United States Government Accountability Office

Report to Congressional Committees

October 2025

INFORMATION ENVIRONMENT

DOD Needs to Address Security Risks of Publicly Accessible Information

GAO-26-107492

GAO Highlights

INFORMATION ENVIRONMENT

DOD Needs to Address Security Risks of Publicly Accessible Information

GAO-26-107492 October 2025

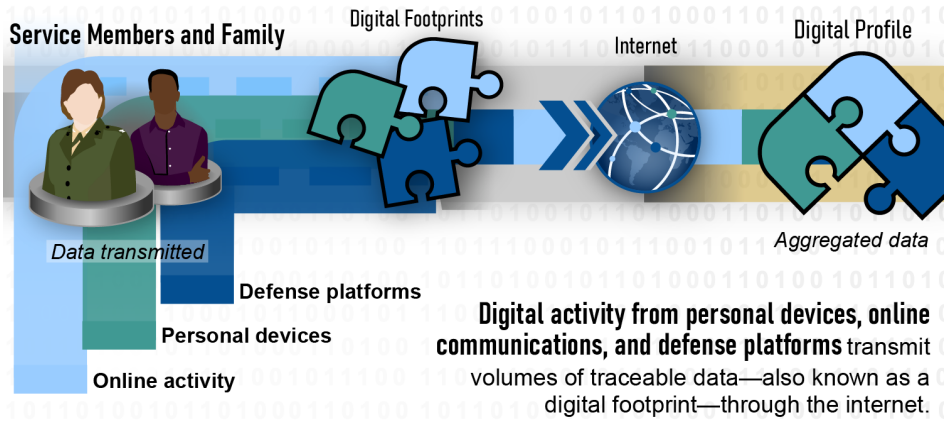
A report to congressional committees.

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

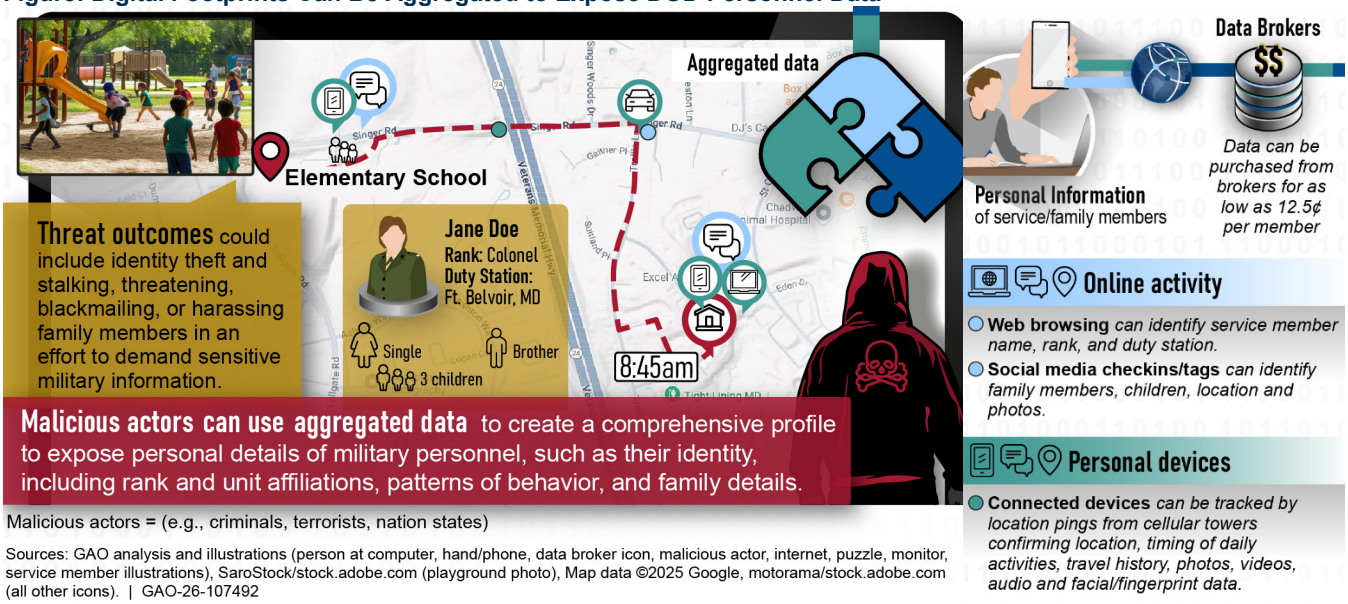
GAO is making 12 recommendations to DOD to assess its policies and guidance; collaborate to reduce risks; provide training on the digital environment and its associated risks across security areas; and complete required security assessments. DOD concurred with 11 of 12 recommendations and partially concurred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



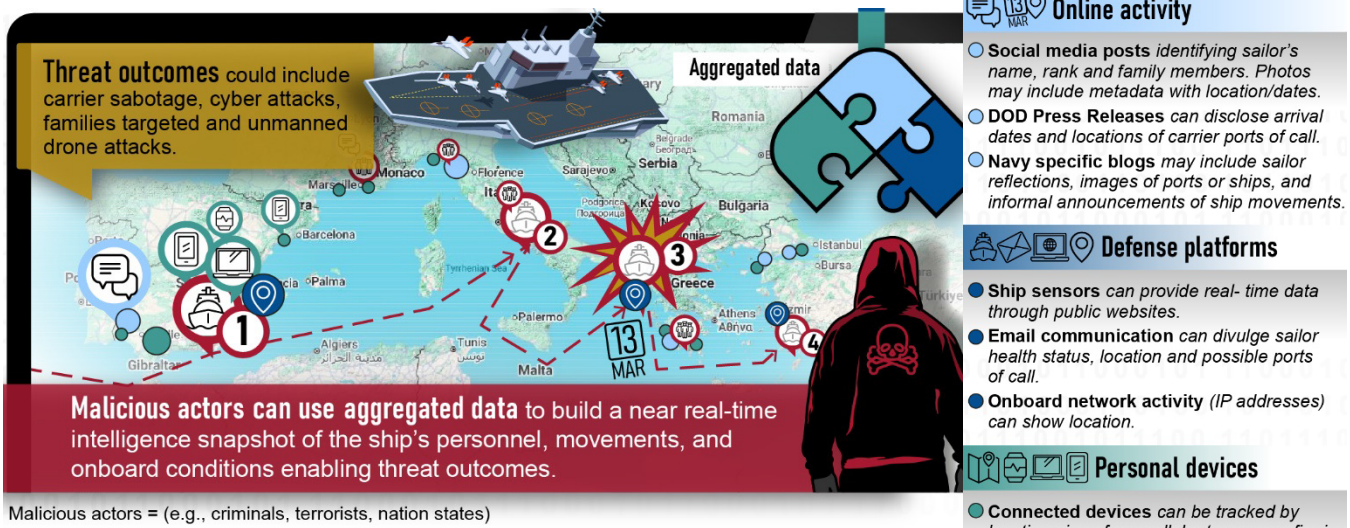
Malicious actors = (e.g., criminals, terrorists, nation states)

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

Contents

Abbreviations

DOD	Department of Defense
OPSE	operations security
OSD	Office of the Secretary of Defense

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

October 7, 2025

Congressional Committees

Today's digital communication has transformed the once-popular military slogan "loose lips sink ships" into "loose tweets sink fleets." The message that careless speech can undermine national security remains especially applicable in the age when we are compelled to have a digital identity. Massive amounts of traceable data about military personnel now exist due to the proliferation of personal and government devices and the resulting widespread availability of digital information. In addition, defense platforms (e.g., weapon platforms, connected devices, sensors, training facilities, test ranges, and business systems) depending on wireless technology can generate tremendous amounts of data.

Advances in technology have made the accessibility to this information easier and more efficient. Specifically, data generated by personnel and defense platforms—also known as digital footprints—can be gained through public websites, stolen and posted on the dark web, or acquired and sold by data brokers from anywhere in the world.[1] These digital footprints, when aggregated into a digital profile, can threaten military operations; the privacy and personal safety of service members, civilian employees, contractors, and family members; and ultimately our national security.

Over the years, congressional testimonies, reports, and news articles have identified concerns about the risks of information about national security personnel and operations in the public sphere. For example, in January 2025, the nominee for Director of the Central Intelligence Agency told the Senate Select Committee on Intelligence that remote surveillance (also known as ubiquitous technical surveillance) is presenting unprecedented challenges to the Central Intelligence Agency's ability to

[1]The dark web is a collection of websites that have hidden Internet Protocol addresses and may require specific software to access. Data brokers are companies that collect, aggregate, and sell personal information to third parties for the purposes of marketing, advertising, law enforcement, enterprise security, criminal justice and recruitment, among other areas.

collect human intelligence.[2] In the last few years, the Office of the Director of National Intelligence issued an unclassified report and fact sheet highlighting the risks associated with commercially available information—that is, any data or other information bought or sold by a company for commercial purposes.[3]

Reports published by the NATO Strategic Communications Centre of Excellence highlight risks and vulnerabilities related to commercially available data.[4] In 2022, a Yale fellow testified about the risk posed to individuals in national security positions or in the military from data acquired on the open data market.[5] Similarly, a 2023 Duke University research study found that data brokers—companies that collect and resell information on individuals—pose a national security risk by compiling large, detailed datasets on U.S. military personnel and subsequently selling that data on the open market.[6] The study noted that adversaries with access to these datasets could use this information for coercion, reputational damage, and blackmail.

We have previously issued reports on risks and threats to national security attributed to emerging technology in the information environment (including 5G wireless technologies), Internet of Things devices (e.g., wearable fitness devices and smartphones), and technology tracking

[2]Senate Select Committee on Intelligence, 119th Cong. (Jan. 2025) (opening statement of Honorable John L. Ratcliffe). Additionally, the Director of the National Security Agency wrote a letter to Congress stating that personal devices and accounts of U.S. government personnel remain prime targets for adversarial exploitation.

[3]The Office of the Director of National Intelligence defines commercially available information as any data or other information that is sold, leased, or licensed to the general public or to non-governmental entities for non-government purposes. Commercially Available Information also includes information for exclusive government use provided by corporate entities.

[4]See, for example, *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*; *Camouflage for the Digital Domain: A Force Protection Framework for Armed Forces*; and *The Current Digital Arena and Its Risks to Serving Military Personnel*.

[5]Senate Judiciary Subcommittee on Privacy, Technology and the Law, 117th Cong. 10 (2022) (statement of Yale Law School senior fellow Samm Sacks).

[6]Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan, *Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security* (Duke University, Nov. 2023).

military aircraft.[7] For example, in 2017, we reported on challenges DOD faced due to Internet of Things technologies, security risks, and associated policy gaps.[8] In 2018, we reported how DOD and the Federal Aviation Administration had identified security and mission risks stemming from information broadcasted by Automatic Dependent Surveillance-Broadcast Out technology, among other things.[9] In 2022, we reported how the modern escalation in the volume and interconnectedness of data had changed the landscape of information and national security.[10] DOD took actions to address our recommendations in these reports, such as signing a memorandum of agreement with the Federal Aviation Administration to jointly address aircraft position reporting.

A Senate report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2024 and the conference report accompanying the Act include provisions that we review and assess DOD's efforts to mitigate the national security risks and threats stemming from the digital footprint of DOD personnel; and assess DOD components' efforts to protect personal information of its personnel from exploitation by foreign adversaries, respectively.[11] This report (1) describes the security, privacy, and safety risks of publicly accessible data about DOD personnel and operations; and assesses the extent to which (2) the Office of the Secretary of Defense (OSD) has taken action to reduce associated risks to DOD personnel and operations; and (3)

[7]The Internet of Things is the set of Internet-capable devices that interact with the physical environment and typically contain elements for sensing, communicating, processing, and actuating.

[8]GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-514SU (Washington, D.C.: June 7, 2017).

[9]Automatic Dependent Surveillance-Broadcast Out technology is a key component of the Federal Aviation Administration's Next Generation Air Transportation System, which seeks to modernize the current ground-based radar system to a satellite-derived system for automated aircraft position reporting, navigation, and digital communications. This technology uses an aircraft's avionics equipment to broadcast the aircraft's position, altitude, and velocity to any ground, air, or space-based receiver. GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[10]GAO, *Information Environment: Opportunities and Threats to DOD's National Security Mission*, GAO-22-104714 (Washington, D.C.: Sept. 21, 2022).

[11]S. Rep. No. 118-58, at 318-319 (2023); and H.R. Rep. No. 118-301, at 1298 (2023) (Conf. Rep.). DOD defines "DOD components" as the Office of the Secretary of Defense, military departments, Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, combatant commands, DOD Office of Inspector General, defense agencies and field activities, and all other entities within DOD.

DOD components have conducted training and assessments to reduce risks to DOD personnel and operations.

The scope of this review includes digital data that can be generated by and transmitted from disparate sources, such as personal and government devices; DOD personnel working in an official capacity (such as a military unit's public affairs employee); and defense platforms that transmit information outside the DOD information network.

For the first objective, we reviewed literature that discussed the security implications of digital footprints, remote technical surveillance, and misuse of publicly accessible information. We interviewed officials from the DOD organizations listed below to gain an understanding of their technical responsibility for managing digital footprint data and to identify the risks and threats to DOD's personnel and operations when digital data about DOD and its personnel become publicly accessible. We also conducted our own investigation to determine the accessibility of sensitive DOD-related information and assess associated risks to DOD's personnel and operations stemming from the aggregation of publicly accessible digital data. We developed and examined notional threat scenarios that depict potential consequences stemming from the exploitation of publicly accessible digital data. We developed these scenarios based on analyses of literature research, interviews, and our own investigation. Officials from the Office of the Under Secretary of Defense for Intelligence and Security reviewed the scenarios and provided input on their plausibility and potential impact.

For both the second and third objectives, we identified common OSD and DOD component security responsibilities that could reduce risks generated from digital profiles. We reviewed DOD guidance for six select security disciplines and security-related functions (hereafter referred to in this report as "security areas"): counterintelligence, force protection, insider threat, mission assurance, operations security (OPSEC), and critical program information protection (program protection). We excluded six security areas—cybersecurity, industrial security, information security, personnel security, physical security, and special access programs—because those security areas are primarily focused on protecting information within DOD's network, while the scope of our review was focused on information that is publicly accessible.

For the second objective, we focused on five OSD offices. These include four OSD offices that oversee the security areas within the scope of our review: Offices of the Under Secretary of Defense for Intelligence and

Security, the Under Secretary of Defense for Policy, the DOD Chief Information Officer, and the Under Secretary of Defense for Research and Engineering. We also included the Office of the Assistant to the Secretary of Defense for Public Affairs since it is responsible for releasing DOD information to the public. To evaluate OSD's actions, we requested and obtained current policies and guidance that OSD officials identified as relevant to the digital profile threat. We reviewed each document provided to assess whether it discussed the digital profile threat and its associated risks, and established any best practices to reduce risk (e.g., countermeasures or mitigations). We also interviewed officials from the Offices of the Under Secretary of Defense for Intelligence and Security, the Under Secretary of Defense for Policy, and the DOD Chief Information Officer to discuss their efforts to coordinate and collaborate across other security areas.

