A Roadmap to Launching Survey Operations Within the U.S. Department of Defense

Karl G. Feld

E. Lee Hill

Victoria A. Leoni

The Department of Defense (DOD) is acutely focused on harnessing the rising strategic value of information for decision-making and advanced capabilities from the boardroom to the battlefield.[1] In June 2022, the newly established Chief Digital and Artificial Intelligence Office, charged with leading the department-wide push to adopt and leverage data, analytics, and artificial intelligence, reached full operating capacity.[2] At the same time, the Military Operations Research Society hosted its annual symposium featuring dozens of working groups dedicated to operational research topics, including assessments, social science methods and applications, and data science and analytics.[3] This article discusses lessons Vistra Communications has learned while consulting with the Defense Media Activity (DMA), a DOD field activity, to establish its Office of the Chief Data Officer and associated data collection and analysis programs. DMA seeks to employ surveys, focus groups, and other applied social science methods to generate new data to inform the organization's strategic initiatives and improve its services to the DOD public affairs enterprise.

Surveys are used throughout the DOD to inform data-driven decision-making for a wide variety of purposes. For example, DOD Instruction 5010.43, *Implementation and Management of the DoD-Wide Continuous Process Improvement/Lean Six Sigma* (CPI/LSS) *Program*, requires all DOD components to use Lean Six Sigma/continuous process improvement techniques, which often rely on surveys to improve organizational performance.[4] Information operations doctrine also calls for the use of surveys for assessment purposes.[5] Additionally, DOD personnel regularly participate in surveys from DOD components and other U.S. government agencies (e.g., Office of Personnel Management's Federal Employee Viewpoint Survey). Surveys are so widely used throughout the DOD, many agencies and activities have departments that provide support services to other components seeking to use surveys to generate data-driven insights (e.g., Office

Army Reserve soldiers fill out crew evaluation worksheets 11 September 2019 at the George W. Dunaway Reserve Center in Sloan, Nevada. The Army launched a new survey that allows soldiers to voice their concerns directly and anonymously to Army leadership in 2020. (Photo courtesy of the U.S. Army)

of People Analytics, Defense Manpower Data Center, Directorate of Human Research Protections). Surveys are defined here using the Office of Management and Budget (OMB) and DOD definition of "systematic data collections using … interviews or self-administered questionnaires … from a sample or census of 10 or more persons … to identical questions that are to be used for statistical compilation for research or policy assessment purposes."[6]

Within the DOD, surveys and other social science methods that collect information from individuals (e.g., focus groups, interviews) are termed "information collection" and come with a host of requirements outlined in various DOD instructions, manuals, and directives. Numerous entities within and outside the department are involved in the approval and licensing of information collection activities, which can make the process

complex and constraining for DOD components. This article brings the disparate requirements and entities together in one place and provides a concrete roadmap for DOD components to launch surveys, focus groups, and similar research activities. In 2017, a group affiliated with the DOD TriService Nursing Research Program made a similar effort to identify, clarify, and consolidate DOD and service-specific survey approval processes to make cross-component surveys more feasible within military nursing.[7] Other articles have focused more narrowly on human subjects research and its unique requirements within the DOD.[8] This article provides a more comprehensive roadmap than previous work for DOD information collection activities at large. The methods section discusses the role of each governing entity while the results section weaves the relevant requirements together in a single, continuous process flow. The

article concludes with a discussion of tensions inherent in DOD requirements and practical recommendations for how they might be navigated or resolved.

Background

DMA graduates classes of qualified public affairs practitioners from its Defense Information School. It also produces content for and manages DOD's American Forces Network radio and television broadcasting as well as a wide array of DOD website platforms and social media channels.[9] DMA seeks to measure the reach and impact of its public affairs media content and transmissions on DOD target audiences. DMA is also considering social science research to gather feedback from its customers and graduates on how well they perceive DMA meets their requirements.

These types of research involve collecting information from individuals using surveys and other social science methods. DOD information collection (IC) requires compliance with a wide variety of DOD authorities and instructions to protect the interests of research subjects and information security, especially in today's online IC and electronic data storage environment. In some cases, OMB also has a role. These governing rules and regulations address topics like human research protection, participant privacy, personally identifiable information (PII) protection, cost control, cybersecurity, cross-DOD coordination, and data-sharing requirements. IC at the DOD is controlled by authorities originating from different offices, each providing its own set of instructions. In any research undertaking, it is incumbent upon each DOD component to ensure it follows all instructions from all authorities impacting IC.

Method: Review of Relevant Authorities

Seven different DOD entities govern IC in the department. Each entity has its own set of instructions that impose standards and approval requirements on DOD components conducting IC activities. The purpose of these requirements is to ensure nonduplication of effort and respect for research subjects' privacy and civil liberties while maximizing the value of data collected and minimizing costs and burden on participants. Each authority covers a different facet of IC and has a separate approval process.

As a result, the DOD does not provide a comprehensive roadmap for components to launch new IC in compliance with the many governing DOD instructions and parts of the code of federal regulations. This article addresses this shortcoming with a summary of each governing entity's role provided below. The

Lee Hill is the contracted research program manager for the Defense Media Activity's analysis, analytics, assessments, and evaluation team. A former infantry officer, Hill has over twenty years' experience consulting for both the Department of Defense and Department of State. He provided social science research with the U.S. Army human terrain teams in Iraq, research and analysis for the Afghan Assessment Group, and data science for the U.S. Army Test and Evaluation Office. Hill has a BS in applied mathematics from Auburn University and two master's degrees from Norwich University and Troy University.

Karl Feld is a contracted subject-matter expert for analytics and applied research methods at the Defense Media Activity. For more than twenty years, he has applied his social science research and data science expertise to defense, diplomacy, international development, and healthcare issues worldwide. His engagements have included the U.S. Special Operations Command; Army Corps of Engineers; U.S. Departments of Homeland Security, State, and Health and Human Services; as well as the U.S. Agency for International Development, U.S. Agency for Global Media, and global nonprofits and corporations. Feld is widely published on social science methods in four languages, his work is frequently cited, and he regularly speaks on research methods and findings. Feld holds an MA from Georgetown University and is completing his PhD dissertation in the social sciences at North Carolina State University.

Victoria Leoni is a research analyst and the senior technical writer/editor on the analysis, analytics, assessments, and evaluation contract team at the Defense Media Activity. She received her BA in journalism and mass communication (Phi Beta Kappa) from George Washington University. She works at the intersection of military and media and previously wrote for the *Military Times* family of publications.

