Understanding Federal Cybersecurity Culture:
An Expert Perspective on Current and Ideal State

by Richard Joseph Sousane

A Dissertation submitted to

The Faculty of
The Graduate School of Education and Human Development
of The George Washington University
in partial fulfillment of the requirements
for the degree of Doctor of Education

May 20, 2018

Dissertation directed by

Michael J. Marquardt
Professor of Human and Organizational Learning and International Affairs

The Graduate School of Education and Human Development of the George Washington University certifies that Richard Joseph Sousane has passed the final examination for the degree of Doctor of Education as of March 12, 2018. This is the final and approved form of the dissertation.

Understanding Federal Cybersecurity Culture:
An Expert Perspective on Current and Ideal State

Richard Joseph Sousane

Dissertation Research Committee:

Michael J. Marquardt, Professor of Human and Organizational Learning and International Affairs, Dissertation Director

Ralph T. Soule, Adjunct Assistant Professor of Clinical Research and Leadership, Committee Member

William H. Money, Associate Professor of Information Systems, The Citadel, Committee Member

Dedication

I want to thank my family, friends, and work colleagues for their support during the development of this dissertation. In particular, I would like to thank my parents, Dick and Ellen, who inspired me throughout my doctoral studies, and my wife, Amanda, and son, Jack, for their unwavering love and support.

Acknowledgments

I would like to thank my dissertation director, Dr. Michael Marquardt, dissertation committee members, Dr. William Money and Dr. Ralph Soule, the faculty and staff of George Washington University's Executive Leadership Doctoral Program, and all the U.S. federal cybersecurity experts who graciously volunteered to participate in this study.

Abstract of the Dissertation

Understanding Federal Cybersecurity Culture:
An Expert Perspective on Current and Ideal State

As history has taught us, cybersecurity incidents can be devastating to individuals, organizations, and nations. Unfortunately, the U.S. federal government has not been immune from the reality of the devastation caused by cybersecurity incidents. However, it has been suggested that a stronger federal cybersecurity culture can help to avoid cybersecurity incidents. Unfortunately, the current literature is silent on what constitutes federal cybersecurity culture, which would include core elements, possible variations, development, and management.

The purpose of this study was to better understand cybersecurity culture in U.S. federal organizations. To complete this study, a qualitative, exploratory inquiry regarding the core elements of U.S. federal cybersecurity culture was conducted. Specifically, interviews were conducted with 30 federal cybersecurity experts to better understand cybersecurity culture in U.S. federal organizations. The study resulted in seven significant conclusions: (1) employee lack of compliance with cybersecurity policies necessitates greater accountability; (2) U.S. federal organizations need more effective methods of cybersecurity training; (3) U.S. federal organizations should establish a cybersecurity strategic plan; (4) U.S. federal organizations should establish cybersecurity standard operating procedures; (5) U.S. federal organizations need innovative approaches to compete with the private sector in the recruitment of cybersecurity personnel; (6) U.S. federal organizations should collaborate in developing cybersecurity strategy; and (7) U.S. federal organizations need to shift their focus from cybersecurity compliance to

cybersecurity maturity. The study concludes with implications for theory and practice as well as recommendations for further research.

The results of this research should serve as a guide for U.S. federal leaders in their efforts to establish a stronger cybersecurity culture, which would enhance the protection of critical information technology assets and sensitive information.

Table of Contents

Page

Dedication iii

Acknowledgments iv

Abstract of the Dissertation v

List of Figures xii

List of Tables xiii

CHAPTER 1: INTRODUCTION 1

Overview 1

Federal Cybersecurity Challenges 4

Statement of the Problem 7

Research Purpose and Questions 7

Statement of Potential Significance 8

Conceptual Framework 9

Summary of Methodology 12

Limitations and Delimitations 14

Definitions of Key Terms 15

CHAPTER 2: LITERATURE REVIEW 16

Organizational Culture 17

Information Technology: An Overview 23

Information Technology and Organizational Culture 25

Cybersecurity 30

Cybersecurity Categories 31
Cybersecurity Policies and Regulations 32
Cybersecurity Culture 34
Culture and Cybersecurity Effectiveness 34
Significance of Cybersecurity Culture 35
Leadership and Cybersecurity Culture 36
Promoting a Cybersecurity Culture 37
Call for the Study of Cybersecurity Culture 39
Implications for the Current Study 39

CHAPTER 3: METHODOLOGY 41

Research Assumptions 42
Qualitative Research Design 43
Population for the Study 44
Data Collection 46
Interview Approach 46
Interview Guide Development 47
Data Collection Procedures 49
Data Analysis 49
Content Analysis and Thematic Coding 50
Verification and Trustworthiness 51
Subjectivity Statement 54
Human Participants and Ethics Precautions 55

CHAPTER 4: RESULTS 57

Demographic Profiles of the Participants 57

Interview Results 61

Similarities in Cybersecurity Culture 63

Differences in Cybersecurity Culture 93

Current Cybersecurity Culture Development 100

Ideal Cybersecurity Culture Development 105

Summary 132

CHAPTER 5: INTERPRETATIONS, CONCLUSIONS, AND RECOMMENDATIONS 136

Summary of Findings 136

Conclusions 138

Conclusion 1: Employee Lack of Compliance with Cybersecurity Policies in U.S. Federal Organizations Necessitates Greater Accountability 139

Conclusion 2: U.S. Federal Organizations Need More Effective Methods of Cybersecurity Training 141

Conclusion 3: U.S. Federal Organizations Should Establish a Cybersecurity Strategic Plan 144

Conclusion 4: U.S. Federal Organizations Should Establish Cybersecurity Standard Operating Procedures 145

Conclusion 5: U.S. Federal Organizations Need Innovative Approaches to Compete with the Private Sector in the Recruitment of Cybersecurity Personnel 147

Conclusion 6: U.S. Federal Organizations Should Collaborate in Developing Cybersecurity Strategy 150
Conclusion 7: U.S. Federal Organizations Need to Shift Their Focus from Cybersecurity Compliance to Cybersecurity Maturity 152
Implications for Theory 155
Theoretical Alignment and Contributions 155
Schein's Culture Model 158
Recommendations for Practice 159
Recommendation 1: Include Cybersecurity Compliance in Employee Performance Appraisals 159
Recommendation 2: Improve Cybersecurity Training Methods 160
Recommendation 3: Develop a Cybersecurity Strategic Plan 161
Recommendation 4: Establish Cybersecurity Standard Operating Procedures 162
Recommendation 5: Establish Innovations in the Recruitment of Cybersecurity Personnel 162
Recommendation 6: Establish a Framework for Improved Collaboration Between U.S. Federal Organizations in Developing Cybersecurity Strategy 164
Recommendation 7: Change Emphasis from Cybersecurity Compliance to Cybersecurity Maturity 165
Recommendations for Future Research 165
Concluding Remarks 169
REFERENCES 170

APPENDIX A: Initial Email Contact Letter 181

APPENDIX B: Informed Consent Form 182

APPENDIX C: Interview Guide 184

List of Figures

Page

1.1. Conceptual Model 10

2.1. Schein's Cultural Model 18

2.2. Hatch's Cultural Dynamics Model 20

4.1. Gender of Research Participants 58

4.2. Cybersecurity Experience of Research Participants 58

4.3. Education Level of Research Participants 59

4.4. Cybersecurity Certifications of Research Participants 59

4.5. CISSP Certification of Research Participants 60

4.6. Level in Organization of Research Participants 60

List of Tables

Page

1.1. Key Terms and Definitions 15

2.1. Nine Primary Problems Associated with Rapid IT Change in Organizations 24

2.2. Five Coping Mechanisms for Rapid IT Change in Organizations 24

3.1. Relation Between Interview Questions and Research Questions 48

4.1. Findings from the Research 62

5.1. Summary of Research Findings 137

5.2. Summary of Conclusions and Associated Research Findings 138

CHAPTER 1:

INTRODUCTION

Overview

Given the heightened information security concerns in society today, many organizations are placing significant emphasis on cybersecurity culture. The traditional approach taken by many organizations in safeguarding their information assets has been primarily to rely on technical controls such as hardware and software. However, in today's information-risk work environments, technical controls alone are not sufficient to combat cybersecurity risks (Alnatheer, 2014). This assertion has been evidenced in many U.S. federal government organizations, in which human action, either intentional or unintentional, has directly contributed to cybersecurity breaches. Accordingly, federal organizations have implemented information security policies, employee user agreements, personnel security training, and standard operating procedures to improve information security and to incorporate cybersecurity into the organizational culture at a basic level (Department of Homeland Security, 2009; Government Accountability Office, 2011; National Initiative for Cybersecurity Education, 2012; Office of Management and Budget, 2008).

Organizational cybersecurity culture can be broadly described as a union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and direct actions focused on sustaining cybersecurity within organizations (Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009). However, the definition constitutes a high-level perspective of cybersecurity culture; the core elements of cybersecurity culture have not been clearly or consistently defined. In

fact, the constantly evolving state of cybersecurity makes it challenging to define cybersecurity culture (Alnatheer, 2014; Da Veiga & Eloff, 2007; Herath & Rao, 2009).

The use of information technology provides substantial benefits to individuals and organizations, but it also presents significant information technology security risks or, more specifically, cybersecurity risks (Alnatheer, 2014; Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009). This is certainly the case with U.S. federal government organizations, which have been significantly affected by cybersecurity breaches. In fact, the abundance of sensitive information accessible to many federal employees makes it particularly susceptible to cybersecurity risks. A few examples of cybersecurity breaches faced by federal agencies include the theft of confidential medical records from the Department of Veterans Affairs (VA) (Nagesh, 2010) and Edward Snowden's release of sensitive security information obtained from the National Security Agency (NSA) (Greenberg, 2013). As a result of the many cybersecurity breaches, the U.S. Government Accountability Office, an independent, nonpartisan agency with a mission to improve performance and ensure accountability, includes cybersecurity on its list of key issues facing the nation (Government Accountability Office, 2016).

The use of information technology has certainly helped to refine federal business practices. However, safeguarding the security of federal information technology assets has become increasingly challenging (Government Accountability Office, 2016). In fact, the government faces new cybersecurity threats and crime opportunities every day (Government Accountability Office, 2016). Given these facts, prudent organizations have

taken security to the next level by fostering a more complete, or holistic, cybersecurity culture.

The current literature on cybersecurity culture has underscored that it takes more than technology to advance cybersecurity culture within organizations (Alnatheer, 2014; Astakhova, 2014; Batteau, 2011). Specifically, it has been suggested that people and processes should be incorporated in a holistic cybersecurity culture (Batteau, 2011). However, these nontechnical elements of cybersecurity culture have not been clearly or consistently defined, which makes it challenging for organizations to conceptualize and assess their cybersecurity culture (Alnatheer, 2014). Accordingly, the purpose of this research effort was to further explore and understand federal cybersecurity culture. A more thorough understanding of federal cybersecurity culture has the potential to help organizations drive the creation of a more holistic cybersecurity culture (Alnatheer, 2014; Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009).

It is important to note that the cybersecurity challenges faced by the U.S. federal government are not unique. Private-sector organizations clearly face similar cybersecurity challenges. In fact, the National Institute of Standards and Technology's (2017) *Framework for Improving Critical Infrastructure Cybersecurity*, which outlines the federal approach to cybersecurity, has incorporated several private-sector best practices in its control objectives. These best practices include the Control Objectives for Information and Related Technologies (COBIT), which are published by the Information Systems Audit and Control Association. However, federal organizations arguably receive greater scrutiny than the private sector when cybersecurity breaches occur. Further, federal organizations, given their inherent bureaucratic and political nature, have unique

cultural differences from private-sector organizations (National Institute of Standards and Technology, 2017).

Federal Cybersecurity Challenges

Federal organizations continue to face significant cybersecurity challenges (Government Accountability Office, 2016). As a result, the protection of their information technology assets has become a critical focus (Government Accountability Office, 2016). For many, this emphasis has brought to light the need for a more holistic cybersecurity culture and, in particular, the significant role that employees play in sustaining a strong cybersecurity posture. In developing a more holistic cybersecurity culture that incorporates people, processes, and technology, federal organizations stand a greater chance of establishing and sustaining cybersecurity resiliency (Batteau, 2011).

In a survey of federal information technology workers, which was sponsored by Hewlett-Packard and conducted by the Ponemon Institute, respondents viewed the people in their own agencies as greater sources of cybersecurity threats than hackers from foreign organizations. Respondents did not believe federal organizations were fully prepared to address cybersecurity threats. The survey responses suggested that the largest threat to federal cybersecurity was negligent employees and contractors. These findings directly call for a greater understanding of the influence of employees on federal cybersecurity culture (Risen, 2015).

Many federal organizations are increasingly dependent on information technology to carry out their operations. In fact, virtually all business functions in federal organizations are supported by automated systems and electronic data. A few examples of these types of systems and related electronic data include automated financial payment

(e.g., Social Security Administration) and personnel processing systems (e.g., Office of Personnel Management). Many of these organizations would find it difficult, if not impossible, to carry out their missions, deliver services, and account for their resources without the use of information technology assets. As such, the security of these systems is critical to ensuring the confidentiality, integrity, and availability of federal information technology resources (Alnatheer, 2014; Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009).

Technical controls, such as hardware and software, certainly play a critical role in federal cybersecurity posture. However, there are several examples of federal cybersecurity breaches where technical controls were not sufficient to avert the breach. A stronger, more dynamic cybersecurity culture that emphasized policies and employee responsibilities could have facilitated prevention. For example, between April and May of 2010, two unencrypted laptops were stolen from VA contractors. One provided direct access to sensitive medical data, including identifiable information of 644 veterans. These were not the first incidents of their kind at the VA. In May 2006, another laptop containing confidential personal data of more than 26 million veterans was stolen from the VA. At the time, the data theft prompted Congress to mandate that the VA encrypt all data. The theft cost taxpayers approximately $28 million in notification procedures for those impacted and another $20 million to settle a class action lawsuit on behalf of the personnel whose information was stolen (Nagesh, 2010). As a result, one might ask, did the thefts result from failures in the VA's cybersecurity culture? Further, had the VA instituted a more holistic cybersecurity culture, could these information technology security breaches have been avoided?

Cybersecurity is not just an issue for the VA. In September 2012, a contractor at the U.S. Army Chief of Public Affairs erroneously uploaded an Army awards database to a public server and made the personal records of 500 employees, including their Social Security numbers, available to the public (Rosenzweig, 2012). In October 2012, an unencrypted laptop was stolen from the vehicle of a National Aeronautics and Space Administration (NASA) employee; the laptop contained personal information on more than 10,000 current and former agency employees. At the time of the NASA incident, it was estimated that the cost to taxpayers would be approximately $960,000, which did not include ongoing credit monitoring services for affected employees (Sternstein, 2012). Was there something unique about the cybersecurity culture in both the U.S. Army Chief of Public Affairs and NASA that made these security incidents more likely? Should changes have been made to either organization's cybersecurity culture that would have prevented future incidents from occurring?

In 2013, in one of the most famous security breaches in U.S. history, Edward Snowden, a former contractor with the U.S. government, leaked highly classified NSA information to the media that revealed details of the NSA's extensive internet and phone surveillance intelligence programs. The manner in which Snowden gained access to this information continues to be debated in the media (Greenberg, 2013). If Mr. Snowden did gain access to highly classified NSA information either by manipulating his coworkers into sharing their network passwords or by exploiting full-system access, what was it about the NSA's cybersecurity culture that allowed this to occur? In retrospect, were there specific elements of NSA's information security culture that should have been changed prior to Snowden's leak of highly classified information? Further, could the

NSA security leaks have been completely avoided had a more holistic cybersecurity culture been implemented?

Statement of the Problem

The growing number of cybersecurity breaches, related to both personally sensitive and national security information, highlights the need to understand and implement a more holistic cybersecurity culture in federal organizations. A cybersecurity culture that is not holistic presents the potential for significant security breaches, particularly those related to human behavior. In some cases, cybersecurity breaches present significant national security risks. However, the current literature, and related research, has not sufficiently explored federal cybersecurity culture. Specifically, there is a lack of consensus regarding the following: (1) What currently constitutes federal cybersecurity culture? (2) Are there significant variations in the core elements of cybersecurity culture across federal organizations? (3) What should the core elements of cybersecurity culture in federal organizations be? (4) How should federal cybersecurity culture be developed and sustained?

Research Purpose and Questions

While it is clear that the development of cybersecurity culture has become a priority for many federal organizations, it is not clear what the core elements of cybersecurity culture should be. Accordingly, the purpose of this study was to contribute to the understanding of federal cybersecurity culture, its uniqueness, importance, and benefits.

This research effort drew from a sample of cybersecurity experts from federal organizations, with an emphasis on more clearly defining federal cybersecurity culture. In exploring expert views of cybersecurity at these federal organizations, it was expected that convergences and divergences in cybersecurity culture would be identified. Thus, this study addressed one primary research question with four secondary questions:

RQ: What is and what should be the cybersecurity culture in U.S. federal organizations?

1. What are the similarities in cybersecurity culture in U.S. federal organizations?
2. What are the differences in cybersecurity culture in U.S. federal organizations?
3. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?
4. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

Statement of Potential Significance

Ultimately, it is expected that this exploratory study will lead to an enhanced understanding of federal cybersecurity culture. The results have the potential to better inform federal organizations in their efforts to establish a more holistic cybersecurity culture and to provide a better understanding of the desired versus the current state of cybersecurity culture. In addition, the results have the potential to help federal organizations design a stronger cybersecurity posture, which could lead to better protection of information technology assets and critical information.

A more holistic cybersecurity culture will better prepare all federal organizations to mitigate cybersecurity threats. Such threats include those presented from willing and unwilling actors, from both inside and outside of federal organizations, and from technical and nontechnical sources. A holistic cybersecurity culture, if implemented effectively, should better position federal leaders and their respective organizations to combat all threats to their information technology assets. Further—and possibly most significant in the minds of U.S. citizens—a strong cybersecurity culture has the potential to significantly reduce unnecessary costs to taxpayers that result from federal cybersecurity breaches (Alnatheer, 2014; Batteau, 2011; Jenlink, 2001, 2006; National Academy of Science, 2013).

The insights from this study also have potential to contribute to the advancement of current literature concerning cybersecurity and, in particular, the professionalization of the nation's cybersecurity workforce. In addition, this study should provide a bridge between organizational culture theory and its practical application (Jenlink, 2001, 2006; National Academy of Science, 2013).

Conceptual Framework

This section establishes the conceptual framework for exploring organizational cybersecurity culture. Figure 1.1 provides a graphic display of the research conducted, including key constructs and research elements. The narrative that follows the conceptual framework provides further understanding of how theory contributes to the research inquiry.

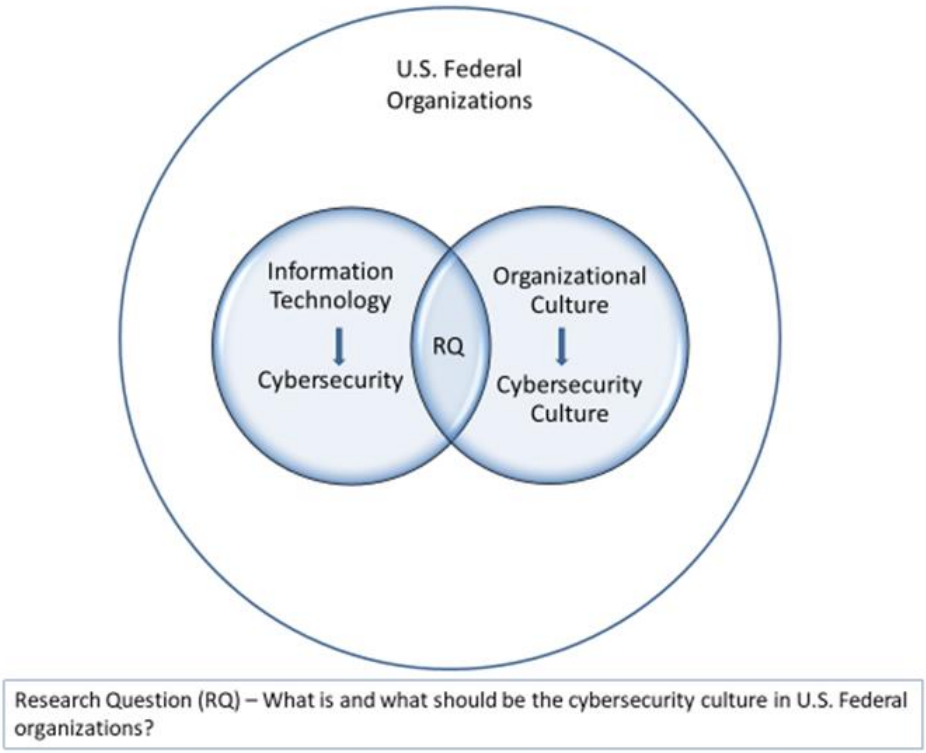

Figure 1.1. Conceptual model.

Information technology includes all resources (people, processes, and technology) used in collecting, classifying, storing, processing, transferring, and presenting information (data). The means include the use of computers and telecommunications equipment to store, retrieve, transmit, and manipulate data, often in the context of a business enterprise. The term is commonly used as a synonym for computers and computer networks. However, it is important to note that humans often play a critical role in information technology. Several industries are associated with information technology, such as computer hardware, software, electronics, semiconductors, internet, telecom equipment, e-commerce, and computer services (IEEE, 1998; National Initiative for Cybersecurity Education, 2012; Odintsova, Kenesova, & Sarsekeyeva, 2013).

Computer and network security, or cybersecurity, is a critical issue for businesses and governments across the globe. However, merely protecting the systems that hold data about citizens, corporations, and government agencies is not enough (Bishop, 2003). Current cyber defense architectures and tools can help address many common concerns, but they are often insufficient in addressing all possible threats. In fact, architecture and tools are only one piece of the complex cybersecurity equation. Prudent organizations understand that people and processes are also a major component of organizational cybersecurity (Batteau, 2011).

Culture can be broadly defined as the shared assumptions, beliefs, values, symbols, artifacts, and behaviors of a group (Schein, 1992). Culture can have multiple layers of analysis and can be viewed through a three-perspective lens: integration, differentiation, and fragmentation (Martin, 2002). The integration perspective focuses on cultural unity, with organization-wide consensus and consistency. The differentiation perspective is frequently seen in loosely coupled organizations, in which subcultures are common. Under the fragmentation perspective, there is an overall lack of consensus regarding organizational culture (Martin, 2002).

Culture is a central driving force behind the actions that occur in organizations (Schein, 1992). Individual members typically have deeply held beliefs about their organization, coworkers, customers, competitors, and industry. These beliefs and assumptions—and their associated behaviors—determine the culture of an organization. The way that these individuals make sense of situations and events will affect their actions. Consequently, these individuals need to find a common understanding and

purpose for the organization to function consistently and effectively (Martin, 2002; Schein, 1992**).**

Organizations that have the best cyber defense strategies establish a well-developed cybersecurity culture. Cybersecurity culture, as has been noted, can encompass a union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and actions focused on furthering cybersecurity within organizations. It also includes the associated values, norms, assumptions, perceptions, and beliefs associated with organizational cybersecurity (Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009; Schein, 1992). Under the current cyberthreat environment, an effective organizational culture is needed to mitigate cybersecurity threats sufficiently (Department of Homeland Security, 2009; Government Accountability Office, 2011; National Initiative for Cybersecurity Education, 2012; Office of Management and Budget, 2008).

Summary of Methodology

The study was a qualitative, exploratory inquiry regarding the core elements of federal cybersecurity culture. Data were collected from a population of 30 cybersecurity experts across the federal sector. This sample size was deemed appropriate for the study, given the fact that informants have a profound understanding of cybersecurity culture based on significant experience in the field. The research participants were identified using purposeful sampling techniques (Boyatzis, 1998; Lincoln & Guba, 1985).

To the extent possible, face-to-face interviews were conducted with participants at their work site or other preferred location. Follow-up interviews were conducted as necessary to further explore or clarify data collected during initial interviews. Each

interview lasted no longer than 90 minutes. Data were collected by audio recording, when approved by the participant, and field notes were generated during and after interviews.

The study utilized an inductive approach to analyzing the data collected, drawing on and building from the concepts and words provided by targeted federal cybersecurity experts (Creswell, 2003; Patton, 2002). Findings were developed by interpreting and clustering the statements made by interviewees, which also enables readers to arrive at their own understanding of the applicability of the findings (Creswell, 2003; Patton, 2002). With an inductive orientation as its foundation, this study utilized Creswell's (2003) data analysis spiral to manage and analyze the data and to generate findings. The researcher used analytic circles, rather than a fixed linear approach, to derive meaningful narratives from the data.

Data management comprises the first loop in the data analysis spiral. In this loop, the researcher maintained transcripts from interviews in hard-copy format as well as in backed-up audio computer files. Once the data were organized, the researcher read the transcripts several times, taking notes and simultaneously trying to get a sense of the whole of the interviews before breaking them into parts or coding (Creswell, 2003). In the next phase of Creswell's spiral, the researcher reflected on the larger thoughts identified in the data and created initial analytic categories, organizing the data into logical clusters and looking for multiple forms of evidence to support each chosen analytic category. Finally, the researcher developed the general themes emerging from the study. The resulting data were then organized thematically by research question. During the final loop of analysis, larger findings emerged from the question-specific themes (Creswell, 2003).

Limitations and Delimitations

The following are limitations and delimitations associated with this study.

1. The boundaries of this research project present certain limitations. Specifically, this research project was scoped to focus on understanding organizational cybersecurity culture in a U.S. federal government context. As a result, the research results may not be easily extended outside of this context.
2. The study was limited to cybersecurity professionals in federal organizations. As a result, generalizability of the findings beyond federal organizations would not be appropriate.
3. Transferability, in a strict sense, is impossible with a naturalistic study. A naturalistic researcher cannot specify the external validity of an inquiry but can only provide a thick, rich description necessary to enable readers to determine whether transfer is a possibility. However, a demonstration of the trustworthiness and dependability of this qualitative analysis and resultant findings can be used as a proxy for transferability and external validity (Lincoln & Guba, 1985).
4. The interviews were limited to a purposeful sample of U.S. federal cybersecurity experts. The study did not directly incorporate a non-U.S. perspective of cybersecurity culture in government organizations.
5. Questions about the reliability of the interview process are a common concern for qualitative research. However, to alleviate this concern, the researcher used an interview guide informed by the research literature to provide rigor. The researcher conducted pilot testing of the interview guide.

Definitions of Key Terms

Table 1.1 defines the key terms used in this dissertation.

Table 1.1
Key Terms and Definitions

Term	Definition
Artifacts	Visual organizational structures and processes (Schein, 1992).
Assumptions	Unconscious, taken-for-granted beliefs, perceptions, thoughts, and feelings—ultimate source of values and actions (Schein, 1992).
Behavior	Group and individual performance, activity, language, customs, and traditions (Schein, 1992).
Cybersecurity	The body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access (National Initiative for Cybersecurity Education, 2012).
Cybersecurity culture	A union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and actions focused on furthering cybersecurity within organizations. It also includes the values, norms, assumptions, perceptions, and beliefs associated with organizational cybersecurity (Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009; Schein, 1992).
Federal organization	A U.S. federal government organization established for the oversight and management of public resources, industries, or national security concerns. Such organizations are typically created by legislative action but can also be created by a presidential order. The senior leadership of these organizations is typically selected by presidential appointment (Investopedia, 2016).
Holistic cybersecurity culture	A union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and direct actions focused on sustaining cybersecurity within organizations (Batteau, 2011; Da Veiga & Eloff, 2007; Dutta & Roy, 2008; Herath & Rao, 2009).
Information technology	The methods, technical means, and application of processes for collecting, classifying, storing, processing, transferring, and presenting information (data). These means include computers and telecommunications equipment to store, retrieve, transmit, and manipulate data, often in the context of a business enterprise. It is important to note that humans often play a critical role in information technology. Several industries are associated with information technology, such as computer hardware, software, electronics, semiconductors, internet, telecom equipment, e-commerce, and computer services (IEEE, 1998; National Initiative for Cybersecurity Education, 2012; Odintsova et al., 2013).
Norms	The standards or patterns of group social behavior (Schein, 1992).
Organizational culture	The shared beliefs, norms, values, assumptions, symbols, artifacts, and behaviors of an organization (Martin, 2002; Schein, 1992).
Values	Publicly announced strategies, goals, and philosophies—espoused justifications for actions (Schein, 1992).

CHAPTER 2:

LITERATURE REVIEW

This literature review provides an overview of the current state of scholarly research pertaining to the identified problem statement and research question. The review process involved an extensive examination of seminal and contemporary literature, centered on five relevant topic areas: organizational culture, information technology, information technology and organizational culture, cybersecurity, and cybersecurity culture. These topic areas served as the primary research terms.

Literary works were identified through an exhaustive search of available resources, which included traditional library research and utilization of online scholarly research databases. The five relevant topic areas, and variations within the group, were the initial list of search terms. Fourteen scholarly databases were utilized as part of the literature review: George Washington University Library databases, ABI/Inform, Academic Search Complete, ArticlesPlus, ERIC (EBSCO), Google Scholar, IEEE/IEEE Electronic Library, JSTOR, LexisNexis Academic, ProQuest Research Library, Project Muse, PsycINFO, Web of Science, and WorldCat.

The initial list of literary works, which included hundreds of items, was formally catalogued. The list was pared down after a more detailed review of each item. The effort resulted in a concise collection of books and peer-reviewed articles expected to best inform investigation of the problem statement and research questions.

Organizational Culture

At its core, organizational culture is the shared assumptions of an organization (Schein, 1992). The most useful way to think about culture is to view it as the accumulated shared learning of a given group, covering behavioral, emotional, and cognitive elements of the group members' total psychological functioning. These basic assumptions are adopted by the organization as it solves its problems of external adaptation and internal integration; they are also taught to new members as the correct way to perceive, think, behave, and feel in relation to those problems (a product of joint learning). Ultimately, these assumptions have great impact on organizational performance. Given the significance of culture, Schein asserted it was management's ultimate responsibility to develop, change, and sometimes break down culture in order to ensure organizational success. Schein's (1992) theory and definition of culture served as the foundation for this research effort.

Schein (1992) depicted culture as being difficult to describe concretely. However, he believed culture could be analyzed from three levels: artifacts, espoused values, and underlying assumptions. Espoused values are explicitly stated organizational values, but it is important to note that these values may not be directly related to action. Artifacts include broadly recognized organizational symbols. Underlying assumptions are not easily defined or identified, but reflect the tacit understanding or unspoken norms of the organization. Figure 2.1 provides a graphical overview of Schein's culture model.

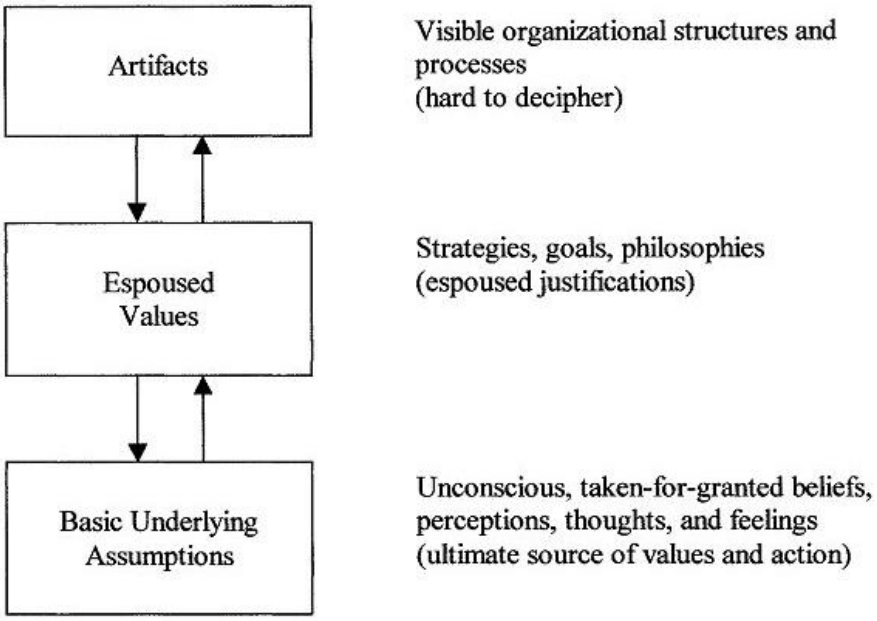

Figure 2.1. Schein's cultural model (1992).

Schein (1992) also believed that there were 10 major categories of overt phenomena associated with organizational culture:

1. Observed behavioral regularities when people interact (language, customs, traditions, and rituals)
2. Group norms
3. Espoused values
4. Formal philosophy
5. Rules of the game
6. Climate
7. Embedded skills
8. Habit of thinking, mental models, and/or linguistic paradigms
9. Shared meanings
10. Root metaphors

Schein (1992) observed that the concept of culture is most useful if it helps to explain some of the seemingly incomprehensible and irrational aspects of groups and organizations. Schein further stated that shared assumptions derive their power from operation outside of awareness; they become a defining property of the group and allow the group members to differentiate themselves from others. Schein also explained that the most decisive function of a leader is the creation and management of culture. He noted that culture and leadership were two sides of the same coin: (1) leaders first establish cultures when they create groups and organizations, and (2) once cultures exist, they have a significant role in determining the criteria for leadership. In some cases, this responsibility can require management to tear down and completely rebuild culture. Culture change involves a process of changing basic assumptions and is difficult, often time consuming, and highly anxiety provoking. Ultimately, understanding culture is desirable for all of us, but it is essential for leaders if they are to lead effectively (Schein, 1992).

