



November 2022

DOD CYBERSECURITY

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

Accessible Version

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.

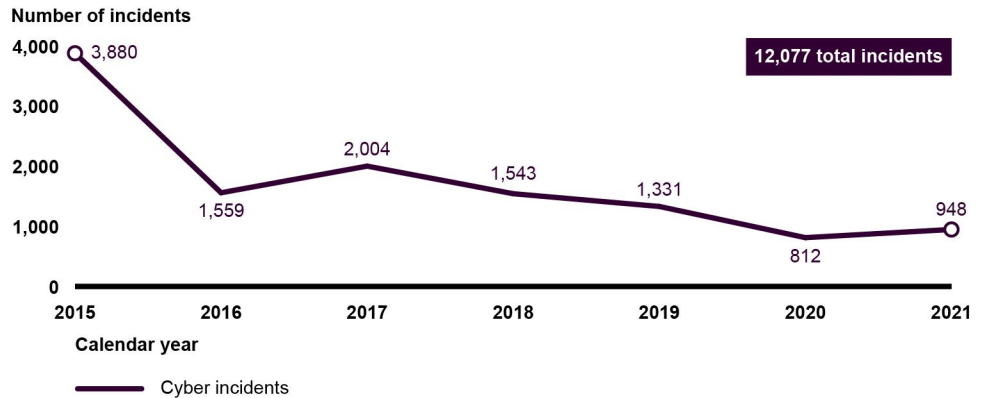
November 2022

DOD CYBERSECURITY

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

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

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

Calendar year	Number of incidents
2015	3880
2016	1559
2017	2002
2018	1543
2019	1331
2020	812
2021	948

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.

Contents

GAO Highlights		ii
	Why GAO Did This Study	ii
	What GAO Recommends	ii
Letter		1
	Background	4
	DOD Established Cyber Incident Reporting and Notification Processes but Has Not Fully Implemented Them	11
	DOD Has Not Fully Established or Implemented Processes to Report and Share Selected Cyber Incidents Affecting the DIB	19
	DOD's Reported Data Breaches of PII Have More Than Doubled since 2015 and DOD's Notification of Affected Individuals Is Unclear	30
	Conclusions	37
	Recommendations for Executive Action	38
	Agency Comments	39
Appendix I: Objectives, Scope, and Methodology		42
Appendix II: Survey of DOD Cybersecurity Service Providers		53
Appendix III: List of DOD's Cybersecurity Service Providers		64
Appendix IV: Comments from the Department of Defense		66
Accessible Text for Appendix IV: Comments from the Department of Defense		70
Appendix V: GAO Contacts and Staff Acknowledgments		72
Tables		
	Table 1: Total Number of Department of Defense Cyber Incidents by Category	11
	Table 2: Survey Respondents' Determination of Accuracy of Joint Incident Management System (JIMS) Elements	61
Figures		
	Figure 1: Cyber Incidents Reported by Department of Defense's Cyber Security Service Providers	10

Accessible Data for Figure 1: Cyber Incidents Reported by Department of Defense’s Cyber Security Service Providers	10
Figure 2: Extent to Which Cyber Incident Reporting Data Fields Required by Department of Defense (DOD) Policy Are Included in the Joint Incident Management System (JIMS)	17
Figure 3: DOD Cyber Crime Center’s (DC3) Mandatory Cyber Incident Handling Process	22
Figure 4: Defense Counterintelligence and Security Agency’s (DCSA) Cyber Incident Handling Process	24
Figure 5: Estimated Response Rates for Defense Industrial Base’s Mandatory Incident Report Key Information, calendar years 2015 through 2021	27
Accessible Data for Figure 5: Estimated Response Rates for Defense Industrial Base’s Mandatory Incident Report Key Information, calendar years 2015 through 2021	27
Figure 6: Data Breaches of PII Reported by DOD in Calendar Years 2015 through 2021	31
Accessible Data for Figure 6: Data Breaches of PII Reported by DOD in Calendar Years 2015 through 2021	31
Figure 7: Process for Reporting Data Breaches of PII and Notifying Affected Individuals	34

Abbreviations

CART	Compliance and Reporting Tool
CIO	Chief Information Officer
CSSP	cyber security service provider
CYBERCOM	U.S. Cyber Command
DC3	Department of Defense Cyber Crime Center
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	defense industrial base
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOD Privacy Office	Defense Privacy, Civil Liberties, and Transparency Division
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act of 2014
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
JIMS	Joint Incident Management System
OMB	Office of Management and Budget
NIST	National Institute of Standards and Technology
PII	personally identifiable information
SIGACT	significant activity report

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



November 14, 2022

Congressional Committees

The Department of Defense (DOD) and our nation's defense industrial base (DIB)¹ are dependent on information systems and electronic data to carry out operations as well as process and report essential information (including controlled unclassified information and personally identifiable information (PII)).² However, the risks to DOD and DIB information systems are increasing as cybersecurity threats evolve and become more sophisticated.

For example, in November and December 2021, Chinese hackers breached five U.S. defense and technology firms. The hackers obtained passwords to access the organizations' systems and intercept sensitive communications. Similarly, between May and July 2019, hackers breached the Defense Information Systems Agency's (DISA) network, potentially compromising personal information, including Social Security numbers. Further, in February 2017, an Iranian hacker group targeted actors associated with the DIB in a campaign to steal credentials and other data. Cyber incidents like these can disrupt critical military

¹The DIB is the worldwide industrial complex that includes the Department of Defense, government, and the private sector with capabilities to perform research and development and design, and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB contains companies such as manufacturers of everything from complex platforms like aircraft carriers to commercial products such as laptops and semiconductors.

²Controlled unclassified information is information the federal government—or an entity on behalf of the federal government—creates or possesses that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, controlled unclassified information does not include classified information or information a non-executive branch entity possesses and maintains in its systems that did not come from, or was not created or possessed by or for an executive branch agency or an entity acting for an agency. PII is any information about an individual maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual such as medical, educational, financial, and employment information.

operations, lead to inappropriate access to and modification of sensitive information, and threaten national security.³

Concerned with the risk to cybersecurity across federal government systems, we initially designated information security as a government-wide high-risk area in 1997—a designation it retains today.⁴ In March 2021, we issued an update to this high-risk area that identified actions needed to address the nation’s cybersecurity challenges, including improving federal response to cyber incidents.⁵

The House Report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2021 included a provision that we review DOD’s cyber incident management efforts.⁶ This report describes the extent to which DOD (1) has established and implemented a process to report and notify leadership of cyber incidents that affect DOD information networks; (2) has established and implemented a process to report and share information about selected DIB cyber incidents; and (3) has experienced data breaches of PII and established and implemented a process to notify affected individuals of the breach.

To address objective one, we identified DOD policies and guidance relevant to the reporting and notification of cyber incidents. We then reviewed Joint Incident Management System (JIMS) information for all the cyber-related incidents reported by 24 DOD organizations that provide cybersecurity services to DOD components (commonly known as cybersecurity service providers, or CSSPs). These incidents were submitted in calendar years 2015 through 2021. The purpose of our

³DOD defines a cyber incident as actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

⁴See GAO, *High-Risk Series: An Overview*, [GAO-HR-97-1](#) (Washington, D.C.: February 1997); *High-Risk Series: Information Management and Technology*, [GAO-HR-97-9](#) (Washington, D.C.: February 1997) and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021). In 2003, we expanded this area to include computerized systems supporting the nation’s critical infrastructure and, in 2015, we further expanded this area to include protecting the privacy of PII.

⁵GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

⁶H.R. Rep. No. 116-442, at 250-251 (2020).

review of the JIMS information was to determine whether the data submitted in JIMS was complete and up-to-date.

We also reviewed a generalizable sample of incidents from eight randomly selected CSSPs to determine whether the steps taken by the CSSPs to report and share cyber incident information and notify leadership aligned with DOD guidance. In addition, we reviewed all significant activity reports submitted by selected CSSPs to determine if CSSPs followed DOD guidance on submitting the reports. We also interviewed the eight selected CSSPs and officials from various DOD components responsible for cyber incident management. In addition, we surveyed 24 CSSPs on how they collect, maintain, and report cyber incident data. We administered the survey from November 5, 2021, to December 21, 2021, and received responses from all 24 DOD CSSPs, for a 100 percent response rate.

To address the second objective, we identified DOD criteria relevant to the reporting and sharing of cyber incidents affecting the DIB, such as the Defense Federal Acquisition Regulation Supplement (DFARS).⁷ We then reviewed DOD Cyber Crime Center (DC3), Defense Counterintelligence Agency (DCSA), and CSSP documented processes and practices and examined whether those processes were fully implemented. We also selected a generalizable sample of incident reports submitted to DC3 to determine the completeness and timeliness of such reports. To supplement our analysis, we convened two group discussions with representatives from DIB companies to obtain their views on reporting cyber incidents to DOD.

To address the third objective, we reviewed DOD, Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) criteria relevant to data breaches of PII. We analyzed a random sample of 152 data breaches reported to the Defense Privacy, Civil Liberties, and Transparency Division's (commonly known as the DOD Privacy Office) Compliance and Reporting Tool (CART) from calendar

⁷Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (December 2019).

years 2015 through 2021.⁸ Finally, we interviewed officials from the DOD Privacy Office regarding the results of our analysis and the reliability of the CART data. A full description of our objectives, scope, and methodology can be found in appendix I and a copy of the survey submitted to CSSPs can be found in appendix II.

We conducted this performance audit from March 2021 to November 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal Law and Guidance Established to Improve Cyber Incident Management Programs

The Federal Information Security Management Act of 2014 (FISMA) requires executive branch agencies to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their operations and assets.⁹ FISMA requires that agency information security programs include procedures for detecting, reporting, and responding to security incidents and that agencies report annually on the total number of information security incidents to OMB and Congress.

FISMA also requires that agency programs include policies and procedures that comply with standards issued by the Director of OMB

⁸We collected raw data on all the data breach forms submitted to CART during calendar years 2017 through 2020 to include the CART data breach form identification number. From this raw data, we selected a sample of 152 breaches and reviewed the corresponding data breach form. DOD Privacy Office officials stated that a CART system error prevented them from accessing the raw data for 2015 and 2016. In addition, at the time of the selection of our sample, data for 2021 was incomplete. As a result, we could not identify the data breach identification numbers for these years and did not review the data breach forms.

⁹*Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283 (2014).

based on standards issued by NIST.¹⁰ NIST has responsibility for developing standards and guidelines, including minimum requirements, for securing the information systems used or operated by a federal agency, contractor of an agency, or other organization on behalf of an agency. NIST has issued special publications that guide agencies, including those for detecting and handling cyber incidents. Specifically, NIST Special Publication 800-61 provides guidance on policies, plans, and procedures for implementing incident response.¹¹ The publication has guidelines for establishing an effective incident response program, including detecting, analyzing, prioritizing, reporting, and handling an incident.

NIST Special Publication 800-53 identifies specific incident response control activities that agencies should address to effectively respond to a cyber incident.¹² These control activities include:

- *Developing incident response policies.* Agencies should develop incident response policies that include information on purpose and scope, roles and responsibilities, coordination among organizational entities, and compliance and policy implementation procedures.
- *Reporting and sharing incident information.* Agencies should establish the types of incidents to report, the content and the timeliness of the reports, and who should receive the report.
- *Tracking and documenting incidents.* Agencies should maintain records about each incident, including documentation of how they addressed the incident and detailed incident information to support analysis.

In addition to information security program requirements, FISMA mandated that federal agencies report to selected congressional

¹⁰OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016), requires federal agencies to implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security, the General Services Administration, and the Office of Personnel Management which includes applying the standards and guidelines contained in the NIST Federal Information Processing Standards and NIST Special Publications (e.g., 800 series guidelines).

¹¹NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, Revision 2 (August 2012).

¹²NIST Special Publication 800-53, *Recommended Security and Privacy Controls for Information Systems and Organizations*, Revision 5 (September 2020).

committees on each major information security incident involving a data breach of PII as defined by the Director of OMB. FISMA also required OMB to issue and periodically update data breach notification policies and guidelines. To that end, OMB Memorandum M-17-12 set forth the policy for federal agencies to prepare for and respond to a data breach of PII and included a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach.¹³ The memorandum also included guidance on whether and how to provide notification and services to those individuals.

DOD Has Established Various Policies and Guidance for Cyber Incident Management and Reporting

DOD has established policies and guidance governing the management and reporting of cyber incidents to include:

- **Department of Defense Instruction 8500.01, Cybersecurity.** This instruction assigns the Commander of U.S. Cyber Command (CYBERCOM) the responsibility to direct and coordinate Department of Defense network (DODIN) operations and defense in accordance with the Unified Command Plan.¹⁴ In addition, the order provides that CYBERCOM and Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) coordinate all defensive actions that affect more than one DOD component or have impacts outside the realm of the network owner. It notes that such actions are under the direction of the Commander of CYBERCOM and conducted as described in CYBERCOM orders or other directives. The instruction also assigns the Director of DISA responsibility for developing, implementing, and in coordination with the Commander of CYBERCOM, managing cybersecurity for the department's network.
- **Department of Defense Instruction 8010.01, Department of Defense Information Network (DODIN) Transport.** This instruction states that the Director of DISA serves as the Commander of JFHQ-DODIN to command and control, plan, direct, coordinate, integrate,

¹³OMB, Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017).

