NISTIR 8420

Federal Cybersecurity Awareness Programs

A Mixed Methods Research Study

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8420

Federal Cybersecurity Awareness Programs

A Mixed Methods Research Study

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420

March 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8420
48 pages (March 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Prior industry surveys and research studies have revealed that organizational cybersecurity awareness (hereafter shortened to "security awareness") programs may face a number of challenges, including lack of: leadership support; resources; and staff with sufficient background and skills to implement an effective and engaging program. However, no prior research has explored security awareness programs specifically in the United States (U.S.) government (federal) sector. To address this gap, NIST conducted a two-phase, mixed methods research study to understand the needs, challenges, and practices of federal security awareness programs. This report describes the research background and methodology, along with the characteristics of the participants, organizations, and programs represented in the study. Research results can serve as a resource for federal security awareness professionals, managers, and organizational decision makers to improve and advocate for their organizations' security awareness programs. Results can also inform the development of federal security awareness guidance, policies, sharing forums, and initiatives meant to aid programs in becoming more effective. While focused on the U.S. government, findings may also have implications for organizational security awareness programs in other sectors.

Keywords

cybersecurity; cybersecurity awareness; focus groups; mixed methods; security professionals; survey; training; usable cybersecurity

Table of Contents

List of Appendices

List of Figures

1 Introduction

Despite an abundance of cybersecurity guidance and technologies, employees continue to fall prey to cyber attacks, putting both themselves and their organizations at risk. This problem was exemplified by an Office of Management and Budget report that stated 53% of U.S. government cyber incidents in 2020 resulted from employees violating acceptable usage policies or succumbing to email or phishing attacks [OMB2020]. Cybersecurity awareness (hereafter shortened to "security awareness") training can be a first step towards helping employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change [WILSON]. In some organizations and sectors this training is mandated for all employees, as is the case for U.S. government agencies [FISMA][OMB2016].

Unfortunately, security awareness efforts may face significant challenges. Industry surveys and research studies have discovered that security awareness programs in organizations of all sizes may be underfunded and often rely on part-time security awareness professionals who may lack sufficient background, skills, tools, or resources necessary for managing an effective program [SANS][WOELK][BADA][STEWART]. Furthermore, employees may view training as boring and burdensome [BADA]. While mandates enforce a minimum baseline for security awareness, when viewed simply as a "check-the-box" exercise, organizations may begin to measure program success simply in terms of compliance metrics, like training completion rates. However, these metrics reveal little about the effectiveness of the training in changing and sustaining workforce attitudes and behaviors [FERTIG].

Although evidence of security awareness challenges and recommendations abound, it is currently unknown whether these apply to programs within the U.S. government (federal) sector and if government organizations experience additional issues. To address this gap, NIST completed research to better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs. The research consisted of two phases: eight focus groups of federal security awareness professionals which informed the development of a follow-on, online survey completed by 96 federal employees involved in their security awareness programs. Research results are directly informing government efforts to produce guidance and resources to aid federal security awareness programs.

This report provides an overview of the research, including a description of the research methodologies and the participants, organizations, and security awareness programs represented in the study. Two companion documents report on the results of the study. Each document addresses an overarching theme focused on a subset of research questions:

NIST 8420A "Approaches and Challenges of Federal Cybersecurity Awareness Programs"

- What approaches and techniques do federal agencies employ in their security awareness programs?
- What's working well with respect to security awareness programs in federal agencies?
- What's not working well? What are the challenges and concerns of federal security awareness programs?
- How do organizations determine the effectiveness of the security awareness program?
- What resources and guidance are used to inform the security awareness programs?

- What do programs feel like they need to be more successful? What kinds of resources would be most beneficial?

NISTIR 8420B "The Federal Cybersecurity Awareness Workforce: Professional Backgrounds, Knowledge, Skills, and Development Activities"

- What job classifications and work roles do federal security awareness professionals currently have?
- What are the professional backgrounds of these professionals?
- What are the desired knowledge and skills of federal security awareness professionals?
- What professional development activities do these professionals engage in?
- Do federal security awareness professionals feel they have adequate professional development opportunities?

The target audience of this report consists of individuals involved with federal security awareness programs. The report can serve as a resource for federal security awareness professionals, managers, and organizational decision makers to improve and advocate for their organizations' security awareness programs. Those who develop and manage federal security awareness guidance, policies, sharing forums, and initiatives may also benefit in their efforts to aid programs in becoming more effective. The report may also be valuable to security awareness professionals outside of the government who face similar challenges. Additionally, although this study refers to security awareness programs, its focus is not only relevant to awareness but also to security training issues as well.

This report is organized as follows. Section 2 describes the research methodology, including study design, participant recruitment, data collection, and analysis. Section 3 provides information about the participants and organizations represented in the study. Section 4 summarizes the report.

2 Study Methodology

To explore federal security awareness programs, the study used a "mixed methods" research approach that leveraged both qualitative and quantitative methodologies [CLARK]. Qualitative research is used to capture why or how a phenomenon occurs as well as people's experiences, beliefs, and motivations. Quantitative research methodologies involve "quantifiable" data (e.g., numerical or ordinal data) and are more focused on establishing generalizability or magnitude. Mixed methods studies take advantage of the strengths of both approaches.

We conducted the study in two sequential phases. In the first phase, we collected qualitative data via eight focus groups of federal employees involved in their organizations' security awareness programs. The focus groups provided an understanding of how people think and talk about security awareness topics and what concepts and challenges participants viewed as most important. These insights then informed a second phase consisting of a predominantly quantitative online survey (96 responses) of federal employees involved in their security awareness programs. This report integrates the results from both the focus groups and the survey.

The National Institute of Standards and Technology Research Protections Office reviewed the

protocol for this research project (ITL-2020-0238) and determined it meets the criteria for "exempt human subjects research" as defined in 15 CFR 27, the Common Rule for the Protection of Human Subjects. Prior to data collection, participants were informed of the study purpose and how their data would be protected. Data were recorded without personal identifiers and not linked back to individuals or organizations. Throughout this report, any mentions of participant organizations or other potentially identifying information has been redacted.

2.1 Focus Group Methodology

2.1.1 Focus Group Design

When designing the focus groups, we consulted seven subject matter experts (SMEs), including veteran security awareness professionals and past and current coordinators of federal security collaboration forums that address security awareness topics. The SMEs provided input into the study's overall direction, focus group questions, and participant recruitment strategies.

We selected a multiple-category design for the focus groups, which involved focus groups with several types of participants to allow for comparisons across or within categories [KRUEGER]. Based on SME discussions, we decided on three categories: 1) Department-level organizations (e.g., U.S. Department of Commerce), 2) Sub-component agencies, which are semi-autonomous organizations under a Department (e.g., NIST is a sub-component under Department of Commerce), and 3) Independent agencies, which are not in a Department.

The focus group protocol consisted of 11 questions covering topics such as security awareness approaches, successes, challenges, measures of effectiveness, wish lists, and necessary knowledge and skills for security awareness teams. See Appendix C for the full protocol.

2.1.2 Focus Group Recruitment

We selected potential focus group participants to represent the diversity of federal agencies. We identified participants via several avenues: recommendations from the SMEs; researchers' professional contacts; an online cybersecurity-focused mailing list for the Small and Micro Agencies Chief Information Security Officer (CISO) Council [SMAC]; speakers and security awareness material contest participants from the last three years of the Federal Information Security Educators (FISSEA) conference [FISSEA]; and LinkedIn and Google searches. Participants had to be federal employees and have knowledge of the security awareness programs in their organizations either because they had security awareness duties or oversaw the programs.

2.1.3 Focus Group Data Collection

Between December 2020 and January 2021, we conducted eight virtual focus groups with 29 total participants. Focus group sessions lasted 60-75 minutes, with each having 3-5 participants. Multiple focus groups were conducted for each category of organization. Table 1 shows the number of participants in each focus group. The sub-component #2 focus group included two participants from the same organization. In all, 12 independent agencies and 9 of the 15 unique Executive Branch Departments (considering both the department-level and sub-component participants) were represented in the focus groups.

Table 1: Focus Groups

Focus Group	Number of Participants
Department #1	3
Department #2	3
Sub-component #1	3
Sub-component #2	5
Sub-component #3	3
Independent #1	4
Independent #2	4
Independent #3	4

All focus groups were audio recorded and transcribed. Participants also completed a short, online survey to gather demographic and organizational information (Appendix B). To ensure anonymity and to be able to confidentially link data between the focus groups and demographic survey, we assigned each participant a reference code.

2.1.4 Focus Group Data Analysis

Data analysis started with coding, which involves categorization of focus group data. Units of text within the focus group transcripts were labeled based on their topic or concept represented, with these labels being called "codes." Units may consist of a phrase, sentence, or multiple sentences. For example, the unit of text "I partner with our internal communication group on a lot of activities to lean on their communication expertise" was assigned the code "Collaboration - Internal."