For the third objective, we focused on a non-generalizable sample of 10 DOD components: all five military services, U.S. Cyber Command, U.S. Special Operations Command, National Security Agency, Defense Counterintelligence and Security Agency, and Defense Intelligence Agency.[12] In assessing these components' efforts, we collected a non-generalizable sample of training and awareness documents and the most recent security assessments from select DOD components with security responsibilities. We reviewed these documents to assess whether they addressed security risks related to the digital profile. We also interviewed officials from the components to discuss ongoing actions to address and reduce risks relating to information about DOD and its personnel being publicly accessible. Further details on our scope and methodology can be found in appendix I.

We conducted this performance audit from May 2024 to October 2025 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.

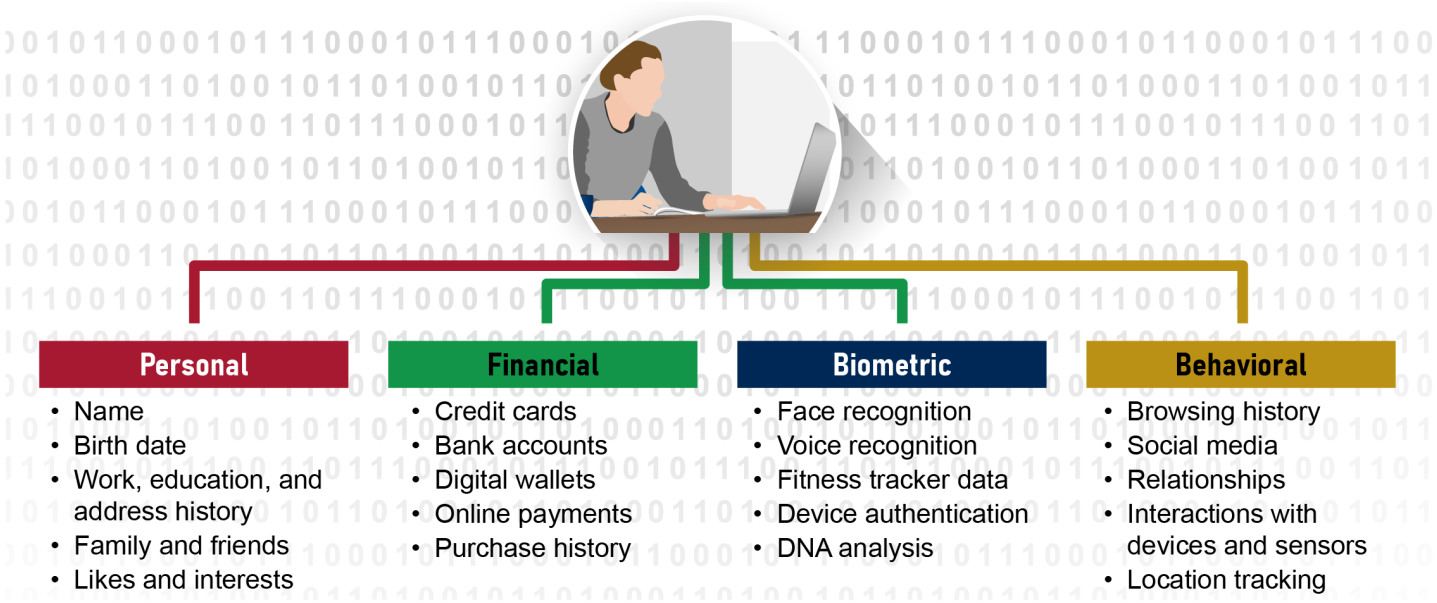
[12]For purposes of this report, 'military services' includes the Army, Air Force, Marine Corps, Navy, and Space Force.

Background

Development of DOD and Personnel Digital Profiles

Throughout the day, people—including DOD service members, civilian employees, contractors, and family members— knowingly or unknowingly leave behind sensitive information through digital activity (see fig. 1).

Figure 1: Types of Sensitive Information (Un)knowingly Traceable Through Digital Activity



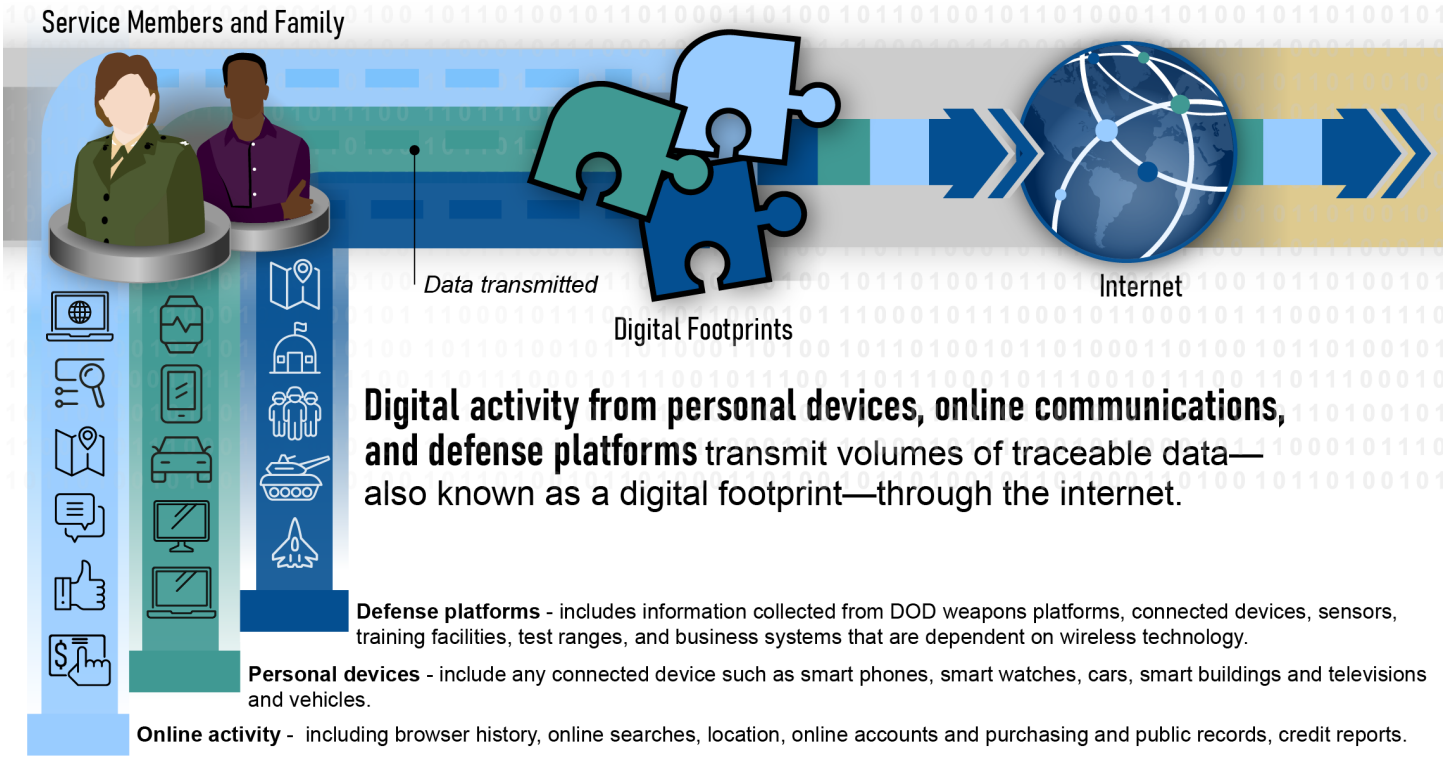
Sources: Department of Defense Identity Awareness, Protection, and Management Guide, GAO (illustrations). | GAO-26-107492

Digital activity from military personnel using personal and government devices (e.g., computers, tablets, and phones) and interacting online with websites, search engines, applications, and software programs generate volumes of traceable data about them and potentially those in proximity. In addition, defense platforms (e.g., weapon platforms, connected devices, sensors, training facilities, test ranges, and business systems) depending on wireless technology can generate data. For example, ships, aircraft, and ground vehicles are equipped with technology that communicates traffic details such as routes, position, and speed. All this digital activity generates volumes of traceable data—also known as a digital footprint.

Digital footprints can be knowingly or unknowingly collected through a variety of technologies and transmitted through the internet. These technologies include cookies and permissions that track online behavior;

telemetry technology that monitors precise locations (i.e., geolocation); sensing technology (e.g., Internet of Things sensors and wearables) that collect data from various environments and movements; and advertising technology that track and leverage geolocation data to create highly targeted, location-based advertising. Figure 2 depicts the typical data flow, beginning with the range of digital activities where digital footprints are generated and transmitted through the internet.

Figure 2: Digital Activity Generates Digital Footprints That Are Transmitted Through the Internet

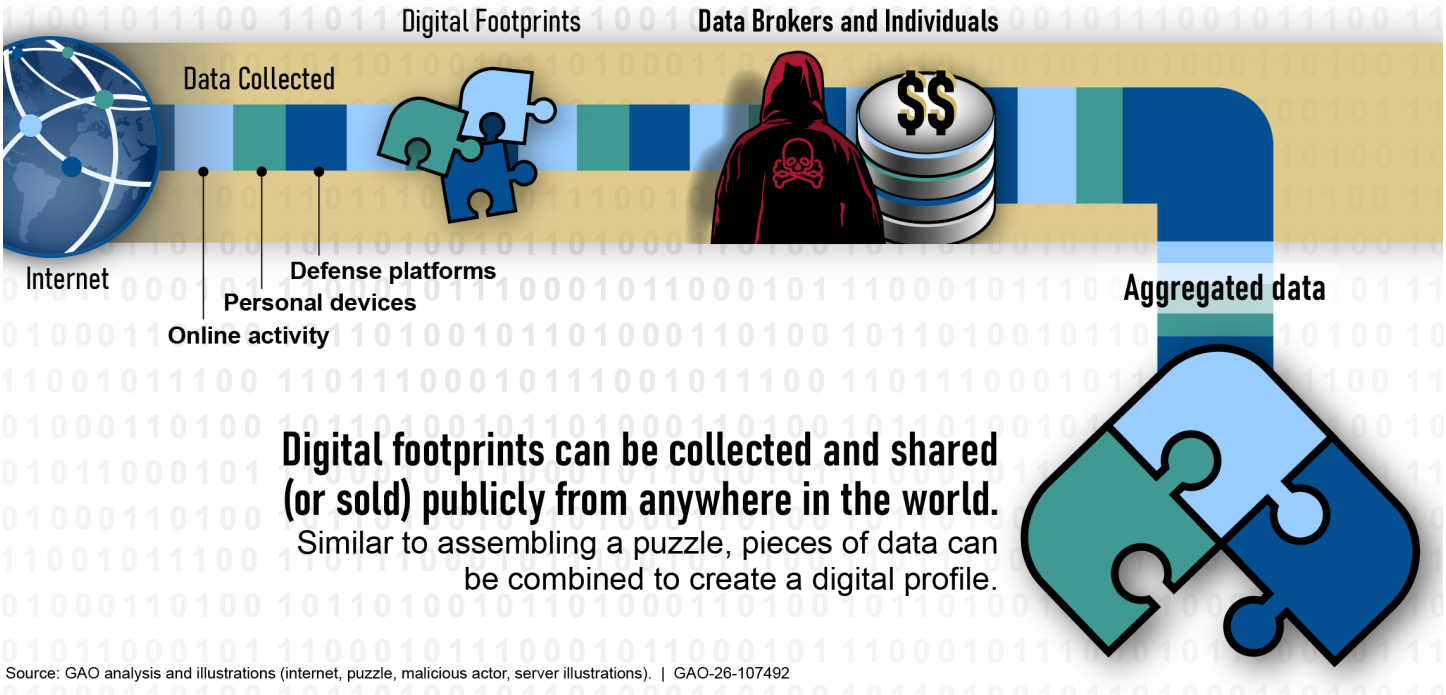


Sources: GAO analysis and illustrations (service member/family, puzzle pieces, background and internet illustrations); motorama/stock.adobe.com (all other icons). | GAO-26-107492

Once transmitted through the internet, digital footprints can be collected and shared (or sold) publicly from anywhere in the world. While a single footprint may seem insignificant (because that single data point is not considered sensitive or classified), when tied to other sources, multiple footprints can create a digital profile. This aggregation of information, no matter how small and seemingly insignificant, over time develops a detailed profile and can reveal potentially sensitive or classified

information (i.e., actions, interests, and vulnerabilities) that was not initially apparent, as shown in figure 3.

Figure 3: Digital Footprints Are Collected from the Internet and Can Be Aggregated into a Digital Profile



Source: GAO analysis and illustrations (internet, puzzle, malicious actor, server illustrations). | GAO-26-107492

Emerging technological capabilities (such as artificial intelligence, machine learning, and data mining) have the potential to advance the continued aggregation and analysis of data on individuals' personal and professional lives. These technologies enhance the speed, accuracy, and ability to predict behavior across large data sets, but they also introduce a number of risks to DOD. Those risks include counterintelligence, force protection, safety and security of family members, insider threat, mission assurance, OPSEC, and program protection.

DOD Responsibilities Relating to the Digital Profile

DOD has senior-levels officials within OSD that oversee various security areas:

- Under Secretary of Defense for Intelligence and Security establishes and oversees the implementation of policies and procedures for the

conduct of DOD counterintelligence, insider threat, OPSEC, and program protection.[13]

- Under Secretary of Defense for Policy establishes and oversees the implementation of policies and procedures for DOD mission assurance and anti-terrorism, which includes force protection.[14]
- Under Secretary of Defense for Research and Engineering establishes policies for development and approval of systems engineering plans and program protection plans, among other things.[15]
- Assistant to the Secretary of Defense for Public Affairs acts as the sole authority for releasing to news media representatives official DOD information and visual information materials, including press releases. DOD guidance states that information will be withheld only when disclosure would adversely affect national security, threaten the safety or privacy of service members, or if otherwise authorized by statute or regulation.[16]
- DOD Chief Information Officer develops the department's cybersecurity policy and guidance.[17]

DOD components are responsible for implementing DOD issuances to protect information, personnel, equipment, and operations. More specifically:

- Military departments and DOD components conduct OPSEC assessments; delegate responsibilities for mission assurance assessments; and assess appropriate classification of critical program

[13]DOD Directive 5143.01, *Under Secretary of Defense for Intelligence and Security (USD(I&S))* (Oct. 24, 2014) (incorporating change 2, effective Apr. 6, 2020).

[14]DOD Directive 5111.01, *Under Secretary of Defense for Policy (USD(P))* (June 23, 2020); and DOD Instruction 2000.12, *DOD Antiterrorism Support to Force Protection* (June 11, 2025).

[15]DOD Directive 5137.02, *Under Secretary of Defense for Research and Engineering (USD (R&E))* (July 15, 2020).

[16]DOD Directive 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))* (Aug. 7, 2017).