Department of the Army civilians are being asked to fill out the annual Federal Employee Viewpoint Survey so leadership can gauge what the workforce thinks on a variety of employment topics in order to improve the workplace. (Photo by Jon Micheal Connor, Army Sustainment Command Public Affairs)

relevant DOD instructions are provided in the notes at the end of the article.

DOD chief information officer. The DOD chief information officer (CIO) sets policy for all DOD IC. The office of the CIO (OCIO) seeks to reduce the number and frequency of IC activities, approves IC budgets, and monitors IC execution. As part of this effort, the OCIO explicitly states intended users of proposed IC should first see if the same information is available elsewhere and use methods that minimize IC activity. The OCIO also enjoins all DOD components using internet services for IC to adhere to all DOD IC regulations and guidance protecting DOD personnel and their families as well as other federal agency personnel, contractors, and members of the public.[10]

DOD undersecretary of defense for personnel and readiness. The undersecretary of defense for personnel and readiness (USD [P&R]) provides mandatory coordination for all IC that includes DOD

employees in more than one component.[11] The USD (P&R) is also responsible for recommending approval or disapproval of this kind of IC to the director, Washington Headquarters Services. As part of its review, the USD (P&R) assesses all IC for compliance with laws, regulations, and policies prior to approval.[12]

The director, Office of People Analytics (OPA) (under the authority of director, Defense Human Resources Activity) manages these tasks for the USD (P&R).[13] OPA reviews proposed IC for validity, data protection, and consent procedures. Component action officers (AO) are required to request assistance from OPA survey experts on the technical and scientific aspects of a survey as part of the mandatory review of a public IC classified as a survey.[14] OPA can disapprove collection instruments or methodologies. OPA also reviews public IC applications before submission to OMB, if applicable.

Director, Washington Headquarters Services. The Washington Headquarters Services (WHS) director

controls DOD IC activity. The chief of the Directives Division, Executive Service Directorate acts as the DOD information collections officer (ICO) for the WHS director.[15] The ICO determines if the IC is internal to the DOD and provides licensing numbers appropriately. If the ICO deems the IC is not internal, they forward the IC request to another approving authority (e.g., OMB). The ICO is the primary point of contact with OMB for all DOD IC involving the public.[16] The ICO sends sixty-day notices of public IC to the Federal Register for public comment as required. The ICO also submits the required thirty-day notice when proposed IC has been sent to OMB for review.[17]

DOD Directorate of Human Research Protections. The DOD Directorate of Human Research Protections (DOHRP) operates under the authority of the undersecretary of defense for research and engineering. It oversees DOD research involving human subjects with a focus on the welfare of research participants and their rights. Information collection involving human beings is considered human subjects research and subject to DOHRP regulation. All DOD components conducting IC are required to have their activities reviewed by a DOHRP-designated exemption determination official to determine if a human research protection program is required.[18]

Director, Defense Manpower Data Center. The Defense Manpower Data Center (DMDC) director maintains the master list of DOD personnel and their PII used to generate survey samples of DOD personnel. The DMDC director is responsible for establishing and renewing DOD matching agreements with other federal agencies and components to govern DMDC data on systems of records to which the data has been added. DMDC submits matching agreements to the chief, Defense Privacy, Civil Liberties, and Transparency Division. DMDC also ensures compliance with those matching agreements.[19]

Chief, Defense Privacy, Civil Liberties, and Transparency Division. The Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) chief coordinates and maintains DMDC matching agreements and reviews changes to system of records notices that protect survey sample PII on component IT systems.[20]

Director, Directorate for Oversight and Compliance. In conjunction with the DOD CIO, the Directorate for Oversight and Compliance director is required to ensure all DOD components comply with OMB requirements for the protection of PII.[21]

Office of Management and Budget. When DOD IC is proposed with ten or more members of the public within twelve months, OMB regulations apply. This includes cases when automated collection techniques are used, and structured collection is expected to elicit the same or similar responses. Members of the public include current federal employees if the collection of information is addressed to them in their capacity as individual private citizens. Defense contractors and foreign nationals are also defined as members of the public.[22]

OMB provides a report control symbol and expiration date for approved IC. OMB approval can be a six-month process unless expedited, though faster generic and emergency clearances are possible.[23] As part of its review, OMB gathers comments based on a thirty-day notice in the Federal Register about the proposed IC. Comments are used to ensure the information proposed to be collected is not already available and appropriate efforts are made to minimize the public burden and maximize practical utility.[24]

Component information management control officer and action officer. Figure 1 (on page 6) highlights the roles of the component action officer (the DOD equivalent of the principal investigator) and the component information management control officer (IMCO). The component action officer is the study lead designated to represent a specific study's interests and coordinate with other components and officers to effectively execute the research. The IMCO coordinates the action officer's interface with numerous governing authorities, works through the study execution process, and issues control numbers for work within the component. The IMCO also serves as the component human research protection representative responsible for reviewing surveys against the component human research protection plan, if applicable, and managing any institutional review board requirements.[25]