Mary Jo Hatch (1993) built on the work of Edgar Schein (1992) with her model of organizational culture dynamics. Figure 2.2 provides a graphical display of Hatch's cultural model, which directly links organizational culture processes with leadership and learning. She established culture as an ongoing process of organizational stability and change. Hatch (1993) expanded Schein's (1992) model of culture by incorporating symbols. Unlike artifacts, symbols do more than simply represent something else. Symbols allow those who employ them to supply meaning. However, the four core elements of her model—i.e., values, assumptions, artifacts, and symbols—are less central individually, and the focus shifts to the relationships between the elements.

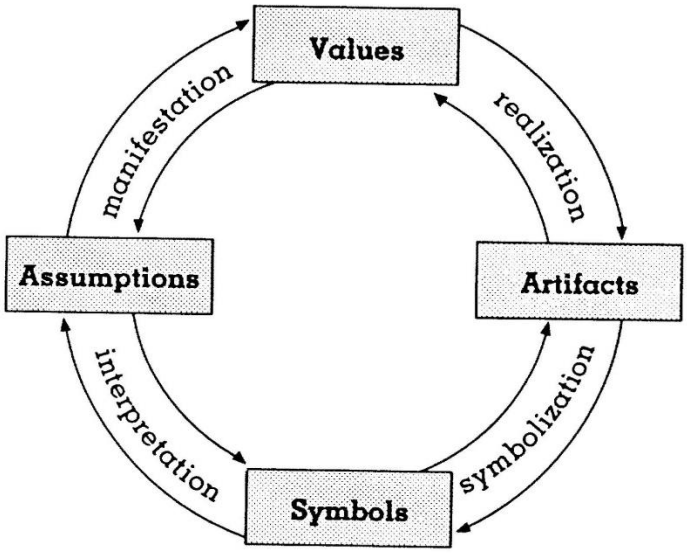

Figure 2.2. Hatch's cultural dynamics model (1993).

In her model, Hatch (1993) presented four relational elements:

1. Manifestation. In moving clockwise around the model (proactive), cultural assumptions are revealed in the perceptions, cognitions, and emotions of organizational members. In moving counterclockwise (retroactive), assumptions are maintained or altered.
2. Realization. Proactive realization is defined as the process by which values or expectations receive some degree of representation in tangible forms. Conversely, retroactive realization involves a process of value realignment with artifacts.
3. Symbolization. Proactive symbolization is the process by which cultural symbols develop true meaning. The retroactive process devolves symbols into artifacts—a wider, usually more abstract, concept or meaning.
4. Interpretation. Prospective interpretation maintains or challenges basic assumptions, whereas the retrospective process reconstructs the meaning of symbols based on cultural assumptions.

There are some distinct differences between the Schein and Hatch models. Schein's culture model centers on the ways that artifacts and values are linked to basic assumptions. Schein focused primarily on how to change culture. In contrast, the Hatch model is constituted by the elements of the model and the processes that link them. The Hatch model maintains a dual focus on stability and change. Hatch implied that stability and change are dual products of the same cultural process. In essence, old culture elements can leak into the new culture (Hatch, 1993).

Denison and Mishra (1995) created an instrument, based in large part on Schein's (1992) work, that views organizational culture as a reflection of the past and an enabler of the future. Their model focuses on four primary elements of culture: involvement, adaptability, understanding of mission, and consistency. Their model has proven to be an effective predictor of quality, employee satisfaction, and organizational performance (Denison & Mishra, 1995).

Giblin and Amuso (1997) contended that corporate values and corporate culture are two critical elements in an organization's strategic plan and evolve as interchangeable terms to highlight leader vision to institutionalize corporate values and behavior. Castellano, Rosenzweig, and Roehm (2004) contended that management by objectives and management by results provide the critical framework of an organization that supports its culture because they require leadership to foster cooperation, teamwork, and collaboration, which are the essential ingredients for creating socially interdependent organizational relationships. Dess et al. (2003) highlighted organizational learning and knowledge as the foundation for an organization's performance and organizational change strategies. Burgelman and Doz (2001) defined the ways that the organizational

structure directly influences the organizational culture, integrates the organizational environment, and internalizes embedded learning and shared expectations for organizational sustainability.

Joanne Martin (2002) presented a three-perspective view of organizational culture: integration, differentiation, and fragmentation. The integration perspective focuses on cultural unity, with organization-wide consensus and consistency. Under the integration perspective, deviations from consistency, organization-wide consensus, and clarity are viewed as problematic. The differentiation perspective is frequently seen in loosely coupled organizations, in which subcultures are common. Relationships among subcultures can be mutually reinforcing, conflicting, or completely independent. Cultural consensus typically exists only within particular subgroups. However, subgroups can share common cultural elements. The fragmentation perspective involves multiplicity and flux with regard to organizational culture. In many organizations, there are multiple, conflicting interpretations regarding culture. Ultimately, under the fragmentation perspective, there is an overall lack of consensus regarding organizational culture (Martin, 2002).

For most organizations, an integrated culture is certainly ideal. However, the reality for large, or loosely coupled, organizations is more likely to be a differentiated culture. This places a significant burden on leadership to establish and sustain core cultural values across the organization. A fragmented culture is not ideal for any organization. It would be advisable for leaders in fragmented organizations to focus on initiatives to strengthen cultural integration (Martin, 2002; Schein, 1992).

Information Technology: An Overview

There are many perspectives on information technology. Roberts (1996) defined information technology as the hardware and software used to obtain, store, apply, communicate, and render information. Porter and Miller (1985) viewed information technology as the information developed and utilized by an organization and the tools used to process this information. Lee (2006) defined information technology as all the resources used in the management of organizational data.

Regardless of the definition of information technology, it is arguably the most important development in the modern business world (Roberts, 1996). Information technology has had a broadly positive impact across the globe, enabling large and small organizations to successfully exploit its business benefits (Roberts, 1996). Sakaguchi and Dibrell (1998) found a positive correlation between the intensity of information technology usage by global firms and their success. They also suggested that information technology is a source of competitive advantage that should be employed by every organization (Sakaguchi & Dibrell, 1998).

Information technology is a powerful tool that has virtually unlimited business application and flexibility. However, the rapid changes in information technology standards require constant attention by trained professionals (Roberts, 1996). Benamati and Lederer (2010) proposed that the constant rate of change in information technology causes nine primary organizational problems (Table 2.1).

Table 2.1
Nine Primary Problems Associated with Rapid IT Change in Organizations

Problem	Description
Vendor neglect	Insufficient experience, knowledge, or problem determination ability from suppliers of IT
Vendor oversell	Premature marketing or the setting of unrealistic expectations by suppliers of IT
Acquisition dilemma	Difficulty staying informed about or choosing new IT
Support burden	Lack of external expertise about, control over, or IS organization structure to properly administer new IT
Resistance	Disagreement about use, or reluctance to accept new IT
Cascading needs	Unanticipated need for or dependence on new IT
New integration	Incompatibility or need for interfaces between multiple ITs
Errors	Inadequate documentation of or shortcomings in new IT
Training demands	Long learning curves, diminished productivity with and difficulty retaining staff experienced in new IT

Note. From Benamati and Lederer (2010).

However, Benamati and Lederer (2010) also suggested five possible coping mechanisms for these nine problems associated with the rapid rate of information technology change (Table 2.2). The challenges and coping mechanisms described by Benamati and Lederer (2010), although not explicitly stated, establish a connection between information technology and organizational culture. This is particularly evident with the call to use education, training, and internal procedures as coping mechanisms for information technology challenges.

Table 2.2
Five Coping Mechanisms for Rapid IT Change in Organizations

Mechanism	Description
Consultant support	Engage external IS professionals to help plan for, implement, problem solve, or provide ongoing support for new IT
Education and training	Stay informed of new IT as it becomes available and instruct or provide guidance in the use of new IT
Vendor support	Rely on IT suppliers for problem determination and resolution, customization to, interfaces with, and functional enhancement to new IT
Internal procedures	Develop processes to aid in the evaluation, acquisition, and implementation of new IT
Endurance	Ignore or work around problems, and learn new IT without formal education

Note. From Benamati and Lederer (2010).

Information Technology and Organizational Culture

In the modern business world, successfully managing the constant changes in information technology can be an extreme challenge for any organization. Jackson and Philip (2010) suggested that successfully managing these changes requires a technocultural fusion. Further, efforts to institute information technology changes with a lack of attention to organizational culture are less likely to be successfully. By blending culture and technology, organizations can better position themselves to manage technology changes (Jackson & Philip, 2010).

Culture has the ability to inhibit or to promote the adoption of information technology in organizations. Similarly, new technology has the power to change organizational culture. The influence that culture and technology have on each other can directly impact business strategy and performance. Organizations will either resist the adoption of new technology or adapt and modify business practices. However, organizations that resist the adoption of new technologies may risk not being able to keep up with their more agile competition. The primary reason why businesses refuse to adopt new technologies is their culture: their shared patterns of beliefs and assumptions do not promote the integration of new technologies. To sustain success, however, organizations must develop a culture that is open to learning and adopting new technologies (Yu & Kwan, 2015).

Organizational culture has the ability to orient its members with regard to change. Accordingly, the information technology adoption within an organization will be directly influenced by its culture. Harrington and Guimaraes (2005) suggested that an organization with a learning culture is best suited for the adoption of technology. In

addition, they contended that a culture that has a strong external focus tends to have greater adoption of technology. They added that an external focus, in this sense, means an organizational emphasis on flexibility and maintaining a competitive position within its operating environment (Harrington & Guimaraes, 2005).

What is often lost in the move to implement new technologies in organizations is the impact on people and what they think and believe (Larkin, 2008). New technologies can have a dramatic positive impact on business functions, but this positive impact can be drastically reduced by certain cultural norms, such as a general organizational resistance to change (Larkin, 2008). In addition, an organization that does not promote learning as part of its culture may have difficulty with the adoption of new technologies (Larkin, 2008).

Gallivan (1997) discussed the importance of fit between organizational culture and new technologies. Specifically, how suitable is the new technology, given the culture of the organization? Further, endeavors to introduce new technologies without consideration of culture are likely to fail. Gallivan (1997) identified three general strategies for implementing new technologies in organizations: (1) ensure the existing culture is aligned with the proposed technology, (2) make a simultaneous change in the culture and technology, and (3) use the new technology as a catalyst for change. The first two strategies are more likely to lead to the acceptance of a new technology, with users expected to actively facilitate the change. The final strategy is less likely to succeed, with the flawed assumption that culture will automatically change with the introduction of a new technology (Gallivan, 1997).

U.S. federal organizations face significant challenges in adopting new technologies. This is particularly true with the shift of work to more decentralized environments, where the adoption of new technologies is essential to fulfilling organizational missions. In a study that included federal employees, a direct correlation was identified between individual perception of organization culture and adoption of new technologies (Melitski, Gavin, & Gavin, 2010). The authors also noted that when the culture of an organization is supportive, the probability of adoption of new technology is significantly higher, and they called for further research and development in the field of technology management, with an emphasis on the relationship between technology adoption and organizational culture (Melitski et al., 2010).

Larkin (2008) suggested that federal organizations should mirror the best practices in industry when implementing new technologies. Specifically, developing a cultural understanding and acceptance for new technologies is critical. This cultural acceptance of technology must be developed through marketing, education, and on-the-job training. Only through a full technical-cultural integration will most federal organizations maximize their investments in information technology (Larkin, 2008).

Martinsons and Davison (2003) reviewed a wide array of cultural issues believed to be significant in the management of information technology. Their review indicated that cultural concerns should be at the forefront in planning any information technology implementation. However, while it is clear that organizational culture has an impact on information technology implementation and management, the theories that explain and predict the impact are lacking. This deficiency calls directly for theory building with

regard to the link between information technology and organizational culture (Martinsons & Davison, 2003).

Gallivan and Srite (2005) stated that information technology and culture research have historically been conducted separately and, hence, not been connected effectively with each other. In response, Gallivan and Srite developed a new conceptualization of culture, which directly incorporates information technology. Specifically, they created a more holistic approach to defining culture and understanding how it shapes human behavior, to include an emphasis on information technology–related beliefs and assumptions. The framework is believed to further the understanding of the influence of culture on the adoption of information technology. Gallivan and Srite's framework can be used as a guide for managers in the implementation of new technologies. Cultural awareness and its potential influences should always be considered with the introduction of new technologies (Gallivan & Srite, 2005).

A high-quality information technology strategic plan can allow organizations to assert priorities to meet information technology goals (Bradley, Pridmore, & Byrd, 2006). In some cases, these plans detail the allocation of human and financial resources needed to meet strategic information technology goals. In fact, in the absence of a quality strategic plan, the risk of failure associated with information technology initiatives can increase dramatically (Bradley et al., 2006). However, corporate culture is often a critical missing element in information technology strategic plans. Even the strongest information technology strategic plan is destined for failure if the corporate culture does not support planned initiatives (Bradley et al., 2006). Accordingly, a management focus

on organizational culture is a critical element of every information technology strategic plan (Bradley et al., 2006).

Culture is unquestionably a critical factor in the success or failure of information technology adoption in organizations (Jackson, 2011). This is evidenced in the growing number of studies focused on the relationship between information technology and culture, which includes the following broad categories: (1) culture and information technology adoption, (2) culture and information technology use, (3) culture and information technology outcomes, (4) culture and information technology management, and (5) culture's influence on information technology (Jackson, 2011). However, these studies tend to focus only on an integrated perspective of organizational cultures in which everyone in the organization has the same perspective regarding information technology. In reality, Martin's (2002) three perspectives of culture—integration, differentiation, and fragmentation—can be used to deepen understanding of the influence that culture has on information technology in organizations. Within any given organization, subgroups can certainly have different perspectives regarding information technology adoption (Jackson, 2011).

The role of culture has become a key focus in information technology strategic planning. Kummer and Schmiedel (2016) reviewed the literature regarding culture and information technology strategy and revealed a literature stream that focused on describing, explaining, and interpreting observed information technology culture. In addition, they cited significant literature that focused on the importance of culture in driving the success of information technology initiatives. However, there is a gap in the literature regarding culture management and information technology change. Kummer

and Schmiedel (2016) called for more research that theorizes about information technology culture development and management.

Cybersecurity

Computer and network security, or cybersecurity, are critical issues in businesses and governments across the globe. Cybersecurity is the focus on protecting all information technology assets against attack, damage, access, or unauthorized use (Meeuwisse, 2017b). Cybersecurity involves the body of technologies, processes, and practices designed to protect networks, computers, programs, and data (National Initiative for Cybersecurity Education, 2012). However, merely protecting the systems that hold data about citizens, corporations, and government agencies is not enough (Bishop, 2003). Current cyber defense architectures and tools can help address many common concerns, but they are often insufficient in addressing all possible threats. In fact, architecture and tools are only one piece of the cybersecurity equation. Prudent organizations understand that people and processes are also a major component of organizational cybersecurity (Batteau, 2011).

In fact, human behavior is one of the biggest challenges to organizational cybersecurity (Chou, 2007; Von Solms & van Niekerk, 2013). For example, employees often do not safeguard their network passwords, or they use simple passwords that make it easy to hack their work accounts. Serious security breaches have occurred when individuals chose to carry sensitive data on unencrypted devices, such as laptops or flash drives, and accidently lost the device. In addition, employees often do not follow access control policies, letting others use their account or permitting physical access to restricted areas. Also, employees frequently fall for phishing scams, which can lead to the

compromise of usernames, passwords, and sensitive information (Chou, 2007). Von Solms and van Niekerk (2013) noted that humans can be knowing or unknowing participants in cyberattacks. The human element also brings ethical considerations for particularly vulnerable groups, such as mentally challenged, young, and elderly individuals. As such, cybersecurity should be viewed as a societal responsibility (von Solms & van Niekerk, 2013).

Cybersecurity is a critical issue for countries and organizations across the globe. In fact, there is a direct correlation between the worldwide increase in the use of information technology and cybersecurity threats. These threats are pervasive in both public- and private-sector organizations. The result is a universal increase in the resources dedicated to furthering cybersecurity (Kesswani & Kumar, 2015).

The use of information technology has become pervasive, shaping the lives of individuals worldwide. The use of smart devices with the ability to connect to anyone or anything, from almost anywhere, has become an international standard. The use of technology has made it possible, literally and figuratively, to have a more connected world. However, the ubiquitous use of technology, with all of its potential societal good, also brings significant risk and possible danger to individuals and organizations (Meeuwisse, 2017a).

Cybersecurity Categories

Cybersecurity can be broadly divided into four distinct categories: (1) network cybersecurity, securing data on the network, whether wired or wireless; (2) host cybersecurity, protecting software applications and operating systems; (3) storage cybersecurity, securing stored data locally and on larger database repositories, such as

backup tapes and database management systems; and (4) administrative cybersecurity, the nontechnical element of cybersecurity, consisting of human and process security (Chou, 2007).

Stacey, Helsley, and Baston (1998) presented a structured approach for identifying an enterprise-specific threat to an organization's information systems. Their research indicated that one of the major information security threats to an organization is from its own personnel. They also discussed the changing role of cybersecurity practitioners, the categories of threat, and consistent definitions of terms. The publication also provided safeguards for cyberthreats and discussed the importance of assigning agents to deal with specific threat categories (Stacey et al., 1998).

Cybersecurity Policies and Regulations

Securing information within organizations has become essential as organizations depend more and more on information systems to conduct business operations and processes. The research study by McFadzean, Ezingeard, and Birchall (2007) indicated that cybersecurity is increasingly important due to a variety of internal and external security threats. Additionally, governance and regulations such as the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act, and the American Recovery and Reinvestment Act of 2009 have placed new requirements on businesses to secure information and meet specific process requirements.

In December 2008, the Cyberspace for the 44th Presidency Report identified cybersecurity as an essential strategic national security issue that presents challenges on a global enterprise scale, beckons public diplomacy practitioners, and challenges academics to analyze the economic influence (Baker, 2009). Emerging technologies

increase the number of cyberattacks on information networks, which may result in data transfer vulnerabilities and data communication infiltration of enterprise networks (Holstein, 2009). The globalization of information technologies might require the U.S. federal government to develop cybersecurity strategies to enforce information assurance policies and support metrics on a broad social scale (Vaughn, Henning, & Siraj, 2003; Wilshusen, 2010). Chabinsky (2010) emphasized that cybersecurity is a process requiring continual assessments of technologies, policies, and related resources within organizations. A commitment by senior leadership within organizations to plan effective strategies for the evolution of security policies, ensuring the confidentiality, integrity, and availability of organizational information, is vital (Government Accountability Office, 2006).

On February 12, 2013, the president of the United States issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which established "the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (National Institute of Standards and Technology, 2014, p. 1). The order resulted in the National Institute of Standards and Technology (2014) publishing a *Framework for Improving Critical Infrastructure Cybersecurity*. This framework clearly highlights the fact that cybersecurity threats present great risk to the overall security of the United States. Accordingly, the document outlines a process for identifying, assessing, and managing cybersecurity risks to the nation's critical infrastructure. The framework is viewed as a cybersecurity risk-

management tool that organizations can use to determine activities that are most important to critical service delivery and to prioritize expenditures to maximize the impact of the investment. While this tool certainly provides great value, it does not directly address the significance of organizational culture in sustaining critical infrastructure cybersecurity (National Institute of Standards and Technology, 2014).

Cybersecurity Culture

Originally, organizations depended on technical controls such as hardware and software techniques to safeguard their information. Organizational information security policies**,** employee user agreements, personnel security training, and standard operating procedures were developed to improve information security and to incorporate cybersecurity into the organizational culture at a basic level. However, in today's information-risk environment, technical controls, policies, and procedures alone are not sufficient. In fact, cybersecurity leaders must develop and sustain an organizational culture of cybersecurity (Department of Homeland Security, 2009; Government Accountability Office, 2011; National Initiative for Cybersecurity Education, 2012; Office of Management and Budget, 2008).

Culture and Cybersecurity Effectiveness

Chang and Lin (2007) analyzed the influence that organizational culture has on the success of cybersecurity initiatives. Based on an extensive literature review, they developed a model of the relationship between organizational culture and cybersecurity. Both organizational culture characteristics and cybersecurity effectiveness were measured empirically. They delivered questionnaires to respondents in organizations that made

significant use of information systems and investigated how various organizational culture traits influenced cybersecurity principles. The research centered on the relationship between organizational culture traits (including cooperativeness, innovativeness, consistency, and effectiveness) and cybersecurity principles (which include confidentiality, integrity, availability, and accountability). The objectives of this study were to find out how organizational culture influences cybersecurity effectiveness and to identify what kind of organizational culture is conducive to effective cybersecurity implementation. A regression analysis was used to derive the impact of organizational culture on the effectiveness of cybersecurity. The study results indicated that organizational culture had a significant impact on the success of cybersecurity programs. These results were expected to benefit enterprise managers and decision makers in establishing organizational cybersecurity goals.

Significance of Cybersecurity Culture

Ghernouti-Hélie, Tashi, and Simms (2010) acknowledged the importance of a culture of cybersecurity in organizations. The state of cybersecurity in an organization is a direct reflection of the security norms and behaviors that individuals in the organization voluntarily follow. Accordingly, they noted that incorporating cybersecurity directly in organizational culture is a best practice to further cybersecurity efforts in organizations (Ghernouti-Hélie et al., 2010).

A cybersecurity culture has two primary elements: constitutive and activities (Ghernouti-Hélie et al., 2010). The constitutive element is concerned with the weakest link in the cybersecurity chain, human beings, and calls for greater awareness and clarity

regarding individual responsibilities. This includes establishing a foundational level of organizational cybersecurity culture (Ghernouti-Hélie et al., 2010).

Leadership and Cybersecurity Culture

Cybersecurity is one of the most critical global issues of countries and organizations. With the ever-increasing use of computers and the internet, there has been a tremendous rise in cyberattacks. The attackers target not only high-end companies, but also banks and government agencies. As a result, companies and governments across the globe are emphasizing the need for a stronger cybersecurity culture (Kesswani & Kumar, 2015). Arnold (2017) suggested that treating cybersecurity as simply an information technology concern will leave an organization unprepared for the reality of cyberthreats. Accordingly, leaders must take charge to instill a sense of the magnitude of cybersecurity, beyond technical controls, within their organizations (Arnold, 2017). The visible and regular support of cybersecurity by top management is an effective means to reduce information security risks and establish an information security culture (Harrington, 1996). When employees see that their senior managers support organizational cybersecurity, it becomes more important to them (Harrington, 1996). A cybersecurity policy endorsed by top management and signed by employees indicates that the organization is serious about information security (Harrington, 1996).

Similarly, Da Veiga and Eloff (2007) discussed how the development of an effective cybersecurity culture within an organization is related to the specific actions of management. They discovered that leadership could directly impact the success or failure of an organization's cybersecurity program. It is essential that cybersecurity leaders effectively instill a sense of organizational urgency around information security and

related policies. In most cases, this will require cybersecurity leaders to transform the security culture of their organization (Herath & Rao, 2009).

Promoting a Cybersecurity Culture

Promoting security awareness should be a part of an organization's overall cybersecurity culture, philosophy, and vision (Spurling, 1995). Spurling presented a case study of a major Australian organization, tracing the history of computer security within the organization, how commitment was built, and the security awareness initiatives that were rolled out. Cybersecurity leaders played a critical role in the organization's security culture, developing and implementing various security awareness initiatives that kept employees conscious of security concerns and helped maintain a security culture (Spurling, 1995).

Thomson and von Solms (1998) described the evolution of computing, with specific reference to cybersecurity issues. These security issues were then developed further to determine the need to educate the workforce through a cybersecurity awareness program. This publication identified a number of psychological issues that can effectively influence one's attitude and/or behavior. Considering that changing attitudes and behavior should be a primary objective of security awareness programs, the identified psychological principles could be integrated into awareness programs to make them more effective. Thomson and von Solms (1998) went on to describe how social psychology methods could be integrated in awareness programs and the potential positive impact. This article concluded that for security awareness programs to be more effective, social psychological principles need to be tailored to address specific groups of employees

within the organization. Ultimately, this should be an important emphasis for cybersecurity leaders.

Cybersecurity is a critical issue for all organizations that depend on information technology. Security policies are only effective if company employees know, understand, and follow them. This implies that appropriate security training and awareness is conducted within organizations. However, many smaller organizations find it difficult to implement comprehensive information security training due to the lack of expertise within the organization. Cybersecurity leaders in smaller organizations should make use of computer-based training that is interactive and user friendly as a solution. Well-developed training programs are a key element to furthering cybersecurity culture, whether the organization is large or small (Furnell, Gennatou, & Dowland, 2002).

Rotvold (2008) also focused on training, noting that if human behavior is part of the information security problem, it can also be part of the solution. Accordingly, employees should be an integral part of any organization's information security defense posture. Specifically, a formal security awareness training program should be established in organizations interested in developing a stronger security culture (Rotvold, 2008).

The purpose of the study by Chen, Shaw, and Yang (2006) was to investigate how cybersecurity leaders could mitigate risks by developing security awareness in organizations. To accomplish this, they used a systems development approach consisting of five steps: constructing a conceptual framework, developing a system architecture, analyzing and designing the system, building a pilot system, and observing and evaluating the system. Additionally, they conducted a limited number of interviews of two senior cybersecurity leaders and one training manager within the organization. Their

findings indicated that greater information security awareness was needed to provide effective system management. Further, a systems manager needed the ability to customize the interface to meet individual needs (Chen et al., 2006).

Call for the Study of Cybersecurity Culture

In his detailed literature review on cybersecurity culture, Alnatheer (2014) found no mutual agreement on what factors comprise cybersecurity culture. In fact, not only was there little evidence as to the factors that constitute cybersecurity culture, but there was also an absence of literature regarding what drives the creation of cybersecurity culture. Ultimately, the true contribution of the study was the identification of a gap in the existing literature regarding cybersecurity culture. Specifically, the study called for additional empirical research regarding the composition of cybersecurity culture (Alnatheer, 2014).

Implications for the Current Study

The literature reviewed provided unmistakable evidence of a need to improve the understanding of core elements of cybersecurity culture. This evidence starts with the indication in the literature that technical controls, policies, and procedures alone are not sufficient to protect organizations. As a result, prudent cybersecurity leaders must develop and sustain an organizational culture of cybersecurity (Department of Homeland Security, 2009; Government Accountability Office, 2011; National Initiative for Cybersecurity Education, 2012; Office of Management and Budget, 2008).

The significance of organizational culture can be traced directly to Edgar Schein (1992). He asserted that organizational culture is, at its core, the shared assumptions of an

organization. Further, these assumptions have great impact on organizational performance. Given the significance of culture, it is management's ultimate responsibility to develop, change, and sometimes break down culture (Schein, 1992).

Da Veiga and Eloff (2007) discussed how the development of an effective cybersecurity culture within an organization is directly related to the specific actions of management within the organization. In addition, Harrington (1996) stated that the visible and regular support of cybersecurity by top management is an effective means of reducing information security risks and establishing an information-security culture.

Alnatheer's (2014) identification of a gap in the existing literature regarding cybersecurity culture and his call for additional empirical research regarding the composition of cybersecurity culture has strong implications in the federal sector. While there is certainly an emphasis on cybersecurity culture in the literature, there has not been a thorough exploration of federal cybersecurity culture. Specifically, the literature is silent on what constitutes federal cybersecurity culture, to include core elements, possible variations, development, and management. Accordingly, this study was expected to contribute significantly to the understanding of federal cybersecurity culture.

CHAPTER 3:

METHODOLOGY

This research effort centered on a mix of cybersecurity experts from federal organizations, with an emphasis on developing a deeper understanding of federal cybersecurity culture. In interviewing cybersecurity experts from federal organizations, it was expected that convergences and divergences in federal cybersecurity culture would be identified. The study addressed one primary research question with four secondary questions:

RQ: What is and what should be the cybersecurity culture in U.S. federal organizations?

1. What are the similarities in cybersecurity culture in U.S. federal organizations?
2. What are the differences in cybersecurity culture in U.S. federal organizations?
3. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?
4. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

Creswell (2003, 2007) professed that qualitative approaches are best suited for exploring a human problem, especially when theories have not been developed. This would certainly apply to federal cybersecurity culture, where there is a deep understanding of neither its constituent factors or what drives its creation (Alnatheer, 2014). Accordingly, qualitative inquiry methods were used in conducting this research

effort. Specifically, this research effort was an exploratory study designed to investigate federal cybersecurity culture.

This chapter presents the study's assumptions and describes the qualitative research design. It then presents procedures for selecting participants, collecting data, and analyzing data. Final sections discuss trustworthiness, present a subjectivity statement, and review ethics precautions.

Research Assumptions

There is little doubt that individuals in society have a tendency to interpret the world differently. What one person perceives as objective fact, another may view as subjective reality. Whether explicitly or implicitly, individuals rely on a philosophy of science to interpret the meanings, logical relations, and consequences of their observational and theoretical statements. Therefore, it is critical to establish a clear philosophical viewpoint for any research. Underlying any form of research is a philosophy of science that informs the nature of what can be known about the phenomenon examined (ontology) and the methods chosen by the researcher for knowing it (epistemology) (Ponterotto, 2005).

A research paradigm is a set of interrelated assumptions about the social world that provide a philosophical and conceptual framework for an organized study of that world. The paradigm selected by a researcher is based on philosophical assumptions about the phenomenon under study, and it influences the selection of tools, instruments, participants, and methods for the study. Numerous paradigms have been used to guide research, and researchers incorporate different paradigmatic schemas to conceptualize and classify research (Ponterotto, 2005).

For the purpose of this study, which focused on developing an understanding of the core elements of federal cybersecurity culture, the constructivism–interpretivism paradigm was the central focus (Ponterotto, 2005). Under this paradigm, reality is constructed in the mind of discrete individuals (i.e., the researcher and the participants), rather than being considered an externally singular entity. The constructivist–interpretivist position espouses a hermeneutic approach to understanding the world, which maintains that meaning is hidden and must be brought to the surface through deep reflection. This reflection can be stimulated by interactive dialogue between the researcher and participants. A distinguishing characteristic of constructivism is the interaction between the investigator and the object of investigation. Further, only through this interaction can deeper meaning be uncovered.

The goals of research based on constructivism–interpretivism are both idiographic and emic. Research under constructivism–interpretivism tends to be qualitative (Ponterotto, 2005). In this case, the study was emic in nature, with an emphasis on the analysis of a cultural phenomenon from the perspective of individuals who participate in the culture. Specifically, this was a qualitative, exploratory study of federal-sector organizations, with an emphasis on understanding federal cybersecurity culture.

Qualitative Research Design

Lincoln and Guba (1985) suggested that the use of qualitative approaches is ideal for dealing with multiple realities formed by different actors; they also placed emphasis on the use of the natural setting to perform the inquiry, as realities cannot be understood in isolation from their contexts. This would certainly apply to cybersecurity culture, where a common definition and understanding of the phenomenon does not exist

(Alnatheer, 2014). Further, the investigation focused on federal-sector organizations, where direct interaction was needed to better understand cybersecurity culture in this context.

Beall (2002) argued that exploratory research can be particularly useful for building new knowledge. Further, he stated that exploratory research naturally lends itself to studies of uncharted areas. Beall's view of exploratory research can certainly be applied to an investigation of federal cybersecurity culture, where there is an apparent lack of understanding regarding its core elements.

Population for the Study

This research effort involved the population of cybersecurity experts from federal-sector organizations. There are hundreds of federal organizations, with each employing its own cybersecurity workforce. For the purpose of this study, 30 participants were selected from across the federal cybersecurity workforce. This sample size was considered adequate for the study, given that each participant was a key informant with a profound understanding of federal cybersecurity culture.

The research participants were identified using purposeful sampling techniques (Boyatzis, 1998; Lincoln & Guba, 1985). The following qualifying criteria were used to identify potential participants for the study:

- Domain-related expertise. Research participants had to be cybersecurity experts working within federal organizations. The research literature supports general definitions of expertise as being 10,000 hours, or 10 years, of specialized, domain-related work. The greater the participant's amount of applied, high-quality experience, the greater the expertise (Ericsson & Charness, 1994; Ericsson

& Lehmann, 1996; Maxwell, 2013; Patton, 2002). Thus, quantifiable identifiers led the participant selection standard and definition of expertise that were used for this study.