Initially, each member of the research team individually coded a subset of three transcripts (one from each category of focus group) using a preliminary code list based on the focus group questions and then added new codes as needed. We met several times to discuss codes for this subset and develop a codebook (a list of codes to be used in analysis). As part of the final codebook, all codes were "operationalized," which involves formally defining each code to ensure understanding among all coders. Coding continued until all transcripts were coded by two researchers, who met regularly to discuss code application and resolve differences. The entire research team convened to discuss overarching themes identified in the data and areas of interest to include in the subsequent survey.

2.2 Survey Methodology

2.2.1 Survey Design

We developed survey questions and answer options based on areas of interest identified in the focus groups. Several demographic or organizational questions that were asked in the focus groups were removed or changed in the survey for one of several reasons: 1) many focus group participants were not able to answer the question (e.g., a question on the budget of the program); 2) the question was not deemed necessary for answering the research questions (e.g. gender, age); or 3) the question needed to be reworded or response style changed to obtain more precise

data (e.g., converting an open-ended question about job title to a "select one answer" question with specific job classification responses).

An initial draft of the survey was reviewed by five SMEs: a CISO in an independent government agency, a security awareness program lead in a sub-component agency, two coordinators of a government security forum, and the manager of a cybersecurity workforce program who was formerly involved in security awareness programs.

The final survey (see Appendix D) addressed the following overarching topics:

- Participant professional background and organizational role
- Organizational information
- Required security awareness activities
- Phishing simulations
- Security awareness approaches
- Sources that inform security awareness content
- Determining security awareness program effectiveness and success
- Organizational support for the security awareness program
- Knowledge, skills, and professional development of security awareness professionals

Of note, role-based training (specialized security training tailored to certain positions within the organization) was mentioned as a major challenge in the focus groups but is outside the scope of security awareness for the general workforce. Therefore, in an effort to reduce the length of the survey and time commitment for respondents, we did not include this topic in the survey, but it may be a future area of investigation.

The survey included several question types:

- Multiple choice questions, which prompt participants to either select one option or check all options that apply
- Likert scale questions, which provide a range of options (e.g., Strongly Disagree – Disagree – Neither agree nor disagree – Agree – Strongly Agree) and are used to gauge participants' opinions and perceptions
- Open-ended questions, which require participants to type their answers into a comment box and are used to obtain qualitative responses that may not be otherwise anticipated

2.2.2 Survey Recruitment

Criteria for participation in the survey was the same as for focus groups: federal employees directly involved in or overseeing their organization's security awareness program. Survey recruitment was conducted in several ways. A research team member introduced the survey to attendees at a Small and Micro Agency CISO Council quarterly meeting and the FISSEA Summer Forum. We then sent a survey invitation and link to those forums' respective email lists. Invitations were also sent to three other security-focused government mailing lists known to reach security executives and security awareness professionals and one external security awareness forum that included some government employees. The research team also forwarded the invitation directly to prior focus group participants and other individuals known to be working on security awareness programs in the federal government. We asked email recipients to forward the invitation to eligible colleagues both within and outside their organizations. Prior

focus group participants were allowed to participate in the survey because the scope of the survey was much broader.

2.2.3 Survey Data Collection

The survey was implemented on an online survey platform. Prior to survey launch three security awareness professionals who had participated in the focus groups piloted the survey. Subsequently, we made minor adjustments to the survey formatting and wording to improve clarity. We officially launched the survey on June 15, 2021, and it was available through July 2, 2021.

The first page of the survey included an information sheet detailing the purpose of the study, participation criteria, study procedures, and how survey data would be protected. Prospective participants were then asked if they were federal employees. Those that indicated yes were permitted to continue the survey. All survey responses were anonymous.

2.2.4 Survey Data Analysis

Once the survey was closed, we compiled a final data set. We removed partial responses in which participants did not at least complete the demographic and organizational questions and those responses appearing to have been randomly completed (e.g., all options for all questions were selected). Ninety-six survey responses were included in the final dataset.

For responses generating quantitative data, we calculated descriptive statistics (e.g., frequencies and percentages of participants selecting particular responses) to provide a summary of responses. Additional inferential statistical tests looked for response differences amongst groups within different variables of interest, with an overall significance level set at $\alpha = 0.05$. The independent variables of interest were:

- ***Organization type***
  - Department
  - Sub-component
  - Independent agency

- ***Program size*** - based on number of employees (federal employees and contractors) covered under the organization's security awareness program
  - Small – Less than 1,000 employees
  - Medium – 1,000 – 4,999 employees
  - Large – 5,000 – 29,999 employees
  - Very Large – 30,000+ employees

- ***Team size*** - the number of individuals directly tasked with security awareness duties
  - Very small – 1-2 people
  - Small – 3-5 people
  - Medium – 6 – 10 people
  - Large – More than 10 people

Because data were not normal, we utilized nonparametric statistical tests. Depending on the response data type, statistical tests included Kruskal-Wallis H test plus post-hoc Mann-Whitney

U test for pairwise comparisons, Chi-square test, or Fisher's exact test. To account for multiple comparison issues, we used the Bonferroni correction with an adjusted α = (0.05 / <number of independent groups>). For example, since there are three organization type groups, the adjusted α was 0.05/3 = 0.017.

Since it is valuable to report positive and negative sentiment expressed in Likert scales, when conducting statistical analyses, we grouped similar valence Likert scale responses together. The groupings also helped achieve greater statistical power. We grouped the following responses for each type of scale:

- ***Level of challenge***:
  - Very challenging and Moderately challenging
  - Slightly challenging and Not challenging at all
  - Does not apply

- ***Agreement***:
  - Strongly disagree and Disagree
  - Neutral – Neither agree nor disagree
  - Strongly agree and Agree

- ***Success***:
  - Very unsuccessful and Unsuccessful
  - Slightly successful
  - Moderately successful and Very successful

We coded open-ended survey responses in a manner similar to the focus group data. The initial codebook was based on codes used in related questions from the focus groups, with new codes added as needed. Two research team members individually coded all responses for each open-ended question, then met to resolve any differences in code application.

3 Represented Participants, Organizations, and Programs

Focus group participants completed a short online survey to collect participant demographics and information about their organizations and security awareness programs. Survey participants provided similar information. This section reports on this high-level information to provide insight into what kind of participants, organizations, and security awareness programs were represented in the study. We differentiate between data collected in the focus groups and data from the survey.

3.1 Participants

In this report, we provide information about the participants in the study as related to their security awareness duties. NISTIR 8420B contains additional demographics related to participants' job classifications, work roles, and professional backgrounds.

3.1.1 Security Awareness Role

Focus Groups

Figure 1 shows the distribution of focus group participants' roles with respect to their organizations' security awareness program. Over half of participants were security awareness program leads (55%). Only three (10%) were team members who have awareness duties but do not lead the program. Managers or executives who oversee the security awareness program accounted for 14% of survey participants, while 21% identified as both program leads and managers/executives. Approximately 14% indicated that they oversaw the security awareness contract in their organization (not included in the figure) while also serving as a lead, member, or manager.

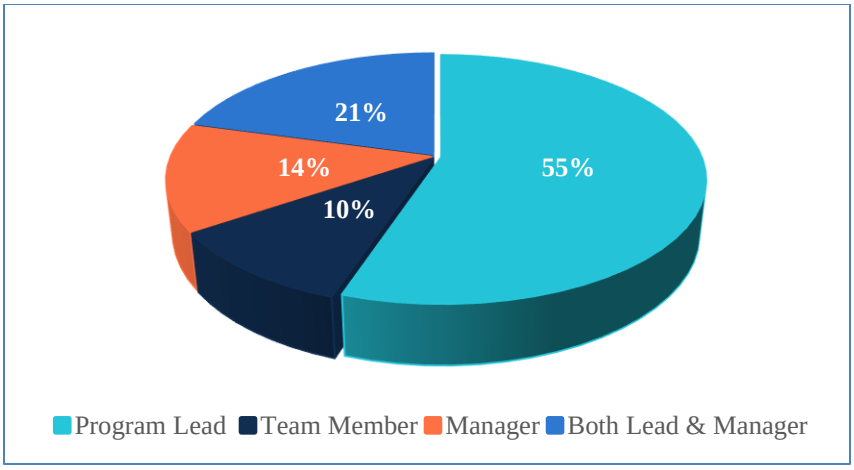

Figure 1: Focus Groups - Security awareness role (n=29)

Survey

Figure 1 shows the distribution of survey participants' security awareness roles. There were a fairly equal number of security awareness program leads (33%) and security awareness team members (35%). Managers or executives who oversee the security awareness program accounted for 9% of survey participants, while 10% identified as both program leads and managers/executives. Eleven percent indicated that they oversaw the security awareness contract in their organization (not included in the figure) while also serving as a lead, member, or manager.

