

UNAUTHORIZED DISCLOSURES OF SENSITIVE AND CLASSIFIED INFORMATION:
A META-SYNTHESIS OF LEADERSHIP SUPPORT, SECURITY POLICY, AND
SECURITY EDUCATION, TRAINING AND AWARENESS WITHIN THE
FEDERAL GOVERNMENT INFORMATION SECURITY CULTURE

by

CALVIN J. SIMPSON

A DISSERTATION

Submitted in partial fulfillment of the requirements for the degree
of Doctor of Education in Educational Leadership
in the Doctoral Program of
Delaware State University

DOVER, DELAWARE
May 2019

This dissertation is approved by the following members of the Final Oral Review Committee:

Dr. Richard Phillips, Committee Chair, Education Department, Delaware State University
Dr. Patricia Carlson, Committee Member Education Department, Delaware State University
Dr. Joseph Falodun, Committee Member, Education Department, Delaware State University
Dr. Sae Yeol Yoon, Committee Member, Education Department, Delaware State University
Dr. Michelle Ennis, External Committee Member, Department of Accounting and Legal Studies,
Salisbury University

© Calvin J. Simpson

All Rights Reserved

DEDICATION

“The discipline which makes the soldiers of a free country reliable in battle is not to be gained by harsh or tyrannical treatment. On the contrary, such treatment is far more likely to destroy than to make an army. It is possible to impart instructions and to give commands in such a manner and in such a tone of voice to inspire in the soldier no feeling but an intense desire to obey, while the opposite manner and tone of voice cannot fail to excite strong resentment and a desire to disobey. The one mode or other of dealing with subordinates springs from a corresponding spirit in the breast of the commander. He who feels the respect which is due others cannot fail to inspire in them regard for himself; while he who feels, and hence manifests, disrespect toward other, especially his inferiors, cannot fail to inspire hatred against himself.”

Major General John M. Schofield
Address to the Corps of Cadets, U.S. Military Academy
11 August, 1879

To my family and friends who have encouraged me throughout this journey. A special feeling of gratitude to my loving parents, Calvin and Sharon, whose words of encouragement always resonated. The greatest appreciation to my true love, Angie, whose prayers for me were heard and answered. An unparalleled gratefulness to my children and their spouses, Calvin and Alaina, Kourtney, Chris and Katrina, and Carlin and Alexis, for encouraging, motivating, and believing in me to achieve.

This dissertation is also dedicated to the many security professionals who work tirelessly to safeguard our nation’s sensitive and classified information, contributing to national security.

ACKNOWLEDGEMENTS

I am deeply indebted to my supervisor, Edward “Ed” Wuyscik, whose unquestionable support of my career goals and never-ending willingness to accommodate my academic desires are truly appreciated. This research would not have been possible without Ed’s unwavering flexibility and support. I am especially indebted to Dr. Richard Phillips, chairman of my dissertation committee, whose tutelage challenged me, guided me, and educated me through the entire journey. Dr. Phillips has taught me much more than I knew about myself and much more than I could ever give him credit for. A special thanks to the members of my dissertation committee, Dr. Carlson, Dr. Falodun, Dr. Yoon, and Dr. Ennis, who were more than generous with their expertise and valuable time. My committee members have provided me with extensive personal and professional guidance, while teaching me a great deal about scholarly research. I am also grateful to all of those with whom I have had the pleasure to work with during this journey. Last, but not least, my deepest appreciation to my family, co-workers, and friends for encouraging and inspiring me to pursue and achieve something previously thought unreachable.

**Unauthorized Disclosures of Sensitive and Classified Information: A Meta-Synthesis
of Leadership Support, Security Policy, and Security Education, Training and
Awareness within the Federal Government Information Security Culture**

Calvin J. Simpson

Committee Chairperson: Dr. Richard Phillips

ABSTRACT

This meta-synthesis study examined federal government information security culture through the factors of leadership support, security policy, and security education, training, and awareness (SETA). The occurrence of unauthorized disclosures is a continuing and increasing problem within the federal government, and end-users are identified as the weakest link. The federal government not only remains unsuccessful in its efforts to prevent unauthorized disclosures in previous years, it acknowledges this threat will persist in the future. Selection of studies used in support of this meta-synthesis consisted of two subject matter experts who served as raters that determined inter-rater agreement. Inter-rater reliability was achieved using the Cohen's Kappa equation while ATLAS.ti 8 supported the semantic coding process. Semantic coding of the 13 studies used in this research resulted in the identification of 4 networks consisting of 36 total nodes (5 - information security culture, 13 - leadership support, 7 - security policy, and 10 - SETA). There was a total of 398 total sub-nodes selected across selected studies. The findings indicate that the greatest positive influences on information security culture and end-user threat-response behaviors were leadership support and SETA. However, these influences are offset by employee behavioral conflicts, inconsistent leadership involvement, varying degrees of policy awareness and non-compliance, and ineffective training.

An emphasis on teamwork was noted at all levels across the federal government. There was an overwhelming consensus for tighter controls to protect information. In the area of policy, there is an admitted lack of awareness for the policies, consequences, and penalties associated with security violations. To prevent the occurrence of future security incidents, a better understanding of information security culture within the federal government is needed to assist in further refining and implementing organizational information security programs. This study separates itself from other studies by presenting a new research model supported by a theoretical framework.

TABLE OF CONTENTS

List of Tables	viii
List of Figures	ix
List of Abbreviations	x
Chapter I: Overview of the Study	1
1.1. Introduction.....	1
1.2. Background of the Problem	4
1.3. Statement of the Problem.....	17
1.4. Purpose of the Study	19
1.5. Research Questions.....	20
1.6. Theoretical Framework.....	22
1.7. Significance of the Study.....	26
1.8. Definition of Terms	30
1.9. Limitations	36
1.10. Delimitations.....	38
1.11. Ethical Issues	40
1.12. Summary	41
Chapter II: Literature Review.....	43
2.1. Introduction.....	43
2.2. Factor Literature Review	44
2.3. Leadership Support	50
2.4. Security Policy	52
2.5. Security Education, Training, and Awareness.....	56
2.6. Quantitative Research Models	61
2.7. Summary	85
Chapter III: Research Methods.....	87
3.1. Introduction.....	87
3.2. Research Design	88
3.3. Participants.....	91
3.4. Qualitative Tools	94
3.5. Inter-Rater Reliability	94
3.6. Data Analysis	96
3.7. Method	96
3.8. Risks and Benefits	107

3.9. Ethical Assurances	107
3.10. Assumptions	108
3.11. Summary	109
Chapter IV: Findings	110
4.1. Introduction.....	110
4.2. Literature Search.....	111
4.3. Inter-Rater Agreement	116
4.4. Inter-Rater Reliability	119
4.5. Semantic Coding.....	121
4.6. Summary	141
Chapter V: Conclusion	143
5.1. Introduction.....	143
5.2. Discussion	144
5.3. Implications	149
5.4. Recommendations.....	151
5.5. Conclusion	156
References	158
Appendices	177
6.1. Appendix A.....	178
6.2. Appendix B	179
6.3. Appendix C	180
6.4. Appendix D.....	181
6.5. Appendix E	182
6.6. Appendix F	183
6.7. Appendix G.....	184
6.8. Appendix H.....	185
6.9. Appendix I	186

LIST OF TABLES

Table 1: The Number of Employees Eligible (In-Access) for FY14 and FY15	8
Table 2: The Number of Employees Eligible (Not In-Access) for FY14 and FY15	9
Table 3: Total Number of Employees Eligible for FY14 and FY15FY14 and FY15	9
Table 4: Cited theories from pervious security-related literature	22
Table 5: Organizational Climate Definitions	44
Table 6: Information Security Culture Definitions	46
Table 7: Types of qualitative meta-synthesis.....	89
Table 8: National Guard / Reserve Strength	92
Table 9: Active Duty Strength	92
Table 10: DoD Civilian Strength	92
Table 11: DoD Military and Civilian Employee Grand Total	93
Table 12: Active Duty and Reserve Demographics.....	93
Table 13: Inclusion/Exclusion Evaluation Matrix	113
Table 14: Research Question Screening Tool.....	115
Table 15: Inter-Rater Agreement Table	117
Table 16: Inter-Rater Agreement Matrix	118
Table 17: Inter-Rater Reliability Rating Matrix	119
Table 18: Code Document Table	122

LIST OF FIGURES

Figure 1: Per capita cost by industry classification.	5
Figure 2: Total FOIA requests received by the federal government between 2013-2017.....	13
Figure 3: Security compliance research model.....	61
Figure 4: Security compliance intention research model.....	64
Figure 5: Fear appeals research model.	67
Figure 6: Individual security behavior research model.	68
Figure 7: Protective security behavior continuance research model.	70
Figure 8: The recomposed TPB research model.....	73
Figure 9: Organizational information security key factors research model.....	75
Figure 10: Comprehensive information security culture research model.....	77
Figure 11: Contributors to security culture research model.	81
Figure 12: Extended general deterrence theory research model.....	83
Figure 13: Search, retrieval, and validation process.....	101
Figure 14: Appraisal criteria for assessing quality of qualitative research process.....	104
Figure 15: Consolidated network diagram.....	123
Figure 16: Information security culture network.....	124
Figure 17: Leadership support network.	128
Figure 18: Security policy network.	133
Figure 19: SETA network.....	137
Figure 20: Proposed federal government information security culture model	156

LIST OF ABBREVIATIONS

CIPA	Classified Information Procedures Act
CMI	Classified military information
CT	Compliance theory
COMSEC	Communications security
CUI	Controlled unclassified information
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoJ	Department of Justice
DMDC	Defense Manpower Data Center
DNI	Director of National Intelligence
FOIA	Freedom of Information Act
GAO	Government Accounting Office
GDT	General deterrence theory
INFOSEC	Information security
ISCA	Information security culture assessment
ISSP	Information systems security policy
IT	Information technology
IS	Information system
MT	Mosaic theory
OCAI	Organizational cultural assessment instrument
PKI	Public Key Infrastructure
POS	Theory of perceived organizational support

SBU	Sensitive but unclassified
SBT	Social bond theory
SCG	Security classification guide
SCT	Social cognitive theory
SET	Social exchange theory
SPSS	Statistical Package for the Social Sciences
SETA	Security education, training, and awareness
TRA	Theory of reasoned action
TPB	Theory of planned behavior
USD	Under Secretary of Defense

CHAPTER I: OVERVIEW OF THE STUDY

1.1 Introduction

The unauthorized disclosure of classified military information (CMI) and controlled unclassified information (CUI) places our citizens, military, and nation at unnecessary risk, and at times has resulted in the loss of lives. Unauthorized disclosures of CMI and CUI divulge government secrets and weaken the government's ability to manage and control the accountability of CMI and CUI (DIA, 2014; Papandrea, 2014). Unauthorized disclosures also threaten America's safety and security by causing potentially long-lasting, grave, and irreversible harm in the government's ability to contend with and react to the numerous threats and adversaries. The occurrence of unauthorized disclosures is a continuing and increasing problem within the federal government, with end-users identified as the weakest link (Fujii, Sato, Yamauchi, & Taniguchi, 2016; Lutkenhaus, 2014; U.S. Government Accounting Office (GAO), 2015). As the growing complexity of technology and the availability of automated systems increases, the extent and threat of unauthorized disclosures intensifies. The federal government not only remains unsuccessful in its efforts to prevent unauthorized disclosures in previous years, it acknowledges the threat will persist for years to come. As noted over the previous three years in the Director of National Intelligence (DNI), Statement for the record: Worldwide Threat Assessment of the US Intelligence Community, "trusted insiders who disclose sensitive or classified U.S. Government information without authorization will remain a significant threat in 2018 and beyond." (DNI, 2016, p. 10; DNI, 2017, p. 10; DNI, 2018, p. 11).

There is no single demographic within the federal government that is responsible for unauthorized disclosure. Senior executives, servicemembers, and low-level government contractor contribute to unauthorized disclosures that address a myriad of subject matter (Barton,

2016). In 2015, former CIA director David Petraeus pleaded guilty to illegally disclosing classified documents and was sentenced to two years of probation and fined \$100,000 (GAO Report to Congressional Committees: Many High-Risk Areas (2017)). In 2013, Edward Snowden, a former National Security Agency defense contractor employee, disclosed 1.7 million classified documents to foreign and domestic news outlets. Snowden was subsequently charged with multiple counts of espionage, “theft of government property, unauthorized communication of national defense information, and willful communication of classified communications intelligence information to an unauthorized person” (Bakken, 2013; Barton, 2016; Kasner, 2015; The Surveillance State and its Discontents, 2013). In May 2010, Bradley (Chelsea) Manning, a U.S. Army Intelligence Analyst, was convicted for disclosing approximately 750,000 pages of classified documents and videos, and subsequently sentenced to 35 years in prison (Bakken, 2013; Maxwell, 2015). In two of the three aforementioned cases, the impact to national security still remains unknown and are among the largest known cases of unauthorized disclosure in American history (U.S. GAO, 2015). These examples not only highlight some of the more prominent unauthorized disclosures, they also provide clear evidence for attributing the responsibility of unauthorized disclosures within multiple levels of the federal government. Additionally, there are countless other unauthorized disclosures that have occurred and are not reported through official channels, or the government does not release to the general public. Hence, the occurrence of this ongoing problem underscores the importance of creating a more effective, efficient, and secure organizational information security culture that places the handling of CMI and CUI at the forefront.

The handling of CMI and CUI occurs within the public sector (i.e., local, state, and federal government organizations), private sector (i.e., defense contractors), and to a somewhat

lesser extent, the volunteer sector (i.e., non-profit organizations). Previous research addressing mitigations for unauthorized disclosure generally encompasses two broad areas. The first involves a technology-based approach that focuses on the development of innovative technology and software applications for information systems that aim to negate vulnerabilities and mitigate the effects of adversarial attacks. The second encompasses a human-based approach that seeks to deter individuals within the organization from initiating unauthorized disclosures. According to Tang, Li, and Zhang (2016), the human factor is increasingly recognized as a more critical issue than technology when considering unauthorized disclosures. The scope of this meta-synthesis will address the human-based aspect of information security culture within the public sector by examining key information security culture factors (security policy, leadership support, and security education, training, and awareness (SETA) within the federal government.

The organization of this chapter describes the problem background from a top-down approach, then by each information security culture factor. First, a problem statement discusses continued challenges that suggest a need for this research. Second, the study purpose, central question, and supporting sub-questions provide a focus for this research. Third, general deterrence theory (GDT), theory of perceived organizational support (POS), social exchange theory (SET), and mosaic theory (MT) constitute the theoretical framework for this research. Fourth, the importance of this research is discussed in terms of benefit from increased awareness of organizational information security culture. Fifth, the limitations, delimitations, and ethical issues are provided to recognize the parameters associated with this research. Sixth, a list of definitions for terms specific to this research ensures a common understanding of content. Chapter I concludes by describing the organization of subsequent chapters for ease of navigating this study. This study intends to provide valued findings on information security culture that

actively support developing and implementing of an effective information security culture for organizations within the federal government.

1.2 Background of the Problem

Global. The impact of globalization on information security is tremendous. According to Livanis (2016), the widespread use of information technology has increased the pace of interconnectedness and remains embedded in almost every facet of our globalized world. Globalization has given rise to the cross-border transfer of information across the World Wide Web and is accompanied by an equally significant degree of security risks associated with the protection of CMI and CUI. Based on current trends, threats to information security will continue and evolve into considerably more complex challenges in the future. Wibowo and Batra (2010) and Fitzpatrick and DiLullo (2013) suggest the implementation of policies, procedures, and technical controls to ensure acceptable levels of information security. Therefore, it is essential stakeholders implement and enforce protocols by protecting data and ensuring equity of information security for those authorized access. When viewing unauthorized disclosures from a globalized perspective, Key findings from the global state of information security survey (2018) encompassed 419 companies across 17 countries (United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, South Africa, United Arab Emirates, Saudi Arabia, Singapore, Indonesia, the Philippines and Malaysia) and revealed an average total cost of \$3.62 million per data breach. Additionally, the frequency, number, and scope of data breaches have also increased from previous years. Organizational leaders should prepare for continued security incidents, as the study indicates an estimated 27.7 percent of participating organizations can expect to experience an unauthorized disclosure in the next two years. The consequence management cost associated with post-security incident cleanup can

include physical or automated assistance, notifications to personnel involved, investigations, legal fees, identity protection, and hardware/software remediation. The United States and Canada pay the highest post-security incident cleanup costs, while India and Brazil cleanup costs are the least expensive of surveyed countries. In addition, the United States, United Arab Emirates, and Saudi Arabia pay out the highest post-security incident notification costs. In a listing of 17 industrial categories, health care (#1) and financial services (#2) were the most prone to security incidents. Surprisingly, the technology (#6), communications (#8), and research (#16) industries had the lower average costs per incident. Figure 1 shows the per capita cost for all 17 industrial categories.

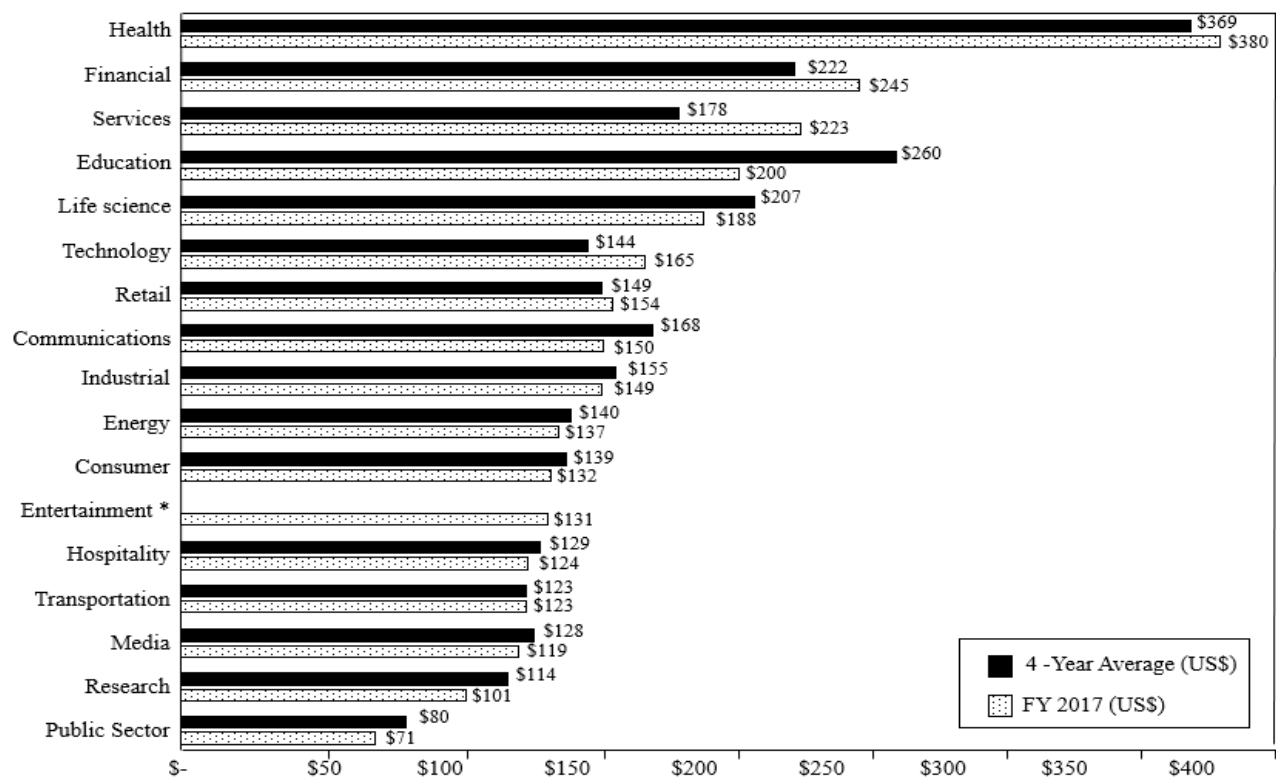


Figure 1. Per capita cost by industry classification.

Data reflect 4-year averages per category and the 2017 total cost per category. A critical take away from the study is that almost half (47%) of all organizations represented attribute security

incidents to hackers and insider threats, to which the United States and Canada expend the greatest amount of resources to resolve.