[17]DOD Directive 5144.02, *DOD Chief Information Officer (DOD CIO)* (Nov. 21, 2014) (incorporating change 1, effective Sept. 19, 2017).

information. Additionally, military departments and DOD components are to provide training to educate their personnel.[18]

- Defense Counterintelligence and Security Agency establishes security education, training, certification, and professional development programs.[19]

Defense Security Enterprise

The Defense Security Enterprise is a system of organizations, infrastructures, and measures (including policies, processes, procedures, and products) intended to safeguard DOD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system comprises personnel, physical, industrial, information, and operations security, as well as special access program security policy, critical program protection, and security training. The Defense Security Enterprise framework must align with and be informed by other DOD security-related functions such as counterintelligence, force protection, insider threat, and mission assurance.[20]

[18]DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program* (June 20, 2012) (incorporating change 2, effective Aug. 20, 2020); DOD Directive 3020.40, *Mission Assurance (MA)* (Nov. 29, 2016) (incorporating change 1, effective Sept. 11, 2018); and DOD Instruction 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)* (May 28, 2015) (incorporating change 3, effective Oct. 1, 2020).

[19]DOD Directive 5105.42, *Defense Counterintelligence and Security Agency* (Jan. 16, 2025).

[20]Since the scope of this review was on data or information that was publicly accessible, we did not focus on security areas that primarily focus on protecting information within DOD's systems and facilities (e.g., information security, cybersecurity, and physical protection). However, DOD data knowingly or unknowingly leaked outside of DOD's systems and facilities into the public can provide critical information in an otherwise incomplete profile of DOD operations, units, personnel, and family members.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

Force protection: Preventive measures taken to mitigate hostile actions against Department of Defense (DOD) personnel (including family members), resources, facilities, and critical information.

Insider threat: A threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of DOD and knowingly or unknowingly commits an act in contravention of law or policy that resulted in or might result in harm through the loss or degradation of government or company information, resources, or capabilities, or a destructive act, which may include physical harm to oneself or another.

Mission assurance: A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains critical to the execution of DOD mission-essential functions in any operating environment or condition.

Operations security: An activity that identifies and controls critical information and indicators of friendly force actions.

Critical program information protection: U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Source: GAO analysis of DOD documents. | GAO-26-107492

DOD has established policies, procedures, and guidance to help defend mission-critical security areas—such as DOD Directive 5200.43, *Management of the Defense Security Enterprise*.[21] Among other things, this directive establishes the Defense Security Enterprise Executive Committee. This committee is to provide interdisciplinary perspectives to strengthen the department's security posture through strategic administration and policy coordination. Specifically, is to advise the Under Secretary of Defense for Intelligence and Security on security and training; provide recommendations on key policy decisions and on opportunities for standardization and improved effectiveness and efficiency; and facilitate coordination of policies across security areas, among other things.[22]

This cross-functional governance body is chaired by the Defense Security Executive—the official under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security. The committee includes stakeholders from across the department— the Under Secretary of Defense for Intelligence and Security, Under Secretary of Defense for Policy, DOD Chief Information Officer, and DOD General Counsel.

[21]DOD Directive 5200.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 3, effective July 14, 2020).

[22]While these responsibilities are not specific to the protection of publicly accessible digital data on DOD personnel and operations, this committee provides a forum for identification, documentation, and dissemination of best practices for security risk management.

Public Accessibility of Digital Data Poses Security, Privacy, and Safety Risks to DOD Personnel and Operations

Malicious Actors Can Exploit Data Through Various Digital Activities

DOD officials and documents identify the public accessibility of digital data as a real and growing threat that poses risks to personnel privacy and safety, mission success, and national security. According to officials from the OSD offices and the select DOD components we interviewed, digital footprint data or an aggregated digital profile poses risks to the privacy and safety of service members and their family members.[23] For example, in June 2021, a senior DOD official testified that digital footprints could pose a risk to new recruits who may later serve in sensitive or covert roles by exposing their identities, thus compromising broader counterintelligence and surveillance efforts.[24] Similarly, a National Security Agency official told us that the digital footprint and the potential for an aggregated digital profile creates vulnerability in the "cog of the machine." The official expressed that if the cog (i.e., personnel) is vulnerable, the mission will also be vulnerable.

According to DOD guidance, this risk can be attributed to the rapid advancement and global use of communications systems and information technology, easily obtainable technical collection tools, and growing use of the internet and various social and mass media outlets.[25] While DOD can provide guidance on how to limit the amount and type of information that is transmitted to the public (as discussed later in the report), DOD has limited control over the extent to which others—including data brokers and malicious actors—collect, use, and exploit this information.

[23]For this review, we focused on actions taken by DOD organizations with security responsibilities, including all of the military services, U.S. Cyber Command, U.S. Special Operations Command, National Security Agency, Defense Counterintelligence and Security Agency, and Defense Intelligence Agency.

[24]*Fiscal 2022 Defense Intelligence Enterprise Posture Hearing*, 117th Cong. (2021) 20-21 (statement of Under Secretary of Defense for Intelligence and Security, U.S. Department of Defense, Ronald Moultrie).

[25]Joint Chiefs of Staff, Joint Pub. 3-55, *Joint Operations Security* (Feb. 20, 2025).

- **Data brokers** collect, aggregate, and sell personal information on individuals to third parties for the purposes of marketing, advertising, law enforcement, enterprise security, criminal justice, and recruitment, among other areas. According to a U.S. Cyber Command briefing, the activities of third-party data brokers have real-world implications for foreign intelligence gathering, targeted phishing attacks of military personnel, stalking, and harassment, among other things. In April 2023, a Duke University researcher testified that data brokers threatened U.S. national security and noted that their research team was able to purchase personally identifiable information on military service members from data brokers for as low as 12.5 cents per member.[26] The threat of a malicious actor exploiting these data poses privacy, security, and safety risks to DOD personnel—including family members. In January 2025, the Department of Justice issued a final rule to implement an executive order that prohibits and restricts certain data transactions of bulk sensitive personal data and government-related data with certain countries or persons due to national security risks.[27] According to officials from the Office of the Under Secretary of Defense for Policy, this order will not, however, restrict the collection or sale of data domestically or internationally to foreign entities not associated with countries of concern.
- **Malicious actors** (e.g., adversaries, such as hostile nation-states and terrorists or criminals) can leverage digital profile data over time as intelligence to establish patterns or better understand military intent and capabilities.[28] For example, DOD's joint doctrine on OPSEC describes how an adversary can quickly search multiple sources (e.g., social networking sites, geotags, website data) and derive indicators necessary to counter a mission or operation.[29] Similarly, a 2011 Defense Intelligence Agency report described how a military enthusiast used social media to share and discuss military personnel

[26]Sherman, Barton, Klein, Kruse, and Srinivasan, *Data Brokers.*

[27]28 C.F.R § 202. The executive order was issued by the President in February 2024. Exec. Order No. 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15421 (Mar. 1, 2024).

[28]Malicious actors are individuals or groups that seek to harm organizations or individuals through deliberate, often covert, actions, including cyberattacks, surveillance, or information theft. Malicious actors may include criminal groups, nation-state actors, hacktivists, or insiders. Criminals are a subset of malicious actors whose activities violate criminal statutes and are prosecutable under federal law, such as cybercriminals engaged in fraud, identity theft, or unauthorized system access.

[29]Joint Pub. 3-55.

movements and operational locations, which revealed details of U.S. military air operations in Libya. This information could be exploited by an adversary.

Notional Threat Scenarios Illustrate Risks Stemming from Public Accessibility of Digital Data

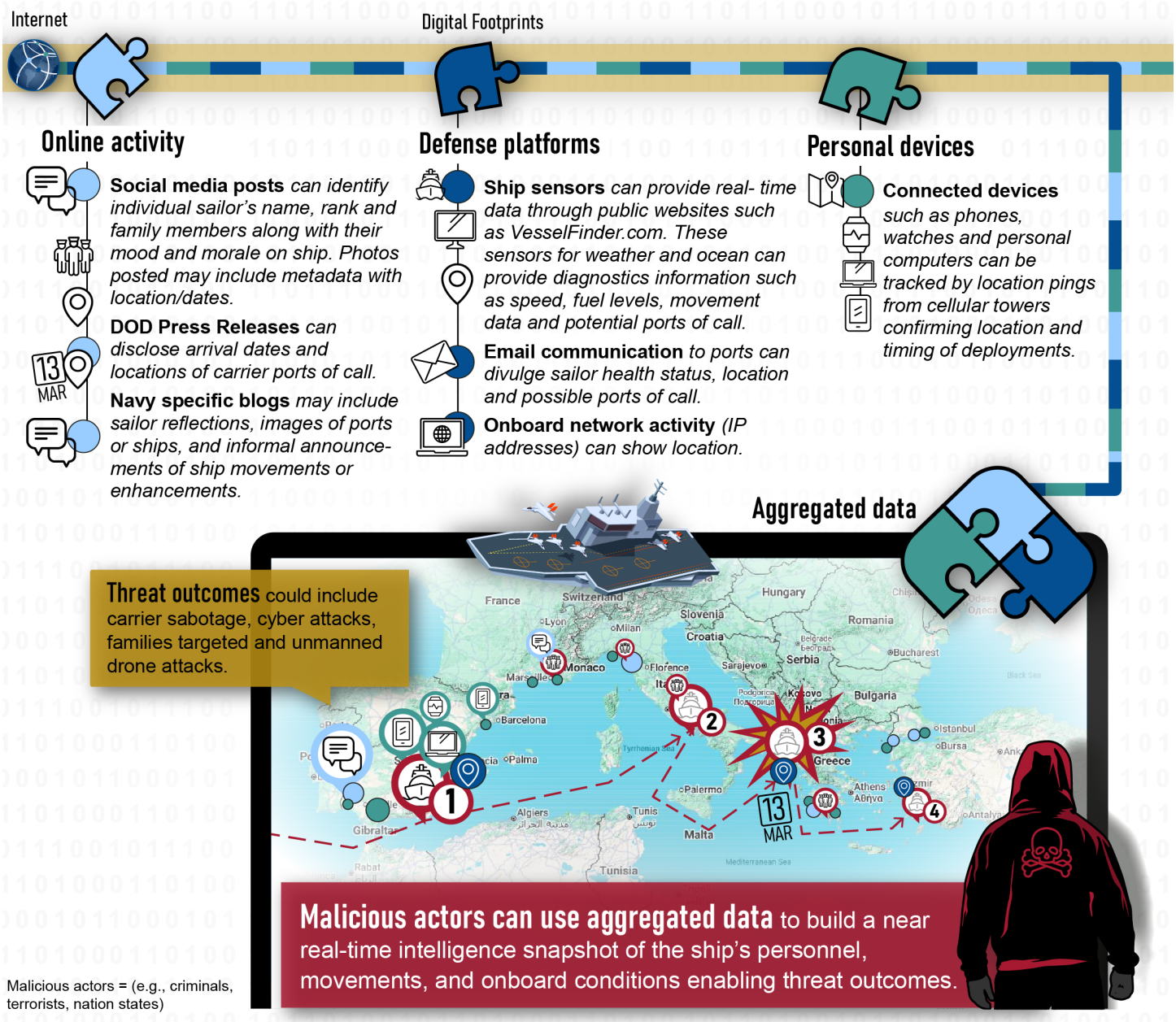
We developed notional threat scenarios that exemplify how the public accessibility of information about DOD operations and its personnel introduces risks across multiple security areas. We discuss risks in four areas—operations, military capabilities, personnel and their families, and leadership—along with illustrative information graphics.[30] Officials from the Office of the Under Secretary of Defense for Intelligence and Security agreed that our scenarios were both realistic and plausible, and that the aggregation of digital footprints could have significant security implications. They told us they have, in fact, seen family members targeted during deployments and acknowledged its adverse impact on mission. Further, they stated that digital profiles as presented in our scenarios have significant security implications for DOD's mission and the physical safety of service members and their families.

Risk to Operations

The first notional threat scenario, as shown in figure 4, illustrates how aggregated information—including DOD press releases, news sources, online activity, social media posts, and ship coordinates—could be used by malicious actors to disrupt naval carrier operations.

[30]In using notional scenarios that would allow this report to be publicly accessible yet DOD officials would acknowledge as security concerns, we either collected evidence or leveraged third-party reports to demonstrate that the information sources noted provide the type of identifiable information in the scenarios. We discussed the plausibility and impact of these notional threat scenarios with officials from the Office of the Under Secretary of Defense for Intelligence and Security.

Figure 4: Notional Digital Profile Threat Scenario Disrupting Aircraft Carrier Operations



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

For example, a news article may publicly announce an aircraft carrier's deployment and include the number of personnel aboard, the vessel's capabilities, and the recent installation of commercial Wi-Fi for sailors. A subsequent press release issued by the Navy's public affairs office may confirm the aircraft carrier's arrival to and departure from scheduled ports. Such announcements could be supplemented by publicly accessible tracking data. Our investigators found real-time tracking information in online forums and posted coordinates from online fleet and marine tracking websites. We also found social networking support groups created by family members of deployed sailors sharing details about communications (i.e., photos and messages); several family members shared photos and posts about visiting the port and seeing their sailors during the holiday season. Further, a private social media group was identified in which the aircraft carrier's public affairs team published petty officer promotions, including ranks and photos; information about aircraft assignments and strike groups; and the composition of squadrons.

Digital footprints, when aggregated, can form a comprehensive profile that adversaries may exploit to disrupt carrier operations and target personnel and their families through social engineering. For example, malicious actors could link sailors to their immediate family members from social media posts. Once this relationship is established, the malicious actor could begin compiling additional photos and information that may provide deeper insights, such as the exact location based on the geolocation or metadata, that may lead to a personal residence and behavioral patterns (e.g., the number of times or frequency of performing a particular activity).

This type of information creates the potential for blackmail or coercive tactics. For example, individuals may be stalked, threatened, or harassed in exchange for military information. Additionally, a malicious actor could use information on the ship's movements from official press releases in combination with a real-time ship tracking website to project the route of the vessel. This could enable the vessel to be targeted by uncrewed systems or sabotaged while docked. This type of profiling introduces risks across multiple security and privacy areas, including force protection, mission assurance, OPSEC, and program protection.

Risk to Military Capabilities

The second notional threat scenario, as shown in figure 5, illustrates how aggregated information could expose DOD-related training materials and military capabilities.

Figure 5: Notional Digital Profile Threat Scenario Exposing DOD-Related Training Materials and Military Capabilities

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

Sensitive information about military personnel and operations can be found online across multiple social media sites, news articles, and online forums on the surface and dark web. In 2018, cybersecurity researchers identified hacker information on the dark web for sale that included sensitive military data: course books and military personnel related to a piece of military equipment, military manuals on tank platoon operations, and improvised explosive device training. Furthermore, our investigators found photos of a military facility's training slides posted in an online military forum. The training slides included information about a prior international military exercise that revealed strategic partnerships. Additionally, a social media post depicted posts and videos of an internal military jump training, including live military flights, internal views of military aircraft, as well as equipment used by paratroopers. Based on the photos of the equipment, the applicable user manuals could be purchased from the dark web.