¹⁴Department of Defense Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014) (incorporating Change 1, Oct. 7, 2019).

and synchronize DODIN operations and DOD defensive cyberspace operations.¹⁵

- **Department of Defense Instruction 8530.01, Cybersecurity Activities Support to DOD Information Network Operations.** This instruction requires components to implement cyber incident handling programs.¹⁶ These programs should include a capability to analyze and respond to incidents. In addition, the instruction states that cyber incident handling programs should be able to collect and distribute incident information through a joint incident management system.
- **Chairman of the Joint Chiefs of Staff Manual 6510.01B, Cyber Incident Handling Program.** This manual establishes guidance for reporting cybersecurity incidents.¹⁷ In addition, it includes specific staff roles, responsibilities, and procedures for incident reporting. The procedures include time frames for reporting incidents, required data for each incident, and methods for incident reporting. The manual also designates the Joint Incident Management System (JIMS) as the official system for recording all cyber incidents in DOD. JIMS is then to be used to report these incidents to the appropriate individuals and components and to serve as a tool for enterprise-wide visibility of cyber incident reporting. The information in JIMS is also to be used to help shape tactical, strategic, and military strategies for response. The manual assigns CSSPs with responsibility for monitoring, detecting, analyzing, and responding to cyber incidents.¹⁸
- **Operation Gladiator Shield 2017.** This order describes JFHQ-DODIN's responsibilities for defensive cyber operations.¹⁹ The order also requires DOD components to submit significant activity (SIGACT)

¹⁵DOD Instruction 8010.01, *Department of Defense Information Network (DODIN) Transport* (Sept. 10, 2018).

¹⁶DOD Instruction 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (Mar. 7, 2016) (incorporating change 1, July 25, 2017).

¹⁷Chairman of the Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program* (July 10, 2012). In this report, we refer to this document as the Cyber Incident Handling Program Manual.

¹⁸The manual uses the term Cybersecurity Network Defense Service Providers. However, subsequent guidance, such as Department of Defense Instruction 8530.01, uses the term cyber security service provider, or CSSP. According to DOD officials, the terms are equivalent. For the purposes of this report, we use CSSP.

¹⁹JFHQ-DODIN, *Operation Gladiator Shield 2017* (June 30, 2017).

reports to provide information on enemy, suspected enemy, and anomalous activity on DOD networks.

- **US Cyber Command Operation Order, Required Use of the Joint Incident Management System.** The order designates JIMS as the official, authoritative repository for reports of cyberspace incidents of malicious or adversarial activities against DOD.²⁰ The order also requires all DOD entities to use JIMS as the official database to report cyber incidents.
- **Deputy Secretary of Defense Memorandum, Defense Industrial Base Cyber Incident Notification Process.** This policy memorandum designated DOD's Cyber Crime Center (DC3) as the focal point for receiving all initial DIB cyber incident reports.²¹ It requires DC3 and the Defense Counterintelligence Agency (DCSA) to share DIB cyber incident reports with relevant stakeholders and to notify DOD senior leadership of certain DIB cyber incidents.²² These include incidents involving significant loss of controlled unclassified information from a cleared defense contractor; significant loss of PII of civilian or service members; and detection of a new threat or emerging tactic, technique, or procedure, among other categories.
- **DFARS Safeguarding Covered Defense Information and Cyber Incident Reporting.** The DFARS includes a clause requiring DOD contractors to provide adequate security for covered defense information²³ that is processed, stored, or transmitted on an unclassified information system that is owned or operated by or for a

²⁰U.S. Cyber Command, Operation Order 18-0103, *Required Use of the Joint Incident Management System (JIMS)*.

²¹Deputy Secretary of Defense Memorandum, *Defense Industrial Base Cyber Incident Notification Process* (May 6, 2019). (FOUO)

²²Per the memorandum, DCSA is to notify DC3 and the Under Secretary of Defense for Intelligence & Security.

²³Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies and is 1) marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or 2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

contractor and to rapidly report cyber incidents.²⁴ It requires, among other things, that when a DOD contractor discovers a cyber incident that affects defense information or the contractor's ability to perform operationally critical contract requirements, the contractor is to report the cyber incident to DOD within 72 hours. It also provides the required elements that are to be included in such cyber incident reports.

- **DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan.** This plan establishes requirements for addressing data breaches involving PII.²⁵ Specifically, the plan establishes roles, responsibilities, and procedures for reporting data breaches. In addition, the plan provides guidance for assessing the risk of harm for individuals affected by a breach and indicates that when a determination has been made that it is necessary to notify individuals potentially affected by a breach, DOD should notify as expeditiously as practicable and without unreasonable delay.

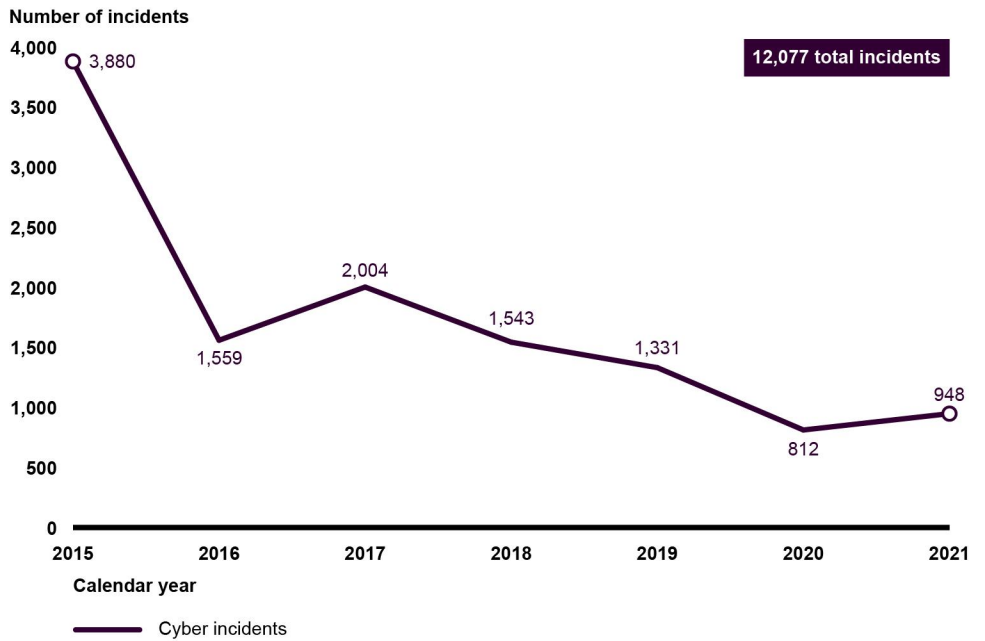
DOD Has Reported Over 12,000 Cyber Incidents in Calendar Years 2015 through 2021

According to data in JIMS, DOD CSSPs reported 12,077 cyber incidents affecting their networks from calendar years 2015 through 2021. Over this period, the incidents reported by CSSPs declined from a high of 3,880 in 2015 to 948 in 2021 (see figure 1). According to JFHQ-DODIN and DOD CIO officials, the reduction in cyber incidents can be attributed to an increase in the department's deployment of defense mechanisms during this time period.

²⁴Defense Federal Acquisition Regulation Supplement section 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (December 2019).

²⁵DOD Manual 5400.11, *DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan*, Volume 2 (May 6, 2021).

Figure 1: Cyber Incidents Reported by Department of Defense's Cyber Security Service Providers



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

Accessible Data for Figure 1: Cyber Incidents Reported by Department of Defense's Cyber Security Service Providers

Calendar year	Number of incidents
2015	3880
2016	1559
2017	2002
2018	1543
2019	1331
2020	812
2021	948

CSSPs are to report cyber incidents in JIMS using one of the following four categories:

- **Root-level intrusion:** Unauthorized privileged access to an information system. Privileged access, often referred to as administrative or root access, provides unrestricted access to the information system.

- **User-level intrusion:** Unauthorized non-privileged access to an information system. Non-privileged access, often referred to as user-level access, provides restricted access to the information system based on the privileges granted to the user.
- **Denial of service:** An activity that denies, degrades, or disrupts the normal functionality of a system or DOD information network.
- **Malicious logic:** The installation of software designed and/or deployed by adversaries with malicious intentions for gaining access to resources or information without the consent or knowledge of the user.

Malicious logic incidents make up the vast majority of the cyber incidents reported in JIMS from calendar years 2015 through 2021, as shown in table 1. Other categories of incidents are rarely identified and reported. Specific details of the cyber incidents and the affected DOD components are classified and do not appear in this report.

Table 1: Total Number of Department of Defense Cyber Incidents by Category

Calendar year	Root-level intrusion	User-level intrusion	Denial of service	Malicious logic
2015	15	23	35	3,681
2016	64	11	14	1,466
2017	2	12	17	1,968
2018	2	2	10	1,518
2019	4	3	14	1,302
2020	7	7	6	785
2021	6	7	3	924
Total	100 (0.84 percent)	65 (0.55 percent)	99 (0.83 percent)	11,644 (97.78 percent)

Source: GAO analysis of Joint Incident Management System Data. | GAO-23-105084

Note: We omitted 169 of the 12,077 incidents because the information related to these incidents did not meet our data reliability standards. Specifically, officials at one cybersecurity service provider (CSSP) said they did not have quality control standards, and six CSSPs did not consistently finalize incident reports. More information on this issue can be found in appendix I.

DOD Established Cyber Incident Reporting and Notification Processes but Has Not Fully Implemented Them

DOD established two processes for reporting cyber incidents occurring on its information network and notifying department leadership. One process—the cyber incident management process for all cyber

incidents—requires CSSPs, acting on behalf of their components, to report all cyber incidents into a central repository known as JIMS and to notify appropriate leadership. In the other process—an operational reporting process which we refer to as the critical cyber incident management process—CSSPs report critical cyber incidents in the format of a significant activity report (SIGACT), used to notify commanders at all levels.²⁶ However, the department has not fully implemented either process.

DOD Established Two Processes to Report Cyber Incidents on Its Information Network and to Notify the Appropriate Leadership

Cyber Incident Management Process for All Cyber Incidents

The Cyber Incident Handling Program Manual established JIMS as the central repository for reporting all cyber-related incident reports and assigned CSSPs the primary responsibility for identifying an incident, reporting incident data into JIMS, and updating JIMS as the incident is investigated.²⁷ The manual states that incidents should be reported in JIMS within 6 to 24 hours of incident discovery. The manual identifies 46 data fields required for reporting a cyber incident in JIMS. For example, the manual requires CSSPs to identify the:

- **Delivery vector**, which indicates the primary path or method used by the adversary to cause the incident or event to occur (e.g., social engineering, software flaw, or authorized user). The delivery vector information can be used to identify trends in the prevalence of various vectors. By understanding the most prevalent vectors, tactical and strategic plans can be developed to improve the defensive posture of DOD networks.
- **Operational impact**, which indicates whether the incident has had a detrimental impact on an organization's ability to perform its mission.

²⁶DOD uses SIGACTs for incidents related to enemy activity, potential enemy activity, or anomalous activity on the department's information networks. For the purposes of this report, we refer to these as critical incidents.

²⁷The manual uses the term Cybersecurity Network Defense Service Providers instead of CSSP. According to DOD officials, the terms are equivalent. For consistency, we use CSSP.

Identifying operational impact determines whether appropriate leadership or which organizational level needs to be notified.²⁸

The manual requires incident reports to be reviewed and updated to maintain situational awareness since each update provides a more comprehensive understanding of the incident. The manual also recognizes that the operational reporting channel is designed to notify commanders at all levels of the ability of their information systems to support operations and the operational impact of any reported incidents.²⁹

Critical Cyber Incident Management Process

In addition to the process of reporting cyber incidents in JIMS, JFHQ-DODIN specified a second operational reporting requirement using SIGACTs³⁰ in June 2017 for critical incidents.³¹ According to a JFHQ-DODIN order titled *Operation Gladiator Shield 2017*, DOD components—and CSSPs acting on their behalf—are required to submit SIGACT reports to provide information on critical incidents.³² The reports are to include information about the status of the affected systems and

²⁸DOD organizational levels are divided into tiers for its cyber incident handling program. The first tier consists of entities that direct and coordinate incident handling, such as CYBERCOM and JFHQ-DODIN. The second tier, consisting of DOD components and CSSPs, implements the cyber incident handling program.

²⁹According to the Cyber Incident Handling Program Manual, operational impact may include direct and/or indirect effects that diminish or incapacitate information system or information network capabilities, the compromise and/or loss of DOD data, or the temporary or permanent loss of mission-critical applications or information systems.

³⁰*Operation Gladiator Shield 2017* also refers to SIGACT reports as “red reports.” For the purposes of this report, we use only the term SIGACT throughout.

³¹JFHQ-DODIN, *Operation Gladiator Shield 2017* (June 30, 2017). JFHQ-DODIN is responsible for, among other things, command and control, planning, directing, coordinating, integrating, and synchronizing DOD defensive cybersecurity operations. These responsibilities include directing and coordinating the department and components’ response to cyber incidents. JFHQ-DODIN also maintains a portal for the submission of SIGACTs.

³²Examples of critical incidents include DODIN outages or degradations, escalation of privileges, data exfiltration, and evidence of malware.

networks, and the potential effects of incidents.³³ JFHQ-DODIN analyzes and aggregates the information in SIGACTs to determine trends and enable timely regional global responses.

³³JFHQ-DODIN, *Operation Gladiator Shield 2017* (June 30, 2017) was issued to organize the DODIN for sustained conflict because it is a high value target that has been infiltrated and attacked. The Commander, JFHQ-DODIN subdivides the DODIN into areas of operation, which correspond to the authorities vested in DOD component leaders to conduct DODIN Operations and Defensive Cyberspace Operations-Internal Defensive Measures within their organizations. As areas of operation commanders and directors, these leaders establish their areas of operation boundaries based on responsibility for and ownership of the information systems, networks, applications/software, and data within their organizations.

