November 2022

DOD CYBERSECURITY

Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared

GAO Highlights

Highlights of GAO-23-105084, a report to congressional committees

Why GAO Did This Study

DOD and DIB information technology systems continue to be susceptible to cyber incidents as cybersecurity threats have evolved and become more sophisticated. Federal laws and DOD guidance emphasize the importance of properly reporting and sharing cyber incident information, as both are vital to identifying system weaknesses and improving the security of the systems.

House Report 116-442 included a provision for GAO to review DOD's cyber incident management. This report examines the extent to which DOD established and implemented a process to (1) report and notify leadership of cyber incidents, (2) report and share information about cyber incidents affecting the DIB, and (3) notify affected individuals of a PII breach.

To conduct this work, GAO reviewed relevant guidance, analyzed samples of cyber incident artifacts and cyber incident reports submitted by the DIB and privacy data breaches reported by DOD, and surveyed 24 DOD cyber security service providers. In addition, GAO interviewed officials from DOD and cyber security service providers and convened two discussion groups with DIB companies.

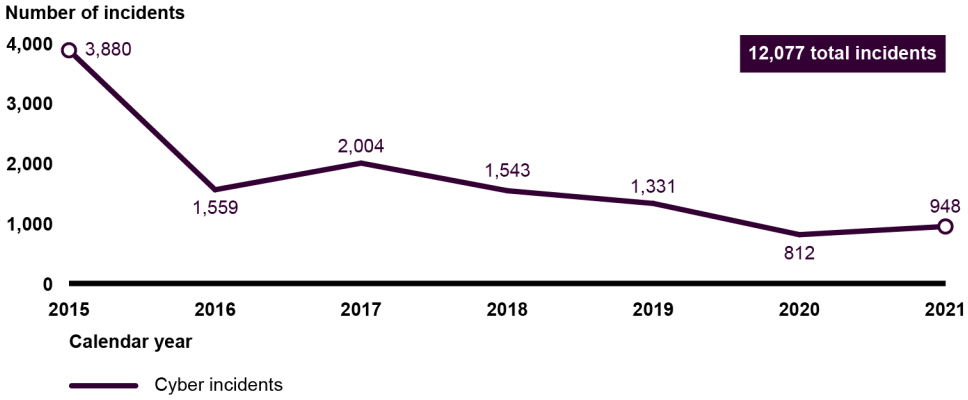
What GAO Recommends

GAO is making six recommendations, including that DOD assign responsibility for ensuring proper incident reporting, improve the sharing of DIB-related cyber incident information, and document when affected individuals are notified of a PII breach. DOD concurred with the recommendations.

View GAO-23-105084. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov or Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

The Department of Defense (DOD) and our nation's defense industrial base (DIB)—which includes entities outside the federal government that provide goods or services critical to meeting U.S. military requirements—are dependent on information systems to carry out their operations. These systems continue to be the target of cyber attacks, as DOD has experienced over 12,000 cyber incidents since 2015 (see figure).To combat these incidents, DOD has established two processes for managing cyber incidents—one for all incidents and one for critical incidents. However, DOD has not fully implemented either of these processes.

Cyber Incidents Reported by Department of Defense's Cyber Security Service Providers from Calendar Years 2015 through 2021



Source: GAO analysis of Department of Defense Joint Incident Management System (JIMS) data. | GAO-23-105084

Despite the reduction in the number of incidents due to DOD efforts, weaknesses in reporting these incidents remain. For example, DOD's system for reporting all incidents often contained incomplete information and DOD could not always demonstrate that they had notified appropriate leadership of relevant critical incidents. The weaknesses in the implementation of the two processes are due to DOD not assigning an organization responsible for ensuring proper incident reporting and compliance with guidance, among other reasons. Until DOD assigns such responsibility, DOD does not have assurance that its leadership has an accurate picture of the department's cybersecurity posture.

In addition, DOD has not yet decided whether DIB cyber incidents detected by cybersecurity service providers should be shared with all relevant stakeholders, according to officials. DOD guidance states that to protect the interests of national security, cyber incidents must be coordinated among and across DOD organizations and outside sources, such as DIB partners. Until DOD examines whether this information should be shared with all relevant parties, there could be lost opportunities to identify system threats and improve system weaknesses.

DOD has established a process for determining whether to notify individuals of a breach of their personally identifiable information (PII). This process includes conducting a risk assessment that considers three factors—the nature and sensitivity of the PII, likelihood of access to and use of the PII, and the type of the breach. However, DOD has not consistently documented the notifications of affected individuals, because officials said notifications are often made verbally or by email and no record is retained. Without documenting the notification, DOD cannot verify that people were informed about the breach.