GAO Highlights

INFORMATION ENVIRONMENT

DOD Needs to Address Security Risks of Publicly Accessible Information

GAO-26-107492 October 2025

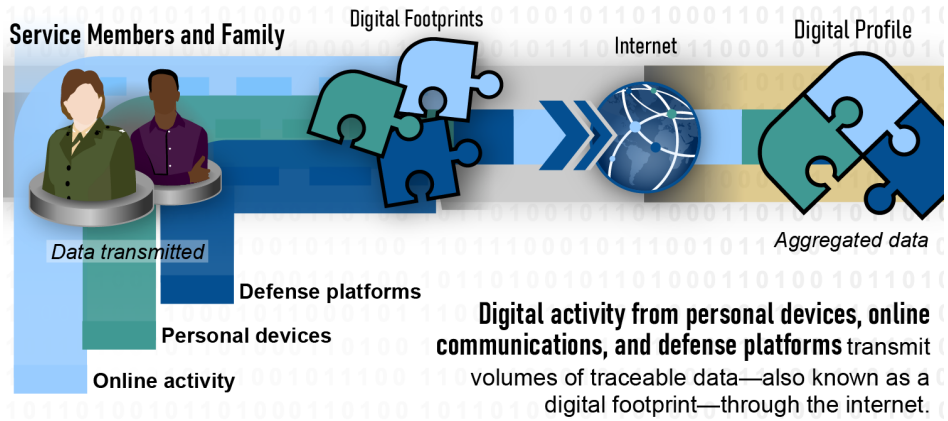
A report to congressional committees.

For more information, contact: Joe Kirschbaum at KirschbaumJ@gao.gov or Marisol Cruz Cain at CruzCainM@gao.gov.

What GAO Found

Digital activity from personal and government devices, online communications, and defense platforms such as ships and aircraft can generate volumes of traceable data, known as digital footprints. When these digital footprints are aggregated into a digital profile, they can threaten Department of Defense (DOD) personnel and their families, operations, and ultimately national security.

Figure: Digital Activity Generates Digital Footprints That Can Be Aggregated into A Digital Profile



Sources: GAO analysis and illustrations (service member/family, puzzle pieces, background and internet illustrations). | GAO-26-107492

GAO determined that three of five offices under the Office of the Secretary of Defense (OSD) have issued policies and guidance on the risks associated with the public accessibility of DOD's digital information. However, the policies and guidance are narrowly focused, do not include all stakeholders, and do not include all relevant security areas. As a cross-functional governance body that includes stakeholders across DOD, the Defense Security Enterprise Executive Committee is well-positioned to lead a department-wide collaborative assessment of policies and guidance on digital footprint and profile risks. Without such an assessment, DOD will have difficulty in determining whether risks are being sufficiently managed within the boundaries of their legal authorities. Also, DOD will face ever-increasing threats to personnel privacy and safety, mission success, and national security.

GAO also determined that 10 DOD components were not fully addressing two areas essential to reducing the risk of digital threats—training and security assessments.

- Nine of ten components' training materials did not consistently train personnel on risks of digital information in the public across all relevant security areas.
- Eight of ten components did not conduct assessments of threats across the required security areas of force protection, insider threat, mission assurance, and operations security. Instead, most components focused assessment efforts solely on operations security.

Why GAO Did This Study

Massive amounts of traceable data about military personnel and operations now exist due to the digital revolution. Public accessibility of this data enables malicious actors to exploit critical information and jeopardize DOD's mission and the safety of its personnel.

Senate Report 118-58 and House Report 118-301 include provisions that GAO assess DOD's efforts to mitigate national security risks and assess DOD components' efforts to protect the digital footprint of DOD personnel. This report assesses the extent to which (1) OSD has taken action to reduce risks to DOD personnel and operations and (2) DOD components have conducted training and assessments to reduce risk to DOD personnel and operations. The report also describes security risks of publicly accessible data about DOD personnel and operations.

GAO focused on actions taken by five OSD offices and 10 select DOD components with security responsibilities—the five services and five other cognizant components such as U.S. Cyber Command and Space Force. GAO reviewed policies and documentation from these offices and components, and interviewed agency officials regarding actions taken to reduce information about DOD and its personnel being publicly accessible.

