Resolving Constraints on the Creation of U.S. Department of Defense Survey Information Collection Capabilities

Karl G. Feld & E. Lee Hill

Vistra Communications, Washington D.C.

Author Note

Karl G. Feld https://orcid.org/0000-0002-4337-6425

E. Lee Hill https://orcid.org/0000-0002-4386-5632

The authors would like to recognize the invaluable contribution of Judith M. Thompson to assembling the reference materials used for this paper and Victoria A. Leoni to the preparation of the manuscript.

Correspondence concerning this article should be addressed to Karl G. Feld, Vistra Communications, 217 Mantle Drive, Clayton, NC 27527, United States. Email: karlf@consultvistra.com.

Abstract

Vistra Communications is consulting with the Defense Media Activity (DMA) to establish new survey information collection programs within the Activity that better service the Department of Defense (DoD) public affairs enterprise. No single narrative document exists to outline the changes in business processes or organizational practices necessary for a DoD office, agency, activity, or command to launch new survey information collection activities in compliance with the many governing DoD Instructions and parts of the Code of Federal Regulations. These governing rules and regulations address human research protection, participant privacy, Personally Identifiable Information (PII) protection, cost control, cross-DoD coordination, and data sharing requirements. This case study discusses the organizational change steps Vistra Communications recommended DMA develop to implement in-house survey information collection activities in compliance with the requirements. The presentation highlights natural tensions in DoD policy between data privacy, cybersecurity, consent, survey response rates, questionnaire design, and sample administration. It addresses lessons learned and provides advice for others who want to launch new survey information collection activities for elements of the DoD. References to governing DoD Instructions and regulations are included.

Keywords: DoD, PII, human subjects research, privacy, consent, cybersecurity

Constraints on the Creation of U.S. Department of Defense Survey Information Collection Capabilities

This article contributes to human subject research protection and privacy literature by outlining and attempting to resolve tensions in U.S. Department of Defense (DoD) requirements imposed by different DoD Instructions (DoDI). It is based on lessons learned by Vistra Communications while providing consultive services to the Defense Media Activity (DMA) to develop survey programs to inform the organization's Lean Six Sigma (LSS)/Continuous Process Improvement (CPI) work. Specifically, Vistra Communications has consulted with DMA on conducting probability-based surveys with various DoD customer and media audience populations. We conclude by providing advice for others who seek to launch survey initiatives for DoD components using probability-based sampling.

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" (Chief Information Officer, 2020a).

Background

In May 2006, the Deputy Secretary of Defense directed the use of LSS/CPI approaches throughout the many agencies, military services, and field activities of the DoD (known as DoD components) to improve operating effectiveness in support of the warfighter (Deputy Secretary of Defense, 2006). The 2010 Government Performance and Results Modernization Act (U.S. House of Representatives, 2010) also requires each U.S. Government agency to set objectively quantifiable performance goals and report progress against those goals using valid, verifiable data.

The Continuous Process Improvement Transformation Guidebook (2006) was issued to outline how the LSS/CPI process should unfold within each DoD component. Vistra Communications is engaged with DMA to incorporate LSS/CPI measurement, analysis, and control elements into the organization's designs to improve its activities and outputs. LSS/CPI work is grounded in social science techniques used to measure and track various initiatives. These techniques include surveys (Munro et al., 2015).

DMA is considering using surveys to inform LSS/CPI metrics for media measurement and Voice of the Customer (VoC) research. DMA manages the DoD's American Forces Network (https://www.dma.mil/DMA-Products/American-Forces-Network/) radio and television broadcasting as well as a wide array of DoD website platforms and social media channels. DMA also produces content for these platforms. For performance metrics, DMA seeks to measure the reach and impact of its public affairs media content and transmissions on DoD target audiences.

VoC research provides the key metrics for LSS/CPI programs (Munro et al., 2015). It gathers business intelligence on customers' requirements and perceptions of the organization's performance. To support its CPI efforts, DMA is considering VoC social science research to gather feedback from its customers on how well they perceive DMA is meeting their requirements.

VoC and media research by definition involve human subjects. DoD human subjects research (HSR) requires compliance with a wide variety of DoD authorities and instructions to protect the interests of HSR subjects and information security, especially in today's online information collection (IC) and electronic data storage environment. In some cases, the 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, cross-DoD coordination, and data sharing requirements. HSR and 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 component of the DoD to ensure it follows all the instructions from all the authorities that impact HSR and IC.

