-status commander:** We found that key DSCA documents do not identify the role of the dual-status commander in supporting civil authorities during a cyber incident.[60] For example, Joint Publication 3-28, provides guidance on dual-status commanders to include establishing the area of operation, roles and responsibilities of DOD components and the dual-status commander, training program requirements, and provides exclusions on incidents that the dual-status commander cannot be used. However, the publication does not address the roles and responsibilities of the dual-status commander in responding to and in support of civil authorities in a cyber incident. According to the *Joint Action Plan for Developing Unity of Effort,* a dual-status commander could be appointed when federal military forces and state military forces are employed simultaneously in support of civil authorities and is the usual and customary command and control arrangement.[61] A recent exercise highlighted uncertainty as to the roles and responsibilities of the dual-status commander in a cyber incident. Specifically, U.S. Northern Command officials told us that the dual-

[60]In 2012, we reported that gaps in dual-status commander guidance exist because DOD had not developed comprehensive policies and procedures regarding the use and availability of dual-status commanders and that the dual-status commander construct may not be appropriate for all scenarios. For example, we found that DOD has not developed guidance for the use of dual-status commanders for incidents affecting multiple states and territories. We recommended—and DOD concurred—that DOD should develop implementation guidance on the dual-status commander construct. GAO, *Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance* GAO-13-128 (Washington, D.C.: Oct. 24, 2012).

[61]DOD has been using dual-status commanders for select planned and special events since 2004. For example, DOD used the dual-status commander for the 2012 Colorado wildfire response. In its technical comments, DOD identified four distinct phases of examining a dual-status commander: (1) appointment of a dual status commander after approval by the Secretary of Defense; (2) issuing military or state orders; (3) request and sourcing of federal military forces; and (4) assignment of federal military forces to the dual status commander.

status commander who participated in the 2015 U.S. Cyber Command exercise—called Cyber Guard 15—did not have tactical control of cyber units that reported to U.S. Cyber Command. As a result, the officials stated, the cyber units were not able to fully participate in the exercise and log onto the network of the private entity that was used in the exercise. According to the U.S. Northern Command officials, this led to a lack of unity of effort among the units responding to the emergency that were not under the control of the dual-status commander. The National Guard Bureau, in its 2014 *Cyber Mission Analysis Assessment*, similarly highlighted the need for clarification and recommended examining the role of the dual-status commander to determine applicability to both cyberspace and domestic operations within a cyberspace component.[62]

DOD officials acknowledged the limitations of current guidance to direct the department's efforts in supporting civil authorities in a cyber incident and discussed with us the need for clarified guidance on roles and responsibilities. Specifically, officials from 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 told us that current DOD guidance does not adequately address or guide DOD's efforts to support civil authorities in a cyber incident because current guidance does not have specific cyber-related details such as defining what type of support DOD would provide. Further, DOD officials responsible for supporting DSCA requests for assistances from civil authorities including those from the Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities, the Office of the Deputy Assistant Secretary of Defense for Cyber Policy, the National Guard Bureau, U.S. Cyber Command, and U.S. Army Cyber Command acknowledged that DOD needs to develop guidance that more clearly defines roles and responsibilities and provides operating procedures to DOD components. Similarly, 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

[62]National Guard Bureau, *National Guard Bureau Cyber Mission Analysis Assessment* (Washington, D.C.: Sept. 29, 2014).

about the element's roles in supporting civil authorities for a cyber incident.[63]

We found that DOD has not clearly defined the roles and responsibilities of DOD components in supporting civil authorities in a cyber incident because of various factors:

- U.S. Northern Command officials said that DOD had not received a request for assistance from the Department of Homeland Security or any lead federal agency for DOD to support a civil authority in a cyber incident. Consequently, according to the officials, it is unclear which circumstance would lead to such a request. However, an official from the Office of the Deputy Assistant Secretary of Defense for Cyber Policy told us that the department expects to receive more requests to support civil authorities in cyber incidents and acknowledged the need to clarify roles and responsibilities in advance of any requests given the growing focus on cybersecurity among federal agencies.

- DOD officials told us that the department had not yet determined the approach it would take in handling a request for assistance to support a civil authority in a cyber incident. Specifically, officials from the Office the Assistant Secretary of Defense for Homeland Defense and Global Security told us the department was in the process of deciding whether to issue guidance within DOD's current process for providing technical cyber-related assistance, within the existing DSCA framework, or a combination of the two. For example, officials from the Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities told us the department is pursuing efforts to provide guidance that clarifies the current process that DOD uses to provide technical cyber-related assistance.[64] These officials stated that the proposed guidance would be

[63]According to Joint Publication 3-28, a defense coordinating element is staff and military liaison officers who assist the defense coordinating officer in facilitating coordination and support to activated emergency support functions. A defense coordinating officer is DOD's single point of contact within each Federal Emergency Management Agency region for domestic emergencies who is assigned to a joint field office to process requirements for military support.