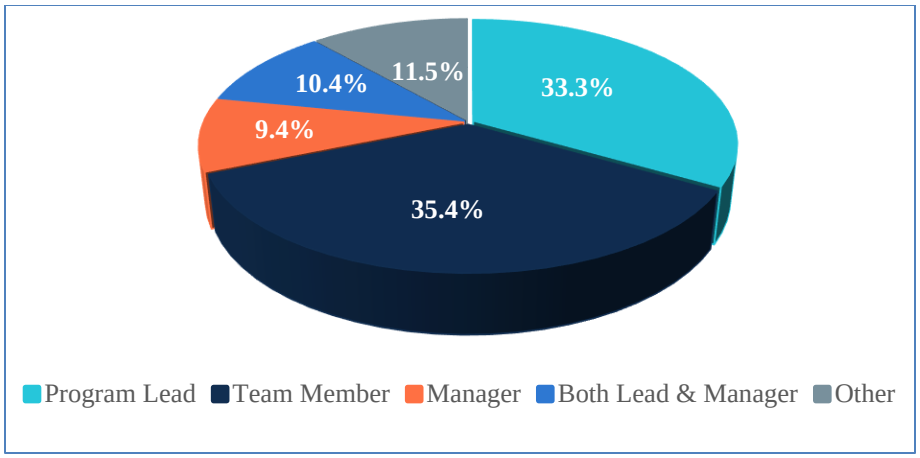

Figure 2: Survey - Security awareness role (n=96)

3.1.2 Time Spent on Security Awareness

Focus Groups

The focus group demographic survey asked what percentage of time participants spend on their security awareness duties. One focus group participant did not answer this question. As shown in Figure 3, 93% are part-time, with 39% spending less than half of their time on security awareness.

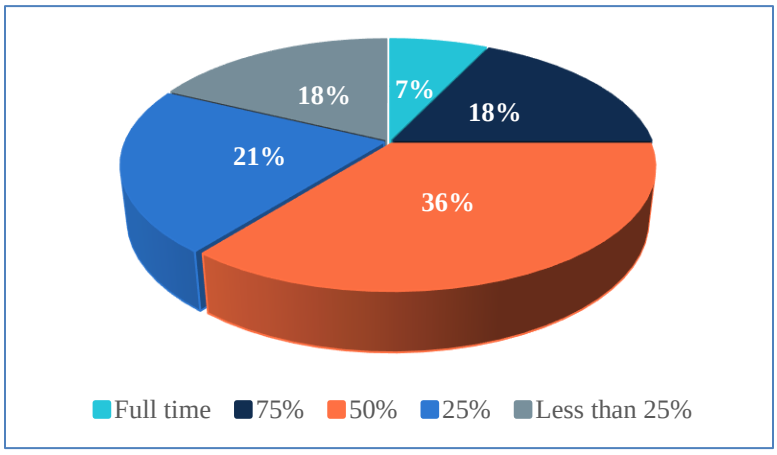

Figure 3: Focus Groups - Time spent on security awareness duties (n=28)

Survey

Figure 4 shows the percentage of time spent on security awareness among survey participants. Ninety percent of survey participants are part-time, with almost 56% spending less than 50% of their time on security awareness.

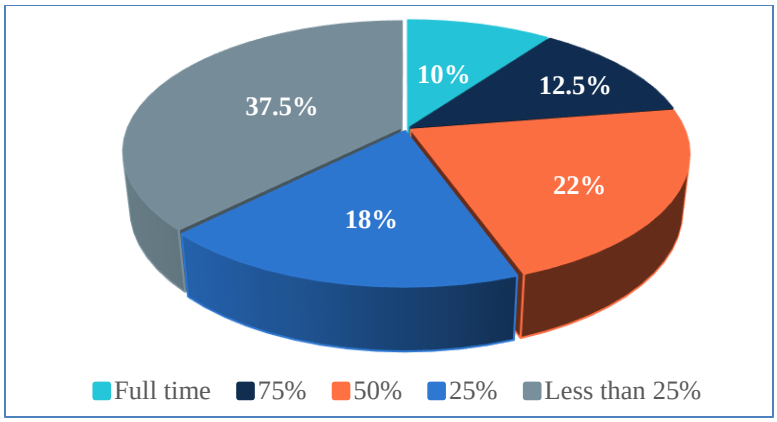

Figure 4: Survey - Time spent on security awareness duties (n=96)

3.2 Organizations

In this section, we describe characteristics of the organizations represented in our study.

3.2.1 Organization Type

Focus Groups

Twenty-eight unique organizations were represented in the focus groups. Figure 5 shows the percentages of each organization type. Independent agencies were the most represented in the focus groups (43%), while Departments were the least represented (21%).

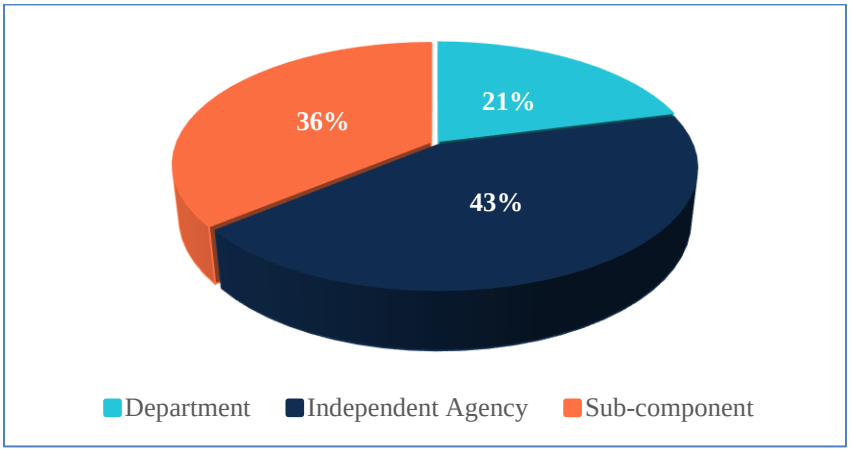

Figure 5: Focus Groups - Organization types (n=28)

Survey

The organizations represented in the survey were fairly equally distributed between Departments (32.3%), sub-components (31.3%), and independent agencies (35.4%) (Figure 6). One participant selected “I’m not sure” for the organization type.

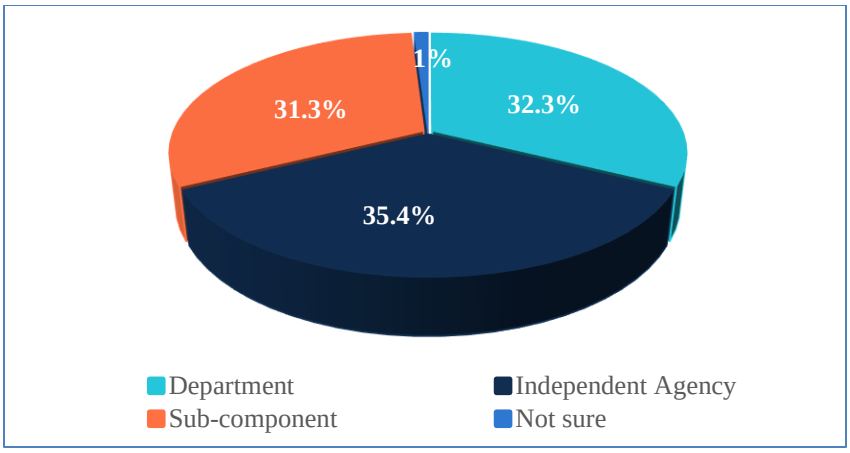

Figure 6: Survey - Organization types (n=96)

3.2.2 Organization Size

Organization size was determined by the number of federal employees. Participants from Departments were instructed not to include employees working in sub-components in the total size count.

Focus Groups

Focus group participants were from 28 unique organizations of various sizes, with half from organizations with fewer than 10,000 federal employees.

Figure 7 shows the distribution of organization sizes.

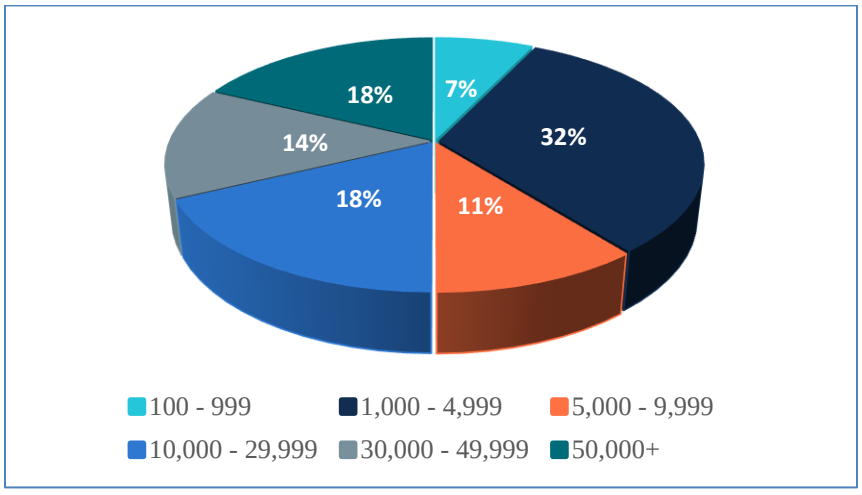

Figure 7: Focus Groups - Organization size (number of federal employees) (n=28)

Survey

Figure 8 shows the granular distribution of organization sizes represented in the survey. Organizations with between 1,000 and 4,999 federal employees made up the largest subset (29.2% of organizations), followed by organizations with 50,000 or more employees (21.9%).