DOD Had Not Fully Implemented the Two Cyber Incident Management Processes

DOD Lacks an Accountable Organization and Consistent Guidance to Ensure Complete and Updated Reporting of All Cyber Incidents

DOD had not fully implemented the cyber incident management process for cyber incidents, as incident reports in JIMS were often incomplete and not always updated. Specifically, CSSPs did not include all information required by the Cyber Incident Handling Program Manual. For example, from the JIMS cyber incident reports submitted in calendar years 2015 through 2021,

- 91 percent did not include information on the discovery date of the incident, hindering DOD's ability to determine whether incidents were reported in JIMS in a timely manner.
- 68 percent did not include information on an incident's delivery vector, limiting DOD's ability to identify trends in the prevalence of various threats affecting its networks.

In addition to incomplete incident information, CSSPs also did not consistently notify DOD leadership of incidents that had a detrimental impact on DOD's ability to perform its mission or availability of its networks. Specifically, CSSPs did not have evidence that they notified the appropriate leadership for an estimated 47 percent of the incidents they reported in calendar years 2015 through 2020.³⁴ With respect to the identification of operational impact and notification of leadership, when operational impact was determined, evidence of notification of leadership was shown in an estimated 81 percent of the cyber incidents. When operational impact was not determined, we estimate that 60 percent of incidents lacked evidence that leadership was appropriately notified of the incidents.

CSSPs also did not always update incident reports as required by the Cyber Incident Handling Program Manual, which states that initial incident reports should be updated throughout the incident lifecycle as further analysis and information become available. Three of the 24 CSSPs responding to our survey reported they did not regularly update and close cyber incidents in JIMS with finalized information once an incident had

³⁴The margin of error for this estimate at a 95 percent confidence interval is plus or minus 10 percentage points.

been resolved. In addition, one CSSP reported in our survey that it did not have quality assurance procedures for entering or updating information related to the cyber incident reports in JIMS. Further, two other CSSPs, which entered 69 percent of the incidents in JIMS, reported in our survey that they did not provide any information into JIMS until the incidents had been resolved—indicating that the CSSPs were not making regular updates into JIMS.

Two primary reasons may explain these outcomes. First, DOD has not clearly assigned an organization responsible for ensuring that DOD components—and CSSPs acting on their behalf—follow policy and guidance. Specifically, the officials in organizations with roles and responsibilities for cyber incident management said they were not responsible for overseeing cyber incident reporting and compliance. For example,

- CYBERCOM and DISA officials said they were not responsible for ensuring the completeness of information submitted to JIMS.
- JFHQ-DODIN officials said they focus on cyber incident response at the operational level and do not have the capacity or the responsibility to review incidents reported in JIMS and ensure that all required information is included. The officials also noted that JFHQ-DODIN did not have the authority to direct the CSSPs to ensure data quality since CSSPs report to their respective components. Although a CYBERCOM operation order tasked JFHQ-DODIN with the responsibility to ensure that all reportable cyber incidents are populated in JIMS, the order does not assign any responsibility for ensuring the completeness and currency of incident information.³⁵ In addition, JFHQ-DODIN officials stated that they do not use JIMS for cyber-related incident management.

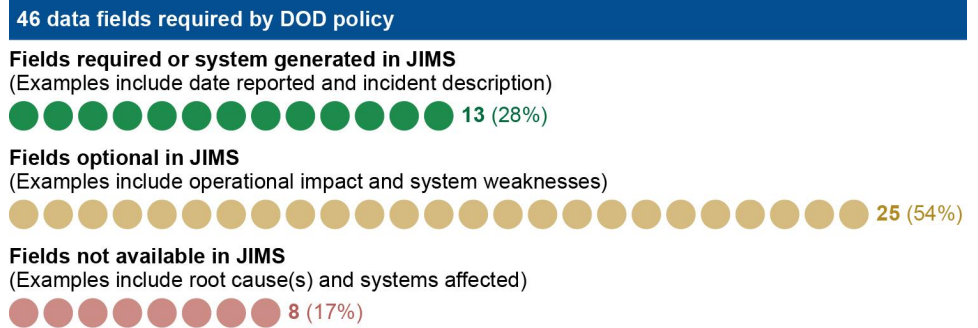
Until DOD assigns responsibility for ensuring complete and updated incident reporting and proper leadership notification, the department will not have assurance that its leadership has an accurate picture of its posture. As a result, the department may miss opportunities to assess threats and weaknesses, gather intelligence, support commanders, and share information. Further, until DOD improves the reporting of cyber incidents, DOD will be limited in its ability to achieve the department's

³⁵U.S. Cyber Command, *Operation Order 18-0103, Required Use of the Joint Incident Management System (JIMS)*, (June 20, 2018).

goals and policy for enabling cyberspace accountability of DOD components and information systems.³⁶

Second, differences between the reporting requirements in DOD guidance and the required data fields in JIMS to enter a cyber incident has resulted in the lack of complete reporting. As previously discussed, the Cyber Incident Handling Program Manual requires 46 different data fields for reporting a cyber incident. However, JIMS does not allow or require users to provide all of the information called for by the manual. For example, JIMS requires users to include information on 13 of the 46 data fields required by guidance. However, the remaining fields are either optional fields or are not available fields in the system (see figure 2).

Figure 2: Extent to Which Cyber Incident Reporting Data Fields Required by Department of Defense (DOD) Policy Are Included in the Joint Incident Management System (JIMS)



Source: GAO analysis of DOD guidance and JIMS data. | GAO-23-105084

DOD officials acknowledged that JIMS has limitations and they are considering implementing a new solution to address those limitations. Until DOD updates JIMS or identifies a new technological solution in which policy and system requirements align, the department will continue to lack complete incident information. Without this information, DOD will not have department-wide visibility of all cyber incidents, hindering its ability to mitigate the harm of current and future incidents.

³⁶DOD Directive-type Memorandum (DTM) 20-004, *Enabling Cyberspace Accountability of DOD Components and Information Systems*, (Nov. 13, 2020). Among other things, this directive-type memorandum establishes policy, assigns responsibilities, provides supplementary policy guidance, and prescribes procedures enabling cyberspace accountability within DOD to address risks assumed by commanders and directors in the cyberspace area of operations.

DOD Guidance Lacks Detailed Procedures for Determining Critical Cyber Incidents

DOD also had not fully implemented the critical cyber incident management process due to a lack of detailed procedures for determining which incidents are critical. Specifically, from the sample of eight selected CSSPs, we identified 30 cyber incidents comprised of intrusions or denials of service.³⁷ We selected these incidents because CSSPs identified them as possibly related to enemy activity, potential enemy activity, or anomalous activity on the department's information networks—critical incidents that should have an associated SIGACT report.³⁸ However, the DOD components—or CSSPs acting on their behalf—did not develop SIGACT reports for 29 of these incidents (97 percent).³⁹

A key reason DOD had not fully implemented the critical cyber incident management process is because the Cyber Incident Handling Program Manual lacks detailed procedures for operational reporting that are described in the Operation Gladiator Shield order. For example, the manual has guidance for some operational reporting but does not describe procedures for using the SIGACT process for critical incidents.⁴⁰ CSSP officials agreed and stated that clearer guidance would be useful so they could understand what does and does not need to be reported through SIGACTs. Until DOD ensures that its components have procedures on when and how CSSPs are to use SIGACTs, the department lacks assurance that commanders and others responsible for directing incident response strategies will be fully informed about the potential effect of critical incidents on their missions.

Officials representing DOD's Office of the Chief Information Officer (CIO), JFHQ-DODIN, and CYBERCOM identified actions DOD has initiated or is planning to take to improve the department's cyber incident management efforts. According to these officials, DOD is updating one of its

³⁷We selected eight CSSPs for detailed analysis of the incidents they reported in JIMS.

³⁸According to *Operation Gladiator Shield 2017*, SIGACT reports provide information on enemy, suspected enemy, and anomalous activity on the DOD information network.

³⁹The incidents occurred between July 2017—after JFHQ-DODIN issued the *Operation Gladiator Shield 2017* order, including SIGACT reporting guidance—and December 2020.

⁴⁰The Cyber Incident Handling Program Manual was issued 5 years before the issuance of the Operation Gladiator Shield order.

instructions related to cybersecurity that is expected to include updated guidance on reporting incidents.

Once DOD issues this instruction, CYBERCOM officials said they plan to finalize and issue a policy that provides more specific guidance, such as minimum mandatory reporting information, that could improve DOD cyber incident management by clarifying and aligning reporting requirements in JIMS and operational reports or SIGACTs. DOD officials stated that they plan to issue this policy in 2022. Once DOD issues the new instruction and related policy documents, the department plans to decide on an updated technological solution to improve cyber incident reporting currently provided by JIMS.

While officials believe the updated instruction and additional policy will provide the foundation for improvements, they said DOD has not finalized either document. Thus, it is unclear whether the planned documents and any resulting technological solutions will directly address the weaknesses in cyber incident reporting and notification we identified. Until DOD provides the additional guidance and technological solutions, it will be hampered in its efforts to report, share information on, and respond to incidents.

DOD Has Not Fully Established or Implemented Processes to Report and Share Selected Cyber Incidents Affecting the DIB

DOD has established processes for how DC3 and DCSA will report and share selected DIB cyber incidents. However, the department has not done so for CSSPs. In addition, the department has not fully implemented these various processes, as DIB companies often submitted information that was not comprehensive or timely.

DOD Has Not Fully Established Processes for Reporting and Sharing Cyber Incident Information Affecting the DIB

DOD has established processes for DC3 and DCSA to report and share selected cyber incidents affecting the DIB but has not done so for CSSPs. Regarding the DC3 process, a DFARS clause requires DOD contractors—also referred to as DIB contractors—to report cyber incidents affecting covered defense information or contractors' ability to

perform operationally critical contract requirements to DC3.⁴¹ DIB contractors are to report these incidents within 3 days of discovery via a web-based submission portal. According to the clause, DIB contractors are to submit incident reports for cyber incidents that affect:

- covered defense information on covered contractor information systems,
- a covered contractor information system, or
- a contractor's ability to perform contract requirements designated as operationally critical support and identified in the contract.

DOD requires DIB contractors to include certain information in their incident reports. This information includes, among other things:

- impact to covered defense information;
- incident outcome;
- DOD programs, platforms, or systems involved; and
- contract information or a U.S. government point of contact.

In May 2019, the Deputy Secretary of Defense issued a *Defense Industrial Base Cyber Incident Notification Process* memorandum outlining an updated notification process.⁴² The memorandum was issued in response to weaknesses in the department's process for notifying the appropriate stakeholders of cyber incidents involving the DIB. It states that the Secretary of Defense and the Chairman of the Joint Chiefs of

⁴¹DFARS section 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (December 2019). A covered contractor information system is an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

⁴²Deputy Secretary of Defense Memorandum, *Defense Industrial Base Cyber Incident Notification Process* (May 6, 2019) (Unclassified//FOUO). We refer to this as the 2019 Deputy Secretary of Defense memorandum.

Staff shall be notified of all cyber incidents involving the DIB that require congressional notification.⁴³ Those types of incidents include

- any compromise of classified information likely to cause significant harm or damage to the national security interests of the U.S.;
- determination of a significant loss of controlled unclassified information from a cleared defense contractor;⁴⁴
- significant loss of PII of civilian or uniformed members of the armed forces; and
- congressional reporting requirements.

The memorandum also states that other DOD senior leaders are to be notified in a timely manner of all cyber incidents involving the DIB that meet the following criteria, among others

- cyber incidents being reported to the Secretary of Defense;
- determination of a significant loss of controlled unclassified information from an uncleared defense contractor; and
- detection of a new threat or emerging tactic, technique, or procedure.

DC3 is to receive two types of reports from DIB companies—mandatory and voluntary. Mandatory reports are those submitted in accordance with the DFARS requirements previously described. Voluntary reports are those that detail cyber activity that does not meet the reporting requirements for mandatory reports. DC3 developed detailed standard operating procedures for handling mandatory reports.

Per the 2019 Deputy Secretary of Defense memorandum, DC3 is required to document all reported incidents in a SECRET-level information repository hosted on DOD's SECRET Internet Protocol

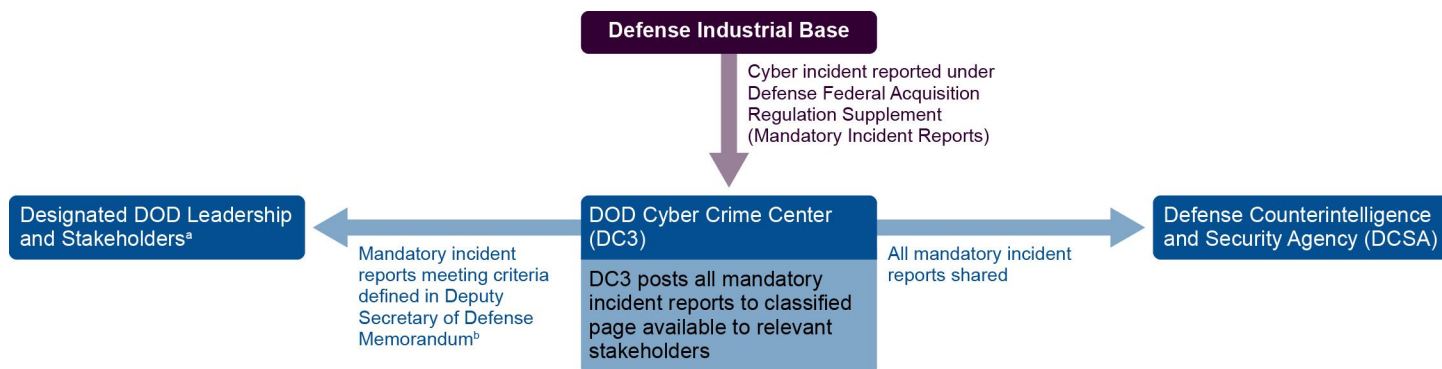
⁴³The 2019 Deputy Secretary of Defense memorandum includes responsibilities for multiple DOD entities, including DC3, DCSA, military department counterintelligence organizations, and the National Joint Operations and Intelligence Center, among others. For the purpose of this review, we examined DC3 and DCSA; however, these are not the only DOD entities that may learn of and share information related to cyber incidents affecting the DIB. For example, similar to DCSA, military department counterintelligence organizations are also directed to notify DC3 of DIB cyber incidents involving controlled unclassified information or unclassified information systems.