According to research findings, human error is the primary contributor to information security incidents (Millar, 2006; Shelton, 2014; Chen, Ramamurthy, & Wen, 2015; and New research: most companies fault employees for data breaches, 2011). A study of 709 information technology (IT) professionals assessed insider threats - includes intentional and unintentional - as the source of most organizational security incidents that occurred within the last 24 months. The primary cause of incidents includes loss of property [mobile, hand-held, and removable computing devices at 35%, third-party misappropriation at 32%, and hardware/software mishaps at 29%. Surprisingly, only 19% of employee-initiated incidents were assessed as being reported, while two-thirds of employees believe internal audits and assessments are only 36% effective (New research: Most companies fault employees for data breaches, 2011).

Federal. To understand the breadth and scope of managing CMI and CUI documents within the federal government, it is important to acknowledge that in the American post-911 environment the number of CMI documents (confidential, secret, and top-secret) the government manages has grown exponentially. To put things in perspective, Shapiro (2007) indicates the federal government classified 5.8 million documents in 1996. By 2005, the figure aggressively surged to 14.2 million classified documents. These numbers only account for documents deemed classified by an approved classifier and do not account for the masses of hard copy and digital documents subsequently derived through derivative classification, compilation, duplication, or reproduction.

Although the classification and handling of CUI information is distinctly separate from the traditional government classification and handling standards for CMI, the unauthorized

release of CUI also poses a risk. The federal government has taken great steps to identify and safeguard CUI. Executive Order 13556 (2010) governs CUI and encompasses 18 categories of controlled information.

- Critical Infrastructure
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- NATO
- Natural and Cultural Resources
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Statistical
- Tax
- Transportation

As such, the totality of CUI documents managed by the federal government is greater in number than that of classified documents, thus poses a greater degree of security risk when managing. Additionally, a parallel importance that needs distinguishing is that CUI differs from CMI in that the potential impact to national security from unauthorized disclosure of CUI is a lesser degree of damage.

According to the GAO, Report to Congressional Committees (2017), approximately 4.2 million federal employees (military, civilian, and defense contractors) possessed or were eligible to possess a security clearance during the fall of 2015. A Director of National Intelligence (DNI), annual report on security clearance determinations (DNI, 2015) provides corroborating support by citing the number of federal government and contractor employees eligible to handle classified information at 4,514,567 in fiscal year 2014 (FY14) and 4,249,053 in FY15 (a 5.9%

decrease). Concurrently, it is important to understand that eligibility does not equal access. Although an employee may be eligible to handle classified information, approval for access to such information is conditional upon three conditions. The conditions for determining access include a need-to-know, a signed non-disclosure agreement, and the appropriate level of eligibility that is based on a security clearance investigation. Of the 4,249,053 employees cited as eligible during FY 2015, only 2,865,402 met access requirements – a 63,074 (6.6%) decrease from 2,927,476 in FY14. Tables 1-3 highlight eligibility and security clearance access levels for government and defense contractors from FY14 to FY15.

Table 1

Employee type	As of 10/1/14:		As of 10/1/15:	
	Conf/secret	Top secret	Conf/secret	Top secret
Government	1,307,183	144,155	1,191,382	124,287
Contractor	40,699	20,127	44,868	17,690
Other	69,993	5,003	4,596	828
Sub-total:	1,417,815	169,285	1,240,846	142,805
Total:	1,587,100		1,383,651	

The Number of Employees Eligible (In-Access) for FY14 and FY15

Note. Eligible (in access), refers to individuals who were investigated and adjudicated favorably and were briefed into access to classified information. Adapted from "National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations," by Director of National Intelligence, National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations (2015).

Table 2

Employee type	As of 10/1/14:		As of 10/1/15:	
	Conf/secret	Top secret	Conf/secret	Top secret
Government	2,412,126	771,151	2,261,587	746,836
Contractor	483,185	456,700	478,227	445,759
Other	212,375	179,039	145,756	170,888
Sub-total:	3,107,686	1,406,890	2,885,570	1,363,483
Total:	4,514,576		4,249,053	

The Number of Employees Eligible (Not In-Access) for FY14 and FY15

Note. Eligible (not in access), refers to individuals, such as those supporting the military, that may be determined eligible due to the sensitivity of their positions and the potential need for immediate access to classified information, but may not have actual access to classified information until the need arises. Adapted from "National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations," by Director of National Intelligence, National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations (2015).

Table 3

Total Number of Employees Eligible for FY14 and FY15

Note. Total Eligibility, refers to individuals who were investigated and adjudicated favorably and had

Employee type	As of 10/1/14:		As of 10/1/15:	
	Conf/secret	Top secret	Conf/secret	Top secret
Government	1,104,943	626,996	1,070,205	622,549
Contractor	442,486	436,573	433,359	428,069
Other	142,442	174,036	141,160	170,060
Sub-total:	1,689,871	1,237,605	1,644,724	1,220,678
Total:	2,927,476		2,865,402	

access to classified information as well as those who were favorably adjudicated but did not have access to classified information. Adapted from National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations, by Director of National Intelligence, National Counterintelligence and Security Center: 2015 Annual Report on Security Clearance Determinations (2015).

When considering the overwhelming task of managing the sheer number of CMI documents, CUI documents, and the personnel with access to those documents, the importance of creating a positive information security culture becomes readily apparent. According to Lutkenhaus (2014), all information that is government-owned, government-produced, or government-held is considered government property, and is therefore subject to all government

protocols put in place to safeguard such information and ensure an adequate information security culture.

Weaver (2017) connotes human causes of unauthorized disclosures of CMI are not new. For decades, some of our nation's most highly guarded secrets have found their way into the hands of adversaries. The Director of National Intelligence: Worldwide Threat Assessment of the U.S. Intelligence Community (2018) states “trusted insiders who disclose sensitive or classified U.S. Government information without authorization will remain a significant threat in 2018 and beyond” (p. 11). As the complexity and convenience of IT systems increases the extent and consequence of unauthorized disclosures and will continue to exacerbate this challenge. According to Fujii, Sato, Yamauchi, and Taniguchi (2016), 57% of known security incidents result from improper handling and mismanagement. With various worldwide data collection methods, the amount of classified information within the federal government increases daily. As the volume and sensitivity of CMI and CUI becomes increasingly more valuable, the need to prevent unauthorized disclosures also increases exponentially. With such a vast and annually increasing volume of CMI and CUI, coupled with the number of personnel eligible for access to CMI and CUI, efforts to ensure secrecy are not infallible when creating an information security culture for personnel who possess a security clearance (Aftergood, 2010).

Leadership support. Both leaders and subordinates are responsible for promoting the proper handling of CMI and CUI. Shelton (2014) notes an obvious failure of people to comply with information security policies. Although employees may understand security requirements, some view security requirements as conflicting with work efforts, as opposed to supplementing work. This, in turn, leads to the human element as a discriminator for selective implementation of policy and protocols. Concurrently, Rutherford (2014) attributes some degree of culpability to

leaders as the source of security incidents in organizations. Leaders must find a balance between subordinate information security education, training, and awareness and promoting organizational values that drive organizational culture. While end-users may be considered the weakest link because of their human element, they simultaneously serve as the vital last of defense for preventing unauthorized disclosures (Aloul, 2012; Parsons, McCormac, Butavicius, & Ferguson, 2010; Rutherford, 2014; Dahbur, Bashabsheh, & Bashabsheh, 2017). The onus is on the leadership to establish a positive tone for the work environment that directly contributes to valued end-user security education and compliance intent with existing information security policy.

Security policy. The federal government goes to great lengths to document policies that ensure the safeguarding of sensitive and classified information by end-users. Potential impacts from the unauthorized disclosure of sensitive information may counter U.S. infrastructure, financial, economic, social, military, and foreign efforts. A study conducted by Escaleras and Register (2010) addresses transparency in that the federal government implements protocols that require the appropriate reviews and approvals prior to the public disclosure of sensitive information. The Classified Information Procedures Act (CIPA), Freedom of Information Act (FOIA), and internal public release approval processes struggle to regulate the disclosure of CMI and CUI while seeking a balance between transparency and national security (Chandran, 2015; Escaleras, Lin, & Register, 2010; MacDougall, 2014; Radsan, 2010).

The CIPA (1980) serves as a control mechanism for prosecuting federal cases that involve classified information. Some of the well-known cases involving espionage (Aldrich Ames, Robert Hanssen, and Harold Nicholson) and terrorism (Zacarias Moussaoui) have tested the government's protection of sources and methods when the intelligence gathered is essential

for prosecution. The challenge with these cases lies in a three-way clash between source protection, transparency, and American justice. Any potential of public disclosure during legal proceedings poses a legal dilemma for the judicial system. The implication is balancing disclosure with defendant rights when exculpatory evidence is critical to proceedings (Radsan, 2010; MacDougall, 2014; and Chandran, 2015).

The FOIA (1996) aims to balance the right of the public to know and the need of the Government to keep information in confidence to the extent necessary without permitting indiscriminate secrecy. According to Escaleras, Lin, and Register (2010, p 7), establishing a full and even balance consists of:

- 1) Promoting an informed population that can hold the Government accountable, and
- 2) Defending legitimate privacy and national security interests.

Since the FOIA policy overwhelmingly supports disclosure, narrow interpretations of its legal exemptions require interpretation, especially when resolving all doubts in support of openness (Zamaray, 2010). The FOIA grants the right for any American to request information from any government entity and is frequently referred to as “the law that keeps citizens informed of government activities” (DOJ, FAQ, 2018, p. 16). The FOIA requires agencies within the federal government disclose any information requested provided the information does not conform to one of the nine stated exemptions. The nine exemption categories that authorize government agencies to withhold information are (DOJ, FAQ, 2018).

Exemption 1: Information that is classified to protect national security.

Exemption 2: Information related solely to the internal personnel rules and practices of an agency.

Exemption 3: Information that is prohibited from disclosure by another federal law.

Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged.

Exemption 5: Privileged communications within or between agencies.

Exemption 6: Information that, if disclosed, would invade another individual's personal privacy.

Exemption 7: Information compiled for law enforcement purposes.

Exemption 8: Information that concerns the supervision of financial institutions.

Exemption 9: Geological information on wells.

Exemptions under these categories are made for executive and legislative agencies. Analysis of federal government FOIA requests over previous five years indicates between 53,160 and 67,679 were processed annually (Aftergood, 2010; Escaleras, Lin, & Register, 2010; Castellano, 2017; U.S Department of Justice, 2018). Figure 2 outlines FOIA requests received, processed, and pending with the federal government and illustrates the total number for each category over a five year period (2013-2017).

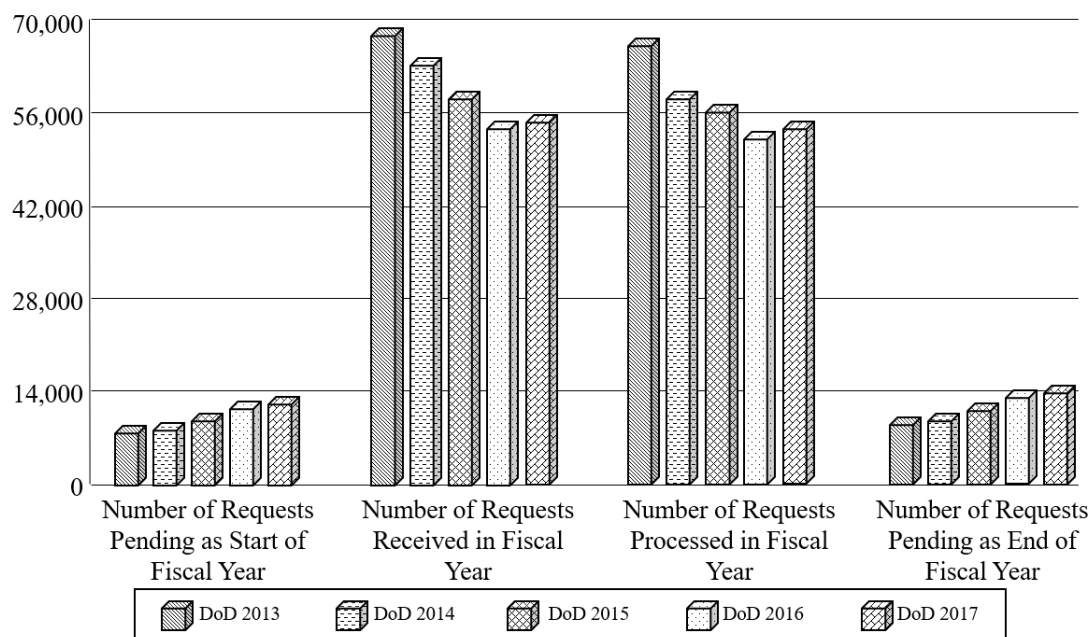


Figure 2. Total FOIA requests received by the federal government between 2013-2017.

With over 4 million employees eligible for access to classified information, the federal government has established single, common adjudicative criteria for assessing individuals who serve in sensitive positions. Eligibility for access is regulated through an adjudicative process that evaluates an individual's loyalty and allegiance to the United States. Information relating to the strength of character, honesty, stability, reliability, trustworthiness, judgement, and ability to protect classified information is evaluated through the 13 adjudicative guidelines listed below. Access to classified information is granted after an evaluation of each individual demonstrates eligibility is consistent with the interests of the United States. Evaluation of these adjudicative guidelines continues even after access to classified information is granted (USD Memo, 12 JAN 2018).

- Guideline A: Allegiance to the United States
- Guideline B: Foreign Influence
- Guideline C: Foreign Preference
- Guideline D: Sexual Behavior
- Guideline E: Personal Conduct
- Guideline F: Financial Considerations
- Guideline G: Alcohol Consumption
- Guideline H: Drug Involvement and Substance Misuse
- Guideline I: Psychological Conditions
- Guideline J: Criminal Conduct
- Guideline K: Handling Protected Information
- Guideline L: Outside Activities
- Guideline M: Use of Information Technology

According to a U.S. GAO Report to Congressional Committees (2017), ineffective implementation of information security policies and practices contribute to continued risks. An evaluation of 24 federal agency information security programs determined an absence of effective information security programs during 2016. Within the federal government and its lower echelons there exists numerous supplemental manuals, regulations, and policies that reside within each echelon and support an interlocking system of safeguards against the unnecessary release of CMI and CUI while contributing to an information security culture mindful of protecting U.S. personnel and interests. Some of them include:

- Executive Order No. 13526, 75 F.R. 707-731 (2009).
- Executive Order No. 13556, 75 F.R. 68675-68677 (2010).
- DoD Manual 5200.01, Vol 1, Information Security Program: Overview, Classification, and Declassification (4 May 2018)
- DoD Manual 5200.01, Vol 2, Information Security Program: Marking of Classified Information (19 MAR 2013)
- DoD Manual 5200.01, Vol 3, Information Security Program: Protection of Classified Information (19 MAR 2013)
- DoD Manual 5200.01, Vol 4, Information Security Program: Controlled Unclassified Information (CUI) (9 May 2018)
- DoD Manual 5200.45, Instructions for Developing Security Classification Guides (6 APR 2018)
- Army Regulation 380-5, Department of the Army Information Security Program (29 SEP 2000)
- Army Regulation 380-67, Personnel Security Program (25 JAN 2014)

- Army Regulation 530-1, Operations Security (26 SEP 2014)

Wibowo and Batra (2010) and Fitzpatrick and DiLullo (2013) suggest the implementation of policies and procedures to ensure acceptable levels of information security. All employees working within the federal government who handle sensitive or classified information attest to an oath (See Appendix A) and serve in a position of trust that encompasses an inherent responsibility to safeguard the data to which they have access (Kasner, 2015; Weaver, 2017). Regardless of the grade, position, or work performed, policies are also in place to ensure every individual granted access to CMI and CUI receives specific training and education on their individual responsibility for safeguarding such information, as well as potential repercussions that may result when unauthorized disclosures occur. However, the challenges associated with unauthorized disclosures endures, as the human element is still regarded as the source cause of many information security incidents (Da Veiga, & Martins, 2015; Dahbur, Bashabsheh, & Bashabsheh, 2017; Bulgurcu, Cavusoglu, & Benbasat, 2010; Vance, Anderson, Kirwan, & Eargle, 2014).

Security education, training and awareness (SETA). Organizational information security culture is a driving factor of workforce information security compliance. Unauthorized disclosures adversely affect the organization, as well as employees involved in the incident. Francois (2016) notes a lack of awareness and understanding of policy as the cause of unauthorized disclosures; further noting that many organizations consider security awareness programs as inefficient or costly. The ultimate success of an organization's information security culture is dependent upon information security policy compliance and the behaviors of end users. The value of information security policy, leadership support, and SETA are principal aspects for creating an effective information security culture for any organization seeking to mitigate

security risks, and ultimately negate security incidents. End-users play a vital function in the information security culture of organizations through their compliance with security policy, support from leadership, and SETA provided by the organization.

As previously noted, end-users are a critical link to securing CMI and CUI. Therefore, SETA planning and execution as part of creating an information security culture is imperative. Without of an effective SETA program, employees will not have the knowledge and understanding necessary to properly safeguard CMI and CUI. The posture of information security is a government-wide high-risk area, as noted by the U.S. GAO Report to Congressional Committees (2015). The report assessed employee SETA training and compliance with organizational security policy. Report findings concluded that many agencies failed to implement an effective information security program based in three significant findings. The specific findings included decreases in the percent of:

- 1) Agencies with established SETA programs,
- 2) Employees who received security awareness training, and
- 3) Agencies that tracked security training provided to personnel.

The SETA challenges noted in the 2015 GAO report continued as highlights in the following years U.S. GAO Report to Congressional Committees (2016). Agencies within the Federal government have a responsibility to establish and implement an effective organization-wide information security program. However, congressional reports clearly indicate agencies still struggle to fully or effectively implement SETA programs on a consistent basis.

1.3 Statement of the Problem

A preponderance of literature reviewed for this research cites a lack of leadership emphasis, loosely followed security policy, and ineffective SETA programs as sources of

unauthorized disclosures in large organizations (GAO, 2015). Failure to follow security procedures, non-conformance with established policy, and an inability to acknowledge and understand training and education emerge as key contributors to unauthorized disclosures. The handling and protection of CMI and CUI in today's increasingly interconnected and dynamic environment faces many challenges. Early on, a realization that measures for protecting data required the implementation of safeguards on information systems (IS) for the transfer of data. An assortment of approaches such as Public Key Infrastructure (PKI) encryption, firewalls, and digital certificates now affords protection for the secure transfer of information. While these automated functions secured our networks and IS from those attempting to obtain illegal entry, they have had little impact on the human aspect, with some end-users still failing to observe controls or conform with established policy. In a study addressing the relationship between information security and leadership practices, Rutherford (2014) provides further validation that human error exceeds technical defense as a primary failure point.

As a standard point of business, the federal government does not disclose data on the total number of reported unauthorized disclosures to the public. However, sources such as the Center for Development of Security Excellence (2018) release case studies highlighting some of the unauthorized disclosures that have occurred for education and awareness purposes. A search of the Central Intelligence Agency (CIA) FOIA electronic reading room (2018) revealed the 23 March 2009 declassification of a previously classified top-secret report that indicated 292 unauthorized disclosures between 1959 and 1977. Of the 292 unauthorized disclosures reported, 15 had occurred within the previous six months of the reporting window.

Although there is one overall standard for determining classification by an approved classification authority, there exist circumstances where additional clarification is necessary in

preventing unauthorized disclosures. In the area of research, development, and engineering, the federal government requires the establishment of security classification guides as an increased measure for preventing unauthorized disclosures through clarification. Security classification guides aid in the safeguarding of classified and unclassified critical program information related to ongoing research, development, and engineering efforts by defining guidelines for what constitutes compilation and data aggregation (DoDM 5200.01-V3, 2012). Organizational policies, procedures, and protocols that are in place are effective only if observed by employees. Within recent years, consequences of unauthorized disclosures to the federal government have included significant unexpected costs, reduced resource availability, strained international relationships, and lost lives. The amount of effort invested in consequence management of unauthorized disclosures far surpasses the damage from the incident itself. To prevent the occurrence of future security incidents, a better understanding of information security culture within the federal government is needed to assist in further refining and implementing organizational information security programs. While significant research exists addressing the information security culture within the private sector, a paucity of research exists addressing the information security culture within the federal government. This research considers GDT, the theory of POS, SET, and MT as a basis for examining the security climate within the federal government.