[64]According to an Office of the Assistant Secretary of Defense for Homeland Defense and Global Security official, DOD technical cyber-related assistance can include cyber indications and warning, vulnerability assessment, incident impact analysis, malware analysis, mitigation techniques, characterization, and digital media analysis.

called "DOD technical cyber assistance," would clarify how DOD would support civil authorities in a cyber incident, and would exist outside of the existing DSCA framework. In another example, an official from the Office of the Deputy Assistant Secretary of Defense for Cyber Policy told us that once developed, DOD's guidance on "DOD's technical cyber assistance" would be incorporated into the existing DSCA framework. Meanwhile, National Guard Bureau officials told us that developing a separate DOD technical cyber-assistance framework would not be necessary to support civil authorities in a cyber incident. Rather, DOD can address the challenges of responding to a cyber incident by clarifying roles and responsibilities within existing DOD policies and guidance. Regardless of which approach or combination of approaches DOD decides to take, as of January 2016, DOD had not begun efforts to develop or issue updated guidance on how DOD will support civil authorities during a cyber incident and did not have an estimate on when the guidance will be finalized.

The absence of clearly defined roles and responsibilities contrasts with the direction stated in DOD and federal guidance described above for creating and preserving unity of effort, coordination, and clarity in roles and responsibilities. This absence has caused uncertainty about who in DOD would respond to support civil authorities in a cyber incident and how they would coordinate and conduct such a response. DOD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* recognizes that the department must be prepared to support civil authorities in all domains, including cyberspace, and that information networks are subjected to increasing cyber intrusions and are vulnerable to physical attack and natural disasters.[65] Without providing specific details on how military forces will support civil authorities in cyber incidents including roles and responsibilities either as part of the DSCA framework or a separate cyber-technical assistance framework, DOD guidance, such as the department's joint doctrine, will not be complete or able to provide military forces with the guidelines and principles needed to assist in planning, conducting, and providing cyber support.

Until DOD clarifies the roles and responsibilities of its components, supported command, and the dual-status commander for cyber incidents either in a separate cyber-technical assistance framework or through updating DSCA guidance, DOD may not be positioned to effectively employ its forces and capabilities to support civil authorities in a cyber

[65]DOD, *Strategy for Homeland Defense and Defense Support of Civil Authorities*.

incident. Additionally, there would continue to be uncertainty within DOD and among federal, state, and local partners about which DOD component or command should be providing support to civil authorities in the event of a major cyber incident.

Further, DOD is required by Congress to develop a comprehensive plan (due in May 2016) for U.S. Cyber Command to support civil authorities in response to a cyber attack by a foreign power. 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. Without clarifying roles and responsibilities in general, the comprehensive plan DOD develops may be incomplete.[66]

Conclusions

DOD has developed a significant body of guidance on how the department is to effectively provide support to civil authorities in a broad range of circumstances. However, the absence of clarity in roles and responsibilities to address a cyber incident represents a clear gap in guidance. The gap, and the uncertainty that results, could hinder the timeliness or effectiveness of critical DOD support to civil authorities during cyber-related emergencies that DOD must be prepared to provide. In addition to the relevant DOD guidance—such as DOD directives or instructions—that are important for guiding DOD planning and processes, the comprehensive plan DOD is required by Congress to develop in 2016 would be another opportunity for DOD to address the gap that we identified. Whether DOD updates DSCA guidance or issues additional guidance on a separate cyber-technical assistance framework, without clarifying guidance on DOD roles and responsibilities in a cyber incident, DOD cannot reasonably ensure that the department will be able to most effectively employ its capabilities to support civil authorities in a cyber incident.

Recommendation for Executive Action

To help improve DOD's planning and processes for supporting civil authorities in a cyber incident, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Policy in coordination with the Chairman of the Joint Chiefs of Staff to issue or update guidance that clarifies roles and responsibilities for relevant entities and officials—including the DOD components, supported and supporting commands,

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

and dual-status commander—to support civil authorities as needed in a cyber incident.

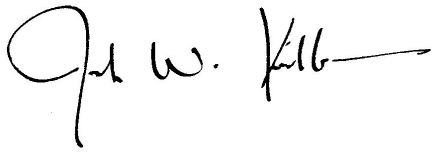
Agency Comments and Our Evaluation

We provided a draft of this report to DOD and the Department of Homeland Security for review and comment. DOD's written comments are reprinted in their entirety in appendix II. DOD also provided technical comments, which we incorporated into the report as appropriate. The Department of Homeland Security did not comment on the report.