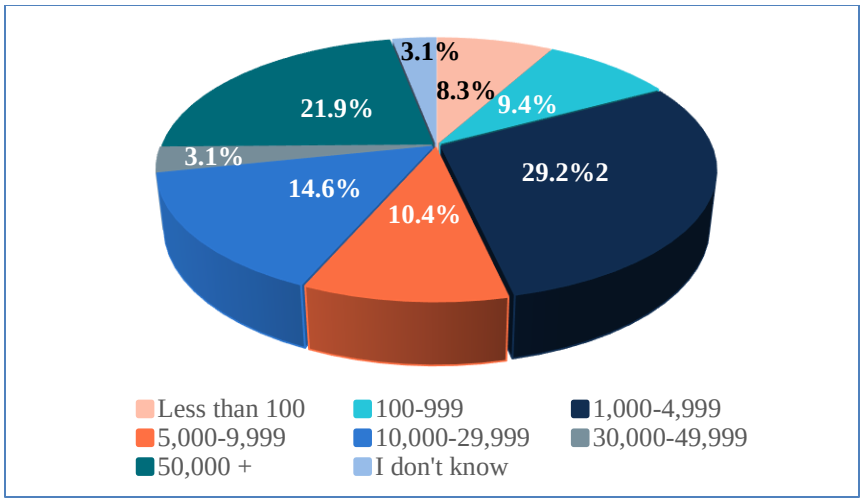

Figure 8: Survey - Organization size (number of federal employees) (n=96)

3.3 Security Awareness Programs

3.3.1 Program Size

Participants in both the focus groups and survey were asked how many people (including federal employees and contractors) were covered by the organization's security awareness program (i.e., how many people were required to take mandatory security awareness training). This was an important distinction from organization size (measured by number of federal employees) since government organizations may be required to provide security awareness training to their contractors as well as federal employees. In addition, some organizations have employees who, because they do not access information systems, may not be required to complete security awareness training.

Focus Groups

In the focus groups, 32% of the 28 organizations had programs of less than 10,000 federal employees and contractors (none less than 1,000), with the same percentage having programs covering more than 50,000 employees. One participant did not know the size of the program. Figure 9 shows the breakdown of program sizes.

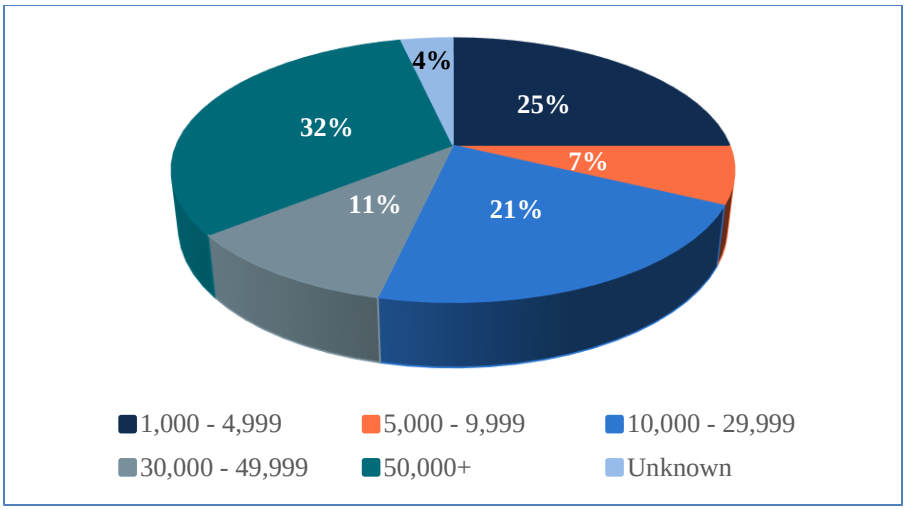

Figure 9: Focus Groups - Program size (n=28)

Survey

Survey participants were from a more diverse sample of organizations with program sizes ranging from less than 100 to over 50,000 employees, with close to half (47.4%) having programs less than 5,000 (see Figure 10).

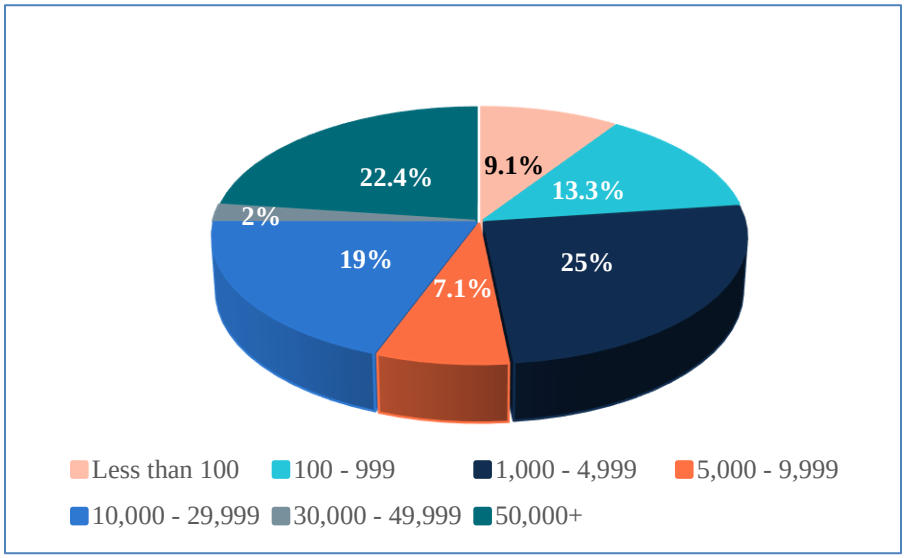

Figure 10: Survey - Program size (n=95)

In conducting further statistical analysis to look for differences in survey question responses based on program size, we grouped organizations into a smaller number of program size categories:

- Small – Less than 1,000 employees
- Medium – 1,000 – 4,999 employees
- Large – 5,000 – 29,999 employees
- Very Large – 30,000+ employees

Figure 11 shows the distribution for these condensed categories. These categories will be used when referring to program size in the companion reports.

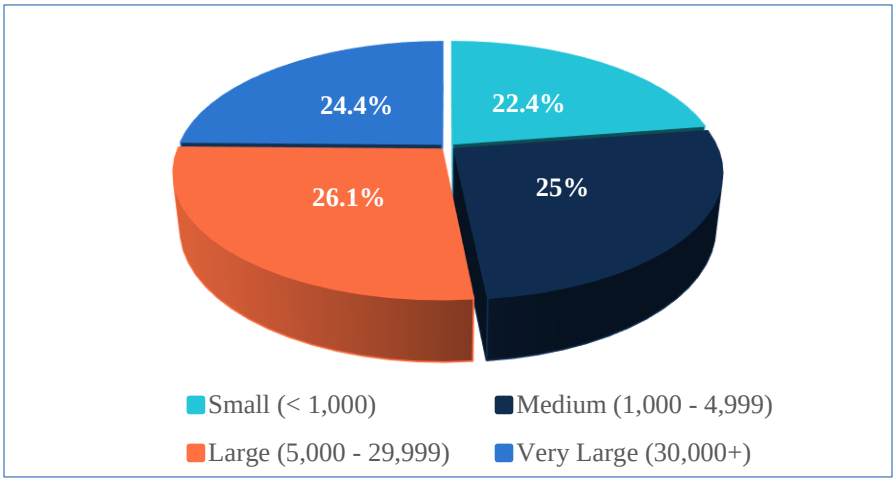

Figure 11: Survey - Program size - condensed categories (n=95)

3.3.2 Team Size

In both phases of the research project, we asked several questions to collect data on the number of individuals having security awareness duties within the surveyed organizations. For simplicity, we refer to the individuals with security awareness program duties as a "team" while acknowledging that the concept of a security awareness team may not exist in all organizations. Additionally, team size does not necessarily equate to full time equivalents (FTEs).[1]

Focus Groups
We asked participants how many federal employees and contractors work on the security awareness program, not including managers who only oversee the program administratively. This was an open-ended question. We also attempted to discern the number of FTEs dedicated to security awareness. However, few focus group participants were able to estimate FTEs, so the responses are omitted in this report, and this question was not included in the survey.