- Higher education degree or domain-related certification. The role of education and training in expertise formation is important (Ericsson & Charness, 1994), but the impact of any one area of study on cybersecurity expertise is uncertain. Accordingly, a minimum of an undergraduate degree and/or domain-related certification in cybersecurity was required for this study. In fact, an undergraduate degree and cybersecurity certification are common requirements for federal employers hiring cybersecurity specialists and technologists (Ericsson & Charness, 1994; Ericsson & Lehmann, 1996; Maxwell, 2013; Patton, 2002).
- Limited relationships. No more than two individuals from the same organization were included in this study. Experts were solicited from a broad set of federal organizations. This was intended to limit the bias that may result from a homogenous sample and to allow investigation of similarities or dissimilarities among federal organizations (Ericsson & Charness, 1994; Ericsson & Lehmann, 1996; Maxwell, 2013; Patton, 2002).
- Role. The final criterion for inclusion was current practice. All participants had to currently work within the field of cybersecurity in the federal government (Ericsson & Charness, 1994; Ericsson & Lehmann, 1996; Maxwell, 2013; Patton, 2002).

Potential participants were initially contacted by phone or email to provide an introduction to both the researcher and the study. For those contacted by email, a standard letter was used (see Appendix A). Subjects who agreed to participate were provided, and signed, an informed consent form (see Appendix B). Informed consent was necessary to protect the rights of the participants and to ensure that they understood that their participation in the study was voluntary. The informed consent form outlined the purpose of the study, possible risks and/or benefits of participating, the voluntary nature of the study, and the participant's right to withdraw from the study at any time.

Data Collection

Data were collected by the researcher using in-depth, open-ended interviews, employing an established interview guide derived directly from the research questions and literature review (see Appendix C). Thirty interviews of federal cybersecurity experts were completed between February 2017 and August 2017.

Interview Approach

Qualitative interviews are useful for drawing detailed information from research subjects (Seidman, 1991). The use of open-ended interview questions gives researchers the flexibility to explore more deeply information shared by participants. Further, open-ended questions increase the probability that viable themes will emerge to help further the understanding of the phenomenon under study.

According to Patton (2002), there are three basic types of open-ended interviews: informal, standardized, and interview-guided. With an informal approach, the interviews have less structure and tend to be more conversational in nature. Under a standardized

approach, a set of structured interview questions is developed and used with each participant. Typically, the standardized approach reduces the risk of researcher bias but offers less flexibility to explore topics or ideas that that may emerge during the interview process.

The interview guide approach offers a compromise between the informal and standardized interview approaches. The researcher develops a guide with a set of predetermined topics to be discussed during the interviews. However, the questions related to each topic can vary between interviews, giving the researcher the flexibility to further probe the answers to questions (Patton, 2002). Given its inherent flexibility, the interview guide approach was selected for this study.

Interview Guide Development

The interview guide was prepared based on the research questions identified as part of this study and the guidelines provided by Patton (2002). The questions included in the guide were designed to deepen the understanding of federal cybersecurity culture. The guide was tested through pilot interviews with two research participants, and modifications were made as appropriate. Pilot testing also allowed the researcher to prepare more effectively for potential challenges in using the interview guide prior to formal implementation. Table 3.1 shows the direct relationship between the interview questions and research questions.

Table 3.1
Relation Between Interview Questions and Research Questions

Interview questions	Primary question	Subquestion 1	2	3	4
1. I am trying to understand how your organization approaches cybersecurity.					
a. Please describe the general nature of the cybersecurity policies at your organization and how they are enforced. What do you consider to be the strengths and weaknesses of your organization's approach to cybersecurity?	X	X	X		
b. How is cybersecurity conveyed to workers or promoted within your organization? If I walked around the organization's working areas, would I see physical things that relate to cybersecurity? What would I see?	X	X	X	X	X
c. Do you follow requirements set by another organization, and do you have any latitude for local modifications?	X	X	X	X	X
d. What role do procedures, training, and technologies play in your organization's approach to cybersecurity?	X	X	X	X	X
e. What challenges do you see with compliance? How do they concern you? How have you become aware of these challenges? If I were to ask employees about their concerns with the approach to cybersecurity, what would they tell me?	X	X	X		
f. Do you monitor cybersecurity performance or compliance? What metrics or tools do you have? Are there tools that would improve network security monitoring?	X	X	X	X	X
g. How are cybersecurity problems resolved in your organization? Can you give an example of a cybersecurity problem and what you learned from it?	X	X	X	X	X
h. If you could make one change to significantly improve your cybersecurity posture not related to hardware, what would it be and why?	X				X
2. I also want to learn about your perception of cybersecurity based on work you do with other federal organizations:					
a. Is there a formal way to learn about problems and share best practices with other federal organizations? Describe how you use this.	X	X	X	X	X
b. What do you know about the approach these organizations take with regard to cybersecurity? Are there standards common to all federal entities to include rules, regulations, policies, procedures, technologies, etc.? From where do these standards originate? Do you see any differences in how other organizations approach compliance? What have you learned from other federal organizations?	X	X	X	X	X
c. Are federal cybersecurity goals and accomplishments formally published? If so, please describe how this is accomplished and what follow-up exists. Do you think this is effective?	X	X	X	X	X
d. Would you do anything differently to improve federal cybersecurity posture across organizations?	X	X	X	X	X
3. In order for me to understand the approach of federal organizations to cybersecurity and challenges therein, is there anything else you would like to tell me or think I should have asked?	X	X	X	X	X

Note. Identified interview questions cover the subquestions directly or indirectly. *Primary question:* What is and what should be cybersecurity culture in U.S. federal organizations? *Subquestion 1:* What are the similarities in cybersecurity culture in U.S. federal organizations? *Subquestion 2:* What are the differences in cybersecurity culture in U.S. federal organizations? *Subquestion 3:* How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations? *Subquestion 4:* How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

Data Collection Procedures

At a minimum, one interview was conducted with each participant. However, as necessary, follow-up interviews were scheduled to explore more deeply, or to clarify, research results. To the extent possible, all interviews were conducted with participants at their designated work sites. However, if necessary, the interview location was changed to accommodate participant needs. In some cases, a phone interview was the only reasonable option for the participant. Each interview lasted no longer than 90 minutes. Data were collected by audio recording and in separate field notes. Participant approval was obtained before any recording was made. If requested, participants were afforded the opportunity to review and approve their interview transcript. In terms of data preservation and security, all electronic files were encrypted and hard-copy records were stored in a secure location accessible only to the researcher.

Data Analysis

Lincoln and Guba (1985) suggested that for a naturalistic, qualitative inquiry, researchers make sense of the data in a manner that maximizes the understanding of the phenomena explored. There are three primary ways to analyze and interpret data: deductive, inductive, and integrative (Miles & Huberman, 1994; Seidman, 1991). This study utilized an inductive approach, analyzing data collected from interviews with federal cybersecurity experts. Findings were developed through inductive interpretation of the data and presented with supporting statements from participants. This should allow readers to make their own interpretations of the research data (Creswell, 2003; Patton, 2002).

Lincoln and Guba (1985) preferred inductive over deductive investigation because it is more likely to result in multiple realities and applicability from the same data. This type of analysis has the potential to make the investigator–respondent interaction explicit, recognizable, and accountable. Further, inductive investigation allows for full description of the setting and greater ease in the transferability of the data to other settings (Lincoln & Guba, 1985).

Content Analysis and Thematic Coding

With an inductive orientation as a foundation, this study utilized Creswell's (2003) data analysis spiral to manage and analyze the data and to generate findings to answer the research questions. Accordingly, the researcher used analytic circles, rather than a fixed linear approach, to derive a meaningful narrative from the data. Data management comprised the first loop in the spiral. Under this loop, the researcher maintained transcripts from interviews in hard copy as well as in backed-up audio computer files. Once the data were organized correctly, the researcher read the transcripts several times, taking notes and simultaneously trying to get a sense of the whole of the interviews before breaking them into parts (Creswell, 2003).

The next phase of Creswell's spiral involved reflecting on the larger ideas discerned from the data and establishing initial categories or groups. This is referred to as the describing, classifying, and interpreting phase of content analysis, during which the researcher starts to organize the data into logical clusters, looking for multiple forms of evidence to support each chosen category. The next step was to discern the general themes emerging from the study. During this stage of the analysis, the data were

organized thematically by question, with the expectation that larger findings would emerge from each theme (Creswell, 2003).

Boyatzis (1998) suggested that thematic analysis provides a way for researchers to observe before they fully understand a phenomenon. The recognition of an important moment precedes encoding, which, in turn, precedes interpretation. He also suggested that a good thematic code captures the qualitative richness of the phenomenon. Further, good codes share three characteristics: a label, a definition, and a description of how the theme occurs.

Verification and Trustworthiness

Significant emphasis was given during this research effort to ensure the study's trustworthiness, to include the credibility, dependability, and transferability of the research results. Lincoln and Guba (1985) stated that transferability is, in a strict sense, impossible in naturalistic studies. They contended that the researcher cannot specify the external validity of an inquiry. The naturalist can only provide a thick, rich description to enable interested parties to reach their own conclusions about whether transfer is a possibility. Lincoln and Guba (1985) did argue that demonstration of trustworthiness and dependability in qualitative analysis is useful as a proxy for transferability and external validity.

Merriam (2009) suggested that research studies must be rigorously conducted to have an effect on theory or practice. Further, research needs to present insights and conclusions that resonate with readers, practitioners, and other researchers. In addition, trustworthiness should be a critical focus for professionals in applied fields because of their intervention in people's lives. Accordingly, several verification and trustworthiness

techniques were employed as part of this research, to include (1) rich description, (2) triangulation, (3) peer review, (4) member checking, and (5) audit trail. The specific approach used in the employment of each verification and trustworthiness technique is detailed below. In addition, a review of the approach used to manage researcher bias is also provided.

Rich description. A rich, thick, detailed description was used to provide readers with sufficient evidence to deem analysis and conclusions credible and to enable assessment of transferability (Merriam, 2009). Rich description is evidenced in the detailed narrative account of the interviews, to include participant quotations, and appropriate use of figures and tables.

Triangulation. Triangulation is a critical element in fostering trustworthiness in studies employing the constructivism–interpretivism paradigm (Merriam, 2009; Ponterotto, 2005). For this exploratory study, triangulation of data collection methods and sources (i.e., interview transcripts and notes) was utilized.

Member checking. The research participants served as a check throughout the analysis process. There was an ongoing dialogue regarding interpretation of the participants' meanings and reality to ensure value in the results. This process included review of interview transcripts and all themes resulting from the research.

Peer review. Two alumni from the George Washington University's Executive Leadership Doctoral Program served as peer reviewers. Their role was to review the research results to ensure validity and trustworthiness. At a minimum, two interview transcripts and related findings (themes) were reviewed by each peer reviewer.

Audit trail. Merriam (2009) stated that an audit trail "describes in detail how data were collected, how categories were derived, and how decisions were made throughout the inquiry" (p. 223). Accordingly, a detailed audit trail was maintained throughout the research process. The audit trail involved a combination of notes and memos for file, regarding key researcher activities, questions, decisions, and resolutions. It is important to note that these documents were not intended to be published, but they could be shared with those interested to explain the research process, analysis, and consistency with related results.

Researcher bias. The aforementioned verification and trustworthiness techniques directly contributed to the ability to manage researcher bias. In addition, I offer the following subjectivity statement to make my potential "biases, dispositions, and assumptions regarding the research" (Merriam, 2009, p. 219) known.

Given my background and education in both organizational culture and information technology, it was difficult for me to resist the desire to draw conclusions based on my understanding and perceptions of the research phenomenon. Accordingly, I took precautions to suspend personal bias and use validated qualitative analysis techniques to develop sound themes and conclusions related to the research phenomenon. This approach to analyzing the research data included the use of available software analytical tools. I also purposely paused after initial analysis and interpretation of the research data in order to consider different explanations and contradicting evidence. My primary goal was to ensure that the analysis and conclusions are credible, truly reflecting the perspectives of the research participants (Merriam, 2009).

Subjectivity Statement

The motivation to pursue this research was largely personal, based on my educational and professional experiences. I have both a master's of business administration and master's of science in information systems technology degrees. Both of these master's degree programs emphasized an ongoing dialogue regarding the current challenges facing management and what could be done to address these challenges. In my opinion, there is no greater challenge facing management today than cybersecurity. The cybersecurity risks faced by both public- and private-sector organizations are immense. Further, a successful cybersecurity attack can be devastating to individuals, organizations, and national security.

As a student in the George Washington University's Executive Leadership Doctoral Program, I have come to fully comprehend the significant role of leadership in establishing—and sometimes breaking down and rebuilding—organizational culture (Schein, 1992). This is certainly true when it comes to combating cybersecurity threats, where it is clear from the literature that it takes a culture of cybersecurity to protect organizations. However, what is missing from the current literature is a consensus on what constitutes organizational cybersecurity culture.

As a current employee of the U.S. federal government, I take very seriously risks that threaten the well-being of our nation. Cybersecurity presents a major risk to the citizens of the United States. Further, federal organizations operate in a constant state of cyberthreats, with malevolent and agile actors constantly posing new threats. Accordingly, I feel compelled to help provide a better understanding of federal cybersecurity culture, to include its significance and ideal characteristics. I sincerely hope

that the results of this research will help federal organizations in their ongoing struggle to establish a stronger posture against both internal and external cyberthreats.

Human Participants and Ethics Precautions

This study was expected to present minimal risk to participants. However, in conducting this dissertation research study, an emphasis was placed on the following three ethical principles (Dillman, 2000):

1. Protecting participants from harm. Efforts were made to ensure that participants in the study were protected from physical or psychological harm.
2. Ensuring confidentiality of research data. Any data collected from or about a respondent was held in confidence. Furthermore, the names of respondents will not be used in any publication that describes the research.
3. Conducting deception-free research. The research was conducted in a manner that did not require respondent deception with regard to research scope or purpose.

The regulation most directly affecting this research pursuit was the National Research Act of 1974, which requires that all research institutions that receive federal funds establish institutional review boards (IRBs). The criteria emphasized throughout this research effort, which are a requirement for approval by IRBs, were as follows (Dillman, 2000):

1. Risks to subjects are minimized.
2. Risks to subjects are reasonable in relation to (a) anticipated benefits, if any, to subjects, and (b) importance of the knowledge that may reasonably be expected to result.
3. Selection of subjects is equitable.

4. Informed consent will be sought from each prospective subject or the subject's legally authorized representative unless this requirement is waived by the IRB.
5. Additional safeguards will be included in the study to protect the rights and welfare of subjects vulnerable to coercion or undue influence.
6. Participants have the right to withdraw from the study at any time without penalty.
7. Where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

CHAPTER 4:

RESULTS

This chapter presents the research results from analysis of the data collected from interviews conducted with 30 federal cybersecurity experts. This chapter is organized into three primary sections. The first section provides a demographic profile of the research participants. The second section details the results of the analysis of the data collected in answering the primary research question, through the exploration of the subquestions. For each subquestion, findings that emerged from the analysis are presented. In addition, select excerpts from the interviews are provided to support these findings. The final section of this chapter provides a summary of the themes identified during analysis of the data collected as part of this research project.

Demographic Profiles of the Participants

This section describes the characteristics of the 30 individuals who participated in the study. It describes the profile of the respondents, to include gender, years of cybersecurity experience, highest level of education completed, any cybersecurity certifications, and current level in their organization. The demographic and professional profile variables collected helped in validating the participants' qualifications for the research and interpreting the results from each research questions.

The 30 individuals interviewed as part of this research represented 23 unique U.S. federal organizations. As stipulated under the requirements for the population of this study, all the participants worked for a U.S. federal organization, and there were no more than two participants from the same organization.

Gender was not equally represented in this study. As shown in Figure 4.1, 80% of the respondents were men.

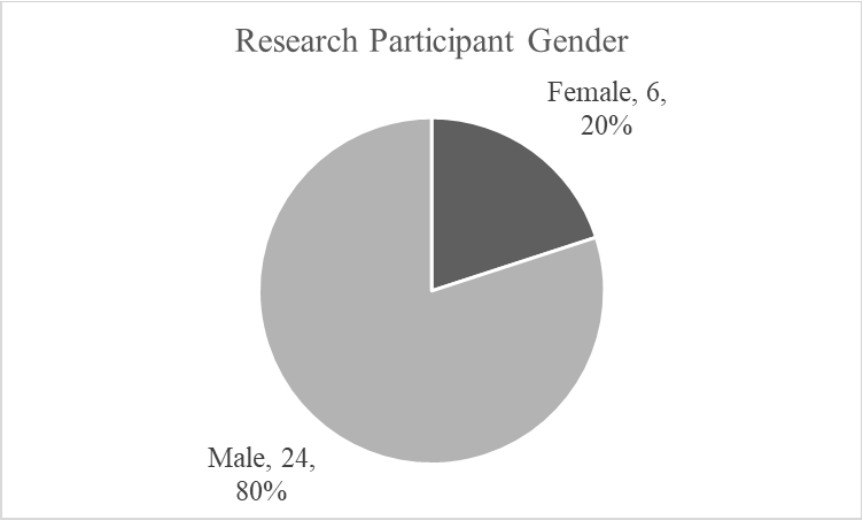

Figure 4.1. Gender of research participants.

The cybersecurity experience for each participant ranged from 11 to 41 years, with 63% of participants having between 16 and 25 years of experience (Figure 4.2).

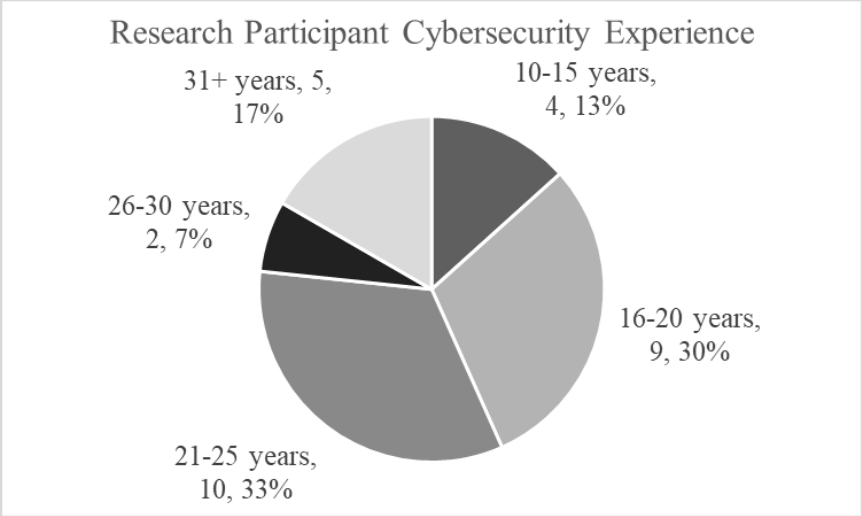

Figure 4.2. Cybersecurity experience of research participants.

The education level of the participants in this study ranged from high school diploma to doctoral degree; 73% of participants indicated that a master's degree was their highest level of education (Figure 4.3).

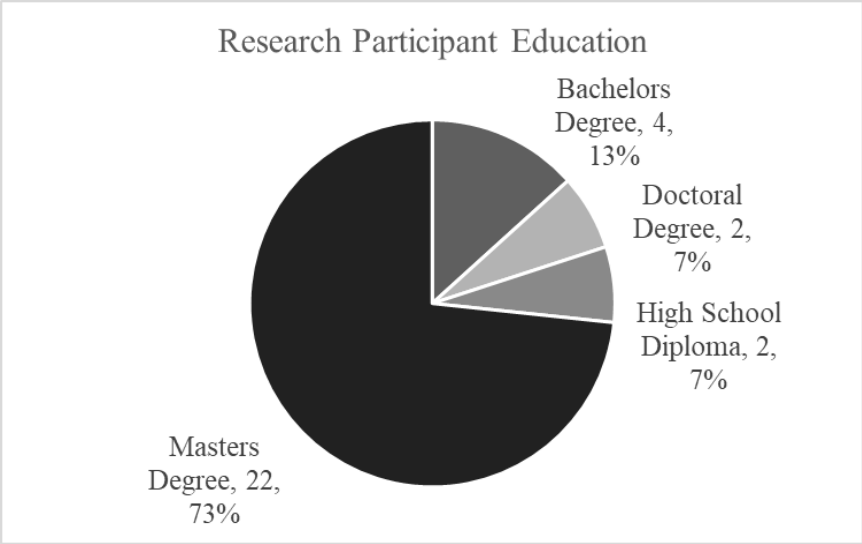

Figure 4.3. Education level of research participants.

Seventy percent of research participants had obtained a major cybersecurity certification (Figure 4.4).

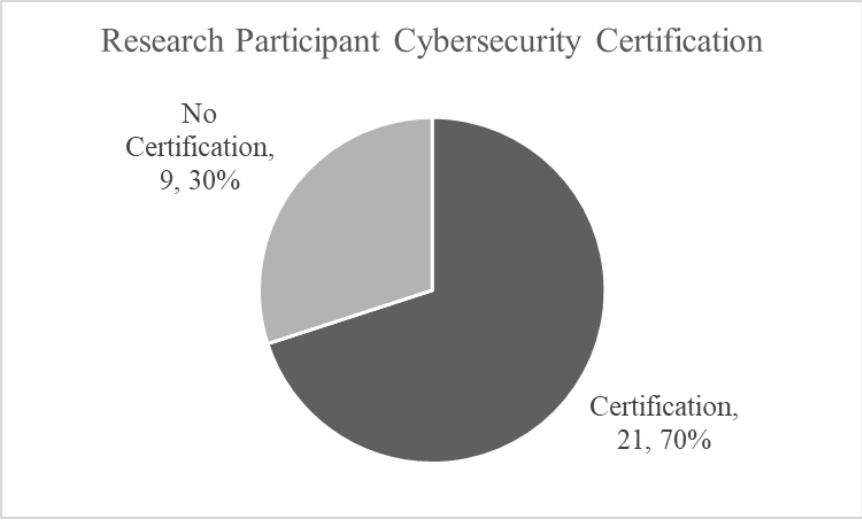

Figure 4.4. Cybersecurity certifications of research participants.

Participants had obtained a wide range of cybersecurity certifications, but the Certified Information Systems Security Professional (CISSP) certification was the most represented (Figure 4.5).

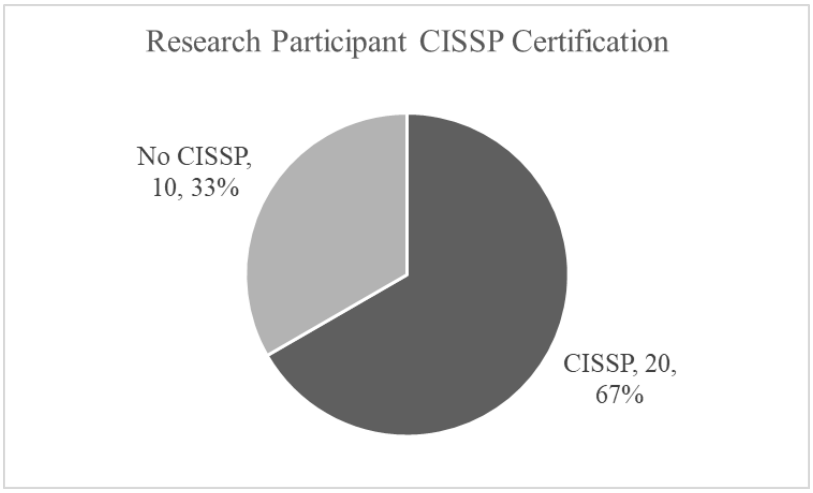

Figure 4.5. CISSP certification of research participants.

With regard to the participants' current level in their organization, 16 participants were federal executives, 10 were supervisors or managers, and 4 were nonsupervisory professional staff (Figure 4.6).

Figure 4.6. Level in organization of research participants.

Interview Results

This section details the results of the analysis of the data collected in answering the primary research question through a detailed exploration of the four subquestions:

RQ: What is and what should be the cybersecurity culture in U.S. federal organizations?

1. What are the similarities in cybersecurity culture in U.S. federal organizations?
2. What are the differences in cybersecurity culture in U.S. federal organizations?
3. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?
4. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

For each subquestion or area of research focus, the findings from the analysis are presented. In addition, select excerpts from the interviews are provided to support these findings. The research findings were limited to those referenced by a majority of the study participants. All findings identified were associated with a minimum of 18 participants. Table 4.1 summarizes the findings identified for each area of research focus. The narrative that follows the table provides the detail for the findings.

Table 4.1
Findings from the Research

Primary research question: What is and what should be the cybersecurity culture in U.S. federal organizations?	
Focus area	Findings
Similarities in cybersecurity culture	1. The importance of cybersecurity is perceived to be understood by most federal employees (24 participants). 2. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures (21 participants). 3. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats (26 participants). 4. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture (27 participants). 5. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns (28 participants). 6. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations (30 participants). 7. Federal cybersecurity culture is primarily a compliance-driven culture (22 participants). 8. Federal organizations face challenges hiring cybersecurity professionals (23 participants). 9. Federal organizations are reluctant to detail the technologies employed in their cybersecurity program (20 participants).
Differences in cybersecurity culture	1. The varying missions of U.S. federal organizations drive different approaches to cybersecurity (25 participants). 2. U.S. federal organizations accept varying levels of cybersecurity risk (26 participants).
Current cybersecurity culture development	1. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations (30 participants). 2. The varying missions of U.S. federal organizations drive different approaches to cybersecurity (25 study participants). 3. Training is a significant element in establishing a cybersecurity culture in U.S. federal organizations (27 participants).
Ideal cybersecurity culture development	1. U.S. federal organizations should focus on cybersecurity risk management and maturity instead of compliance (24 participants). 2. U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information (27 participants). 3. U.S. federal organizations should establish a cybersecurity strategic plan (21 participants). 4. U.S. federal organizations should establish standard operating procedures for cybersecurity (23 participants). 5. U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals (19 participants). 6. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level (21 participants). 7. U.S. federal organizations should adopt more effective methods for cybersecurity training (18 participants).

Similarities in Cybersecurity Culture

This section reveals the perceptions of cybersecurity experts from federal-sector organizations regarding similarities in cybersecurity culture in U.S. federal organizations. Drawn from participant interviews, there were nine primary findings:

1. The importance of cybersecurity is perceived to be understood by most federal employees.
2. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures.
3. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats.
4. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture.
5. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns.
6. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations.
7. Federal cybersecurity culture is primarily a compliance-driven culture.
8. Federal organizations face challenges hiring cybersecurity professionals.
9. Federal organizations are reluctant to detail the technologies employed in their cybersecurity program.

The importance of cybersecurity is perceived to be understood by most federal employees. Twenty-four study participants indicated there is a strong underlying assumption that employees in U.S. federal organizations, at least at a basic level,

understand the importance of cybersecurity. In the words of one participant, "There is a broad understanding by rank-and-file workers regarding the significance of cybersecurity." As stated by another participant, "Generally speaking, there is a decent understanding of the need and the importance of cybersecurity."

As indicated by one study participant through the sharing of an organizational story, federal employees appear to have an inherent understanding of cybersecurity concerns:

> Cybersecurity is culturally innate. People just know that there are certain things that you should and should not do. I'll give you an example: we had an employee that found a thumb drive on the floor of the office garage. The natural instinct for most people is to plug the thumb drive into your computer to try and figure out who owns it. However, she immediately called security and reported the thumb drive she found in the garage. She inherently understood the potential risk: that "bad actors" may have deliberately placed the thumb drive in a public place hoping an employee would plug it into their work computer and infect the network with malware.

The increased awareness and emphasis on the significance of cybersecurity, at all levels of federal organizations, was attributed by many participants to the publicity generated by federal cybersecurity breaches. This increased focus on federal cybersecurity was highlighted succinctly by one study participant:

> I do believe that there is a broad awareness of the importance of cybersecurity. I believe that most federal employees have an appreciation for cybersecurity. As we continue to read about significant breaches in agencies, such as the OPM [Office of Personnel Management] and the ramifications of such breaches, the importance of cybersecurity has been significantly heightened.

A second participant reinforced the broad emphasis on cybersecurity in U.S. federal organizations:

> The good news message is that in federal organizations, at the most senior levels, there is not only attentiveness to cybersecurity but there are specific actions driving the management of risk. However, I also see federal employees acting

> every day towards reducing risk to the organization in the areas that people are assigned across the organization. There's definitely an information technology component to cybersecurity, but the emphasis isn't limited to information technology.

There was even evidence from one study participant that cybersecurity had started to permeate all aspects of federal work:

> Pretty much every project, every program, everything that we do includes cybersecurity. There are very few initiatives that do not include a cybersecurity focus during the early stages of development. It's rare that a project is in the later stages of deployment and all of the sudden someone says, "Have we considered cybersecurity?" Employees understand the importance of cybersecurity.

Another participant went on to describe the passion of federal employees regarding cybersecurity:

> I will say that the passion and the interest of trying to secure federal information systems is there and they are slowly but surely finding ways to address cybersecurity, address the concerns and issues on all levels from—you know the top, where the executives are, all the way down to the system administrators who implement preventative methods.

Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. Despite the belief in a general understanding of the importance of cybersecurity by most federal employees, there was a strong perception, by 21 participants in this study, that federal employees' lack of compliance with cybersecurity policies and procedures presents significant challenges for federal organizations. Employee lack of compliance could be either intentional or unintentional, but the risk remained the same. The concern regarding employee compliance with cybersecurity policies and procedures was summarized concisely by one participant:

> As we know, the weakest link in the cybersecurity chain is the human link. When it comes to cybersecurity, we know employees do bad things, either intentionally

> or unintentionally, and it is a real challenge for organizations. You are never going to be able to completely control human behavior.

As described by some study participants, employees fell under the broad category of "insider threat" and could conduct intentional, or unintentional, acts that threaten a strong cybersecurity posture. In the words of one participant, "Nearly 80% of cybersecurity incidents come from internal sources, insiders, either accidental or intentional." In describing the insider threat problem, another participant stated:

> Most people realize that an authorized insider can do almost as much harm—if not more harm—than someone who has gained unauthorized access from the outside. You can stop 100 adversaries from the outside, but if one insider does something, it could be really harmful and very painful to resolve.

The following is an example provided by one participant regarding an unintended employee insider threat:

> You still have a significant insider threat problem. Like for example, it's my last day at work and I didn't really plan. I want to get my résumé off of my hard drive, and I can't remember where it is, so I dump my entire hard drive onto a USB drive, and I walk out the door with top-secret information, or other types of sensitive data, that I didn't intend to take.

In the words of another study participant, solving the cybersecurity challenges associated with insider threats, or human behavior, is not easy:

> No matter how much information you put out there—to include training, articles, email notices with alerts—you still will have people that continue to do things in an ill-advised or insecure fashion. People continue to do silly things; some are even dangerous, and if I knew how to perfectly resolve the problems with human behavior, I would certainly not be doing what I am doing today—I would have cashed that chip in a long time ago. Maybe it takes implants in employee brains that prevents certain behaviors?

Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats. Twenty-six participants in this study

expressed a deep concern over the constantly changing cybersecurity landscape. In the words of one participant, "We can't execute quickly enough to keep up with the changing landscape that we have." Another participant stated, "We try to educate people continuously because the threat is continuously changing." However, as was noted by the same individual, "I am not sure that our efforts with education will ever keep up with the technology. The changes in technology and related cybersecurity threats are happening so fast that we are constantly chasing the tail." A separate study participant stated:

> The challenge is this is not physics. This is not steady state; what worked 5 years ago or 10 years ago for security doesn't work now. How do you mature the process such that it is much more fluid, much more real time, and is recognizing that you have to always be updating your approach?

One participant described an 18-month cycle of change in information technology, indicating that cybersecurity always seems to lag the changes in technology:

> The problem that we have in cybersecurity is that technology changes, generationally, approximately every 18 months, and cybersecurity always seems to lag behind the change in technology. Cybersecurity is never going to be ahead of the technology game, I don't believe.

One participant discussed in detail the cybersecurity challenges faced with new and emerging approaches to information technology development:

> We're going through a pretty fundamental change in how we're developing software. There's an emphasis on being more agile, or providing business value in shorter periods of time. As part of this emphasis on shorter software development cycle time, there's also a focus on the use of open source code. These changes in development approach require building an entirely new security capability. That's been tough because people I think have the notion that "security is security"—if it works here, we can use it there, right? And it's like well, no, you don't see the same type of security in an airport that you do at a train station or in a private automobile. These are all different environments and different types of operations.
>
> A lot of the work here, especially once you start talking about open source code, the security is very different, and one of the challenges I've had recently is explaining how when I get software from a major vendor, such as Microsoft or

> Adobe or whoever, it's been through a fairly rigorous software assurance process that includes security testing. Microsoft publishes their security testing process, Adobe publishes theirs, etc. When I pull something from an open source, I have zero assurance that security is a consideration or how it is being handled. For example, right now I'm telling my management, we need to spend the money to build up an assurance process to handle what we don't know is there, and that's a tough sell. It's a tough sell because that's not what they were told. They were advised by some consultant to use open source code—it's free, it's cheap. Well, there are reasons for that, you know. There's a reason you would pay for commercial off-the-shelf, versus open source, but you know the discussion of that trade-off is not on the table. The discussion is that we are going to use open source. This change has truly been a cybersecurity challenge.