What GAO Recommends

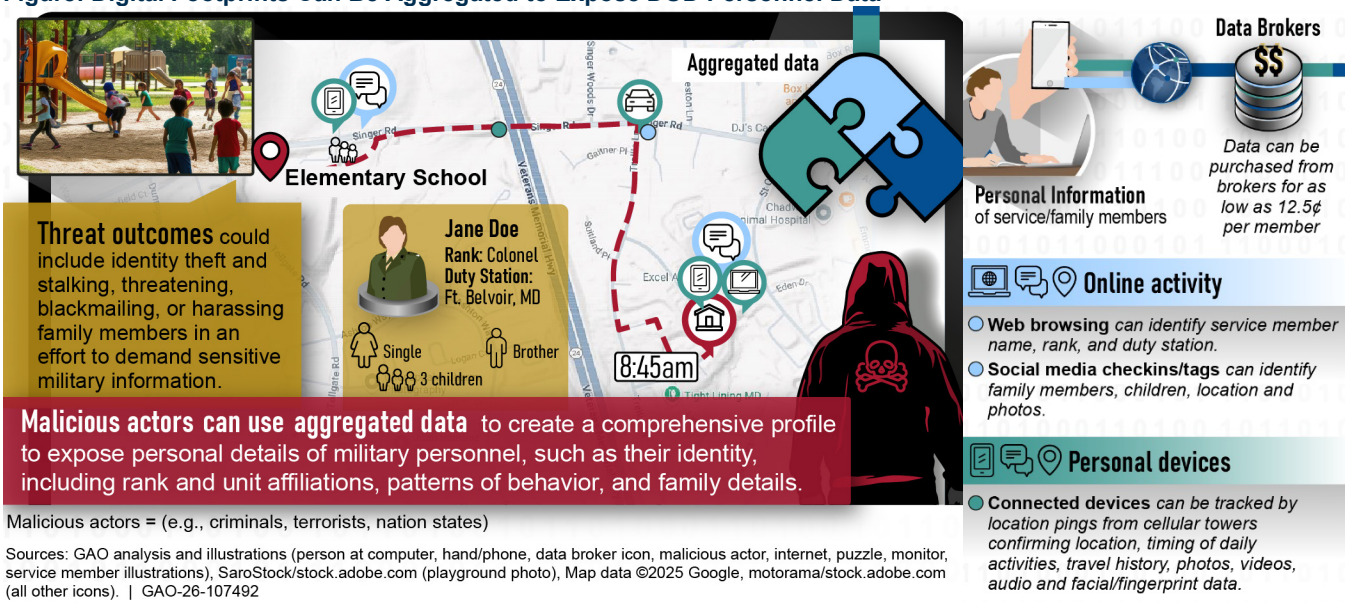
GAO is making 12 recommendations to DOD to assess its policies and guidance; collaborate to reduce risks; provide training on the digital environment and its associated risks across security areas; and complete required security assessments. DOD concurred with 11 of 12 recommendations and partially concurred with one. GAO maintains that all recommendations are warranted.

GAO developed the notional threat scenarios below to exemplify how publicly accessible information about DOD operations and its personnel introduces risks across multiple security areas.

Risk to Personnel and Their Families

This scenario illustrates how a malicious actor could use digital information purchased from data brokers or collected from the web to identify and harm DOD personnel and their families.

Figure: Digital Footprints Can Be Aggregated to Expose DOD Personnel Data



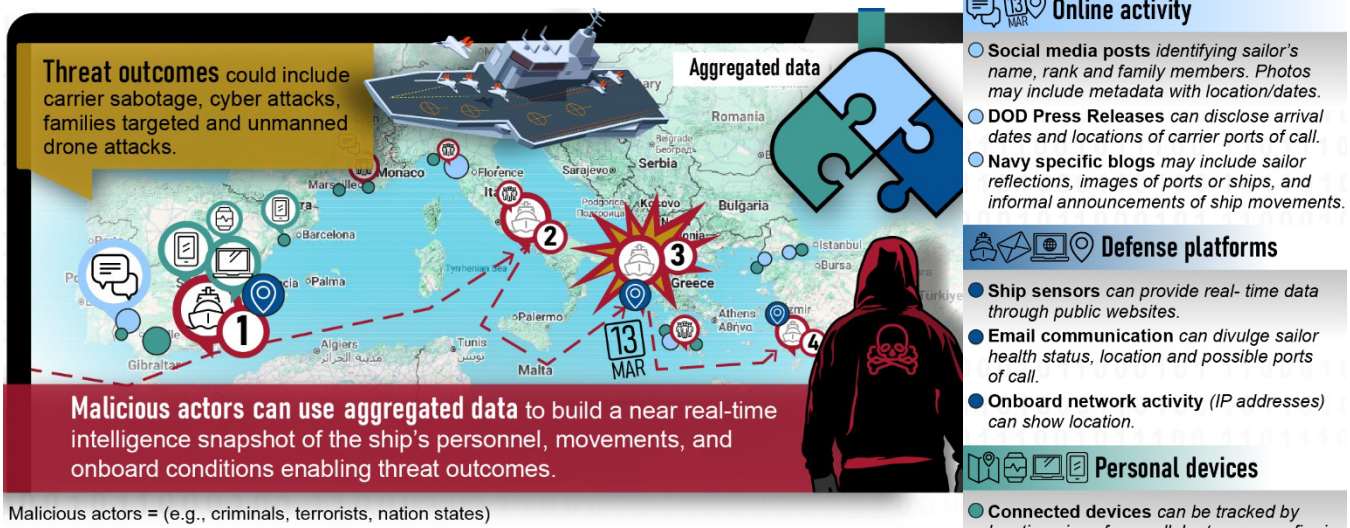
Malicious actors = (e.g., criminals, terrorists, nation states)

Sources: GAO analysis and illustrations (person at computer, hand/phone, data broker icon, malicious actor, internet, puzzle, monitor, service member illustrations), SaroStock/stock.adobe.com (playground photo), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-107492

Risk to Operations

This scenario illustrates how a malicious actor could use digital information—including DOD press releases, news sources, online activity, social media posts, and ship coordinates—to project the route of a vessel and disrupt naval carrier operations. When aggregated, this information could enable targeting the vessel with uncrewed systems or sabotaging the ship while in port.

Figure: Digital Footprints Can Be Aggregated to Disrupt Aircraft Carrier Operations



Malicious actors = (e.g., criminals, terrorists, nation states)

Sources: GAO analysis and illustrations (malicious actor, internet, puzzle, monitor illustrations), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-107492