These digital footprints, when aggregated, create a comprehensive profile that a malicious actor could exploit to undermine DOD military operations. For example, a malicious actor could leverage information about military equipment (including hardware and software systems) from training materials, internal aircraft layouts, and photos from training exercises. Specifically, photos may reveal equipment or aircraft modifications, and the accompanying manual may provide detailed instructions on how to apply the modification or perform maintenance. A malicious actor could use this information to clone products, duplicate military capabilities, or identify and exploit vulnerabilities. Similarly, photos of the paratrooper in the international military exercise may reveal unique markings that could be critical indicators of overall combined military planning and operations. This type of profiling introduces risks across multiple security and privacy areas, including force protection, mission assurance, OPSEC, and program protection.

Risk to Personnel and Their Families

As referenced previously, according to a 2023 Duke research study, personally identifiable information on military service members from data brokers could be purchased for as low as 12.5 cents per member. These data may include information such as names, ranks, unit affiliations, and family details to identify individuals involved in sensitive operations.[31] Our investigation found that data brokers were selling alleged personal details

[31]Sherman, Barton, Klein, Kruse, and Srinivasan, *Data Brokers.*

(e.g., title, name, personal emails, and phone numbers) of service members across surface, deep, and dark web platforms.

Surface web is the portion of the internet that is easily accessible and searchable. Examples include social media platforms, online forums and blogs, business websites, and public databases.

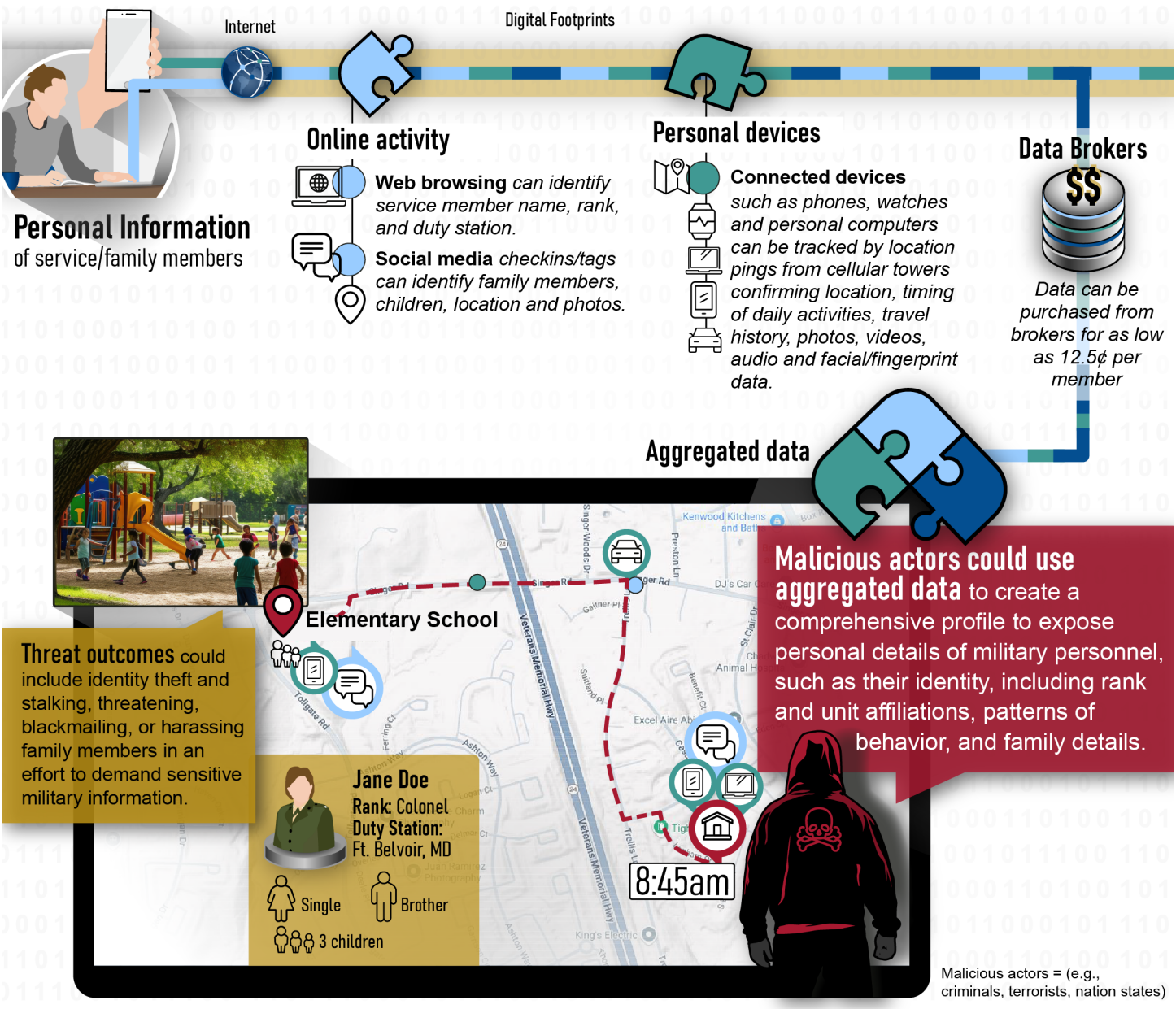
Deep web is the portion of the internet that is accessible but not easily searchable. These websites cannot be indexed by search engines. Examples include databases, academic journals, login-protected websites, private networks, and personal social media accounts.

Dark web is the portion of the internet that is hidden. The dark web can only be accessed using specialized software and is not searchable. It is where the internet's illegal activities reside.

Source: GAO analysis. | GAO-26-107492

The third notional threat scenario, as shown in figure 6, illustrates how aggregated information purchased from data brokers or collected from the web could be used to identify and harm DOD personnel and their families.

Figure 6: Notional Digital Profile Threat Scenario Exposing DOD Personnel Data



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

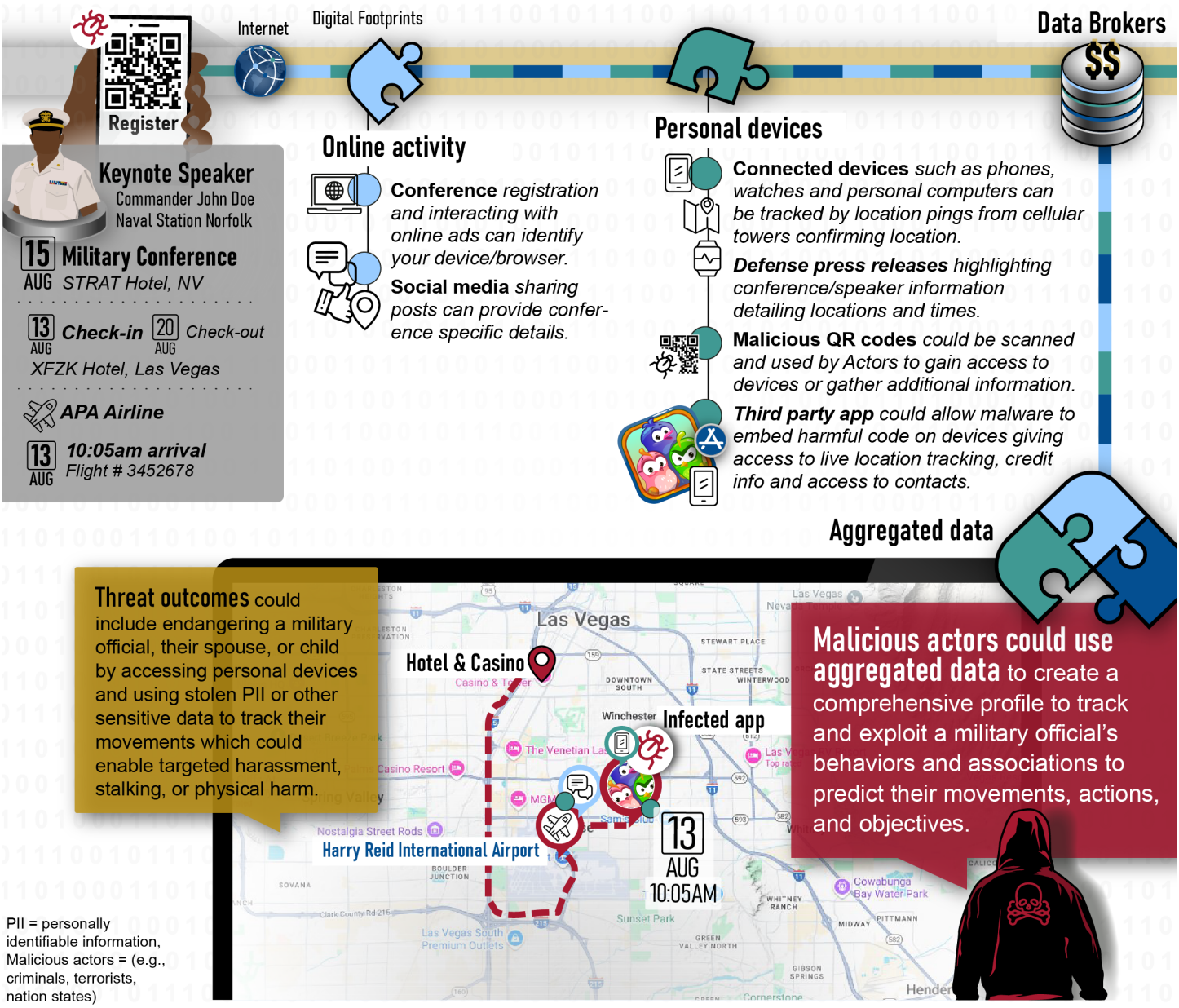
For example, our investigators found a DOD public affairs office's press release that identified and pictured a service member who completed urban sniper training. Using this identifier, the service member's data could be purchased on the dark web and include identifiable contact information, demographic details, rank, and unit affiliation. With contact information, additional research could be conducted to identify family associations, such as the names of parents, siblings, spouses, and even children. Using an identifier contained in a DOD public affairs office's press release, our investigators identified photos of family members and the service member's date of birth.

These digital footprints, when aggregated, create a comprehensive profile that adversaries could exploit to harm DOD personnel and their families. Specifically, a malicious actor could use this information to stalk, threaten, and harass the service member or their family members to obtain sensitive military information. Beyond that, a malicious actor could use information about school locations and after-school activities to target the service member's child when they are most vulnerable, using details about the family to gain trust and potentially abduct the child. This level of surveillance of a loved one could be leveraged to exploit that service member, undermine their credibility among subordinates, and gather additional intelligence to disrupt military operations. This type of profiling introduces risks across multiple security and privacy areas, including force protection, insider threat, and OPSEC.

Risk to Leadership

The fourth notional threat scenario illustrates how aggregated information could be used to reveal a military official's daily routines and relationships to predict their future actions and endanger military leadership. This scenario centers around a military conference. It highlights how various digital footprints, such as travel details, the presence of family members, interactions with other military personnel, public announcements, and the use of mobile applications, can be used to form a comprehensive digital profile of the official. (see fig. 7)

Figure 7: Notional Digital Profile Threat Scenario Endangering Military Leadership



Sources: GAO analysis and illustrations (naval officer, hand/phone, data broker icon, malicious actor, internet, puzzle, monitor, service member illustrations), lilu330/stock.adobe.com (kids app icon), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-107492

For example, a press release issued by the Navy's public affairs team announces that a military official will serve as the keynote speaker at a high-profile military conference focused on emerging technologies and strategic planning. The release includes their name and title, and the conference location and dates. Upon arrival at the conference venue, the official engages with a socially engineered QR-code for conference registration and uses a digital wallet to pay for parking. Additionally, the official's spouse confirms arrival to the conference by sharing a photo on social media with their child from the hotel lobby that includes other military panelists in the background. Before the trip, the official downloaded on their phone an unverified third-party mobile gaming application for their child to use during travel and while the official attended the conference. However, the application had extensive permissions and was able to access sensitive information and functions on the official's phone, including location, credit card, contacts, camera and microphone, SMS messages, storage, and network access.

These digital footprints, when aggregated, create a comprehensive profile that adversaries could exploit to track the senior official's behaviors and associations to predict their movements, actions, and objectives. Specifically, the press release identifies the official as high-profile. When combined with access permissions from the third-party gaming application, this could reveal the official's associations and contacts. Further, the official's daily routine may be known—including behavioral patterns (e.g., routine coffee stops), travel history, routes taken, and time spent in an area.

In addition, the QR code could direct the official to a fraudulent website that could steal personal or financial information or install malware that embeds harmful code on their phone. This can allow a malicious actor to gain unauthorized access and collect the official's personally identifiable information, nonpublic DOD information not approved for public release, and other sensitive data, all without the official's consent or knowledge. Further, the spouse's social media check-in and photo includes geolocation data that reveals the real-time location of the family. A malicious actor could use this combined pool of information to inflict physical harm on the official or the spouse and child to gain further intelligence. This type of profiling introduces risks across multiple security and privacy areas, including counterintelligence, insider threat, mission assurance, and OPSEC.

OSD Has Not Fully Taken Action to Reduce Risks of Publicly Accessible Digital Data

As presented in our scenarios above, digital profile risks could compromise critical information, jeopardize the mission and safety of DOD personnel, and ultimately undermine DOD's ability to achieve its overall mission to defend and protect the United States—including its operational and tactical goals. DOD guidance generally requires OSD offices to manage the six select security areas by issuing policy and guidance; and coordinating and collaborating with each other on security matters. However, OSD has not consistently issued policies and guidance to address the digital profile threat. Furthermore, OSD has limited coordination and collaboration across the existing security areas—specifically, counterintelligence, force protection, insider threat, mission assurance, OPSEC, and program protection—to reduce risks from the digital profile.

OSD Has Issued Policies and Guidance to Address Digital Profile Risks to Varying Degrees

DOD guidance generally requires OSD offices to develop policies and prescribe guidance that implement procedures, integrate strategies, and provide oversight of security areas.

Three of the five OSD offices we reviewed issued policies or guidance to address the risks of information about DOD and its personnel being publicly accessible to varying degrees. Specifically, the Offices of the Under Secretary of Defense for Intelligence and Security, DOD Chief Information Officer, and Assistant to the Secretary of Defense for Public Affairs have issued policies or guidance focused on two types of digital profile threats—digital ecosystems (i.e., applications, websites, or devices with data collection capabilities) and social networking.

- Under Secretary of Defense for Intelligence and Security issued a policy providing digital personal protection and protective intelligence measures as necessary if potential access and exploitation of accessible information threaten the security of an official designated as high-risk personnel and the performance of their official duties.[32]

[32]DOD Instruction O-2000.22, *Designation and Physical Protection of DOD High-Risk Personnel* (June 19, 2014) (incorporating change 2, effective Nov. 2, 2023). Digital persona protection is protection against unauthorized access to and exploitation of personal and official information that could threaten high-risk personnel and their performance as well as potential countermeasures and protection requirements for high-risk personnel. In 2016, a law was enacted that authorized the Secretary of Defense to provide cyber protection support for the personal technology devices of certain at-risk DOD personnel, for example, personnel determined to be highly vulnerable to cyberattacks and hostile information collection activities. Pub. L. No. 114–328, §1645 (Dec. 23, 2016).