Participants also described the challenges associated with planning and executing a successful cybersecurity strategy under a state of constant change. In fact, one participant alluded to the fact that cybersecurity vulnerabilities arise at a faster rate than federal organizations can react:

> Cybersecurity vulnerabilities are changing at a rapid pace. Unfortunately, it takes time to figure out what all those weaknesses are. It takes time to implement technical controls. It takes time to write the policy that says what you can and cannot do, and an organization cannot adopt these changes overnight.

Another participant discussed the rapid pace of change and the difficult, if not impossible, task of planning a successful cybersecurity strategy in federal organizations:

> I think there's this constant rat race and it's—everybody is in this like overdrive mode all the time when it comes to cybersecurity. And while the—I mean, we like to plan. There is just never a time to plan, and I think because the speed of technology and then the speed of power to compute it's almost—I mean, it's like—the speed of light—you can't catch your breath because there's an endless amount of cheap, powerful computing power out there used for cybercrimes. For us to humanly try to stay ahead of cybersecurity it's almost—I'm not saying it's impossible, but extremely, extremely challenging. By the time you finish planning something and then, you know, start implementing the plan, the plan is already dated.

Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture. Twenty-seven participants in this study expressed a deep

concern over the impact of limited budgets on the ability to establish a strong federal cybersecurity culture. In the words of one participant, "The biggest gap that still remains is the lack of funding to implement all of the requirements that would, to the greatest extent possible, ensure that federal agencies protect their information technology investments." Another study participant stated, "We simply do not have the funding necessary to obtain the resources required, particularly regarding the pay and training required to keep high-quality personnel." In describing the current state of federal cybersecurity budgets, another participant stated the following:

> No, I don't believe budgets are sufficient or there is full understanding of the impact of cybersecurity mandates on federal agency budgets. For example, we get mandates, such as HSPD-12, the mandatory PIV [personal identity validation] Card deployment, where there was no plus-up in the budget for this. There was significant implementation cost associated with this effort and others like it. The continuous diagnostics and monitoring that are being pushed forward by the DHS [Department of Homeland Security] has significant cost associated with it, but I haven't seen my budget go up to cover these costs.

In looking to the future, one study participant had a bleak view of federal cybersecurity, given budgetary constraints. In particular, this participant did not believe funding was adequate to meet the growing list of federal cybersecurity mandates:

> As we look out over the next several years, there will be a significant hit to budgets related to cybersecurity mandates. The overall cost of operations has gone up considerably, and I am not just referring to personnel, I mean the hardware, software, and infrastructure required to support these mandates. If these are absolute requirements, and budgets don't go up, what do we sacrifice and what are the risks associated with the sacrifices? Most federal agencies have essential functions that, if not performed, can cause grave harm to the nation's overall health.
>
> You can only add so much to the plate. If you are at the buffet table and you don't stop adding to the plate, something is going to fall off. That's exactly where we are with federal cybersecurity budgets. If the mandate is to get more efficient and effective, that's great, but tell us what we are going to stop doing. Much of what we do is legislative driven and we can't change the law. If the money's not there,

> what are we supposed to do? How can we effectively execute our mission? There must be more recognition that cybersecurity mandates don't come free and they certainly don't happen overnight.

There was additional evidence of the frustration associated with trying to meet federal cybersecurity mandates with a limited budget:

> Another thing that also factors into it is budget. You can have your budget cut by 20% and then you're asked to—well, you still need to comply with all mandates, but you don't have the money. Do you fault the person for not complying or do you fault those responsible for not allocating the right amount of money?

Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns. There was evidence from 28 of the interviews conducted that federal acquisition policies and procedures present significant challenges to U.S. federal organizations in their ability to address cybersecurity. A common complaint, which was expressed by several participants, was the frustration with the slow acquisition process in many U.S. federal organizations. One participant expressed this frustration by comparing the speed to the movement of glaciers and indicated that the fast pace of change in cybersecurity naturally demands a faster procurement process:

> The government procurement process is very dated and it's, you know, the opposite of agile [chuckle]; it's, you know, it makes glaciers look fast. You know, cybersecurity is a fast-moving industry, always has been, always will be, and you know the procurement process for buying cybersecurity products and services should be very different from buying office furniture.

A separate study participant echoed the previous participant's frustration with the slow pace of federal procurements and the bad match with cybersecurity:

> The federal procurement process is in general way too slow. We have had a security support contract that took over a year to get to the point that we could get

> the work done. By the time we started the work, the requirements are no longer relevant simply because of the rapid pace of change in cybersecurity.

Another study participant described the frustration with her organization's 120-day procurement cycle and its negative impact on cybersecurity:

> Right now the procurement process we've been given is 120 days for purchasing, making procurements on just about anything. So obviously, if you do planning correctly and so forth, you can plan for that 120 days, but with cybersecurity, it changes every week, so 120 days is a lifetime.

Another common concern expressed by several study participants was the perceived strict nature of federal acquisition policies and procedures. There was a general appreciation for the need to provide fair and open competition. However, the federal acquisition policies were, in many cases, perceived to impede the success of federal cybersecurity programs. In the words of one study participant, "I understand that the FAR [Federal Acquisition Regulation] is there to prevent fraud, waste, and abuse, but the process is too restrictive." From the perspective of another study participant:

> You know, I totally understand the burden we bear in making sure that acquisitions are fair and open, and I work hard to adhere to that. At the same time, in our space there is often a very clear market leader for various products and support. There's a great deal of concern about doing procurements that are, you know, pointing at a single vendor or a single provider even though there is—even when evidence is provided that they are the clear market leader. Even when we do research that indicates that they're the clear market leader, they still want to have full and open competition.

One study participant suggested that forcing competition, particularly when there was a logical tool or service provider, was not good stewardship and, in fact, was counter to the spirit of the federal acquisition policies and procedures:

> We had to pay considerably more—thousands of dollars more—for a second purchase of a software package we were already using, additional licenses, because we were forced to recompete the bid versus buy directly from the vendor

> we had previously purchased the software from. How is this good for federal agencies or taxpayers? Once again, I understand the need to create opportunities and be fair, particularly if it's a new requirement, but this just doesn't make sense to me at a fundamental level. How is this good stewardship?

From the perspective of another participant, there should be exceptions to stated policies and procedures when addressing cybersecurity risks:

> I believe that the federal acquisition rules are created for a good reason, that you don't want undue advantages to large corporations or any abuse, right, but at the same time it has to be balanced where when you have a cybersecurity risk, and the situation needs to be addressed very quickly, you should allow exceptions.

The notion of exceptions to the federal acquisition rules, or a more streamlined process, to more efficiently and effectively meet cybersecurity requirements was a common focus. From the perspective of one participant:

> I think if the federal government came out with some particular standards from the top down that, for cybersecurity specifically, approved you know tools and services that we didn't have to compete to procure it would be ideal. The Department of Homeland Security, under its CDM [Continuous Diagnostics and Mitigation] program, has attempted to establish such a program. However, because of the way the program was deployed, the tools have not been easy to access.

Several study participants also expressed concern with targeted procurements, specifically, that many federal procurements are targeted for small businesses or minority- and woman-owned firms. This concern was not driven from an objection to allowing these targeted businesses to fairly compete for work; rather, there was a genuine concern over the ability of these firms to meet and sustain cybersecurity requirements. Simply stated, they just did not have the resources to compete with larger firms when it came to critical federal cybersecurity requirements. In the words of one participant:

> You have to follow the FAR and the direction of the contracting officer, and you know it could be a smooth or a rocky path towards procurement depending on

> who you're partnering with in contracting. But the FAR is—you know, I mean, that's the FAR. I mean, it's onerous, and it's not easy, and they push you to small business, and that's not always where you're going to find the best solutions, the best cybersecurity solutions. I think that all businesses should be given an opportunity to you know step forward and provide their proposal, and the federal government makes it very difficult to move outside of the small business realm in procuring. I've been involved, I was involved in a cybersecurity procurement, and they were very much pressuring the team to go small business whether they wanted to or not.

One participant went so far as to suggest there were quota systems requiring the use of small or minority-owned businesses:

> There are quota systems, like, oh, we've got to give this much to a small business, oh, we've got to give this much to a minority-owned business type of thing, but the work really requires a unique skill set and experience. There is no way a mom-and-pop business can recruit and retain a highly qualified security professional forever, and if you give a contract—so it's not that like I have not given a contract to small business or some minority-owned business, but I have seen the turnover in the employees and the contractors where it hurts me, right? When somebody leaves, I say: Okay, now where is this position going to be filled; what type of person you are going to fill? If you are not going to give them what industry is paying, you are going to get sub-quality people, or they are going to learn on the job, right; they don't bring the experience or knowledge.

From the perspective of another participant, there was a bias toward small business awards:

> There's definitely a heavy bias towards small business awards. I'm not exactly—I don't particularly have anything against that, but sometimes you do need a larger vendor to support a particular service that smaller vendors just aren't able to provide. That can also be very constraining. There's really—there's literally no requirement for agencies to do that beyond "make your best effort" according to a law. Our agency has for whatever reason taken it to an extreme, and it makes it challenging to work any procurement here because they want to force everything down the small business path.

Another participant stated an understanding of the need to create opportunity, but suggested there was budgetary risk in specifically targeting small businesses and not allowing direct access to larger firms. The argument was that smaller firms were often

used as a pass-through, or access point, for larger firms to win contract awards. Under a pass-through scenario, costs could go up significantly, as fees were paid to both the small and large firms. Below is a direct quotation from the participant:

> The biggest complaint I have heard is that we are so often driven to use small businesses, 8a firms, disadvantaged business, who just can't do the work required. Trust me, I completely understand the need to provide opportunities, but when it comes to cybersecurity, we are taking a real risk by limiting direct access to the very best contractors. Limiting access to the best contractors limits the possibilities of what could be when it comes to federal cybersecurity. I have also witnessed situations where smaller firms are simply used as a pass-through to the bigger firms. Under this scenario, not granting direct access to the bigger firms drives up the budget and, as we already discussed, budgets are limited.

One participant went on to discuss his frustration with the lack of cybersecurity expertise amongst federal procurement personnel and the negative impact this could have on cybersecurity:

> I think another challenge being in the federal space is that the IT acquisition plan or the acquisition plan itself sometimes is so stringent, you can't veer too far from the federal acquisition regulation guidebook. So you have those two entities, acquisition office or division lacking the technical knowledge or the experience and then the FAR. With those two combined make everything—makes everything very challenging, very frustrating to acquire services and equipment. I think the one thing that we all keep going back and discussing is that it would be nice if acquisition would imbed themselves or us with them and both of us work closely and not them on the eleventh floor, we're on the fifth and sixth floor, almost like side by side. I mean if you have questions or if you have, you know, if an acquisition plan isn't sounding the way it needs to sound, you have SMEs [subject matter experts] that are like literally right next door to you. So I think increase in collaboration, and that's all it takes and it's so simple, but we don't seem to get past that. While we like to think that we are communicating, I don't really see that happening all that often.

There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations. All of the interviews conducted revealed that there are common laws and regulations that create the foundation for

cybersecurity culture in U.S. federal organizations. In the words of one participant in the study:

> The strength of the federal cybersecurity approach lies in the fact that we have some guidance that says here is how you should be configuring your systems, here are the things you should mindful of, here are some of the processes that you should follow to ensure that you meet the expected standard.

From the perspective of several individuals interviewed as part of this study, the U.S. federal government's approach to cybersecurity derives directly from the White House and the Office and Management and Budget (OMB). As stated by one participant, "We are driven by everybody else in the federal government, I mean like everybody! You've got OMB and you've got, you know, the whole Executive Office of the President." From the perspective of another study participant:

> It's really driven from the White House and from OMB. Very few organizations are going to come up with their own plans that are not somehow attached to policies driven by the White House and by OMB. So, if they're directives and OMB releases, then they'll do it, but if not, the chances of them being proactive are very low; they can't argue for the money. I mean, this is their shield when they go ask for money from the secretary of their agency is we have to have this for cyber and it's an excuse.

OMB Circular A-130 and the Federal Information Security Modernization Act of 2014 (FISMA) were cited most frequently as the primary sources of legislation concerning U.S. federal cybersecurity. In addition, guidance provided by the National Institute of Standards and Technology (NIST), which is required to be followed under FISMA, was mentioned frequently as establishing the standard approach to cybersecurity in the U.S. federal government. In the words of one study participant, "Being a federal agency, it all stems from A-130, FISMA, and then we have NIST standards and guidelines." As described by another participant, "The big ones, of course, are OMB—

anything they put out we have to follow. We also have FISMA, the Federal Information Security Management Act, which basically says anything NIST puts out is a standard we have to follow." A third study participant went on to say, "We're dictated by mandates that come from the federal government, like OMB A-130, for example. We follow A-130 and we also are bound by FISMA, especially FISMA 2014, to specifically follow NIST guidance."

FISMA was emphasized considerably by many participants as being the primary driver for U.S. federal cybersecurity. In the words of one study participant, "FISMA is the Holy Grail, right, it's at the top of the food chain, and with that then the FISMA law chartered the National Institutes of Science and Technology to write the standards for cybersecurity." In the words of another study participant, "I think the one kind of pinnacle document that recently was issued had to do with the Federal Information Security Modernization Act, which outlined across the entire government the standards for cybersecurity."

In addition, guidance provided by NIST, which is required to be followed under FISMA, was mentioned frequently as establishing the standard for the approach to cybersecurity in the U.S. federal government. In the words of one participant, "We all follow the NIST guidance for implementing cybersecurity, right, especially the 800 series publications." A separate study participant stated, "On the NIST website on cyber, you will find dozens upon dozens upon dozens of cyber-related standards and requirements and just knowledge out there that allows all federal agencies to implement a consistent and comprehensive cyber program."

Several of the federal cybersecurity experts that were interviewed provided a clear description of the relationship between FISMA requirements and NIST guidance. For example, one study participant stated, "The policies in the federal government, across the board, stem from the Federal Information Security Modernization Act. They are further enhanced and informed by guidance and standards that come from the National Institute of Standards and Technology." Another study participant stated the following regarding the relationship between FISMA and NIST:

> FISMA sets forth the federal policy for cybersecurity. FISMA guidance is provided by the National Institute of Standards and Technology, a part of the Department of Commerce, and sets forth the specific guidelines for federal cybersecurity. It provides guidance on all aspects of information technology security: operating systems, infrastructure, telecommunications, and systems development.

A third study participant went on to detail a connection between FISMA, NIST, and OMB reporting with regard to cybersecurity in U.S. federal organizations:

> The federal requirements for cybersecurity all stem from the Federal Information Security Management Act. That act holds the National Institute of Standards and Technology responsible for promulgating the guidance for agencies to follow. So nearly everything we do here, we do because an external organization provided us that guidance and, as is typically done any time you're asked to do something, somebody tests to see that you're actually doing it, and that would be the Office of Management and Budget, who regularly requires quarterly updates and an annual summation of cybersecurity progress in key functional areas.

In addition to referring to the aforementioned laws and regulations, several study participants referenced the Federal Information Technology Acquisition Reform Act (FITARA), passed by Congress during December 2014, which was intended to refine the way the U.S. federal government buys and manages computer technology. Specifically, the intent was to give chief information officers in federal organizations greater control over information technology investments. The ultimate goal was to reduce security risk,

streamline the acquisition process, and eliminate related waste. However, based on the numerous comments from study participants regarding the inefficiencies in the U.S. federal acquisition process, the effectiveness of FITARA with regard to streamlining the acquisition process could be questioned. In the words of one participant, "FITARA has given broader authority to federal organizations in managing IT investment and inherent risks." As was stated by another study participant:

> FITARA is intended as a tool for chief information officers to oversee expenditures on information technology products and services so that they can say, "No, we don't want to do that, that's not a very secure technology or not a very secure capability."

A separate participant alluded to the positive intent of FITARA, but the challenges faced in its implementation:

> FITARA was mandated across the board for all federal agencies to ensure that cybersecurity requirements were baked into the selection process for acquisitions. Furthermore, it required that where there is a shortfall of funding, and funding becomes available for particular information technology investments, that the funding first and foremost is spent to shore up any cybersecurity weaknesses before it is spent on enhanced functionality. FITARA certainly helps! However, it's brand new, so there's still, you know, a catch-up moment for FITARA. The governance model needs to be strengthened to ensure that the requirements of FITARA are actually implemented, but like most new laws, policies, it will need time to be fully successful.

Federal cybersecurity culture is primarily a compliance-driven culture.

Twenty-two of the federal cybersecurity experts interviewed as part of this study indicated that federal cybersecurity culture is primarily a compliance culture. This includes strict adherence with the mandates outlined in OMB Circular A-130 and FISMA. In addition, compliance with the control objectives outlined in NIST guidance is mandated. However, there was a divide amongst the participants regarding the significance of compliance with established federal cybersecurity standards. Some of the

experts interviewed indicated that compliance with standards, such as FISMA requirements and NIST guidelines, was a positive approach for the federal government. In support of compliance, one participant stated, "I'm not one of these guys that say compliance is not important—I think compliance is important. There's a role for compliance in cybersecurity, so it helps. I don't think it hinders. I don't think it can hinder." Another study participant viewed compliance as a positive, equating it to a broad perspective across the federal government that provides focus:

> That's probably one of our strengths, because we're able to show a global view. Often you hear people say, you know, "What gets the light shined on gets attended to." By having that visualization on a global scale to see what's going on, it's very, very helpful to manage security. We have oversight activities, where data is collected and analyzed, that help us to evaluate our posture.

A separate study participant stated that compliance requirements had helped her organization maintain an emphasis on important security controls:

> Compliance is important. I think that recently a shift has occurred to evaluate compliance activities relative to the importance they bring to a security program. As I say that, the organization I work with now, they have focused on the more important compliance controls and increased the frequency of those controls even though it adds costs to the organization while decreasing the frequency associated to those compliance controls that have lesser impact to the overall security posture.

Another participant equated compliance to a needed minimum standard of cybersecurity efficiency:

> I think this gets to a fundamental question about—you know, does compliance equal risk or does risk equal compliance? Everybody loves saying compliance doesn't give you security. I always liken it to the—you know, compliance is designed for the slowest swimmer. Compliance is really designed to say [that] somewhere we need to have an agreed upon kind of minimum as to what we're going to do, and if we don't meet it, we need to have some good reasons why.

One participant used the analogy of a good pilot going through a preflight checklist when describing the importance of cybersecurity compliance in the federal government. Neither the preflight checklist nor cybersecurity compliance guarantees perfection, but both are important for ensuring that important safety/security requirements are not missed:

> I think compliance is important. It is a list. I view it as a list of things that I need to be doing. In cybersecurity, there are hundreds of different things we need to be looking at, and without that—you know, a pilot doesn't get on a plane without a checklist, and that's how I—that's the analogy I like to use. So it's just—it's our checklist to make sure we're applying all the security practices that have been learned and demonstrated to be effective throughout.
>
> If I am flying airplanes that take people from place to place, subject to the compliancy requirements of the FAA flight checklist, does anybody want to get on an airplane where they say the pilot said, "That's not real flying. We don't need that. I know how to fly airplanes"? Does anybody want to fly that plane? I'd rather not. Okay. And it doesn't say that the pilot doesn't have the experience to understand what he or she is doing. It says that this is a means of making sure we didn't accidentally miss something because we're human. Okay. And so compliancy in information security doesn't live unto itself. Compliancy is a means by which we make sure that we didn't forget something and that we can demonstrate that we're doing the things that should result in an assured environment, which should also demonstrate that you should give us more money or manpower in order to continue doing so because we're doing it effectively, right, so all those pieces tie together. I think what's the problem here is that people misunderstand compliance. They see it as an inspection or checklist and not as a means of assuring mission effectiveness.

There was evidence that compliance adds value, but is only a basic standard for security. As was stated by one study participant, "FISMA for me is a minimum compliance issue—if you meet all your FISMA requirements, that's going to be the minimum standard and not the gold standard."

From the perspective of another study participant, having compliance standards certainly adds value, but it does not necessarily equate to having a strong security posture:

> I guess one of the strengths is that they have a pretty comprehensive and systematic risk management framework that is supposed to be applied across agencies. However, because it's comprehensive and systematic, I think at times it can turn into paperwork and compliance exercises rather than exercises that are truly aimed at improving an operational security posture.

In contrast, several study participants had a negative view of federal cybersecurity compliance standards. The consensus from this group was that a focus on compliance standards resulted in a lack of emphasis on real federal cybersecurity concerns. To this point, one participant stated, "People in my organization tend to be focused on compliance rather than the real cybersecurity issues, and, unfortunately, that culture is not unique to my organization or the federal government." From the perspective of another participant, a focus on cybersecurity compliance took away from a focus on good security:

> I have always believed and seen in real life that people have paid more attention to compliance activities, and, in my opinion, you should flip the equation and focus on good security. If you do what is right, compliance should be a byproduct of your effort. You should automatically be compliant if you have paid attention to your risks. So, I've been trying to, everywhere that I have worked, trying to change the culture of the organization where they are asking me questions like: Hey, are we compliant? Do we have this and that? I turn it around and say: Well, those are obviously good questions and we should be compliant, but compliance doesn't automatically mean that you are secure. So, we need to change culture everywhere where people don't just focus on compliance, or bare minimum standard, versus what is required to secure an organization's data and assets.

One participant emphasized that meeting the requirements of the federal cybersecurity compliance "checklist" did not necessarily equate to good security:

> I would say the challenges of cybersecurity in the U.S. government are that it is still on the civilian side pretty much a checklist. You can do everything right in the checklist and still not be secure. For example, OPM prior to its breach were certified that they were secure. They checked the boxes, but that did not mean they were actually secure, and so this is a challenge for cybersecurity, which is if you have an audit checklist, you can do everything on the audit checklist and still

> not be secure, and similarly you can fail an audit checklist, but that does not necessarily mean you aren't secure.

A separate study participant stated that there was too much emphasis on cybersecurity compliance in the federal government. Specifically, the compliance-based approach to cybersecurity in the U.S. federal government did not keep pace with new and emerging cybersecurity threats:

> There is too much emphasis on FISMA compliance. Again, it's a compliance-based thinking that as long as you comply with these standards and requirements, everybody is—life is good, you have addressed everything. In reality, we know that even if I comply with FISMA, I could have a breach tomorrow. Why? Because I may not have addressed the new emerging risks that may not have been identified in FISMA, or the control from the NIST may have missed something that is brand new that when the standard or control was written a year, 2, 3, 5 years ago, it didn't even exist! Every single day something new comes up. Somewhere somebody is still trying to get into my system. It's a 24/7, every-single-day process, and I can't approach it from one-size-fits-all compliance approach.

Another study participant emphasized the risk associated with the perceived gap between compliance and the constant changes in technology:

> Compliance tends to lag the changes in technology. Just because you're compliant doesn't necessarily mean you have the best defenses in a cyber environment. Technology moves at the speed of light, so when it comes to compliance it has to be something that's—that can evolve quickly with the environment, that can keep up with technology.

A group of study participants indicated that federal cybersecurity compliance requirements forced the allocation of scarce resources, both financial and personnel, away from more important mission priorities. As summarized by one participant, complying with cybersecurity mandates led to investment of scarce resources in areas that were not optimized:

> A lot of resources go into complying with cybersecurity mandates. Unfortunately, there's often a much bigger need, a more pressing need from a security perspective that goes unmet because, again, with limited resources you invest it to make the auditors happy rather than doing what was objectively most important for a system or an organization. I think compliance will—it will often drive prioritization or decision making around investments that are not optimized.

Another participant supported the idea that too much money was spent on check-the-box cybersecurity audits that led to a false sense of security:

> We spend so much money on doing check-the-box auditing, and it has become the end all, be all. I understand the importance of it to less well-resourced agencies to better understand the risks, but I mean we spend a lot of time—with internal audits and external audits—that I just don't see how it's beneficial, and honestly some of the FISMA reporting questions, they're really not well defined, and they answer them in a lot of different ways that make it look as though you actually are secure when you're not.

A separate study participant indicated that limited resources forced some organizations to focus solely on checking the box to meet federal cybersecurity mandates versus focusing on real cybersecurity concerns:

> One of the challenges has been between checking the box versus digging into the real security issues. I mean, sometimes all you can do to check the box, because of limited resources. I mean in the federal government you always have limited resources and you constantly have to balance those resources against requirements.

One study participant suggested that successful cybersecurity compliance exercises in federal organizations provided a false sense of overall security, which was not representative of the never-ending journey of federal cybersecurity and could influence senior federal leaders to reallocate resources to other perceived mission priorities:

> The problem that I see with compliance is that it doesn't allow for rapid adaptability or the ability to adopt lessons learned so that you can get to a more innovative stance. My concern is that you could have a fully well-documented

> compliant system that is not ground-truth secure and that if you were just to look at those documents or those scores you would say, "Hey, we're doing pretty well." In reality, that's not representative of the journey of security and in fact could lead executive decision makers to think that you could reallocate resources or that you have sufficient vigilance and will not underscore the fact that cybersecurity is not a destination, it's a never-ending journey, and it requires consistent investment and focus and that if—if you are not proactive on an ongoing basis, the adversaries we are facing will not give you a pass, right, they are relatively relentless either for their own amusement or because they have very precise goals in their attacks.

Another study participant indicated that federal personnel resources could not keep pace with federal cybersecurity compliance requirements and related audits:

> There is so much coming at us, the data crawl, I think at some point people should realize that there is a limit to what organizations can spend time on trying to do the paper exercises or data calls and these compliance activities, right? It cannot be done at the cost of the real mission and cybersecurity work. If you want to do that much compliance work, then you need to allow people to be hired to do just the compliance work. It's like one of the very good observations I have made over the years that you can hire as many auditors as you want, right, and you send them to an organization, and they will audit. They turn every stone upside down. What do you think is going to happen, right? They will find hundreds, thousands, 5,000 things because there are 5,000 auditors looking at these things. Are there 5,000 security people or IT people to take care of those things? No! So that balance has to be there, that you do not do a reverse order where there are more people auditing you and those who have to actually implement it and remediate are a very, very small group. They will have the compliance or audit fatigue, right?

One study participant suggested that he had lost employees due to their dissatisfaction with the heavy burden of federal cybersecurity compliance work:

> One of the bad things that I have heard from people that leave is that there is more to life than this compliance work. If all I'm doing is spending 40 hours a week doing the compliance work, that's not what I signed up for! If I had to do 5 or 10 hours a week, I don't mind, but if you are saying that the majority of my time is spent on compliance, that's not ideal.

Federal organizations face challenges hiring cybersecurity professionals.

Twenty-three of the cybersecurity experts interviewed as part of this study expressed frustration with the hiring practices in the U.S. federal government. In particular, the

hiring process for federal cybersecurity professionals was perceived to be too slow, and the salary structure, in general, was not competitive with the private sector. In describing the challenges faced in hiring cybersecurity professionals in the federal government, one participant summarized the major issues as follows:

> I think it is an artifact of the higher salaries private industry is offering and the lengthy hiring process that people have to go through. Consider, for example, the fact that candidates have to go through background checks. There is a much higher level of due diligence associated with getting hired in the federal space, and that is an absolute impediment to onboarding cyber talent.

Frustration with the slow process for hiring cybersecurity professionals in the federal government was a fervent topic for many study participants. In fact, one participant stated, "The hiring process is ridiculously slow! My average turnaround time to hire an employee, if I were to lose someone today, would probably take between 6 and 9 months." Another study participant stated the following:

> The hiring process is definitely a negative! Hiring almost anybody in the federal government is definitely a big headache compared to how it works in the private sector. It just takes too long. . . . It can be difficult to find good qualified candidates.

A separate study participant described the process as awful. With the slow process, by the time a job offer letter was sent, a prospective employee had already accepted another job offer. This sad reality for the recruitment of federal cybersecurity professionals often forced the organization to restart the recruitment process completely:

> I have to say our hiring process is awful. We take so long to bring on an employee that most of the times candidates remove themselves from the process before we can even give them an offer letter. It takes anywhere from 3 to 5 months to get the letter to them, and by then they've found another job, and we have to start all over again.

One federal cybersecurity expert alluded to the fact that the slow hiring process in the federal government prevented him from hiring cybersecurity professionals in a timely manner. Further, cybersecurity professionals were in high demand, and excellent job candidates would not wait for the time it took to get through the complex federal hiring process:

> Hiring is so unbelievably complex and bad that you can't hire the people when you need them. Cybersecurity is so hot right now. Good candidates are not going to wait for months to give them the decision and offer letter, right? They are going to get multiple offers in a very short time and they will take whatever comes their way. This is definitely an area where I think the federal government needs to revise and improve their approach.

Another study participant elaborated on the notion that cybersecurity professionals are getting multiple job offers and that the slow federal hiring process is not keeping up with the high demand for cybersecurity professionals:

> We have actually lost cybersecurity personnel, made selections and lost them because of certain problems in the hiring process. One of them is just the time, you know, when it takes 4 to 6 months to just hire someone off the bat. I mean, those individuals are getting offers every week, especially your top-tier individuals. We've lost a couple individuals for that reason, just taking so long, even though we made a selection, we notified them, we just didn't get through process and they decided to go elsewhere.

Clear frustration was expressed by many of the federal cybersecurity experts when comparing private-sector and federal hiring practices. Specifically, the speed of private-sector hiring practices was viewed as a positive, and federal hiring practices have failed to keep pace with private-sector hiring standards. As described by one federal cybersecurity expert, there was a considerable gap between private-sector and federal sector hiring time:

> The process itself is interminably long, so a lot of folks who are used to what is in the private sector, which would be a 2 to 3 days, you know, at most a week

> turnaround from initial interview to hire. You know from application, interview, background checks it can take us 6, 10 months to a year to make a job offer.

From the perspective of another research participant, general decision-making within the realm of federal cybersecurity was slow. This was highlighted by the slow process for making hiring decisions in the federal government:

> I find the slowness of making decisions is the most impactful thing within cybersecurity in general. You take our work to a private sector—they're more effective than the government because they are fast to hire, they're fast to make a change. They're fast and on the top of their game, unlike the federal government. For us, yes, you might find the right person, but if she or he is highly qualified, someone else probably interviewed these people and made a more, a better offer than ours, and they're willing to give them the job within 2 weeks. For us it takes forever.

It is important to note that not every federal cybersecurity expert had a negative view of the lengthy hiring process in the federal government. In fact, one participant, while admitting the hiring process was cumbersome, indicated that the process was purposely slow to prevent fraud in the hiring process and to ensure that the right individuals were hired for federal jobs:

> Your standard federal hiring process, which is cumbersome, takes a lot of time, but then, understanding federal governments, you sort of realize that all those things that slowed down the hiring process and make it cumbersome are there to prevent fraud and to ensure that we hire the right people.

It was clear from the interviews conducted that obtaining federal employment can be challenging. For example, employment qualification advantages are often granted for specific groups, such as U.S. veterans, which can limit federal job accessibility to the general population. In addition, hiring freezes, that are either self-imposed, forced through legislation, or due to lack of appropriated funding, further limit federal hiring opportunities. As stated by one individual, "Hiring freezes have negatively impacted our

ability to fill critical positions." These hiring freezes not only place restrictions on new hires, but often limit career growth for federal cybersecurity personnel. In fact, limits on opportunities for career growth were suggested to lead directly to exploration of private-sector careers by federal cybersecurity professionals.

The U.S. federal cybersecurity experts interviewed as part of this study did indicate that federal organizations were afforded a more streamlined hiring process for critical cybersecurity positions, referred to as direct hire authority, which provides for direct hire of a candidate for a federal cybersecurity job without following the normal, lengthy federal hiring process. However, while direct hire authority provides a framework for the faster recruitment of cybersecurity professionals, its use for a targeted position requires a grueling approval process and, as a result, the overall hiring time is still considerably longer when compared to private-sector hiring practices. As described by one federal cybersecurity expert:

> There is direct hire authority, which allows for the hiring of federal cybersecurity professionals in a more streamlined fashion. This is typically much faster than the standard, lengthy bureaucratic hiring process. However, it still is much longer than the private-sector hiring process.

One federal cybersecurity expert described his experience with direct hire authority, in which a candidate can literally be selected directly from the pool of qualified applicants and offered a job. However, due to organizational politics, direct hire authority was rarely used in his organization:

> We do, you know, like every other agency, have direct hiring authority. Literally we can basically point a finger at somebody in a candidate pool and say I want to hire that person without any interaction. That's basically what direct hire authority gets you. However, in our organization we actually tend to follow what the rest of the agency does, even though we are technically free to not do so. They tend to, I guess, frown upon any avoidance of the full process here. So, in order to—you

> know, be good stewards and, you know, partners with the rest of the agency, we follow the more strenuous normal hiring path. We basically play nicely with everyone else.

A federal chief information security officer described the challenges faced in recruiting cybersecurity professionals. He indicated that, despite the availability of direct hire authority, even he was given a hard time when he did not follow the standard federal hiring process:

> Cybersecurity is so hot right now. People are not going to wait for you for months to give them the decision and offer letter, right? They are going to get multiple offers in a very short time and they will take whatever comes their way. This is where I think the federal government needs to revise and improve. Even though there is a direct hire authority, people—CISOs [chief information security officers] like me—are given a hard time when not following the standard hiring process.