Method: Review of DoD Authorities

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

As a result, no single narrative document exists to outline the business processes or organizational practices necessary for a DoD component to launch new HSR IC in compliance with the many governing DoD Instructions and parts of the Code of Federal Regulations. These governing rules and regulations address topics like human research protection, participant privacy, Personally Identifiable Information (PII) protection, cost control, cross-DoD coordination, and data sharing requirements. This paper addresses this shortcoming with a summary of each governing entity's role provided below. The relevant DoDIs are provided in the References section of this paper.

DoD Chief Information Officer (CIO)

The DoD CIO sets policy for all DoD IC. The Office of the CIO (OCIO): (1) seeks to reduce the number and frequency of IC activities, (2) approves IC budgets, and (3) 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 (CIO, 2012).

DoD Under Secretary of Defense for Personnel and Readiness (USD(P&R))

The USD(P&R) provides mandatory coordination for all HSR IC that includes DoD employees in more than one component (Department of Defense, 2017). The USD(P&R) is also responsible for recommending approval or disapproval of this kind of HSR 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 (Director of Administration and Management, 2022b).

The Director, Office of People Analytics (OPA) (under the authority of Director, Defense Human Resources Activity) manages these tasks for the USD(P&R) (Department of Defense, 2017). OPA reviews proposed HSR 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 (Director of Administration and Management, 2022b). OPA can disapprove collection instruments or methodologies. OPA also reviews public IC applications before submission to the OMB, if applicable.

Director, Washington Headquarters Services (WHS)

The WHS Director controls HSR IC activity. The Chief of the Directives Division, Executive Service Directorate acts as the DoD Information Collections Officer (ICO) for the WHS Director (Director of Administration and Management, 2022a). The ICO determines if HSR 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 DoD approving authority (e.g., OMB). The ICO is the primary point of contact with the OMB for all DoD HSR IC involving the public (Director of Administration and Management, 2022b). The ICO sends 60-day notices of public IC to the Federal Register for public comment as required. The ICO also submits the required 30-day notice when proposed HSR IC has been sent to the OMB for review (Department of Defense, 2017).

DoD Directorate of Human Research Protections (DOHRP)

The DOHRP operates under the authority of the Under Secretary of Defense for Research and Engineering. A DOHRP-approved component Human Research Protection Program management plan (CMP) must be in place at the DoD component before it can conduct or support any HSR IC. The DOHRP conducts component Human Research Protection Program assessments every year and can conduct site inspections. The DOHRP can also halt studies or rescind component IC authorities as needed (Office of the Under Secretary of Defense for Research and Engineering, 2020).

Director, Defense Manpower Data Center (DMDC)

DMDC maintains the master list of DoD personnel and their Personally Identifiable Information (PII) used to generate DoD survey samples of employees, internal customers, and internal audiences. 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 (DPCLTD). DMDC also ensures compliance with those matching agreements (Office of the Chief Management Officer, 2020).

Chief, Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD)

The DPCLTD coordinates and maintains DMDC matching agreements and reviews changes to System of Records Notices (SORNs) that protect survey sample PII on component IT systems (Office of the Chief Management Officer, 2020).

Director, Directorate for Oversight and Compliance (DO&C)

In conjunction with the DoD CIO, the DO&C Director is required to ensure all DoD components comply with OMB requirements for the protection of PII (Office of the Chief Management Officer, 2020).

Office of Management and Budget (OMB)

In cases when DoD HSR IC is proposed with 10 or more members of the public within 12 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