1.4 Purpose of the Study

The purpose of this meta-synthesis is to examine federal government information security culture through the factors of leadership support, security policy, and SETA.

1.5 Research Questions

This research contributes to existing literature by examining and evaluating information security culture constructs that are key factors for the planning, development, and implementation of a successful information security culture. A qualitative purpose statement signifies the intent to explore or understand the central phenomenon involving participants at an explicit research location (Creswell, 2015). According to Creswell (2014) and Creswell and Creswell (2018), the central phenomenon equates to the concept explored in qualitative research. The central phenomenon for this study is information security culture. Creswell (2014) and Creswell and Creswell (2018) also notes the consideration of the intent to explore external factors that shape the phenomenon. This research is confined to three factors that shape the phenomenon of information security culture - leadership support, security policy, and SETA. These factors were specifically selected because of their prominent use in previous information security culture research and the role they perform in contributing to organizational information security culture. These factors were also selected because no single study considered during this literature review identified a construct consisting solely of these specific factors. Additionally, research conducted by Karjalainen and Siponen (2011), Pierce (2012), D'Arcy and Greene (2014), Hwang, Kim, Kim, and Kim (2017), Tang, Li, and Zhang (2016), Chen, Ramamurthy, and Wen, (2015), Johnston, A. C. and Warkentin, (2010), Wibowo and Batra (2010), Fitzpatrick and DiLullo (2013) and Donahue (2011) indicates leadership support, security policy, and SETA as key factors of a comprehensive information security culture and are further discussed in Chapter II. Working under the guidelines described by Creswell (2015), five to seven questions are adequate for emphasizing information to be learned, as opposed to what this researcher seeks to understand. The construct of a research question should include the central phenomenon,

participants, and research site and is supported by sub-questions. Sub-questions possess similar qualities but provide increased specificity respective of the research question. The sub-questions for this research are designed so that each address an external factor.

Central question: What is the information security culture within the federal government?

Sub-questions: This meta-synthesis is guided by the below sub-questions.

- 1: What are workforce perceptions of leadership support and federal government information security culture?
- 2: What are workforce perceptions of security policy and federal government information security culture?
- 3: What are workforce perceptions of SETA and federal government information security culture?
- 4: What relationship exists between leadership support, security policy, and SETA within the federal government information security culture?

1.6 Theoretical Framework

Several references were used to inform this study. A review of the cited theories from literature reflects various theoretical commonalities among publications, as shown in Table 4.

Table 4

Cited Theories from Previous Security-Related Literature

Author(s)	Title and Publication	Cited Theory
<u>Aurigemma, S.</u> (2013)	A composite framework for behavioral compliance with information security policies.	Theory of planned behavior
Chen, Y., Ramamurthy, R., & Wen, K. (2015)	Impacts of Comprehensive Information Security Programs on Information Security Culture.	Organizational culture theory
D'Arcy, Hovav, & Galletta (2009)	User Awareness of Security Countermeasures And Its Impact on Information Systems Misuse: A Deterrence Approach.	General deterrence theory (Extended)
Da Veiga, A. (2016)	Comparing the information security culture of employees who had read the information security policy and those who had not.	No theory cited
<u>Dahbur, K., Bashabsheh, Z., & Bashabsheh, D.</u> (2017)	Assessment of security awareness: A qualitative and quantitative study.	No theory / framework cited
D'Arcy, J., & Greene, G. (2014)	Security culture and the employment relationship as drivers of employees' security compliance.	Theory of reasoned action Theory of planned behavior Social bond theory
Donahue, S. E. (2011)	Assessing the impact that organizational culture has on enterprise information security incidents.	Organizational-culture theory
Herath, T., & Rao, H. R. (2009)	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.	General deterrence theory Agency theory
Hwang, I., Kim, D., Kim, T., & Kim, S. (2017)	Why not comply with information security? an empirical approach for the causes of noncompliance.	Prospect theory
<u>Ifinedo, P.</u> (2014).	Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition.	Compliance theory Theory of planned behavior Social cognitive theory Social bond theory
Johnston, A. C., & Warkentin, M. (2010)	Fear appeals and information security behaviors: An empirical study.	Protection motivation theory
Pierce, R. E. (2012).	Key factors in the success of an organization's information security culture: A quantitative study and analysis.	No theory cited
Rutherford, A. J. (2014)	Information security, leadership practices inventory, and their relationship.	Stratified systems theory
Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016)	Continuance of protective security behavior: A longitudinal study.	Protection motivation theory
Workman, M., Bommer, W. H., & Straub, D. (2008)	Security lapses and the omission of information security measures: A threat control model and empirical test.	Protection motivation theory
Yoon, C., & Kim, H. (2013)	Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms.	Theory of reasoned action Moral obligation theory Protection motivation theory

Of the 16 major quantitative studies used to inform this research, 13 studies linked information security culture to a theory. Among those 13 studies, 12 different theories were drawn upon to support research constructs, some citing multiple theories.

A closer examination of these studies demonstrates that, while all of them model aspects of information security, no sole construct applied to more than one study. Additionally, the 16 studies listed in Table 4 implemented a combined total of 80 variables. As a noteworthy observation, 72 of the 80 variables related to three primary central constructs - compliance intention, behavior intention, and security culture. The terminology used for each construct varied. While it may be fairly easy to discern construct similarity as in the instance of “security culture” and “organizational security culture”; congruence in other cases cannot be determined without a cautious review of variable utilization for the specific study. For example, Yoon and Kim (2013) define the term “omissive behavior” as the intention to observe information security protections that is influenced by the perceived worth of effort needed for protection. For the purpose of this study, “omissive behavior” equates to compliance intent. The deficiency in naming convention consistency may be confusing for the casual reader. Initial theoretical findings indicate progress in the use of theory in information security culture research. Research by Karlsson, Åström, and Karlsson (2015) reveals 81 percent of existing information security research between 1990-2004 generally lacked theory. In their 2015 study, references lacking theoretical framework reduced to 24 percent. Based on the theoretical findings used for this research, the number of studies with no reference to theory fell to 17 percent. These numbers serve as evidence of increased theoretical maturity within the framework of information security culture.

Information security policy is essential to security culture. The success however, depends on management attitudes toward promoting a security culture (Da Veiga, 2016). A challenge for organizational leaders involves encouraging employee compliance with information security management and risk mitigation through codified policy (PwC, 2014). Policies set the formal direction and course of organizations by establishing the framework for security controls (ISO/IEC 27002, 2013). However, employee compliance with established security policy and procedures remains a challenge for many organizations. Many employees prioritize convenience over security when deciding to violate security policy, while others possess more destructive intentions. Regardless of the intent, the majority of information security breaches originate from employee non-compliance with information security policy (D'Arcy & Greene, 2014). When unauthorized disclosures occur, employees develop perceptions about how the incident is handled and their organization. The theory of POS explains how employee perceptions about the extent to which they receive organizational support impact their work efforts. This means that when employees feel the organization values their contributions and cares about their general well-being, they reciprocate with increased dedication and loyalty in their efforts to comply with rules and achieve organizational goals. In conjunction, SET serves as a theoretical basis for the relationship between POS and compliant behavior. When employees hold POS at high levels, a social exchange occurs in which employees may feel obligated to reciprocate the affective support from organizational leadership by engaging in higher levels of acceptable performance (D'Arcy & Greene, 2014; Dawley, Houghton, & Bucklew, 2010; Newman, Thanacoody, & Hui, 2012). In the context of security culture, commitment to higher levels of employee performance will lead to an increased compliance with information security policies. Considering the POS and SET empirical findings

and their association with increased commitment and allegiance to the organization, a relationship between leadership support and information security culture may be predicted.

Chen, Ramamurthy and Wen (2015) note organizational SETA programs as a significant influencing factor of information security culture. Communication through security policies, education sessions (formal and informal), and training materials (posters, screen saving messages, briefings, and posters) provide a strong indication of an information security program. These SETA opportunities prepare employees with the tools necessary for effectively functioning within the organization. Drawing upon the GDT, SETA programs may serve as a procedural control by acting as a deterrence instrument to discourage unacceptable workplace behavior. GDT posits the greater the perceived swiftness and certainty of sanctions, the greater the degree of deterrence from the act. Thus, one assumption of GDT is that individuals make rational decisions regarding compliance or non-compliance based on the associated costs-benefit analysis (Chen, Ramamurthy, & Wen, 2015; D'arcy & Herath, 2011; Yuryna, Lang, Gathegi, & Tygar, 2017). The potential of issuing sanctions that occur from policy violations impact the employee's perception of information security culture. Considering GDT, empirical findings and its association with building a strong sense of security among employees within the organization, a relationship between SETA and information security culture may be predicted.

From a conventional perspective, Mosaic Theory (MT) refers to the data research and collection process of arriving at a conclusion by piecing together numerous pieces of available information. In MT, seemingly insignificant pieces of data may become significant when combined with other data. Mosaic theory does not view respective processes as important; it views the concept of data quantity as a focus (Rooney, 2017). Through data collection, "bits, fragments, and pieces of seemingly innocuous data can be analyzed and fitted into place to reveal

with startling clarity how the unseen whole must operate" (Jaffer, 2010, para 2). The government uses MT as powerful argument for its justification to deny the release of information requested from the general public. In parallel, mosaic theory can be viewed as a double edge sword. Adversaries who are the recipient of CMI and CUI form unauthorized disclosures may also analyze bits and pieces of data to develop a complete picture of classified government intent or operations, thus impacting national security (Jaffer, 2010).

1.7 Significance of the Study

The unauthorized disclosures of classified information within the federal government are not new. For decades, some of our nation's most highly guarded secrets have found their way into the hands of adversaries and the general public. As classified information becomes increasingly more valuable, the need for preventing unauthorized disclosures also increases. To prevent unauthorized disclosures, users must clearly understand the impact on national defense and acknowledge a risk averse approach to handling classified material. The ever-increasing occurrence of unauthorized disclosures indicates a clear need for research efforts to investigate the relationships of potential contributors to establishing an information security culture.

In a study of existing information security culture literature, Karlsson, Åström and Karlsson (2015) scrutinized the development and advancement of information security knowledge. The approach encompassed an extensive review of information security literature published between 2000 and 2013. The review suggests two common themes: First, literature seemingly falls short of providing details on research methods used or describing the literature review process. Second, many of the studies reviewed drew upon influence from organizational science frameworks, such as organizational culture, to study information security culture. The findings note that although expansive research exists, there is a paucity of research addressing

the effects of different information security cultures that is compounded by a limited collection of research methods. As a result, the abundance of descriptive, philosophical, or theoretical research and lack of empirical data indicate immaturity in the area of information security culture research. The research calls for a wide-ranging set of additional research methods that delve into the effects of differing information security cultures. Of note, the use of intervening or ethnographic approaches is especially lacking in this area of research because frameworks for cultivating or assessment tools are not empirically validated, also indicating immaturity. This research will attempt to lessen the noted lack of empirical data and widen knowledge by focusing on information security culture within the federal government workforce.

A review of research conducted by Shelton (2014) reveals no broad consensus of why security practices and procedures are not followed. The study, “Reasons for non-compliance with mandatory information assurance policies by a trained population”, examined compliance by Information Assurance (IA) trained federal employees with IA practices and policies and yielded general results that may be applicable across all federal government organizations. This proposed research is different in that it seeks to provide additional insight by expanding data collection beyond IA professionals, and includes all skill-sets and grades within the government workforce, conducting an all-encompassing study that includes workers and leaders at all levels with varying experience and skills will provide greater insight on overall security culture. This is an important deviation in that:

- 1) IA-trained employees receive more IA training than do other workforce employees,
- and
- 2) IA-trained employees do not accurately represent those responsible for preponderance of documented unauthorized disclosure incidents.

Research conducted by Rutherford (2014) sought to gain insight into the root cause of security incidents. While the human factor was identified as the greatest vulnerability in safeguarding information, leadership was noted as holding the responsibility for enforcing compliance with established policy and procedures. Citing leadership as the root cause, Rutherford's (2014) approach focused on employee perceptions, company values, training, and awareness. One of the foundations of this proposed research is based on the concept that all who possess classified information are ultimately responsible for its safeguarding. This research will not focus solely on leadership and/or perceptions of leadership. Instead, this research is different in that it seeks to better understand the culture of those directly responsible for, and in possession of, classified information – both leaders and employees.

This study may contribute to the safety and security of the nation. The U.S. has entered intelligence sharing agreements with several countries. When other countries discover the information provided to the U.S. is available in the public domain, their willingness and trust to exchange additional CMI and CUI is impacted (Weaver, 2017). Safeguarding our nation's secrets remains a priority and any progress toward reducing unauthorized disclosures increases trust with allies and their willingness to engage in future exchanges of classified information to further support American national strategy.

This research intends to benefit organizations within the federal government. However, it may also benefit other organizations outside the federal government that must also conform to federal security policy, security training, and other similar security-related requirements. To somewhat of a commensurate degree, private sector organizations contracted by the federal government may also benefit. Defense contractor employees are often embedded within federal

government agencies and organizations and often work alongside federal employees. They are also subject to the same governing security and information technology policies and procedures.

Providing the right SETA to the right employees is a priority of any organization. Training provides assurance by increasing employee understanding of what to do and why it needs to be done. Benefits in the areas of information security and information assurance may emerge through shortcomings identified in SETA programs. This research may also benefit other public and private organizations by providing insight on differences between leader and subordinate perceptions of organizational security culture.

Another benefit that may materialize is a reduced number of unauthorized disclosures. Unauthorized disclosures often costly and require the immediate re-allocation of resources and mitigation actions. According to Warkentin, Johnston, Shropshire, and Barnett (2016), the average cost of a major security breach is \$415,000. Lost work hours and costs associated with restoring networks and IS back to approved configurations strains personnel availability and budgets. Organizations that review these findings and acknowledge recommendations may benefit from decreased consequence management responses associated with unauthorized disclosures.

Lastly, leadership may benefit through a better understanding the organizational security culture and contributors to unauthorized disclosures. Gaining an understanding of the organizational culture based on quantitative data and not perceptions will inform leaders and managers on where to place emphasis on preventing future unauthorized disclosures. Increased awareness of the organizational security climate may also help bridge differences between leadership perspectives and employee perspectives within the organization.

1.8 Definition of Terms

This section provides a more detailed definition of the terms and phrases previously introduced and used throughout this research. There are other terms or phrases that are not referenced in this chapter but are particular to subsequent chapters. Those terms or phrases are defined and described in their respective chapters, as appropriate.

ATLAS.ti 8: A qualitative data analysis tool that serves as a workbench for analysis of large bodies of textual, graphical, audio and video data to help the users arrange, reassemble, and manage material in creative and systematic ways (ATLAS.ti, 2018).

Authorized Person: A person who has a favorable determination of eligibility for access to classified information, has signed a SF-312, and has a need to know for the specific classified information in the performance of official duties (DoDM 5200.01-V3, 2013).

Automated information system: An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information (DoDM 5200.01-V3, 2012).

Classified information procedures act (CIPA): Rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court (Classified Information Procedures Act, Title 18 U.S.C. App III, 1980).

Classified information: Information that has been determined pursuant to Executive Order 13526, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form (DoDM 5200-01-V3, 2013)

Classifier: An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide (AR 380-5, 2000).

Confidential information: The level of classification applied to information in which the unauthorized disclosure could reasonably be expected to cause damage to the national security (AR 380-5, 2000).

Compilation: An aggregation of preexisting items of information (DoDM 5200.01-V1, Change 1, 2018).

Compilation and data aggregation: The ability to create large databases as well as nearly universal Internet posting of information makes use of search, data mining, and other data correlation tools convenient and easy. All of these capabilities facilitate creation of classified compilations of data (DoDM 5200.01-V3, Change 2, 2013).

Compromise: An unauthorized disclosure of classified information (DoDM 5200.01-V3, Change 2, 2013).

Classified military information (CMI): Information and material that has been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form (AR 380–5, 2000).

Controlled unclassified information (CUI): Unclassified information requiring safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies, policies, excluding information that is classified pursuant to Executive Order 13526. CIU information can include, procurement sensitive information,

personal health information, personally identifiable information, restricted data, and other designated categories of agency information deemed sensitive (DoDM 5200.01-V1, Change 1, 2018).

Damage assessment: A formal multi-disciplinary analysis to determine the effect of a compromise of classified information on the national security (DoDM 5200.01-V3, Change 2, 2013).

Damage to the national security: Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information. (DoDM 5200.01-V3, Change 2, 2013).

Density: Identifies the number of linkages to other codes or sub-codes (ATLAS.ti, 2018).

Derivative classification: Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. (DoDM 5200.01-V3, Change 2, 2013).

Distribution statement: A statement used on a technical document to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement is distinct from and in addition to a security classification marking and any dissemination control markings included in the banner line. A distribution statement is also required on security classification guides (DoDM 5200.01-V1, Change 1, 2018).

Executive Order 13526: Prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism (Executive Order No. 13526, 2009).

Foreign disclosure: Conveying information, in any form or manner, to an authorized representative of a foreign government, foreign entity supporting U.S. interests and/or security objectives or international organization. Disclosures may be accomplished through oral, visual, or documentary modes (AR 380-10, 2015).

Freedom of information act (FOIA): Provided the public the right to request access to records from any federal agency. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement (FOIA, 1996).

Groundedness: The degree or frequency of "groundedness" refers to the number of quotations that are linked to a code. (ATLAS.ti, 2018).

Information assurance (IA): The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities. This regulation designates IA as the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (AR 25-2, 2017).

Information security (INFOSEC): The system of policies, procedures, and requirements established under the authority of Executive Order 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive order, statute, or regulation (AR 380-5, 2000).

Information systems (IS): Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections (AR 25-2, 2017).

Insider threat: The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities (DoDD 5205.16, Change 2, 2017).

Node: Any object displayed in a network (ATLAS.ti.8, 2018)

Public release: The act of making information available to the public with no restrictions on access to or use of the information. Authorization and release of information to the public is the responsibility of the originating office (DoDI 5230.29, 2017).

Safeguarding: Measures and controls that are prescribed to protect classified and controlled unclassified information (DoDM 5200.01-V4, 2018).

Security classification guide (SCG): A documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must

be classified and establishes the level and duration of classification for each such element. Any instruction or source that prescribes the classification of specific information (DoDM 5200.01-V1, 2018; AR 380-5, 2000).

Security clearance: A determination that a person is eligible in accordance with the standards of Reference (1) for access to classified information (DoDM 5200.01-V1, 2018).

Sensitive but unclassified (SBU): Information originated within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act (AR 380-5, 2000).

Secret information: The level of classification applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security (AR 380-5, 2000)

Top secret information: The level of classification applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security (AR 380-5, 2000).

Unauthorized disclosure: Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient (DoDM 5200.01-V1, 2018)

1.9 Limitations

Similar to many other studies, this study has limitations. Limitations are beyond the researcher's control and may impact the study outcome. The first limitation for this study acknowledges that while employees may know the right thing to do, it does not mean they will actually do the right thing. While data gathered for this study include employee knowledge, perceptions, and experiences, it is limited in data gathered through direct observations to observe individual actions while working in classified environments.

Second, the participants in qualitative studies collected for this research include security specialists and technology professionals. Security specialists and technology professionals play an active role in creating and enforcing organizational security policy. It is possible that data collection from these demographics is biased because these groups possess a greater awareness of information security requirements than other employees. As such, data provided by security specialists and technology professionals may not be a true representation of the federal workforce.

The third limitation concerns study applicability. While this study is a meta-synthesis, it is not generalizable. A cautious approach is recommended when attempting to apply these research findings to information security cultures within private and non-profit organizations.

A fourth limitation of this study is consideration for environmental influences that could influence security culture. While leaders desire to achieve a positive organizational security culture, no controls were implemented to account for employees who selectively choose to sacrifice security over convenience when performing work tasks.

For the fifth limitation, a literature review is an important part of much scholarly research. The internet and various libraries provide access to vast amounts of publicly available

literature. However, researching government information that has not been released for public consumption impacts study strength. The sensitivity of unauthorized disclosures has proven difficult to acquire information on the number of incidents within the U.S. government. Several FOIA requests were submitted in support of this study. However, the length of government processing time and redirection of FOIA requests limits the inclusion of any publicly releasable information concerning numbers of unauthorized disclosures within the federal government.