⁴⁴A cleared defense contractor is an organization granted clearance by DOD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the DOD.

Router Network, commonly known as SIPRNet.⁴⁵ DC3 is also required to forward the cyber incident report to various stakeholders. On an annual basis, DC3 is to develop an aggregated report detailing all known exfiltration incidents and post the report to SIPRNet.⁴⁶

When DC3 becomes aware of a cyber incident that meets the criteria of the 2019 memorandum (described above), the office is to submit a cyber incident notification to various DOD designated leadership and stakeholders within 3 business days of the discovery of the incident. For DC3, designated leadership and stakeholders include DCSA, the Under Secretary of Defense for Intelligence and Security, and the DOD CIO, depending on whether the cyber incident meets certain criteria. Figure 3 depicts DC3’s process for handling mandatory cyber incident reports.

Figure 3: DOD Cyber Crime Center’s (DC3) Mandatory Cyber Incident Handling Process



Source: GAO analysis of Department of Defense (DOD) information. | GAO-23-105084

^aThe Deputy Secretary of Defense Memorandum, Defense Industrial Base Cyber Incident Notification Process, requires designated leadership and stakeholders to be notified of cyber incidents that meet certain criteria. These criteria include incidents involving significant loss of controlled unclassified information from a defense contractor; significant loss of personally identifiable information of civilian or uniformed service members; and detection of a new threat or emerging tactic, technique, or procedure.

^bDesignated leadership and stakeholders include the Department of Defense Chief Information Officer, Under Secretary of Defense for Intelligence and Security, and Defense Counterintelligence and Security Agency, depending on whether the cyber incident meets certain criteria.

DIB contractors are also required to notify DCSA directly of certain incidents that they discover. Specifically, part 117 of title 32 of the Code

⁴⁵SIPRNet is a global network used to transmit secret data in support of homeland security activities.

⁴⁶An exfiltration incident is the removal of information from a network via cyber-enabled means.

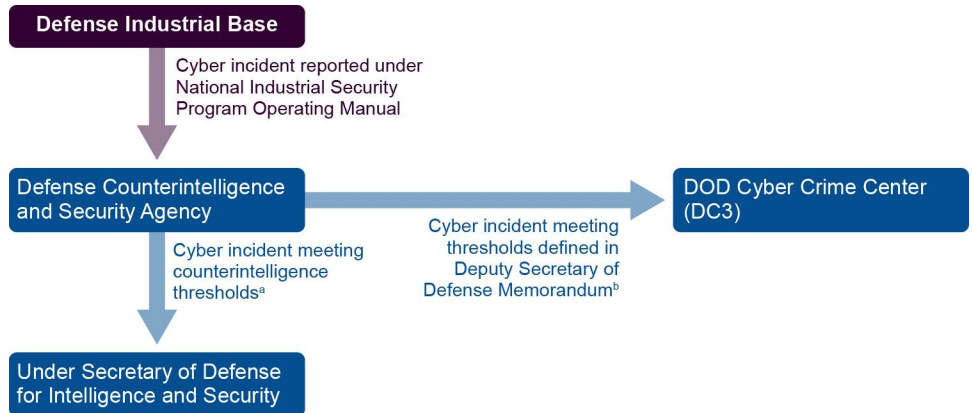
of Federal Regulations requires DIB contractors that DOD has approved to handle classified information to promptly report to the cognizant security agency about additional activities.⁴⁷ These activities include actual, probable, or possible espionage or sabotage, whether on a classified or unclassified information system.

The 2019 Deputy Secretary of Defense memorandum requires the Defense Security Service, later renamed DCSA, to notify DC3 of any cyber incidents that it becomes aware of involving controlled unclassified information or affecting unclassified information systems. DCSA is also required to notify the Under Secretary of Defense for Intelligence and Security of all cyber incidents related to counterintelligence affecting the DIB.

In April 2022, DCSA issued standard operating procedures for sharing information and notifying leadership. Specifically, the procedures require any DCSA employee who receives notification of a cyber incident to notify the DCSA Cyber Mission Center, among other key stakeholders, within 12 business hours of the notification. The center is then responsible for notifying DC3 and the Office of the Under Secretary of Defense for Intelligence and Security within 12 business hours of the center's notification. Because of this action, DCSA should be better positioned to share all relevant DIB-related cyber incident reports with stakeholders and leadership. Figure 4 depicts DCSA's process for handling cyber incident reports.

⁴⁷32 C.F.R. § 117.8, *National Industrial Security Program Operating Manual*, (July 1, 2021). DCSA serves as the organizational unit that administers industrial security services on behalf of the DOD cognizant security agency, the Under Secretary of Defense for Intelligence and Security.

Figure 4: Defense Counterintelligence and Security Agency’s (DCSA) Cyber Incident Handling Process



Source: GAO analysis of Department of Defense (DOD) information. | GAO-23-105084

^aAccording to the Deputy Secretary of Defense Memorandum, Defense Industrial Base Cyber Incident Notification Process, DCSA is to notify DC3 of any cyber incidents they become aware of involving controlled unclassified information or affecting unclassified information systems.

^bDCSA is to notify the Under Secretary of Defense for Intelligence and Security of cyber incidents affecting the defense industrial base that meet certain counterintelligence thresholds, such as counterintelligence failures relating to any defense operation, system, or technology of the United States that will likely cause significant harm or damage to the national security interests.

DOD fully established processes for DC3 and DCSA to share DIB-related incidents with relevant stakeholders, but it has not fully done so for CSSPs. According to officials, CSSPs are responsible for monitoring DIB connections to the DOD information network and handling incidents on those connections.⁴⁸ If a CSSP detects an incident on a DIB connection, it would use the same processes we previously described to report and share information on DOD cyber incidents—using JIMS and SIGACTs, if applicable. However, these processes do not include DC3 or DCSA. As a result, DC3 and DCSA may not be aware of all of the cyber-related incidents that affect the DIB.

DC3 and DCSA officials confirmed that they do not receive information from CSSPs regarding DIB-related cyber incidents. Additionally, the DC3 officials said they were not aware that DIB-related cyber incidents were reported by CSSPs via the JIMS and SIGACT channels. DC3 officials said that receiving DIB-related cyber incidents through these channels may support their mission. However, because they did not know what

⁴⁸DOD may approve DIB contractors to maintain networks connected to the DOD information network. According to DOD officials, the department considers these connections federal networks.

information is reported through these channels, they could not definitively state whether the information would be useful.

The Cyber Incident Handling Program Manual 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. However, DOD has not determined whether the CSSP-identified incidents regarding the DIB should be shared across the enterprise, according to officials. Until DOD examines whether information on DIB-related cyber incidents handled by CSSPs is relevant to the missions of other DOD components, including DC3 and DCSA, and takes action to identify when and with whom that information should be shared, these entities may not have all the information needed to alert relevant stakeholders of cyber incidents that may affect them.

DOD Has Not Fully Implemented the Processes to Report and Share Information on Cyber Incidents Affecting the DIB

DC3 followed its established process for receiving and notifying stakeholders of DIB-related cyber incidents. However, DIB companies did not always submit reports to DC3 with complete information or in a timely manner. The DCSA process, which was established in April 2022, was too new for us to evaluate, and DOD has not yet established a CSSP process, as previously mentioned.

As part of its established process to report and share information on DIB-related cyber incidents, DC3 received over 1,500 mandatory incident reports from calendar years 2015 through 2021.⁴⁹ For cyber incidents that met the criteria described in the 2019 Deputy Secretary of Defense memorandum, DC3 notified designated DOD leadership and other DOD stakeholders as appropriate and posted records of these notifications on

⁴⁹The mandatory reporting requirement began in 2015, and DIB organizations began submitting reports in September 2015. DIB organizations also submitted 4,371 voluntary reports from calendar years 2015 through 2021. Prior to 2015, the DFARS clause included a cyber incident reporting requirement. However, it covered only the protection of and reporting of incidents affecting controlled technical information and not other incidents within the contractor system. The version issued in 2015 expanded the protection and reporting to entire contractor systems and to covered defense information, which included controlled technical information as a subset. See 80 Fed. Reg. 51,739 (Aug. 26, 2015).

SIPRNet.⁵⁰ Further, as per the memorandum, DC3 posted mandatory incident reports on SIPRNet—accessible to all relevant stakeholders—and provided copies to DCSA. Finally, DC3 developed an aggregated report detailing all mandatory and voluntary reports and posted it to SIPRNet and to an unclassified site.

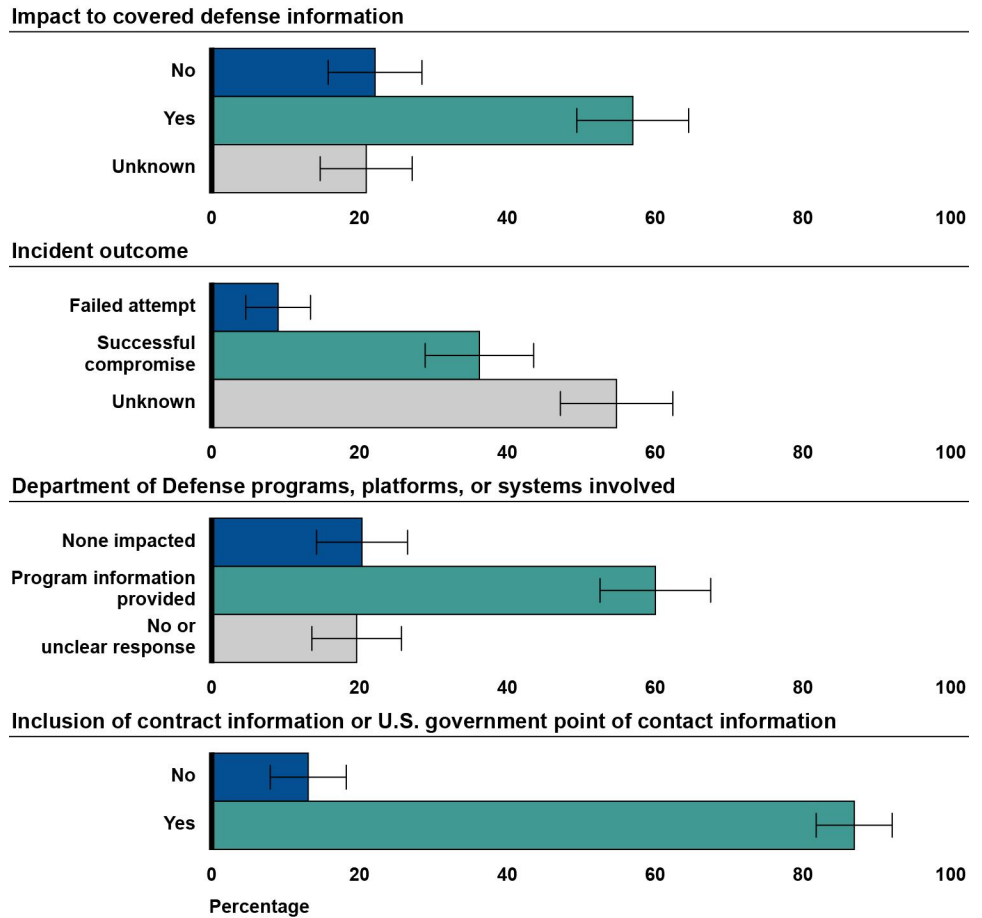
However, the information submitted by DIB companies to DC3 was not always comprehensive or timely. Specifically, the DIB’s mandatory cyber incident reports from calendar years 2015 through 2021 did not always contain required information or indicated that the information was unknown. For example:

- An estimated 20 percent of the incident reports provided no response or an unclear response as to whether DOD programs, platforms, or systems were involved in the incident.⁵¹
- An estimated 21 percent of the mandatory incident reports received by DC3 indicated that it was unknown whether there was an impact to covered defense information.
- An estimated 55 percent of the incident reports indicated that an incident outcome—successful compromise or failed attempt—was unknown. Figure 5 summarizes the extent to which required information was included in mandatory incident reports from calendar years 2015 through 2021.

⁵⁰As previously described, among other things, the criteria for leadership notification include compromise of classified information likely to cause significant harm or damage to the national security interests of the U.S.; significant loss of controlled unclassified information from a cleared defense contractor; significant loss of PII of civilian or uniformed members of the Armed Forces; and congressional reporting requirements.

⁵¹All percentage estimates from the analysis of DIB mandatory incident reports have margins of error at the 95 percent confidence level of plus or minus 8 percentage points or less unless otherwise noted. See appendix I for more information on sampling error for survey estimates.

Figure 5: Estimated Response Rates for Defense Industrial Base’s Mandatory Incident Report Key Information, calendar years 2015 through 2021



Source: GAO analysis of Department of Defense information. | GAO-23-105084

Accessible Data for Figure 5: Estimated Response Rates for Defense Industrial Base’s Mandatory Incident Report Key Information, calendar years 2015 through 2021

Category	Response	Percentage
Impact to covered defense information	No	22.1
Impact to covered defense information	Yes	56.98
Impact to covered defense information	Unknown	20.91
Incident outcome	Failed attempt	8.99
Incident outcome	Successful compromise	36.22
Incident outcome	Unknown	54.78
Department of Defense programs, platforms, or systems involved	None impacted	20.34

Category	Response	Percentage
Department of Defense programs, platforms, or systems involved	Program information provided	60.04
Department of Defense programs, platforms, or systems involved	No or unclear response	19.62
Inclusion of contract information or U.S. government point of contact information	No	13.06
Inclusion of contract information or U.S. government point of contact information	Yes	86.94

Note: Error bars display 95 percent confidence intervals for estimates and are within +/- 8 percent.