We grouped the number of individuals working on security awareness into four categories of team size:

- Very small – 1-2 people
- Small – 3-5 people
- Medium – 6-10 people
- Large – 11 or more people

[1] A full-time equivalent is a unit of measurement indicating the workload of an employee, with 1.0 FTE being a full-time employee and 0.5 FTE being a half-time employee.

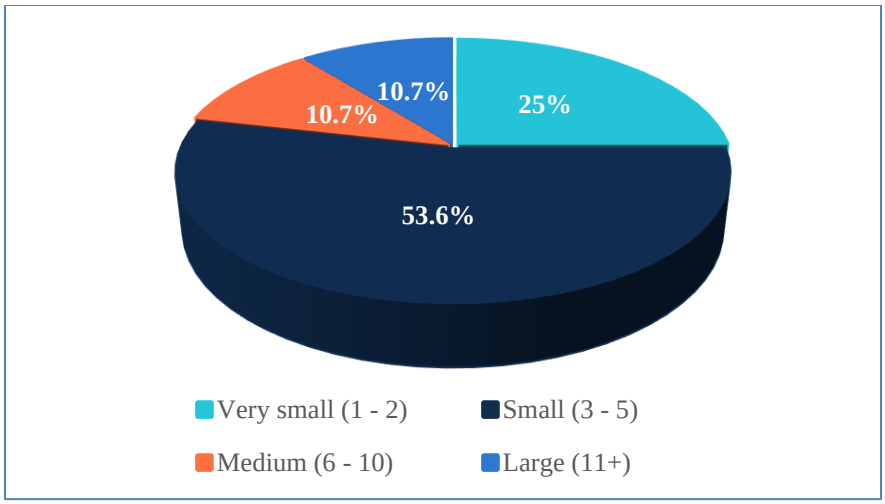

Figure 12: Focus Groups - Security awareness team size (n=28)

Figure 12 displays the distribution of team sizes amongst represented organizations. Over half of focus group participants worked on teams with 3-5 individuals. A quarter only had 1-2 individuals with security awareness duties.

We also asked what kinds of individuals make up the team. Only four organizations (14%) had a security awareness program that is handled all in-house by federal employees. The remainder (n=24, 86%) have a mix of federal employees and contractors working together on the program.

Survey

Similar to the focus groups, survey participants were asked in an open-ended question how many federal employees and contractors (i.e., individuals, not FTEs) work on the security awareness program. Despite instructing respondents not to include employees who just take the training, some participants misinterpreted the question. For example, some entered the number of employees in their organizations. After removing unlikely responses, 74 responses remained.

Figure 13 displays the distribution of team sizes among the represented organizations. Of particular note, about 1/3 of participants worked in organizations in which only one or two individuals have direct security awareness duties. In all, 63.4% of respondents had five or less individuals on their security awareness teams.

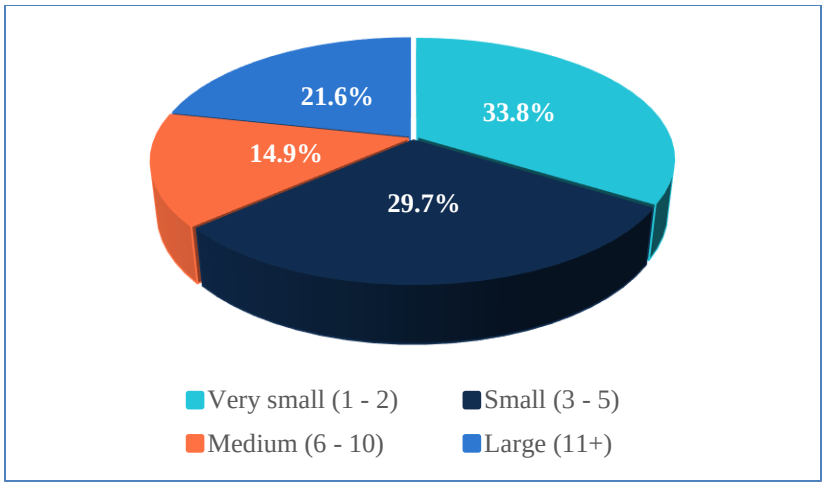

Figure 13: Survey - Security awareness team size (n=74)

About 31% (n = 23) of these organizations had teams that consisted of only federal employees. Approximately 68% (n = 50) had teams consisting of both federal employees and contractors. Only one had a contractor-only team.

We also explored whether larger programs have larger teams. Figure 14 shows the distribution of team size for different program sizes. A visual inspection suggests that Very Small teams (1-2 individuals) were common for all program sizes except for Very Large programs (30,000+ employees).

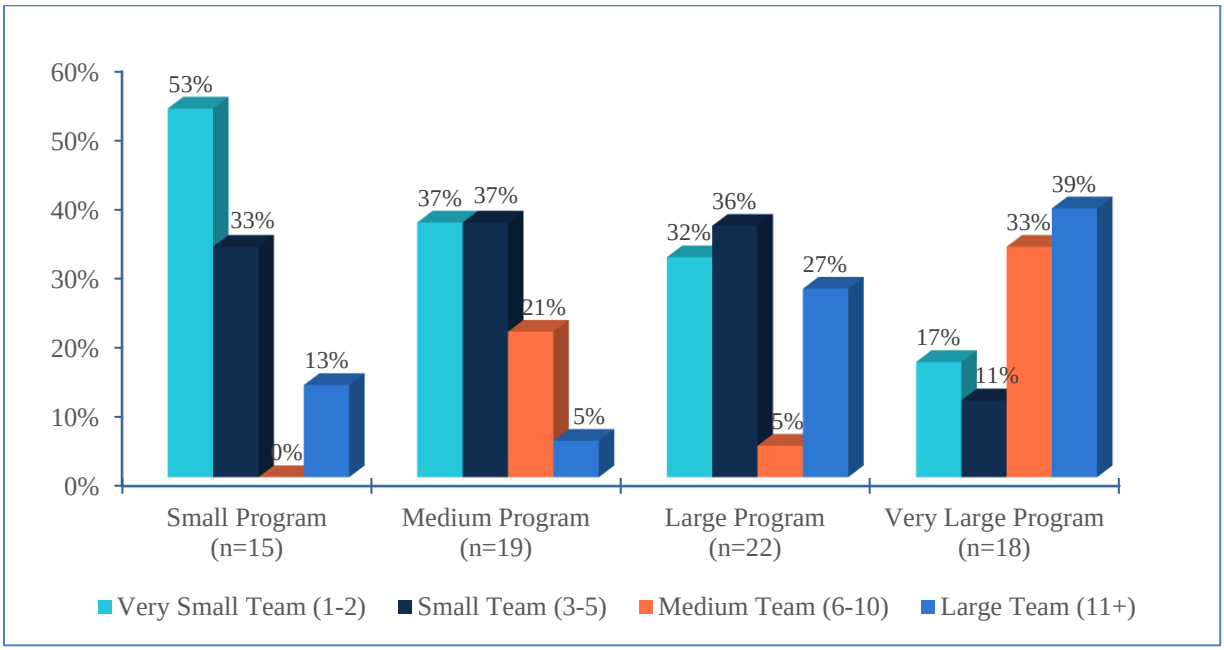

Figure 14: Survey - Team sizes for different program sizes (n=74)

We found a statistically significant difference in team size only between programs that were Small (< 1,000 employees) and Very Large (30,000+ employees) (Fisher's exact test). Very Large programs tended to have larger security awareness teams than small programs.

4 Conclusion

This report describes the background and methodology of a NIST research study to better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs. The research study was conducted in two phases: a series of eight focus groups of 29 federal professionals involved in their organizations' security awareness program followed by an online survey of 96 professionals.

Information about the participants and organizations is also included in the report. This document serves as a foundation for research results reported in two companion documents:

- NISTIR 8420A "Approaches and Challenges of Federal Cybersecurity Awareness Programs"
- NISTIR 8420B "The Federal Cybersecurity Awareness Workforce: Professional Backgrounds, Knowledge, Skills, and Development Activities"

These documents can serve as a resource for organizations and inform guidance to aid federal organizations in building more effective cybersecurity awareness programs.

Acknowledgements

The authors of this document would like to acknowledge those who have made this work possible. We would like to thank the federal employees who took time out of their busy schedules to participate in the focus groups and survey and provide their valuable perspectives. We would also like to thank the following individuals who provided valuable input and feedback on the study: Rodney Petersen, Marian Merritt, Danielle Santos, Karen Wetzel, Alen Kirkorian, Dan Jacobs, Sarah Moffat, Clarence Williams, and Daniel Eliot.