A sixth limitation involves bias. It concerns difficulty with distinguishing between the reporting of salient study aspects. This concern emerges from an observation that some important aspects of studies are never reported. The lack of reporting on salient aspects of a studied is particularly problematic in relation to the factor coding on the effectiveness of studies. Any omission of important study aspects adversely impacts coding and reduces the effectiveness of meta-synthesis.

A seventh limitation concerns previous research used to support a meta-synthesis. It may be difficult to systematically review diverse studies that are produced and documented in very different ways. This researcher is limited by the quality and thoroughness of the original data used to support this study. As a result, the appropriateness of meta-synthesis coding for studies that are poorly designed or have little coding value may impact findings.

Eighth, classic and current literature on approaches to meta-synthesis recommend a research team with a diverse mix of disciplines and expertise. Differing interdisciplinary perspectives and experiences contribute to the emergence of important insights that otherwise would not have been uncovered. A team with knowledge of research methodologies, theoretical perspectives, and content area of the meta-synthesis topic is recommended. The constraints

applied to this study preclude a team effort. As such, the potential exists for omission of salient insights that may have been identified by a team with diverse perspectives.

A ninth limitation involves researcher experience with the ATLAS.ti.8 software. The researcher for this study had limited experience in meta-synthesis and coding tools. The researcher sought consistent guidance from a mentor with expertise in meta-synthesis research and coding throughout the process of this study. While this study contained the researcher's own constructions and perceptions of the material, the categorizing of the studies was interpretative and thus is limited by experience of the researcher. The researcher's lack of experience may compromise the reliability of a study.

A tenth limitation involves inter-rater reliability. Two subject matter experts with similar backgrounds determined inter-rater reliability. Although ratings for each coder were completed independently and efforts to remove bias were observed, there may be a possibility of likeminded coding due to similarity of backgrounds.

1.10 Delimitations

This researcher has elected to delimit this study in a number of important ways. The first delimitation was selection of a problem. Several other information security culture related topics were considered, but were rejected because of time constraints, data access and availability, academic limitations, or over-ambitiousness. This study was selected because its relevance increasingly continues, as leaders in the federal government acknowledge security incidents will persist and increase in the future.

A second delimitation of this study involves the exclusion of certain studies to facilitate meta-synthesis. Certain studies addressing PMT, compliance theory, theory of planned behavior, social cognitive theory, and social bond theory were excluded for two reasons. First, the

variables used in these studies were perception focused (threat, severity, and self). Second, the excluded studies did not address any of the selected factors for this study. Although relevant, these studies were associated with examining employee rewards, punishments, and obligations.

The third delimitation involves this researcher's decision to include peer-reviewed, published data and apply certain inclusion/exclusion criteria for the synthesis portion of this study. While this delimitation provides an increased focus and relevance for the research questions, it may also risk susceptibility to publication bias. Furthermore, exclusion criterion limits the amount of usable studies, as a number of studies in this discipline were produced by the same author.

A fourth delimitation is the inclusion of grey data. The decision to use materials that are outside the traditional commercial or academic publication and distribution channels is intended to provide readers with a greater appreciation of the problem this research addresses. The use of executive orders, congressional reports, sections of the U.S.C. and other government data provides information relevant to this study not available from any other primary source.

The fifth delimitation concerns research factors. The literature review for this study identified over forty information security culture related factors that were used across dozens of studies. This meta-synthesis will only focus on those studies addressing leadership support, security policy, and SETA. These factors are of particular interest to the researcher as the federal government looks for research to support improving information security culture, and further reduce the number of security incidents.

The sixth delimitation addresses the organizational demographic needed to answer the research problem. Although no constraints were imposed on the type of work in which an organization engages, efforts were made to omit non-profit and private sector studies from

synthesis. Aligning with the focus of this research, relevant studies include those with a federal government or government entity emphasis. While some private sector organizations directly support the government, security incidents that involve contractor negligence are attributed to the government organization in which they are embedded.

As the seventh delimitation, this study seeks to examine the current state of information security culture. It does not intend to assess the effectiveness of controls implemented over time. It also does not utilize longitudinal approaches that conduct multiple samples for data collection. This study encompasses several different samples for comparison. As such, all data supporting this meta-synthesis are cross-sectional studies that are an observation of factors at one specific point in time.

For the eighth and final delimitation, all federal employees are held to a higher expectation of conduct than their private sector counterparts. Their actions and adherence to standards are governed by a specific set of values, swearing an oath of allegiance, and abiding by an established code of conduct that is supported by a table of penalties. As a result, participant responses and findings may not validate private sector applicability.

1.11 Ethical Issues

Institutional Review Board (IRB) approval was required for this study; however, the nature of design is a meta-synthesis and will not involve interaction with human subjects. As such, this study qualifies for IRB exemption. This study complies with professional standards. All appropriate citations are applied in an effort to alleviate potential discrepancies with authorship for publication. All content used for this study is approved for public release and retrieved from publicly available sources to avoid any potential conflict with the government. No disruption of work participant operations occurred. There is no concern with impartiality, as

the researcher does not have a need, and is not in a position, to engage participants from selected studies. Confidentiality was paramount during and after this study. Participants were not required to provide any personally identifiable information. Data collected resided in a controlled access area equipped with alarms and monitoring. Visual recognition served as a second layer of security to safeguard against unauthorized access (Creswell, 2015).

1.12 Summary

This study highlights the importance of a security culture intended to mitigate or negate the occurrence of unauthorized disclosures. The specific problem of unauthorized disclosures remains concern for organizations due to ongoing occurrences and whether leadership support, security policy, and SETA serve to effectively improve information security culture. Questions that prompted this study revolved around the continuing number of unauthorized disclosures within the federal government and their key contributing factors. Specifically, what are the assessed factors of an information security culture? The factors identified herein are considered principal to determining the degree of information security culture within an organization. Through this process, factors were integrated into a research model to achieve an end result.

This study is organized into five chapters. Chapter I introduces the relationship between unauthorized disclosures and information security culture. This chapter articulates the study need and defines terms used throughout this research. Chapter II consists of a literature review that investigates how leadership support, security policy, and SETA contribute to establishing an information security culture security culture. Chapter II concludes with an analysis of variables used in previous research and their relevance to this research. Chapter III discusses the methodology for this research by introducing the research design and participants. It discusses the research tool and methodology for determining inter-rater reliability. Chapter III also

describes the approach to data collection and the instrument used for data collection. The chapter concludes by addressing risks and benefits, ethical issues, and assumptions. Chapter IV discusses the results and analysis of focused data collection. Chapter V provides a discussion of the relevant key findings and emerging themes, proposes a new research model, and concludes with a summary and implications of this research.

CHAPTER II: LITERATURE REVIEW

2.1 Introduction

The organization for this literature review comprises an introduction that describes the chapter arrangement and four additional sections. The second section addresses organizational climate, information security culture, and the factors specifically selected for this study (leadership support, security policy, and SETA). The third section includes quantitative research models addressing the factors specifically selected for this study. Although this is a quantitative study, the decision to include quantitative data supports the inclusion of multiple research methods to ensure a range of existing and sufficient data that provide increased knowledge and understanding of this research topic. This literature review aligns with that outlined by Rowe (2014), in that it is a summary that critically examines previous research, discusses previous research results, and brings to light the differing views of past research. Chapter II concludes with a discussion and summary of the literature.

The research approach for this literature review is straightforward. Information security research occurs in dissertations, articles, studies, and technical papers. Research conducted for this study utilized libraries, databases, professional journals, and government sources to ensure a broad coverage of national and international literature. The research parameters considered recent scholarly, peer reviewed data primarily between 2010 and 2018. A dynamic search plan encompassed resources and key words that were reviewed and revised as necessary. The abstract of each document was evaluated for relevance and an initial determination was made as to whether the literature retrieved was germane to this dissertation. During literature evaluation, a database recorded pertinent data (i.e., author, date, abstract, variables, theory, and search criteria) into fields that allowed for sorting and easy retrieval of data. A continuous method was

refined throughout the process that originated from a macro perspective and ultimately reduced to a micro view of specific areas. Pre-determined limits of investigation helped prevent embarking on research tangents not germane to the topic. The acceptable literature consists of scholarly articles, longitudinal studies, quantitative research, qualitative research, case studies, government documents, and books.

2.2 Factor Literature Review

While this section addresses information security culture, it is appropriate to include some discussion on climate. The close relation between climate and culture imposes a need for providing clarity and describing applicability to this study. Hwang et al. (2017) suggested that information security compliance behaviors arise from an organization's security climate, which is based on the actual compliance behavior of coworkers. The concepts of climate and culture share an understanding of some aspect of the organizational context. When viewing security climate, employee perceptions serve as a reference point for guiding employee behavior. Organizational events that are observed by employees can serve as indicators for key priorities valued by the organization. Therefore, climate is considered a medium through which events of organizational context are translated into an employee's behavior (Chan, Woon, & Kankanhalli, 2005). Additional research by Karlsson, Åström and Karlsson (2015) suggest information security climate has a significant positive influence on security policy compliance. The generally accepted definition of climate involves perception of practices, policies, procedures, and routines in the organization. When these perceptions are shared, organizational climate can be interpreted (Ostroff, Kinicki, Muhammad, 2013, p. 643). Table 5 depicts generally used organizational climate definitions.

Table 5

Organizational Climate Definitions

Definition	Reference
"A set of attributes specific to a particular organization that may be induced from the way the organization deals with its members and its environment."	Chan, Woon, & Kankanhalli (2005, p. 22)
"The policies, practices, and procedures and the behaviors that get rewarded, supported, and expected in a work setting and the meaning those imply for the setting's members."	Schneider et al., (2011, p. 39)
"A perception of practices, policies, procedures, and routines in the organization."	Ostroff, Kinicki, and Muhammad, (2013, p. 643)
"A multidimensional construct that encompasses a wide range of individual evaluations of the work environment."	Iljins, Skvarciany, & Gaile-Sarkane, (2015, p. 11)
"A set of characteristics that describe an organization, distinguishes one organization from another, is relatively stable over time and can influence the behavior of the organization's members."	Eustace & Martins (2014, p. 4)
"The way in which employees perceive their organization and its purposes."	Berberoglu (2018, p. 2)

Security culture is part of an organization's overall culture (Mubarak, 2016). A critical goal of comprehensive information security policies and programs is to develop an information security culture reflecting the organizational security values and norms. The intent is for information security culture to serve as a collection of common security values and beliefs that promote positive employee behaviors toward security. Several definitions of information security culture were identified during the literature review, as depicted in Table 6. For the purpose of this study, an adequate definition for "information security culture" is defined as a shared environment of security behavior, values, and norms observed by all members and pursuant to achieving organizational goals. Essentially, an operational term for information

security culture can be viewed as the collective, social bond that govern the way things are done within the organization.

Table 6

Information Security Culture Definitions

Definition	Reference
"A shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security."	Karlsson, Åström, & Karlsson (2015, p. 247)
"A way of doing things around the information security, including creation of an environment that fosters and nurtures shared security attitudes, values and beliefs in a given organization."	Chen, Ramamurthy, & Wen (2015, p. 13)
"The manifestation of information security practices or behaviors evolving from the shared beliefs and values in the organization."	Tang, Li, & Zhang, (2016, p. 180)
"The values and beliefs of information security shared by all members at all levels of the organization."	D'Arcy & Greene (2014, p. 476)
"Patterns of behavior, belief, assumptions, attitudes, and ways of doing things."	Donahue (2011, p. 5)
"A portion of the overall corporate culture where information security becomes as common and routine as budgeting, accounting, planning, or any other business aspect of the organization."	Pierce (2012, p. 12)
"The manner in which employees perceive and interact (behave) with the controls that are implemented to protect information."	Veiga, Adéle, & Martins (2014, p. 50)
"The attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time."	Da Veiga & Eloff (2010, p. 198)
"The way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process."	AlSabbagh et al. (2012, p. 33)

End-users are a first point of attack and the weakest line of defense for two reasons. First, sending emails embedded with malicious code to end-users is much easier than spending time discovering system vulnerabilities; second, insider threats pose a risk that is hard for organizations to identify or control. According to Chen, Ramamurthy and Wen (2015),

employee negligence causes a large number of unauthorized disclosures. Therefore, it is crucial for organizations to develop and implement an effective information security culture. It is also important for organizations to understand that just as the human element is considered their greatest asset, it should also be recognized as a significant security risk (Dahbur, Bashabsheh, & Bashabsheh, 2017; Donahue, 2011; Hwang, Kim, Kim, & Kim, 2017; Rutherford, 2014; Warkentin, Johnston, Shropshire, & Barnett, 2016).

The Karlsson, Åström and Karlsson (2015) study findings reveal that although a broad range of information security culture topics have been investigated, only a few topics account for most of the research carried out. Organizational science emerged as the preeminent basis of research questions. With much of the research that was reviewed either descriptive or philosophical, references to theory are minimal. The study also found that the most researched meta-question among literature reviewed sought to identify the roots of information security, while questions inquiring about the fruits of different information security cultures were not addressed at any length. In several of the papers reviewed, research methods were ambiguous, making the findings difficult to assess. This lack of attention on the benefits of different cultures for performance may be viewed as a point of departure, as opposed to an area needing further empirical testing. Concurrently, the majority of the studies reviewed during their research insufficiently addressed information security research theory. Few studies were noted as exploring the progress of present studies on information security culture. The discoveries from exploring different types of research can extend beyond current knowledge, allowing for critical discussion on the culture of information security. With the acknowledgement for deeper investigation in the area of information security, the cultural aspect has not received a commensurate degree of attention as other aspects information security. Alternatively, most

studies have overwhelmingly focused on technical aspects, while much fewer studies have focused on individual information security behavior and designing methods to create information security. Consequently, those fewer studies noted a need for empirical research such as surveys, case studies, and action research for various reasons. This research will attempt to bridge the gap of knowledge by building upon current research and providing a deeper understanding of information security culture with theoretical research and of empirical data. A limitation noted in the study was the search strategy and subsequent selection of papers for consideration. Use of a single database widens the potential that other relevant studies may not have been considered. Additionally, the implementation of an analytic framework that involves subjective decision-making allows for the potential introduction of bias. While the study purpose was to examine existing research on information security culture and assess how related knowledge has moved forward, a narrow selection of research topics and an undersized range of research approaches connote a limited range of information security culture research. As a result, the widespread portion of literature addressing explanatory viewpoints or supposition hinders the ability to distinguish knowledge of relationships among differing information security cultures.

Chen, Ramamurthy and Wen (2015) conducted a study addressing the impacts of comprehensive information security programs on information security culture. Their study acknowledged a consensus by recent scholars on the importance of employees' value and belief systems (i.e., practiced morals, ethics, social values, and work standards) in security policy compliance intention and the impact on information security culture. The research model evaluated the influence of security policy, SETA, and monitoring on information security culture. Study results indicate a significant, direct influence of SETA program awareness on security culture and organizational security policy. Study findings imply the importance of an

organizational security culture where everyone assumes responsibility and all are included when designing, developing, and implementing supporting policies. A second implication noted was the mere presence of security policy was marginalized when not supplemented by a good SETA program. Liu (2015) notes information security policy as one of the most important aspects of implementing an effective information security program. Organizations must create a balance between too few and too many policies. Alternatively, the Chen, Ramamurthy and Wen (2015) study findings revealed no relationship between security policy and security culture. One possible reason for this finding is when organizations over-emphasize [security] policies, they become commonplace and are not considered as part of security culture by employees.

The commitment of employees to do the right thing is essential to maintaining a positive information security culture. According to Mayer, Gerber, McDermott, Volkamer, and Vogt (2017), employees who display high affective organizational commitment are more prone to display higher job performance than those who lack affective commitment. Considering that employee compliance with security policy and procedures is an inherent job function, employees displaying high commitment are likely to perform with a higher regard for security compliance. Da Veiga (2016) asserts “threat perceptions about the severity of breaches, organizational commitment, and social influences and resource availability” (p. 141) as influences to security policy. Adding to this assertion, D'Arcy and Greene (2014) consider leadership emphasis on compliance with policies and procedures as reflecting increased commitment. Concurrently, it is necessary for leaders to take swift and prudent action against policy violations to convey a clear message of the organization's commitment to safeguard its information and related assets (Narain Singh, Gupta, & Ojha, 2014).

In a study addressing the reasons for non-compliance with mandatory information assurance policies by a trained population, Shelton (2014) validates the degree of end-user noncompliance with policy for federal employees by addressing specifically two areas: 1) number of subjects who have failed to comply, and 2) the frequency of failures to comply. An interesting aspect of this study revealed no participant motivation (positive or negative) to comply with security policy. An initial interpretation from this observation could consider pursuing reward or punishment methods as motivational processes to gain compliance from the workforce as a waste of time. A second interpretation could be that federal employees simply feel that doing the right thing does not need an incentive, rather safeguarding CMI and CUI is simply an accepted duty or obligation of service for all. Irrespective of these interpretations, other researchers contend the leader-follower relationship as a force for compliance. Hamstra, Sassenberg, Van Yperen, and Wisse (2014) note that when followers feel valued by their leaders, both leaders and followers become aligned in the same values that govern an organization. The study, however, falls short by not identifying the specific causes for non-compliance. Shelton (2014) goes on to note the crucial answer to the question of non-compliance lies in the absence of a single question, as there appears no published study that simply ask end users for their reason(s) for non-compliance.

2.3 Leadership Support

The success of an information security program depends on both leadership support to information security policy and leadership emphasis for compliance Puhakainen and Siponen (2010). It is the inherent responsibility and obligation of leadership to provide training and grow a positive and encouraging work environment (Scully, 2014). Action research by Puhakainen and Siponen (2010) focused on improving employee compliance with security policy through

information security training. Their study noted information security as a continuous process that involves leadership, the information security staff, and end users to ensure a continuous flow of communication that is necessary to further information security compliance. Leadership support ensures employee understanding and underscores the importance of information security culture. Employee behaviors obligate management actions to ensure proper usage of information systems. Employees not willing to accept current policy often oppose the implementation of new policies within organizations. When managers fail to motivate employees to accept change, there is resistance and a lack of motivation for altering of behavior. Any adverse change in organizational security culture is therefore a management obligation. If managers do not embrace the information security culture, the organization is at a disadvantage when it comes to combating security incidents. Thus, it is imperative that leadership and information security managers serve as the champion for implementing various methods of information security culture within the organization. Many organizations have adopted a set of established values and policies that serve as guidelines for a coherent organizational culture. Only those who willingly acknowledge and accept these guidelines will contribute positively to the organizational vision (Chen, Ramamurthy, & Wen, 2015; Da Veiga, 2016; Dahbur, Bashabsheh, & Bashabsheh, 2017; Donahue, 2011; Johnston & Warkentin, 2010).

The success of organizational security culture relies on emphasis and support of its leadership for policy implementation, enforcement, and accountability. A quantitative study by Rutherford (2014) addressed information security and leadership practices within a federal government organization and their relationship to information security. The study notes “leadership is the root cause of data breaches in large organizations for a variety of reasons, including leadership style, perception of employees, training, awareness, and the instillation of

organizational values.” Although the study pointed to the human factor as the cause of unauthorized disclosures, as cited in much of the security culture literature reviewed, a lack of policy enforcement by leadership was named as the reason. Rutherford (2014) further noted that ineffective, inefficient, or inadequate policies, procedures, and other documentation promulgated by the leadership are not technical failures, they are the direct result of poor leadership decisions. Thus, the assigning of roles and responsibilities and ensuring accountability are principal characteristics of effective information security program execution. Herath and Rao (2009) suggest one approach for managers to enhance information security compliance is by encouraging the appropriate security climate in the organization. Furthermore, when employees trust that their work activities contribute to achieving overall security, they are inclined to observe information security policies. According to Ifinedo (2014), the leadership regulates organizational socialism, influence, and perceptions about its workforce. As discussed in Chapter I, the lack of POS from leadership and reciprocating degree of SET may shed light on reason for some of the unauthorized disclosures within the federal government (D'Arcy & Greene, 2014; Dawley, Houghton, & Bucklew, 2010; Newman, Thanacoody, & Hui, 2012).