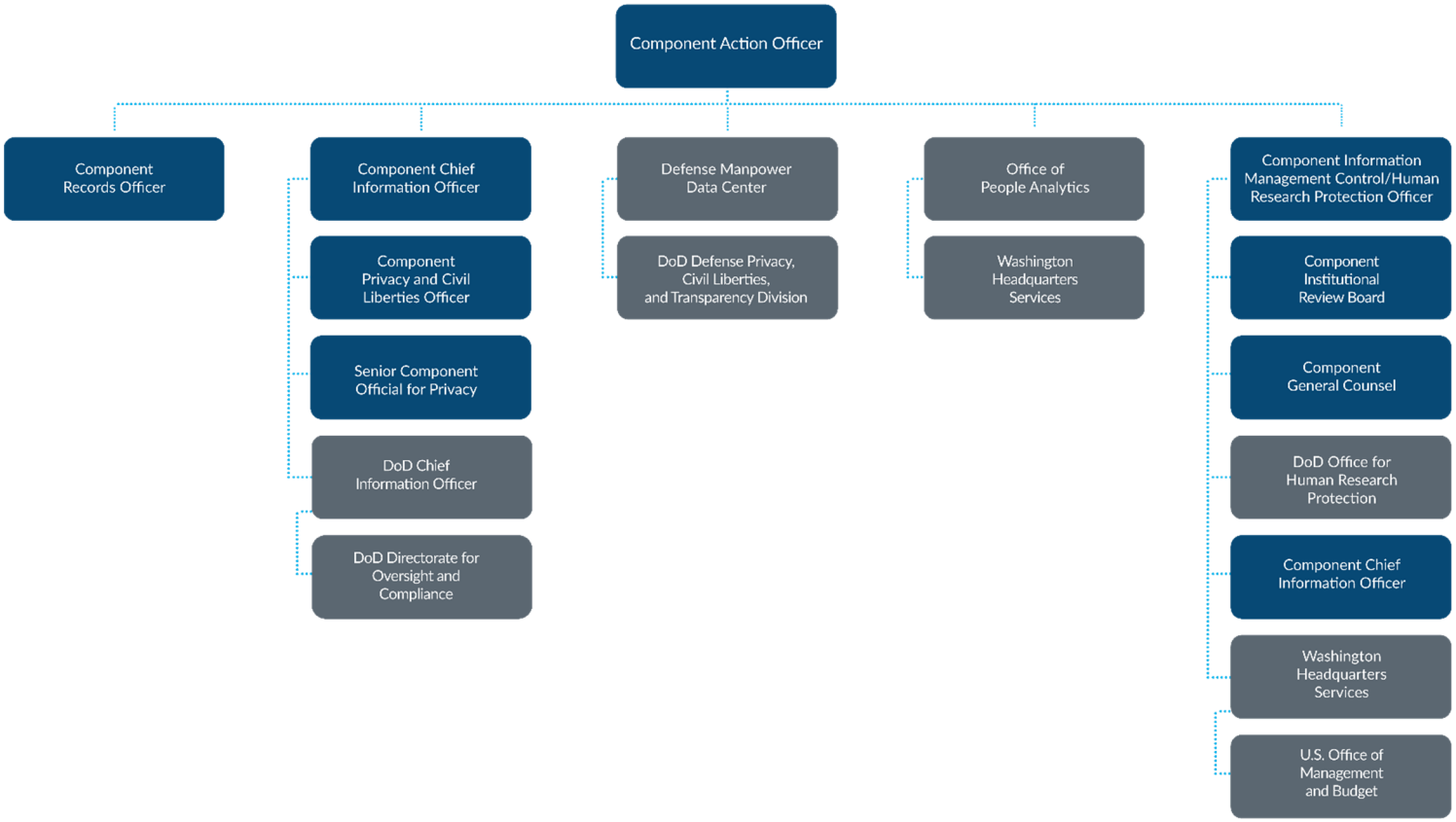
individual private citizens. Defense contractors and foreign nationals are also defined as members of the public (Director of Administration and Management, 2022b).

The OMB provides a Report Control Symbol (RCS) and expiration date for approved HSR IC. OMB approval can be a six-month process unless expedited, although faster generic and emergency clearances are possible (Director of Administration and Management, 2022b). As part of its review, OMB gathers comments based on a 30-day notice in the Federal Register about the proposed HSR IC. Comments are used to ensure the information proposed to be collected is not already available and appropriate efforts are being made to minimize the public burden and maximize practical utility (Director of Administration and Management, 2022b).

The Component Information Management Control Officer and Action Officer

Figure 1 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 (AO) 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 AO's interface with numerous governing authorities as he/she 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 (COHRP) responsible for reviewing surveys against the component Human Research Protection Plan and managing any Institutional Review Board requirements (Director of Administration and Management, 2022a).

Figure 1. Coordination relationships for DoD digital information collections. Each entity represented is responsible for coordinating with those it is connected to. Entities that are part of a single DoD component are shown in blue. Entities outside the component conducting the survey are shown in gray.



Discussion: Approaches to Tensions in DoD Guidance

In the course of designing and preparing survey work with DMA AOs and IMCO, we have identified a number of tensions in the relevant DoDIs and other 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 (i.e., 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 (Sue & Ritter, 2011). 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 (Sue & Ritter, 2011).

Each mouse click or other task a participant must complete to begin a survey has the potential to reduce survey response rates (Crawford et al., 2001; Heerwegh & Loosveldt, 2002). There is a direct relationship between survey response rate and total survey data quality (Stoop et al., 2010). This relationship is so important the OMB mandates minimum survey and item response rates in U.S. government studies to protect data quality (Office of Management and Budget, 2006).