References

[BADA] Bada, M, Sasse, AM, Nurse, JRC (2019) Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? *arXiv preprint*. https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

[CISA] Cybersecurity and Infrastructure Security Agency (2021) *National Cybersecurity Awareness Month (NCSAM)*. Available at https://www.cisa.gov/national-cyber-security-awareness-month

[CLARK] Clark, VLP (2019) Meaningful integration within mixed methods studies: Identifying why, what, when, and how. *Contemporary Educational Psychology* 57(2019):106-111. Available at https://www.sciencedirect.com/science/article/pii/S0361476X19300128

[FERTIG] Fertig, T, Schütz, AE, Weber, K (2020) Current Issues of Metrics For Information Security Awareness. European Conference on Information Systems (Online). Available at https://aisel.aisnet.org/ecis2020_rp/184

[FISMA] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[FISSEA] National Institute of Standards and Technology (2021) *FISSEA – Federal Information Security Educators*. Available at https://csrc.nist.gov/projects/fissea

[HANEY] Haney, J, Lutters, W (2020) Security Awareness Training for the Workforce: Moving Beyond "Check-the-box" Compliance. *IEEE Computer* 53(10):91-95. Available at https://ieeexplore.ieee.org/document/9206408

[INDEED] Indeed (2021) 15 Professional Skills (Plus Definition and Tips). Available at https://www.indeed.com/career-advice/career-development/professional-skills

[KRUEGER] Krueger, RA, Casey, MA (2015). *Focus Groups: A Practical Guide for Applied Research* (Sage Publications), 5th Ed.

[OMB2016] Office of Management and Budget (2016) Circular A-130 Managing Information as a Strategic Resource. (The White House, Washington, DC), July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/ omb/circulars/A130/a130revised.pdf

[OMB2020] Office of Management and Budget (2020) Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2020. (The White House, Washington, DC). Available at https://www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf

[OPM] U.S. Office of Personnel Management (2018) Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need. (U.S. Office of Personnel Management, Washington, DC). Available at https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need

[SANS] SANS (2021). 2021 SANS Security Awareness Report: Managing Human Cyber Risk. Available at https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/

[SMAC] CIO.gov (2021) *About the SACC and SMAC Councils*. Available at https://www.cio.gov/about/members-and-leadership/SMACC/

[STEWART] Stewart, G, Lacey, D (2012) Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness. *Information Management & Computer Security* 20(1):29-38.

[WILSON] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[WOELK] Woelk, B (2015) The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies. *EDUCAUSE Center for Analysis and Research*. Available at https://library.educause.edu/~/media/files/library/2016/8/ erb1608.pdf

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CIO	Chief Information Officer
CISO	Chief Information Security Officer
FISSEA	Federal Information Security Educators
FTE	Full Time Equivalent
IT	Information Technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
SMAC	Small and Micro Agency CISO Council
SME	Subject Matter Expert

Appendix B—Focus Group Demographics Questions

Note: All questions (except the first question) were optional and could be skipped by the participant. Participants had signed the informed consent before taking the survey.

1. What is your participant code? This was provided by the NIST research team in an email.
   _____

This first set of questions is about you and your professional background.

2. What is your job title? _____

3. What is your role with respect to the security awareness program at your organization? Please check all that apply.
   - ☐ I am the government lead for the program
   - ☐ I am a member of the security awareness team, but not the lead
   - ☐ I oversee the contract for the program
   - ☐ I am a manager or executive who oversees the program administratively
   - ☐ Other: _____

4. Aside from security awareness responsibilities, what other job functions/roles do you have within the organization? _____

5. How many years have you been involved with security awareness programs in your current organization or in other organizations? Include time spent working on security awareness training and managing/overseeing security awareness programs.
   - o Less than 1 year
   - o 1 – 5 years
   - o 6 – 10 years
   - o 11 – 15 years
   - o 16 – 20 years
   - o More than 20 years

6. Approximately what percentage of your time at work do you spend on tasks related to the security awareness program?
   - o Full-time
   - o 75%
   - o 50%
   - o 25%
   - o 10%
   - o Less than 10%
   - o Other: _____

7. How many years have you been a federal employee?
   - Less than 1 year
   - 1 – 5 years
   - 6 – 10 years
   - 11 – 15 years
   - 16 – 20 years
   - More than 20 years

8. How many years did you spend as a contractor supporting the federal government?
   - None
   - Less than 1 year
   - 1 – 5 years
   - 6 – 10 years
   - 11 – 15 years
   - 16 – 20 years
   - More than 20 years

9. How many years have you worked at your current organization (including years as a contractor)?
   - Less than 1 year
   - 1 – 5 years
   - 6 – 10 years
   - 11 – 15 years
   - 16 – 20 years
   - More than 20 years

10. How many years have you worked in some kind of cybersecurity role?
    - Less than 1 year
    - 1 – 5 years
    - 6 – 10 years
    - 11 – 15 years
    - 16 – 20 years
    - More than 20 years

11. Please list any security certifications you have earned: _____

12. What is your age range?
    - 18 – 29
    - 30 – 39
    - 40 – 49
    - 50 – 59
    - 60+

13. What is your highest level of education?
    - o Less than high school degree
    - o High school degree or equivalent
    - o Some college
    - o Associate degree
    - o Bachelor's degree
    - o Master's degree
    - o Doctoral or Juris Doctoral degree
    - o Other: _____

14. If you have any degrees beyond a high school degree, in which disciplines/fields are your degrees? _____

15. What is your gender?
    - o Female
    - o Male
    - o Other
    - o Prefer not to answer

This next set of questions is about your organization and security awareness program.

16. Approximately how many federal employees work in your organization?
    _____

17. Approximately how many people within the organization are covered by your security awareness program? Include federal employees and contractors as applicable.
    _____

18. Which of the following describes your security awareness program?
    - o Handled all in-house by federal employees
    - o Mix of federal employees and contractors working on-site
    - o All contractors working on-site
    - o Outsourced completely to an external company working off-site
    - o Other: _____

19. Where is the placement of the security awareness program within the organization (for example, in the CIO's office)? _____

20. How many federal employees within your organization have at least some day-to-day security awareness responsibilities? Do not include managers who only oversee the program administratively. _____

21. How many contractors within your organization have at least some day-to-day security awareness responsibilities? _____

22. Approximately how many total full-time equivalents are allocated to security awareness responsibilities? Include federal employees and contractors. _____

23. What is the approximate budget allocated towards security awareness in your organization? _____

24. Please enter any additional information you feel is necessary to clarify any of your responses. _____

Appendix C—Focus Group Questions

1. Please tell us your name, organization, and your role with respect to security awareness. *[This question was not audio-recorded. Participants could decide what they wanted to share.]*

2. When I say "security awareness and training," what does that mean to you? What comes to mind?

3. Tell me about your organization's approach to security awareness and training.

4. How do you decide what topics and approaches to use for your security awareness program?
    a. *[Probe for sub-components:]* What kind of guidance/direction, if any, does your department provide? How much leeway do you have to tailor the training to your own organization?
    b. *[Probe for department-level agencies:]* What kind of guidance/direction, if any, do you push down to sub-components within your department?

5. What's working well with your program?

6. What's not working as well? What are your challenges and concerns with respect to security awareness in your organization?

7. How do you determine the effectiveness of your program, if at all?

8. If you could have anything or do anything for your security awareness program, what would that be?
    a. *[Probe:]* What would you do to solve the challenges you currently experience?
    b. *[Probe:]* What kinds and formats of resources and information sharing would be most beneficial?

9. What knowledge, skills, or competencies do you think are needed for those performing security awareness functions in your organization?

10. If you had one or two pieces of advice for someone just starting a security awareness program in an agency like yours, what would that advice be?

11. Is there anything else that we should have talked about, but didn't?

Appendix D—Survey Questions

For the purposes of the survey:

The term **organization** refers to your federal agency.

The term **employees** refers to both federal employees working for your organization and contractors supporting your organization unless explicitly categorized as one or the other (i.e., "federal employees" or "contractor employees"). **Contractors** are considered to be non-federal individuals supporting the organization.

The term **security** will be used as a shorthand for "cybersecurity" or "information security." Reference to physical security is different and will be labeled as such.

Security awareness programs help employees recognize and appropriately respond to security issues. Security awareness involves security information being disseminated to the general workforce within your organization. This is not to be confused with specialized role-based training, which is out of scope for this survey (but may be addressed in a future survey).

As a reminder, in order to maintain anonymity, when responding to open-ended questions, please do not include any information that might identify you or your organization. However, should you accidentally include such information, the researchers will redact it from the research record.

Information About You

In this first section, we'll ask you about your job and professional background.