2.4 Security Policy

The federal government classifies unauthorized disclosures into three categories – willful, negligent, and inadvertent (OSD, Aug 2014). Unauthorized disclosures involving employees who are working within the organization are the most difficult to prevent. This may be partially attributed to the challenge with monitoring the security behavior of end user (Hearth and Rao, 2009). Shelton (2014) notes inconsistent policy compliance among users. According to Hwang, Kim, Kim and Kim (2017), employees feel security policies reduce their work efficiency. Employees who view security policies as ambiguous may develop anxiety when using IS.

Employees also tend to follow the culture of the organization. If co-workers are known not to comply with security policy, the chance increases that others will act similarly. Information security policies, like many other policies, address potential penalties for non-compliance. These penalties can also result in anxiety, which may be a cause for not compliance.

Research by Shelton (2014) addressing reasons for non-compliance with policies contends that end-users fail to consistently comply with established information security policies. In a quantitative study by Dahbur, Bashabsheh and Bashabsheh (2017) that addressed security awareness, 52 percent of employees acknowledge awareness of an implemented information security policy. The number represents a slight decline from previous research that held at 58 percent. Study results also revealed a decline in the number of employees that acknowledged awareness of any information security policy, from 53 percent to 40 percent. The decline in both numbers indicate policy challenges within organizations that may not be caused by the mere presence of a policy; rather, educating the workforce to acknowledge and understand these policies. According to Da Veiga (2016), employee reading of security policy significantly contributes to improving information security culture.

A recent case study by Da Veiga (2016) compared information security culture among employees in two parts. The first involved information security culture differences of employees who had reviewed the current information security policy as opposed to those who had not done so. The second involved determining whether time permits for a stronger information security culture for employees who acknowledge reading the supporting guidelines and procedures. The primary aim of research was to provide empirical evidence to corroborate literature perspectives on the influence of information security policy on information security culture. A secondary aim was presenting empirical evidence that a strong information security culture can be developed

over time, provided employees become aware of, and understand information security policy. The study was conducted at four separate intervals, spanned an eight-year period, and involved a single company with a presence in 12 countries. A validated information security culture assessment (ISCA) questionnaire served as the measurement tool. The ISCA consists of nine constructs, one relating to information security policy. Responses to 44 total ISCA-related statements are used to assess information security culture. Of the 44 statements, 18 specifically relate to information security awareness. A five-point Likert scale assessed ISCA statement responses. A cross-sectional design collected data on multiple cases, at a single point, across different variables. For the initial iteration, the ISCA assessed existing levels of information security within the organization. Based on the results of the initial assessment, identification and implementation of numerous interventions occurred. A second ISCA was then conducted to determine if the interventions had a positive or negative impact on information security culture. This cycle occurred four times. During the first year of study, the company employed 3,972 personnel. The number rose to 8,220 by the fourth, and final, iteration. Surveys were disseminated by electronic means to all employees in all countries. Each ISCA data collection period lasted five weeks and responses for each period achieved 95% confidence levels. The study findings signify overall improvement of security culture following each ISCA and associated set of interventions. Essentially, this indicates that information security culture can cultivate and become more positive over time. The findings also indicate strong support for the positive influence that reading security policy has on security culture. Based on data analysis, there exists a clear distinction in the responses provided between employees who reviewed the policy and those who did not. Employees who had reviewed the information security policy presented an obviously stronger information security culture that was indicated by risk-averse

behavior. A documented information security policy that employees read by is crucial for formulating an effective information security culture. Employees who did not review the information security policy, for whatever reason, will be less effective in contributing to a positive information security culture (Da Veiga, 2016).

Research conducted by D'Arcy and Greene (2014) addressing security culture and employment relationships as drivers on security compliance indicates many organizations remain challenged with employees failing to comply with information security policies and procedures. Employees who prioritize work production over security or who possess other sinister motives account for over half of all security incidents. Security incidents can pose significant hardships for organizations by damaging reputations, causing financial strain, and a loss of trust. Of note, the estimated average cost of a major security breach was \$415,000. Over half of all security incidents originate from a human source internal to the organization. Ergo, it is imperative organizations approach security policy development with employees in mind. As previously noted, Da Veiga (2016) provides evidence of increased security compliance by employees who read the organizational information security policies as compared those employees who do not. Organizations that fail to focus on individual and other organizational issues, alongside technology-based solutions, may fail to achieve the necessary levels of success in their efforts (Donahue, 2011; Ifinedo, 2014; Karlsson, Åström, & Karlsson, 2015; Warkentin, Johnston, Shropshire, & Barnett, 2016). Rhee, Kim and Ryu (2009) note that merely identifying information security requirements through policy and not implications for non-compliance limits the effectiveness of security measure applicability. When considering primary motivation theory (PMT), Workman, Bommer and Straub (2008) suggest policy that educates employees on security requirements along with penalties that indicate severity to prevent unauthorized

disclosures. As a result, employees exercise security measures with a higher regard when employees realize such measures are accompanied by swift and severe consequences.

2.5 Security Education, Training, and Awareness

Karjalainen and Siponen, (2011) contend a major concern for organizations is insufficient employee non-conformance with security policy. Training is the most widely adapted approach for improving employee security behavior. While numerous training methods focus on changing employee behavior, literature falls short of studying the characteristics of how information security training differs from other training. With wide agreement by scholars and practitioners on the need and importance of information security training, the void of information security training theory defaults to a training focus on practical application that fails to recognize fundamental characteristics. The study presents a supported framework and meta-theory orientations that distinguishes distinct pedagogic characteristics of information security training and was detached from other training methods, thus providing a basic azimuth for the conduct of information systems security application. Additionally, four pedagogic pillars for creating and assessing information systems security training methods are provided, as no single information systems security training approach exists that reflects all four of these requirements. Lastly, a pedagogic model was presented for evaluating the conduct of information systems security training. A qualitative study assessed 32 information systems security training approaches and grouped them into seven distinct training categories (psychological, learning theory, security awareness, process-oriented, situational, social engineering preventive, and computer-based training). Of the 32 information systems security approaches reviewed, only 12 (37.5%) addressed a theoretical concept, while others were void of any theoretical notation. The study findings provide support for development and implementation of a meta-theory approach

conducive to effective information security training. The supporting meta-theory framework consists of three levels (intuitive thinking, critical thinking, and meta-level thinking). The intuitive level signifies a status quo to the extent that training validity and methods are not questioned. Indicating, utilization of a standardized approach that never changes over time will cause stagnation, devalue training, and prevent progression into the higher realm of critical thinking. The researcher finds it was only when the training validity and methods are contested that a transition into the critical level of thinking occurs. Critical thinking connects pedagogical requirements for information systems security training to find the most appropriate means for enabling employees to analyze, synthesize, evaluate, and apply knowledge within the organizational context and individual work experiences. This occurs through feedback, self-critique, and indications of training ineffectiveness. At the critical level, intuition and innovation set the stage for modification, refinement, or omission of information systems security training. At the meta-level, thinking facilitates understanding of how information systems security training diverges from other information systems security teaching practices because of organizational-specific, non-cognitive contexts. Within the organizational context of information systems security training at the meta-level, a non-cognitive and persuasive approach is needed as altering procedures and established norms contend to be more challenging for employees who may not be fully committed to embrace the changing information security culture (Karjalainen & Siponen, 2011). Thus, the theoretical framework for IS security training presented was based on pedagogical pillars of meta-theory orientations. Meta-orientations allow an understanding the fundamentals of educational philosophy and permit a more solidified examination of information systems security training. Karjalainen and Siponen (2011) explain the four pedagogical requirements (psychological context, content, teaching method, and

evaluation of learning) for designing and assessing information systems security training approaches. The first pedagogical pillar, psychological context, styles teaching and learning from a group-oriented theoretical approach focused on the collective rather than the individual. The focus was developing the collective ability to improve effectiveness in complex working environments, especially when collaborating or working in teams. The second pillar was content focused and emphasizes teaching content built upon employee collective experiences, as security policies promote community-centered understanding and collective implementation. The third pillar consists of teaching methods and emphasizes collaborative learning intended reveal and produce collective knowledge. This teaching method facilitates communal change in employee information security attitudes and behavior. The fourth pedagogical requirement, active experimentation, aims to integrate learning experiences from the learning community to determine the way forward for defining new policy and instruction. Learners then implement and evaluate these new changes as validation and acceptance. The ultimate objective of IS security training is changing employees' behavior so that compliance with information security policy emerges as a normal and accepted occurrence within organizational culture.

The researcher believes the sole reliance on technology-based approaches to ensure a positive information security culture is inadequate. It is imperative that information security give ample attention to users' behavioral perspectives. Regardless of an organization's technological prowess, insufficient employee consciousness of information security poses an unnecessary risk. Users' behavior plays a crucial role in information security. The onus is on organizations to shape employees' views and beliefs toward protecting information by integrating and aligning information security culture with organizational culture. Thus, the criticality for organizations to create an environment of employee conscious responsibility exists. According to a case study

performed by Tang, Li and Zhang (2016), organizational cultures that promote information security policies related to the handling of information will improve overall information security posture. Their study examined how organizational culture influences the information security culture of a large organization utilizing a comprehensive case study. Organizational culture is unique and its character and its norms is defined using an assortment of values that can include leadership styles, reward and punishment systems, workforce communication, and manners of decision-making. The case study utilized a theoretical framework that defines organizational culture as "the manifestation of information security practices or behaviors evolving from the shared beliefs and values in the organization." This supposes a relationship between an organizations culture, and actual practices or observable actions implemented by said organizations. The literature review for the case study highlighted three key points:

- 1) security culture consists of social, cultural, and technical security measures that contribute to organizational culture;
- 2) the need for a standard system of certification and measurement of employees' information security attitudes toward and knowledge of information security; and
- 3) the need for an integration of information security behaviors with organizational culture. (p. 180-181).

The research framework utilizes two constructs; one for organizational culture, and one for information security culture. The organizational construct consists of six dimensions:

- Process oriented versus results oriented.
- Employee oriented versus job oriented.
- Parochial versus professional.
- Open system versus closed system.

- Loose versus tight control.
- Normative versus pragmatic (p. 184-185).

Tang, Li and Zhang (2016) suggest these dimensions stem from perceptions that emerge out of normal employee and organizational operations. The information security construct separates into four dimensions (compliance, communication, accountability, and governance) that shape the collective beliefs and values of employees. The study also decomposed four dimensions of information security within the theoretical framework that drew a relationship to technical, human, and organizational views. They include conformity with information security guidelines (compliance), information security communication to employees (communication), organizational response to violations of information security procedure (accountability), and the degree of information security importance within the organization (governance). The researchers find these dimensions serve as the variables of information security construct for the study. The qualitative case study involved the largest garment manufacturing organization in China. The firm produces many internationally recognized brands, with over 50,000 employees located in China. A three-stage data collection process utilizing interviews occurred over a six-month period. Three groups separated workers into three groups: senior management, middle management, and regular employees. Senior and middle management interviewees possessed at least 10 years of company experience. All regular employees had at least five years of company experience. The first stage of data collection intended to collect interviewee opinions to understand the employee knowledge of daily organizational practices. The second stage implemented an open-ended questionnaire addressing organizational culture that supported qualitative analysis. During stage three, focus groups consisting of a mix of interviewees met to discuss findings from the first two steps, and each presented their opinions of the findings. The

study findings suggest the influence of organizational culture on information security culture. Although each of the six dimensions of organizational culture did not directly influence each of the four information security culture dimensions, the totality of influence relationships does cover all dimensions from both cultures. The case analysis demonstrates a framework suitable for further explaining the relationship between organizational culture and information security culture. This research will supplement that of Tang, Li and Zhang (2016) by attempting to validate a measure for information security culture and by proposing and empirically examining an information security model.

2.6 Quantitative Research Models

Security compliance intention research model. Ensuring employee security conformity with established security policy and procedures remains a challenge for organizations. D'Arcy and Greene (2014) developed a security compliance intention research model (Figure 3) to examine security culture and employee relationships as forces shaping employee security compliance decisions.

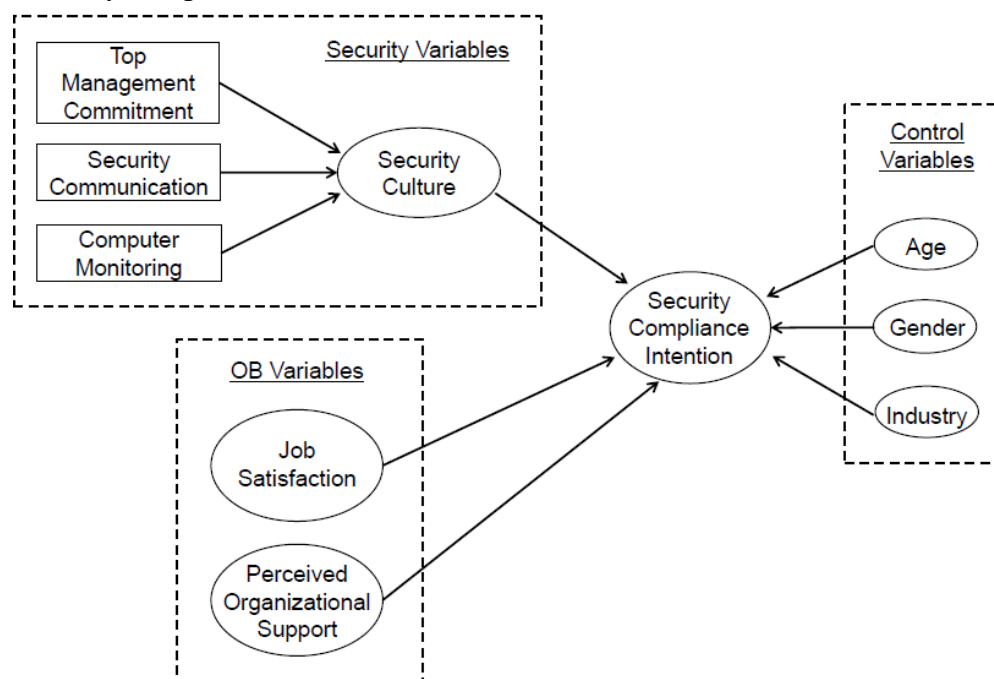


Figure 3. Security compliance research model.

Their intended purpose of contributing to existing security compliance literature involved investigating influences of employee behavior, security culture and employment relationship. Senior manager commitment, security correspondence, and information system monitoring were antecedents to security culture. The construct of organizational behavior consisted of two variables; job satisfaction and perceived organizational support. The security variable and the two organizational behavior variables were predictors of the independent variable, security compliance intention. The demographics of age, gender, and industry served as control variables. Interviews conducted with 13 security professionals provided an additional measure for validation for the three dimensions. Interviewees were information security officers, information assurance specialists, and security incident response personnel from small-to-medium sized organizations. Interview transcripts were coded into a multidimensional construct using ATLAS.ti.8 (version 5.5). Data collection utilized two internet-based surveys administered two weeks apart and approved by the institutional research board. Demographics and security compliance were measured for the first survey and the three dimensions addressed in the second. The two-stage survey allowed the separate collection for independent and dependent variables, reducing the possibility of patterned responses by participants. The survey used was a compilation of formerly validated measurements and original items. Response measures used a five-point Likert scale. Survey participants includes 223 computer-literate employees of various organizations throughout the mid-Atlantic region. Participants were selected from a professional contact list and received an email invite for survey participation. The first survey resulted in 146 responses, 134 were usable. The second survey resulted in 127 usable responses. The study results suggest security related and common work-related tasks are contributors to employee security compliance. Study findings support security culture not only

serving as an indicator of workplace security compliance, but also as an essential factor for implementing information security management programs. There also exists supplementary evidence that position and tenure within the organization moderate these factors. Since the effect of security culture was noted as having a comparatively strong influence among groups, no significant distinction was possible with respect to years of organizational experience. The organizational behavior variable [job security] sheds light on compliance factors that motivate behavior. A study finding that emerged was the connection between employees' work relationship and security compliance intention. Elevated levels of job security appear to portend increased predisposition for compliant security behavior. Accordingly, this suggests that positive employee satisfaction with their work environment can augment information security culture. Unexpectedly, there was a negative association between perceived organizational support and security compliance intention. The researcher indicates employee perceptions of high levels of organizational support contribute to the belief that information technology or security professionals will handle information security issues, making individual compliance practices less important. Another possible rationale for lower levels of security vigilance is when end-user perceptions of increased organizational support are interpreted as an abundance of security controls. The study provides empirical validation of information security culture. Encouraging information security compliance with policy and procedures remains a challenge for organizations. Employees routinely make conscious decisions of whether or not to comply with established policy. Violations of such mandates occur when employees elect to prioritize work productivity over compliance with existing security policy and practices. More than half of all information security breaches originate from unsatisfactory security compliance. The researcher implies, organizations must clearly communicate end-user responsibilities, regardless

of the technical features or security measures in place. Employee security compliance is the key to information security success and achieved through the actions and awareness of employees.

Compliance intention [non-compliance] research model. Security incidents are classifiable into a number of different categories. Among those categories, incidents involving human perpetrators who are working within the organization are the most difficult to prevent. Hwang, Kim, Kim and Kim (2017) investigated the causal relationships between information security efforts and causes of non-compliance, which negatively leads to compliance intention. Their research model (Figure 4) highlighted organizational security efforts as important influencing factors in reducing employee non-compliance.

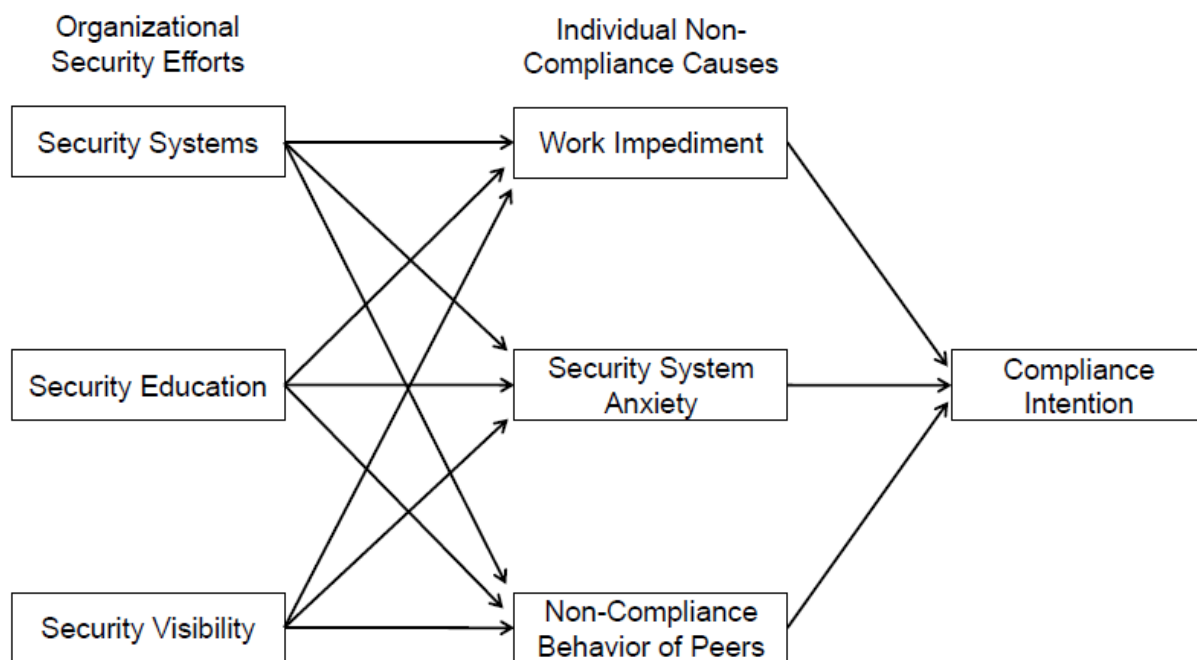


Figure 4. Security compliance intention research model.

In their model, the construct of organizational security efforts (security systems, security education, and security visibility) serves as antecedents for individual non-compliance causes. According to Hwang, Kim, Kim and Kim (2017) employees feel security policies reduce their work efficiency. Employees who view security policies as ambiguous may develop anxiety

when using information systems. Employees also tend to follow the culture of the organization. If co-workers are known not to comply with security policy, the chance increases that others will act similarly. Information security policies, just like many other policies, address potential penalties for non-compliance. These penalties can result in anxiety, which may be a reason for not complying. Individual non-compliance causes (work implementation, security system anxiety, and non-compliance behavior of peers) served as antecedents for security compliance intention.