A separate study participant acknowledged the flexibility afforded by direct hire authority but noted that every agency did not employ it successfully. This was attributed to a lack of understanding regarding the provision provided by direct hire authority and the objection of human resources to not following the standard federal hiring process:

> Well, we have, within the federal government, we have expanded hiring authorities for cybersecurity professions where we can—I won't so much say "circumvent"—we have expedited activities that allow us to identify and bring cybersecurity talent on in a different way than we can with other career areas. One of the challenges we face with that is understanding fully the latitude that's provided and HR [human resources] being comfortable with the fact that hiring outside of the normal practice doesn't equal increased liability as a result of the hiring mechanisms. So, I'm not sure every agency employs that as successfully as they could.

Similarly, another federal cybersecurity expert stated that his agency used to use direct hire authority more frequently, but concerns expressed by human resources regarding perceived organizational risk had limited its use:

> We used to have a fair amount of direct hire authority, which meant that we could go out and almost grab a résumé and say I want to hire this person. It was almost that easy. And then, of course, HR gets involved and they say: Well, you still need to protect yourself against equal employment opportunity concerns, discrimination, and other things, so we should post the position traditionally, we should collect résumés, we should interview, etc.

The federal cybersecurity experts who participated in this research also indicated that salaries were a concern when hiring cybersecurity professionals. In most cases, the salaries offered for equivalent cybersecurity jobs in the private sector were much higher than could be offered in the federal government. As was stated by one research participant, "With few exceptions, it's hard to be competitive with the private sector, from a salary perspective, when trying to hire quality cybersecurity professionals." Another study participant stated, "I think the salaries are obviously always an issue because the government will never offer the kind of salaries that I think some of the really skilled cybersecurity professionals would get in the private sector."

One study participant stated his belief that federal hiring practices are fair and that the federal government provides job opportunities that are competitive compared to those of the private sector. However, the best cybersecurity professionals would still be able to command higher salaries in the private sector:

> In general, the hiring practices are fair enough. I think the federal government has the ability to hire a lot of talent. My observation is that the best of the best, though, can still demand the higher salaries in the private sector. There is a risk to the federal government that the top 10% to 15% of staff will eventually move off into the private sector because it pays more.

One cybersecurity expert described a time when they had found a great candidate for a job who was a good fit personally and with the mission of the organization, but were unsuccessful hiring the individual due to a private-sector job offer for more money:

> We have had challenges in the hiring space, and I have an example related to salary. We had interviewed a candidate, an excellent candidate, who wrote some highly visible international guidelines relative to cybersecurity. At the end of the day, in spite of a very good personal fit, in spite of a very good fit with the ambitions of the team and the organization, the individual ended up going to the private sector for more money.

One federal cybersecurity expert emphasized the difficulty in attracting and retaining cybersecurity talent. He suggested that even if he brought in new employees who had no cybersecurity skills and trained them himself, there was a strong probability they would eventually leave for a higher-paying job in the private sector:

> The reality is that attracting good cyber talent in a federal workforce is hard. If you bring someone in with no cybersecurity skills, you train them, and once you've trained them in about 3 or 4 years they're going to have some very enticing job offers to go work in private sector as a contractor or go work for a Google or a Facebook, and we're talking massive increases in pay, and so it's very hard to retain that talent.

Another research participant suggested that restrictions on federal salaries directly prohibited competition with private-sector pay for cybersecurity personnel. As a result, federal organizations would frequently rely on costly contractor support for their cybersecurity programs. However, if the federal government could pay a premium for contractor support, why could that funding not be allocated for the recruitment and development of federal cybersecurity personnel? This reallocation of funding was suggested to have the potential to provide significant cost savings:

> The U.S. government can only pay so much—we do have pay scales, and there is not a provision for uniformly paying more for cybersecurity experts. So, most cybersecurity experts that you get, aside from chief information security officer, which have to be a government employee, are usually contractors, and that's not to say they're bad, that's just to say it's costly. Why can't we redirect the contractor dollars to developing federal staff? This has the potential to save taxpayers millions, if not billions, of dollars government-wide.

There was a small minority of participants in this study who felt the salaries offered were competitive. In fact, one study participant agreed that on the surface salaries were higher in the private sector. However, he wondered if that was a fair comparison when considering the value of federal benefits:

> Pay is definitely less competitive on the surface than private sector, and I don't know—well, I don't know if they are just looking at you know straight salary or if they consider all the benefits that tie into being a federal employee versus a private-sector employee. I sense if they viewed the complete package, salary and benefits, the comparison may be more favorable.

Federal organizations are reluctant to detail the technologies employed in their cybersecurity program. Twenty study participants indicated, directly or indirectly, a reluctance to share the specific technologies used in their cybersecurity program. As stated by one study participant, "I cannot discuss the specific technologies we employ because there is a fear the information could be used to socially architect or defense posture." Another study participant stated, "If I share our technologies with anyone, and that information gets in the wrong hands, it could easily be used in planning an attack against us."

Despite the reluctance by the study participants to share the specific details of the technologies employed, it was clear that technology played a significant role in cybersecurity programs across the federal government. In fact, the study participants were willing to indicate the broad uses of technology in federal cybersecurity programs. The use of technology in federal cybersecurity programs included the following:

1. Information technology asset management and loss control: technology used in deploying, operating, securing, maintaining, upgrading, and disposing of information technology assets.

2. Network, system, and physical access control: limiting access to only approved users or groups of employees.
3. Continuous network and system monitoring: tools that identify and report cybersecurity risks on an ongoing basis.
4. Data loss prevention: technologies employed to reduce the risk of loss of sensitive information.
5. Network and system firewalls: technologies designed to prevent unauthorized access to a system or network.
6. Email and web traffic monitoring: technologies that provide insight into employees' email and online activities.
7. Endpoint protection: protecting the network when accessed via remote devices such as laptops or mobile devices.
8. Program communication: technologies used to update employees regarding cybersecurity concerns, to include system and network status.
9. Training programs: technologies used to implement training programs, such as simulated phishing attacks and computer-based training programs.

Differences in Cybersecurity Culture

This section reveals the perceptions of federal cybersecurity experts regarding differences in cybersecurity culture in U.S. federal organizations. Drawn from participant interviews, two primary findings were identified:

1. The varying missions of U.S. federal organizations drive different organizational approaches to cybersecurity.
2. U.S. federal organizations accept varying levels of cybersecurity risk.

The varying missions of U.S. federal organizations drive different organizational approaches to cybersecurity. Twenty-five study participants indicated that the varying missions of U.S. federal organizations drove different organizational approaches to cybersecurity. There were common laws and regulations that provided the foundation for a cybersecurity culture in most U.S. federal organizations. These laws and regulations included OMB Circular A-130, FISMA, and NIST standards. However, it was clear in conducting this research that U.S. federal organizations had varying approaches to implementing these laws and regulations based on their unique mission objectives and interpretation of what was required. In addition, some organizations established organizational-specific cybersecurity policies and procedures. As stated by one study participant, "We have a general set of policies that are common across government, and then we develop unique policies that we develop because of our mission." As noted by another study participant, "We certainly follow the standard federal cybersecurity policies, but we also have other policies that are developed because of our unique mission and nature."

Another study participant indicated an understanding that federal cybersecurity laws and regulations allowed, in some cases, interpretation and modification. However, his organization tried to comply with all the requirements because they were generally good cybersecurity standards. He did indicate that his organization reviewed the fit between federal cybersecurity requirements and the organization's mission objectives and, if needed, would alter the organization's approach to cybersecurity to ensure mission success:

> There is some allowance for interpretation and modification. We have some legal wiggle room on some of these. However, in spirit we generally follow them, these

> requirements and laws and other things, because they're usually pretty good ideas. We do, however, look at our very specific business, or I should say mission objectives, and where we don't think the NIST guidelines, or some of the laws, are in the best interest of the mission, we will sometimes do something else that we find to be more optimal.

One participant stated that both an organization's unique mission and its information technology environment impact the approach to cybersecurity:

> The organizational mission can impact ability to meet requirements, but it's the IT environment that primarily drives modification to cybersecurity requirements. The infrastructure, tools being used—software and hardware that dictate what can be done, or turned on, from a cybersecurity perspective. Not every federal organization has the same IT architecture, which necessitates variety in the approach to cybersecurity.

A separate participant in this study indicated that his organization fully complied with FISMA requirements, which were implemented through adherence with NIST standards, and that he viewed this as a minimum standard for cybersecurity. However, there was an understanding that his organization could go above and beyond the minimum cybersecurity standard, but they certainly could not do less than the minimum:

> So we have to follow, as you know, FISMA requirements. There are several different laws, regulations, and mandates from various places that apply to federal cybersecurity. We have a list of those, and we endeavor to follow them as best we can. So, we produce FISMA reports that are reviewed by OMB and others that grade us across a wide range of IT security controls. Those IT security controls are based on the NIST cybersecurity framework, and, in my mind, those are the minimum controls required to secure an environment. We are free to enhance or go above and beyond those controls, but we can't do less than the minimum as required.

Yet another study participant suggested that some federal organizations did not understand that they could tailor implementation of cybersecurity requirements to better fit the mission of their organization. In some cases, this led to strict implementation of

requirements, which could make security too restrictive and, ultimately, counterproductive for the organization:

> The biggest challenge when it comes to compliance with FISMA compliance is that most federal agencies don't understand that they can tailor the standards and guidelines to meet their agency needs, but they interpret them as mandatory requirements, and just by doing that, they're trying to employ way too many requirements, making security too restrictive and then end up being counterproductive.

Another study participant agreed that federal organizations have some flexibility in deciding whether to adopt FISMA requirements, but that it is not an informal process. Specifically, organizations have to provide a very strong justification for not adopting required standards:

> For the most part, I mean it truly depends on what it is. If it's FISMA, you have to provide a really, really good justification as to why you're not going to do something, and it has to be a rock solid, a really good justification.

One study participant indicated that NIST includes a clause in its standards and guidance that provides federal organizations with great latitude in the manner in which they comply with cybersecurity requirements:

> The policies specific to our agency are contextual, and opportunity exists to modify the approach to policies based on mission requirements. For example, in the NIST standards and guidelines, there is a clause that says while agencies are required to comply with the guidance provided therein, that agencies have great discretion with the manner in which they comply. So, in that guise, we do have the ability to tailor and navigate the policies for our use.

A third study participant indicated that there really is not a great deal of latitude when it comes to complying with OMB, FISMA, and NIST requirements. However, there was acknowledgment that NIST offers some flexibility in implementing its cybersecurity standards, but that changes cannot be made simply for organizational convenience. An

example was provided to highlight when modifying or tailoring a NIST requirement might be appropriate:

> When it comes to things like FISMA, NIST, OMB—OMB there's not a lot of latitude there, you have to do what they require. NIST actually does give you quite a bit of flexibility through scoping and tailoring of the standards. What's important—and NIST is very clear about this—when you're scoping and tailoring, you can't scope something out just because you don't like it. If it's required, you have to address it. So, the example I always give when they ask me, I say well you know scoping is you've built a completely isolated system like in a secure facility and there is no internet connection, period. Well there's no need for a perimeter firewall. You may legitimately scope that out. In an environment that is connected to the internet, not so much!

On the negative side of varying approaches to cybersecurity in U.S. federal organizations, there was evidence that some federal organizations had unilaterally decided to ignore mandates because they were simply perceived to be inconvenient. However, in reality, these controls are necessary to create a secure environment. In fact, not following cybersecurity mandates could result in unnecessary security risk for federal organizations:

> In other instances, requirements are simply ignored because they are inconvenient or unilaterally determined not to apply to the organization. In fact, this has become a serious cultural issue across the government. Organizations, or subsets of the organization, will just decide to ignore cybersecurity requirements that they deem to be too burdensome when, in fact, they are actually necessary to create a secure environment. When sending an email message, with information that is sensitive to national security, how inconvenient is it to secure that message? Ironically, these same individuals would probably take the time to secure their personal information. This is a real cultural problem that federal organizations face.

U.S. federal organizations accept varying levels of cybersecurity risk.

Twenty-six study participants indicated that U.S. federal organizations accept varying levels of cybersecurity risk and that they have the latitude to operate under an accepted level of risk. The level of cybersecurity risk accepted by U.S. federal organizations

varies. In general, the accepted level of risk in an organization must receive approval from the senior cybersecurity executive in the organization, traditionally the chief information officer or chief information security officer.

Federal organizations typically determine the acceptable level of risk based on a detailed assessment of the impact on the organization's mission if the identified risk was remediated immediately versus remediation and/or acceptance of the risk over a longer term. In addition, most federal acceptance of risk evaluations include a short-term and long-term cost benefit analysis of addressing the risk. With most cases of acceptance of risk in federal organizations, a plan of action and milestones (POA&M) is also required. The POA&M typically details the corrective action plan for the identified risk, tasks to be completed, related milestones, resources required, and timeline for completion. One study participant stated the following about the risk acceptance process, "Yes, we live in a world of risk acceptance. It's certainly not ideal, but it's the reality of federal cybersecurity. No large federal organization can operate without some level of risk." A separate study participant stated, "We are a small organization, and, fortunately, it's very rare that we have an acceptance of risk scenario. However, there have been situations where we felt an acceptance of risk was prudent."

In describing the risk acceptance process, one federal chief information officer interviewed as part of this study stated the following:

> No organization can be risk free, so most organizations have a risk acceptance process. However, most federal CISOs and CIOs [chief information officers] definitely don't like to see it used very often. As a result, you see great variation in the acceptance of risk in organizations.

Another study participant described risk acceptance as a positive for the federal government:

> NIST, in their guidance, and in recognition of the reality of the world we live and operate in, has said you can take exception or deviate from standard until there is a better solution, or you move off a platform. That is the goodness of the federal approach to cybersecurity.

In contrast, a federal chief information security officer alluded to the political pressure associated with the risk acceptance process and the associated concerns related to the acceptance of risk:

> There also tend to be exceptions in the federal government called an acceptance of risk. The owner of some business function can put pressure on you, directly and through political connections, to get you to sign a piece of paper and say I accept this risk or I've been made aware of this risk. I don't think the people who generally push these truly understand the magnitude of the risks. They are more concerned with continuing to do business, and when they get hacked later, they blame people like me for not stopping them from operating.

Another study participant stated that there was an abundance of risk acceptance across federal organizations, primarily driven by budgetary constraints, without a full understanding of the potential negative ramifications. From his perspective, most decision makers in federal organizations are mission focused, with cybersecurity being only an afterthought:

> There's so much risk acceptance without necessarily considering the full ramifications that it's very budget driven, and since the primary focus of most people is the mission and that functionality, cybersecurity in many organizations that I've dealt with is an afterthought, at best, and that what happens is a letter justifying why the risk was accepted, and then if it goes from risk to incident or risk to issue, that they just scapegoat it.

From the perspective of one study participant, the real concern is remediating the identified risk, and that risk often goes consciously unaddressed in federal organizations due to time and budgetary constraints:

> The big thing is the amount of time and money that it takes to remediate an issue. Those acceptances typically result in a plan of action of milestones. The real issue

> is the response to the plan of action and milestones. That's where things start to fall apart, because that's where you're saying I need to take some time from the system administrator or a software developer who's got another project going on and go back and fix something that's already deployed and it's—it's a balancing act. You know, how much do you invest in trying to reduce the outstanding risk that you have versus focus on new project? In general, I think you're going to see that there's an awful lot of risk that's being consciously unaddressed. Because you know it's going to take money and time you don't have to fix it.

Current Cybersecurity Culture Development

This section reveals the perceptions of cybersecurity experts from federal sector organizations regarding how U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained. Drawn from participant interviews, three primary findings were identified:

1. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations.
2. The varying missions of U.S. federal organizations drive different organizational approaches to cybersecurity.
3. Training is a significant element in establishing cybersecurity culture in U.S. federal organizations.

There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations. As detailed previously, all 30 U.S. federal cybersecurity experts participating in this study acknowledged that there are common laws and regulations that create the foundation for cybersecurity culture in U.S. federal organizations. These laws and regulations include OMB Circular A-130, FISMA, and NIST standards. U.S. federal organizations have adopted different approaches to

implementing these laws and regulations based on their unique mission objectives and interpretation of what was required.

The varying missions of U.S. federal organizations drive different organizational approaches to cybersecurity. As noted previously, 25 participants indicated that U.S. federal organizations have varying approaches to implementing cybersecurity, based on their unique mission objectives and interpretation of what is required. In addition, some organizations have established organization-specific cybersecurity policies and procedures. The research findings related to the varying approaches used to implement cybersecurity in U.S. federal organizations were detailed previously. Collectively, the common cybersecurity laws and regulations—and organization-specific approaches to cybersecurity—provide the foundation for the development of a cybersecurity culture in U.S. federal organizations.

Training is a significant element in establishing a cybersecurity culture in U.S. federal organizations. Twenty-seven of the U.S. federal cybersecurity experts interviewed as part of this study indicated that employee training plays a significant role in establishing a cybersecurity culture in U.S. federal organizations. In the words of one study participant, "Cybersecurity, at this organization, is promoted and sustained through training, which lets employees know what they can and can't do." As another study participant stated, "Most employees get their cybersecurity policy information from the annual training that they're required to take." A third research participant concurred: "Cybersecurity awareness comes primarily from training and includes online and facilitated classroom training." One U.S. federal cybersecurity expert suggested that the only way to promote good cybersecurity culture is through awareness training:

> The main way to convey it or promote good cybersecurity culture is through security awareness training. We have mandatory security awareness training that all employees have to go through annually. We try to do other small things, with different campaigns, but there is no substitute for actual training.

From the perspective of one expert, humans are the weakest link in the cybersecurity chain. It's very difficult to control human behavior. However, good cybersecurity training frequently leads to enhanced awareness and improved behavior:

> The best we can truly do right now is educate employees and hope it leads to their thinking about and modify behavior. If it leads employees to asking questions, or seeking guidance, if they aren't sure about what is or is not appropriate when it comes to cybersecurity, that's also a plus. However, we know education and training won't stop everything.

Another study participant suggested that 80% or more of cybersecurity incidents in the federal government were the result of insider incidents, so awareness training is extremely important. Good cybersecurity awareness training should increase consciousness of acceptable behavior and let employees know how to identify and report inappropriate behavior:

> Well, awareness, I think, comes from cybersecurity training. There is quite a bit of that—you know, every year you've got to take an hour or two to sort of refresh your awareness, cybersecurity awareness. You know 80% or higher of cybersecurity incidents come from internal, insiders, either accidental or intentional, but there's a fair amount that goes on internally. So, it's extremely important to provide awareness training that explains what's acceptable, good behavior, and the signs of bad behavior and where to report it.

One study participant emphasized the importance of cybersecurity training in his organization and stated that he wanted to do more, but resource constraints limited his ability to expand training opportunities. However, in general he felt training was a cost-effective way to promote a secure workplace:

> Training is a big emphasis in our organization. It's a high priority! I'd like to do more of it. However, we have limited resources to you know do everything we want to do, but in general it's a cost-effective way to help secure your environment.

A separate study participant indicated that training was important, but it was a challenge to keeping cybersecurity training current. In particular, the rapid pace of change in technology and related threats had the potential to limit the effectiveness of training:

> Training plays a significant role in establishing cybersecurity culture. Training helps to establish an understanding of what is and is not acceptable in the workplace. However, I am not sure that training will ever keep up with the technology. The changes in technology, and related cybersecurity threats, are happening so fast that we are constantly chasing the tail when it comes to training.

Another research participant highlighted the fact that his organization has used multiple training methods, including mounting posters with cybersecurity tips, broadcasting email updates to employees, and promoting anti-phishing campaigns. The ultimate goal is to improve the culture of cybersecurity by keeping cybersecurity on the minds of workers:

> We provide training in a number of different ways. We do the standard cybersecurity awareness training every year. I'm sure you're familiar with that. We have posters with cybersecurity tips, we do broadcasts through email to all of our employees, and we run anti-phishing campaigns. I look at anti-phishing campaign as a training and an awareness vehicle. We send out an email, and that email will look like a legitimate business email, but it's a phishing email, and if you click on the link in the email, it will take you to extra training, you know, two or three charts that explain why you shouldn't have done that. The benefit there is that contributes to getting to the workers, telling them what's important, keeping cybersecurity on their frontal lobe, and I think it contributes to improving the culture of cybersecurity.

As described by many study participants, phishing is a form of fraud in which an attacker sends an email that resembles a legitimate personal or business email, with the

intent to distribute malicious code and/or obtain sensitive information (personal or work). With an anti-phishing campaign, an email might be sent to an employee that looks like a legitimate business email, but contains some clues that it is potentially not legitimate (e.g., the sender's email address comes from an unfamiliar domain). Employees who open an attachment included with the anti-phishing email or select an embedded link receive immediate feedback explaining the cybersecurity risk and what to be aware of going forward.

A number of study participants emphasized the importance of going beyond generic cybersecurity awareness training and developing a cybersecurity culture by providing role-based cybersecurity training. Specifically, cybersecurity training should be expanded to cover the specific security concerns of employees' particular jobs and where they sit in the organizational hierarchy. As one study participant stated, "I think it's definitely important to have both general awareness training as well as more specific role-based training." Another study participant noted,

> We do annual training for all users, and we also conduct role-based training. The annual training gives everyone a basic understanding of what they're supposed to do to help keep our systems and environment secure. The role-based or specialized training is intended to educate individuals with, you know, specific roles on their unique responsibilities in terms of cybersecurity.

A separate study participant suggested that he had seen improvement in his organization's approach to cybersecurity training, with a shift from a single generic cybersecurity training course to a training program that included an emphasis on role-based training:

> Training is critical. I have seen an evolution over the past few years where there was one generic cyber training course that everybody had to take, to what exists now, which is a good implementation, hopefully soon to be great, where training

is tailored to the roles staff members play within the organization. So, the role of a privileged user that monitors a network needs different framing of security than the average casual employee of the organization.

Ideal Cybersecurity Culture Development

This section reveals the perceptions of cybersecurity experts from federal-sector organizations regarding how U.S. federal cybersecurity should be developed, demonstrated, and sustained. Drawn from participant interviews, seven primary findings were identified:

1. U.S. federal organizations should focus on cybersecurity risk management and maturity instead of compliance.
2. U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information.
3. U.S. federal organizations should establish a cybersecurity strategic plan.
4. U.S. federal organizations should establish standard operating procedures for cybersecurity.
5. U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals.
6. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level.
7. U.S. federal organizations should adopt more effective methods for cybersecurity training.

U.S. federal organizations should focus on cybersecurity maturity and risk management instead of compliance. There was a strong belief by 24 of the study participants that the current culture of cybersecurity compliance in U.S. federal

organizations is counterproductive. Further, there was a perception that compliance, or adherence to strict guidelines and controls, does not equate with good security. It was believed that U.S. federal organizations would be better served by focusing on improving cybersecurity maturity and risk management. As one study participant observed, "Compliance does not equal security. I think compliance has failed us. Compliance is 5 or 6 years behind the latest cybersecurity threats." A separate study participant stated, "I think that a lot of the compliance work, while good in its intention, has resulted in an overhead that's unwieldy and not productive from a risk reduction perspective." One federal cybersecurity expert suggested that the current culture of cybersecurity compliance negates or minimizes cybersecurity risk management:

> I'd like to mention that this culture of compliance and adherence to rigid controls often negates or minimizes security risk management. Too often cybersecurity professionals think about implementation of controls, avoiding breaches or incidents, when cybersecurity professionals really need to adopt the language of risk management and be able to explain cybersecurity risks to senior leadership in a language that they can understand. We suffer mightily in this area.

One study participant reinforced the notion that the current culture of cybersecurity compliance in the U.S. federal government, and related extensive paperwork, limits the federal community from focusing on cybersecurity risk management:

> We as a cybersecurity organization, and even as part of the larger federal community, spend our time making sure we comply, ensuring we don't have an audit finding, and that's not where we should be focused. We should be focused on making sure applications are not subject to attacks. We should make sure our operating systems are not subject to privilege escalation. Right? We end up spending as an organization too much of our time filling out security plans and the paperwork and making sure we're compliant. We don't focus on the work. We focus on the paperwork to cover ourselves. I think that's the single biggest problem in federal cybersecurity: We say we're managing risk, but we can't be, because the culture doesn't allow for it.

A separate study participant suggested that the U.S. government's compliance-based approach to cybersecurity is the equivalent of a check-the-box approach to cybersecurity and that it is not conducive to reducing cybersecurity risk:

> With respect to compliance, I think one of the challenges is that it is kind of a check-the-box approach to security, and it's not risk based. We have been trained by the audit community to dot every "i" and cross every "t," whether or not there's a risk associated with it. So, I think that a lot of the compliance stuff, while good in its intention, has resulted in an overhead that's unwieldy and not productive from a risk reduction perspective.

One participant in this research emphasized that he would like to see a shift in U.S. federal organizations from a culture of cybersecurity compliance to a culture of cybersecurity maturity:

> I would want to change the role of the federal government and cybersecurity from a culture of compliance to a culture of maturity. By that I mean that right now the government publishes standards. They publish cybersecurity frameworks, scorecards that agencies work hard to achieve the minimum so that they get a green dot instead of a yellow or a red one. Some agencies go further and have very mature scores and success in this area, but I would want to change the culture of compliance to one of a culture of cybersecurity maturity because that implies that organizations aren't focusing on a small set of controls to improve a single score, they're focusing on the broad set of cybersecurity controls described in a framework to improve the whole organization and every area that's operations from supply chain management to the delivery of services in a cybersecurity framework that makes an end-to-end statement about how well they're doing and then cultivate the sharing of those best practices across the sectors where it makes sense to do so. A culture of compliance, as I said before, sometimes drives organizations to check the box to say okay, I've done enough in this area; I'm going to move on to something else.

U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information. Twenty-seven of the research participants stated that there are formal mechanisms for collecting and sharing cybersecurity information across the U.S. federal government. The Department of Homeland Security (DHS) and the OMB were most frequently cited for

collecting and sharing cybersecurity information. For example, DHS was noted for collecting information from U.S. federal organizations regarding cybersecurity breaches. In addition, OMB was identified for collecting information from U.S. federal organizations regarding compliance with cybersecurity laws and regulations. As deemed appropriate, both DHS and OMB disseminated pertinent federal cybersecurity information to U.S. federal organizations. The information shared by DHS and OMB could cover a broad range of federal cybersecurity concerns, to include federal mandates, general federal guidance, federal cybersecurity program maturity reporting, and information concerning imminent cyberthreats. Cyberthreat information generally came from DHS in its capacity as the perceived lead for U.S. federal cybersecurity operations.

Fifteen U.S. federal cybersecurity experts interviewed as part of this study expressed general satisfaction with the formal process of collecting and sharing cybersecurity information across the federal government. In contrast, 24 revealed that there is a perceived deficiency in the sharing of cybersecurity information directly between U.S. federal organizations. As one expert stated, "I would like to see a more collaborative approach to cybersecurity in the federal space. Most federal organizations are tackling cybersecurity on their own, with little to no collaboration between organizations, and that's ineffective on many levels." Another participant stated, "I would like to be able to talk directly with other federal agencies and say: Okay, did you experience this? How did you handle it? How did you do that? Unfortunately, it just doesn't happen that way." Another expert stated the following when discussing the direct sharing of cybersecurity information between federal organizations, "I think this is one of

the places where we fail the most. Every federal organization seems to be recreating the wheel, developing their approach to cybersecurity in isolation."

The interviews also revealed that concerns over the potential for an external perception of weakness in an organization's approach to cybersecurity—and the possible resulting embarrassment—limit the sharing of information between U.S. federal organizations. Below is an excerpt from one of the interviews, which highlights the fear of embarrassment that arises in discussions of cybersecurity concerns with peer organizations:

> There are issues of trust. Nobody wants to come to a table or a meeting and say here's what's wrong with my organization or here's the bad thing that just happened, because there's this feeling of attribution. I know organizations are very reluctant to share cybersecurity vulnerabilities or issues that they're having because they think it will result in being placed on the "wall of shame." That attitude really reduces the cooperation between people who want to get better but don't want to tell the world they are having issues. So, we as cybersecurity professionals need to figure out how to cultivate information sharing on common vulnerabilities and best practices without putting each other on report. We have to get better at that.

Another study participant highlighted the reluctance of federal organizations to share cybersecurity "dirty laundry" because it might lead to organizational embarrassment:

> One of the challenges here is that nobody wants to "air their dirty laundry." Organizations don't necessarily want the world to know that they have been compromised. They don't want to look bad in front of their peers. I am not sure that there is an effective means to share problems and best practices, and, given the possible embarrassment, I am not sure there ever will be. However, in an ideal world there should be a "safe" way to share this type of information.

One study participant suggested that the lack of cybersecurity information sharing between U.S. federal organizations is directly attributable to politics:

> Unfortunately, the people who are practitioners in this area, no one is going to want to share information. I mean, I have good relationships with people at agencies that I will talk with about high-level concerns, but, I mean, the climate in the government is not built to support sharing, and it's—unfortunately, it's kind of an artifact of politics more than anything.

A separate study participant suggested that U.S. federal organizations should reach out to each other for help with cybersecurity concerns, and, with encouragement and understanding that all federal organizations should be focused on the same concerns, it could be done without the threat of repercussion or embarrassment:

> If you don't do things well, you should ask your sister agencies, ask your counterparts how they are doing it, right, without repercussion, without embarrassment, without appearing as though you're weak. I mean it's like any kid, you know, would want to show off if they do something well, and then those that don't do well tend to be a little bit more quiet. You are less likely to ask for help if you are worried about being called out as being weak. I think with encouragement, with just this sense of unity that we're all trying to protect our people, we're all trying to protect our government, we're all trying to protect you know our families and friends, information sharing benefits everyone.

Another study participant emphasized the need to establish a safe environment for U.S. federal organizations to share cybersecurity information, the timely sharing of which could avert a national cybersecurity concern:

> I think we need to create an environment that allows people to share failures without reprisal. I think so many of the things that have gone wrong in cybersecurity—people knew about them early enough to help others. I always joke, if I am hearing about it today, it probably happened 2 to 3 weeks ago. Why should we allow pride to get in the way of doing what is best for our country? Sharing a failure today could save the country from a larger-scale disaster tomorrow.

One study participant emphasized that, when it comes to cybersecurity, U.S. federal organizations are stronger when they are working together:

> One of the prevailing themes is that we're stronger when we're all working together, and so I'm starting to see some of those barriers come down. I'm

> starting to see intragovernment sharing of information, of tools and of techniques, and I'm encouraged when I see it. I'm discouraged when I still see people are trying to isolate it and go their own way.

Another study participant suggested that U.S. federal organizations should not be reinventing the wheel when it comes to cybersecurity:

> There's no sense in reinventing the wheel. If something is working in the federal government, we should be leveraging that and reusing it. If there's a technology out there that an organization is using that is blowing the doors off everybody, then we should all be made aware of it and move toward use of that technology.

A separate study participant suggested that he would like to see more sharing between U.S. federal organizations regarding cybersecurity philosophy, policy, and working or technical approaches:

> I would have some kind of formal sharing at two levels. One, policy and philosophy—actually let me reverse that. Philosophy and policy because without a philosophy there, you can't get to policy. You have to first decide what's important. Once you know what's important, then you can write policy and procedures that reflect what you've decided is important, and that's not easy to do. Anybody who thinks that's trivial is wrong, in my opinion. Number two, there has to be some kind of formal way to share information at more of a working or technology level.

Similarly, another study participant stated a desire to see greater exchange of ideas between U.S. federal organizations, particularly cybersecurity policy development:

> I would like to see more exchange of ideas: Hey, who does this? Hey, which vendor works well? Who has this policy? You know, we all create policies, right, security policies? How is my policy any different from [another agency]; why is that not shared? Policy templates, why is that not shared? Aren't we all working for Uncle Sam?

Several of the study participants suggested that there were some informal mechanisms for the direct sharing of information between U.S. federal organizations, such as lunch meetings and working groups, but that these mechanisms were not

inclusive of all U.S. federal organizations and, ultimately, were not terribly effective. In the words of one study participant:

> There are informal mechanisms for sharing cybersecurity information between agencies. I know there is a group of federal CISOs that get together every month to discuss concerns. In addition, there are working groups that are established to address specific concerns. However, while these groups are certainly a step in the right direction, they certainly don't involve all agencies, and I don't believe they are overly effective. There needs to be a better way for all agencies to benefit from information sharing.

U.S. federal organizations should establish a cybersecurity strategic plan. Twenty-one of the research participants indicated that U.S. federal organizations should establish a cybersecurity strategic plan. Such a plan was perceived as essential for outlining the short- and long-term cybersecurity strategy for federal organizations. The period of time covered by a strategic plan, as identified by the research participants, ranged from 1 to 7 years. In addition, given the constant change in the federal cybersecurity landscape, study participants noted that strategic plans should be updated regularly to reflect changes in priorities. As described by one study participant, cybersecurity should be incorporated in every aspect of U.S. federal organizations, and a cybersecurity strategic plan is essential for this focus:

> Cybersecurity should be incorporated in the very fabric of everything you are doing, but we are not there today. It's important that this is a strategic focus for every organization. Having a cybersecurity strategic plan is an important part of this focus. So, yes, I believe it's very important for federal organizations to have a cybersecurity plan.