1. Are you a federal employee?
    - Yes
    - No

2. Which of the following best matches your official position title?
    - Chief Information Officer (CIO)
    - Chief Information Security Officer (CISO)
    - Computer Scientist
    - IT Specialist (Cybersecurity/INFOSEC)
    - IT Specialist – Other
    - Program/Project Manager
    - Supervisory Computer Scientist
    - Supervisory IT Specialist (Cybersecurity/INFOSEC)
    - Supervisory IT Specialist – Other
    - Training Specialist
    - Other: _____

3. Has your organization assigned you to one or more NICE (National Initiative for Cybersecurity Education) Framework cybersecurity work roles?
   - o Yes
   - o No
   - o I don't know

   3A. <if yes> Which of the following NICE Framework cybersecurity work roles have you been assigned? Check all that apply.
   - ☐ Cyber Instructional Curriculum Developer
   - ☐ Cyber Instructor
   - ☐ Cyber Policy and Strategy Planner
   - ☐ Cyber Workforce Developer and Manager
   - ☐ Executive Cyber Leadership
   - ☐ Information Systems Security Manager
   - ☐ IT Investment/Portfolio Manager
   - ☐ IT Program Auditor
   - ☐ IT Project Manager
   - ☐ Privacy Officer/Privacy Compliance Manager
   - ☐ Program Manager
   - ☐ Other: _____

4. What is your role with respect to the security awareness program at your organization? Check all that apply.
   - ☐ I am the lead for the program responsible for implementation or management
   - ☐ I am a member of the security awareness team but not the lead
   - ☐ I oversee the contract for the program
   - ⊟ I am a manager or executive who oversees and is responsible for the program administratively
   - ☐ Other: _____

5. How many years have you been involved with security awareness programs in your current organization and in other organizations (rounded to the nearest year)? Include time spent working on security awareness training and managing/overseeing security awareness programs.
   - o Less than 1 year
   - o 1 – 5 years
   - o 6 – 10 years
   - o 11 – 15 years
   - o 16 – 20 years
   - o More than 20 years

6. Approximately what percentage of your time at work do you spend on tasks related to the security awareness program?
    - o Full-time
    - o 75%
    - o 50%
    - o 25%
    - o Less than 25%
    - o Other: _____

7. If you have any degrees beyond a high school degree, in which disciplines/fields are your degrees? _____

8. What professional certifications, if any, have you earned? Check all that apply.
    - ☐ Security+
    - ☐ Certified Information Systems Security Professional (CISSP)
    - ☐ CISSP specialized concentration (including CISSP-ISSEP, CISSP-ISSAP, CISSP-ISSMP)
    - ☐ Certified Information Security Manager (CISM)
    - ☐ Project Management Professional (PMP)
    - ☐ Certified Authorization Professional (CAP)
    - ☐ SANS Security Awareness Professional (SSAP)
    - ☐ I don't have any professional certifications
    - ☐ Other: _____

9. In which of the following fields have you worked professionally? Check all that apply.
    - ☐ Cybersecurity
    - ☐ Information technology (not a cybersecurity focus)
    - ☐ Software development
    - ☐ Communications
    - ☐ Marketing
    - ☐ Graphic design
    - ☐ Human resources
    - ☐ Legal
    - ☐ Audit/compliance
    - ☐ Instructional design or education
    - ☐ Psychology or sociology
    - ☐ Physical security
    - ☐ Other: _____

Information about Your Organization

In this section, we'll ask you about your organization and the size of your security awareness program.

10. In which kind of organization do you work?
    - Department-level - for example, Department of Commerce or Department of Transportation
    - Sub-component agency or bureau under a Department - for example, NIST is a sub-component under Department of Commerce and FAA is a sub-component under Department of Transportation
    - Independent agency
    - I'm not sure

11. Approximately how many **federal employees** work in your organization? If working at the department level, please do not include employees working in any formal sub-component agencies under the department.
    - Less than 100
    - 100 – 999
    - 1,000 – 4999
    - 5,000 – 9,999
    - 10,000 – 29,999
    - 30,000 – 49,999
    - 50,000+
    - I don't know

12. Approximately how many employees within your organization (**federal employees and contractors**) are covered by your security awareness program? If working at the department level, only include employees in sub-component agencies if the sub-components do not have a security awareness program of their own.
    - Less than 100
    - 100 – 999
    - 1,000 – 4999
    - 5,000 – 9,999
    - 10,000 – 29,999
    - 30,000 – 49,999
    - 50,000+
    - I don't know

13. How many federal employees and contractors work on the security awareness program in your organization? Do not include managers who only oversee the program administratively or employees or contractors who just take the training.

	Number of individuals
Federal employees	
Contractors	

Required Security Awareness Activities

This set of questions is about **required** security awareness training for employees in your organization. Other security awareness activities in your organization will be covered in a later section.

14. In what ways can employees fulfill their annual cybersecurity awareness requirement? Check all that apply.
    - ☐ Online, computer-based course
    - ☐ Live (in-person or virtual) training event held by my organization
    - ☐ Live (in-person or virtual) training event held by external organizations
    - ☐ Other: _____

15. How does your organization obtain required security awareness training or content? Check all that apply.
    - ☐ Create within the organization
    - ☐ Purchase from outside of the organization
    - ☐ Receive from the Department (if you are a sub-component)
    - ☐ Obtain at no cost from another organization
    - ☐ Obtain from another government organization (other than your Department, if applicable)
    - ☐ Other: _____

16. How often is the required cybersecurity awareness training content updated?
    - o At least once a year
    - o Every 1 – 3 years
    - o More than every 3 years
    - o I don't know

17. What happens to employees who do not complete their required training by the deadline? Check all that apply.
    - ☐ They receive an email reminder.
    - ☐ Their supervisor is contacted.
    - ☐ Their account is disabled/suspended.
    - ☐ Their annual performance rating is negatively impacted.
    - ☐ Nothing
    - ☐ Other: _____

18. Please rate the level of challenge encountered by your security awareness program for the following:

	Very Challenging	Moderately Challenging	Slightly Challenging	Not Challenging at all	Does not apply
Getting employees to complete their training by the appointed deadline	•	•	•	•	•
Tracking which **federal employees** have completed their required training	•	•	•	•	•
Tracking which **contractors** have completed their required training	•	•	•	•	•
Finding courses/materials for required training	•	•	•	•	•
Finding guidance on what to include in required security awareness training	•	•	•	•	•
Updating required security awareness content	•	•	•	•	•

Phishing Simulations

In this section, we'll ask about your organization's phishing simulation program (if you have one). Phishing simulations involve sending emails that mimic real-world phishing attempts in order to train employees to recognize and appropriately respond to phishing emails.

19. Does your organization perform phishing simulations?
    - o Yes, and I am familiar with the phishing simulation process
    - o Yes, but I am not familiar with the phishing simulation process
    - o No
    - o I don't know

<if "yes but not familiar," "no," or "I don't know," skip the remaining questions in this section>

20. Approximately how often are phishing simulations conducted within your organization?
    - o 1 -2 times a year
    - o Quarterly
    - o Monthly
    - o More frequently than once a month
    - o Other: _____

21. What happens to "repeat clickers" (individuals who repeatedly fall victim to simulated phishes)? Check all that apply.
    - ☐ They have to complete additional training
    - ☐ They are counseled by a member of the security or security awareness team
    - ☐ Their supervisors are notified
    - ☐ Nothing
    - ☐ Other: _____

Disseminating Security Awareness Information

We'll now ask questions related to the ways in which your program distributes security awareness information within your organization and the topics you cover.

22. In addition to the required security awareness training, how many additional, optional security awareness activities or events (for example, speaker events, information fairs) does your organization offer on average per year?
    - o None
    - o 1 – 2
    - o 3 - 4
    - o More than 4

23. How is security awareness information disseminated within your organization? Check all that apply.
    - ☐ Online, computer-based courses
    - ☐ Videos
    - ☐ Webinars
    - ☐ Posters/flyers
    - ☐ Pamphlets/handouts
    - ☐ Email
    - ☐ Newsletters
    - ☐ Live (in-person or virtual) events
    - ☐ Activity fairs
    - ☐ Escape rooms
    - ☐ Website
    - ☐ Other: _____ <have a larger text box>

24. Which of the following topics have been addressed by your security awareness program via training courses, events, or other communications in the past 1-2 years? Check all that apply.
    - ☐ Social engineering, for example, phishing and phone scams
    - ☐ Passwords and authentication
    - ☐ Use of removable media (like USB drives, removable hard drives)
    - ☐ Malware, including viruses, ransomware, etc.
    - ☐ Web browsing
    - ☐ Telework
    - ☐ How to respond to potential cybersecurity incidents
    - ☐ Privacy, including handling personally and business identifying information
    - ☐ Installing and updating software
    - ☐ Organizational/government security policies, requirements, and guidance
    - ☐ Mobile device security
    - ☐ Social media
    - ☐ Physical security and safety
    - ☐ Other: _____

25. How often does your security awareness program provide employees with information applicable to their personal/home lives?
    Never – Rarely – Occasionally – A moderate amount – A great deal

26. If there have been changes in your program due to the COVID-19 pandemic, which, if any do you anticipate continuing post-pandemic? <open-ended text box>

27. Please rate the level of challenge encountered by your security awareness program for the following:

	Very Challenging	Moderately Challenging	Slightly Challenging	Not Challenging at all	Does not apply
Providing security awareness information in an engaging way	•	•	•	•	•
Customizing security awareness information to people with varying needs and levels of IT and security knowledge	•	•	•	•	•
Communicating security awareness information to a distributed work force	•	•	•	•	•
Finding existing security awareness materials to use	•	•	•	•	•
Ensuring security awareness materials are 508 compliant	•	•	•	•	•

28. In what ways, if any, does your program reward or recognize employees for practicing good security behaviors? (Check all that apply.)
    - ☐ Personal "thank you"
    - ☐ Certificate or virtual badge
    - ☐ Organizational recognition
    - ☐ Monetary award
    - ☐ Other: _____
    - ☐ We don't reward or recognize people

Informing Security Awareness Content

In this section, we ask about sources that inform your security awareness program, including with whom you collaborate.