Paradoxically, the DEE service disables embedded links in emails. As a result, DoD personnel receiving email invitations on DEE must then copy and paste that link address into a separate browser on their DoD mobile device or desktop machine. 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 (DoD Cyber Exchange Public, 2022). This is likely to further reduce survey response rates (Heerwegh & Loosveldt, 2002).

Unfortunately, there are few DISA-approved survey platforms available on the DoD network. DoD users created milSurvey to fill this gap. Some DoD components use the survey capabilities inside ServiceNow, and others use Microsoft Forms. Unfortunately, none of these solutions provide sample management and respondent tracking capabilities required to understand and effectively manage the performance of probability sample during the IC process (Sue & Ritter, 2011). These solutions also lack other fundamental capabilities of industry-standard survey engines used for probability surveys.

The exceptions to this 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. While the DoD CIO does allow the use of Software-as-a-Service (SaaS) solutions by components (Chief Information Officer, 2012), the potential impact on survey response rate would likely be significant as a result of the external survey site blocking issue noted above. Additionally, the information that can be collected from DoD personnel and reside on a SaaS solution may be limited, as subjects related to employment and other sensitive topics are considered Controlled Unclassified Information (CUI) that must be collected and stored on official DoD systems (Office of the Undersecretary of Defense for

Intelligence and Security, 2020). Moreover, classified IC would not be possible with a SaaS configuration. As a result, the utility of a cost-effective SaaS survey solution will depend on the specific use case.

Participant Burden & Cybersecurity Versus Consent

Socio-demographic information is commonly used in surveys to: (1) design sample frames, (2) draw differential samples based on non-respondent characteristics, and (3) adjust data to reflect the population being measured (Stoop et al., 2010). 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 up to date (Office of the Chief Management Officer, 2020). 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 CUI (Office of the Director, Administration and Management, 2007). Re-asking for PII 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.

However, the Paperwork Reduction Act (U.S. House of Representatives, 2011) explicitly directs government agencies not to ask for information they have already gathered from other sources so as to reduce the burden on the public. The IMCO is directed to promote this practice within DoD components (Director of Administration and Management, 2022a). 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 so as to shorten the time required of participants to complete surveys. Survey length is also a known factor in partial non-response, especially with the increasing use of mobile devices to take surveys (Revilla & Höhne, 2020; Kaplowitz et al., 2012). Reducing survey length therefore also potentially increases data quality.

Cybersecurity Versus DoD Foreign National Protections

The DoD employs foreign nationals in overseas locations. HSR 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 (Office of the Under Secretary of Defense for Research and Engineering, 2020).

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 (Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, 2020; Official Journal of the European Union, 2016). DoD regulations require DoD data be housed on servers within the United States (U.S. Government Services Administration, 2020). This makes the collection of survey data from DoD EU nationals located in Europe problematic.

Recommendations

Cybersecurity Versus Survey Response

DoD components can consider vetting, acquiring, 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.

Survey literature and practice recommend sending participants pre-notification 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 (Bosnjak et al., 2008; Stoop et al., 2010; Kaplowitz et al., 2012). DoD components should consider sending pre-invitation emails to online surveys as a standard practice.

Participant Burden & Cybersecurity Versus Consent

DMDC offers the types of socio-demographic 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 (Stoop et al., 2010).

Cybersecurity Versus DoD Foreign National Protections

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

References

Bosnjak, M., Neubarth, W., Couper, M. P., Bandilla, W., & Kaczmirek, L. (2008). 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*(2), 213-223. https://journals.sagepub.com/doi/abs/10.1177/0894439307305895

Chief Information Officer. (2012). DoD Internet Services and Internet-Based Capabilities. DoDI 8550.01. [Operating Instruction]. US Department of Defense. http://fas.org/irp/doddir/dod/i8550_01.pdf

Chief Information Officer. (2014). Cybersecurity. DoDI 8500.01. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

Chief Information Officer. (2020a). Information Collection and Reporting, Incorporating Change 1. DoDI 8910.01. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/891001p.pdf

Chief Information Officer. (2020b). Risk Management Framework (RMF) for DoD Information Technology (IT), Incorporating Change 3. DoDI 8510.01. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

Crawford, S. D., Couper, M. P., & Lamias, M. J. (2001). Web Surveys: Perceptions of Burden. *Social Science Computer Review, 19*(2), 146-162. https://journals.sagepub.com/doi/abs/10.1177/089443930101900202

Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems. Case C-311/18, 559 (ECLI:EU:C 2020). https://curia.europa.eu/juris/documents.jsf?num=C-311/18

Defense Protection of Human Subjects. 32 C.F.R. § 219 (2021). https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-M/part-219?toc=1