- DOD Chief Information Officer issued a policy prohibiting military personnel, civilian employees, and contractors from using personal email or other nonofficial accounts to exchange official information.[33]
- Assistant to the Secretary of Defense for Public Affairs issued a policy providing core principles and guidance on social media use, along with guidance for social media records management.[34]

However, gaps remain in how DOD's policies and guidance address security risks associated with the public accessibility of digital information about DOD and its personnel. Specifically, these policies and guidance are narrowly focused (i.e., do not fully address the range of potential risks from digital information about DOD and its personnel being publicly accessible), do not include all relevant stakeholders, and do not include all relevant security areas.

- **Policies and guidance are narrowly focused.** Some existing policies and guidance are narrowly focused and thereby do not fully address the range of potential risks from digital information about DOD and its personnel being publicly accessible. For example, DOD Instruction 8170.01, *Online Information Management and Electronic Messaging*, issued by DOD Chief Information Officer, establishes policy and procedures for online information management and electronic messaging.[35] However, the instruction does not establish a policy or instruct its components or personnel to implement any security procedures that address the risk from digital ecosystems (i.e., applications, websites, or devices with data collection capabilities); threats to identity; or defense platforms.

  Similarly, the DOD Chief Information Officer issued a memorandum that prohibits the use of personal email accounts, messaging systems, or other nonpublic DOD information systems in conducting official business involving controlled unclassified information.[36] The memorandum provides direction on the requirements and proper safeguards for the use of mobile applications on unclassified government-owned devices (e.g., smartphones or tablets). However,

[33]DOD Instruction 8170.01, *Online Information Management and Electronic Messaging* (Jan. 2, 2019) (incorporating change 2, effective Mar. 12, 2025).

[34]DOD Instruction 5400.17, *Official Use of Social Media for Public Affairs Purposes* (Aug. 12, 2022) (incorporating change 2, effective Feb. 14, 2025).

[35]DOD Instruction 8170.01.

[36]DOD Chief Information Officer, *Use of Unclassified Mobile Applications in Department of Defense* (Oct. 6, 2023).

the memorandum does not address the use of personal email accounts or messaging systems on personal devices in conducting unofficial business involving unclassified information—such as official travel hotel reservations, military travel orders, or social media—which could present comparable risks, if aggregated. As discussed earlier in this report, digital activity from personal and government devices (e.g., computers, tablets, and phones) and online communications generate volumes of traceable data about the military personnel and potentially about those in proximity. In addition, defense platforms depending on wireless technology can generate data, such as traffic details that provide routes, position, and speed.

- **Policies do not include all relevant stakeholders.** Existing policies related to the use of social media do not include or acknowledge the involvement of stakeholders responsible for privacy, safety, and security risks. Specifically, DOD Instruction 5400.17, *Official Use of Social Media for Public Affairs Purposes*, issued by the Office of the Assistant to the Secretary of Defense for Public Affairs, does not mention the Office of the Under Secretary of Defense for Intelligence and Security.[37] However, the Under Secretary of Defense for Intelligence and Security's office is responsible for establishing and overseeing the implementation of policies and procedures for the conduct of OPSEC, among other things. According to DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program*, the Assistant to the Secretary of Defense for Public Affairs is responsible for developing policy and guidance to ensure OPSEC is incorporated into Public Affairs's process for releasing information.[38] As the authority on the release of information, Public Affairs is often the first line of defense in identifying the aggregation of risks when reviewing information for public release. However, an OPSEC program manager would determine how to reduce the risk of aggregation, thus creating the need for coordination and collaboration.
- **Policies and guidance do not include all relevant security areas.** Two OSD offices that have policy and oversight responsibilities associated with security areas had not issued policy or guidance addressing security risks associated with the public accessibility of digital information about DOD and its personnel. Specifically, the Offices of the Under Secretary of Defense for Policy (responsible for force protection and mission assurance) and the Under Secretary of

[37]DOD Instruction 5400.17.

[38]DOD Directive 5205.02E.

Defense for Research and Engineering (responsible for program protection) do not have any policies or guidance that identify actions DOD personnel should take to reduce risks associated with the public accessibility of digital information.

OSD Has Coordinated on Policies and Guidance but Not Fully Collaborated to Address Digital Profile Risks

DOD guidance generally requires OSD offices to coordinate on policy and guidance development and to collaborate with each other on security matters through working groups or security forums.

According to officials from the OSD offices, the five OSD offices we reviewed coordinated with one another when they developed and issued policies and guidance addressing the digital profile threat. For example, the Offices of the Under Secretary of Defense for Intelligence and Security and DOD Chief Information Officer coordinated to issue guidance on the use of geolocation-capable devices, applications, and services. According to OSD officials, they coordinated on the policy and guidance by sending draft copies to other OSD and DOD components for review.

However, OSD offices have not collaborated to address risks associated with the digital profile—such as through working groups. When we spoke to OSD officials about efforts to reduce risks associated with the digital profile, they often deferred responsibility to other organizations and cited a lack of equity in the issue. For example, a mission assurance official from the Office of the Under Secretary of Defense for Policy did not understand how digital footprints could pose some vulnerability that could rise to the level of mission failure. The official thus deferred responsibility to the Office of the DOD Chief Information Officer. However, as shown earlier in the report, publicly accessible data that are aggregated can identify mission assurance-related risks. When we discussed this topic with an official from the Office of the DOD Chief Information Officer, the official in turn deferred responsibility to the Office of the Under Secretary of Defense for Intelligence and Security. OSD officials acknowledged the need for a coherent risk management approach for the digital environment but stated that the department has deferred risk mitigation of the digital profile threat to the unit level—such as to a commanding officer preparing for a ship's departure.

OSD Needs to Leverage the Defense Security Enterprise Executive Committee to Reduce Risks

OSD officials acknowledged that the policies and guidance related to the digital profile threat do not fully address the range of potential risks of digital information about DOD and its personnel being publicly accessible. The officials stated they believe the department has limited authority to issue policy that controls the actions of DOD personnel and contractors outside of an operational area. The officials also acknowledged that while they had coordinated to review existing policies and guidance, they had not collaborated to address digital profile risks because they did not believe the digital profile threat and its associated risks aligned with the Secretary of Defense's priorities that were established in January 2025. The priorities focus on reviving the warrior ethos, restoring trust in the military, rebuilding military capabilities, and reestablishing deterrence by defending the homeland. However, OSD officials had not taken needed action to reduce risks of digital information before these priorities were established.

Recognizing that uncertainty can exist with evolving security risks, we asked OSD officials whether the Defense Security Enterprise Executive Committee had performed any review or assessment of existing security policies and guidance to identify gaps associated with risks in the digital environment. According to an official from the Office of the Under Secretary of Defense for Intelligence and Security, the executive committee meets quarterly but has not discussed the digital profile as a risk. Instead, the executive committee has been mostly focused on Trusted Workforce, an initiative to modernize U.S. government personnel vetting processes.

As discussed earlier in the report, the Defense Security Enterprise Executive Committee—a cross-functional governance body that includes stakeholders from across the department, including the General Counsel—is responsible for providing recommendations to the Under Secretary of Defense for Intelligence and Security on key policy decisions and on opportunities for standardization and improved effectiveness and efficiency; and for facilitating cross-functional security policy coordination.[39] Specifically, the executive committee can commission reviews and in-depth studies of security issues and make recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging

[39]DOD Directive 5200.43.

security challenges, such as those associated with risks in the digital environment.

In addition to conducting in-depth studies of security issues and making recommendations for developing or improving policies, the *Defense Security Enterprise Strategy* states that the executive committee should collaborate across traditional organizational boundaries to establish and measure Defense Security Enterprise strategic direction and provide cross-discipline perspectives to strengthen the department's security posture.[40] The strategy also states,

> In the face of evolving challenges, the Defense Security Enterprise must establish and implement a robust security framework to enable cooperation and collaboration across the enterprise. The Defense Security Enterprise must improve and elevate the security culture within the department and posture to maintain strategic and operational dominance against dynamic threats.

As a cross-functional governance body that includes stakeholders from across the department, including the General Counsel, the Defense Security Enterprise Executive Committee is well-positioned to lead an assessment with the Assistant Secretary of Defense for Public Affairs and OSD officials who oversee security areas that could be impacted by digital profiles. Until DOD leverages the Defense Security Enterprise's Executive Committee to assess DOD's existing security policies and guidance on the digital profile threat and recommend any appropriate updates to policy and guidance, the department will have difficulty in determining whether risks are being sufficiently managed within the boundaries of their legal authorities.

DOD Components' Actions for Reducing Risks of Public Accessibility of Digital Data Are Inconsistent

Most of the 10 DOD components we selected for our review raise awareness of and administer training on the digital profile and its associated risks.[41] However, this training does not consistently cover threats associated with digital profiles in security areas other than OPSEC. Furthermore, DOD components we reviewed have not consistently conducted assessments associated with the risks.

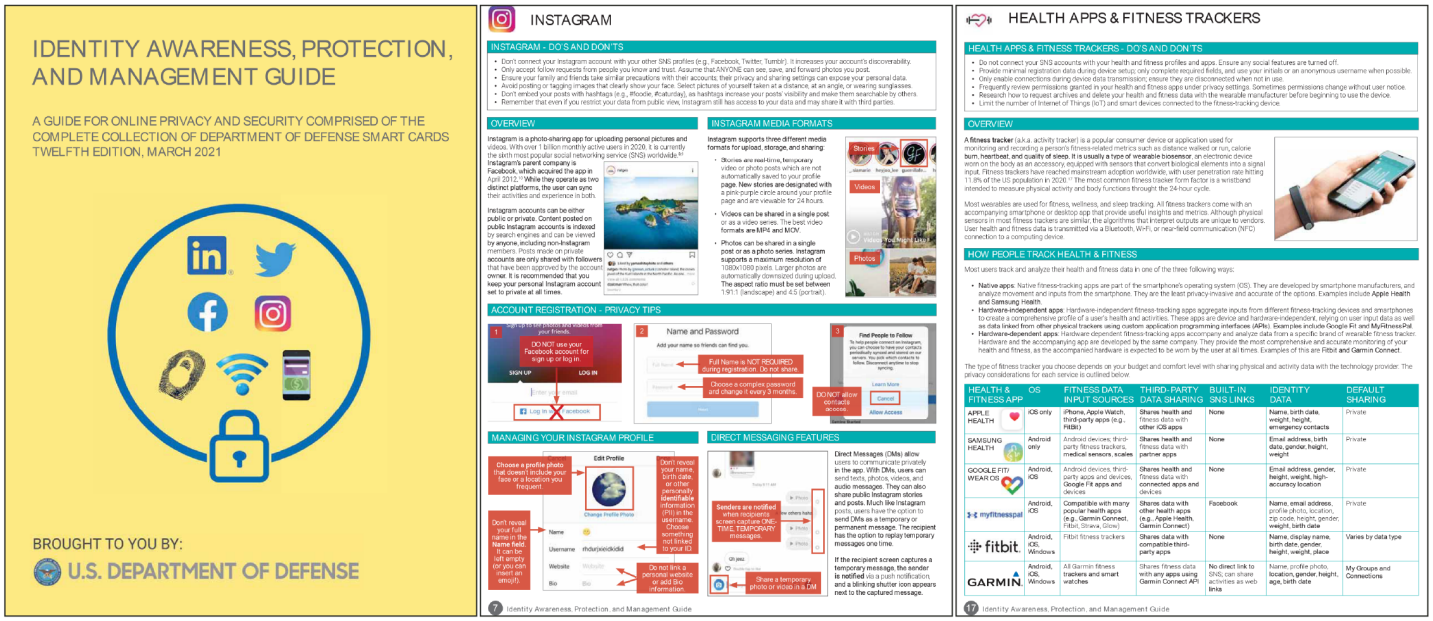
[40]Office of the Under Secretary of Defense for Intelligence and Security, *Defense Security Enterprise Strategy*.

[41]These components are the military services, U.S. Cyber Command, U.S. Special Operations Command, National Security Agency, Defense Counterintelligence and Security Agency, and Defense Intelligence Agency.

Most DOD Components Raise Awareness of Digital Profile Risks Through Multiple Efforts

In addition to formal training, seven of the 10 select components we reviewed provided examples of efforts to raise awareness about the digital profile and its associated risks, although awareness efforts are not required. In reviewing these examples, we found 59 percent (33 of 56) of the examples incorporated digital profile content by acknowledging the risks of digital information in the public, highlighting methods to counter digital profile risks, or a combination of the two. These awareness campaigns used posters, emails, and smart cards, among other things, as communication channels. For example, DOD issued an *Identity Awareness, Protection, and Management Guide* to help readers understand how to keep their identities private and secure online.[42] This collection of smart cards provide the tools, recommendations, and series of steps for implementing settings that maximize an individual's security in a variety of digital sources, such as Facebook, fitness trackers, online dating services, and smartphones (see fig. 8).

Figure 8: Example of Department of Defense's Smart Cards on Securing Digital Profiles



Source: DOD Identity Awareness, Protection, and Management Guide. | GAO-26-107492

[42]"*Identity Awareness, Protection, and Management Guide*", Washington, D.C., accessed September 22, 2025, https://www.odni.gov/files/NCSC/documents/campaign/DoD_IAPM_Guide_March_2021.pdf.

Additionally, DOD components have taken the following actions to understand and inform others about security risks associated with digital data in the public:

- **Identity management programs.** Some DOD components have begun creating identity management programs that protect the identities of certain personnel. For example, officials in an Army Counterintelligence Command told us the command has restructured their OPSEC and counterintelligence offices into a singular identity management program to enhance collaboration across teams as they manage risks posed by the digital profile threat.
- **Research efforts.** The Army Threat Systems Management Office has performed threat experiments that relate to the digital footprint. An official from this office told us these experiments led to the creation of teams assessing digital profiles for critical installations, missions, and programs/technologies. Specifically, the Threat Systems Management Office provides digital profiling services for Army units by request. The official described how a threat OPSEC team is using public information, commercial information, and data analysis tools to understand the digital signatures and profiles of Army units and programs. Similarly, the official stated the office's supply chain team focuses on reducing risk and vulnerabilities posed by public or commercial supply chain information that a malicious actor may target or collect for future exploitation.
- **Family readiness efforts.** DOD officials acknowledge the role of families in supporting OPSEC. As discussed earlier in our scenarios, malicious actors can target families to obtain sensitive military information about service members. For this reason, the military services have established family readiness groups, which are responsible for hosting outreach events and providing resources to educate families on OPSEC and the security implications of their digital activities. For example, the Marine Corps, U.S. Special Operations Command, and Defense Counterintelligence and Security Agency have developed guidance and training that incorporate best practices for identity management to educate family members on practicing good social media habits and on protecting themselves against threats to their identity.

