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.