Results: DOD Information Collection Activity Process Flow

Vistra Communications has developed a multiphase process flow to assist DMA and other DOD components interested in undertaking fully compliant IC activities. The first-of-its-kind diagram brings the
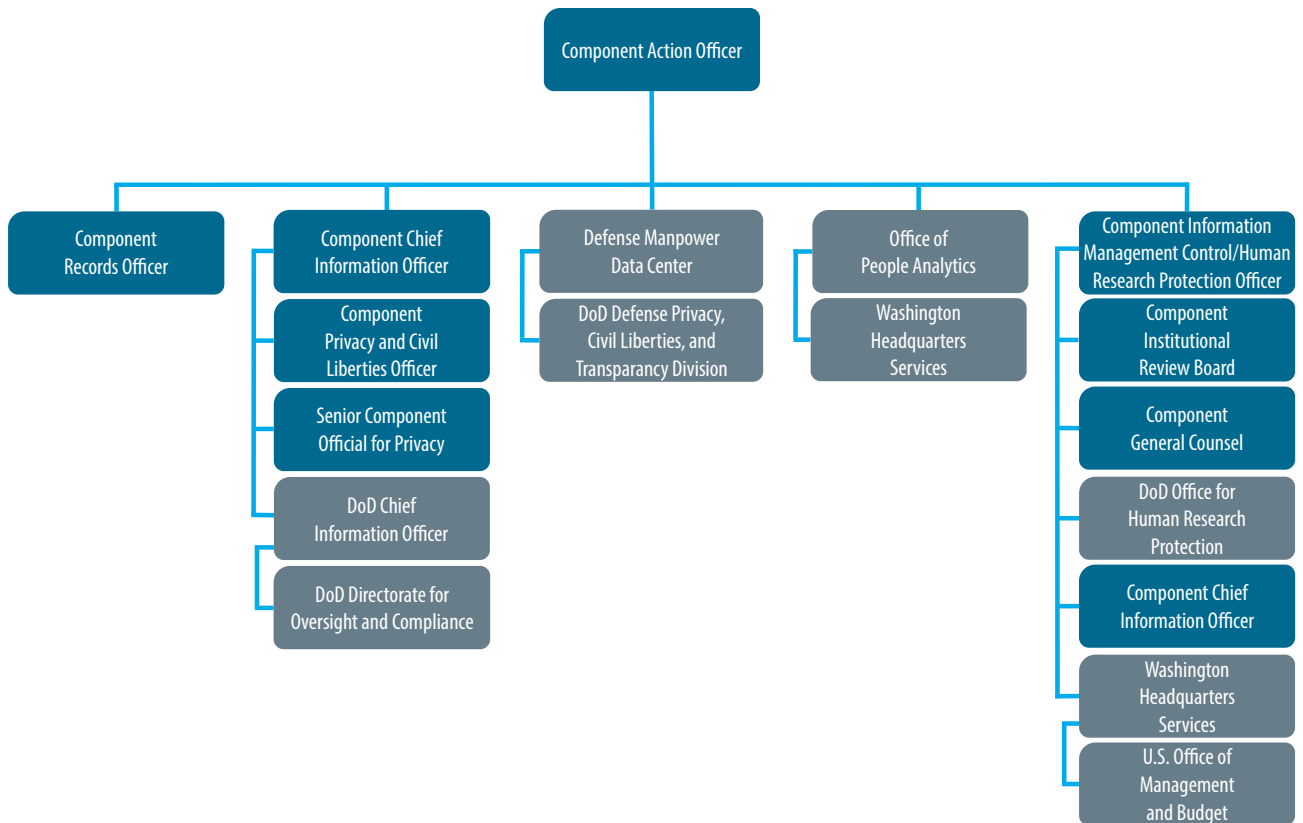
Figure 1. Coordination Relationships for DOD Computer-Assisted Information Collection (e.g., Web-Based Surveys)

(Figure by authors)

Information collected using digital or paper forms requires a slightly different configuration. Each entity represented is responsible for coordinating with those to which it is connected. Entities that are part of a single Department of Defense (DOD) component are shown in blue. Entities outside the component conducting the information collection are shown in gray.

disparate DOD entities and requirements together into a single field of view for practical application.
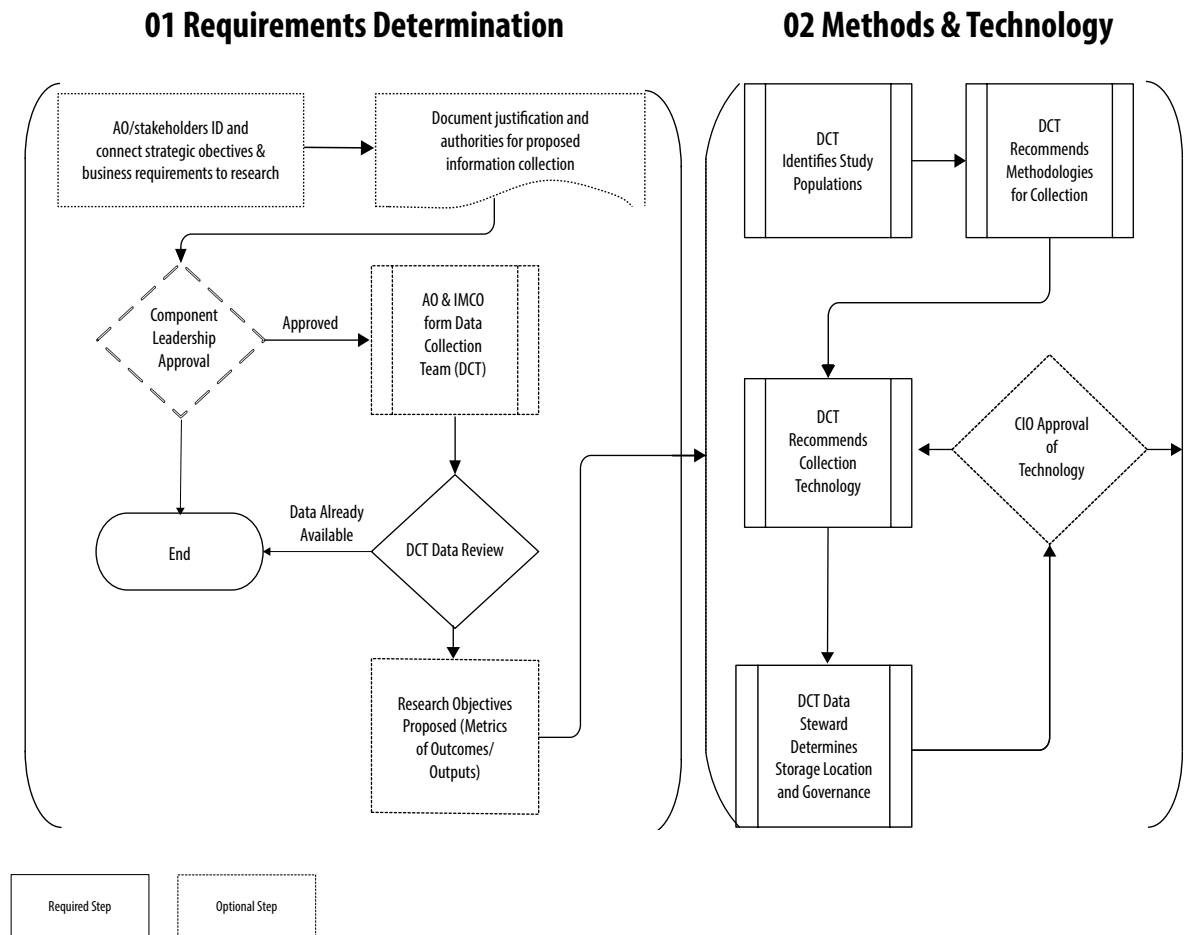
Phase 1 requires the component action officer and stakeholders to define the requirement for the information collection; namely, how the research connects to organizational strategic objectives and fulfills business requirements. Once component leadership has approved the proposed IC, the action officer and IMCO form a data collection team (DCT), which determines whether sufficient data exists to satisfy all or parts of the research requirement. If it does not, the DCT moves to phase 2, as shown in figure 2 (on page 7).