The cybersecurity strategic plan was viewed as critical in justifying the allocation of resources (financial and personnel) for cybersecurity initiatives. As one research participant said, a strategic plan helps to gain support for current and future cybersecurity investments:

> I think you should have a plan as to what you're going to invest in now and in the future. It should provide a layered view of the future of cybersecurity. You want to have a plan for the future, you know, in terms of what investments you want to make, you want to make it cogent, you want to be able then to present it to your CFOs [chief financial officers] and your CIOs [chief information officers] so that they understand it and that they can support it.

In the words of a separate study participant, a cybersecurity strategic plan provides a framework for prioritizing work in the face of limited resources:

> The plan provides a framework for prioritization of cybersecurity work. There is an understanding that resources are limited and you can't do everything. What are you going to do and what are you not going to do? And those prioritizations are not always done well without a plan. You may do—you may have 20 things you want to accomplish, but if you did these other five instead of those 20, it might be much more effective from a security posture perspective because of either—because of the effectiveness of these particular investments or because of the threats that you're facing or because of the—you know, compensating controls or other security that's inherited from other parts of your infrastructure. So, it's a complicated thing, and if you don't have a good basis for prioritization, it's easy to spend resources on things that are just not the most important things.

One study participant suggested that a cybersecurity strategic plan would help to show how cybersecurity investments contribute value to the organization, which helps in cultivating support for resources:

> I think it's absolutely critical to have a cybersecurity strategic plan, because if you don't have that, you can't show how you're contributing value year over year in meeting those goals that you established. No one is going to want to give you money or support to do anything. They're going to look at you and see you don't have a plan and if your results are not measurable, your support will evaporate. I think it's got to be done. I mean it's crucial. If you don't have a plan you are going to be fumbling in the dark without support.

From the perspective of another study participant, a cybersecurity strategic plan would help to establish accountability across the organization in reaching cybersecurity goals. In fact, it was suggested that some goals be incorporated in employee performance plans, creating a level of individual accountability for accomplishing goals:

> Well, I absolutely think that a plan is essential because the strategy discussions that take place in the development of the plan [create] a vision for the organization for cybersecurity. The most effective cybersecurity strategic plans that I've been involved with the development of have not only security professionals, but the involvement of the business, the people who'd be subject to the plan or required to follow it. That business involvement makes the cybersecurity strategic plan actionable so that it doesn't become shelfware. We have one here; it's open and available on people's desks. We constantly refer to it in our team meetings, and maybe most importantly some of the goals in the strategic plan are actually implemented in people's performance plans, so you're held to a certain level of accountability for accomplishing goals.

One U.S. federal cybersecurity expert suggested that having a cybersecurity strategic plan is important in detailing important goals and expected outcomes. However, the plan does not necessarily need to be standalone, but should, at a minimum, be a significant part of the overall information technology plan for the organization:

> I think it's important to have a cybersecurity plan. I mean, you want to have goals, some objectives, and measure outcomes. It's always easier to do that when you have a plan versus when you don't, so yes, I think it's very important. Whether it's a cybersecurity strategic plan or significant portion of your IT strategic plan, I think a cybersecurity strategic plan is essential. It's important to know where you are, where you want to be, what the gaps are between the current state and your desired state, and then a plan to get there. It helps you figure out what kind of resources you need and how much time you need.

U.S. federal organizations should establish standard operating procedures for cybersecurity. In addition to a cybersecurity strategic plan, 23 of the 30 U.S. federal cybersecurity experts indicated that the use of standard operating procedures is essential for ensuring an efficient and effective cybersecurity program in U.S. federal organizations. In particular, standard operating procedures help establish consistency and reliability in addressing cybersecurity concerns. It was also suggested that standard operating procedures help organizations to identify and address cybersecurity concerns more quickly. The speed with which organizations identify and resolve cybersecurity

incidents was highlighted as a key metric in measuring the success of federal cybersecurity programs. As one study participant explained, standard operating procedures are critical for establishing a strong cybersecurity posture, and organizations that do not have them tend to struggle with cybersecurity:

> Well, operating procedures are critical to maintaining a strong cybersecurity posture. Operating procedures, workflows, processes that people follow in their day-to-day execution of their duties must have cybersecurity components built in for the overall cybersecurity program to be effective—everything from clean desk initiatives to locking your screen when you walk away to using complex passwords and using separate passwords for home and work access. Those, all the workflows, the actual things that people do as a part of their job, day to day, need to have elements of cybersecurity built in so that they can be successful, and they don't have to shift gears or alter behavior between home and work. So, I think most mature organizations have operating procedures with cyber built in; organizations struggle when they don't.

A separate study participant suggested that cybersecurity standard operating procedures play a critical role because they define what employees are supposed to do. However, organizations should make sure that standard operating procedures are being used effectively. In some cases, standard operating procedures are developed that employees do not use—or know about:

> I think they play a critical role because they clearly define what people are supposed to do and how they do it, but I think that the biggest challenge with, again, work and operating—standard operating procedures or any kind of document at that level—is to make sure that it reflects what needs to be done and what's being done, and at the same time that what's being done—it's that maturity metric, right, that you have SOPs [standard operating procedures] that work, that are relevant, and that are used by employees. You shouldn't just have SOPs for the sake of having SOPs that people don't use or people don't even know they exist.

Another study participant indicated that cybersecurity standard operating procedures are critical, and, absent their existence, essential cybersecurity work probably would not be done:

> Well, I think operating procedures critical. So, for example, I mean, operating procedures, desk guides, if you will, procedures on how, you know—you know, from the data center physical security and signing into a data to how you're going to incident response—because if it isn't written down as a policy or procedure, or something of that nature, it's probably not going to get done.

One study participant suggested that the current culture of cybersecurity in the U.S. federal government necessitates crisp operating procedures. Specifically, federal cybersecurity staff understand the ramifications if they make a mistake, and procedures help them to operate effectively and reduce risk:

> The culture demands—and the employees want—very crisp operating procedures to follow. In today's world where there is—especially for cyber staff—a great appreciation for what can happen if the implementation is not done to perfection, demands that very crisp and comprehensive operating procedures are being defined and given to them such that they can execute well and avoid risk and the consequences falling on their shoulders.

Another study participant suggested that standard operating procedures are essential for establishing a strong security posture in the U.S. federal government. In addition, it would be ideal, although not necessarily possible, to have standard operating procedures to cover every cybersecurity scenario:

> SOPs are absolutely essential in maintaining a security posture. I mean, if—it's one of the first things I ask people—and I mean what are your SOPs for each of the following circumstances? If the answer is, "Well, I don't know. I have this tool to do it," you're like, "Okay, that's not a good answer." You have to have a standard operating procedure to deal with almost—I say "almost" because you could never do all, but *almost* every circumstance that you run into.

A separate study participant suggested that standard operating procedures are helpful in the sense that they establish a standard approach that reduces the risk of missing something important:

> Operating procedures help out in general, you know, through establishing standards, to standardize the approach to cybersecurity. We don't want to risk

> missing something important because we are operating from seat of our pants. There is way too much at risk!

One U.S. federal cybersecurity expert suggested that standard operating procedures are important to ensure repeatable success:

> Without procedures you would never be able to make anything repeatable, and it would become ineffective. So, procedures are very important at night when certain actions are required. We have procedures that have been preapproved by our leadership such that we could take certain actions knowing that it's already been approved, which makes things happen a lot quicker. So, procedures are critical for repeatable success.

Another participant expert suggested that standard operating procedures play an important role in cybersecurity, whether it is a federal or nonfederal organization, providing guidance regarding how to operate or respond when something happens. U.S. federal organizations have varying levels of maturity when it comes to standard operating procedures, but there has been marked improvement over time. For example, it was suggested that most, if not all, federal organization now have a standard operating procedure to deal with a breach of personally identifiable information. This certainly was not always the case in the U.S. federal government, and 5 or 6 years ago, most organizations probably did not have a standard operating procedure, but the increase in personally identifiable information breaches across the federal government has resulted in most organizations establishing a breach response plan. One participant described this at length:

> I think in theory they would play the same role they do in nonfederal agencies. It's when something happens, standard operating procedures should tell you what to do, how to respond. I think different agencies have different levels of maturity when it comes to how complete and comprehensive their standard operating procedures are, whether they exist and how robust they are. Sometimes you'll have situations where there should be but there isn't a standard operating procedure to deal with it. So, for example, now most agencies have a PII

> [personally identifiable information] breach response plan, which is enacted if there's ever a breach of personal identifiable information at the agency, but if you go back, say, I don't know, 5 or 6 years ago, most agencies didn't have that kind of plan, and then there were some big—within the federal government—some big PII breaches, and people didn't know what to do. They were caught off guard, and it became very, not just embarrassing, but people just didn't know . . . do we do credit reporting or not, do we identify affected people or not? There were no standard procedures for that kind of thing. So, I think the government is getting more mature with those types of things, but there's—there's room for improvement.

A different research participant remarked that in a maturity model for cybersecurity, if your program is truly mature, it is consistent. Not every U.S. federal organization has reached this level of cybersecurity maturity, but to get there agencies must have strong cybersecurity operating procedures:

> There's a maturity model where if your program is really mature it's repeatable, it's consistent; you have documentation throughout that people can follow, right? So, follow the procedure, and you should come up with consistent results. Not everybody is there, but to get there you have to have strong procedures.

One research participant suggested that within U.S. federal cybersecurity operations, incident response is an essential standard operating procedure. When an incident occurs, emotions elevate, and people tend not to think or operate rationally. As a result, it is much safer to access the plan and follow the established cybersecurity incident response plan. In addition, it helps to test response procedures, with some regularity, to ensure effectiveness in the event of an actual incident:

> Within operations and infrastructure, the two areas where the procedures are absolutely critical—and we do test this routinely—is on the contingency planning for disaster recovery and for incident response. Because when a crisis hits, emotions kick in, and people don't think what would a rational person do because they're not rational at the time. It's grab the binder, kick it open to the sheet, follow the list. And so we test twice a year for that, and it's great because it's always random, and so we'll just pick up the phone on a random day and say this is random, an incident response test, here's the situation . . . go! And we watch them perform.

Similarly, another study participant identified incident response as the most important standard operating procedure:

> From a procedure perspective, definitely incident response is number one. How do you handle incidents? How do you—first of all, how do you define those incidents? How do you handle them, and what are the rules and responsibilities? What are people supposed to be doing? Those are critical because someone can pick up the phone and call in an incident. Someone can call today and say: Hey, I just noticed something. Is this all right? You need someone to handle that. They need to know: What do you do? Who do you notify? And that's why incident response procedures are most important.

One research participant acknowledged that standard operating procedures help to create needed consistency in U.S. federal cybersecurity. However, on the negative side, procedures tend not to be very agile, which presents risk concerning the ability of organizations to respond to constantly changing threats:

> The role that procedures play in cybersecurity for my organization is very important because security personnel are not always independently capable of responding to issues. Following standard operating procedures ensures a consistent response. The downside to requiring formal documented procedures is that they are not very agile or adaptable to rapidly changing cyberthreats.

Yet another research participant acknowledged the importance of standard operating procedures to technical staff. However, he emphasized that the greatest organizational value comes from the use of standard operating procedures by nontechnical staff, who leverage the procedures for a broad range of cybersecurity concerns, which is perceived to have a more significant impact in lowering risk:

> It's funny because especially as a young man starting out in this field, I used to think: Ah, these procedures, you know, they're step-by-step so the operations folks know what to do and they don't make mistakes. Actually, the biggest value we get out of operating procedures is helping our end users, who may not be technologists, understand how to innately use secure technology. And so things like here's how you encrypt an email, things like here's how you encrypt a mobile media device, here's how you report an incident, here's how you use a VPN [virtual private network] with a PIV [personal identity validation] card. Getting

> that information out into the hands of the users has done more to lower the level of risk in this organization than any of the procedures we've written for, say, operations folks or procedural folks.

Finally, one U.S. federal cybersecurity expert encouraged others in the federal space to develop standard operating procedures for cybersecurity. He admitted that they could be difficult to develop, but good standards definitely provide great benefit in the long run:

> We definitely have a lot of SOPs that have been done for cybersecurity, covering a multitude of concerns, which helps to ensure we handle cybersecurity the right way. So, they have definitely helped out tremendously. It's not always easy to develop SOPs, but it definitely benefits you in the long run, so put the time in to develop good SOPs.

U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals. As was noted previously, U.S. federal organizations have faced great challenges in the hiring of cybersecurity professionals. As a result, it was not surprising that 19 participants called for change in the way the U.S. federal government recruits cybersecurity professionals. As one U.S. federal chief information security officer summarized, the ability to hire the staff he needs was the number one concern, and the process of hiring in the federal government was extremely frustrating. He also noted that his workforce was truly his only appreciating asset. Tools and procedures would break down over time, but employees could improve over time:

> The ability to hire the staff I need, that is the number one thing. Tools I can get. Even money I can usually get. It's—the times I've been hamstrung by the federal hiring process and the constraints around my workforce, it's just infuriating, and, you know, people are the only asset I have that will actually appreciate over time—they get better over time. My tools don't. Oftentimes policies, procedures break down and have to be reconstructed, but my people, they can get better over time with care and nurturing. And it's—I can't get 'em fast enough and I can't keep 'em long enough.

Another professional suggested that the problem was not the hiring process but the fact that the U.S. government cannot compete with private-sector salaries:

> It's not because the hiring practices are slowing us down. It's because of the offers in the private sector. I can tell you that the government as a whole has struggled to attract, train, and retain qualified cyber talent because we get somebody in the door, we train them up, we give them a few years of experience, and they get an offer from a private firm or contractor that's twice what the government can pay them.

A separate research participant suggested that it was hard to compete with the private sector for employees when your biggest selling point was work-life balance:

> It's hard enough to find somebody when my biggest selling point is that I can give you a tremendous work-life balance. I can make sure you're going to work 40 hours a week. I'm going to make sure that you're going to have telework when you need it. I'm going to give you great training and career advancement, to the extent I can. That's about the only negotiation I have! I can't compete with the private sector on money! I can't pay for things like their certification, their annual fees for that, and so it's really hard to attract the talent you need.

Several study participants expressed frustration with the general schedule (GS) pay scale, which is the predominant pay scale within the U.S. federal government. The GS pay scale was perceived in general to establish low employee salaries when compared to the private sector, and, in particular, these salaries were certainly not adequate to attract cybersecurity professionals to federal work. One study participant suggested that U.S. federal cybersecurity professionals should get a salary commensurate with market demand. Unfortunately, under the GS pay scale, U.S. federal employees of the same grade, regardless of profession, are paid the same:

> If you're a GS-14 accountant or a GS-14 HR person, you get paid the same as if you're a GS-14 cybersecurity expert, even though from a—you know, just a workforce market perspective, it is worth a lot more. It's hard to get them to come into the federal government at all because they usually can—good ones—can earn more money working in the private sector because the government just doesn't pay at a commensurate level, so it's a challenge.

A separate study participant suggested that the U.S. federal government may want to consider broad adoption of pay bands for cybersecurity jobs. Pay bands have been used successfully in some U.S. federal organizations and can provide greater flexibility in salaries offered to employees:

> The last two agencies I worked for, in particular, are not like other agencies. Their pay scale is very different. So, a typical GS scale, yes, there's definitely pay issues, right. You can go out in the commercial industry and make a lot of money, being paid commercially, but the two agencies that I've worked for have a wider banding scale. These agencies have more latitude in pay and can sometimes pay more money than jobs at a similar type of level than typical GS scale agencies. This definitely helps in attracting and retaining talent. Broadening the pay band and creating pay flexibility for cybersecurity professionals should be considered across the federal space.

Another research participant said that he had considered the use of retention bonuses, which are allowed in his organization, to retain cybersecurity staff. However, the bureaucratic process involved in getting a retention bonus approved limits its effectiveness. Further, even with a retention bonus, cybersecurity employees tend to leave eventually anyway:

> Once you've got it, you've got the talent, you're lucky to keep it for a year or 2 years. And going through the process of even trying to say: Well, can I offer a retention bonus? Well, yes, you can, but as a manager that's probably going to take me between 40 and 60 hours to go through the approvals, the presentations, the justifications, etc., to say this person is worth it, and then if I do a year or two years, I lose them anyway. So, it's a really challenging space to be in.

Given the perception that the U.S. government would never be able to compete with salaries offered cybersecurity professionals in the private sector, there was a call for other motivators for public service. One study participant suggested the motivation might be opportunity or exposure to something not offered in the private sector:

> I don't think we're going to get to the point where we will get top-notch cybersecurity experts at the salaries that we—it will not be salary driven. It may

> be a different motivation for them to come to the government, like unique opportunities or exposure, but on a continuous basis I don't see the salaries catching up.

Another study participant suggested that job security, which was believed to be afforded most employees in the U.S. federal government, might be a motivation for some cybersecurity professionals:

> You know people can make more money in the private sector. You know the government—the public sector—is going to appeal to a certain kind of person, you know, a person who is looking for certain things that the government offers, [like] job security, long-term employment, stability. . . . If you're in cybersecurity and you're looking for money, then the federal government may not be the best place for you, but if—not everybody is motivated by money.

A different study participant stated that public service might motivate cybersecurity professionals to seek employment in the U.S. federal government:

> So, budgetary constraints definitely cause cybersecurity issues. On one part, from a financial perspective, we're not competitive with market rates for cyber professionals. So, typically the best and brightest are not looking for federal positions unless they have some sort of unfulfilled yearning to serve in the public community.

One U.S. federal cybersecurity expert recommended looking for cybersecurity professionals with great loyalty to the country. Such individuals were believed to be more likely to place less emphasis on monetary demands and to focus more on public service:

> When it comes to getting the best and the brightest, it's difficult to bring them on board if you just take a look at it monetarily. However, if you take a look at whether they truly care for the country, have a strong loyalty to the country, we find that some individuals are willing to give up the monetary demands out of loyalty for their country.

Similarly, another study participant emphasized that work in the U.S. federal government might be ideal for those cybersecurity professionals looking to serve their country and work in a more stable environment:

> I know that the commercial world has more flexibility when it comes to salary, and, therefore, if it becomes a bidding war, then the resources that are the most in demand are more likely to be in the commercial space than they will be in the federal government space. So, if someone has a personal motivation, if they want to either serve their country or stay in government work because they feel like it may be more stable and reduce their own personal risk, those would be the things that would motivate people to work for the government and put up with a lower salary, if you would.

A separate study participant suggested that rigid employment restrictions were limiting the ability of the U.S. federal government to recruit an effective cybersecurity workforce:

> You want these white-collar, clean people, that have a certain track record of education. You can't hire the people that you need because you have these ridiculous rules. It's a different world today! It's a different workforce! You won't be able to hire the people needed until you break the mold as to what you think you should be hiring. Do you think other countries have these absurd hiring restrictions? No, they hire the people needed to perform the work.

One study participant professed that the cybersecurity work in the U.S. federal government is appealing. Unfortunately, there is a stigma associated with working in the federal government, which limits the number of individuals who are willing to work in the federal space. Emphasis needs to be placed on changing the negative perceptions of working in the U.S. federal government:

> I mean, the work fundamentally itself is attractive. Unfortunately, I think a problem is there's a lot of stigma with regards to government employment and government work. Some of the things that are obvious that we could do is make the jobs more appealing with pay or better benefits. There's a big problem in that, of course; the federal government is limited in that we are limited regarding what can be offered. We need to work toward changing the perception of government work.

A U.S. federal chief information officer proposed establishing a culture in which individuals can come into the U.S. federal government and have a positive impact on cybersecurity: reduce the complexity and overhead often associated with federal

employment and concentrate on helping the nation address its cybersecurity concerns. The ability to make a positive contribution to U.S. federal cybersecurity, combined with job stability and work-life balance, has the potential to make federal employment more appealing:

> I think it really comes down to having a culture where you can come in and make a big difference. Limit the complexity and overhead and focus on getting the work done that helps the nation. If you can combine the ability to make an impact with the stability and work-life balance, we probably measure favorably against the private sector.

U.S. federal organizations should establish stronger cybersecurity accountability at the employee level. Twenty-one federal cybersecurity experts who participated in this study suggested the need to establish more accountability for cybersecurity at the employee level in the U.S. federal government. To this point, there was a push by several study participants to include cybersecurity in all federal employee performance evaluations. As stated by one study participant, "Nothing drives home the importance of something to an employee more than putting it in their performance appraisal. Incorporating cybersecurity in performance appraisals will get people's attention." Another study participant stated, "If you don't measure it on an individual level, you will never get cybersecurity to be incorporated into the daily mindset of employees." One expert stated that all employees play a role in cybersecurity, and that in his perfect world they would all have at least one performance measure focused on cybersecurity:

> In my perfect world every employee, in every organization, would have at least one performance element focused on cybersecurity. Every employee in any organization has some role, however small, in cybersecurity. I think if you put something like that in a performance measurement system, that would go a long way to raising awareness.

Another participant expressed a desire for all employees to have cybersecurity included as part of their performance evaluation but would stop short of holding employees accountable for 100% compliance with cybersecurity policies. The example used in justifying not holding employees fully accountable for compliance with cybersecurity policies centered on training. Specifically, who should be held responsible for the results of employee cybersecurity training? If the training is unsuccessful, not resulting in desired behavior, is it the employee's fault or poor presentation of the training material? As stated by the participant:

> Some would argue that this is a slippery slope and that you would be furthering the notion of "big brother" always watching. However, whether you are in the public or private sector, there are rules we all must follow, and if we don't follow these rules, it could be grounds for termination. I think they have to be incorporated as part of the overall rules of behavior for federal employment. Compliance with these rules of behavior should certainly be considered as part of employee performance metrics. I would stop short of saying that employees should be 100% compliant with cybersecurity policies. For example, should employees be required to take training? Yes, I think we would all agree that training is important. Who should we hold accountable for the results of the training? That's a tricky question to answer. If training is unsuccessful, or doesn't result in the employee behavior we would like, is it simply the employees' lack of compliance or could it be poor delivery of the training material?

Similarly, a separate U.S. federal cybersecurity expert suggested that cybersecurity should be included in employee performance evaluations to drive home the idea that the employee is responsible for cybersecurity, but employees should not be held accountable for honest mistakes:

> I think that's a good idea as long as people aren't punished for honest mistakes because it's really easy in our world for that to happen. And, I mean, I've worked in the field, especially incident response, long enough where you can sometimes see people get into trouble for things that they shouldn't have done, but was really not their fault. So, I think it's a great idea just to make sure that people really—that really brings home the fact that they're responsible for cybersecurity.

In contrast, one U.S. federal cybersecurity expert suggested that cybersecurity should be included in employee performance evaluations only if they are held accountable for the results. In the participant's words, "Unfortunately, very frequently people have things in their performance plans that they're not held accountable for doing. So, if you put cybersecurity in the performance plan, hold the employee accountable for the results." Yet another expert declared that cybersecurity should be included in all employee performance evaluations to emphasize that it is everyone's responsibility and that there should be penalties for violations and rewards for good behavior:

> Make it part of their performance evaluation, make it clear that it's part of everyone's role, make penalties for violations, even if accidental, serious enough impact that they wake up. And then—you know, you also have, offer some mechanism for rewarding good behavior.

Another study participant declared that cybersecurity is already a part of every employee's performance evaluation in his organization. This change has helped to instill a collective organizational culture of cybersecurity responsibility. To this point, there has been a marked decrease in cybersecurity incidents—about 25%—related to data loss and data breaches since cybersecurity was added as an element in performance evaluations:

> We've really instilled a culture of accountability in almost all the performance plans—well, as of last month, it's in every performance plan. There is a whole critical mandate around the protection of PII and sensitive information, and so employees are objectively measured on how well they protect that information. It's that old adage, "what gets measured and monitored gets done." And so, you know, even if it's twice a year that it comes up as part of the performance evaluation, it's like, one, it's a pretty easy metric to meet if you're willing to you know do the training and not commit a violation. However, if you miss the metric, it could be anywhere between a quarter to a third of your performance evaluation, and just having that significance, that priority focus on protecting the enterprise, protecting the information that's entrusted to us, it makes a world of difference. We saw a decrease in incidents of about 25% related to data loss or data breach once that element got added to the performance plans.

U.S. federal organizations should adopt more effective methods for cybersecurity training. As noted previously, training plays a critical role in developing and sustaining cybersecurity culture in U.S. federal organizations. However, the quality of the training methods employed was questioned by 18 of the participants in this study. In fact, some of the participants in this research project suggested strongly that more effective methods of training were needed in the U.S. federal government.

One of the concerns expressed by many of the U.S. federal cybersecurity experts was the ineffectiveness of standard computer-based training (CBT) for cybersecurity. The primary concern with CBT is that employees move through the material as quickly as possible without truly absorbing the content. As one U.S. federal cybersecurity professional stated:

> You know, employees have to take cyber training every year, but it's usually computer based, and the focus is on, you know, how fast can I click through it, get through this. It's, you know, it's more of a nuisance to them. In my opinion that's one of the things that a lot of people, you know, tend to not put a lot of emphasis on, but in my opinion, I think it's a huge, huge emphasis we need to put on, but we need to address the deficiencies in security training. It can't just be a bunch of slides that employees click through. We need to make it, how can I say, more, you know, more of an impression on people.

Another U.S. federal cybersecurity expert suggested that the use of CBT, while not ideal, is necessary because of budgetary constraints:

> In an ideal world, I would like to see more live scenarios and workshops. In reality, with a large workforce, that's probably pretty expensive. CBT is born from a desire to get information out to employees in a cost-effective manner. We don't have the resources to do anything more ideal. Unless we get increased budgets, which we know isn't going to happen, we are stuck with CBT.

A separate study participant acknowledged that a large percentage of employees jumped to the end of CBT, but that could be countered by requiring employees to pass a test at the end of training:

> So, we still do computer-based training, and we've discovered there are about 20% to 30%, yes, they just scroll, yes, they click through. One of the things we do to kind of counterbalance that is we have a pretty strong test in the back of that when you get done, and if you fail the test, sorry, you're taking the training over again, and you're going to continue to take it over again until you pass it.

Similarly, another expert voiced a similar perspective that the challenges faced with CBT could be addressed, at least in part, by forcing employees to view all of the training material and to require that employees successfully pass a test at the end of the training. However, it was also acknowledged that classroom training is probably better suited for those with significant cybersecurity responsibilities. In addition, certification programs should also be considered for those with significant cybersecurity responsibilities:

> CBT used to just allow staff to jump to the end. They have gotten that piece resolved where you have to touch all the content within the presentation and then take a test at the end of it, so that's a positive, but overall, I do believe that the CBT-oriented coursework is still lacking. CBT may be adequate for non–security staff members, but maybe more traditional training, classroom training, for those with significant security responsibilities. This might include a requirement to obtain certain certifications related to cyber.

One research participant suggested that face-to-face, or classroom, training is more influential than CBT because it allows for active participation in the training and provides a forum for open discussion and questions:

> Training is the key element to successful organization, security-wise, and often in training, via a computer where you'll log into the system and flip through the slides quickly and, say, check the box, it's not influential. I think personally face-to-face is extremely influential. What I like about face-to-face, it allows them to participate, to ask questions.

Another expert proposed that successful cybersecurity training must have two components: (1) a classroom setting, where there is engagement in learning about cybersecurity fundamentals and (2) simulations to explore day-to-day cybersecurity issues and responses. These two components were perceived to be important for all employees, not just cybersecurity professionals, because cybersecurity is part of everyone's job. Ultimately, this twofold approach to cybersecurity training was believed to result in greater retention of training material by employees:

> So, I think there's two components. I think the classroom setting is really an imperative where there's hands-on engagement to learn some of the fundamentals. I also think we need overlay of simulation. I don't think we get enough time to engage in some of the simulation that really explores the day-to-day issues and response process. Create a scenario and let the employees walk through the response process. This is the only way training will have a sustained impact on employees. It's important not just for cybersecurity staff, but for everyone in the organization. Cybersecurity should be part of everyone's job in government.

The clear majority of U.S. federal cybersecurity experts interviewed avowed that continuous training is the key to establishing a successful cybersecurity culture. As one participant affirmed, "We try to educate people continuously because the threat is continuously changing. However, I fear this isn't being done consistently or effectively across the government." As another study participant stated:

> Organizations should be focusing on continuous training. What I mean by that, for example, once a week, or whatever the cycle is, they should push questions out to employees related to cybersecurity. If the employee answers the questions correctly, they get immediate, positive feedback and can move on with their workday. Should they get any of the questions incorrectly, they receive immediate feedback to reinforce what they should be thinking or what is important when it comes to cybersecurity. Should they choose to ignore the questions, they would be automatically enrolled in a formal classroom-type training session.

A separate U.S. federal cybersecurity expert emphasized that continuous training is crucial in the federal government and has been highlighted as an effective way to train federal employees against phishing attacks:

> I think continuous training is necessary. I see a lot of challenges in designing such training and delivering such training, but I definitely see the need. Something we are trying to do, again it's very specific to phishing, is, again, have these monthly campaigns and hit every single user in the environment, and then the same thing, if they do click on the link, they get a little page of very brief, digestible content that explains what they did wrong. They are not punished for what they did, but again they're sort of taken to this page where we hope they at least read. And again, we cannot enforce the read, enforce the reading of the educational content. We try to make it really brief and straight to the point and interesting at the same time, so they do get something out of it.

Another study participant described receiving daily questions regarding cybersecurity as part of his organization's continuous training program, which has resulted in employees being more conscientious of cybersecurity:

> Every morning when I log into my system, I'm asked a set of questions based on cybersecurity awareness, and I will be honest—I've gotten a question wrong, and when you get the question wrong you get an explanation as to why your answer was wrong. At the end they actually show you how many questions that they've sent for you to respond to and show you which ones you got right, which ones you got wrong, and then you're able to retake or redo those questions. So, I think, you know we are improving the training process, helping users to be more aware, conscientious of security.

Several study participants stressed the importance of tailoring cybersecurity training in the U.S. federal government to better meet individual and organizational needs. As stated by one study participant, "Cybersecurity training must be tailored. It should be tailored at the organizational level and individual level." One research participant described how his organization embraced continuous cybersecurity training by randomly sending cybersecurity-related questions to employees. However, the organization enhanced this approach to continuous training by tailoring the questions to

the employee's role in the organization. This approach to cybersecurity training was believed to be quick and effective, emphasizing topics that are important for employees to understand based on their role in the organization:

> In our agency, training is actually not once a year, it's actually continuous. So, what happens is at random intervals throughout the year, you'll start—you'll get the five questions sent to you through email, right, based on your position in the organization and activity. If you answer the questions incorrectly, you get additional training. The training is quick and effective. It focuses on the topics that are important, and it spreads training and awareness out throughout the year.

One interesting suggestion, which was provided by a chief information security officer, was to provide employees who successfully complete an organization's targeted cybersecurity training program an official agency certificate of completion that would be signed by the head of the agency. It was noted that the certificate has the potential to provide a sense of pride for the employee and the agency:

> One of the notions, when it comes to training, is this idea of certifying employees, either through an external group or coming up with an internal certification process. If the employee successfully completes all targeted cybersecurity training, they would actually receive a certificate signed by the head of the agency. It lets them know and you know that they've gone through the training successfully, and it helps them to understand the value. It's something that they can take pride in and maybe the organization can as well.

Summary

This chapter has presented the research findings resulting from analysis of the data collected from interviews conducted with 30 federal cybersecurity experts. Each of the four research subquestions was used as the framework for structuring the presentation of the findings, with an emphasis on answering the primary research question. The analysis revealed nine findings related to similarities in cybersecurity culture, two findings related to differences in cybersecurity culture, three findings related to the

current development of cybersecurity culture, and seven findings related to the ideal development of cybersecurity culture. Selected excerpts from the interview transcripts were provided to support the findings identified. Collectively, the findings inform the answer to the primary research question: What is and what should be cybersecurity culture in U.S. federal organizations?

The first section reviewed perceptions of cybersecurity experts from federal-sector organizations regarding similarities in cybersecurity culture in U.S. federal organizations. Drawn from participant interviews, nine primary findings were identified:

1. The importance of cybersecurity is perceived to be understood by most federal employees.
2. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures.
3. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats.
4. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture.
5. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns.
6. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations.
7. Federal cybersecurity culture is primarily a compliance-driven culture.
8. Federal organizations face challenges hiring cybersecurity professionals.

9. Federal organizations are reluctant to detail the technologies employed in their cybersecurity program.

The second section reveals the perceptions of federal cybersecurity experts regarding differences in cybersecurity culture in U.S. federal organizations. Drawn from participant interviews, two primary findings were identified:

1. The varying missions of U.S. federal organizations drive different approaches to cybersecurity.
2. U.S. federal organizations accept varying levels of cybersecurity risk.

The third section reveals the perceptions of federal cybersecurity experts regarding how U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained. Drawn from participant interviews, three primary findings were identified:

1. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations.
2. The varying missions of U.S. federal organizations drive different approaches to cybersecurity.
3. Training is a significant element in establishing cybersecurity culture in U.S. federal organizations.