In addition to excluding required information, DIB companies often submitted mandatory incident reports outside of the 3-day window required for reporting. For example, we estimate that 51 percent of the cyber incidents submitted by DIB organizations from calendar years 2015 through 2021 were submitted more than 4 days after discovery.⁵² In addition, we estimate that 20 percent were submitted more than 20 days after discovery.

DC3 officials said that much of the information is unknown within the 3-day window required for reporting. The officials said it was unrealistic to expect a company to always have the required information within 3 days of discovering a cyber incident. To illustrate, in two discussion groups with representatives from DIB companies, participants said that although 3 days is reasonable for an initial report, only limited information is available at that time.

DC3 officials stated that DIB companies occasionally submit additional reports with updated information, called follow-up reports.⁵³ The officials said that DC3 analysts follow up with DIB companies to gather additional information, but doing so is a resource-intensive process. According to the officials, DIB companies are sometimes not responsive to follow-up inquiries about the incident reports.

According to DC3 officials, it is generally more important to receive complete information than to receive reports as quickly as possible.

⁵²Due to limitations in the data, we could not determine the specific hour from incident discovery to incident reporting. Therefore, we used 4 days (instead of the 3-day reporting requirement) to account for potential differences in hours.

⁵³We estimate that 11 percent of the cyber incident reports submitted to DC3 in calendar years 2015 through 2021 included follow-up reports.

However, there are instances when timely reporting is important, according to the officials. For example, if a cyber incident affects the ability of a contractor to provide support to DOD, quick reporting of that information would be essential. Further contributing to the weaknesses in the timeliness of the reporting, DC3 officials said that they do not have the authority to enforce the 3-day deadline. Instead, officials stated the contracting officer who oversees the individual DIB company contract is responsible for enforcing the requirement.

DC3 officials also stated that current language in the DFARS clause might not be clear enough to elicit the information needed from the DIB because the cyber incident and discovery definitions are not explicit enough. As a result, DIB companies may interpret the clause differently. For example, DC3 officials stated that during the SolarWinds cyber event, multiple DIB entities observed the presence of the malware but did not report it since they did not see the malware execute or see data being extracted.⁵⁴ The officials also said that, in some cases, companies interpret “discovery” of a cyber incident to be the date after the incident has been validated in an internal review, leading to a delay of several weeks in getting the information to DOD.

According to standards for internal control in the federal government, management identifies information requirements in an iterative and ongoing process that occurs throughout an effective internal control system.⁵⁵ DOD has identified information requirements for mandatory cyber incident reports and time frames for submission; however, the current requirements are not eliciting complete and timely reporting from the DIB. Until DOD takes steps to evaluate potential improvements to ensure mandatory cyber incident reports are complete and timely,

⁵⁴Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company, according to the company’s Chief Executive Officer. The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service. The threat actor first injected test software code into SolarWinds network management and monitoring suite of products called Orion. Then, beginning in February 2020, the threat actor injected malicious code into a file that was later included in SolarWinds Orion software updates. SolarWinds released the software updates to its customers not realizing that the updates were compromised with backdoor access from the threat actor. We have previously reported on this breach. See GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, [GAO-22-104746](#) (Washington, D.C.: January 2022).

⁵⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#), (Washington, D.C.: September 2014).

including a review of current reporting requirements and how they are implemented, it will continue to lack key information that could assist DOD in the timely mitigation of potential threats to DIB information systems. DC3 officials said there would be a benefit to both them and DIB companies if the current requirements were updated.

DOD's Reported Data Breaches of PII Have More Than Doubled since 2015 and DOD's Notification of Affected Individuals Is Unclear

Reported data breaches of personally identifiable information (PII) have more than doubled in DOD from calendar years 2015 through 2021.⁵⁶ DOD has established a process for determining whether these breaches have affected individuals who should be contacted. This process includes conducting a risk assessment that considers factors such as the nature and sensitivity of the PII, likelihood of access to and use of the PII, and the type of the breach. However, the extent to which this process has been implemented is unclear, because DOD had not consistently documented risk assessments or notifications of affected individuals.

DOD's Reported Data Breaches of PII Have Increased since 2015

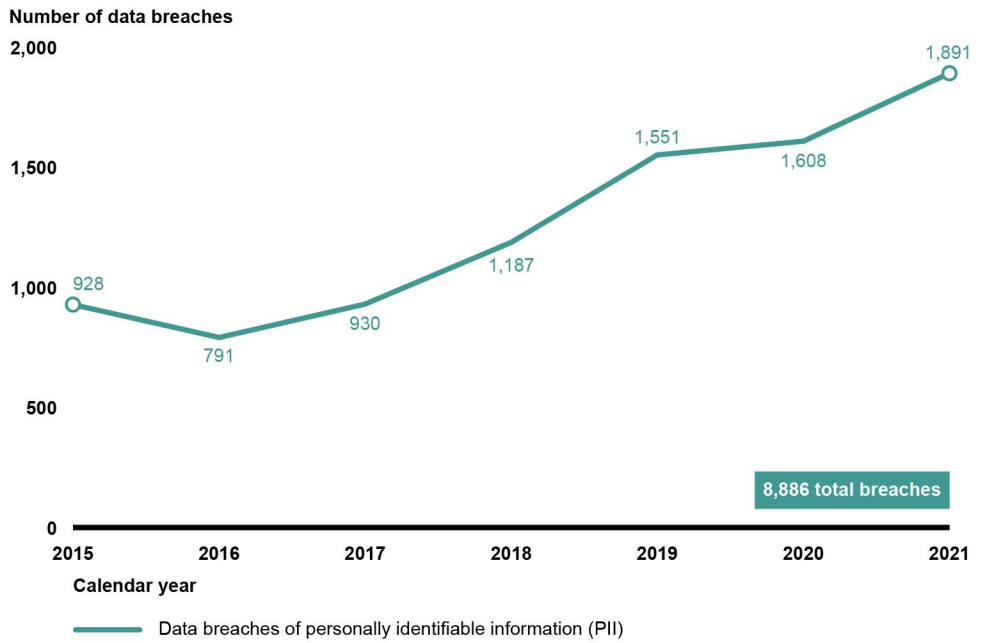
OMB defines a data breach of PII as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for a non-authorized purpose.⁵⁷ Data breaches of PII reported by DOD have increased by 104 percent from calendar years 2015 through 2021. Figure

⁵⁶PII refers to information that can be used to distinguish or trace an individual's identity or can be combined with other information that is linked or linkable to a specific individual.

⁵⁷OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017). DOD refers to the OMB definition in DOD Manual 5400.11, volume 2, *DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan* (May 6, 2021). According to OMB, some common examples of data breaches of PII include a laptop or portable storage device storing PII is lost or stolen, an email containing PII is inadvertently sent to the wrong person, or a box of documents with PII is lost or stolen during shipping.

6 shows the number of data breaches of PII reported by DOD by calendar year.

Figure 6: Data Breaches of PII Reported by DOD in Calendar Years 2015 through 2021



Source: Department of Defense Compliance and Reporting Tool (CART). | GAO-23-105084

Accessible Data for Figure 6: Data Breaches of PII Reported by DOD in Calendar Years 2015 through 2021

Calendar year	Number of data breaches
2015	928
2016	791
2017	930
2018	1187
2019	1551
2020	1608
2021	1891

DOD Has Established a Process for Notifying Affected Individuals of Data Breaches of PII

In May 2021, DOD issued DOD Manual 5400.11, volume 2, *DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan*.⁵⁸ The purpose of the plan is to implement policy, assign responsibilities, and provide procedures for how the department will prepare for and respond to data breaches of PII. Among other things, the plan includes steps that DOD should take to determine the risk of harm to individuals potentially affected by a breach and to determine the notification requirements when notification is deemed necessary.

According to the plan, the decision to notify depends on the specific circumstances of the breach and the assessed risk of harm. The assessed risk of harm caused by the incident considers three factors—(1) the nature and sensitivity of the PII, (2) the likelihood of access to and use of the PII, and (3) the type of breach. The plan includes steps DOD should take to assess these factors.

The Senior Component Official for Privacy, in coordination with the Component Privacy Officer, is responsible for advising senior leaders of whether and when to notify individuals potentially affected by a breach. As noted above, an assessment of the risk of harm—part of the decision of whether to notify—includes consideration of at least three factors. For example, one factor, such as the nature and sensitivity of the PII potentially compromised, may identify an increased amount of harm based on the data elements involved. Other factors, such as the likelihood of use of PII and type of breach, may help identify a reduced risk given the technical safeguards in place.

DOD is to assess data breaches of PII on a case-by-case basis, as the type of harm is unique to each case. In this regard, DOD Privacy Office officials stated that a large amount of discretion is afforded to the Senior Component Official for Privacy when deciding whether to contact affected individuals. If the Senior Component Official for Privacy determines that an individual should be contacted, DOD guidance states that notification should be made as expeditiously as practicable and without unreasonable

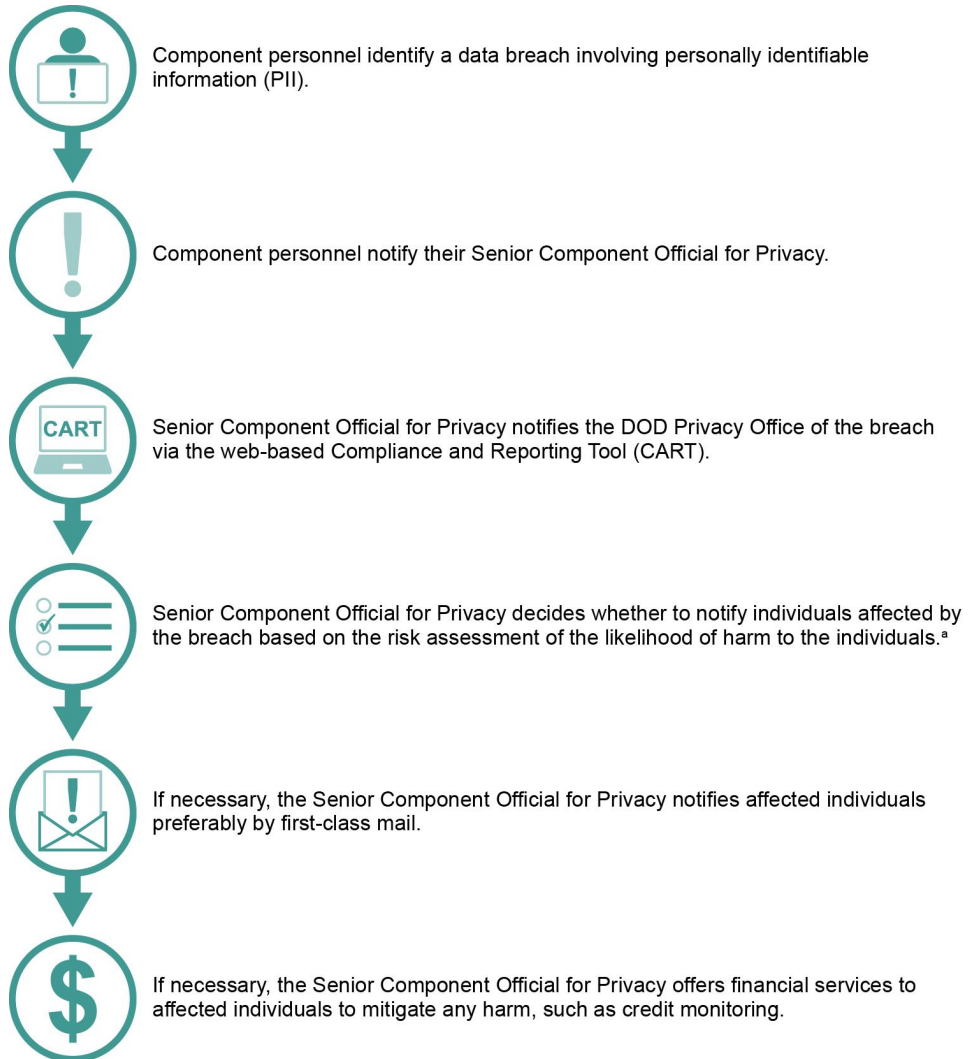
⁵⁸DOD Manual 5400.11, vol. 2, *DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan*, (May 6, 2021). The issuance incorporated the previous DOD Breach Response Plan dated September 28, 2017.

delay.⁵⁹ At the same time, the Senior Component Official for Privacy also determines if any financial services should be provided to affected individuals, such as credit monitoring.

The Senior Component Official for Privacy reports data breaches of PII to the DOD Privacy Office using a standardized form titled “Breach of Personally Identifiable Information (PII) Report.” The data breach form is submitted through the DOD Privacy Office’s web-based Compliance and Reporting Tool (CART)—the official repository for the forms. The form includes fields to indicate whether affected individuals were notified, including whether they were notified within 10 working days. Figure 7 illustrates the process for reporting data breaches of PII and notifying affected individuals if necessary.

⁵⁹DOD Manual 5400.11, vol. 2.

Figure 7: Process for Reporting Data Breaches of PII and Notifying Affected Individuals



Source: GAO analysis of Department of Defense information and officials' statements. | GAO-23-105084

^aThe decision of whether to notify depends on the specific circumstances of the breach and the assessed risk of harm. The risk assessment considers three factors at a minimum: (1) nature and sensitivity of the PII, (2) likelihood of access to and use of the PII, and (3) the type of the breach.