Most DOD Components Administer Training on Digital Profile Risks Primarily Related to Operations Security

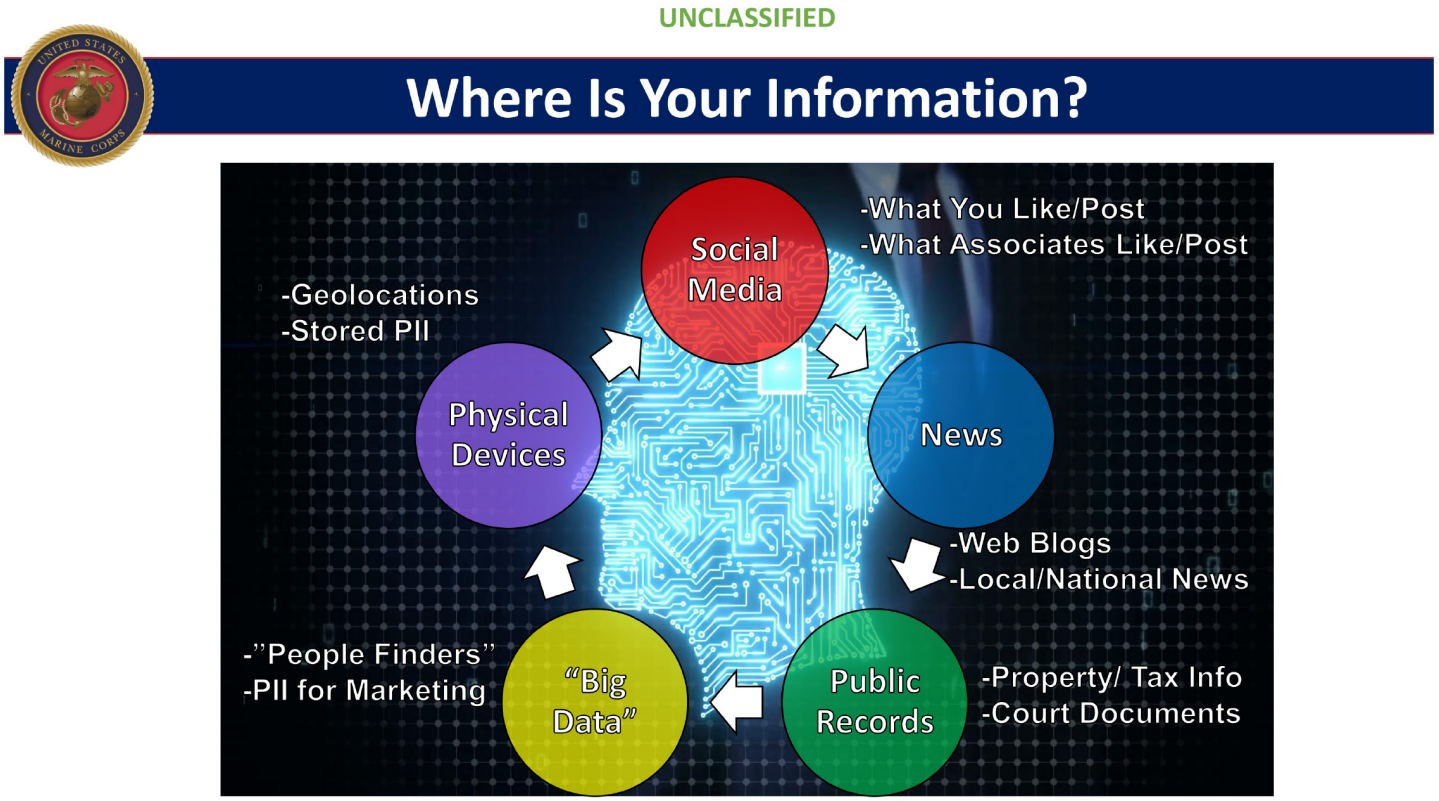
DOD guidance requires DOD components to develop and administer training on OPSEC, counterintelligence, and insider threat. DOD guidance on mission assurance, anti-terrorism/force protection and program protection also address training for certain personnel or under certain circumstances.[43]

Nine of the 10 select components provided evidence of the security training they offered to personnel in the areas of counterintelligence, force protection, mission assurance, and OPSEC. Specifically, 67 percent (24 of 36) of training documents provided to us included content on the digital profile; its associated risks, such as digital ecosystems (i.e., applications, websites, or devices with data collection capabilities), social networking services, social engineering scams, and information collected from defense platforms; and best practices for countering risks. For example:

- The Marine Corps's OPSEC training highlights the various places and ways by which a service member's information can exist, including public records, personal devices, and social networking sites, among other things (see fig. 9).

[43]DOD Directive 5205.02E; DOD Directive 5240.02, *Counterintelligence (CI)* (Mar. 17, 2015) (incorporating change 1, effective May 16, 2018); DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)* (May 17, 2011) (incorporating change 3, effective Aug. 31, 2020); DOD Instruction 5205.16, *The DOD Insider Threat Program* (Dec. 20, 2024); DOD Directive 3020.40; DOD Instruction 2000.12; and DOD Instruction 5200.39.

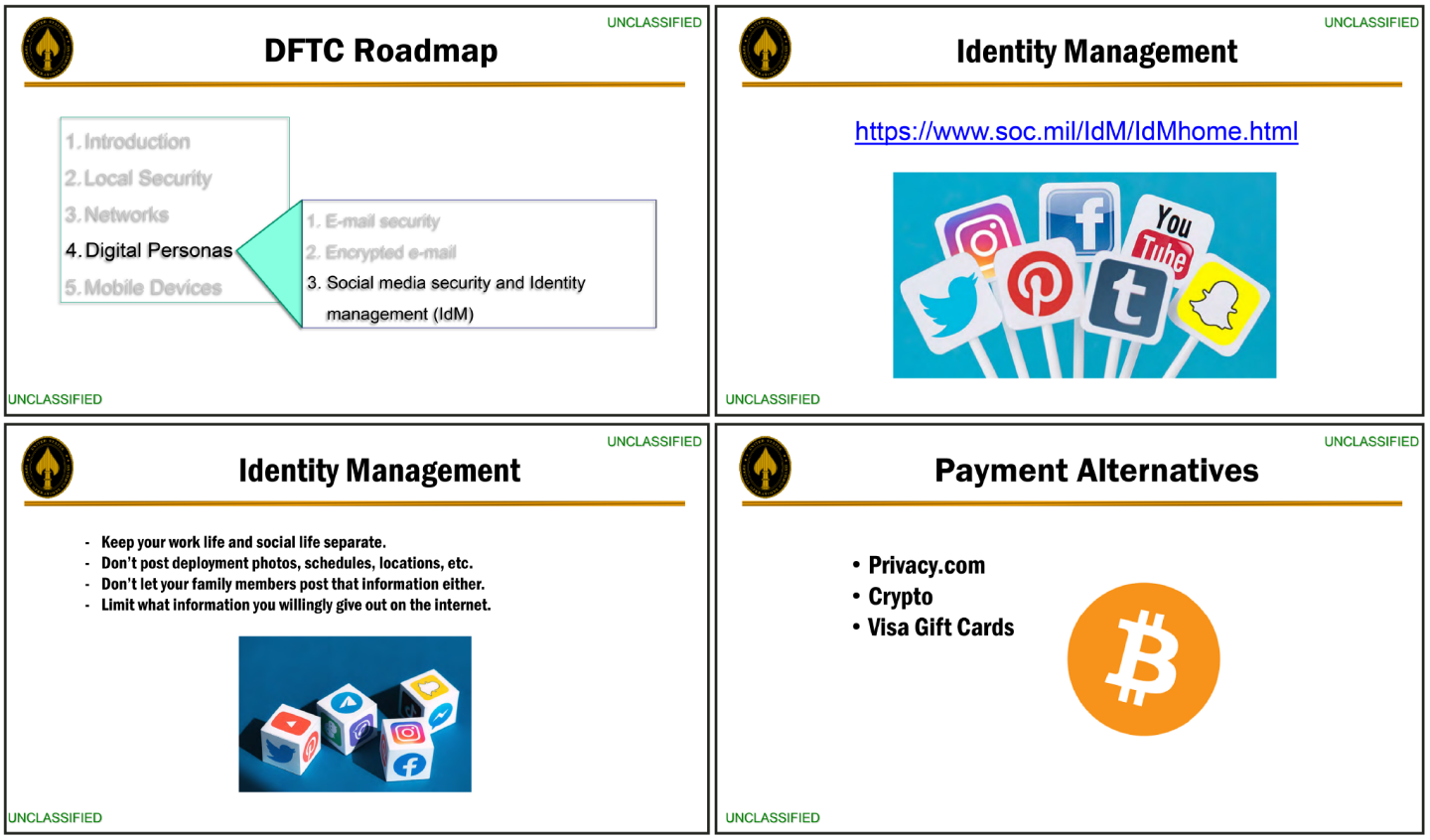
Figure 9: Example of Marine Corps's Training on Securing Digital Profiles



Source: U.S. Marine Corps training documents. | GAO-26-107492

- U.S. Special Operations Command provides a digital force protection training course to help personnel manage their online identities and personas, among other things. This course provides guidance on securing personal communications and devices, including local, network, email, and mobile phone security (see fig. 10).

Figure 10: Example of U.S. Special Operations Command's Training on Securing Digital Profiles



Source: U.S. Special Operation Command training documents. | GAO-26-107492

- The Defense Information Systems Agency offers a cyber awareness course to DOD personnel.[44] This DOD-wide training provides an overview of current cybersecurity threats and best practices to keep information and information systems secure at home and at work. The training also identifies best practices for protecting personally identifiable information, among other things.
- The Defense Intelligence Agency's Joint Counterintelligence Training Academy offers a course on understanding remote surveillance (also known as ubiquitous technical surveillance) and how the five pathways of collection (see text box) integrate to pose a threat to

[44]"Cyber Awareness Challenge", accessed September 22, 2025, https://www.cyber.mil/cyber-awareness-challenge.

intelligence activities. This course is available to DOD counterintelligence personnel.

Ubiquitous technical surveillance is the collection and long-term storage of data in order to analyze and connect individuals with other people, activities, and organizations. Ubiquitous technical surveillance is organized into five pathways of collection:

- Online (e.g., internet searches and websites)
- Electronic (e.g., Bluetooth connections, GPS information, and smart devices)
- Financial (e.g., banking applications and tap to pay)
- Visual-physical (e.g., CCTV cameras and smart doorbell)
- Travel (e.g., flight itineraries and GPS location searches)

Source: International Journal of Trend in Scientific Research and Development. | GAO-26-107492

- The Army Threat Systems Management Office offers a course on the protection of critical information, such as sensitive technology, installation and infrastructure, operations, and missions. This course is available to DOD program protection personnel, signature management professionals, and OPSEC practitioners.
- The Center for Development of Security Excellence offers seven security training courses that specifically address topics relevant to the digital profile threat to DOD personnel and contractors through a variety of learning formats, including self-paced internet learning and instructor-led learning (in person or virtually).

While most components we reviewed administer training, this training does not consistently cover threats associated with digital profiles in security areas other than OPSEC. Specifically, 80 percent (19 of 24) of training documents that addressed the digital profile represented OPSEC, based on our analysis of the evidence of security training provided by nine of the 10 select components. The other 20 percent represented counterintelligence and force protection. For example, DOD's Level I Antiterrorism/Force Protection training discusses the risks presented by the public accessibility of digital information—including information intentionally shared—which could unintentionally provide valuable information to a terrorist planning an attack.[45] DOD components did not provide training examples that addressed the digital profile for insider threat or program protection.

DOD components are relying primarily on OPSEC training to address digital profile risks because OSD officials responsible for other security areas have not recognized the digital profile as a threat. Specifically, the

[45]The training is intended to increase the trainee's awareness of terrorism and improve their ability to apply personal protective measures.

OSD officials with security responsibilities stated that it was not their responsibility to reduce risk associated with the digital profile. As a result, OSD officials responsible for security areas other than OPSEC have not ensured that training had been updated to inform and educate the DOD workforce about these risks. As discussed earlier in this report, digital profiling introduces risks beyond OPSEC and has implications across the security areas, including counterintelligence, force protection, insider threat, mission assurance, and program protection. OSD officials agreed and told us that DOD components cannot rely solely on OPSEC to reduce risks presented by the public accessibility of digital information.

DOD Directive 5200.43, *Management of the Defense Security Enterprise* requires the Defense Security Enterprise Executive Committee to advise the Under Secretary of Defense for Intelligence and Security, as the Defense Senior Security Official, on security policy and training.[46] In addition, the committee is responsible for providing recommendations on key policy decisions and on opportunities for standardization and improved effectiveness and efficiency; and facilitating cross-functional security policy coordination.

However, the Defense Security Enterprise Executive Committee has not reviewed and assessed digital profile training to ensure that it is sufficiently represented in all security areas: counterintelligence, force protection, insider threat, mission assurance, OPSEC, and program protection. By reviewing and assessing digital profile training across the security areas, the executive committee would be well-positioned to make any appropriate recommendations for improvement. Officials from the Under Secretary of Defense for Intelligence and Security agreed the executive committee could be leveraged to support and facilitate accomplishing this type of review.

In 2018, the then-Director of National Intelligence acknowledged that education and awareness programs are the most important weapons in

[46]DOD Directive 5200.43. The Defense Security Enterprise Executive Committee assists with the development of a defense security framework that integrates, across all security levels, personnel, physical, operations security, critical program information protection and security training and must align with and be informed by other DOD security areas or security-related functions, such as: counterintelligence, anti-terrorism, insider threat, and mission assurance, among others.

the cyber battlefield when it comes to personal devices and accounts.[47] Similarly, an official from the Office of the Under Secretary of Defense for Intelligence and Security emphasized that training and awareness programs likely will have a more effective impact than issuing policies. Until DOD takes action to ensure its personnel and contractors are trained on threats in the digital environment and associated risks of digital information in the public across all relevant security areas, DOD components will not fully understand the associated risks affecting personnel DOD-wide. Thereby, decreasing their ability to effectively reduce security and safety risks across the department.

However, one component—U.S. Cyber Command—did not provide evidence of having offered security training to its personnel in any of the security areas–counterintelligence, force protection, insider threat, mission assurance, OPSEC, and program protection. According to a U.S. Cyber Command official, the command provides training and educational programs so that its personnel understand their role in OPSEC, are aware of any current intelligence threats, know the command's critical information and indicators, and understand how to implement directed OPSEC measures and countermeasures. However, U.S. Cyber Command officials were unable to provide us evidence of this training or how it addresses risks associated with digital profiles. Until U.S. Cyber Command can demonstrate that it provides training to its workforce on threats in the digital environment and associated risks of digital information in the public across security areas, the command increases security, privacy, and safety risks.

Half of DOD Components Have Conducted Required Assessments of Security Risks

DOD guidance for four of the six security areas requires DOD components to conduct assessments: force protection, insider threat, mission assurance, and OPSEC.[48] These assessments enable DOD components to identify current or potential risks and vulnerabilities that would decrease the efficacy of that area's mission. For example, according to DOD, a mission assurance assessment should examine, among other things, security risks related to infrastructure devices.[49]

[47]Unclassified Responses to Questions for the Record Senate Select Committee on Intelligence Hearing, Feb. 13, 2018, available at sites-default-files-documents-response-to-ssci-qfrs-unclassified-subset.pdf last visited on Sept. 23, 2025.

[48]DOD Directive 5205.02E; DOD Instruction 5205.16; DOD Directive 3020.40; and DOD Instruction 2000.12.

[49]Chairman of the Joint Chiefs of Staff 3209.01A, *Mission Assurance Construct Implementation* (Aug. 23, 2023).