The fourth section reveals the perceptions of cybersecurity experts from federal-sector organizations regarding how U.S. federal cybersecurity should be developed, demonstrated, and sustained. Drawn from participant interviews, seven primary findings were identified:

1. U.S. federal organizations should focus on cybersecurity risk management and maturity instead of compliance.

2. U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information.
3. U.S. federal organizations should establish a cybersecurity strategic plan.
4. U.S. federal organizations should establish standard operating procedures for cybersecurity.
5. U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals.
6. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level.
7. U.S. federal organizations should adopt more effective methods for cybersecurity training.

In total, 21 findings were identified after analysis of the data collected from interviews conducted with the 30 federal cybersecurity experts. There was some overlap in the findings identified in each section. Specifically, the finding that common laws and regulations provide the foundation for cybersecurity culture in all federal organizations was associated with similarities in U.S. federal cybersecurity culture and how U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained. In addition, the finding that the varying missions of U.S. federal organizations drive different approaches to cybersecurity was associated with differences in U.S. federal cybersecurity culture and how U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained. A detailed discussion of the findings, conclusions, and recommendations associated with this research project is presented in chapter 5.

CHAPTER 5:

INTERPRETATIONS, CONCLUSIONS, AND RECOMMENDATIONS

The purpose of this study was to define what the cybersecurity culture in U.S. federal organizations is and what it should be. To complete the study objective, a qualitative, exploratory inquiry regarding the core elements of federal cybersecurity culture was conducted. Specifically, interviews were conducted with 30 federal cybersecurity experts to deepen understanding of cybersecurity culture in U.S. federal organizations. This chapter presents the study's interpretations, conclusions, and recommendations. There are six primary sections in this chapter: Summary of Findings, Conclusions, Implications for Theory, Recommendations for Practice, Recommendations for Future Research, and Concluding Remarks.

Summary of Findings

Table 5.1 provides a summary of the 21 research findings and their link to the primary research question and each of the four subquestions. It is important to note that there was some overlap in the findings. Specifically, the finding that common laws and regulations provide the foundation for cybersecurity culture in all federal organizations was associated with similarities in U.S. federal cybersecurity culture and how U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained. In addition, the finding that the varying missions of U.S. federal organizations drive different approaches to cybersecurity was associated with differences in U.S. federal cybersecurity culture and the ways that U.S. federal cybersecurity culture is currently developed, demonstrated, and sustained.

Table 5.1
Summary of Research Findings

Primary research question: What is and what should be the cybersecurity culture in U.S. federal organizations?	
Subquestion	Findings
1. What are the similarities in cybersecurity culture in U.S. federal organizations?	1. The importance of cybersecurity is perceived to be understood by most federal employees. 2. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. 3. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats. 4. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture. 5. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns. 6. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations. 7. Federal cybersecurity culture is primarily a compliance-driven culture. 8. Federal organizations face challenges hiring cybersecurity professionals. 9. Federal organizations are reluctant to detail the technologies employed in their cybersecurity program.
2. What are the differences in cybersecurity culture in U.S. federal organizations?	1. The varying missions of U.S. federal organizations drive different approaches to cybersecurity. 2. U.S. federal organizations accept varying levels of cybersecurity risk.
3. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?	1. There are common laws and regulations that provide the foundation for cybersecurity culture in all federal organizations. 2. The varying missions of U.S. federal organizations drive different approaches to cybersecurity. 3. Training is a significant element in establishing cybersecurity culture in U.S. federal organizations.
4. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?	1. U.S. federal organizations should focus on cybersecurity risk management and maturity instead of compliance. 2. U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information. 3. U.S. federal organizations should establish a cybersecurity strategic plan. 4. U.S. federal organizations should establish standard operating procedures for cybersecurity. 5. U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals. 6. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level. 7. U.S. federal organizations should adopt more effective methods for cybersecurity training.

Conclusions

The study resulted in seven significant conclusions, derived from a thorough analysis of the identified research findings. In some cases, multiple findings resulted in a single correlated conclusion. Table 5.2 provides an overview of the seven research conclusions and associated research findings.

Table 5.2
Summary of Conclusions and Associated Research Findings

Conclusion	Associated research findings
1. Employee lack of compliance with cybersecurity policies in U.S. federal organizations necessitates greater accountability.	1. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. 2. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level.
2. U.S. federal organizations need more effective methods of cybersecurity training.	1. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats. 2. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. 3. Training is a significant element in establishing cybersecurity culture in U.S. federal organizations. 4. U.S. federal organizations should adopt more effective methods for cybersecurity training.
3. U.S. federal organizations should establish a cybersecurity strategic plan.	1. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. 2. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats. 3. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture. 4. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns. 5. The varying missions of U.S. federal organizations drive different approaches to cybersecurity. 6. Training is a significant element in establishing cybersecurity culture in U.S. federal organizations. 7. U.S. federal organizations should establish a cybersecurity strategic plan.
4. U.S. federal organizations should establish cybersecurity standard operating	1. Federal organizations face challenges regarding employee compliance with cybersecurity policies and procedures. 2. Federal organizations face challenges associated with the constant state of change regarding cybersecurity threats.

Conclusion	Associated research findings
procedures.	3. The varying missions of U.S. federal organizations drive different approaches to cybersecurity. 4. U.S. federal organizations should establish stronger cybersecurity accountability at the employee level. 5. U.S. federal organizations should establish standard operating procedures for cybersecurity.
5. U.S. federal organizations need innovative approaches to compete with the private sector in the recruitment of cybersecurity personnel.	1. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture. 2. Federal organizations face challenges hiring cybersecurity professionals. 3. U.S. federal organizations need to develop new strategies in the recruitment of cybersecurity professionals.
6. U.S. federal organizations should collaborate in developing cybersecurity strategy.	1. Common laws and regulations provide the foundation for cybersecurity culture in all federal organizations. 2. Budgetary constraints impact the ability of federal organizations to establish an ideal cybersecurity culture. 3. Federal acquisition policies and procedures present challenges for U.S. federal organizations in addressing cybersecurity concerns. 4. Federal organizations are reluctant to detail the technologies employed in their cybersecurity program. 5. The varying missions of U.S. federal organizations drive different approaches to cybersecurity. 6. U.S. federal organizations accept varying levels of cybersecurity risk. 7. U.S. federal organizations should place greater emphasis on interorganizational collaboration and sharing of cybersecurity information.
7. U.S. federal organizations need to shift their focus from cybersecurity compliance to cybersecurity maturity.	1. Federal cybersecurity culture is primarily a compliance-driven culture. 2. U.S. federal organizations should focus on cybersecurity risk management and maturity instead of compliance.

Conclusion 1: Employee Lack of Compliance with Cybersecurity Policies in U.S. Federal Organizations Necessitates Greater Accountability

Despite the perception of a general understanding of the importance of cybersecurity by most federal employees, the participants in this study held a strong belief that federal employees' lack of compliance with cybersecurity policies and

procedures presents significant challenges for federal organizations. Employees fall under the broad category of "insider threat" and can conduct intentional, or unintentional, acts that threaten a strong cybersecurity posture. Employee lack of compliance with cybersecurity policies and procedures, whether intentional or unintentional, presents the same risk to organizations.

Given the perception of the risk presented by employees regarding cybersecurity, it was not surprising that several of the U.S. federal cybersecurity experts who participated in this study suggested the need to increase employee accountability for cybersecurity in the U.S. federal government. To this point, there was a push by several study participants to include cybersecurity in all U.S. federal employee performance evaluations. Including cybersecurity compliance in U.S. federal employee performance evaluations was expected to highlight its importance and drive compliance. In addition, it was suggested that regular measurement of cybersecurity compliance would help to embed cybersecurity in the culture of U.S. federal organizations.

Connection to the literature. The research findings related to the need to increase U.S. federal employee accountability regarding cybersecurity culture aligned directly with the current literature on cybersecurity. Chou (2007) suggested that one of the biggest challenges to organizational cybersecurity is human behavior. Von Solms and van Niekerk (2013) emphasized that cybersecurity extends beyond the traditional technical boundaries of information security and includes the human factor. In addition, Ghernouti-Hélie et al. (2010) highlighted that human beings are the weakest link in the cybersecurity chain. Further, they called for greater awareness and clarity regarding individual responsibilities for cybersecurity (Ghernouti-Hélie et al., 2010).

The perception of employee lack of compliance with federal cybersecurity policies and procedures, and the resulting desire to increase employee accountability, also aligns with Schein's (1992) culture model. Specifically, the belief that employees do not comply with cybersecurity policies, either intentionally or unintentionally, is an underlying assumption in federal cybersecurity culture. The desire to establish stronger employee accountability for cybersecurity is an espoused value associated with federal cybersecurity culture. In addition, including cybersecurity compliance in employee performance appraisals would be an artifact of an ideal federal cybersecurity culture (Schein, 1992).

Conclusion 2: U.S. Federal Organizations Need More Effective Methods of Cybersecurity Training

The cybersecurity experts interviewed as part of this study indicated that employee training plays a significant role in establishing cybersecurity culture in U.S. federal organizations. Federal cybersecurity culture is established through expanded employee awareness, which is primarily established through training. Federal cybersecurity training includes traditional, instructor-facilitated, classroom, and computer-based training.

It was clear from the interviews conducted with experts that training plays a critical role in developing and sustaining a cybersecurity culture in U.S. federal organizations. However, the quality of the training methods employed by the organizations was questioned by several study participants. In addition, it was suggested that many federal employees view federal cybersecurity training to be a hindrance, not

fully appreciating its value. Accordingly, some of the participants in this research project suggested strongly that more effective methods of training were needed.

One of the concerns expressed by some of the study participants was the ineffectiveness of computer-based training (CBT) for cybersecurity. The primary concern with CBT was that employees move through the training material as quickly as possible without learning from the content provided. It was suggested that the challenges acknowledged with CBT could be addressed, at least in part, by forcing employees to touch all the training content and requiring that employees successfully pass a test at the end of the training. However, it was also implied that face-to-face, or classroom, training may be more influential than CBT because it allows for active employee participation in the training and provides a forum to ask questions and receive immediate feedback. It was also suggested that cybersecurity training should be expanded to include live simulations, which is important in exploring day-to-day cybersecurity concerns and appropriate individual and organizational responses. Cybersecurity simulations are also believed to result in greater retention of training content, and associated value, by employees.

The majority of U.S. federal cybersecurity experts interviewed avowed that continuous training was the key to establishing a successful cybersecurity culture. This response was driven by the perceived need to educate employees on cybersecurity threats continually because the threats are constantly changing. Other study participants stressed the importance of tailoring training to individual and organizational needs. Training should provide general organizational cybersecurity awareness, but should also include a tailored element based on an employee's specific role in the organization. For example,

the job-specific cybersecurity concerns for an administrative professional are very different from those of a network administrator. Providing a job-specific, tailored training experience was expected to result in a greater depth of understanding and value regarding individual cybersecurity responsibilities and overall increased organizational compliance with cybersecurity requirements. One interesting suggestion was to award employees who successfully complete an organization's targeted cybersecurity training program an official agency certificate of completion that would be signed by the head of the agency. It was noted that the certificate has the potential to provide a sense of value for the employee and the agency.

Connection to the literature. The study findings related to needed improvements in federal cybersecurity training also align with the current literature on cybersecurity. Spurling (1995) recommended that leaders develop and implement various security awareness initiatives that keep employees security conscious and help maintain a security culture. Furnell et al. (2002) implied that a well-developed training program is a key element to furthering cybersecurity culture, whether the organization is large or small. Rotvold (2008) suggested that a formal security awareness and training program should be established in organizations interested in developing a stronger security culture. Thomson and von Solms (1998) concluded that for security awareness programs to be more effective, they should be tailored to address specific groups of employees within the organization.

The conclusion that U.S. federal organizations need more effective methods of cybersecurity training aligns with Schein's (1992) culture model. There is an underlying assumption that existing training is not sufficient and that more effective training

methods are needed. The stated desire by many U.S. federal cybersecurity experts to reform training in federal organizations is an espoused value associated with an ideal federal cybersecurity culture. In addition, any new cybersecurity training programs established would be an artifact of U.S. federal cybersecurity culture (Schein, 1992).

Conclusion 3: U.S. Federal Organizations Should Establish a Cybersecurity Strategic Plan

The U.S. federal cybersecurity experts interviewed as part of this research project indicated that federal organizations should establish a cybersecurity strategic plan that outlines their short- and long-term cybersecurity strategies. The unique mission requirements of each U.S. federal organization necessitate tailored strategic plans. However, the overarching federal cybersecurity strategic goals (i.e., from Office and Management and Budget Circular A-130, the Federal Information Security Modernization Act of 2014, and the National Institute of Standards and Technology) should be incorporated in each federal organization's strategic plan. The period of time covered by a strategic plan, as identified by the research participants, ranged from 1 to 7 years. In addition, given the constant change in the federal cybersecurity landscape, study participants noted that strategic plans should be updated regularly to reflect changes in cybersecurity program priorities.

Cybersecurity should be incorporated in every aspect of U.S. federal organizations, and a cybersecurity strategic plan was essential for this focus. A cybersecurity strategic plan was viewed as critical in justifying the allocation of resources (financial and personnel) for cybersecurity initiatives. In addition, the cybersecurity

strategic plan would help to show how cybersecurity investments are contributing value to the organization.

Connection to the literature. The emphasis on establishing a cybersecurity strategic plan in U.S. federal organizations aligns with the existing literature on cybersecurity. Specifically, Bradley et al. (2006) suggested that a high-quality information technology strategic plan can allow organizations to formally assert priorities to meet information technology goals. In some cases, these plans detail the allocation of human and financial resources needed to meet strategic information technology goals. In fact, in the absence of a quality strategic plan, the risk of failure associated with information technology initiatives can increase dramatically (Bradley et al., 2006).

The emphasis on establishing a cybersecurity strategic plan in U.S. federal organizations also aligns with Schein's (1992) model of culture. There is an underlying assumption that many federal organizations do not have an effective cybersecurity strategy. A robust strategic plan would detail the espoused cybersecurity values (i.e., strategies, goals, and philosophies) of a federal organization. In addition, a published cybersecurity strategic plan has the potential to be an artifact associated with cybersecurity culture (Schein, 1992).

Conclusion 4: U.S. Federal Organizations Should Establish Cybersecurity Standard Operating Procedures

In addition to a cybersecurity strategic plan, U.S. federal cybersecurity experts indicated that standard operating procedures were essential for ensuring an efficient and effective cybersecurity program in U.S. federal organizations. Specifically, standard operating procedures would help establish consistency and reliability in cybersecurity

operations. It was also suggested that standard operating procedures would help organizations more quickly identify and address concerns. How quickly organizations identify and resolve cybersecurity incidents was highlighted as a key metric in measuring the success of federal cybersecurity programs. In addition, standard operating procedures were identified as critical for establishing a strong cybersecurity posture and, to this point, organizations that did not have them tended to struggle with cybersecurity.

Connection to the literature. There was direct alignment between study findings related to standard operating procedures and the current literature on cybersecurity. Batteau (2011) suggested that standard processes are a major component of organizational cybersecurity. The Government Accountability Office (2006) implied that a commitment by senior leadership within organizations to plan the evolution of security policies strategically is a vital strategy in ensuring the confidentiality, integrity, and availability of organizational information. Harrington (1996) noted that cybersecurity policy endorsed by top management and signed by employees indicates that the organization is serious about information security. Da Veiga and Eloff (2007) discussed how leadership could directly impact the success or failure of an organization's cybersecurity program and, as such, it is essential that cybersecurity leaders effectively instill a sense of organizational urgency around information security and related policies. Stacey et al. (1998) indicated that cybersecurity leaders need to establish a security culture within their organizations and that information security beliefs and understandings should become tightly integrated with formal policies and procedures.

The emphasis on establishing cybersecurity standard operating procedures in U.S. federal organizations also supports Schein's (1992) model of culture. Specifically, there

is an underlying assumption that standard operating procedures do not exist, or are poorly developed, in some federal organizations. In addition, the need for standard operating procedures is a value associated with an ideal cybersecurity culture. Further, well-developed standard operating procedures represent an artifact of federal cybersecurity, detailing cybersecurity operational structures and processes (Schein, 1992).

Conclusion 5: U.S. Federal Organizations Need Innovative Approaches to Compete with the Private Sector in the Recruitment of Cybersecurity Personnel

U.S. federal organizations have faced great challenges in hiring cybersecurity professionals. Of particular concern was the perception that the U.S. government cannot compete with private-sector salaries. In addition, a stigma is frequently associated with working in the federal government, and that limits the number of individuals willing to seek federal employment. As a result, several study participants called for a change in the way the U.S. federal government recruits cybersecurity professionals.

It was noted by several study participants that federal salaries are not adequate to attract the best cybersecurity professionals. Accordingly, there was a suggestion that U.S. federal cybersecurity professionals should get a salary commensurate with market demand. Unfortunately, the salary structure in most federal organizations does not provide for expansive pay flexibility. In fact, the general schedule pay scale, which is the federal government's predominant pay scale, pays the same amount to all employees of the same grade, regardless of profession. However, some federal organizations have adopted pay bands, which have been used successfully in some to provide greater flexibility in salaries offered to employees.

Given the perception that the U.S. government cannot compete with the salaries offered cybersecurity professionals in the private sector, and the stigma often associated with federal employment, there was a call for other motivators for public service. One such motivator was the opportunity for exposure to cybersecurity experiences not available in the private sector. These experiences might include those directly related to national cybersecurity concerns. It was also suggested that job security and work-life balance, which are afforded most employees in the U.S. federal government, might be used as a motivator for some cybersecurity professionals to join the federal workforce. In addition, it was implied that the recruitment efforts for federal cybersecurity personnel should target individuals with a yearning for public service or a strong loyalty to the country.

It was suggested that obtaining federal employment can be challenging. For example, employment qualification advantages are often granted for specific groups, such as U.S. veterans, which can limit federal job accessibility to the general population. In addition, hiring freezes, which are either self-imposed, forced through legislation, or due to lack of appropriated funding, further limit federal hiring opportunities. These hiring freezes not only place restrictions on new hires, but often limit career growth for federal cybersecurity personnel. In fact, limits on opportunities for career growth can lead directly to exploration of private-sector careers by federal cybersecurity professionals. Accordingly, the federal government is encouraged to expand cyber job opportunities for the general public and limit hiring restrictions.

The rigid personal conduct standards for federal employment, including extensive background investigations for certain positions, were perceived to limit the ability to

recruit an effective cybersecurity workforce. In particular, the emphasis on recruiting cybersecurity professionals with a perfect background, including positive education requirements, was deemed unrealistic. It was suggested that employment standards for the federal cybersecurity workforce should be modified to reflect more realistic societal expectations. This was not to suggest that the federal government should be open to hiring criminals, but the current federal hiring standards were believed to be more stringent than is necessary.

Connection to the literature. The findings related to the challenges faced in the recruitment of the federal cybersecurity workforce were not directly addressed in the cybersecurity literature. However, there is little doubt that the U.S. federal government, as a whole, has faced challenges in recruiting a high-quality cybersecurity workforce. These challenges can certainly be attributed to perceived lower salaries, when compared to the private sector, and a general stigma associated with federal employment. Accordingly, consideration should be given to making the hiring process and salaries for federal cybersecurity professionals more favorable when compared with the private sector. This effort may include expanded pay bands for federal cybersecurity professionals and an emphasis on the value of the benefits afforded federal employees. In addition, the nonmonetary motivators identified in this study, such as opportunity for unequaled exposure to national cybersecurity concerns, should be considered by federal recruiters in their efforts to attract and retain a high-quality cybersecurity workforce.

However, there is direct alignment between the need for innovative approaches in the recruitment of U.S. federal cybersecurity professionals and Schein's (1992) model of organizational culture. The suggested changes in recruitment philosophy and related

strategies have the potential to present a dramatic change in U.S. federal government culture. There is an opportunity to change the underlying assumptions regarding cybersecurity work in the U.S. federal government. For example, by focusing on the unique cyber career opportunities, there is a potential to reverse the stigma associated with U.S. federal employment. In addition, established federal salary structures, policies granting preference to certain groups for federal employment (e.g., U.S. veterans), and mandated hiring freezes are all current cultural artifacts. Finally, the proposed changes in the recruitment of federal cybersecurity personnel would require direct, overt support by leadership and would align with Schein's notion of an espoused value (Schein, 1992).

Conclusion 6: U.S. Federal Organizations Should Collaborate in Developing Cybersecurity Strategy

The participants in this study indicated that formal mechanisms existed for collecting and sharing cybersecurity information across the U.S. federal government. In fact, the Department of Homeland Security and the Office of Management and Budget were most frequently cited for collecting and sharing cybersecurity information. In general, there was satisfaction among the study participants regarding the formal processes for collecting and sharing cybersecurity information, but they noted a deficiency in the sharing of cybersecurity information directly between U.S. federal organizations.

There was an expressed desire by the U.S. federal cybersecurity experts interviewed as part of this study to work directly with other federal organizations in developing cybersecurity strategy. Ironically, most federal organizations were believed to

be developing their cybersecurity strategy in isolation. Further, it was emphasized that interorganizational collaboration was an area of failure for federal cybersecurity.

The interviews also revealed that concerns over a potential perception of weakness in an organization's approach to cybersecurity limited the sharing of cybersecurity information among U.S. federal organizations. In exposing an organization's cybersecurity "dirty laundry," the potential for embarrassment exists. It was also suggested that the federal sector does not lend itself to the sharing of information, regardless of the subject matter, and that this could be directly attributed to the federal government's inherent political nature.

The cybersecurity experts further indicated that, when it comes to cybersecurity posture, federal organizations were stronger when they were working together. U.S. federal organizations should feel comfortable in collaborating regarding cybersecurity concerns. In fact, with encouragement and understanding that all federal organizations should be focused on the goal of establishing a stronger federal cybersecurity posture, collaboration between federal organizations could be accomplished without the threat of repercussion or embarrassment. To this point, it was suggested that a standard protocol should be established for the safe sharing of cybersecurity information directly between federal organizations. The timely sharing of relevant information has the potential to avert a national cybersecurity threat.

Connection to the literature. The research findings related to the challenges faced by U.S. federal organizations in sharing cybersecurity information were not directly addressed in the cybersecurity literature. Nonetheless, it is easy to understand how the fear of negative judgment from peers regarding an organization's cybersecurity program

would limit collaboration. In addition, the heavy political climate in the U.S. federal government could also contribute to resistance in sharing of cybersecurity information. However, there was a suggestion in the literature that the constant state of change in information technology requires a broader, more collective approach to cybersecurity (Chabinsky, 2010; Vaughn et al., 2003; Wilshusen, 2010). Clearly, efforts to establish a broader, more collective approach to cybersecurity within the federal sector could be enhanced through stronger collaboration among U.S. federal organizations.

In addition, the perceived need for U.S. federal organizations to collaborate in developing cybersecurity strategy aligns with Schein's (1992) notion of an underlying cultural assumption. The suggested direct collaboration between U.S. federal organizations in developing cybersecurity strategies represents a significant philosophical change for the U.S. federal government. Most U.S. federal organizations are believed to be currently developing their cybersecurity strategies in isolation. As such, an emphasis on collaboration between U.S. federal organizations in developing cybersecurity strategy would require broad support and cooperation across the federal government. Any formal standards established for collaboration between organizations would be an artifact of a model of federal cybersecurity culture. Further, an emphasis on cooperative development of cybersecurity strategies in the U.S. federal government would equate to an espoused value for an ideal cybersecurity culture (Schein, 1992).

Conclusion 7: U.S. Federal Organizations Need to Shift Their Focus from Cybersecurity Compliance to Cybersecurity Maturity

The participants in this study strongly affirmed that the current culture of cybersecurity compliance in U.S. federal organizations is counterproductive. Further,

there was a perception that compliance, or adherence to strict guidelines and control standards, does not equate to good security. It was believed that U.S. federal organizations would be better served by focusing on improving cybersecurity maturity.

The experts also contended that federal cybersecurity compliance requirements lag several years behind the latest threats. In addition, while it was certainly established with the best of intentions, federal cybersecurity compliance work has resulted in an unwieldy and unproductive overhead. For example, the National Institute of Standards and Technology (2017) has published an expansive list of control objectives for managing federal cybersecurity in its *Framework for Improving Critical Infrastructure Cybersecurity*. Unfortunately, despite the best efforts by many federal organizations, these cybersecurity control objectives have proven to be an overwhelming mandate of compliance requirements. In fact, efforts to adhere with strict cybersecurity compliance requirements place an unruly burden on limited federal budgetary and personnel resources. The current culture of cybersecurity compliance in the U.S. federal government, and its related extensive paperwork, limits the federal community from focusing on the important work of improving cybersecurity.

Simply stated, the current culture of cybersecurity compliance inhibits cybersecurity maturity in the federal government because its compliance-based approach to cybersecurity has been equated to a check-the-box attitude to cybersecurity. Compliance narrows the focus on cybersecurity to a standard framework of control objectives. Further, the dedicated resources, both budgetary and personnel, required to sustain these control objectives is untenable. Accordingly, U.S. federal cybersecurity experts have called for a shift in federal cybersecurity culture, from a culture that focuses

on compliance to a culture that emphasizes maturity. A culture of cybersecurity maturity should include a focus on enhanced organizational awareness, management support, policies and procedures, marketing and communication strategies, training programs, internal and external collaboration, and emphasis on continuous improvement.

Connection to the literature. The research findings related to cybersecurity maturity in U.S. federal organizations were not explicitly addressed in the cybersecurity literature. However, these findings could certainly be connected to the importance of leadership actions in establishing an effective cybersecurity culture. The visible and regular support of cybersecurity by top management is an effective means to reduce information security risks and establish an effective cybersecurity culture (Harrington, 1996). Cybersecurity leaders need to establish a security culture within their organizations so that information security beliefs and understandings can become tightly integrated with formal policies and procedures (Stacey et al., 1998). It is essential that cybersecurity leaders effectively instill a sense of organizational urgency around information security and related policies. In most cases, this will require that cybersecurity leaders transform the security culture of their organization (Herath & Rao, 2009).

In addition, there is a connection between the emphasis on the need for U.S. federal organizations to focus on cybersecurity maturity and Schein's (1992) model of organizational culture. The U.S. federal government currently stresses compliance with an established set of cybersecurity control objectives. There is an underlying assumption, or belief, by many of the participants interviewed that compliance with cybersecurity control objectives limits the maturity of federal cybersecurity. Shifting the emphasis of

U.S. federal cybersecurity from compliance to maturity would represent a dramatic shift in cybersecurity philosophy, requiring significant support by leadership. Consequently, this dramatic change in federal cybersecurity philosophy, and related strategies, aligns with Schein's notion of an espoused value in an ideal federal cybersecurity culture (Schein, 1992).

Implications for Theory

This section provides a summary of the theoretical implications resulting from this study. The implications for theory are divided into two primary categories: theoretical alignment and contributions, and Schein's cultural model.

Theoretical Alignment and Contributions

Employee challenges with cybersecurity. The results of the research align with current theory regarding the challenges employees present in establishing a strong cybersecurity culture (Chou, 2007; Ghernouti-Hélie et al., 2010; von Solms & van Niekerk, 2013). Despite the perception of a general understanding of the importance of cybersecurity by most federal employees, the participants in this study strongly agreed that federal employees' lack of compliance with cybersecurity policies and procedures presents significant challenges for federal organizations. Including cybersecurity compliance in U.S. federal employee performance evaluations was expected to highlight its importance, drive compliance, and embed cybersecurity in the culture of U.S. federal organizations.

Needed improvements in cybersecurity training. The study findings related to needed improvements in federal cybersecurity training align directly with the current

literature on cybersecurity (Furnell et al., 2002; Rotvold, 2008; Spurling, 1995; Thomson & von Solms, 1998). Federal cybersecurity culture is established through expanded employee awareness, which is primarily established through training. However, participants in this research project suggested strongly that more effective methods of training were needed in the U.S. federal government.

Significance of a cybersecurity strategic plan. The emphasis on establishing a cybersecurity strategic plan in U.S. federal organizations aligns with the existing literature on cybersecurity, which suggests that a high-quality information technology strategic plan can allow organizations to formalize established priorities to meet information technology goals (Bradley et al., 2006). Cybersecurity should be incorporated in every aspect of U.S. federal organizations, and a strategic plan is essential for this focus. A cybersecurity strategic plan was viewed as critical in justifying the allocation of resources (financial and personnel) for cybersecurity initiatives. In addition, the strategic plan helps to show how federal investments contribute value to the organization.

Significance of standard operating procedures. There was direct alignment between study findings related to the need for standard operating procedures and the current literature on cybersecurity, which confirms that standard operating procedures are a critical component of cybersecurity (Batteau, 2011; Da Veiga & Eloff, 2007; Government Accountability Office, 2006; Harrington, 1996; Stacey et al., 1998). The study participants indicated that standard operating procedures were essential for ensuring an efficient and effective cybersecurity program in U.S. federal organizations. Standard operating procedures help establish consistency and reliability in cybersecurity

operations. In addition, standard operating procedures were identified as critical for establishing a strong cybersecurity posture and, at this point, organizations that do not have standard operating procedures tend to struggle with cybersecurity.

Need for innovations in the recruitment of cybersecurity personnel. The findings related to the challenges faced in the recruitment of the federal cybersecurity workforce were not directly addressed in the cybersecurity literature. Clearly, though, U.S. federal organizations have faced great challenges in hiring cybersecurity professionals. The perception that the U.S. government cannot compete with private-sector salaries was a noted concern. In addition, there is a stigma frequently associated with working in the federal government, which limits the number of individuals willing to seek federal employment. As a result, there was a call for new motivators for federal service.

Need for better collaboration in developing cybersecurity strategy. The research findings related to the challenges faced by U.S. federal organizations in sharing cybersecurity information were not directly addressed in the cybersecurity literature. However, there was a suggestion in the literature that the constant state of change in information technology requires a broader, more collective approach to cybersecurity (Chabinsky, 2010; Vaughn et al., 2003; Wilshusen, 2010). Clearly, efforts to establish a broader, more collective approach to cybersecurity within the federal sector could be enhanced through stronger collaboration between its organizations.

Focus on cybersecurity maturity. The research findings related to cybersecurity maturity in U.S. federal organizations were not explicitly addressed in the cybersecurity literature. However, these findings could certainly be connected to the importance of

leadership actions in establishing an effective cybersecurity culture. Leaders should instill a sense of organizational urgency around information security and related policies. This effort may require cybersecurity leaders to transform the security culture of their organization (Harrington, 1996; Herath & Rao, 2009; Schein, 1992; Stacey et al., 1998).

Schein's Culture Model

Edgar Schein's (1992) theory and definition of organizational culture served as the foundation for this research effort. Schein believed that culture could be analyzed from three levels: artifacts, espoused values, and underlying assumptions. The three were certainly evident in the exploration of federal cybersecurity culture. For example, a cybersecurity strategic plan details the espoused cybersecurity values (i.e., strategies, goals, and philosophies) of a federal organization. Further, a published cybersecurity strategic plan has the potential to be an artifact associated with federal cybersecurity culture. In addition, an emphasis on cybersecurity maturity was an espoused value linked with an ideal federal cybersecurity culture. Similarly, there was an underlying assumption that U.S. federal employees understand the importance of cybersecurity (Schein, 1992).

Schein also explained that the most decisive function of a leader is the creation and management of culture. In some cases, this responsibility can require leaders to tear down and completely rebuild culture. Schein's (1992) emphasis on the importance of leaders in rebuilding culture would certainly apply to the findings from this study, which directly call for federal leaders to implement significant change in U.S. federal cybersecurity culture.

Schein (1992) also indicated that organizational culture change involves a process of altering basic assumptions, which can be difficult and often anxiety provoking. This

would certainly be the case regarding changes to U.S. federal cybersecurity culture. Changing the current culture of cybersecurity to one that emphasizes the ideals identified in this study could prove to be a daunting task for federal leaders.

Recommendations for Practice

The results of this research effort have clear implications for practice, providing a better understanding of the current and ideal state of cybersecurity culture in U.S. federal organizations. In fact, the seven identified research conclusions present an opportunity for action for federal cybersecurity leaders.

Recommendation 1: Include Cybersecurity Compliance in Employee Performance Appraisals

The research results indicated that a lack of employee compliance with established cybersecurity policies and procedures presents a significant challenge for U.S. federal organizations. The lack of compliance can be intentional or unintentional, but the significance of the "insider threat" in weakening federal cybersecurity posture remains the same. Accordingly, federal leaders should take steps to remedy the identified deficiency in employee compliance with cybersecurity policies and procedures.

U.S. federal cybersecurity leaders are encouraged to consider establishing more formal mechanisms for ensuring employee accountability for cybersecurity. One option identified as part of this study is to include cybersecurity requirements in all U.S. federal employee performance evaluations. Such an effort has the potential to highlight the significance of cybersecurity and drive compliance. In addition, regular measurement of

cybersecurity compliance will help to embed cybersecurity in the culture of U.S. federal organizations.

Recommendation 2: Improve Cybersecurity Training Methods

The U.S. federal cybersecurity experts interviewed as part of this study indicated that employee training plays a significant role in establishing a cybersecurity culture in organizations. However, the quality of the training methods employed by U.S. federal organizations was questioned by several study participants. In fact, some participants suggested that more effective methods of training were needed.