The Extent to Which DOD Has Implemented Its Process for Notifying Affected Individuals of PII Data Breaches Is Unclear

For data breaches of PII occurring from 2017 through 2020, it was unclear whether DOD had implemented its process for conducting risk assessments and notifying individuals affected by the breach. As shown by figure 6, 5,276 data breaches were reported by DOD during calendar years 2017 through 2020. We reviewed a random sample of 152 of the data breach forms for these breaches to develop a generalizable sample.⁶⁰ Based on this analysis, we estimate that approximately:

- 20 percent of the forms submitted to CART denoted that DOD had determined that the department needed to notify affected individuals.⁶¹ Of these forms, approximately 18 percent denoted that DOD had notified affected individuals within 10 days.⁶²
- 66 percent of the forms denoted that DOD had determined that notification was not necessary for reasons such as the low likelihood of harm of the breach.⁶³
- 15 percent of the forms indicated that the notification determination was pending.⁶⁴

In addition, DOD officials could not always provide evidence that they had performed risk assessments for data breaches of PII. For example, we

⁶⁰We collected raw data on all the data breach forms submitted to CART during calendar years 2017 through 2020 to include the CART data breach form identification number. From this raw data, we selected a sample of 152 breaches and reviewed the corresponding data breach form. DOD Privacy Office officials stated that a CART system error prevented them from accessing the raw data for 2015 and 2016. In addition, at the time of the selection of our sample, data for 2021 was incomplete. As a result, we could not identify the data breach identification numbers for these years and did not review the data breach forms.

⁶¹The margin of error for this estimate at a 95 percent confidence interval is plus or minus 6.4 percent.

⁶²The margin of error for these estimates at a 95 percent confidence interval is plus or minus 6.3 percent.

⁶³The margin of error for this estimate at a 95 percent confidence interval is plus or minus 7.6 percent.

⁶⁴The margin of error for this estimate at a 95 percent confidence interval is plus or minus 5.6 percent.

reviewed 30 data breach forms and could not fully determine whether a risk assessment had been performed for any of them or that the three factors had been considered.

The DOD Privacy official stated that the DOD Privacy Office has recognized that a more clear and consistent way of documenting the risk assessment for privacy data breaches was needed. According to an official in the DOD Privacy Office, the office is currently developing a new breach reporting system that will have a built-in risk assessment module. The module, according to the official, will provide a standard way to conduct and document the risk assessment. The module will be required to be completed before a breach report can be entered into the system. As a result, every breach report will have an accompanying, standardized risk assessment that will be documented in the same way. As of June 2022, DISA has requested the authority to operate the new system and has begun testing the migration of old CART data into it.⁶⁵ The privacy official said they expect to deploy the system sometime in the early part of fiscal year 2023. Because of these efforts, DOD should be better positioned to consistently document the risk assessment for privacy breaches.

Further, DOD could not provide evidence that the department had always notified affected individuals where the data breach form denoted the department should have taken such action. For example, we reviewed 30 data breach forms where the form indicated that affected individuals were notified. DOD could not provide evidence that it had notified individuals for 26 of the 30 data breach incidents. DOD Privacy Office officials stated that, in many cases, components notify individuals verbally, by phone, or by email and a record of the notification is not retained.

Officials added that in other instances, components might have destroyed the record of notification in accordance with their records retention guidance. OMB guidance states that federal agencies shall develop and maintain a formal process to track and document each breach reported to the agency. The process is to allow the agency to track and monitor certain elements, including whether the agency, after assessing the risk

⁶⁵NIST defines authorization to operate as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.

of harm, provided notification to the individuals potentially affected by a breach.⁶⁶ Without documenting that affected individuals were notified, there is no way to verify that DOD actually contacted affected individuals. Not notifying individuals or notifying individuals inconsistently could leave some affected individuals more exposed to identity theft, which could lead to financial loss and emotional distress.

Conclusions

DOD has recognized the importance of cyber incident management. For example, the department has issued guidance assigning overall responsibilities for protecting the DOD network against unauthorized activity or cyber threats. However, DOD faces challenges in implementing an effective process to report and share information on cyber incidents. The lack of accountable organization to ensure complete incident reporting and proper notification of leadership and the lack of an incident management system that is aligned with policy requirements are concerning because leaders throughout DOD need to have a complete and accurate picture of the department's cybersecurity posture.

Complete incident information and effective notification allows commanders and others responsible for directing incident response strategies to remain informed about the status of their information networks and the effect of the incident on their missions. In addition, complete incident information can help other DOD organizations recognize adversarial activity and mitigate any negative impact on their missions. Further, a properly designed cyber incident reporting system that is aligned with policy requirements would provide DOD with an enterprise-wide view of all adversarial network activity which could help shape tactical, strategic, and military strategies for response.

DOD has also recognized the importance of improving the cybersecurity posture of the DIB, which has long been a target of—and has become increasingly vulnerable to—cyber threats. For example, DOD issued guidance regarding the notification of DOD and congressional leadership of cyber incidents involving the DIB. However, weaknesses remain in the department's processes for sharing and reporting DIB-related cyber incident information. By ensuring that all DIB-related cyber incidents are properly shared with relevant stakeholders, DOD components would be

⁶⁶OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017).

better positioned to alert their communities of interest of cyber incidents that may affect them. Moreover, by evaluating and implementing potential improvements to the completeness and timeliness of cyber incident information reported by the DIB, DOD would have a more complete and accurate understanding of the threat landscape affecting the private sector, which could alert DOD more quickly to potential threats and allow it to employ mitigation measures earlier.

When there is a data breach of PII, DOD is required to determine whether to notify affected individuals. DOD officials told us that they follow this requirement but do not always document the notification. Without documenting the notification, there is no way to verify that DOD actually informed individuals that their privacy data was potentially compromised, which could leave some affected individuals more exposed than others to identity theft.

Recommendations for Executive Action

We are making the following six recommendations to DOD:

The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN assign responsibility for overseeing cyber incident reporting and leadership notification, and ensuring policy compliance. (Recommendation 1)

The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN align policy and system requirements to enable DOD to have enterprise-wide visibility of cyber incident reporting to support tactical, strategic, and military strategies for response. (Recommendation 2)

The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN include in new guidance on incident reporting include detailed procedures for identifying, reporting, and notifying leadership of critical cyber incidents. (Recommendation 3)

The Secretary of Defense should ensure that the Commander of CYBERCOM—in coordination with DOD CIO and Directors of DC3 and DCSA—examines whether information on DIB-related cyber incidents handled by CSSPs is relevant to the missions of other DOD components,

including DC3 and DCSA, and identifies when and with whom such information should be shared. (Recommendation 4)

The Secretary of Defense should ensure that the DOD CIO determines what actions need to be taken to encourage more complete and timely mandatory cyber incident reporting from DIB companies. (Recommendation 5)

The Secretary of Defense should ensure—through the Director of the Privacy, Civil Liberties, and Freedom of Information Directorate—that DOD components document instances where individuals affected by a privacy data breach were notified. (Recommendation 6)

Agency Comments

We provided a draft of this report to the department for review and comment. In written comments, reprinted in appendix IV, DOD concurred with our recommendations.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, DOD's Chief Information Officer, the Commander of Cyber Command, the Chairman of the Joint Forces Headquarter Department of Defense Network, the Director of the Defense Information Systems Agency, and DOD's 24 cybersecurity service providers that were included in our review. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Joseph Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov, or Jennifer Franks at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.



Joseph W. Kirschbaum
Director, Defense Capabilities and Management

A handwritten signature in black ink, appearing to read "Jennifer R. Franks". The signature is fluid and cursive, with the first name being the most prominent.

Jennifer R. Franks
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chair
The Honorable Richard C. Shelby
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Betty McCollum
Chair
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The House Report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2021 included a provision for us to review the Department of Defense's (DOD) cyber incident management efforts.¹ This report describes the extent to which DOD (1) has established and implemented a process to report and notify leadership of cyber incidents that affect DOD information networks; (2) has established and implemented a process to report and share information about selected defense industrial base (DIB) cyber incidents; and (3) has experienced data breaches of personally identifiable information (PII) and implemented a process to notify affected individuals of the breach.

To address objective one, we surveyed 24 of the 26 DOD cyber security service providers (CSSPs). We excluded the DOD Education Activity CSSP because it had not reported a cyber incident in the Joint Incident Management System (JIMS). We also excluded the United States Space Force CSSP because it had not been certified as a CSSP at the time of our survey administration. The 24 CSSPs identified appropriate points of contact within each of their organizations to serve as the survey respondent.

The survey included questions on the organization's incident reporting processes and how they collect, maintain, analyze, and report cyber incident data. The survey also solicited the CSSP organization's views on the quality and reliability of the information in the JIMS. Before distributing the survey, we conducted cognitive testing (pretesting) with officials from five CSSPs and reviewed the survey with our internal survey specialist. During each pretest, all of which we conducted via a web conferencing application, we tested whether (1) the instructions and questions were clear and unambiguous, (2) the terms we used were accurate, and (3) pretest participants could offer a potential solution to any problems identified. We noted any potential problems identified by the reviewers and through the pretests and modified the questionnaire based on the feedback received. Following those revisions, we solicited written

¹H.R. Rep. No. 116-442, at 250-251 (2020).

comments from the five CSSPs with whom we had conducted pretesting and conducted one final pretest with another CSSP of the revised survey.

We distributed the survey using a web-based survey platform and by email, depending on the information technology security policies of the recipient organization. In some instances, survey respondents did not answer all questions because they were not applicable to their organization. To supplement the survey results, we conducted additional follow-up with four CSSPs following the conclusion of our survey to clarify their responses. We used the survey results and follow-up interviews to determine the data reliability of the number of cyber incidents in JIMS and their characteristics.

We calculated the frequency of responses to our closed-ended survey questions and reviewed responses to the open-ended questions to identify examples relevant to our objectives. We administered the survey from November 5, 2021, to January 26, 2022, and received responses from all 24 CSSPs, for a 100 percent response rate. As such, the corresponding responses reflected information and views as of that time. See appendix II for a copy of the survey administered to the 24 CSSPs.

To further address the first objective, we identified and reviewed DOD guidance relevant to the reporting and notification of cyber incidents.² We also randomly selected a sample of eight DOD CSSPs for detailed analysis of a sample of the incidents they reported in JIMS, any incident-related documentation, and their incident response plans. To do this, we divided the 24 CSSPs into four groups of six based on the total number of cyber incidents reported to JIMS from January 2015 through December 2020—(1) the most incidents reported, (2) the second most reported incidents, (3) the third most reported incidents, and (4) the least amount of incidents reported.

We randomly selected two CSSPs from each of the four groups for a total of eight selected CSSPs. The eight CSSPs we selected were

1. Navy Cyber Defense Operations Command;

²E.g., DOD Instruction 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (Mar. 7, 2016) (incorporating change 1, July 25, 2017) and Chairman of the Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program* (July 10, 2012).

2. U.S. Army Combat Capabilities Development Command C5ISR (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance) Center;
3. Defense Contract Management Agency;
4. U.S. Coast Guard;³
5. Defense Intelligence Agency;
6. Defense Finance Accounting Service;
7. Defense Advanced Research Projects Agency; and
8. U.S. Transportation Command.

In addition, we extracted all JIMS incident records submitted by the eight selected CSSPs from calendar years 2015 through 2020. We then selected two different samples from these incidents.⁴ The first sample was inclusive of all the incidents categorized as root level intrusion (Category 1), user-level intrusion (Category 2), and denial of service (Category 4)—54 in total.

Due to the large population of incidents categorized as malicious logic (Category 7), we selected a separate sample of these incidents using simple random sampling.⁵ This resulted in a sample of 100 malicious logic incidents for a total of 154 sampled incidents. Of these 154 sampled incidents, we excluded 16 because CSSPs could not provide documentation for the incidents or there were errors in the JIMS records, such as duplicated entries. This resulted in a sample size of 138 incidents. This selection process resulted in a generalizable sample for incidents reported in JIMS from calendar years 2015 through 2020.

Because we followed a probability procedure based on random selections, our sample is only one of many samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our sample's results as a 95 percent confidence interval (e.g., plus or minus 10 percentage points).

³The U.S. Coast Guard is a service within the Department of Homeland Security, except when operating as a service within the Navy. However, its incident response program reports to and collaborates with DOD.

⁴Because incident documentation would have been incomplete for 2021 at the time of our selection, we limited the sample to calendar years 2015 through 2020.

⁵For random selection, we assigned a random number to each incident and selected incidents with the highest assigned number.

This interval would contain the actual population value for 95 percent of the samples we could have drawn.

For each of the 138 sampled incidents, we reviewed the data contained in JIMS. We also reviewed related documentation from CSSPs' systems and repositories, such as incident reports, notes, emails, and briefing slides. We evaluated this data and documentation to determine whether the steps taken by the CSSPs to report and share cyber incident information and to notify leadership aligned with the guidance established by DOD.

In addition, we obtained and reviewed DOD guidance related to the department's process for reporting significant activities (SIGACTs)—Operation Gladiator Shield.⁶ We then obtained all SIGACT reports submitted by the eight selected CSSPs to the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) from July 2017 through December 2020.⁷ We compared the SIGACT reports to any relevant incidents from the 138 we selected above—such as intrusions and denials of service, which would generally require a SIGACT report submission—to determine the extent to which CSSPs submitted SIGACTs in accordance with the DOD guidance.