Similarly, DOD's Manual 5205.02-M, *Operations Security (OPSEC) Program Manual*, states that an OPSEC assessment should examine the actual practices and procedures of an activity to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions.[50]

Two of 10 components that we reviewed—the Marine Corps and U.S. Special Operations Command—conducted required assessments in all four areas. Both components provided evidence that they had conducted assessments that highlight risks associated with each of the four security areas—force protection, insider threat, mission assurance, and OPSEC. For example:

- U.S. Special Operations Command's OPSEC team conducted an assessment in November 2024 that included activities to analyze publicly accessible information on helicopter technology production. This information could be used by adversaries to understand critical information about equipment capabilities.
- Marine Corps's counterintelligence team assessed Marine Corps Air Station Beaufort in October 2024 and included activities to evaluate the organization's ability to detect, deter, and deny insider threats, as well as threats to force protection and mission assurance. The assessment identified public affairs and social media as critical issues.

However, of the remaining eight components we reviewed, three components—Army, Air Force, and Defense Counterintelligence and Security Agency—had conducted required assessments solely in the OPSEC area. For example:

- Defense Counterintelligence and Security Agency's OPSEC office conducted an OPSEC assessment of its headquarters from May 3 to July 23, 2021, to provide an overall evaluation of the organization's OPSEC posture. The assessment recognized open-source intelligence as a general OPSEC threat. Specifically, the assessment stated that open-source intelligence can provide information on the organization's dynamics, technical processes, and research activities.
- Department of the Air Force OPSEC Support Team conducted an external assessment, between October 2020 and January 2023, that included activities to analyze publicly accessible deployment

[50]DOD Manual 5205.02-M, *DOD Operations Security (OPSEC) Program Manual* (Nov. 3, 2008) (incorporating change 2, effective Oct. 29, 2020).

information that could lead to forewarning a malicious actor of a pending deployment, among other things. The assessment included recommendations to protect future aircraft deployments.

DOD officials agreed that focusing assessment efforts solely on OPSEC overlooks the security risks of the public accessibility of digital data about DOD and its personnel posed to personnel privacy and safety, and national security. Furthermore, these components were unable to provide us evidence that they had completed the required security assessments in the remaining three areas—force protection, insider threat, and mission assurance.

In addition, of the remaining five components we reviewed, three components—U.S. Cyber Command, Defense Intelligence Agency, and National Security Agency—were unable to demonstrate that they conducted the required assessments. The remaining two components—Navy and Space Force—did not complete any of the four required assessments. Specifically, the Navy and Space Force told us they had not completed required assessments because of resource limitations. Although staffing and other resources may be constrained in these components, these assessments are required by DOD policy.

As previously discussed in this report, the aggregation of digital information can be used to determine behavioral patterns for targeting purposes. Although Office of the Under Secretary of Defense for Intelligence and Security officials did not believe the risks associated with digital footprints and ultimately digital profiles are unique to DOD, they acknowledged and agreed the potential risks posed by a malicious actor attempting to determine behavioral patterns for targeting purposes are greater for the department. Without conducting the required assessments in the four required security areas, DOD components increase the risk of not detecting vulnerabilities that malicious actors may exploit. For example, the components might not discover critical information—such as mission plans, geotagged photographs, and personnel data—that can be used by malicious actors for intelligence collection and exploitation is publicly accessible. These risks could compromise critical information, jeopardize the mission and safety of DOD personnel, and ultimately undermine DOD's ability to achieve its overall mission to defend and protect the United States—including its operational and tactical goals.

Conclusions

In the age of digital dependency, the proliferation of devices, the prevalence of digital information, and a communications-oriented culture have led to individuals having a digital identity. The digital activity of

DOD's service members, contractors, and family members—from websites visited to emails sent to photos posted on social media—can generate volumes of traceable data that can threaten their privacy and safety, and ultimately our national security. These digital footprints represent a piece of a larger puzzle that, when tied to other sources, can create a digital profile and adversely affect military functions and missions.

DOD has identified the public accessibility of digital data as a real and growing threat to personnel privacy and safety, mission success, and national security. These risks could compromise critical information, jeopardize the mission and safety of DOD personnel, and ultimately undermine DOD's ability to achieve its overall mission to defend and protect the United States—including its operational and tactical goals. While the department has taken actions related to a wide field of traditional security areas, its actions to reduce safety, security, privacy, and operational risks posed by the digital profile are limited. DOD could better safeguard information and indicators that malicious actors can weaponize to adversely affect operations or the privacy, safety, and security of personnel by assessing existing policies and guidance; collaborating to address security risks; administering training across all relevant security areas; and conducting required assessments of security risks. By implementing these actions, DOD could reduce risks and be better positioned in achieving its goal to protect its personnel, units, and operations and to carry out its missions effectively.

Recommendations for Executive Action

We are making a total of 12 recommendations to DOD:

The Secretary of Defense should ensure that the Defense Security Enterprise Executive Committee assesses existing departmental security policies and guidance to identify gaps associated with risks in the digital environment; and makes recommendations on updating policy and guidance to reduce the risks of digital information about DOD and its personnel being publicly accessible. In conducting this assessment, the executive committee should include all OSD offices that oversee security areas and the Assistant to the Secretary of Defense for Public Affairs. (Recommendation 1)

The Secretary of Defense should ensure that the Defense Security Enterprise Executive Committee improves collaboration across the department to reduce the risks of information about DOD and its personnel being publicly accessible. Collaboration should include all OSD

offices that oversee security areas and the Assistant to the Secretary of Defense for Public Affairs. (Recommendation 2)

The Secretary of Defense should ensure that the Defense Security Enterprise Executive Committee reviews and assesses security training to ensure that digital profile issues are considered in all security areas—counterintelligence, force protection, insider threat, mission assurance, OPSEC, and program protection—and makes any appropriate recommendations for action to improve the representation of digital profile threats in security training across the department. (Recommendation 3)

The Secretary of Defense should ensure that U.S. Cyber Command provides security training to its workforce on threats in the security areas of counterintelligence, insider threat, and OPSEC. (Recommendation 4)

The Secretary of the Air Force should ensure that the Air Force is conducting required assessments in the security areas of force protection, insider threat, and mission assurance. (Recommendation 5)

The Secretary of the Army should ensure that the Army is conducting required assessments in the security areas of force protection, insider threat, and mission assurance. (Recommendation 6)

The Secretary of Defense should ensure that the Defense Counterintelligence and Security Agency is conducting required assessments in the security areas of force protection, insider threat, and mission assurance. (Recommendation 7)

The Secretary of Defense should ensure that the U.S. Cyber Command is conducting required assessments in the security areas of force protection, insider threat, OPSEC, and mission assurance. (Recommendation 8)

The Secretary of Defense should ensure that the Defense Intelligence Agency is conducting required assessments in the security areas of force protection, insider threat, OPSEC, and mission assurance. (Recommendation 9)

The Secretary of Defense should ensure that the National Security Agency is conducting required assessments in the security areas of force protection, insider threat, OPSEC, and mission assurance. (Recommendation 10)

The Secretary of the Navy should ensure that the Navy is conducting required assessments in the security areas of force protection, insider threat, OPSEC, and mission assurance. (Recommendation 11)

The Secretary of the Air Force should ensure that Space Force is conducting required assessments in the security areas of force protection, insider threat, OPSEC, and mission assurance. (Recommendation 12)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for their review and comment. In its written comments, reproduced in appendix II, DOD stated that it concurred with 11 of the 12 recommendations and partially concurred with the remaining one.

For the 11 recommendations with which it concurred, DOD identified initial actions to address them. Specifically, DOD plans to:

- Leverage the Defense Security Enterprise Executive Committee to (1) facilitate collaboration across the Department to mitigate the risks related to DOD information becoming publicly accessible; and (2) review and assess applicable security training to ensure relevance and effectiveness. (Recommendations 2 and 3); and

- Ensure the DOD components are conducting appropriate security assessments and training. (Recommendations 4 through 12)

By implementing these actions, DOD could reduce risks and be better positioned in achieving its goal to protect its personnel, units, and operations and to carry out its missions effectively. We will continue to monitor the agency's efforts in implementing our recommendations.

DOD partially concurred with our remaining recommendation. This recommendation calls for the Defense Security Enterprise Executive Committee to assess existing departmental security policies and guidance to identify gaps associated with risks in the digital environment and make recommendations on updating policy and guidance to reduce the risks of digital information about DOD and its personnel being publicly accessible. In conducting this assessment, the executive committee should include all OSD offices that oversee security areas and the Assistant to the Secretary of Defense for Public Affairs.

In its written comments, DOD stated the existing policies are aimed at safeguarding official DOD data and communications within the scope of the department's operational control. However, DOD stated the

department's authority is limited when it comes to the personal activities of DOD personnel managing their personal information and online presence outside the scope of their official duties, from non-DOD controlled locations, using non-DOD devices and applications, or with non-DOD information.

We recognize that there is a spectrum of who releases information—ranging from information that DOD intentionally releases (e.g., an official DOD press release) to information that a spouse posts on their personal social media account. However, as we depicted in our scenarios, a malicious actor does not care who releases the data. Rather, malicious actors leverage any available data to facilitate their ability to do harm to personnel, equipment, missions, and readiness. That is why we did not limit our recommendation to just policy, but also included improvements to training and awareness campaigns. These efforts could foster a culture change among DOD personnel (and their families) regarding how they share information during their personal activities.

Nonetheless, improvements in policy and guidance could lead to DOD offices and organizations (such as public affairs organizations) to reevaluate the extent to which information they are making publicly available could adversely affect national security or threaten the safety or privacy of service members (e.g. photos, names, ranks, and deployment status of service members). Without DOD sharing this information publicly, malicious actors would have to work harder to identify and potentially target family members whose loved one is deployed overseas. Also, DOD officials acknowledged to us that they had not consulted with their respective general counsel offices about actual legal limitations and parameters; therefore, we believe that an assessment of existing policies and guidance would allow OSD officials and the DOD General Counsel to identify such limitations while trying to manage the risk of publicly accessible information.

In its letter, DOD also expressed concern that we had not included *information security* in the scope of our review. DOD's information security program is a very broad program and includes topics such as determination, marking, releasability, and declassification of classified information, special access programs, special compartmental information, and sensitive information. During our review, DOD officials consistently identified security areas, such as OPSEC and counterintelligence where this issue should be addressed. When we met with officials from within the OSD information security office, they seemed to concur with our understanding of the program and that it was not responsible for actions

that could mitigate risks associated with digital footprints. Nonetheless, DOD's information security program is under the responsibility of the Under Secretary of Defense for Intelligence and Security, who is the chair of the Defense Security Enterprise Executive Committee. Therefore, to the extent that the office of the Under Secretary of Defense for Intelligence and Security believes that information security policy, guidance, assessments, and training should be included in the scope of our recommendations, we believe this would further help the department to make progress in addressing the risks identified in this report.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. We are also sending copies to the Under Secretary of Defense for Intelligence and Security. In addition, the report is available at no charge on the GAO website http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at kirschbaumj@gao.gov or Marisol Cruz Cain at cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

//SIGNED//

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

//SIGNED//

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Roger F. Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Tom Cotton
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

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

The Honorable Rick Crawford
Chairman
The Honorable Jim Himes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

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

Appendix I: Objectives, Scope, and Methodology

The objectives of this report (1) describe the security, privacy, and safety risks of publicly accessible data about Department of Defense (DOD) personnel and operations; and assesses the extent to which (2) the Office of the Secretary of Defense (OSD) has taken action to reduce associated risks to DOD personnel and operations; and (3) DOD components have conducted training and assessments to reduce risks to DOD personnel and operations.

The scope of this review includes digital data that can be generated by and transmitted from disparate sources, such as personal and government devices; DOD personnel working in an official capacity (such as a military unit's public affairs employee); and defense platforms that transmit information outside the DOD information network. We focused on actions taken by five OSD offices that oversee relevant security disciplines and security-related functions (security areas) and 10 select DOD components with security responsibilities.[1]

For the first objective, we reviewed literature identified through a search conducted by a GAO research librarian to understand the security implications of digital footprints, remote surveillance (also known as ubiquitous technical surveillance), and misuse of publicly accessible information. The librarian searched a variety of databases, including ProQuest and Defense Technical Information Center. Our search criteria included scholarly or peer-reviewed material; government reports; trade or industry papers; and association, nonprofit, and think tank publications. The team selected the articles from the literature search that were most relevant to our objectives for further review. We deemed an article relevant if it discussed threats or risks posed by the public accessibility of digital data. This discussion included how digital data are collected, combined, or shared—such as through data brokers or social media. By using this criterion, we determined that 228 of the 353 source documents were relevant.

We also conducted our own investigation to determine the accessibility of sensitive DOD-related information and assess associated risks to DOD's personnel and operations stemming from the aggregation of publicly accessible digital data. For this investigation, GAO's Forensic Audits and Investigative Service Criminal Investigators were authorized, through an approved investigation plan, to examine websites across the surface web,

[1]These components are the military services, U.S. Cyber Command, U.S. Special Operations Command, National Security Agency, Defense Counterintelligence and Security Agency, and Defense Intelligence Agency.

deep web, and dark web.[2] Investigators employed both overt and covert investigative techniques to identify whether information about DOD's personnel and families, operations and planning, units and organizations, or key defense entities could be accessed online. The investigators conducted investigative work in accordance with investigation standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

In addition, we interviewed officials from select DOD organizations, as described below, to identify safety, security, and privacy risks associated with the public accessibility of digital data about DOD and its personnel and to gain a better understanding of their technical responsibility for managing these risks. After these interviews, reviews, and our investigation, we developed notional threat scenarios that depict potential consequences stemming from the exploitation of publicly accessible digital data. Officials in the Office of the Under Secretary of Defense for Intelligence and Security reviewed the scenarios and provided input on their plausibility and potential impact.

For both the second and third objectives, we identified common OSD and DOD component security responsibilities that could reduce risks generated by digital profiles. To identify these common responsibilities, we reviewed DOD guidance for six select security areas. In analyzing this DOD guidance, we identified four responsibilities that OSD and DOD components were consistently supposed to conduct. Specifically, the different guidance documents stated that OSD should establish policy and guidance and coordinate and collaborate with each other on security matters. DOD component security responsibilities should involve developing and administering training, as well as conducting assessments.

For the second objective, we focused on actions taken by the OSD offices with security responsibilities. These include four OSD offices that oversee the security areas within the scope of our review: Offices of the Under Secretary of Defense for Intelligence and Security, the Under Secretary of Defense for Policy, the DOD Chief Information Officer, and the Under

[2]The surface web contains internet content that is indexed and searchable by everyone. The deep web contains internet content that is accessible but not easily searchable via search engines, such as login-protected websites or personal social media accounts. The dark web contains internet content that is available in darknets. Darknets are overlay networks that use the internet but require specific software or configurations for access. Dark websites are not indexed and only accessible via specialized software or discrete communications platforms.

Secretary of Defense for Research and Engineering. We also included the Office of the Assistant to the Secretary of Defense for Public Affairs since it is responsible for releasing DOD information to the public. The information we obtained from the select DOD components provided insight about the capabilities that different types of components are implementing and the challenges they are encountering.