Measurements for variables were derived from existing questionnaires and modified to meet study intent. Ten doctoral students and researchers with practical experience ensured content validity. Questionnaires used a seven-point Likert scale to measure responses. Data collection sources were employees from manufacturing and service organizations in the process of implementing security policies. To increase validity, data received from employees of organizations with no security policies were excluded. The duration of data collection lasted one month and 457 total responses were received. With 42 responses excluded, 415 observations were used for the study. The measurement model was validated through confirmatory factor analysis. The measurement model and data set characteristics were tested to cleanse the model. Four goodness-of-fit indices and one approximation test was conducted. Overall fit indices results were good. Next, item reliability through factor loading analysis was tested using individual item loadings. Item reliability results from factor analysis indicate appropriateness of the survey tool for individual measurement of each construct, with reliability results for all items exceeding 0.5. The measurement model validity was assessed through internal consistency. The results using Cronbach's α fell within the range of 0.843 to 0.968, higher than the minimum score of 0.70, demonstrating internal consistency of the measurement model. Study results

indicate individual non-compliance causes negatively affect compliance intention. Additionally, organizational security efforts (independent variables) reduce individual non-compliance behavior of co-workers. Essentially, all organizational security efforts negatively impact individual non-compliance causes, which are antecedents to compliance intention. Numerous studies have sought to gain insight into the reasons for non-compliance when handling classified information (Hwang, Kim, Kim and Kim, 2017).

The fear appeals model. As part of the SETA program in some organizations, information is disseminated to employees encompassing persuasive messages of security compliance. Accordingly, some of these messages may embed an element of fear, otherwise known as a “fear appeal”. Empirical research by Johnston and Warkentin (2010) consisted of an experiment to study the influence of fear appeals on end-user compliance. The study, *"Dispositional and situational factors: influences on information security policy violation"*, performed an examination of how behavioral intentions are influenced by fear appeals, with a specific focus on end-user compliance. The primary research question sought to find how fear appeals modify behavioral intentions of end-user’s security actions. The experiment conducted in a university setting involved a mix of 780 faculty, staff, and students. Of the total number of subjects, only 311 (40%) participated. The six constructs [variables] used in the study measured "behavioral intent, social influence, response efficacy, self-efficacy, threat severity, and threat susceptibility" (p. 555). Responses were recorded using a five-point Likert scale. A panel comprised of eight individuals with expert knowledge in quantitative and quantitative research convened to validate content. The research was nestled in the theoretical foundations of primary motivation theory (PMT) and the study used a conceptual fear approach model (FAM), as FAM

relates to the theoretical support for cognitive recognition of threat and efficacy when confronted with fear appeal. Figure 5 depicts the fear appeals model.

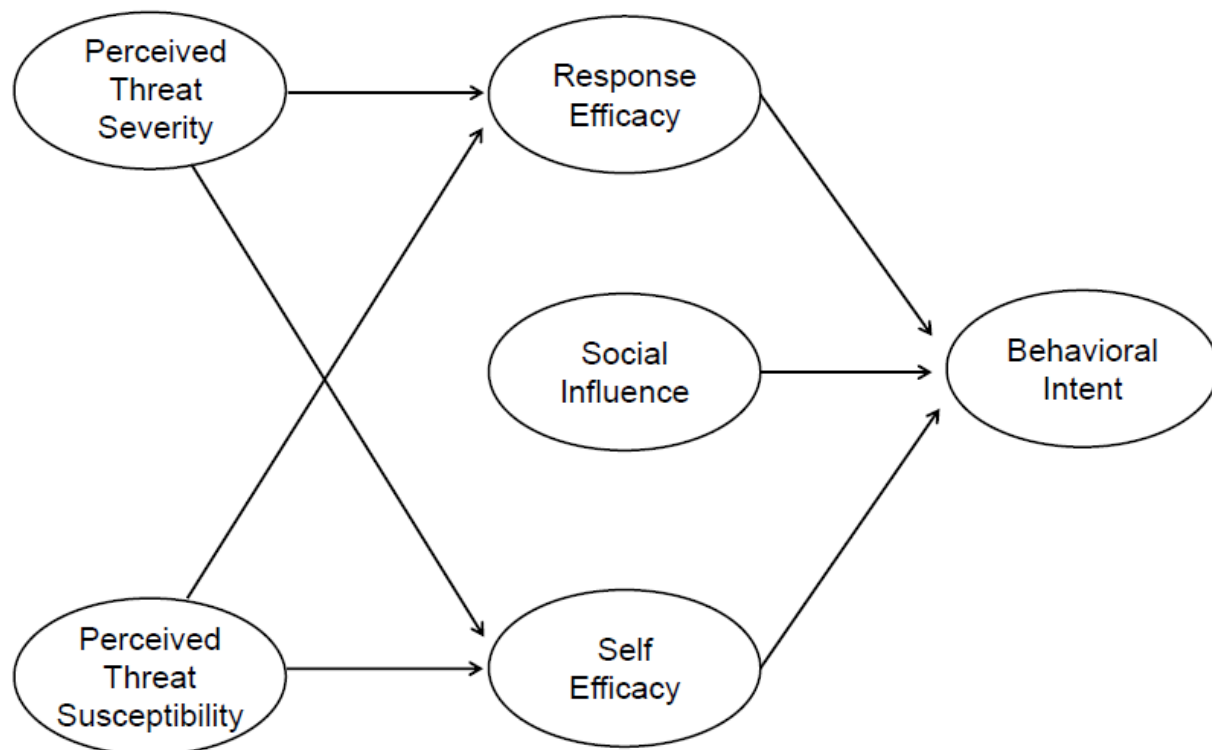


Figure 5. Fear appeals research model.

Perceptions of threat severity and perceived threat susceptibility were direct antecedents of response efficacy and self-efficacy. Response efficacy and self-efficacy served as antecedents directly influencing behavioral intent. Behavioral intent is directly influenced by three antecedents; "response efficacy, self-efficacy, and social influence". Study findings imply fear appeals impact employee behavioral intentions (of compliance or non-compliance) with security policy. However, there is no consistent impact common to all end-users. The findings suggest communication induces diverse outcomes for individuals based on perception of efficacy and threat. Conclusions from this study support using fear-inducing content as a useful method of influencing end-user intentions to comply or non-comply with security policy. However, implementation of a single approach will likely not meet organizational intent of reducing

security vulnerabilities. Instead, leadership must devise a strategy for communication that consists of fear appeals suitable to employee self-efficacy levels

(Johnston & Warkentin, 2010).

The individual security behavior model. Previous literature studying employee behavior within organizations assumed a behavioral approach in an effort to improve security behavior. Other literature considered single fear-based theories, such as primary motivation theory (PMT). Yoon and Kim (2013) empirically tested a model (Figure 6) of individual workplace security behaviors.

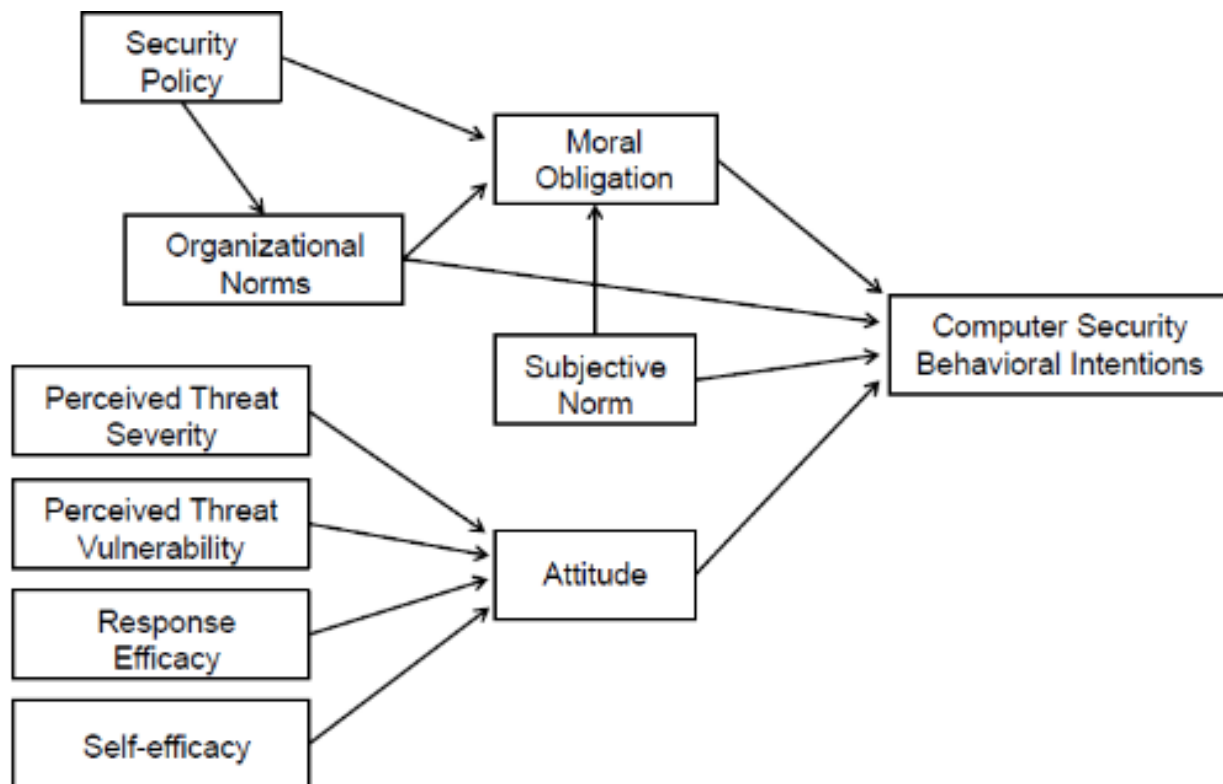


Figure 6. Individual security behavior research model.

The study offered a comprehensive model based on a theory of reasoned action (TRA), moral obligation, PMT, and a series of organizational specific dynamics to understand employee security behavior. Deterrence variables (i.e., rewards and sanctions) were excluded from this model because research indicates the use of sanctions did have an impact on employee intent to

comply with security policy. Alternatively, self-control factors are deemed relevant because compliance with organizational security requirements was seen as a duty, not necessarily requiring a reward. The individual security behavior model positioned four direct antecedents of "computer security behavioral intentions; moral obligation, subjective norm, organizational norm, and attitude" (p. 412). Organizational norms served as an antecedent to moral obligation, subjective norms, and computer security intentions. Information security policy was placed as an antecedent to moral obligation and organizational norms. In addition to serving as an antecedent to behavioral intentions, subjective norm also served an antecedent to moral obligation. The PMT aspect of this model integrated the variables of "perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy" (p. 412) as an antecedent to attitude. Figure 4 depicts the individual security behavior model. Yoon and Kim (2013) used a web-based questionnaire as a survey method. Of those questionnaires received, 162 were analyzed. Respondents included manufacturing, finance, distribution/services, telecommunications firms, and research institute workers. A seven-point Likert scale measured all surveys. The findings asserted that there was no apparent statistical impact of TRA when it comes to employee intentions to comply with information security. Mediation analysis performed supports this assertion. There was a strong impact of moral obligation as a personal norm on employee behavior and intentions. In other studies, moral obligation received attention when it was associated with ethics. However, these researchers find the closeness of moral obligation and personal behavior with respect to duty was cause for increased visibility. Employees engaging in work related security activities may recognize a moral obligation to conform over a personal behavior. The PMT variables were assessed as significantly impacting end-user information security behavior. The strong impact of response efficacy in end-user

attitudes implies that users who feel their security behaviors are effective and practical will place greater emphasis on computer security compliance. Individual attitudes toward computer security were not significantly impacted by the perceived threat vulnerability. One contributor to this finding may be the organizational environment. Most organizations have a dedicated group of information technology personnel responsible for protecting the operating environment. Accordingly, end-users may believe the chance of exposure to an outside threat was minimal (Yoon & Kim, 2013).

The protective security behavior continuance model. Additional research relating to the consensus that end-users are the greatest vulnerability to the protection of IS uses the PMT motivation theory as an underlying theory for motivation. Warkentin, Johnston, Shropshire and Barnett (2016) take a novel approach by looking beyond the initial security behaviors. Their approach implements a protective security behavior continuance research model (Figure 7) to measure the continuance of security measures proceeding initial adoption.

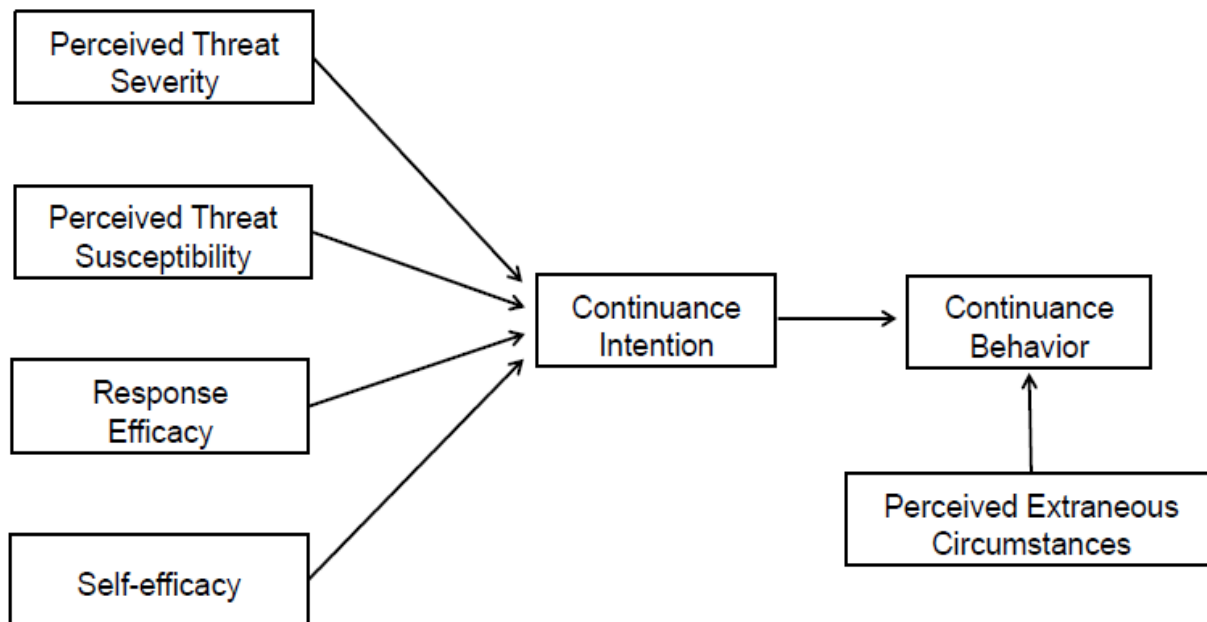


Figure 7. Protective security behavior continuance research model.

Using PMT as a fundamental theory, the constructs of "threat severity, threat susceptibility, self-efficacy, and response efficacy" serve as antecedents to predict intent and continued behavior. Their approach attempts to address the longevity needs of security. End-users tend to comply when there is a perceived threat. This perception may change over time. If there is no situational awareness of incidents, the perception of risk may dissipate and end-users are likely to perceive less susceptibility of risk and less of a need for security compliance. A second aspect of this approach considers continued adherence to policy. Continuance intention serves as an antecedent of continuance behavior. If end-users are adhering to policy and security incidents still occur, despite their valued efforts, they may question the effectiveness of current requirements. To account for attitude-behavior inconsistency, perceived unrelated conditions are included as a significant determinant of security behavior continuance. This construct attempts to measure the degree a person recognizes when unanticipated actions intercede with behavior. While some individuals maintain previously assumed behaviors caused by cognitive intention, others may cease identical actions because of perceived unrelated conditions. Warkentin, Johnston, Shropshire and Barnett (2016) implemented a longitudinal study to measure continuance behavior of subjects covering several weeks. Web-based software recorded information and identified those whose computer received a desktop security application. A questionnaire aimed at testing continuance model constructs was sent via electronic means to those using the security program. Participation was voluntary and there were no incentives. The study findings indicate individual compliance with protective security behaviors was influenced by themes not related to behaviors themselves, but with circumstances surrounding the behaviors. Another finding questions the relationship between response efficacy and continuance intention. According to study's findings, when end-users develop intentions to

continue preventive actions, they consider environmental threats [severity and susceptibility], and the capacity [self-efficacy] to carry out said actions. However, they are inclined to neglect the efficacy of the actions. The researcher implies the impact of protection security behavior discontinuance can be quite harmful to organizations. Damage can occur to hardware, software, data, and in some cases, damage may be beyond repair. Continued emphasis of policy and practice is necessary to protect organizations. While policy can be written to alleviate the human factor as much as possible, it is impractical to remove processes that require judgment or flexibility. In these instances, a trained workforce must be trusted to adhere to security policy (Warkentin, Johnston, Shropshire, & Barnett (2016).

The recomposed theory of planned behavior (TPB) model. Ifinedo (2014) tells us that organizations invest heavily in IS security in today's environment. Information and asset protection are major organizational concerns. Organizations employ technical and digital solutions for the protection of critical IS assets. However, they are inadequate for providing total protection. A good IS protection approach should incorporate technological, individual, and organizational aspects. Organizations that neglect to focus on individuals are bound to fail, as individuals are the weakest IS link. Therefore, organizations need to focus on employee intentions and behaviors as part of safeguarding IS. While organizations may promulgate sufficient guidance and policy for using IS, employee compliance is not absolute. According to Ifinedo (2014), the preponderance of prior security compliance research approached from the view of criminological theories and the health belief model. Ifinedo (2014) investigated behavioral intentions toward security policy compliance from the vantage point of social and cognitive theory. Integration of the theory of planned behavior (TPB), an umbrella for social cognitive theory (SCT), with social bond theory (SBT) was viewed as suitable for work settings

where common ties may influence work related perceptions and behaviors. Their recomposed TPB research model (Figure 8) suggests that normative thinking leads to subjective norms. Meaning, when work-related pressure or social influences indicate individuals or groups recognize and accept a behavior, people feel socially pressured to act in a commensurate manner.

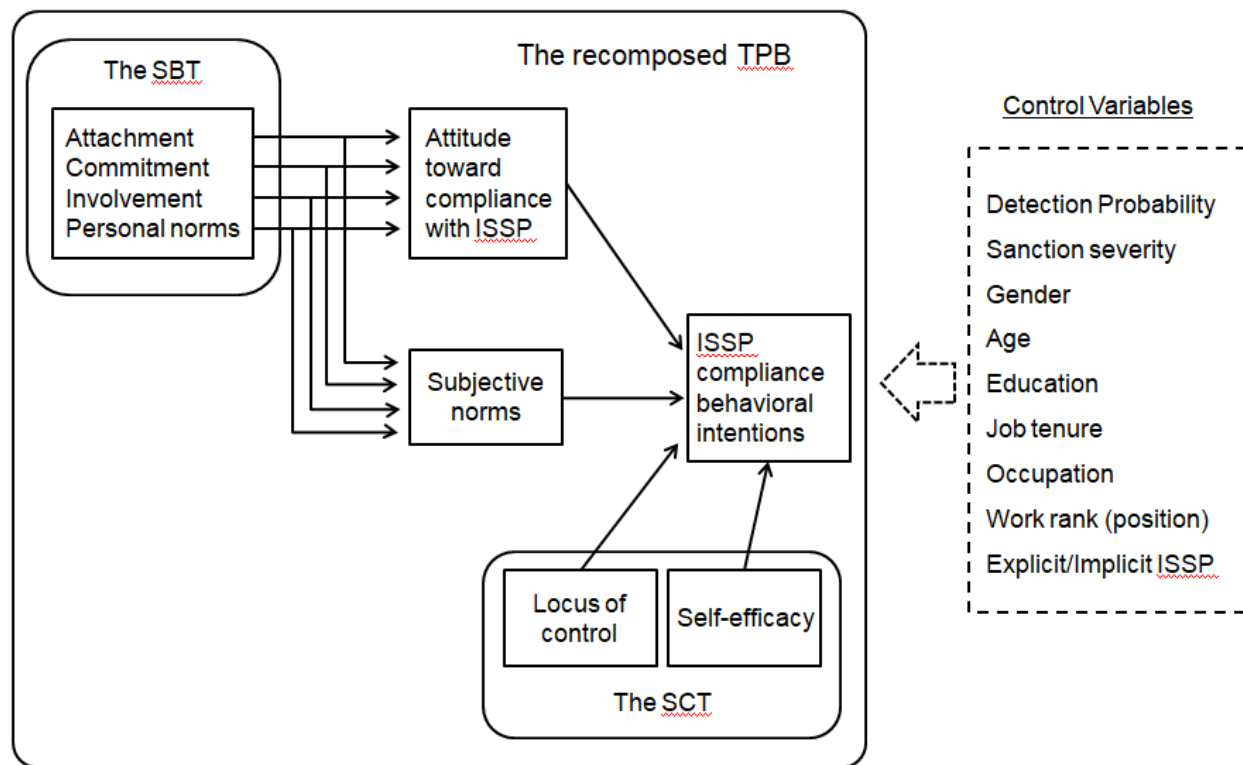


Figure 8. The recomposed TPB research model.

