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.	●
A description of such legislative and administrative action as may be necessary to carry out the plan.	●
Descriptions of the roles, responsibilities, and expectations of the active and reserve components of the armed forces.	◐
Plans for coordination with heads of other federal agencies and state and local governments pursuant to the exercises required in the previous clause.[a]	◐
A list of any other exercises previously conducted that are used in the formulation of the plan.	◐
A plan for internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments.	○

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.