To evaluate OSD's actions, we requested and obtained current policies and guidance that OSD officials identified as relevant to the digital profile threat. We received and reviewed nine policies and guidance related to the digital profile threat—from the Offices of the Under Secretary of Defense for Intelligence and Security, the DOD Chief Information Officer, and the Assistant to the Secretary of Defense for Public Affairs.[3] The Offices of the Under Secretary of Defense for Policy and the Under Secretary of Defense for Research and Engineering did not provide policies related to the digital profile threat. One analyst reviewed each document to determine whether the document discussed the digital profile threat, its associated risks, and established any best practices to reduce risk (e.g., countermeasures or mitigations). For the digital profile threats, we specifically looked for a discussion of one of three threat types—social networking services (e.g., Facebook, TikTok), digital ecosystems (e.g., applications, websites, or devices with data collection capabilities), and threats to identity (e.g., social engineering scams and fraud). We also included defense platforms as a type of digital profile threat because of their dependency on wireless technology that can generate data (e.g., ship transponder communicating routes, position, and speed). This review was used as the basis to assess the extent of action taken by OSD—whether policies and guidance addressed the range of digital profile

[3]These policies and guidance included: DOD Instruction O-2000.22, *Designation and Physical Protection of DOD High-Risk Personnel* (June 19, 2014) (incorporating change 2, effective Nov. 2, 2023). DOD Instruction 8170.01, *Online Information Management and Electronic Messaging* (Jan. 2, 2019) (incorporating change 2, effective Mar. 12, 2025). DOD Instruction 5400.17, *Official Use of Social Media for Public Affairs Purposes* (Aug. 12, 2022) (incorporating change 2, effective Feb. 14, 2025). DOD Chief Information Officer, *Use of Unclassified Mobile Applications in Department of Defense* (Oct. 6, 2023). Deputy Secretary of Defense, *Use of Geolocation-Capable Devices, Applications, and Services* (Aug. 3, 2018). Office of the Secretary of Defense, *Risk Guidance on the Use of Geolocation-Capable Devices, Applications, and Services* (Jan. 30, 2019). Deputy Secretary of Defense, *Records Management Responsibilities for Text Messages* (Aug. 3, 2022). Office of the Secretary of Defense, *Use of Non-Government Owned Mobile Devices* (Aug. 10, 2022). DOD Chief Information Officer, *Use of Text Messaging on Mobile Devices and Records Management of Electronic Messages* (Sept. 27, 2023).

threat types. A second analyst reviewed the information for accuracy; there were no disagreements.

To evaluate OSD's efforts to coordinate and collaborate on security matters, we interviewed knowledgeable officials within the Offices of the Under Secretary of Defense for Intelligence and Security, the Under Secretary of Defense for Policy, and the DOD Chief Information Officer to discuss (1) the extent to which they coordinated and collaborated with other security areas to reduce the privacy, safety, security, and operational risks related to information about DOD and its personnel being publicly accessible; and (2) what mechanisms, if any, they used to facilitate their coordination and collaboration efforts. We also asked the officials to identify any challenges they experienced when coordinating and collaborating.

For the third objective, we focused on a non-generalizable sample of 10 DOD components: the military services, U.S. Cyber Command, U.S. Special Operations Command, National Security Agency, Defense Counterintelligence and Security Agency, and Defense Intelligence Agency. The information we obtained from these select DOD components provided insight about the capabilities that different types of components (i.e., military service, combatant command, and intelligence agency) are implementing and the challenges they are encountering.

In assessing these components' efforts, we collected a non-generalizable sample of training and awareness documents from the select DOD components. We received a total of 92 training and awareness documents across five security areas—counterintelligence, force protection, insider threat, mission assurance, and operations security (OPSEC). This total included 56 awareness documents and 36 training documents. We determined the extent to which these documents included training information on the digital profile threat and its associated risks to DOD personnel and operations. We coded each document as "addressed," "not addressed," or "undetermined." These categories were defined as follows:

- *Addressed:* one or more relevant search terms, such as "social media," "open source," and "online," were discussed within the document.
- *Not addressed:* no relevant search terms were found.

- *Undetermined:* relevant search terms were present but could not be determined if they were being discussed in the context of the digital profile threat and its associated risks.

To conduct this analysis, one analyst organized the 92 training and awareness documents by the component and security area. The analyst then recorded her assessment and the basis for the assessment. A second analyst reviewed the same information and recorded her assessment and the basis for the assessment. The two analysts created a final assessment that reconciled their two assessments and reflected the analysts' consensus. We then analyzed the documents coded as "addressed" to better understand the range of digital profile topics covered. In analyzing the documents, we assessed whether each document included one or more of five target topics: digital ecosystems, social networking services, social engineering scams, and information collected from defense platforms, and best practices for countering those risks. For the next level of review, an analyst recorded her assessment and the basis for the assessment. A second analyst reviewed the same information and recorded her assessment and the basis for the assessment. The two analysts created a final assessment that reconciled their two assessments and reflected the analysts' consensus. This analysis allowed us to assess the extent to which the select DOD components are educating their respective personnel on the digital profile threat and its associated risks across the six security areas.

We also received and reviewed training information on DOD-wide course offerings from the Center for Development of Security Excellence. We assessed whether the DOD-wide course's (1) objectives and descriptions included information about the digital profile or protecting DOD personnel and operations from digital profile threats; and (2) content acknowledged threats and countermeasures related to the digital profile. To conduct this analysis, one analyst reviewed the catalog of course objectives and descriptions, and recorded her assessment and the basis for the assessment. A second GAO analyst checked the information for accuracy; there were no disagreements. The analysts then tallied the codes to determine the extent to which DOD offers department-wide training related to the digital profile and its associated risks.

In addition, we collected a non-generalizable sample of the most recent security assessments required from the select DOD components in four security areas: force protection, insider threat, mission assurance, OPSEC. We received and reviewed a total of 32 assessments. We then determined the extent to which the assessments included information on

the digital profile threat and its associated risks. We coded each document would be rated as either “Acknowledged” or “Not Acknowledged.” These categories were defined as follows:

- *Acknowledged:* relevant search terms such as “social media,” “open source,” and “online” were discussed within the report in the context of the digital profile threat and its associated risks.
- *Not acknowledged:* none of the search terms were identified. One analyst reviewed the assessments and determined whether the assessments did or did not acknowledge the digital profile threat or its associated security risks.

To conduct this analysis, one analyst organized the 32 assessments by component and security area. First, the analyst recorded her assessment and the basis for the assessment. A second analyst reviewed the same information and recorded her assessment and the basis for the assessment. The two analysts created a final assessment that reconciled their two assessments and reflected the analysts’ consensus. We used this analysis to assess whether the select DOD components are conducting required assessments and whether the digital profile threat has been recognized as a security risks.

Furthermore, we interviewed these officials to discuss ongoing efforts and actions to address and reduce risks relating to information about DOD and its personnel being publicly accessible. In addition, we interviewed officials from two non-DOD organizations, including the Office of the Director of National Intelligence and Duke University. We interviewed the Office of the Director of National Intelligence to gain a non-DOD intelligence community perspective of issues related to the digital profile threat and its associated risks. We also interviewed research fellows who led the data brokerage research project under Duke University’s Sanford School of Public Policy to collect insights on their research findings and understand data brokerage issues from a non-governmental organization.

We conducted this performance audit from May 2024 to October 2025 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: Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF WAR
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

OCT 1 2025

MEMORANDUM FOR U.S. GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: Response to U.S. Government Accountability Office (GAO) 107492 Security Implication of Digital Footprints Recommendations

As the Defense Security Executive and chair of the Defense Security Enterprise (DSE) Executive Committee (DSE ExCom), I appreciate GAO's interest in the Department's policy, training, and security assessments related to digital footprints. The Department of War (DOW) recognizes that the world has become increasingly digital and interconnected. Our interactions – both with other people and with the tools and items we rely on – have the potential to leave a record of that interaction (a "digital footprint"). We note that even the absence of a digital footprint can itself be an indicator. Given these realities, the Department is aware of the risks "digital footprints" pose to individuals and the mission. DOW's sensitivity review determining this report to be publicly releasable reflects the obviousness of these risks.

The Department acknowledges the GAO's intent to enhance security and information protection. However, the report appears to conflate several distinct categories, potentially undermining its application and the effectiveness of proposed solutions. Specifically, the recommendations fail to recognize the distinction between non-public DOW information (including but not limited to classified national security information, controlled unclassified information, and other unclassified DOW information that has not been approved for public release) and public information (both DOW and non-DOW); DOW personnel with non-DOW personnel; and DOW information with DOW personnel's *personal* information. It is crucial to distinguish among these categories. In particular, the Department's authority is limited with respect to the personal activities of DOW personnel, their friends, or family members when using their privately-owned devices during their personal time. The Department has limited ability to regulate personal information security practices outside the scope of DOW personnels' official duties, with non-DOW information, outside of DOW locations, or using non-DOW-controlled resources.

In addition, the Department notes the report excludes the information security discipline – despite our repeated requests for its inclusion – because it focuses on "protecting information within DOW's network and the scope of [the] review was focused on information that is publicly available." This exclusion, however, is counter to the inclusion of operations security and counterintelligence, which are focused on preventing certain DOW information *from becoming available to the public* or foreign intelligence entities.

The attachment to this memorandum contains the Department's response to each of the 12 recommendations in the draft report. My point of contact for this effort is Erica S. McLennan, at erica.s.mclennan.civ@mail.mil, (703) 697-5526.

John P. Dixson
Director for War Intelligence
Counterintelligence, Law Enforcement,
& Security

Attachment:
Department of War Comments to the GAO Recommendations

GAO Draft Report September 18, 2025

GAO - SECURITY IMPLICATION OF DIGITAL FOOTPRINTS (GAO CODE 107492)
"SECURITY IMPLICATION OF DIGITAL FOOTPRINTS: RECOMMENDATIONS"

DEPARTMENT OF WAR COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of War should ensure that the Defense Security Enterprise Executive Committee assesses existing departmental security policies and guidance to identify gaps associated with risk in the digital environment; and makes recommendations on updating policy guidance to reduce the risks of information about DOW and its personnel becoming publicly accessible.

DOW Response: Partially Concur. The DSE will update existing risk assessments related to the digital environment and make recommendations on updated policy guidance, to the extent practicable recognizing the modern digital environment. DOW already has robust policy frameworks to mitigate risks associated with DOW information residing on platforms such as electronic messaging systems, geolocation-enabled devices, non-government websites, and various applications. These existing policies are aimed at safeguarding official DOW data and communications within the scope of our operational control. However, it is important to clarify the limitations of DOW's authority.

DOW's authority is limited when it comes to the personal activities of DOW personnel managing their personal information and online presence outside the scope of their official duties, from non-DOW-controlled locations, using non-DOW devices and applications, or with non-DOW information. That authority is even more limited when it comes to non-DOW personnel, such as family members. The responsibility for personal security and privacy rests with the individual. The Department promotes awareness of best practices for safeguarding personal information and ways to mitigate potential vulnerabilities.

RECOMMENDATION 2: The GAO recommends the Secretary of War should ensure that the Defense Security Enterprise Executive Committee improves collaboration across the department to reduce the risks of information about DOW and its personnel becoming publicly available.

DOW Response: Concur. In accordance with DOW Directive 5200.43, the DSE ExCom is responsible for, among other things, policy collaboration within the Defense Security Enterprise. In that role, the DSE ExCom facilitates collaboration across the Department to mitigate the risks related to DOW information becoming publicly available. As part of its ongoing efforts, the DSE ExCom advises the USW(I&S) on security policy and training, provides recommendations on key policy decisions, and directly assists with the development of a comprehensive Defense Security framework. This framework is designed to integrate all security levels and disciplines, ensuring alignment with, and informed by, other DOW security and security-related functions. However, as noted above, there are limits to DOW's ability to reduce the risks associated with all information about DOW and its personnel becoming publicly available.

RECOMMENDATION 3: The GAO recommends that the Secretary of War should ensure that the Defense Security Enterprise Executive Committee reviews and assesses security training to ensure that digital profile issues are considered in all security areas—counterintelligence, force protection, insider threat, mission assurance, OPSEC, and program protection—and makes any appropriate recommendations for action to improve the representation of digital profile threats in security training across the department.

DOW Response: Concur. Based on the results of the risk assessment described in recommendation 1, the DSE ExCom will, through one or more subgroups or other relevant organizations, review and assess applicable security training and make recommendations for improvements related to digital profile threats.

The Defense Security Enterprise Strategy for Fiscal Years 2021-2025 outlines the goals and objectives for the Enterprise to pursue for a more cohesive, integrated, and future-focused security framework. Objective 1.1. of the strategy is to empower and professionalize the security workforce to execute its mission through enhanced and standardized security education, training, and credentialing. The DSE ExCom's subgroups and working groups continuously review and assess security training across all security areas to ensure relevance and effectiveness. Current training curricula already incorporate risks associated with electronic messaging systems, geolocation-enabled devices, non-government websites, and various applications used in the performance of official duties. The Department also promotes awareness of best practices for safeguarding personal information and of ways to mitigate potential vulnerabilities in various training settings, including recommendations on how individuals can manage their personal information or their online presence outside the scope of their official duties, in non-DOW-controlled locations, and using non-DOW resources. These resources are designed to empower personnel to make informed decisions regarding their digital footprint and personal security.

RECOMMENDATION 4: The Secretary of War should ensure that U.S. Cyber Command provides training to its workforce on threats in the areas of counterintelligence, insider threat, and OPSEC.

DOW Response: Concur. U.S. Cyber Command concurs with the intent of this recommendation and assesses it is sound and necessary.

RECOMMENDATIONS 5-7: The Secretary of the Air Force should ensure that Air Force is conducting security assessments in the required security areas of force protection, insider threat, and mission assurance. Recommendations 6 and 7 are identical but directed at the Army and Defense Counterintelligence and Security Agency, respectively.

DOW Response (#5-7): Concur.

RECOMMENDATIONS 8-12: The Secretary of War should ensure that U.S. Cyber Command is conducting security assessments in the required security areas of force protection, insider threat, OPSEC, and mission assurance. Recommendations 8 through 12 are identical but directed at the Defense Intelligence Agency, National Security Agency, the Navy, and Space Force, respectively.

DOW Response (#8): Concur. U.S. Cyber Command concurs with the intent of this recommendation and assesses it is sound and necessary.

DOW Response (#s 9 through 12): Concur.

Appendix III: Contacts and Staff Acknowledgments

GAO Contacts

Joseph W. Kirschbaum, KirschbaumJ@gao.gov.
Marisol Cruz Cain, CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following staff made key contributions to this report: Tommy Baril (Assistant Director), Lee McCracken (Assistant Director), Ashley Houston (Analyst-in-Charge), Nicole Ashby, Tracy Barnes, Prianka Bose, Chris Businsky, Ash Huda, Evan Leiter-Mason, Mark MacPherson, Tyler Mountjoy, Mike Silver, Pamela Snedden, and Angel Zollicoffer.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us