In phase 2, the DCT identifies the study population and recommends appropriate information collection methodologies and technology to formulate a research proposal. From there, the DCT develops the research study sample design, instrument design, and internal/ external data and published findings release plan for the IC (phases 3–5, respectively). The DCT vets these items with appropriate authorities, which may include component stakeholders, data stewards, privacy officers, records managers, general counsels, operational security, and communications offices, as well as the Defense Office for Prepublication and Security Review. These phases of the process flow are shown in figure 3 (on page 7).
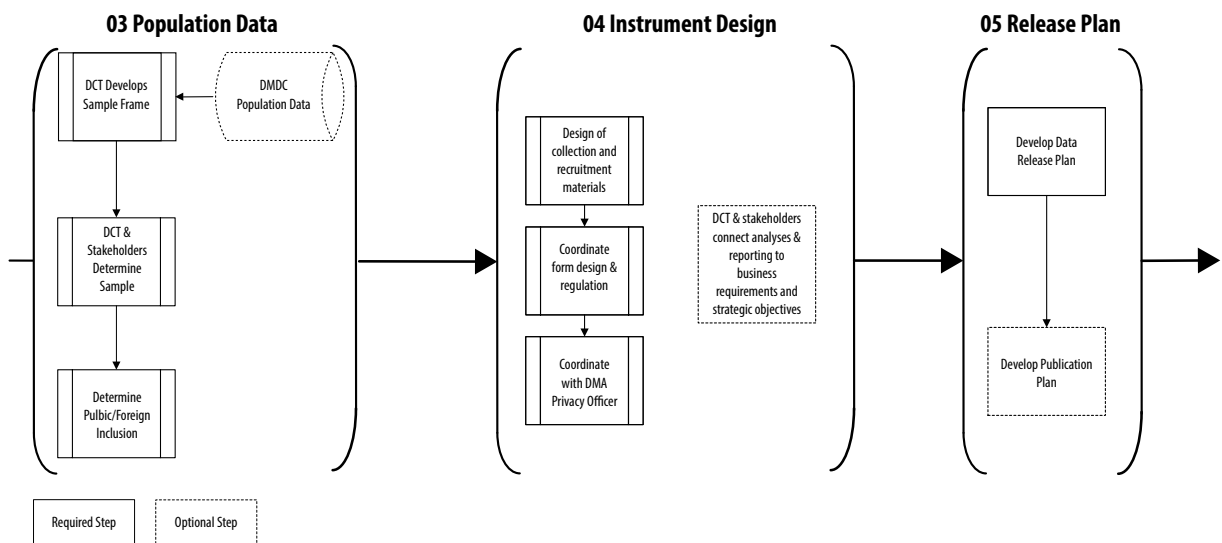
The approvals process begins in phase 6 (see figure 4, page 8). In this phase, the component's assigned exemption determination official determines if a human research protection program is required for the proposed IC. If required, the IC also undergoes human research protection officer and institutional review board vetting and approval before proceeding to phase 7.

In phase 7, the DCT determines whether the IC is internal to the component or will involve other

01 Requirements Determination

02 Methods & Technology

AO/stakeholders ID and connect strategic obectives & business requirements to research

Document justification and authorities for proposed information collection

Component Leadership Approval

Approved

AO & IMCO form Data Collection Team (DCT)

End

Data Already Available

DCT Data Review

Research Objectives Proposed (Metrics of Outcomes/Outputs)

DCT Identifies Study Populations

DCT Recommends Methodologies for Collection

DCT Recommends Collection Technology

CIO Approval of Technology

DCT Data Steward Determines Storage Location and Governance

Required Step

Optional Step

(Figure by authors)

Figure 2. DOD IC Activity Process Flow Phases 1-2

03 Population Data

04 Instrument Design

05 Release Plan

DCT Develops Sample Frame

DMDC Population Data

DCT & Stakeholders Determine Sample

Determine Pulbic/Foreign Inclusion

Design of collection and recruitment materials

Coordinate form design & regulation

Coordinate with DMA Privacy Officer

DCT & stakeholders connect analyses & reporting to business requirements and strategic objectives

Develop Data Release Plan

Develop Publication Plan

Required Step

Optional Step

(Figure by authors)

Figure 3. DOD IC Activity Process Flow Phases 3-5

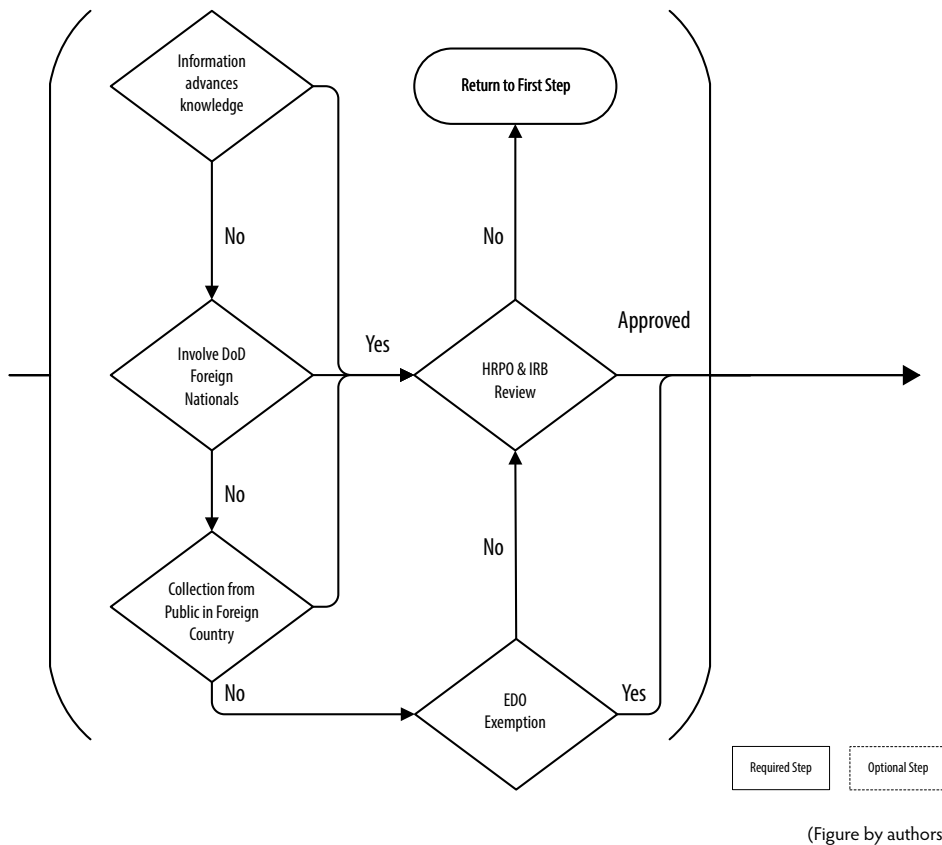## 06 HRPP review and approval

(Figure by authors)

Figure 4. DOD IC Activity Process Flow Phase 6

OPA, and the WHS Office of Information Management, which serves as the office of record and ultimate approval authority. Any planned IC involving ten or more members of the public is also regulated by OMB and requires the series of licensing steps outlined in phase 10 and shown in figure 7 (on page 11).

