August 2017

DEFENSE CYBERSECURITY

DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened

GAO Highlights

Highlights of GAO-17-512, a report to congressional committees

Why GAO Did This Study

DOD acknowledges that malicious cyber intrusions of its networks have negatively affected its information technology systems, and that adversaries are gaining capability over time. In 2010, the President re-designated the director of the NSA as CYBERCOM's commander, establishing a dual-hat leadership arrangement for these agencies with critical cybersecurity responsibilities.

House Reports 114-537 and 114-573 both included provisions for GAO to assess DOD's management of its cybersecurity enterprise. This report, among other things, examines (1) DOD officials' perspectives on the advantages and disadvantages of the dual-hat leadership arrangement of NSA/CSS and CYBERCOM, and actions that could mitigate risks if the leadership arrangement ends, and (2) the extent to which DOD has implemented key strategic cybersecurity guidance. GAO analyzed DOD cybersecurity strategies, guidance, and information and interviewed cognizant DOD officials.

What GAO Recommends

GAO recommends that DOD take the following two actions: (1) modify its criteria for closing tasks from *The DOD Cyber Strategy*; and (2) establish a timeframe and monitoring for implementing an objective of the *DOD Cybersecurity Campaign* to transition to commander-driven operational risk assessments for cybersecurity readiness. DOD partially concurred with these recommendations and identified actions it plans to take. If implemented, GAO believes these actions would satisfy the intent of the recommendations.

View GAO-17-512. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

Officials from Department of Defense (DOD) components identified advantages and disadvantages of the "dual-hat" leadership of the National Security Agency (NSA)/Central Security Service (CSS) and Cyber Command (CYBERCOM) (see table). Also, DOD and congressional committees have identified actions that could mitigate risks associated with ending the dual-hat leadership arrangement, such as formalizing agreements between NSA/CSS and CYBERCOM to ensure continued collaboration, and developing a persistent cyber training environment to provide a realistic, on-demand training capability. As of April 2017, DOD had not determined whether it would end the dual-hat leadership arrangement.

Table: Advantages and Disadvantages of the Dual-Hat Leadership Arrangement, as Reported by Department of Defense (DOD) Officials

Advantages	Disadvantages
Improved coordination and collaboration between NSA/CSS and CYBERCOM	Concern that Cyber Command (CYBERCOM) priorities may receive preference over other commands' priorities with respect to National Security Agency (NSA)/Central Security Service (CSS) support
Faster decision-making	Increased potential of NSA/CSS operations and tools being exposed
Efficiency of resources	Too broad of a span of control that potentially limits effective leadership
	Increases tension between NSA/CSS and CYBERCOM staff who are responsible for military and/or intelligence operation tasks that are not always mutually achievable
	Enables sharing of resources between NSA/CSS and CYBERCOM resulting in resource allocation that is not always easily understood by personnel

Source: GAO analysis of DOD information. | GAO-17-512

DOD's progress in implementing key cybersecurity guidance—the *DOD Cloud Computing Strategy*, *The DOD Cyber Strategy*, and the *DOD Cybersecurity Campaign*—has varied. DOD has implemented the cybersecurity elements of the *DOD Cloud Computing Strategy* and has made progress in implementing *The DOD Cyber Strategy* and *DOD Cybersecurity Campaign*. However, DOD's process for monitoring implementation of *The DOD Cyber Strategy* has resulted in the closure of tasks before they were fully implemented; for example, DOD closed a task that, among other things, would require completing cyber risk assessments on 136 weapon systems. Officials acknowledged they are on track to complete the assessments by December 31, 2019, but as of May 2017, the task was not complete. Unless DOD modifies its process for deciding whether a task identified in its *Cyber Strategy* is implemented, it may not be able to achieve outcomes articulated in the strategy. Also, DOD lacks a timeframe and process for monitoring implementation of the *DOD Cybersecurity Campaign* objective to transition to commander-driven operational risk assessments for cybersecurity readiness. Unless DOD improves the monitoring of its key cyber strategies, it is unknown when DOD will achieve cybersecurity compliance.