To supplement our analysis of cyber incident reports, we also interviewed all eight selected CSSPs regarding our analysis and any anomalies we identified in the information we obtained. In addition, we discussed the selected CSSPs' incident response processes, such as notification procedures, usage of SIGACTs, and incident management systems used. We also interviewed officials from the Office of DOD Chief Information Officer, U.S. Cyber Command, JFHQ-DODIN, and Defense Information Systems Agency regarding their roles in DOD cyber incident management.

To determine the total number of incidents, we extracted all the available data from JIMS for all cyber incidents reported by all 24 surveyed CSSPs during calendar years 2015 through 2021. To determine whether the total number of incidents reported in JIMS was sufficiently reliable, we reviewed the responses from each CSSP to the survey, previously

⁶JFHQ-DODIN, *Operation Gladiator Shield 2017* (June 30, 2017).

⁷JFHQ-DODIN did not require CSSPs to submit SIGACTs prior to July 2017. Because our JIMS-based incident sample did not include calendar year 2021, we did not include SIGACTs from 2021 in our analysis.

discussed above. For example, we reviewed CSSP responses regarding their data entry and quality assurance processes, which allowed us to conclude that the information submitted by all CSSPs was sufficiently reliable for identifying the number of cyber incidents reported to JIMS by CSSPs.

To describe the cyber incidents, we assessed the reliability of the data extracted from JIMS by identifying the percent of incident reports with missing values for required incident data fields. We determined that any field with missing values in 50 percent or more of records was not sufficiently reliable and excluded those fields from our review. We performed further reliability testing of the remaining data fields specifically to evaluate logical relationships and remove clearly erroneous data (e.g., an incident reported as an exercise but not categorized as such). Finally, we analyzed CSSP survey responses about the reliability of these fields. We concluded that the following data fields were sufficiently reliable for describing the characteristics of cyber incidents:

- Organization,
- Issue Type,
- CSSP,
- Primary Incident Category,
- Activity Start Date and Time, and
- Incident Ticket Classification.

We also determined that the following data fields were sufficiently reliable only for the limited purpose of illustrative examples and describing the type of information submitted to JIMS:

- Summary,
- Incident Description, and
- Functional Area.

Information reported by U.S. Special Operations Command was determined to be unreliable for describing cyber incident characteristics because the CSSP stated that they did not have quality assurance procedures for entering or updating information related to the cyber incident reports in JIMS. Information reported by the CSSPs with the National Geospatial-Intelligence Agency, Defense Information Systems Agency Joint Service Provider, National Security Agency, U.S. Marine Corps, Defense Logistics Agency, and U.S. Strategic Command was

determined to be unreliable for describing cyber incident characteristics because these organizations did not finalize 20 percent or more of the incidents they submitted in JIMS.

To address the second objective, we identified DOD guidance relevant to the reporting and sharing of cyber incidents affecting the DIB.⁸ We then reviewed DOD Cyber Crime Center (DC3), Defense Counterintelligence Agency (DCSA), and CSSP documented processes and practices and examined whether those processes were fully implemented. We also analyzed cyber incident reports and data from DC3.⁹ Specifically, we obtained data on the number of mandatory and voluntary incident reports the DC3 received from the DIB from calendar years 2015 through 2021.¹⁰ We then conducted a data reliability assessment of this data to determine its completeness and accuracy examining documentation that officials provided to us and conducting electronic tests on the data we received to check for completeness and accuracy. We also sent data reliability questionnaires and interviewed DC3 officials regarding how they collect and use incident report data. Based on the information collected and data analyzed, we determined that the data from the DC3 were sufficiently reliable for reporting the number of mandatory and voluntary incident reports. We also determined that the data were sufficiently reliable for selecting a generalizable sample of mandatory reports for additional analysis.

In determining the timeliness of mandatory incident reports submitted by the DIB and the inclusion rates of key information, we selected a generalizable sample from the 1,575 mandatory incident reports

⁸E.g., 32 C.F.R. §117.8, *National Industrial Security Program Operating Manual* (July 1, 2021); Deputy Secretary of Defense Memorandum, *Defense Industrial Base Cyber Incident Notification Process* (May 6, 2019); Defense Federal Acquisition Regulation Supplement clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Dec. 2019); and Chairman of the Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program* (July 10, 2012).

⁹We were not able to obtain comparable data for DCSA or the CSSPs. According to DCSA officials, they were migrating data to a new system at the time of our review and could not provide accurate numbers regarding the number of cyber incidents received by DCSA. For CSSPs, due to limitations in the data, we could not identify the entire population of reported cyber incidents related to the DIB contained within the JIMS or SIGACTs databases.

¹⁰Mandatory incident reports are those submitted by the DIB to DC3 under DFARS clause 252.204-7012. Voluntary incident reports are those submitted to DC3 that do not meet the criteria of the DFARS clause.

submitted to DC3 from calendar years 2015 through 2021. The reports included both initial and follow-up reports. We grouped related mandatory incident reports and considered them as one incident, resulting in 1,443 distinct incidents to sample. To ensure we had a sufficient number of reports represented for each of these years, we developed a stratified random sample proportionally allocated across calendar years 2015 through 2021. With this probability sample, each of the 1,443 incidents had a nonzero probability of being included, and that probability could be computed for any report. If a selected mandatory report had related reporting, all mandatory incident reports associated with that cyber incident were included in the selection for review.¹¹ This analysis resulted in a generalizable sample of 168 incidents.

Because we followed a probability procedure based on random selections, our sample is only one of many samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our sample's results as a 95 percent confidence interval (e.g., plus or minus 8 percentage points). This interval would contain the actual population value for 95 percent of the samples we could have drawn.

To determine the extent to which the reports included key information, we obtained a copy of each report in our sample from DC3's classified website. We consulted with DC3 officials to determine which required information fields of a mandatory incident report were most relevant and critical to accomplishing their mission and determining the impact of cyber incidents. Based on these steps, we identified the following four fields:

- Impact to Covered Defense Information;
- Incident Outcome;
- DOD Programs, Platforms, or Systems Involved; and
- Contract information or U.S. government point of contact information.

We then reviewed each report in our sample to determine whether information regarding these four fields was included or not included in the report and calculated the corresponding inclusion rates for each information field. If more than one report was associated with the incident,

¹¹Mandatory incident reports may represent a distinct cyber incident or be a related report providing additional information on a previously reported incident.

we used the most recently submitted report to capture the most recent data available for the incident.

To determine timeliness, we compared the incident discovery date to the incident report date. Due to limitations in the data, we could not determine the specific hour from incident discovery to incident reporting. Therefore, we used 4 days (instead of the 3-day reporting requirement) to account for potential differences in hours. If more than one report was associated with the incident, we used the first report submitted to calculate the timeliness.

To supplement our analysis, we also convened two group discussions with representatives from DIB companies on October 20, 2021, and October 21, 2021. We convened these groups to obtain DIB companies' insight into the process for reporting cyber incidents to DOD. DC3 officials, on our behalf, reached out to organizations that are part of the DIB Cybersecurity Program—a partnership in which DOD and private companies share cyber threat information and mitigation and remediation strategies. DC3 identified 11 companies willing to participate, seven of which participated in the discussion groups. Representatives from the following companies participated in the focus groups:

- Offset Strategic Services
- STI-Tec
- Sentinel Blue
- Booz Allen Hamilton
- Lockheed Martin
- Favor Tech Consulting
- LinQuest

We divided participants into two groups based on the number of employees for each company to separate large companies from small and medium-sized organizations. We included four companies with more than 500 employees in our first discussion group. We included three companies with fewer than 500 employees in our second discussion group. We then summarized the participants' views into written records of the discussions and reviewed them to identify similar or divergent perspectives and themes for us to use as illustrative examples. The information and perspectives of the DIB participants in these groups cannot be generalized to other DIB companies that we did not interview.

They represented only the views and experiences of the individuals that participated in our discussion at that time.

To supplement our analysis and discussions with DIB companies, we interviewed officials from DOD components identified as involved in receiving or sharing DIB-related cyber incident information. Specifically, we interviewed officials from:

- DC3
- DOD CIO Cybersecurity Program
- National Security Agency
 - Cybersecurity Collaboration Center.
- DCSA
 - Industrial Security Directorate
 - National Industrial Security Program Authorization Office
 - Operations Analysis Group
 - Threat Directorate
 - Threat Directorate Cyber Mission Center.

Other components, such as military department counterintelligence organizations or law enforcement, may also learn of cyber incidents affecting the DIB. We did not include those organizations in this review, but focused on the DOD components to which DIB organizations are directed to submit cyber incident reports.

To address the third objective, we identified DOD, Office of Management and Budget (OMB), and National Institutes of Standards and Technology (NIST) guidance relevant to data breaches of PII and summarized DOD's documented processes for handling data breaches of PII.¹² To determine the number of breaches per year, we obtained raw data from the DOD Privacy Office's web-based Compliance and Reporting Tool (CART) for calendar years 2017 through 2020 and CART annual summary reports for

¹²E.g., DOD Manual 5400.11, vol. 2, *DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan* (May 6, 2021); OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017); and NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010).

calendar years 2015, 2016, and 2021.¹³ To determine the extent to which DOD decided to notify affected individuals, we selected a random sample of 152 data breaches reported to CART during calendar years 2017 through 2020 and analyzed the accompanying data breach form for each.¹⁴ We reviewed the data fields on each form to determine:

- the date the breach was identified,
- the component responsible for safeguarding the information at the time of the breach,
- the number of individuals affected,
- whether DOD determined a need to identify affected individuals, and
- the reasons why it was determined that affected individuals did not need to be notified.

Because we followed a probability procedure based on random selections, our sample is only one of many samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our sample's results as a 95 percent confidence interval (e.g., plus or minus 8 percentage points). This interval would contain the actual population value for 95 percent of the samples we could have drawn.

We assessed the reliability of this information by testing the metadata for the total universe and a random sample of incidents to determine the extent to which the data fields above were missing. We also held a data reliability meeting with DOD Privacy Office officials and requested written responses to data reliability questions, which the officials provided. We determined that the above data fields were sufficiently reliable to determine if DOD decided to notify affected individuals of data breaches and if the data breach form included a risk assessment of the harm to affected individuals. In addition to meetings to discuss the reliability of

¹³A CART system error prevented DOD Privacy Office officials from providing raw data for calendar years 2015 and 2016. In addition, at the time of our data request, raw data for 2021 was incomplete. As a result, DOD Privacy Office officials provided CART annual summary reports for 2015 and 2016 in response to our data request and provided an annual summary report for 2021 once the year was completed.

¹⁴The raw data from CART for calendar years 2017 through 2020 included the data breach form identification number. With the identification numbers, we selected a sample of 151 breaches and reviewed the corresponding data breach form. At the time of the selection of our sample, we could not identify the identification numbers for breaches occurring in calendar years 2015, 2016, and 2021 and did not include them in our sample because of the CART data limitations already noted.

data in CART, we also met with officials from the DOD, Army, and Air Force privacy offices to discuss their data breach reporting process.

We conducted this performance audit from March 2021 to November 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Survey of DOD Cybersecurity Service Providers

The U.S. Government Accountability Office (GAO) is responsible for reporting to Congress on federal programs. The House Armed Services Committee report to accompany the National Defense Authorization Act for FY2021 included a provision for GAO to examine DOD procedures for responding to and mitigating risks from cyber incidents.

As part of this review, we plan to use data from the Joint Incident Management System (JIMS) and your agency's systems for documenting cyber incidents. To ensure that we are presenting the data correctly and that any conclusions that we draw based on the data are warranted, we need to understand how the data were collected, maintained, analyzed, and presented. We are sending this survey to you because we understand you are responsible for documenting cyber incidents in JIMS. Therefore, we would like to request your responses to this survey about the completeness and accuracy of the data and the information system that produces the data.

You have been identified as the appropriate point of contact for this survey at your organization. If you are not that person, please send an email to the GAO contact with the contact information for the correct person for survey. Your responses will provide valuable information that will be used to inform Congress about the status of DOD's cyber incident management efforts.

The survey will take approximately 20-30 minutes to complete. Please complete this survey by November 19th.

If you have any questions, please contact Shawn Arbogast at (202) 512-6771 or ArbogastM@gao.gov, or Benjamin Emmel at (202) 512-7858 or EmmelB@gao.gov.

Introductory Questions

CSSP Name

Please select one from the dropdown menu.

Defense Information Systems Agency (1)

Defense Threat Reduction Agency (2)

Joint Service Provider (3)

Missile Defense Agency (4)

National Geospatial Intelligence Agency (5)

Navy Information Warfare Center Atlantic (6)

National Reconnaissance Office (7)

National Security Agency (8)

16th Air Force (9)

Coast Guard Cyber Command (10)

US Special Operations Command (11)

US Strategic Command (12)

US Transportation Command (13)

Defense Advanced Research Projects Agency (14)

Defense Commissary Agency (15)

Defense Finance and Accounting Service (16)

Defense Intelligence Agency (17)

Navy Cyber Defense Operations Command (18)

Marine Corps Cyber Operations Group (19)

DEVCOM C5ISR (20)

Defense Logistics Agency (21)

High Performance Computing Modernization Program (22)

US Army Cyber Command (23)

Defense Contract Management Agency (24)

Contact information for the main point of contact filling out this form

Name (1)

Position/title (2)

Email (3)

Phone (4)

Component-Level Cyber Incident System

The questions in this section refer to the use of your organization's data system for tracking, reporting, or documenting cyber incidents. Please answer the questions in this section as they pertain to your organization's data system.

In what format is your system?

Check all that apply.

Microsoft Access (1)

SQL (2)

Oracle (3)

Text files (*.txt, *.csv, *.pm) (4)

Spreadsheets (*.dbf, *.xls, *.xlsx, *.ods) (5)

Microsoft OneNote, Microsoft Word, or other written documents (6)

Other (*Please specify*) (7)

In your system(s) is it possible to extract cyber incidents for particular date ranges?