Discussion: Approaches to Tensions in DOD Guidance

While designing and preparing survey work with DMA action officers and the IMCO, Vistra Communications has identified several tensions in the relevant DOD guidance issued by the various authorities. Here we begin to approach resolutions for each based on the guidance and its intent.

Cybersecurity versus survey response. There is tension between DOD cybersecurity requirements and the use of the secure DOD Enterprise Email (DEE) service (e.g., john.doe.mil@mail.mil) to recruit participants to online surveys. Where email addresses are known in advance, emailed invitations to online surveys are generally recognized as the most effective method to recruit selected cases from a probability sample.[26] The comprehensive DMDC personnel file presents the only way to draw probability samples of the DOD population at large. The file associates DOD personnel with their DEE addresses for recruitment to surveys. This type of recruitment is generally accomplished by sending participants unique links to the online survey within the body of the invitation email.[27]

Each mouse click or other task a participant must complete to begin a survey has the potential to reduce survey response rates.[28] There is a direct relationship

DOD components. If the latter, the DCT develops and submits the required formal supporting statements to the Office of People Analytics to obtain an IC license. If multiple components will be involved, the initiating component is required to coordinate with the Office of the Secretary of Defense and/or the other DOD components included to collect approval signatures or dissenting comments (phase 8).
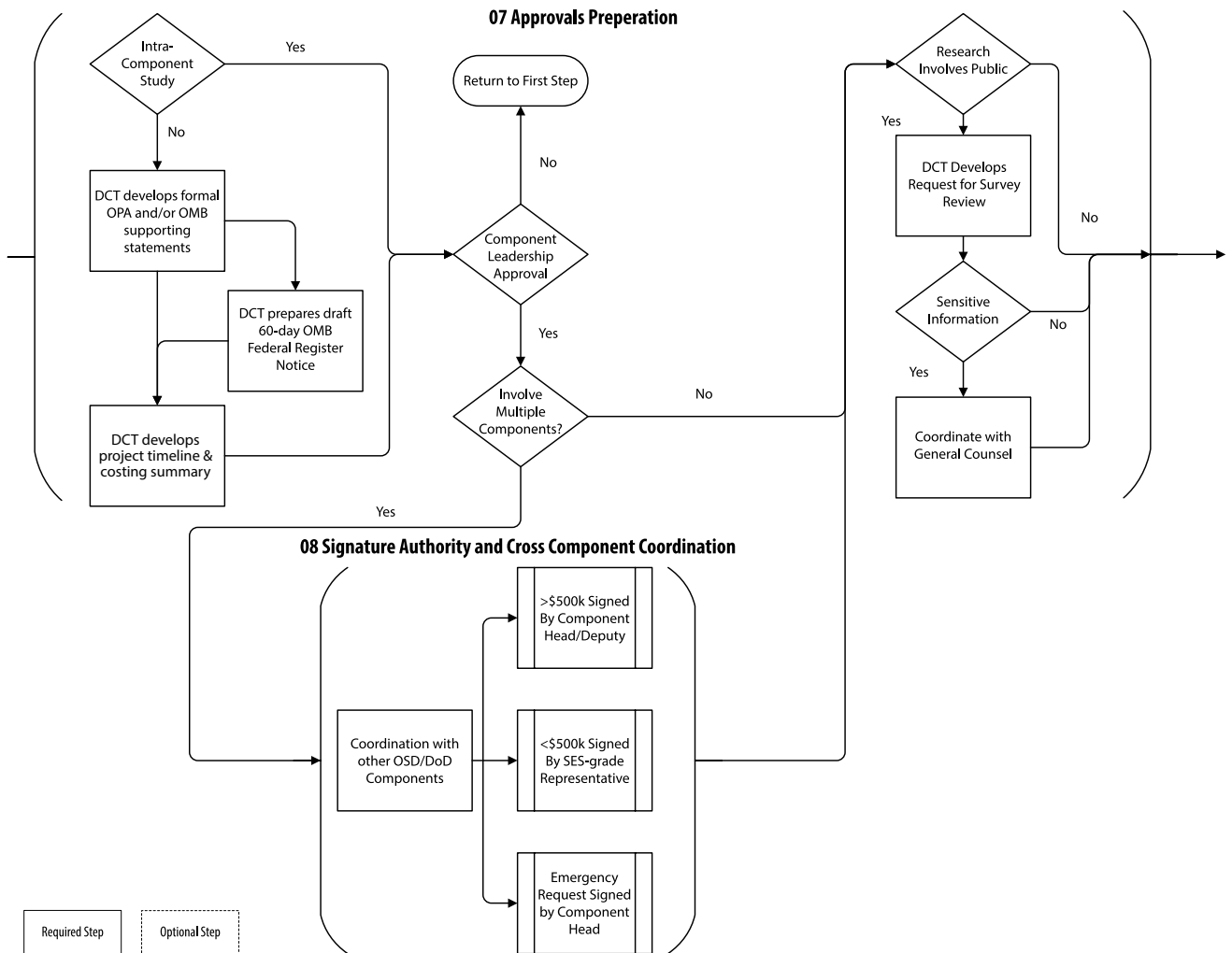
Within phase 7, the DCT also determines whether the proposed IC will involve members of the public—defined as individuals (including DOD contractors and foreign national employees), businesses, organizations, and governments other than federal. If so, the DCT develops the submission packet required to obtain OMB approval. These steps are captured in figure 5 (on page 9).

