September 2016

DEFENSE CIVIL SUPPORT

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

GAO Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

What GAO Found

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

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

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

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

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

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

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