SBT's constructs, antecedents to subjective norms, share a close relationship with subjective norms by overtly measuring social bonding in organizations. SBT constructs (attachment, commitment, involvement, and personal norms) are also positioned as antecedents to attitude toward compliance with IS security policy and subjective norms. The SCT constructs of self-efficacy and self-control, along with subjective norms and attitude toward compliance with IS security policy all serve as antecedents of ISSP compliance behavioral intentions. Twenty knowledgeable professionals with security policy experience assessed the questionnaire

for face validity. A field survey tested the research model. One thousand non-IS managers from a marketing and data firm were mailed a questionnaire and cover letter, along with a self-addressed, stamped envelope. Of those, 106 were undeliverable. Seventy-six (8.5%) total responses were received. Eight responses were excluded for various reasons. The remaining 68 responses provided data from the first source. The second source consisted of IS professionals throughout the country. An online version of the survey questionnaire captured responses. Although participation was voluntary, monetary incentives and the opportunity to view results served as motivation for participation. Both sources totaled 124 usable responses, considered adequate for the study. Findings do not support an employee's decision to conform to organizational security policy was dependent on perceived sanctions and penalties. The study furthers knowledge of security policy compliance by signifying the impact of socialization, influence, and cognition on security policy compliance behavioral intentions. Employees build communal ties on the job and may look toward those of prominence to assess the suitability of particular beliefs and behaviors. These bonds influence employee attitudes towards security policy compliance. The findings did confirm that employees who perceive control over workplace dynamics willingly accept responsibility for their actions. The researcher confirmed that when employees perceive control over workplace issues impacting them, they are likely to accept accountability for their security policy related actions. Employees who are adequately equipped and trained must still decide whether to comply with organizational security policies (Ifinedo, 2014).

Organizational information security culture model. In a quantitative study using descriptive analysis, Pierce (2012) evaluated factors that contribute to the integration, implementation, and maintenance of a successful organizational information security culture.

The research model was limited to five factors that served as independent variables, while information security culture served as the dependent variable (Figure 9).

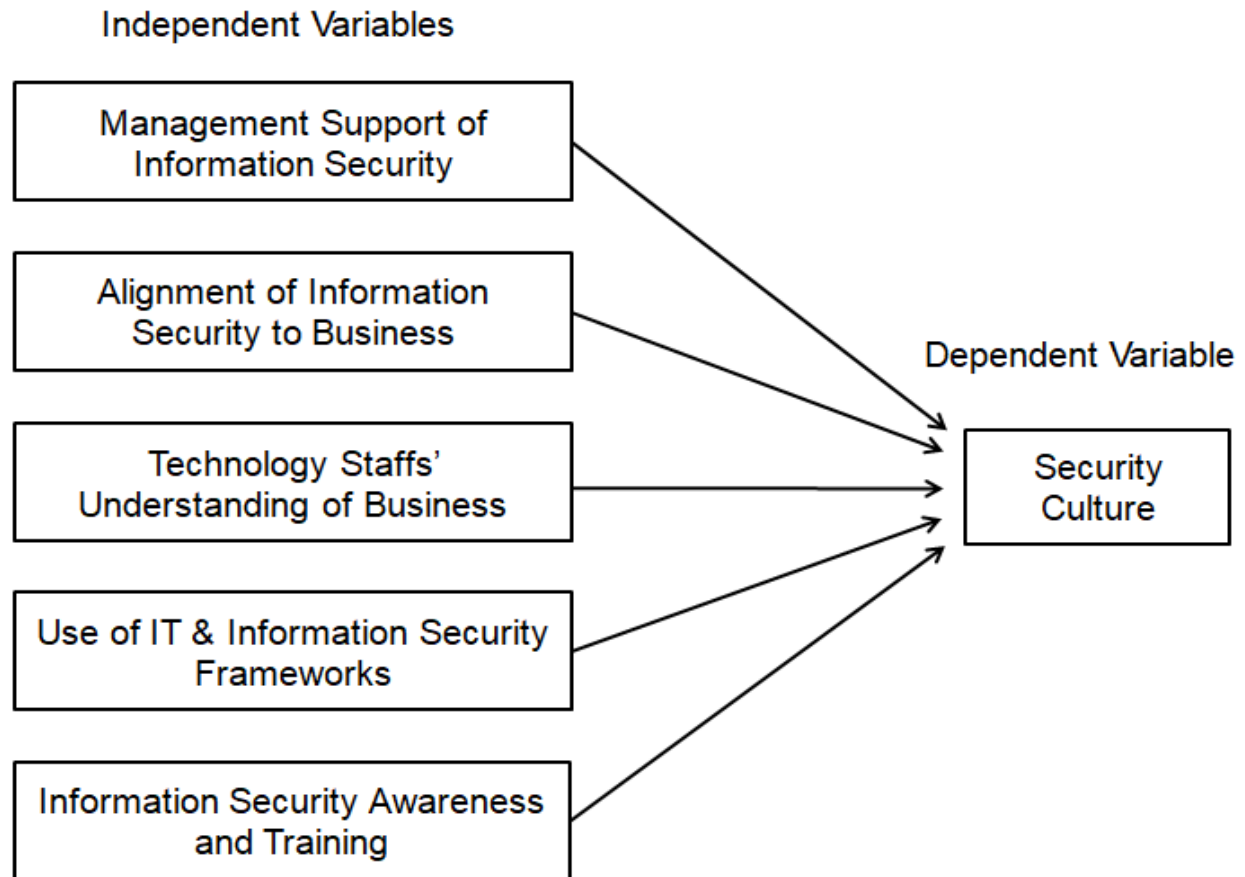


Figure 9. Organizational information security key factors research model.

According to Pierce (2012), factors were chosen because their crucial role in the execution of a comprehensive information security program and include: management support of information security, alignment of information security to business, technical staffs' understanding of business functions, use of information technology and information security frameworks, and SETA programs and training.

Research questions in the study intended to determine the extent of relationship between independent variables and the dependent variable (information security culture). The hypothesis

for all research questions predicted a positive determinant of all variables on information security culture. An internet-based survey instrument created specifically for this study underwent a field test by five experts in the information security field, all possessed an advanced degree.

Modifications to the survey instrument occurred after reviewing the field test feedback. A pilot test of 30 individuals from multiple organizations in northwestern Florida confirmed survey validity and reliability. Statistical Package for the Social Sciences (SPSS) ensured validity, while Cronbach alpha provided reliability. A five-point Likert scale gauged response to participant perceptions of the five independent variables (key factors) and the dependent variable (successful information security culture). The survey instrument was a 35-item questionnaire (five were demographic questions). A random sampling approach collected data from organizational managers, IT professionals, and knowledge workers through random sampling. Of the 282 initial invites sent to participants, 200 of the responses received were ultimately determined useable. With many organizations sensitive about their information security posture, a non-intrusive survey avoided collection of any personally identifiable information. Although relationship strengths were not as strong as expected, findings did indicate a positive relationship between the independent variable perceptions and a successful organizational information security culture. Variables with the strongest to weakest relationship were;

- 1) information security awareness and training,
- 2) use of information technology and information security frameworks,
- 3) management support of information security,
- 4) alignment of information security to business Technical Staff's, and
- 5) understanding of business functions and alignment. (p. 6)

A study limitation is that it is not generalizable because of participant limitations. Another limitation in this study was the specificity of industries selected for participation preclude generalization across a wider range of organizations (Pierce, 2012).

Information security culture model. A large number of security incidents are attributed to employee negligence and originate from within the organization. To prevent such incidents, organizations must implement policies and procedures as part of a comprehensive information security program. A study by Chen, Ramamurthy and Wen (2015) assessed the central aspects of extensive information security programs and their influence on organizational security culture. Their research model (Figure 10) assesses the relationship between principal elements of information security programs and security culture.

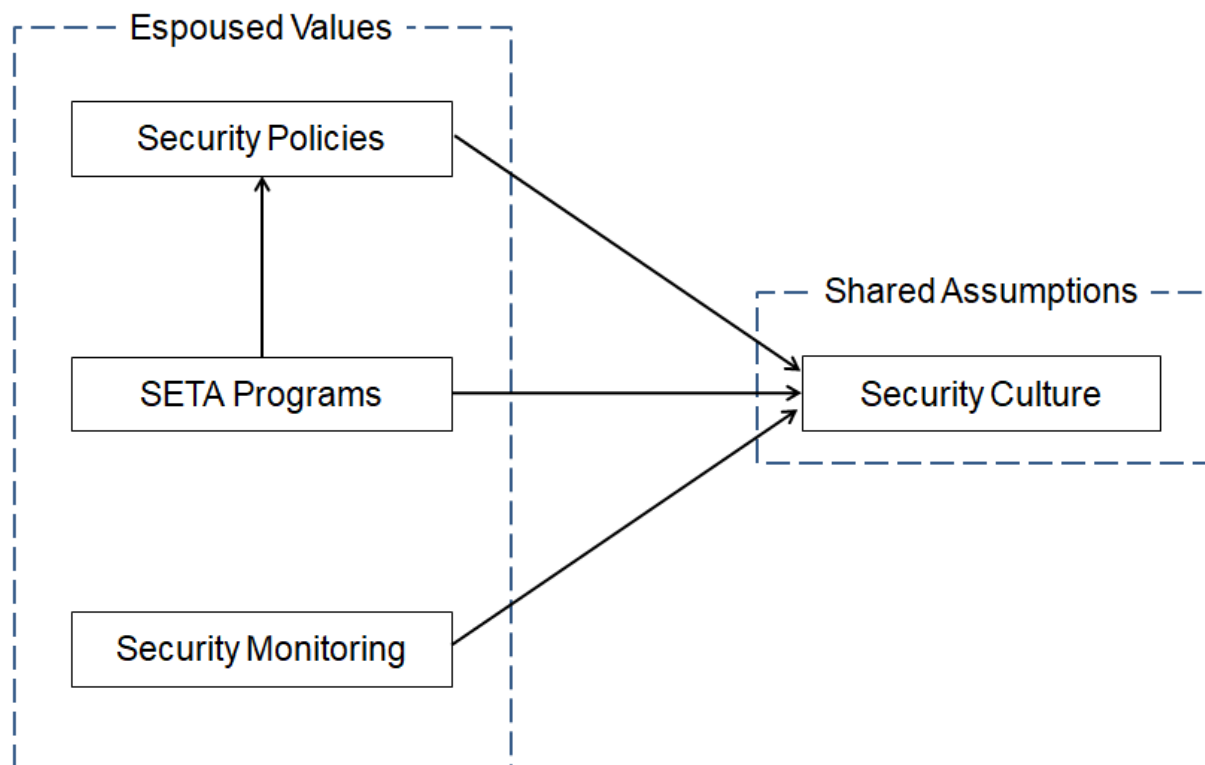


Figure 10. Comprehensive information security culture research model.

Two constructs composed the research model; espouse values and shared assumptions.

Espoused values constitute the dependent variables and include security policy awareness, SETA programs, and security monitoring awareness. Shared assumptions comprised security culture and serves as the independent variable. All espoused values are antecedents of security culture.

Figure 10 depicts the information security culture model.

Chen, Ramamurthy and Wen (2015) note the hypothesis for this study predicts a positive relationship between dependent variables and the independent variable. The results suggest SETA programs awareness significantly influences both security culture and employee awareness of organizational security policy, while employee awareness of security monitoring was found to impact security culture. Using a quantitative approach, measurement indicators were derived from literature reviewed to develop questions using 7-point Likert responses. Three pilot tests validated the survey instrument. The first two pilot tests consisted of eight security professionals from Midwestern companies who were responsible for the development and implementation of security policy within their respective organization. The third pilot test included three IT professionals who were pursuing an advanced degree at a major Midwest university. An online survey collected data. Participants represented four Midwest companies in the US, two of which participated in pilot testing. Participants totaled 124 volunteers and were not involved in any of the previous pilot testing. After removing unusable (incomplete or unanswered) surveys, there were 100 usable responses. The study highlights four key findings. First, SETA programs were noted as a strong influencing factor on organizational security culture. This finding implies that well-made SETA programs may shape workers' understanding of information security and their associated information security actions. Thus, ensuring the protection of information and contributing to an organizational security culture where employees

take ownership and assume responsibility for information security. This finding also validates the value of SETA programs, provided the intent is to create a strong environment that sustains a positive information security culture. A second finding pragmatically sustains the association between SETA program awareness and security policy. In particular the researchers found, the effectiveness of security policies is negated when employees fail to understand information security policy purpose and intent. A third finding highlights the effect of security monitoring that serves to detect employee compliance. According to Chen, Ramamurthy and Wen (2015), the finding implies a fundamental change from ordinary security monitoring philosophies where planning and implementation occurs among a select group of individuals. It implies incorporating employee's feedback into organizational efforts towards developing and implementing monitoring security schemes aimed at fostering a positive security culture. Lastly, findings did not signify a relationship between security policy awareness and security culture. A possible rationale could be the mere presence of organizational policies may not be sufficient for inspiring employee perceptions and beliefs that uphold a strong security culture. Another possible explanation could be that when considering all existing organizational policies, security policies become commonplace, blurring their association with organizational security culture. As such, the association between security culture and security policy should be regularly emphasized [reinforced] through training and enforcement. The study contributes to theory by building on security culture using Schein's (1988) organizational culture theory. It also contributes to practice with the introduction of a new research model that can be used for future studies examining the relationship between security culture and the antecedent espoused values provided in this model. Lastly, the research findings underscore the importance of findings offer significant support to the importance of security policies, security monitoring, and SETA

programs when creating a security culture within organizations (Chen, Ramamurthy, & Wen, 2015).

Contributors to a security culture. Information security has emerged as a legitimate objective for information technology departments. In light of regulatory increases, security mishaps, and emerging technologies, new and emerging threats necessitate that organizations allocate resources to adequately provide protection. While many organizations have increased funding for security-related technologies, they are missing the greatest challenge - the human aspect. A quantitative dissertation by Donahue (2016) assessed the influence of organizational culture on information security incidents. The study purpose was to determine whether relationships exist between the organizational culture and security incidents initiated by employees. The study utilized a modified organizational cultural assessment instrument (OCAI) and a security issue survey to assess current and desired culture. These items provide a snapshot of organizational behaviors perceived as requirements by workers. An online survey questions measured security incident, as well as characteristics that contribute to security culture over a four-week period. A five-point Likert scale recorded responses relating to the OCAI independent variable (organizational-culture type) and dependent variable (employee-initiated security incidents) and the security issue survey's dependent variables consisting of "senior

management support, information security policy, awareness training, and internal information security incidents" (p. 63). Figure 11 depicts the contributors to a security culture model.

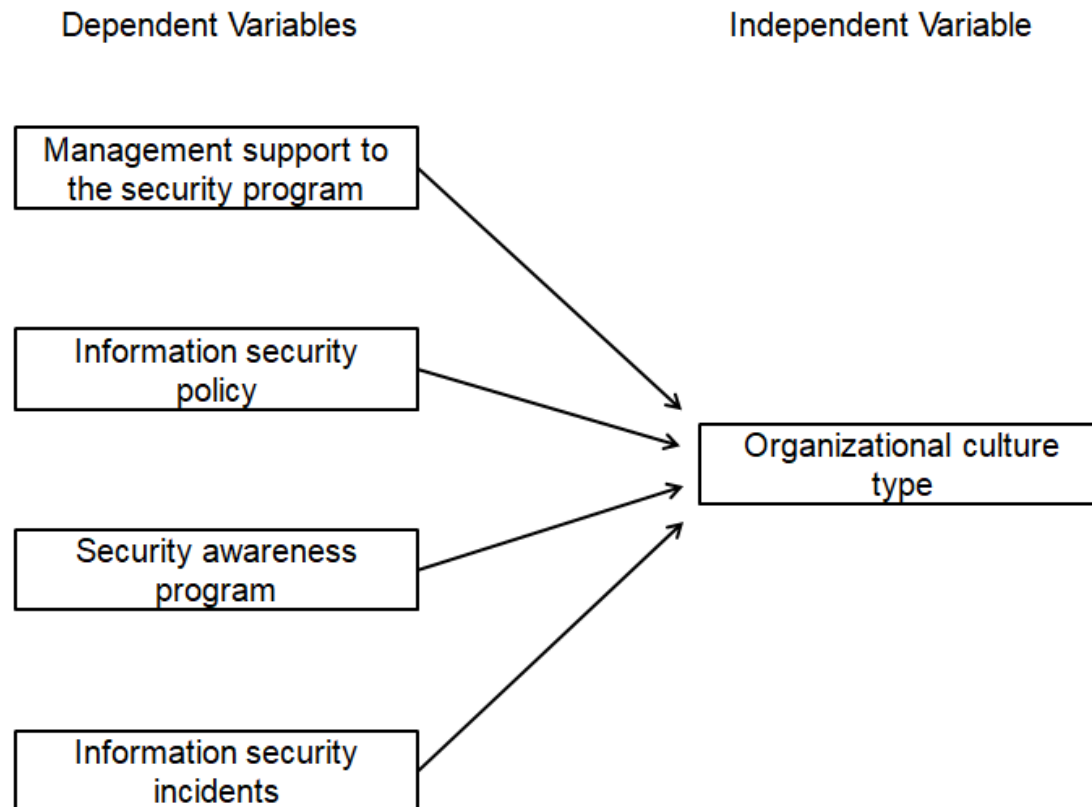


Figure 11. Contributors to security culture research model.

The subjects for this study consisted of 166 information security professionals throughout the United States currently active in the field of information security. Of the total responses received, 115 supported statistical analysis. The Statistical Package for Social Sciences (SPSS) 19.0 analyzed responses. Findings revealed a positive correlation between organizational culture and security incidents caused by employees. A significant positive correlation associated the relationship between organizational culture and employee-initiated security incidents. Additionally, while significant relationships existed between organizational culture and management support for the information security program, no significant relationships existed

between the hierarchy culture type and senior management support. Third, significant relationships existed between organizational cultures and senior management support. Surprisingly, the findings did not reveal a statistically significant relationship between organizational culture and security policies. The study attempted to highlight the relationship between culture and security incidents. Analysis results reveal three of the four dependent variables significantly relate to organizational culture. Since organizations have differing cultures, this study is not generalizable and different variables may be necessary to for similar studies on other organizations. A limitation of this study was the hesitation of participant, and to a greater degree security manager, willingness to provide confidential data that is organization specific, as this data may not accentuate an organizations true security posture (Donahue, 2016).

Expanded general deterrence theory model. Insider threats pose a significant risk to organizations. According to D'Arcy, Hovav and Galletta (2009), up to 75 percent of security incidents originate from within the organization. With such a high percentage of security incidents, it is imperative to understand methods of deterring such behavior. General deterrence theory (GDT) advocates the use of controls to increase individual understanding of certainty and severity for penalties associated with information security misuse. A study by D'Arcy, Hovav and Galletta (2009) offers an extended GDT model suggesting employee awareness [consciousness] of security countermeasures has an impact on employee perceptions [understanding] of the certainty and severity of adverse action that may result from information security misuse, which ultimately impacts information security misuse intent. The study findings advocate modifying the GDT model with an information security perspective to deepen

understanding of the fundamental security countermeasure processes governing employee compliance intent. Figure 12 depicts the extended GDT model.