Yes (1)

No (2)

Maybe (3)

Display this question if "In your system(s) is it possible to extract cyber incidents for particular date ranges?" = Maybe

Please explain.

What quality control procedures, if any, are in place to enhance accuracy and completeness of the data? Check all that apply.

System generated checks to prevent duplicate records (1)

System generated checks such as error messages for out-of-range-entries or inconsistent entries (2)

System generated checks to ensure incidents cannot be submitted without all required elements (3)

Supervisor review of incident reporting process (4)

Formal agency guidance, policies, and/or standard operating procedures (5)

Review trends in number of cases reported over time (6)

Other (*Please describe*) (7)

Display this question if "What quality control procedures if any, are in place to enhance accuracy and completeness of the..." = Supervisory review of incident reporting process

How frequently do these supervisory reviews occur?

Every entry is reviewed (1)

A sample of entries is reviewed (2)

Display this question if "How frequently do these supervisory reviews occur?" = A sample of entries is reviewed

How is the sample selected?

Display this question if "What quality control procedures, if any, are in place to enhance accuracy and completeness of the..." = Supervisory review of incident reporting process

What are the procedures for follow-up if any errors are found?

Are there any written documentation of procedures for entering incident data into the system and conducting quality control checks?

Yes (1)

No (2)

Display this question if "Are there any written documentation of procedures for entering incident data into the system and..." = Yes

Please send copies of written procedures to Benjamin Emmel at EmmelB@gao.gov or Shawn Arbogast at ArbogastM@gao.gov

How does your organization primarily enter information into JIMS?

Hand entering data using the JIMS website and graphical user interface on SIPRNet (1)

Importing comma separated value (CSV) files using JIMS web services (2)

Our organization does not enter information into JIMS (3)

Display this question if "How does your organization primarily enter information into JIMS?" = Importing comma separated value (CSV) files using JIMS web services

Importing comma separated value (CSV) files using JIMS web services

The questions in this section refer to the process that your organization uses to import data from your data system into JIMS

Display this question if "How does your organization primarily enter information into JIMS?" = Importing comma separated value (CSV) files using JIMS web services

Please describe the transfer process.

Display this question if "How does your organization primarily enter information into JIMS?" = Importing comma separated value (CSV) files using JIMS web services

Does your CSSP upload initial data into JIMS on new incidents when an investigation is opened?

Yes (1)

No (2)

Display this question if "How does your organization primarily enter information into JIMS?" = Importing comma separated value (CSV) files using JIMS web services

Does your CSSP upload finalized data into JIMS when an incident is closed?

Yes (1)

No (2)

Display this question if "How does your organization primarily enter information into JIMS?" = Importing comma separated value (CSV) files using JIMS web services

In your opinion, how well does the upload process from your system into JIMS work for *required* data fields?

Our organization is able to create a crosswalk that translates required data fields into JIMS as specified by the JIMS user manual with **no challenges**. (1)

Our organization has **moderate challenges** translating some of our required data fields into JIMS as specified in JIMS user manual. (2)

Our organization has **severe or serious challenges** translating some of our required data fields into JIMS as specified in JIMS user manual. (3)

Display this question if "If in your opinion, how well does the upload process from your system into JIMS work for required data..." = Our

organization has moderate challenges translating some of our required data fields into JIMS as specified in JIMS user manual or Our organization has severe or serious challenges translating some of our required data fields into JIMS as specified in JIMS user manual

Please explain.

Display this question if "How does your organization primarily enter information into JIMS" = Hand entering data using the JIMS website and graphical user interface on SIPRNet

Does your CSSP enter initial data into JIMS on new incidents when an investigation is opened?

Yes (1)

No (2)

Does your CSSP enter finalized data into JIMS when an incident is closed?

Yes (1)

No (2)

Display this question if "How does your organization primarily enter information into JIMS" = Hand entering data using the JIMS website and graphical user interface on SIPRNet

In your opinion, how well are you able to enter required data fields into JIMS?

Our organization is able to enter required data fields into JIMS as specified by the JIMS user manual with **no challenges**. (1)

Our organization has **moderate challenges** entering some of our required data fields into JIMS as specified in JIMS user manual. (2)

Our organization has **severe or serious challenges** entering some of our required data fields into JIMS as specified in JIMS user manual. (3)

Display this question if "In your opinion, how well are you able to enter required data fields into JIMS?" = Our organization has moderate

challenges entering some of our required data fields into JIMS as specified in JIMS user manual or Our organization has severe or serious challenges entering some of our required data fields into JIMS as specified in JIMS user manual

Please explain.

Does your system transmit to or receive information from the cyber incident systems of other DOD components (e.g., Army sharing with Navy)? This question does not include data transmitted to or from JIMS.

No (1)

Yes (2)

Display this question if “Does your system transmit to or receive information from the cyber incident systems of other DOD...” = Yes

Which DOD components does your system transmit information to?

Display this question if “Does your system transmit to or receive information from the cyber incident systems of other DOD...” = Yes

Which DOD components does your system receive information from?

JIMS

Joint Incident Management System (JIMS)

These next set of questions ask about specific data elements that GAO intends to request for use in our engagement. *We will be requesting data from 2015-2021.* Please answer the following questions *regarding your CSSP’s data for closed cases in JIMS* from this time period

Display this question if “Does your CSSP upload finalized data into JIMS when an incident is closed?” = Yes or “Does your CSSP enter finalized data into JIMS when an incident is closed?” = Yes

Please describe the accuracy of each JIMS element as of when an incident has been closed. By accuracy, we mean the extent to which data is complete and reflects the ground truth of an incident. Data limitations

for certain fields may come from the transfer process between your organization's system and JIMS, or may come from challenges accurately recording information into your system in the first place. Choose the best response for each JIMS element based on your assessment of the entire data collection and transfer process.

Table 2: Survey Respondents' Determination of Accuracy of Joint Incident Management System (JIMS) Elements

Category	Accuracy is high with no limitations (1)	Accuracy is moderate with some limitations (2)	Accuracy is low with several and/or serious limitations (3)	Please describe data limitations (1)
Organization (1)				
Issue Type (2)				
Summary (3)				
CSSP (4)				
Primary Incident Category (5)				
Activity Start Date & Time (6)				
Incident Description (7)				
Incident Ticket Classification (8)				
Functional Area (9)				
COCOM Stakeholder(s) (10)				
Privacy Related Event (11)				
Encompassing Cost (12)				
Staff Hours Lost (13)				
Overall Operational Impact (14)				
Overall Technical Impact (15)				

Source: GAO. | GAO-23-105084

We intend to use JIMS data elements listed below to describe the frequency and characteristics of cyber incidents across DOD to Congress. Do you have any concerns or limitations about our use of these data elements for this purpose?

Data elements: Organization, Issue Type, Summary, CSSP, Primary Incident Category, Activity Start Date & Time, Incident Description, Incident Ticket Classification, Functional Area, COCOM Stakeholder(s), Privacy Related Event, Encompassing Cost, Staff

Hours Lost, Overall Operational Impact, and Overall Technical Impact

No (1)

Yes (2)

Display this question if “We intend to use JIMS data elements listed below to describe the frequency and characteristics of...” = Yes

Please describe.

Information Sharing Questions

As part of our review, we are examining how information on cyber incidents is shared within DOD. These questions will assist us in understanding how DOD components receive and share information with each other.

Does your CSSP have responsibility for monitoring any classified DODIN connections located at authorized defense contractors or other private organizations?

Yes (1)

No (2)

Does your CSSP receive cyber incident information from the Defense Cyber Crime Center (DC3)?

Yes (1)

No (2)

Thank You

Thank you for responding to the GAO survey on the Joint Incident Management System and cyber incident data. Your responses will assist us in providing valuable information to the Congress.

If you would like to provide additional information or have any questions about this GAO study or the survey, please contact Shawn Arbogast at (202) 512-6771 or ArbogastM@gao.gov, or Benjamin Emmel at (202) 512-7858 or EmmelB@gao.gov.

Once you hit Submit, your responses will be considered final, and you will not be able to re-enter the survey to change them.

Appendix III: List of DOD's Cybersecurity Service Providers

Cybersecurity Service Providers (CSSPs) are organizations established by the military services and DOD agencies to provide information network protection services under support agreements with system owners. Based on information provided by DOD, there are 26 DOD CSSPs authorized to operate within DOD networks:

- 16th Air Force
- Coast Guard Cyber Command
- Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance
- Defense Advanced Research Projects Agency
- Defense Commissary Agency
- Defense Contract Management Agency
- Department of Defense Education Activity
- Defense Finance and Account Service
- Defense Information Systems Agency
- Defense Intelligence Agency
- Defense Logistics Agency
- Defense Threat Reduction Agency
- High Performance Computing Modernization Program
- Joint Service Provider
- Marine Corps Cyber Operations Group
- Missile Defense Agency
- National Geospatial Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Cyber Defense Operations Command
- Navy Information Warfare Center
- United States Army Cyber Command
- United States Space Force
- United States Special Operations Command

**Appendix III: List of DOD's Cybersecurity
Service Providers**

-
- United States Strategic Command
 - United States Transportation Command

Appendix IV: Comments from the Department of Defense

Note: The report number was changed from
“GAO-22-105084SU” to
“GAO-23-105084” after DOD reviewed the draft report



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

OCT - 5 2022


Mr. Joseph W. Kirschbaum
Director Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-105084SU, "DOD CYBERSECURITY: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared," dated August 22, 2022 (GAO Code 105084).

Enclosed is DoD's response to the subject report. My point of contact is Michele Iversen who can be reached by e-mail at michele.t.iversen.civ@mail.mil or by phone at (703) 697-6101.

Sincerely,


John B. Sherman

Enclosure:
As stated

GAO DRAFT REPORT DATED AUGUST 22, 2022
GAO-22-105084SU (GAO CODE 105084SU)

“DOD CYBERSECURITY: ENHANCED ATTENTION NEEDED TO ENSURE
CYBERINCIDENTS ARE APPROPRIATELY REPORTED AND SHARED”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN assign responsibility for overseeing cyber incident reporting and leadership notification and ensuring policy compliance.

DoD RESPONSE: Concur.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN align policy and system requirements to enable DOD to have enterprise-wide visibility of cyber incident reporting to support tactical, strategic, and military strategies for response.

DoD RESPONSE: Concur.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN include detailed procedures for identifying, reporting, and notifying leadership of critical cyber incidents in the new guidance on incident reporting..

DoD RESPONSE: Concur.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the Commander of CYBERCOM in coordination with DOD CIO, and Directors of DC3 and DCSA, examines whether information on DIB-related cyber incidents handled by CSSPs is relevant to the missions of other DOD components, including DC3 and DCSA, and identifies when and with whom such information should be shared.

DoD RESPONSE: Concur.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO determines what actions need to be taken to encourage better mandatory cyber incident reporting from DIB companies.

DoD RESPONSE: Concur.

RECOMMENDATION 6: The GAO recommends that the Secretary of Defense should ensure, through the Director of the Privacy, Civil Liberties, and Freedom of Information Directorate, that DOD components document instances where individuals affected by a privacy data breach were notified.

DoD RESPONSE: Concur.

Accessible Text for Appendix IV: Comments from the Department of Defense

OCT- 5 2022

Mr. Joseph W. Kirschbaum
Director Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-105084SU, "DOD CYBERSECURITY: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared," dated August 22, 2022 (GAO Code 105084).

Enclosed is DoD's response to the subject report. My point of contact is Michele Iversen who can be reached by e-mail at michele.t.iversen.civ@mail.mil or by phone at (703) 697-6101.

Sincerely,

John B. Sherman

Enclosure: As stated

GAO DRAFT REPORT DATED AUGUST 22, 2022 GAO-22-105084SU (GAO CODE 105084SU)

"DOD CYBERSECURITY: ENHANCED ATTENTION NEEDED TO ENSURE CYBERINCIDENTS ARE APPROPRIATELY REPORTED AND SHARED"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN

assign responsibility for overseeing cyber incident reporting and leadership notification and ensuring policy compliance.

DoD RESPONSE: Concur.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN align policy and system requirements to enable DOD to have enterprise-wide visibility of cyber incident reporting to support tactical, strategic, and military strategies for response.

DoD RESPONSE: Concur.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN include detailed procedures for identifying, reporting, and notifying leadership of critical cyber incidents in the new guidance on incident reporting..

DoD RESPONSE: Concur.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the Commander of CYBERCOM in coordination with DOD CIO, and Directors of DC3 and DCSA, examines whether information on DIB-related cyber incidents handled by CSSPs is relevant to the missions of other DOD components, including DC3 and DCSA, and identifies when and with whom such information should be shared.

DoD RESPONSE: Concur.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO determines what actions need to be taken to encourage better mandatory cyber incident reporting from DIB companies.

DoD RESPONSE: Concur.

RECOMMENDATION 6: The GAO recommends that the Secretary of Defense should ensure, through the Director of the Privacy, Civil Liberties, and Freedom of Information Directorate, that DOD components document instances where individuals affected by a privacy data breach were notified.

DoD RESPONSE: Concur.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov
Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Marisol Cruz-Cain (Director), Tommy Baril (Assistant Director), Nicole Jarvis (Assistant Director), Shawn Arbogast (Analyst-in-Charge), Alexander Anderegg, Michael Dworman, Benjamin Emmel, and Brian Palmer made key contributions to this report. In addition, Mariel Alper, Tracy Barnes, Sara Daleski, Rebecca Eyler, Suellen Foth, Christopher Gezon, Gina Hoover, Franklin Jackson, Suzanne Kaasa, Won Lee, Serena Lo, Richard Powelson, and Jared Smith provided technical support.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.