Depending on these determinations, there are three distinct licensing paths identified in phase 9 (see figure 6, page 10). Intracomponent IC requires only the component IMCO's approval and licensure, whereas intercomponent IC requires approval by the IMCO,

07 Approvals Preperation

(Figure by authors)

Figure 5. DOD IC Activity Process Flow Phases 7-8

between survey response rate and total survey data quality.[29] This relationship is so important, OMB mandates minimum survey and item response rates in U.S. government studies to protect data quality.[30]

Paradoxically, the DEE service disables embedded links in emails. As a result, DOD personnel receiving email invitations on DEE must then copy and paste the survey link into a separate browser on their DOD mobile, laptop, or desktop device. Having done that, the participant must then negotiate DOD cybersecurity protocols that block visits to sites not approved by the Defense Information Systems Agency (DISA). If the survey site resides outside the DOD network, it will likely be blocked for many participants. Potential participants are further discouraged from accessing links

to survey sites outside the DOD network by annual cybersecurity training, which instructs them not to trust links to unknown domains.[31] This is likely to further reduce survey response rates.[32]

DISA-approved survey platforms enable embedded links. Unfortunately, there are few DISA-approved survey platforms available on the DOD network. The exceptions are Qualtrics and Medallia, which offer DISA-approved installations on the DOD network. However, in our experience, their pricing is exponentially greater than most other research industry survey management solutions, and they are unaffordable for many DOD components.

DOD services and components have found other ways to meet their requirements. One component

09 Licensing
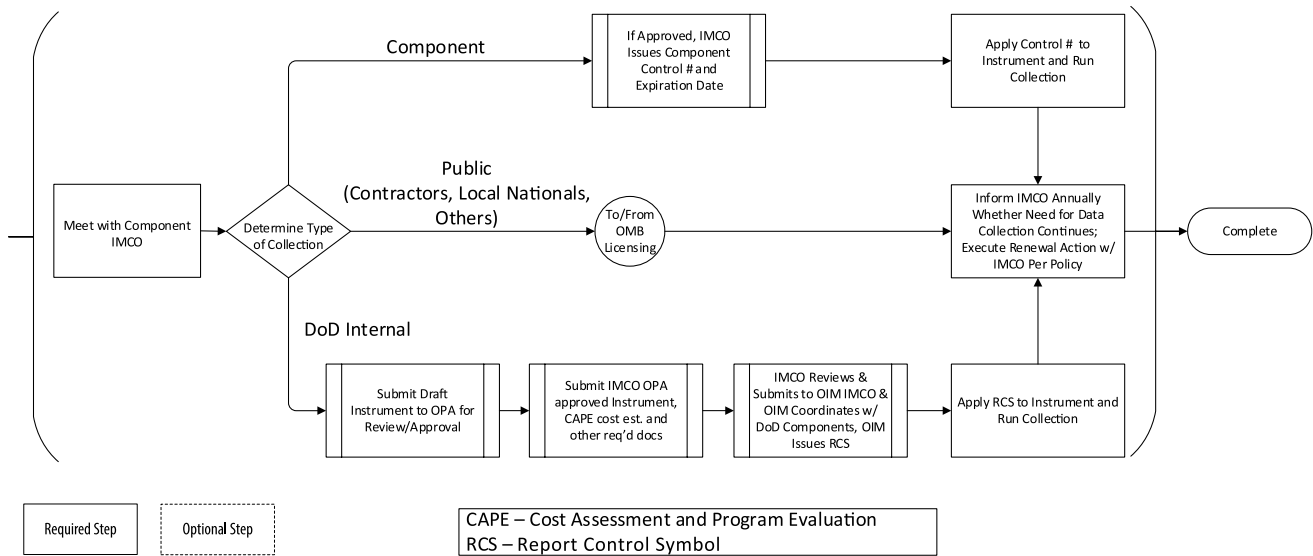
(Figure by authors)

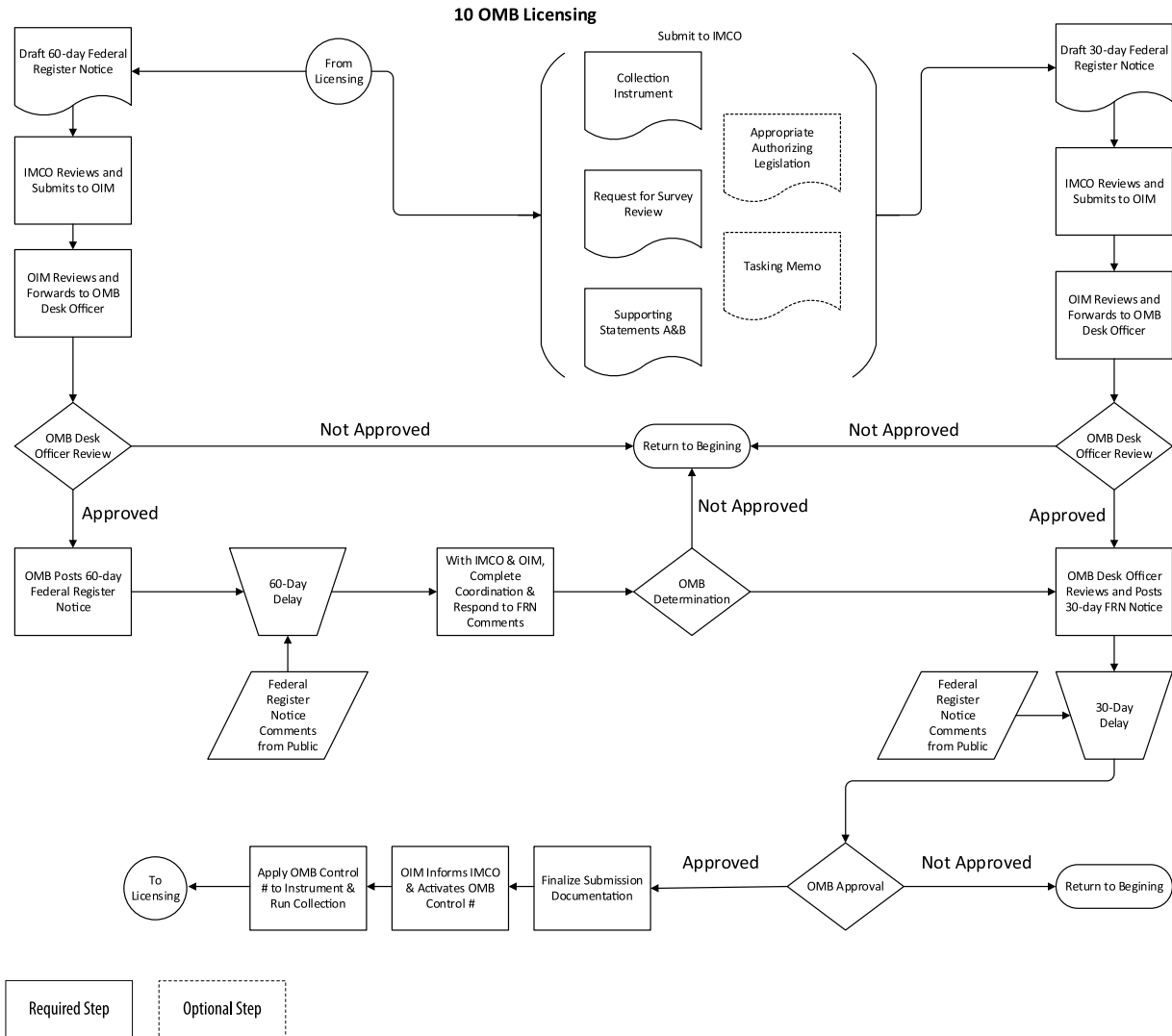## Figure 6. DOD IC Activity Process Flow Phase 9