29. If your organization is a sub-component (agency under a department), which of the following best describes the security awareness relationship with your Department?
    - o Does not apply, not a sub-component
    - o We must use the security awareness training provided to us by the Department
    - o The Department provides training, but using it is optional and/or we can tailor it to meet our needs
    - o The Department provides topics that must be included, but does not provide training
    - o The Department does not provide us with any materials or guidance
    - o Other: _____

30. If your organization is a Department, what types of security awareness training information does your organization push down to your sub-component agencies?
    - o Does not apply, not a department
    - o We provide security awareness training that the sub-components must use
    - o We provide security awareness training, but the sub-components have the option of using it
    - o We provide topics that must be included, but do not provide training
    - o We do not provide sub-components with any materials or guidance
    - o We don't have sub-component agencies under our Department
    - o Other: _____

31. With which groups **in your own organization** does the security awareness team collaborate? Check all that apply.
    - ☐ Cybersecurity incident response
    - ☐ Other cybersecurity groups outside of the security awareness team
    - ☐ Information technology
    - ☐ Physical security
    - ☐ Communications and marketing
    - ☐ Human resources
    - ☐ Privacy team
    - ☐ General Counsel
    - ☐ Other: _____

32. Which of the following sources **within your own organization** inform security awareness topics and approaches? Check all that apply.
    - ☐ Security incidents within the organization
    - ☐ Employee feedback/input
    - ☐ Leadership feedback/input
    - ☐ Other: _____

33. Which of the following **external** sources help inform your organization's security awareness training and approaches? Check all that apply.
    - ☐ Government mailing lists, websites, articles, online resources
    - ☐ Non-government mailing lists, websites, articles, online resources
    - ☐ Government working groups
    - ☐ Non-government working groups
    - ☐ Security incidents in other organizations
    - ☐ Conferences
    - ☐ Other: _____

34. Have you ever attended the Federal Information Security Educators (FISSEA) Conference?
    - o Yes, I have attended FISSEA
    - o No, but I've heard of FISSEA
    - o No, and I've never heard of FISSEA

35. Have you ever used NIST Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" to inform your security awareness program?
    - o Yes
    - o No, but I know of it
    - o No, and I don't know of it

36. Please rate the level of challenge encountered by your security awareness program for the following:

	Very Challenging	Moderately Challenging	Slightly Challenging	Not Challenging at all	Does not apply
Collaborating/sharing information with other groups in my organization	•	•	•	•	•
Collaborating/sharing information with other federal security awareness professionals	•	•	•	•	•
Finding external sources of information relevant to my security awareness program	•	•	•	•	•

Determining Security Awareness Program Effectiveness

We'll now ask about how your organization determines the level of success of your security awareness program.

37. Please rate your level of agreement with the following statements:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Among my organization's leadership, compliance with security awareness training requirements is considered the most important indicator of success for our security awareness program	•	•	•	•	•
In my own opinion, compliance with security awareness training requirements is the most important indicator of success for our security awareness program.	•	•	•	•	•

38. How does your organization determine or measure the effectiveness of your security awareness program? Check all that apply.
    - ☐ Required training completion rates
    - ☐ Audit reports or FISMA (Federal Information Security Modernization Act of 2014) evaluations
    - ☐ Phishing click rates (number of people who click on a simulated phishing email/link)
    - ☐ Employee reporting of simulated phishing emails
    - ☐ Employee reporting of potential phishing emails (outside of phishing simulations)
    - ☐ Employee reporting of other security incidents
    - ☐ Surveys
    - ☐ Informal employee feedback/comments (for example, in-person, emails)
    - ☐ Attendance at security awareness events
    - ☐ Online views of training materials
    - ☐ Security incident trends
    - ☐ We don't try to determine the effectiveness
    - ☐ Other: _____

<If "We don't try to determine the effectiveness," skip next question>

39. How does your security awareness program use program effectiveness data? Check all that apply.
    - ☐ We use the data to demonstrate our compliance with training mandates.
    - ☐ We provide the data to leadership to show the value of the security awareness program.
    - ☐ We use the data to justify additional resources for the security awareness program.
    - ☐ We provide the data to employees so there's more transparency about the security awareness program.
    - ☐ We use the data to improve/inform the security awareness program.
    - ☐ We provide the data to other groups in our organization to help improve/inform their own programs or processes.
    - ☐ Other: _____

40. **If you are a manager or executive** who is involved in making decisions about the security awareness program, what data would help demonstrate the value and effectiveness of the security awareness program? <open-ended text box>

41. Please rate the level of challenge encountered by your security awareness program for the following:

	Very Challenging	Moderately Challenging	Slightly Challenging	Not Challenging at all	Does not apply
Determining what and how to measure	•	•	•	•	•
Effectively presenting data to leadership	•	•	•	•	•
Integrating/correlating security awareness data with data collected by other groups in my organization	•	•	•	•	•
Benchmarking my organization against other federal organizations	•	•	•	•	•

42. What would you say are the **most** successful aspects of your security awareness program? <open-ended text box>

43. In your opinion, how successful is your security awareness program?
Very unsuccessful – Unsuccessful - Slightly successful – Moderately successful – Very successful

Support for the security awareness program

In this section, you'll tell us your perceptions of the level of support within your organization for cybersecurity and the security awareness program.

44. Please indicate your level of agreement with each of the following statements:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Security is a priority for my organization.	•	•	•	•	•
My organization's **leadership** understands how/why security is relevant to them.	•	•	•	•	•
The **employees** in my organization understand how/why security is relevant to them.	•	•	•	•	•
My organization's **leadership** is supportive of the security awareness program.	•	•	•	•	•
The **employees** in my organization are supportive of the security awareness program.	•	•	•	•	•
We have adequate **funding** for the security awareness program.	•	•	•	•	•
We have adequate **staff** dedicated to the security awareness program.	•	•	•	•	•
We have the necessary **technology** to support the security awareness program.	•	•	•	•	•

Knowledge, Skills, Professional development

In this section, we ask about the knowledge and skills needed by your security awareness team.

45. Please rate the level of importance of having the following knowledge and skills in a security awareness team in an organization like yours?

	Not important at all	Low importance	Moderate importance	High importance
Cybersecurity knowledge and skills	•	•	•	•
Privacy knowledge and skills	•	•	•	•
Information technology knowledge and skills	•	•	•	•
Written communication skills	•	•	•	•
Oral communication skills	•	•	•	•
Marketing skills	•	•	•	•
Adult learning/instructional development knowledge and skills	•	•	•	•
Program management skills	•	•	•	•
Creativity and adaptability	•	•	•	•
Interpersonal skills	•	•	•	•
Moderating/group facilitation skills	•	•	•	•
Knowledge of cybersecurity policies	•	•	•	•
Knowledge of organizational mission, processes, and dynamics	•	•	•	•

46. Other than the knowledge and skills listed above, please list any other knowledge and skills you think are of **high importance** for a security awareness team: <open-ended text>

47. Please rate your agreement with the following statement: In my organization, the security awareness team has the right mix of necessary knowledge and skills.

    Strongly disagree – Disagree – Neither Agree nor Disagree – Agree – Strongly Agree

48. Which of the following professional development activities have helped you develop knowledge and skills needed for your security awareness role? Check all that apply.

    - ☐ College courses
    - ☐ Online, computer-based training courses
    - ☐ Live (in-person or virtual) training courses
    - ☐ Professional certifications
    - ☐ Attending conferences
    - ☐ Self-study (for example, reading articles, listening to podcasts, hands-on experience)
    - ☐ Other: _____
    - ☐ I haven't engaged in any professional development activities that have helped me in my role

49. Please rate your agreement with the following statement: In my organization, I have been provided adequate professional development opportunities to help me in my security awareness role.

    Strongly disagree – Disagree – Neither Agree nor Disagree – Agree – Strongly Agree

Final Thoughts

In this last section, we'll give you the opportunity to share your own lessons learned and any other information you think would be useful for us to know.

50. What are the **most important** pieces of advice or lessons learned you might pass on to someone just starting a security awareness program in an organization like yours? <open-ended text box>

51. What could help your organization's security awareness program be more successful? <open-ended text box>

52. Please describe anything else related to your organization's experiences or challenges with security awareness that you'd like us to know. <open-ended text box>