Department of Defense. (2017). DoD Surveys, Incorporating Change 1. DoDI 1100.13. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/110013p.pdf?ver=2019-04-08-125316-290

Deputy Secretary of Defense. (2006). Continuous Process Improvement Transformation Guidebook. US Department of Defense. https://apps.dtic.mil/sti/pdfs/ADA485632.pdf

Director of Administration and Management. (2022a). DoD Information Collections Manual: Procedures for DoD Internal Information Collections, Incorporating Change 3. DoD Manual 8910.01, Vol. 1. [Operating Manual]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol1.pdf?ver=2019-08-13-091528-487

Director of Administration and Management. (2022b). DoD Information Collections Manual: Procedures for DoD Public Information Collections, Incorporating Change 3. DoD Manual 8910.01, Vol. 2. [Operating Manual]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/891001m_vol2.pdf?ver=2017-06-20-125411-733

DoD Cyber Exchange Public. (2022). Cyber Awareness Challenge 2022. Defense Information Systems Agency. http://public.cyber.mil/training/cyber-awareness-challenge/

Heerwegh, D. & Loosveldt, G. (2002). Web Surveys: The Effect of Controlling Survey Access Using PIN Numbers. *Social Science Computer Review, 20*(1). 10-21. https://journals.sagepub.com/doi/abs/10.1177/089443930202000102

Kaplowitz, M. D., Lupi, F., Couper, M. P., & Thorp, L. (2012). The Effect of Invitation Design on Web Survey Response Rates. *Social Science Computer Review*, *30*(3), 339-349. https://journals.sagepub.com/doi/full/10.1177/0894439311419084

Munro, R. A., Ramu, G., & Zrymiak, D. J. (2015). *The Certified Six Sigma Green Belt Handbook* (2nd ed.). ASQ Quality Press.

Office of Management and Budget. (2006). *Standards and Guidelines for Statistical Surveys.* https://www.ftc.gov/system/files/attachments/data-quality-act/standards_and_guidelines_for_statistical_surveys_-_omb_-_sept_2006.pdf

Office of the Chief Management Officer. (2020). DoD Privacy and Civil Liberties Programs. DoDI 5400.11. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540011p.pdf

Office of the Chief Records Officer. (2015). General Records Schedules. Transmittal No. 24. National Archives and Records Administration. https://www.archives.gov/files/records-mgmt/grs/grs-transmittal-24.pdf

Office of the Director, Administration and Management. (2007). Department of Defense Privacy Program. DoD 5400.11-R. [Regulation]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011r.pdf

Office of the Under Secretary of Defense for Intelligence and Security. (2020). Controlled Unclassified Information (CUI). DoDI 5200.48. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF

Office of the Under Secretary of Defense for Research and Engineering. (2020). Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and -Supported Research. DoDI 3216.02. [Operating Instruction]. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/321602p.pdf

Official Journal of the European Union. (2016). Regulation (EU) 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). L 119, 1–88. https://gdpr-info.eu/

Orszag, P. (2010a). Guidance for Online Use of Web Measurement and Customization Technologies. M-10-22. [Policy Memo]. Office of Management and Budget. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

Orszag, P. (2010b). Guidance for Agency Use of Third-Party Websites and Applications. M-10-23. [Policy Memo]. Office of Management and Budget. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

Revilla, M. & Höhne, J. K. (2020). How long do respondents think online surveys should be? New evidence from two online panels in Germany. *International Journal of Market Research. (62)*5, 538-545. https://journals.sagepub.com/doi/full/10.1177/1470785320943049

Stoop, I., Billiet, J., Koch, A., & Fitzgerald, R. (2010). *Improving Survey Response: Lessons Learned from the European Social Survey*. Wiley Series in Survey Methodology (eds. Kalton, G., Couper, M. P., Lyberg, L., Rao, J. N. K., Schwarz, N., Skinner, C.). John Wiley & Sons, Ltd.

Sue, V. M. & Ritter, L. A. (2012). *Conducting Online Surveys.* Sage Publications.

U.S. General Services Administration. (2020). Required storage of data within the United States or outlying areas. Defense Federal Acquisition Regulation 239.7602-2, Vol. 3, Parts 201-253. https://acquisition-uat.gsa.gov/dfars/239.7602-2-required-storage-data-within-united-states -or-outlying-areas.

U.S. House of Representatives. (2011). 111th Congress, 2nd Session. *H.R.2142, GPRA Modernization Act of 2010.* https://www.congress.gov/bill/111th-congress/house-bill/2142