created milSurvey, which is part of milSuite, to fill this gap. Some DOD components use the survey capabilities inside ServiceNow, and others use Microsoft Forms. Unfortunately, none of these solutions provide the sample management and respondent tracking capabilities required to understand and effectively manage the performance of a probability sample during the IC process.[33] These solutions also lack other fundamental capabilities of industry-standard survey engines used for probability surveys.

A small number of components have onboarded survey programs from the market and opinion research industry by completing the required authorization to operate process. These tools generally have all the capabilities required to properly conduct probability surveys. The two programs we have uncovered in the last twenty-four months of discovery are MAX Survey (managed by contractors supporting MAX. gov at OMB) and UNICOM Intelligence. However, as soon as we uncovered MAX Survey, we were advised it is scheduled for replacement with Microsoft Forms. Unfortunately, there is no systematic way for other components to find and review these authorized-to-operate tools because they are not on the DISA list.

Most survey platforms today are offered as software-as-a-service solutions. While the DOD CIO allows components to use software-as-a-service solutions outside the government cloud, the potential impact on survey response rate would likely be significant as a result of the external survey site blocking issue noted above.[34] Additionally, the information that can be collected from DOD personnel and reside on an external software-as-a-service solution may be limited, as subjects related to employment and other sensitive topics are considered controlled unclassified information that must be collected and stored on official DOD systems.[35] Moreover, collection of classified IC would not be possible with an external software-as-a-service configuration. As a result, the utility of a cost-effective external software-as-a-service survey solution will depend on the specific use case.

Recommendation. DOD components can consider vetting, acquiring, authorizing, and installing industry-standard survey engines on their own networks so long as the engines meet configuration and security requirements. This would potentially allow the component to send surveys from its own domain address and meet DOD network security requirements for protecting data while also costing less than current DISA-approved survey platforms. However, the installed survey software would need to meet DOD IT security approval. Commercially available solutions with authorizations to operate issued by other DOD components

Figure 7. DOD IC Activity Process Flow Phase 10

(Figure by authors)

or U.S. government agencies may already exist, but there is no systematic way to identify them. In the absence of a means for finding platforms with preexisting authorizations to operate, onboarding a platform with the strongest fit to the component's specific survey requirements may be the best solution.

Survey literature and practice recommend sending participants prenotification emails on DEE from DOD domains as well as text messages to government-issued mobile phones when possible. This may increase the acceptance and use of links in a later invitation email from the same domain by establishing authenticity.[36] As a standard practice, DOD components should consider sending pre-invitation emails to

online surveys on authorized systems inside the U.S. government network.

Participant burden and cybersecurity versus consent. Sociodemographic information is commonly used in surveys to design sample frames, draw differential samples based on characteristics of nonrespondents, and adjust data to reflect the population measured.[37] Information of this type about DOD personnel is commonly defined as PII. The DOD advocates for reconfirming PII with its source every time it is used to ensure the information is most accurate and current.[38] By implication, this would include surveys that ask PII-related questions. This confirmation practice is intended to allow participants the opportunity

to correct inaccuracies and reconfirm permission to use their data.

The DOD also defines PII as controlled unclassified information (CUI).[39] Re-asking PII questions on surveys therefore results in the collection of CUI on the survey platform selected. As noted above, this can limit the platform options available due to the associated data security requirements when housing DOD PII. For example, milSurvey explicitly excludes the collection of PII on its platform. Choice of platform in turn drives cost and most likely response rate.

In contrast, the Paperwork Reduction Act explicitly directs government agencies not to ask for information they have already gathered from other sources to reduce the burden on the public.[40] The IMCO is directed to promote this practice within DOD components.[41] In our case, this means avoiding asking survey participants questions to which we already have answers. It also means eliminating questions we do not need to ask to shorten the time required of participants to complete surveys. Survey length is a known factor in partial nonresponse, especially with the increasing use of mobile devices to take surveys.[42] Reducing survey length therefore also potentially increases data quality.

Recommendation. DMDC offers the types of sociodemographic information required for survey work. DMDC data can be transmitted and associated with survey records exported from any survey engine. Data from the two can be combined for analysis on CUI-authorized systems like DoD365-J, which is now the standard DOD operating platform. This gives components greater flexibility to select a survey platform based on cost and use case requirements as noted above. DMDC data can also be used to enrich the sampling frame data in ways question data cannot. This may allow for other forms of adjustment to the data to accommodate for any non-response issues the study might encounter.[43]

Cybersecurity versus DOD foreign national protections. The DOD employs foreign nationals in overseas locations. IC conducted outside the United States is required to be conducted in compliance with host-nation laws if applicable, particularly when citizens of the host nation are research subjects.[44]

Recent European Union (EU) court cases interpret the General Data Protection Regulation as restricting the collection and storage of local nationals' data on servers outside the EU.[45] DOD regulations require DOD data be housed on servers within the United States.[46] This makes the collection of survey data from DOD EU nationals located in Europe problematic.

Recommendation. The only straightforward solution to resolving this conflict is to omit all DOD foreign nationals from DOD component surveys where possible. ■

Notes

1. Chief Digital and Artificial Intelligence Office, accessed 29 July 2022, https://www.ai.mil/cdao.html.

2. Ibid.

3. Military Operations Research Society, "90th MORS Symposium Working Group Chairs," Military Operations Research Symposium (Working Groups), accessed 9 December 2022, https://www.mors.org/Events/Symposium/Past-Symposiums/2022-90th-Symposium.