U.S. federal leaders have an opportunity to address the perceived deficiency in cybersecurity training. One of the concerns expressed by many experts interviewed as part of this study was the ineffectiveness of CBT. It was proposed that the challenges acknowledged with CBT could be addressed, at least in part, by forcing employees to touch all the training content and requiring that employees successfully pass a test at the end of the training. However, it was implied that face-to-face, or classroom, training may be more influential than CBT because it allows for active participation in the training and provides a forum for employees to ask questions and receive immediate feedback. It was also suggested that cybersecurity training should be expanded to include live simulations that enhance the exploration of cybersecurity concerns. As a result, there is greater potential for employees to have a better understanding and greater retention of training content.

Continuous training was highlighted as essential for establishing a successful cybersecurity culture in U.S. federal organizations. The focus on continual training was driven by the constant state of change concerning cybersecurity threats. One example

would be to regularly push cybersecurity-related questions, via email, out to employees. Employees who answered the questions correctly would get immediate, positive feedback and move on with their workday. However, employees who answered any of the questions incorrectly would receive immediate feedback to reinforce what they should be thinking and to know what is important when it comes to cybersecurity. Should employees choose to ignore the questions, they would be automatically enrolled in a formal classroom-type training session.

Other study participants stressed the importance of tailoring cybersecurity training in the U.S. federal government to individual and organizational needs. Training programs could be modified to provide general organizational cybersecurity awareness, but include a tailored element based on an employee's unique role in the organization. The more closely a training program is tied to an employee's job duties and responsibilities, the more likely it is that the employee will focus on the training and commit to the learning objectives. Another consideration was to award employees who successfully complete an organization's targeted cybersecurity training program an official agency certificate of completion signed by the head of the agency. It was noted that the certificate has the potential to provide a sense of pride for the employee and the agency.

Recommendation 3: Develop a Cybersecurity Strategic Plan

The experts also indicated that federal organizations should establish a cybersecurity strategic plan. Strategic plans were perceived as critical for outlining the short- and long-term cybersecurity strategy for federal organizations. Federal leaders should be focused on incorporating cybersecurity in every aspect of U.S. federal organizations, and a cybersecurity strategic plan is essential for this focus. The

cybersecurity strategic plan was also viewed as an essential tool for justifying the allocation of financial and personnel resources for cybersecurity initiatives. In addition, strategic plans help to show how cybersecurity investments are contributing value to the organization.

Recommendation 4: Establish Cybersecurity Standard Operating Procedures

In addition to a cybersecurity strategic plan, the cybersecurity experts indicated that standard operating procedures are essential for ensuring an efficient and effective cybersecurity program in U.S. federal organizations. Standard operating procedures help establish consistency and reliability in cybersecurity programs. Further, standard operating procedures help organizations more quickly identify and address cybersecurity incidents. In fact, the speed at which an organization identifies and resolves cybersecurity incidents was highlighted as a key metric in measuring the success of federal cybersecurity programs. In addition, standard operating procedures were identified as critical for establishing a strong cybersecurity posture, and organizations that do not have standard operating procedures tend to struggle with cybersecurity.

Recommendation 5: Establish Innovations in the Recruitment of Cybersecurity Personnel

U.S. federal organizations have faced great challenges in hiring cybersecurity professionals. Of primary concern was the perception that the U.S. government cannot compete with private-sector salaries. In addition, there is frequently a stigma associated with working in the U.S. federal government that limits the number of individuals who

are willing to apply. As a result, federal leaders should consider new innovations in the recruitment of cybersecurity professionals.

Several participants emphasized that federal salaries are not adequate to attract the best cybersecurity professionals. Accordingly, there was a suggestion that U.S. federal cybersecurity professionals should be offered a salary commensurate with market demand. Unfortunately, the salary structure in most federal organizations does not provide for expansive pay flexibility. Accordingly, U.S. federal leaders should consider establishing new pay scales for cybersecurity professionals. In fact, some federal organizations have adopted pay bands, which have been used successfully to provide greater flexibility in salaries offered to personnel.

Given the perception that the U.S. government cannot compete with the salaries offered cybersecurity professionals in the private sector, and the stigma often associated with federal employment, there was a call for other motivators for public service. One such motivator is highlighting the opportunity for exposure to cybersecurity experiences not available in the private sector. These experiences might include those directly related to national cybersecurity concerns. It was also suggested that job security and work-life balance, which most federal employees enjoy, might motivate some cybersecurity professionals to join the federal workforce. In addition, it was implied that the recruitment efforts for federal cybersecurity personnel should target individuals with a yearning for public service or a strong loyalty to the country.

It was also noted that the rigid personal conduct standards for federal employment, which include extensive background investigations for certain positions, were perceived to limit the ability of the U.S. federal government to recruit an effective

cybersecurity workforce. The emphasis on recruiting cybersecurity professionals, who have a perfect background, including positive education requirements, was deemed unrealistic. Federal leaders should consider modifying employment standards to reflect more contemporary societal expectations. This was not to suggest that the federal government should be open to hiring criminals, but the current hiring standards were believed to be more stringent than is necessary, which limits the ability to recruit an effective cybersecurity workforce.

Recommendation 6: Establish a Framework for Improved Collaboration Between U.S. Federal Organizations in Developing Cybersecurity Strategy

The cybersecurity experts indicated that, when it comes to establishing a strong cybersecurity posture, federal organizations are stronger when they are working together. However, there is currently a perceived deficiency in the direct sharing of information between U.S. federal organizations that has been attributed to the potential for embarrassment in exposing an organization's cybersecurity weaknesses and the inherent political nature of the U.S. federal government.

Federal leaders should work to establish a safe protocol for directly sharing relevant cybersecurity information between U.S. federal organizations. These organizations should feel comfortable in collaborating regarding cybersecurity concerns. The primary focus should be to establish a stronger federal-wide cybersecurity posture. To this point, the timely sharing of relevant information concerning cybersecurity concerns and related strategies between U.S. federal organizations has the potential to avert a large-scale national cybersecurity incident.

Recommendation 7: Change Emphasis from Cybersecurity Compliance to Cybersecurity Maturity

The current culture of cybersecurity compliance in the U.S. federal government has been perceived to inhibit cybersecurity maturity. The compliance-based model has been equated to a check-the-box approach to cybersecurity. Further, the resources required to meet compliance standards have narrowed the focus on cybersecurity to a standard framework of control objectives. In reality, adherence to the strict requirements places a considerable burden on limited federal cybersecurity budgetary and personnel resources even as it inhibits maturity.

Accordingly, U.S. federal leaders should work to shift federal cybersecurity culture from a focus on compliance to an emphasis on cybersecurity maturity. Emphasizing cybersecurity maturity does not necessitate eliminating all compliance activities. However, cybersecurity maturity includes incorporating strategic planning, policies and procedures, workforce development, organizational and employee accountability, marketing and communication, internal and external collaboration, and continuous improvement. Ultimately, a culture of cybersecurity maturity has the potential to strengthen the cybersecurity posture across the U.S. federal government.

Recommendations for Future Research

Based on the study conducted and the resulting research findings, below are seven recommendations for future research:

1. This study centered on 30 U.S. federal cybersecurity experts from 23 unique federal organizations. This sample size was deemed appropriate, given that the participants were all key informants with profound understanding of cybersecurity

culture based on decades of experience in the field. However, given the extensive population of U.S. federal organizations and cybersecurity experts, it is suggested that this research be replicated and extended to a broader sample of the population. A comparison of the results from similar research efforts has the potential to lend further credibility to the research results from this study.

2. Although not by design, the 23 U.S. federal organizations represented in this study were all from the executive branch (president, executive departments, independent agencies, independent boards, commissions, and committees) of the U.S. federal government. As a result, it is suggested that future explorations of cybersecurity culture in U.S. federal organizations be expanded to include the judicial branch (federal courts and support organizations) and legislative branch (Senate, House of Representatives, and support organizations). A review of the similarities and differences in cybersecurity culture for each branch of the federal government could prove valuable for both theory and practice.
3. This research project was scoped to focus on understanding organizational cybersecurity culture in a U.S. federal government context. As a result, the research results cannot be generalized outside of this context. Accordingly, it is suggested that future research efforts be extended to include exploration of both public- and private-sector organizations. The ability to compare the cybersecurity culture in public- and private-sector organizations could provide significant implications for theory and practice.
4. This research effort was an exploratory study, designed to investigate U.S. federal cybersecurity culture. The chosen research methodology was deemed appropriate,

given the goal of gaining a broad understanding of cybersecurity culture in U.S. federal organizations. Future research efforts may consider applying different research methodologies to explore U.S. federal cybersecurity culture. For example, a case study methodology could be used to investigate more intricate aspects of cybersecurity culture in U.S. federal organizations.

5. As is noted in the research findings, U.S. federal organizations face significant challenges regarding employee compliance with cybersecurity policies and procedures. This lack of compliance can be intentional or unintentional, but the significance of the "insider threat" to federal cybersecurity posture remains the same. In contrast, the typical high-reliability organization (HRO) is highly complex and operates in an environment with significant operational risk but rarely encounters catastrophe due to a proper balance of system design and incident prevention. HROs understand that employees can be part of the solution when it comes to risk management. Accordingly, HROs emphasize personnel development, shared understanding of risks, information sharing, and collective learning to achieve superior performance. It is recommended that future research focus on the applicability of HRO practices in establishing a stronger federal cybersecurity culture. HRO practices have the potential to convert the current negative narrative regarding federal employees' lack of compliance with cybersecurity policies and procedures to one that emphasizes employees' positive contributions to cybersecurity risk management (Weick & Sutcliffe, 2011).
6. The research findings indicated that one of the key metrics for successful federal cybersecurity programs is timely and effective response to cybersecurity

incidents. It is acknowledged that policies and procedures help in establishing a consistent and effective incident response protocol. However, given the constant state of change regarding cybersecurity threats, policies and procedures cannot cover every possible threat scenario. As such, it is suggested that action learning, which has been proven to be effective in resolving real problems in real time, in addition to providing opportunities for learning through its inherent questioning and reflection process, could be effectively employed by U.S. federal organizations as part of their incident response procedures. Accordingly, it is recommended that future research focus on the applicability of action learning in quickly and efficiently resolving new and emerging cybersecurity incidents (Marquardt & Wadill, 2004).

7. The research findings present opportunities for U.S. federal cybersecurity culture change—and several different theories exist regarding approaches to organizational culture change. For example, Burke (2011) suggested that changing employee behavior is key to changing organizational culture. In contrast, Giddens (1984) recommended changing the organizational structure to effect culture change. Accordingly, additional research is recommended to determine the best approach to successfully execute a cybersecurity culture change initiative in the U.S. federal government. This research should include an exploration of the appropriate pace of cybersecurity culture change, to include analysis of a phased versus comprehensive approach.

Concluding Remarks

As history has taught us, cybersecurity incidents can be devastating to individuals, organizations, and nations. Unfortunately, the U.S. federal government has not been immune from this devastation. In fact, several recent examples of U.S. federal cybersecurity breaches have resulted in significant harm to the nation and its citizens.

It has been suggested that a stronger federal cybersecurity culture can help to avoid cybersecurity incidents. This study resulted in several recommendations for practice, which have the potential to enhance federal cybersecurity culture. In addition, the insights from this study have the potential to contribute to the advancement of the current literature concerning cybersecurity culture. Ultimately, the present study should provide a bridge between cybersecurity culture theory and its practical application.

This research effort has been successful in furthering the understanding of U.S. federal cybersecurity culture. The results of this research should serve as a guide for U.S. federal leaders in their efforts to establish a stronger cybersecurity culture. A stronger federal cybersecurity culture should enhance the protection of critical information technology assets and sensitive information. This is particularly important given the constantly changing state of cyberthreats faced by the U.S. federal government. Further, a stronger federal cybersecurity culture can help to avoid the excessive costs borne by U.S. taxpayers as a result of cybersecurity breaches. In conclusion, it is expected that this study should help to inform federal leaders in their ongoing efforts to establish a more holistic cybersecurity culture.

REFERENCES

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity, 4*(2), 104–107.

Arnold, R. (2017). *Cybersecurity: A business solution. An executive perspective on managing cyber risk*. Winston-Salem, NC: Threat Sketch.

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing, 41*(1), 22–28.

Baker, D. L. (2009). President Obama's chilling cybersecurity challenge: The new administration can reinvent the nation's cybersecurity to reduce risks, increase resiliency, and harness the advantages of the digital age. *Public Manager, 38*(1), 90–92.

Batteau, A. W. (2011). Creating a culture of enterprise cybersecurity. *International Journal of Business Anthropology, 2*(2), 36–47.

Beall, G. H. (2002). Exploratory research remains essential for industry. *Research Technology Management, 45*(6), 26–30.

Benamati, J., & Lederer, A. L. (2010). Managing the impact of rapid IT change. *Information Resources Management Journal, 23*(1), 1–16. doi:10.4018/irmj.2010102601

Bishop, M. (2003). What is computer security? *IEEE Security Privacy Magazine, 1*(1), 67–69.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks, CA: Sage.

Bradley, R. V., Pridmore, J. L., & Byrd, T. A. (2006). Information systems success in the context of different corporate cultural types: An empirical investigation. *Journal of Management Information Systems, 23*(2), 267–294. doi:10.2753/MIS0742-12222302011

Burgelman, R. A., & Doz, Y. L. (2001). The power of strategic integration. *MIT Sloan Management Review, 42*(3), 28–38.

Burke, W. (2011). A perspective on the field of organization development and change: The Zeigarnik effect. *Journal of Applied Behavioral Science, 47*(2), 143-167.

Castellano, J. F., Rosenzweig, K., & Roehm, H. A. (2004). How corporate culture impacts unethical distortion of financial numbers. *Management Accounting Quarterly, 5*(4), 37–41.

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *Journal of National Security Law & Policy, 4*(1), 27–39.

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438–458.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning, and Performance Journal, 24*(1), 1–14.

Chou, W. (2007). Cybersecurity costs: Balancing blanket security with real-world practicality. *IT Professional, 9*(2), 16–20. doi:10.1109/MITP.2007.30

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361–372. doi:10.1080/10580530701586136

Denison, D. R., & Mishra, A. K. (1995). Toward a theory of organizational culture and effectiveness. *Organization Science, 6*(2), 204–223.

Department of Homeland Security. (2009). *2009 Cyberspace policy review*. Retrieved from https://www.dhs.gov/publication/2009-cyberspace-policy-review

Dess, G. G., Ireland, R. D., Zahra, S. A., Floyd, S. W., Janney, J. J., & Lane, P. J. (2003). Emerging issues in corporate entrepreneurship. *Journal of Management, 29*(3), 351–378. doi:10.1016/S0149-2063(03)00015-1

Dillman, D. A. (2000). *Mail and internet surveys: The tailored design method* (2nd ed.). New York, NY: John Wiley.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review, 24*(3), 349–375. doi:10.1002/sdr.405

Ericsson, K. A., & Charness, N. (1994). Expert performance: Its structure and acquisition. *American Psychologist, 49*(8), 725–747.

Ericsson, K. A., & Lehmann, A. C. (1996). Expert and exceptional performance: Evidence of maximal adaptation to task constraints. *Annual Review of Psychology, 47*(1), 273–305.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352–357. doi:10.1108/09576050210447037

Gallivan, M. J. (1997). The importance of organizational culture fit: A technology implementation success story. *Failure and Lessons Learned in Information Technology Management, 1*(4), 243–257. doi:10.3727/108812897792232542

Gallivan, M., & Srite, M. (2005). Information technology and culture: Identifying fragmentary and holistic perspectives of culture**.** *Information and Organization, 15*(4), 295–338. doi:10.1016/j.infoandorg.2005.02.005

Ghernouti-Hélie, S., Tashi, I., & Simms, D. (2010). A multi-stage methodology for ensuring appropriate security culture and governance. In *2010 International Conference on Availability, Reliability and Security*, pp. 353–360. Piscataway, NJ: IEEE. doi:10.1109/ARES.2010.118

Giblin, E. J., & Amuso, L. E. (1997). Putting meaning into corporate values. *Business Forum, 22*(1), 14–18.

Giddens, A. (1984). *The constitution of society*. Los Angeles, CA: University of California Press.

Government Accountability Office. (2006). *Enterprise architecture: Leadership remains key to establishing and leveraging architectures for organizational transformation* (GAO-06-831). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/260/251127.pdf

Government Accountability Office. (2011). *Cybersecurity human capital: Initiatives need better planning and coordination.* Washington, DC: Author. Retrieved from https://www.gao.gov/products/GAO-12-8

Government Accountability Office. (2016). *Key issues: Cybersecurity*. Retrieved from http://www.gao.gov/key_issues/cybersecurity/issue_summary#t=0

Greenberg, A. (2013, December 16). An NSA coworker remembers the real Edward Snowden: 'A genius among geniuses.' *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/12/16/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/?partner=yahootix#13090d782da8

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257–278.

Harrington, S. J., & Guimaraes, T. (2005). Corporate culture, absorptive capacity and IT success. *Information and Organization, 15*(1), 39–63. doi:10.1016/j.infoandorg.2004.10.002

Hatch, M. J. (1993). The dynamics of organizational culture. *Academy of Management Review, 18*(4), 657–693. doi:10.5465/AMR.1993.9402210154

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Holstein, D. K. (2009). A systems dynamics view of security assurance issues: "The curse of complexity and avoiding chaos." *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences*, 1–9.

IEEE. (1998). IEEE guide for information technology—system definition—concept of operations (ConOps) document. *IEEEXplore*. Retrieved from https://ieeexplore.ieee.org/document/761853/ doi:10.1109/IEEESTD.1998.89424

Investopedia. (2016). Federal agencies. Retrieved from http://www.investopedia.com/terms/f/federal-agencies.asp#ixzz4MWVndmkH

Jackson, S. (2011). Organizational culture and information systems adoption: A three-perspective approach. *Information and Organization, 21*(2), 57–83. doi:10.1016/j.infoandorg.2011.03.003

Jackson, S., & Philip, G. (2010). A techno-cultural emergence perspective on the management of techno-change. *International Journal of Information Management, 30*(5), 445–456. doi:10.1016/j.ijinfomgt.2010.01.008

Jenlink, P. M. (2001, April). *Scholar-practitioner leadership: A critical analysis of preparation and practice.* Paper presented at the 2001 Annual Meeting of the American Educational Research Association, Session 39.55, Seattle, Washington.

Jenlink, P. M. (2006). *The school leader as bricoleur: Developing scholarly practitioners for our schools.* Retrieved from https://files.eric.ed.gov/fulltext/EJ1066733.pdf

Kesswani, J., & Kumar, S. (2015). Maintaining cyber security: Implications, cost and returns. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 161–164). New York, NY: ACM. doi:10.1145/2751957.2751976

Kummer, T. F., & Schmiedel, T. (2016). Reviewing the role of culture in strategic information systems research: A call for prescriptive theorizing on culture management. *Communications of the Association for Information Systems, 38*(article 5), 122–144. doi:10.17705/1CAIS.03805

Larkin, B. S. (2008). Increasing information integrity: Cultural impacts of changing the way we manage data. *International Journal of Organization Theory and Behavio*r, *11*(4), 558–578.

Lee, M. (2006). *The impact of IT investment, communication, innovation in participative budgeting systems on performance: Hotel industry in Taiwan as example*. Unpublished M.S. Thesis, Institute of Business Administration, National Dong Hwa University.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage.

Marquardt, M., & Wadill, D. (2004). The power of learning in action learning: A conceptual analysis of how the five schools of adult learning theories are incorporated within the practice of action learning. *Action Learning: Research and Practice, 1*(2), 185–202. doi:10.1080/1476733042000264146

Martin, J. (2002). *Organizational culture. Mapping the terrain*. Thousand Oaks, CA: Sage.

Martinsons, M. G., & Davison, R. (2003). Cultural issues and IT management: Looking ahead. *IEEE Transactions on Engineering Management, 50*(1), 113–117. doi:10.1109/TEM.2003.808299

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd ed.). Thousand Oaks, CA: Sage.

McFadzean, E., Ezingeard, J-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622–660.

Meeuwisse, R. (2017a). *Cybersecurity for beginners*. London, UK: Cyber Simplicity.

Meeuwisse, R. (2017b). *The cybersecurity to English dictionary.* Hythe, Kent, UK: Cyber Simplicity.

Melitski, J., Gavin, D., & Gavin, J. (2010). Technology adoption and organizational culture in public organizations. *International Journal of Organization Theory and Behavior, 13*(4), 546–568.

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation.* San Francisco, CA: Jossey-Bass.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: A sourcebook of new methods* (2nd ed.). Thousand Oaks, CA: Sage.

Nagesh, G. (2010, May 13). VA loses another laptop with veterans' personal data, prompting inquiry. *The Hill*. Retrieved from http://thehill.com/policy/technology/97817-va-loses-another-laptop-with-veterans-personal-information

National Academy of Science. (2013). *Professionalizing the nation's cybersecurity workforce? Criteria for decision-making.* Washington, DC: The National Academies Press.

National Initiative for Cybersecurity Education. (2012). *IT workforce capability assessment survey.* Arlington, VA: Author.

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity.* Gaithersburg, MD: Author. Retrieved from

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2017). *Framework for improving critical infrastructure cybersecurity.* Gaithersburg, MD: Author. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

Odintsova, S. A., Kenesova, N. T., & Sarsekeyeva, Z. E. (2013). Information technology: Definition, essence and content of the concept. *Education and Science Without Borders, 4*(7), 107–109.

Office of Management and Budget. (2008). *The comprehensive national cybersecurity initiative.* Retrieved from http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage.

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of Counseling Psychology, 52(2),* 126–136. doi:10.1037/0022-0167.52.2.126

Porter, M. E., & Miller, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review, 63*(4), 149–160.

Risen, T. (2015, October 2). Government is the biggest cybersecurity threat. *U.S. News & World Report*. Retrieved from http://www.usnews.com/news/blogs/data-mine/2015/10/02/surveys-government-is-the-biggest-cybersecurity-threat

Roberts, C. B. (1996). The impact of information technology on the management of system design. *Technology in Society, 18*(3), 333–355. doi:10.1016/0160-791X(96)00018-8

Rosenzweig, P. (2012, November 13). The alarming trend of cybersecurity breaches and failures in the U.S. government continues. *Heritage Foundation*. Retrieved from http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal, 42*(6), 32–34, 36–38.

Sakaguchi, T., & Dibrell, C. C. (1998). Measurement of the intensity of global information technology usage: Quantitizing the value of a firm's information technology. *Industrial Management & Data Systems, 98*(8), 380–394.

Schein, E. H. (1992). *Organizational culture and leadership* (2nd ed.). San Francisco, CA: Jossey-Bass.

Seidman, I. E. (1991). *Interviewing as qualitative research: A guide for researchers in education and social sciences*. New York, NY: Teachers College Press.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security, 3*(2), 20–26. doi:10.1108/09685229510792988

Stacey, T. R., Helsley, R. E., & Baston, J. V. (1998). *Identifying information security threats.* Retrieved from http://www.ittoday.info/AIMS/DSM/82-10-41.pdf

Sternstein, A. (2012, December 18). Costs mount as NASA responds to October data breach. *Nextgov.* Retrieved from

http://www.nextgov.com/cybersecurity/2012/12/costs-mount-nasa-responds-october-data-breech/60232/

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security, 6*(4), 167–173.

Vaughn, R. B., Henning, R., & Siraj, A. (2003). Information assurance measures and metrics: State of practice and proposal taxonomy. *Proceedings of the 36th Hawaii International Conference on System Sciences*. doi:10.1109/HICSS.2003.1174904

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. doi:10.1016/j.cose.2013.004

Weick, K. E., & Sutcliffe, K. M. (2011). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). San Francisco, CA: Jossey-Bass.

Wilshusen, G. C. (2010). *Cybersecurity: Continued attention is needed to protect federal information systems from evolving threats*. Washington, DC: Government Accountability Office. Retrieved from http://www.gao.gov/new.items/d10834t.pdf

Yu, F. T., & Kwan, D. S. (2015). Coevolution of culture and technology: The business success of Lee Kum Kee. *Global Business Review, 16*(1), 182–195. doi:10.1177/0972150914553529

APPENDIX A:

INITIAL EMAIL CONTACT LETTER

Date

Dear (Name of Research Participant):

I hope all is well with you. I'm writing as a Doctoral Student in George Washington University's Executive Leadership Development Program, with a request to interview you for my dissertation research. The purpose of this study is to explore federal cybersecurity culture.

This project involves interviewing federal cybersecurity experts to gain their perspective on cybersecurity culture. If you agree to be in this study, I would ask that you participate in an interview that would take about 90 minutes of your time. The interview will be conducted at your office, or a place of your convenience, and will be documented using handwritten notes and using a digital audio-recording device. The recording will be used for transcription purposes only. However, the information obtained from the interview will be held in strictest confidence, and you will not be identified in the final research report. The interview would revolve around the following areas:

1. What is and what should be the cybersecurity culture in U.S. federal organizations?
2. What are the similarities in cybersecurity culture in U.S. federal organizations?
3. What are the differences in cybersecurity culture in U.S. federal organizations?
4. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?
5. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

Taking part in this research project is completely voluntary. If you decide to participate, you are free to withdraw at any time. As noted previously, the information obtained from the interview will be held in strictest confidence, and you will not be identified in the final research report. Audiotapes and transcriptions and notes will be locked in a file cabinet accessible only to the principal investigator. Your records will be used for research purposes only. At the end of the study, all research records will be destroyed.

I truly hope that you are willing to participate in my study. Please know that your participation in this study is completely voluntary and that you can discontinue your participation at any time without loss of the rights and benefits to which you are entitled. I know that you would make a substantial contribution to understanding federal cybersecurity culture. This work should be of great value to organizations interested in furthering their cybersecurity culture.

Please let me know if you are willing to participate in this study. Doing so via email will serve as your agreement to participate in the study. I will then coordinate the details of the interview directly with you or with a designee. Should you have questions about this study, please feel free to contact me by email (rsousane@gwu.edu) or phone at (xxx) xxx-xxxx.

Thanks again!

Sincerely,

Rick Sousane

APPENDIX B:

INFORMED CONSENT FORM

I. INTRODUCTION

You are invited to take part in a research study to explore core elements of federal cybersecurity culture. Before you decide to be a part of this study, you need to understand the risks and benefits. This consent form provides information about the research study. I will be available to answer your questions and provide further explanations. If you agree to take part in the research study, you will be asked to sign this consent form. This process is known as informed consent. Your decision to take part in the study is voluntary. You are free to choose whether or not you will take part in the study.

II. PURPOSE

The purpose of this study is to explore the elements of federal cybersecurity culture. The principal and sole investigator is Rick Sousane, Doctoral Candidate at George Washington University.

III. PROCEDURES

This project involves interviewing cybersecurity leaders to gain their perspective. If you agree to be in this study, I would ask that you participate in an interview that would take about an hour of your time. The interview would revolve around the following areas:

1. What is and what should be the cybersecurity culture in U.S. federal organizations?
2. What are the similarities in cybersecurity culture in U.S. federal organizations?
3. What are the differences in cybersecurity culture in U.S. federal organizations?
4. How is cybersecurity culture developed, demonstrated, and sustained in U.S. federal organizations?
5. How would an ideal cybersecurity culture in U.S. federal organizations be developed, demonstrated, and sustained?

With the participant's permission, the interviews may be tape-recorded. The interviews will then be transcribed into written text, as it is considered the most practical way to analyze interviews.

IV. RISKS

The things you will be doing have no more risk of harm than you would experience in everyday life.

V. COSTS & COMPENSATION BENEFITS

There are neither any costs nor compensation involved if you participate in this research project, and there are no anticipated direct personal benefits.

VI. RIGHT TO WITHDRAW FROM THE STUDY

Taking part in this research project is completely voluntary. If you decide to participate, you are free to withdraw at any time.

VII. PRIVACY OF RESEARCH RECORDS

The information obtained from the interview will be held in strictest confidence, and you and your workplace will not be identified in the final research report. Any audiotapes, transcriptions, and notes developed as part of this study will be locked in a file cabinet accessible only to the principal investigator. Research records will only be used for research purposes and will not have any information that can be linked directly to you or your workplace. At the end of the study, all research records will be destroyed.

VIII. QUESTIONS

Should you have questions about this study, please feel free to contact me by email (rsousane@gwu.edu) or by phone at (xxx) xxx-xxxx.

IX. SIGNATURES

By signing this consent form, you agree that you have read this informed consent form, you understand what is involved, and you agree to take part in this study. You do not give up any of your legal rights by signing this informed consent form. You will receive a copy of this consent form.

_____

Participant (Print Name)

_____

Signature

_____

Date

X. RESEARCHER STATEMENT

I certify that the research study has been explained to the above individual by me or my research staff including the purpose, the procedures, the possible risks, and the potential benefits associated with participation in this research study. Any questions raised have been answered to the individual's satisfaction.

_____

Investigator (Print or type name)

_____

Signature

_____

Date

APPENDIX C:

INTERVIEW GUIDE

Understanding Federal Cybersecurity Culture:
An Expert Perspective on Current and Ideal State

Date of Interview: _____
Time: _____
Place: _____
Participant Number: 1 of XX

Thank you for agreeing to spend this time with me. You will be assigned a participant number, and your responses will be kept confidential. This interview will be digitally recorded for the purposes of transcribing and analyzing the data for use in my dissertation. You may stop the interview at any time, for any reason. I will be requesting your name and relevant demographic information to validate your status as a cybersecurity expert. However, I will be the only person with access to the key that connects you to the interview transcript. Further, I will edit any identifying information from the interview transcript. You will also have an opportunity to review the transcript to ensure it accurately reflects your comments. During the interview, please refer to specific people by title and not proper name. Don't worry if you accidentally forget this because I will edit the identifying information from the transcript.

To begin our interview, I would like you to know that my research interest is in understanding U.S. federal cybersecurity culture. While it is clear that the development of cybersecurity culture has become a heightened focus for many federal organizations, it is not clear what should constitute the core elements of cybersecurity culture. Accordingly, the purpose of this study is to contribute to the understanding of federal cybersecurity culture, its uniqueness, importance, and benefits.

This research effort will center on a mix of cybersecurity experts, from federal organizations, with an emphasis placed on more clearly defining federal cybersecurity culture. In exploring expert views of cybersecurity at these federal organizations, it is expected that convergences and divergences in cybersecurity culture will be identified. The results of this research should also have a positive impact on the efforts of federal organizations to establish a strong posture against cybersecurity threats. Ultimately, this study should help to inform federal leaders in their ongoing efforts to establish a more holistic cybersecurity culture.

As a participant in the research study entitled "Understanding Federal Cybersecurity Culture: An Expert Perspective on Current and Ideal State," you will be asked to answer a few questions about your background and previous experiences. These questions are intended as a guide. The interview can explore other aspects of your perspective that you think are particularly relevant to the study.

Questions

Question 1: Please provide your name, the current organization you work for, your current title/role, years of cybersecurity (IT security) experience, previous cybersecurity (or IT security) position/roles, area(s) of cybersecurity expertise, highest educational degree, and any security certifications you may have.

Question 2: I am trying to understand how your organization approaches cybersecurity.

a. Please describe the general nature of the cybersecurity policies at your organization and how they are enforced. What do you consider to be the strengths and weaknesses of your organization's approach to cybersecurity?
b. How is cybersecurity conveyed to workers or promoted within your organization? If I walked around the organization's working areas, would I see physical things that relate to cybersecurity? What would I see?
c. Do you follow requirements set by another organization and do you have any latitude for local modifications?
d. What role do procedures, training, and technologies play in your organization's approach to cybersecurity?
e. What challenges do you see with compliance? How do they concern you? How have you become aware of these challenges? If I were to ask employees about their concerns with the approach to cybersecurity, what would they tell me?
f. Do you monitor cybersecurity performance or compliance? What metrics or tools do you have? Are there tools that would improve network security monitoring?
g. How are cybersecurity problems resolved in your organization? Can you give an example of a cybersecurity problem and what you learned from it?
h. If you could make one change to significantly improve your cybersecurity posture not related to hardware, what would it be and why?

Question 3: I also want to learn about your perception of cybersecurity based on work you do with other federal organizations.

a. Is there a formal way to learn about problems and share best practices with other federal organizations? Describe how you use this.
b. What do you know about the approach these organizations take with regard to cybersecurity? Are their standards common to all federal entities to include rules, regulations, policies, procedures, technologies, etc.? From where do these standards originate? Do you see any differences in how other organizations approach compliance? What have you learned from other federal organizations?
c. Are federal cybersecurity goals and accomplishments formally published? If so, please describe how this is accomplished and what follow up exists. Do you think this is effective?
d. Would you do anything differently to improve federal cybersecurity posture across organizations?

Question 4: In order for me to understand the approach of federal organizations to cybersecurity and challenges therein, is there anything else you would like to tell me or think I should have asked?

This concludes my list of prepared questions. Do you have any questions for me or other information you would like to add? If not, thank you for your participation.