DOD concurred with our recommendation that the Secretary of Defense direct the Under Secretary of Defense for Policy in coordination with the Chairman of the Joint Chiefs of Staff to 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. Specifically, DOD stated that it will issue guidance—or update guidance, as appropriate—that will clarify DOD roles and responsibilities regarding civil support for domestic cyber incidents. DOD noted that it will address the supported and supporting command relationships for cyber in joint doctrine such as Joint Publication 3-12(R), *Cyberspace Operations*. DOD also noted that it will issue separate guidance that will address the use of dual-status commanders when supporting civil authorities in response to a cyber incident. We believe that by issuing or updating guidance that clarifies roles and responsibilities for relevant DOD officials, DOD will be in a better position to plan for and support civil authorities in 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: List of Offices GAO Contacted in Its Review

We obtained documents, interviewed officials, or both from the organizations listed below:

Department of Defense	• Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities • Office of the Deputy Assistant Secretary of Defense for Cyber Policy • Joint Staff (Operations Directorate; Strategic Plans and Policies Directorate; and Command, Control, Communications and Computers/Cyber Directorate) • National Guard Bureau • U.S. Northern Command • U.S. Pacific Command • U.S. Cyber Command • U.S. Army Cyber Command • Defense Coordinating Element (Region X)
Department of Homeland Security	• National Cybersecurity and Communication Integration Center • Federal Emergency Management Agency

Appendix II: Comments from the Department of Defense

HOMELAND DEFENSE & GLOBAL SECURITY

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

Mar 14, 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 GA0-16-332, "CIVIL SUPPORT: DoD Needs to Clarify Its Roles and Responsibilities for Domestic Cyber Incidents," dated February 12, 2016 (GAO Code 100147).

Attached is DoD's proposed response to the subject report. My point of contact is CAPT Edward W Devinney II who can be reached at 703-614-5854 or via email at edward.w.devinney.mil@mail.mil.

Sincerely,

Aaron Hughes
Deputy, Assistant Secretary of Defense
Cyber Policy

GAO DRAFT REPORT DATED FEBRUARY 12, 2016
GA0-16-332 (GAO CODE 100147)

"CIVIL SUPPORT: DOD NEEDS TO CLARIFY ITS ROLES AND RESPONSIBILITIES FOR DOMESTIC CYBER INCIDENTS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION: To help improve DOD's planning and processes for supporting civil authorities in a cyber incident, GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Policy in coordination with the Chairman of the Joint Chiefs of Staff to 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.

DoD RESPONSE: Department of Defense concurs with comment with GAO Report 16-332 recommendations and will issue guidance (or update guidance, as appropriate) that clarify DOD roles and responsibilities regarding Civil Support for Domestic Cyber Incidents.

In accordance with DoD practices, supported and supporting command relationships for cyber will be addressed in Joint doctrine such as JP 3-12(R), *Cyberspace Operations.*

The use of dual-status commanders when supporting civil authorities in responses to cyber incidents will be addressed in a separate issuance.

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.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Department of Defense

Page 1

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

2600 DEFENSE PENTAGON

WASHI NGTON, D.C. 20301 -2600

HOMELAND DEFENSE & GLOBAL SECURITY

Mar 14, 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 GA0-16-332, "CIVIL SUPPORT: DoD Needs to Clarify Its Roles and Responsibilities for Domestic Cyber Incidents," dated February 12, 2016 (GAO Code 100147).

Attached is DoD's proposed response to the subject report. My point of contact is CAPT Edward W Devinney II who can be reached at 703-614-5854 or via email at edward.w.devinney.mil@mail.mil.

Sincerely,

Aaron Hughes

Deputy, Assistant Secretary of Defense

Cyber Policy

Page 2

GAO DRAFT REPORT DATED FEBRUARY 12, 2016 GA0-16-332 (GAO CODE 100147)

"CIVIL SUPPORT: DOD NEEDS TO CLARIFY ITS ROLES AND RESPONSIBILITIES FOR DOMESTIC CYBER INCIDENTS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION: To help improve DOD's planning and processes for supporting civil authorities in a cyber incident, GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Policy in coordination with the Chairman of the Joint Chiefs of Staff to 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.

DoD RESPONSE: Department of Defense concurs with comment with GAO Report 16-332 recommendations and will issue guidance (or update guidance, as appropriate) that clarify DOD roles and responsibilities regarding Civil Suppo1i for Domestic Cyber Incidents.

In accordance with DoD practices, supported and supporting command relationships for cyber will be addressed in Joint doctrine such as JP 3-12(R), Cyberspace Operations.

The use of dual-status commanders when supporting civil authorities in responses to cyber incidents will be addressed in a separate issuance.

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

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

Katherine Siggerud, Managing Director, siggerudk@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