4. Department of Defense Instruction (DODI) 5010.43, *Implementation and Management of the DoD-Wide Continuous Process Improvement/Lean Six Sigma (CPI/LSS) Program* (Washington, DC: Department of Defense [DOD], 17 July 2009), accessed 9 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501043p.pdf.

5. Joint Publication 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office, 2014), accessed 9 December 2022, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

6. DODI 8910.01, *Information Collection and Reporting* (Washington, DC: DOD, 8 July 2020), accessed 9 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/891001p.pdf.

7. Brenda J. Morgan et al., "What Is the Process? Approval of Survey Research in the Department of Defense (DoD)" (presentation, TSNRP Research/EBP Dissemination Course, Ellicott City, MD, 26 April 2017), accessed 15 December 2022, https://apps.dtic.mil/sti/pdfs/AD1037467.pdf.

8. Dale F. Spurlin and Sena Garven, "Unique Requirements for Social Science Human Subjects Research within the United States Department of Defense," *Research Ethics* 12, no. 3 (July 2016): 158–66, https://doi.org/10.1177/1747016115626198.

9. Defense Media Activity, accessed 29 July 2022, https://www.dma.mil/.

10. DODI 8550.01, *DoD Internet Services and Internet-Based Capabilities* (Washington, DC: DOD, 11 September 2012),

accessed 9 December 2022, http://fas.org/irp/doddir/dod/i8550_01.pdf.

11. DODI 1100.13, *DoD Surveys* (Washington, DC: DOD, 31 March 2017), accessed 9 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/110013p.pdf?ver=2019-04-08-125316-290.

12. DOD Manual (DODM) 8910.01, *DoD Information Collections Manual: Procedures for DoD Public Information Collections*, vol. 2 (Washington, DC: DOD, 18 February 2022), accessed 9 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol2.pdf?ver=2017-06-20-125411-733.

13. DODI 1100.13, *DoD Surveys*.

14. DODM 8910.01, *DoD Information Collections Manual*, vol. 2.

15. DODM 8910.01, *DoD Information Collections Manual: Procedures for DoD Internal Information Collections*, vol. 1 (Washington, DC: Department of Defense, 2022), accessed 9 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol1.pdf.

16. DODM 8910.01, *DoD Information Collections Manual*, vol. 2.

17. DODI 1100.13, *DoD Surveys*.

18. DODI 3216.02, *Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and -Supported Research* (Washington, DC: DOD, 15 April 2020), accessed 12 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/321602p.pdf.

19. DODI 5400.11, *DoD Privacy and Civil Liberties Programs* (Washington, DC: DOD, 8 December 2020), accessed 12 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540011p.pdf.

20. Ibid.

21. Ibid.

22. DODM 8910.01, *DoD Information Collections Manual*, vol. 2.

23. Ibid.

24. Ibid.

25. DODM 8910.01, *DoD Information Collections Manual*, vol. 1.

26. Valerie M. Sue and Lois A. Ritter, *Conducting Online Surveys*, 2nd ed. (Los Angeles: SAGE, 2012), 108–9.

27. Ibid.

28. Scott D. Crawford, Mick P. Couper, and Mark J. Lamias, "Web Surveys: Perceptions of Burden," *Social Science Computer Review* 19, no. 2 (May 2001): 146–62, https://doi.org/10.1177/089443930101900202; Dirk Heerwegh and Geert Loosveldt, "Web Surveys: The Effect of Controlling Survey Access Using PIN Numbers," *Social Science Computer Review* 20, no. 1 (February 2002): 10–21, https://doi.org/10.1177/089443930202000102.

29. Ineke Stoop et al., *Improving Survey Response: Lessons Learned from the European Social Survey* (Hoboken, NJ: John Wiley & Sons, 2010), 3–5.

30. Office of Management and Budget, *Standards and Guidelines for Statistical Surveys* (Washington, DC: Office of Management and Budget, September 2006), accessed 12 December 2022, https://www.ftc.gov/system/files/attachments/data-quality-act/standards_and_guidelines_for_statistical_surveys_-_omb_-_sept_2006.pdf.

31. "Cyber Awareness Challenge 2023," DOD Cyber Exchange, accessed 26 July 2022, http://public.cyber.mil/training/cyber-awareness-challenge/.

32. Heerwegh and Loosveldt, "Web Surveys."

33. Sue and Ritter, *Conducting Online Surveys*, 109–10.

34. DODI 8550.01, *DoD Internet Services and Internet-Based Capabilities*.

35. DODI 5200.48, *Controlled Unclassified Information* (CUI) (Washington, DC: DOD, 6 March 2020), accessed 12 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF.

36. Michael Bosnjak et al., "Prenotification in Web-Based Access Panel Surveys: The Influence of Mobile Text Messaging Versus E-Mail on Response Rates and Sample Composition," *Social Science Computer Review* 26, no. 2 (May 2008): 213–23, https://doi.org/10.1177/0894439307305895; Stoop et al., *Improving Survey Response*; Michael Kaplowitz et al., "The Effect of Invitation Design on Web Survey Response Rates," *Social Science Computer Review* 30, no. 3 (August 2012): 339–49, https://doi.org/10.1177/0894439311419084.

37. Stoop et al., *Improving Survey Response*, 55, 59, 211–12.

38. DODI 5400.11, *DoD Privacy and Civil Liberties Programs*.

39. DOD 5400.11-R, *Department of Defense Privacy Program* (Washington, DC: DOD, 14 May 2007), accessed 12 December 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011r.pdf.

40. GPRA Modernization Act of 2010, Pub. L. No. 111-352, 124 Stat. 3866 (2011).

41. DODM 8910.01, *DoD Information Collections Manual*, vol. 1.

42. Melanie Revilla and Jan Karem Höhne, "How Long Do Respondents Think Online Surveys Should Be? New Evidence from Two Online Panels in Germany," *International Journal of Market Research* 62, no. 5 (September 2020): 538–45, https://doi.org/10.1177/1470785320943049; Kaplowitz et al., "The Effect of Invitation Design."

43. Stoop et al., *Improving Survey Response*, 210–12.

44. DODI 3216.02, *Protection of Human Subjects*.

45. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (16 July 2020), accessed 15 December 2022, http://curia.europa.eu/juris/liste.jsf?num=C-311/18; Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, accessed 15 December 2022, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

46. Required Storage of Data Within the United States or Outlying Areas, 48 C.F.R. § 239.7602-2 (2022), accessed 12 December 2022, https://www.ecfr.gov/current/title-48/chapter-2/subchapter-F/part-239/subpart-239.76/section-239.7602-2.