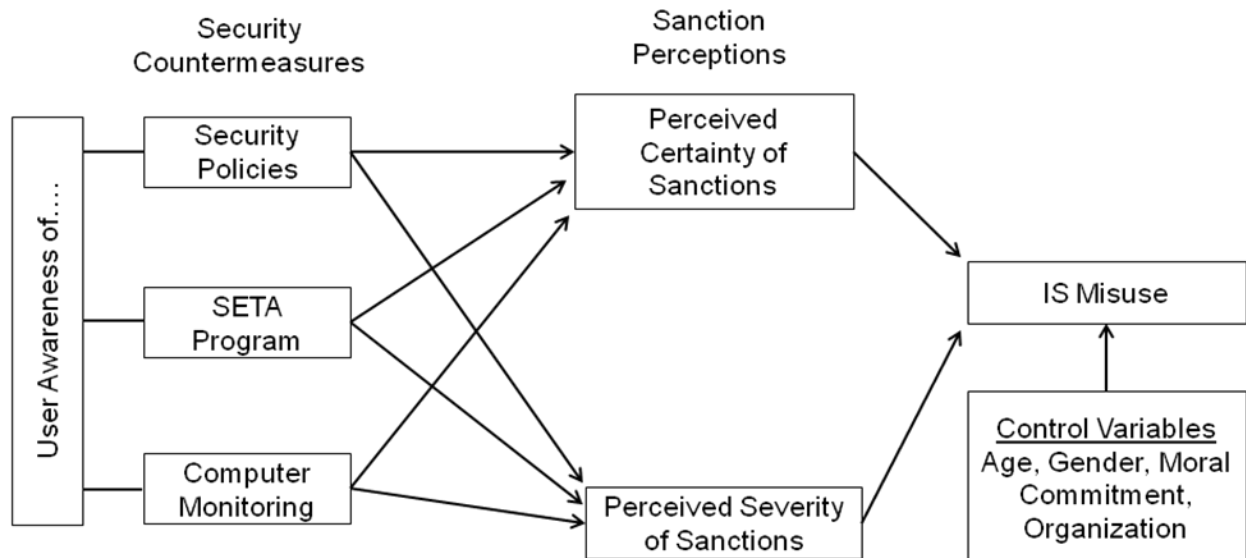


Figure 12. Extended general deterrence theory research model.

In line with GDT, the higher the certainty [probability] and severity [degree] of a punishment, the greater the possibility of employee deterrence for associated acts. Thus, four groups of hypotheses serve as the basis for this study. The first hypothesis group asserts a negative relationship between employee understanding of the certainty and severity of adverse action and information security misuse intention. The second hypothesis group addresses security policy and asserts that employee consciousness of information security policies has a positive association with employee understanding of the certainty and severity of adverse action. The next hypothesis group involves employee consciousness of SETA programs and predicts a positive association with employee understanding of the certainty and severity of adverse action. The final hypothesis group predicts a positive connection between employee consciousness of monitoring practices and employee understanding of certainty and severity of adverse actions (D'Arcy, Hovav, & Galletta, 2009).

Data collection for the study employed a two-part survey instrument. The design approach for the first portion aimed at capturing employee understanding of certainty and severity, moral commitment, and information security misuse intention. Four specifically selected misuse scenarios were developed and aimed to collect unbiased, open-minded responses. Twenty-six professionals enrolled in graduate courses at a Mid-Atlantic university provided scenario validation. They reviewed scenarios and provided feedback to ensure wording was dispassionate and impartial for participants. The design for the second portion measured security policy consciousness, SETA consciousness, and computer monitoring. Survey validity was achieved thorough a six-member group of university faculty members specializing in information security. A pilot sample was also sent to 54 computer savvy professionals. Survey participants represented eight U.S. companies. Of the 805 subjects who received an invite to participate in the survey, 269 usable responses were received (D'Arcy, Hovav, & Galletta, 2009).

The study results signify control variables negatively affect IS misuse. Perceived severity and perceived certainty influence IS misuse, but perceived severity was notes as having a stronger affect, likely attributed to respondents indicating high morality levels. The significant relationship between security policy and IS misuse indicate employee understanding of punishment serves as a valid method preventing IS misuse. SETA program consciousness was found to mitigate IS misuse through its intrinsic communication of the certainty and severity of adverse actions associated with IS misuse. Employee consciousness of IS monitoring was noted the greatest influencing countermeasure on understandings of certainty and severity of adverse actions.

2.7 Summary

The result of limited, well designed, and detailed collection of information security culture research (Karjalainen & Siponen, 2011; Karlsson, Åström, & Karlsson, 2015) invites influences from closely related frameworks as a basis for information security culture. Additional research methods with a sound theoretical foundation and supported by empirical data are needed to further develop this area of research. The information security culture literature reviewed for this study clearly indicate vast differences in research constructs. With much of the current information security culture research focusing on technical aspects and individual information security behavior, one can surmise that work is needed to further develop an acceptable information security culture framework that is widely accepted and used to support future studies. The literature reviewed for this study identified over 40 constructs encompassing organizational, individual perspectives. With such a vast number of dynamics being assessed, the ability to clearly establish and define supported construct relationships with information security culture may be adversely influenced. Of the 16 quantitative studies reviewed, five factors emerged as the most commonly used. They include: SETA programs (7), self-efficacy (6), response efficacy (5), leadership support (5), Security Policy (5). However, no single study was found to encompass a construct containing the five most widely used factors. For this study, SETA programs, leadership support, and security policy were specifically selected as constructs because of their mutually supporting relationship (Chen, Ramamurthy, & Wen, 2015; Liu, 2015; Puhakainen & Siponen, 2010; Rutherford, 2014) and explicit tangible presence in organizational security culture. Constructs dealing with efficacy, perception, and attitude were avoided because they are considered more aligned with behavioral frameworks and associated research.

This study provides noteworthy movement in clarifying associations between security countermeasures, understanding of sanctions, and IS misuse intention. The findings support security countermeasures indirectly effect on misuse intention. Of note, the effect of morality differs because of individual morality levels. This study adds to expands preceding deterrence-based security countermeasure research by expanding GDT to include the perceived certainty and perceived severity constructs. As part of their security culture, many organizations have implemented information security programs and policy to minimize risks to both employees and the organization. As indicated by Chen et al. (2015), D'Arcy, et al. (2009), Dahbur et al. (2017), Donahue (2011), Hwang et al. (2017), Pierce (2012), Rutherford (2014), and Yoon and Kim (2013), the common factors of these programs consist of:

- 1) Security policies,
- 2) SETA (Security Education, Training, and Awareness) programs, and
- 3) Security monitoring.

CHAPTER III: RESEARCH METHODS

3.1 Introduction

The federal government often uses research to identify the cause of specific organizational phenomena. As previously noted, the federal government expects unauthorized disclosures to continue in the foreseeable future. Therefore, a healthier understanding of information security culture within the federal government is necessary to better contend with future challenges associated with unauthorized disclosures. According to Snilstveit, Oliver and Vojtkova (2012), answers to questions that aim to explore or conceptualize an issue may be best addressed through synthesis. The research models cited in Chapter II are based on research relating general deterrence theory, organizational culture theory, protection motivation theory social bond theory, and the theory of planned behavior/reasoned action to inform information security culture. The central question and sub-questions derived from these theories can be explored using qualitative research to interpret specific findings that may not be generalizable. When considering the focus of this study is the federal government information security culture, findings from this study may not be generalized. While the previous studies have adapted differing approaches to assess various factors of information security culture, the specific factors selected for this study were not found in any stand-alone study during the exhaustive literature review process. The federal government currently acknowledges and fully anticipates the occurrence of unauthorized disclosures to remain an ongoing problem. This research intends to shed light on an issue that persists within the federal government while concurrently securing a position as one of federal government's many priorities needing attention - mitigating or negating unauthorized disclosures of CMI and CUI (Fujii, Sato, Yamauchi, & Taniguchi, 2016; Lutkenhaus, 2014; U.S. GAO, 2015). This failure observation purports the fault of end users,

thus the criticality of examining the relationship among factors concerning this construct is deemed appropriate.

3.2 Research Design

The design for this study is a meta-synthesis. Researchers have recently highlighted the need for increased qualitative synthesized research that generates new data and offers enlightenment of particular phenomena. The rationale for selecting a meta-synthesis is that it allows the researcher to identify themes and gaps, provides greater insights, and contributes to the collective whole. The use of schematics, diagrams, and visual aids are recommended for providing transparency in the meta-synthesis research process. These artifacts identify sources of research data, serve as an audit trail for decision-making, and provide a roadmap to aid future meta-synthesis research efforts (Paterson et al., 2009; Thunder & Berry, 2016; Snilstveit et al., 2012). Erwin, Brotherson, and Summers (2011) provide further rationale by noting the synthesis of a collection of data to identify shared themes can provide richer insights not otherwise found in a single study. Additionally, evaluative explorations using qualitative synthesis provide overall contributions to the field of study. According to Snilstveit et al. (2012), methodologies for meta-synthesis apply to a range of qualitative evidence, with each type of methodology being a subset of a single study. These methodologies are delineated into four distinct levels that build upon the synthesis, coding, cross-referencing, and evaluation of the meta-synthesis process. The types of qualitative meta-synthesis are presented in Table 7.

Table 7

Types of Qualitative Meta-synthesis

Types of Qualitative Meta-synthesis	
Meta-ethnography	“In meta-ethnography, the researchers synthesize individual ethnographic studies to describe broader relationships using metaphors” (p. 320).
Grounded formal theory	“In grounded formal theory, the researchers use coding and categorizing to develop an abstract, general theory to explain relationships” (p. 320).
Cross-case analysis	“In cross-case analysis, the researchers systematically code, refine, and cross-reference descriptive meta-themes and meta-categories” (p. 321).
Meta-study	“In meta-study, the researchers sample, evaluate, and analyze studies following a highly linear and structured procedure” (p. 321).

This study implements a qualitative approach to synthesizing text-based, narrative data in an effort to gain an increased understanding across a body of related research literature. It also provides insight beyond summaries of relevant, traditional studies (Snilstveit et al., 2012; Thunder & Berry, 2016). This researcher seeks to go beyond single accounts to reveal the key themes and analogies between those accounts while extending findings through synthesis. “It reduces the accounts while preserving the sense of the account through the selection of key metaphors and organizers. The senses of different accounts are then translated into one another” (Thunder & Berry, 2016, p. 320). An important note is that meta-ethnography “provides a method for explaining different findings and it has therefore been suggested it might be particularly useful in informing policy” (Snilstveit et al., 2012, p. 421).

The selection of a meta-synthesis was determined as the best suited to integrate results from a number of different studies. The differences among studies selected for this meta-synthesis were analyzed. According to Creswell (2013), the use of meta-synthesis ensures adequate population and sample sizes to support synthesis, as well as increasing precision when

estimating the effects. Additionally, the aim of this meta-synthesis is to “integrate and interpret patterns and insights systematically across qualitative studies while maintaining the integrity of the individual studies” (Erwin, Brotherson & Summers, 2011, p.189; Overstreet, 2017). With a focus on the federal government, this meta-synthesis integrates content from a specified pool of studies to achieve a greater understanding through synthesis and interpretation (Thunder & Berry, 2016).

The purpose of this meta-synthesis is to identify and categorize research and findings across qualitative studies. As discussed in Chapter I, this research examines qualitative research studies that focused on three specific factors - leadership support, security policy, and SETA. Answers to the central question and sub-questions presented in Chapter I were identified, categorized, and compiled to support easy reference for future researchers.

Published qualitative studies, and scholarly journal articles served as the principal observation element investigated and were collected after Institutional Review Board approval was gained. To ensure recency, a cut-off year of 2003 was established for all published material. The data limits established best represent current research, as well as establish a relevant set of procedures to support this study. Published materials were specifically selected for various reasons. First, the material produced findings that aligned with research criterion. Second, published materials are scholarly studies that are subject to rigorous review and approval processes that meets the standards of this research. Third, the systematic reviewing of structured data allows for eases of data transfer and future meta-synthesis methodology replication in. Systematic reviewing of scholarly, published data also contributes to virtual ease and efficiency for coding purposes.

Since the federal government is well known for its formalized culture, standardized approaches and regimented processes, this study does not seek to gain an understanding of the circumstances of the phenomena being studied. This study also does not seek to gain an understanding of the peripheral dynamics that may influence information security culture, such as job satisfaction, employee commitment, or environmental work impediments.

The cost associated with this study is insignificant, with published empirical research serving as the primary sources of data collection. The use of published research is a convenient approach that eliminates the need for postage and handling, while negating any required interaction with participants. Non-automated methods are not timely or efficient for managing data collected, especially during the meta-synthesis coding process.

3.3 Participants

The participants were determined after IRB approval (Appendix I). The population affected by this study encompass a workforce of approximately 2,864,053 Soldiers, Sailors, Airmen, Marines, and civilians that constitute the federal government workforce (DMDC, 2018). As noted by Fink (2013) and Shelton (2014), the use of a statistically significant sample size will support meaningful statistical analysis. The population for this study is geographically dispersed around the globe. The sample taken from this population consist of three groups – military, civilian employees, and defense contractor employees. Tables 10-14 represent the numbers of population groups, as of March 2018. The workforce is diverse, consisting of mixed population. Participant effected age distribution ranges from 20 to 60-plus years. Active duty and reserve demographics are identified in Table 15 (DoD, ODASD, MC&FP, 2015).

Table 8

National Guard / Reserve Strength

National Guard / Reserve strength								
Location	Army	Navy	Marine corps	Air Force	Coast Guard	Total	Army	Navy
United states total	328,641	183,052	54,753	34,839	104,731	67,333	6,038	779,387
Overseas total	7,978	7,298	2,842	3,423	1,600	849	85	24,075
Grand total	336,619	190,350	57,595	38,262	106,331	68,182	6,123	803,462

Note: The DMDC data only reflects personnel who are permanently assigned to duty locations. The table does not include personnel on temporary duty, or deployed in support of contingency operations. Adapted from “Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications: 2018 Military and Civilian Personnel by Service/Agency by State/Country”, by DMDC quarterly military and civilian personnel by service/agency by state/country (2018).

Table 9

Active Duty Strength

Active Duty strength						
Location	Army	Navy	Marine corps	Air Force	Coast Guard	Total
United States total	416,667	285,141	153,107	266,167	39,960	1,161,042
Overseas total	47,791	36,119	31,833	52,843	1,204	169,790
Grand total	464,458	321,260	184,940	319,010	41,164	1,330,832

Note: The DMDC data only reflects personnel who are permanently assigned to duty locations. The table does not include personnel on temporary duty, or deployed in support of contingency operations. Adapted from “Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications: 2018 Military and Civilian Personnel by Service/Agency by State/Country”, by DMDC quarterly military and civilian personnel by service/agency by state/country (2018).

Table 10

DoD Civilian Strength

DoD Civilian strength						
Location	Army	Navy	Marine Corps	Air Force	4th estate (DoD)	Total
United States total	234,492	184,161	16,739	164,180	97,966	697,538
Overseas total	11,606	4,905	636	3,378	11,696	32,221
Grand total	246,098	189,066	17,375	167,558	109,662	729,759

Note: The DMDC data only reflects personnel who are permanently assigned to duty locations. The table does not include personnel on temporary duty, or deployed in support of contingency operations. Adapted from “Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications: 2018 Military and Civilian Personnel by Service/Agency by State/Country”, by DMDC quarterly military and civilian personnel by service/agency by state/country (2018).

Table 11

DoD Military and Civilian Employee Grand Total

Location	Grand total
United States total	2,637,967
Overseas total	226,086
Grand total	2,864,053

Note: The DMDC data only reflects personnel who are permanently assigned to duty locations. The table does not include personnel on temporary duty, or deployed in support of contingency operations. Adapted from “Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications: 2018 Military and Civilian Personnel by Service/Agency by State/Country”, by DMDC quarterly military and civilian personnel by service/agency by state/country (2018).

Table 12

Active Duty and Reserve Demographics

Demographic Variable	Active Duty	Reserve and Guard (Select Reserve)
Members		
Total number	1,301,443	826,106
Ratio of enlisted to officer	4.6 to 1	5.3 to 1
% women / % men	15.6% / 84.5%	19.0% / 81.0%
% minorities	31.0%	26.0%
% located in the United States, U.S. territories	87.5%	99.2%
% 25 years of age or younger	43.8%	34.0%
% with bachelors degree or higher	21.1%	22.7%
% married	54.3%	11.7%
% indual-military marriages	6.4%	2.7%

Note: The DMDC data only reflects personnel who are permanently assigned to duty locations. The table does not include personnel on temporary duty, or deployed in support of contingency operations. Adapted from “Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications: 2018 Military and Civilian Personnel by Service/Agency by State/Country”, by DMDC, DoD Personnel, Workforce Reports & Publications (2018).

Participant tenure ranges from new interns to 30-plus years of service. An important note is all participants selected are required to receive SETA upon initial entry to the organization, and annually thereafter. Participants serving in positions requiring access to certain levels of

CMU and CUI receive additional security training as well. Table 12 depicts military workforce demographics.

3.4 Qualitative Tools

Several screening and coding tools are used to form a standardized approach to extracting study-specific information. Coding is intended to balance the extraction and inclusion of data while limiting the need for post extraction re-examinations of a data (Littell et al., 2008). A standardized coding tool provides the direction necessary while allowing variance among studies. The ensuing codes provide high quality descriptions for each study. These coding parameters served as the strategy for developing an efficient and inclusive coding approach (Polanin, 2013; Thunder & Berry, 2016).

3.5 Inter-Rater Reliability

Inter-rater reliability provides an objective measure of consistency among coding data that removes subjectivity and ensures validity and reliability of qualitative studies. This study used two raters who worked independently to rate coding data. The two raters consisted of this researcher (Rater A) and a tenured university professor (Rater B). Rater A is an intelligence and security subject matter expert who possesses 35 years of experience within the federal government. Rater B is an investigative, research, and coding subject matter expert who possesses 40 years of law enforcement and academic experience.

A 3-point Likert scale (1 = No Relevance, 2 = Moderate Relevance; 3 = High Relevance) served as the instrument for identifying inter-rater agreement among categorical factors (leadership support, security policy, and SETA) within the studies selected for this research. Ratings applied to each study were assessed to determine inter-rater agreement among raters utilizing an inter-rater agreement table (Appendix B).

This researcher explored options for determining inter-rater reliability. The use of Cohen's Weighted Kappa was considered. Cohen's Weighted Kappa measures the degree of disagreement among raters. However, this study design requires total rater agreement of selected studies, and those studies reflecting any degree of rater disagreement were disqualified from coding. As such, the use of Cohen's Weighted Kappa was deemed inappropriate. Alternatively, Cohen's [Unweighted] Kappa was considered. Cohen's Kappa measures the degree of agreement among raters and considers the chance agreement among raters. Cohen's Kappa was determined as well suited for this research as it also complements the use of two deliberately selected raters for conducting inter-rater reliability. Cohen's Kappa measured inter-rater reliability among selected studies using the inter-rater reliability rating matrix (Appendix C).

Kappa is always less than or equal to 1. A value of 1 implies perfect agreement and values less than 1 imply less than perfect agreement. For the purpose of this study, and as determined by the dissertation committee, .93 agreement was determined as an acceptable agreement level among raters. The Kappa statistic varies from 0 to 1, where:

- 0 = Agreement equivalent to chance.
- 0.1 – 0.20 = Slight agreement.
- 0.21 – 0.40 = Fair agreement.
- 0.41 – 0.60 = Moderate agreement.
- 0.61 – 0.80 = Substantial agreement.
- 0.81 – 0.99 = Near perfect agreement
- 1 = Perfect agreement.

There are multiple ways of annotating the equation used to solve for Cohen's Kappa. The two examples provided below are the most commonly used, but are different ways of stating the

same equation. Solving for kappa involves a 5-step process. The actual calculations for kappa are presented in Chapter IV (Altermatt, 2014; Poortman & Schildkamp, 2012; Hallgren, 2012, Zaiontz, 2018; Grande 2015; Meyer, 2014).

$$k = \frac{\text{Pr}(a) - \text{Pr}(e)}{1 - \text{Pr}(e)} \quad \text{or,} \quad k = (\text{Pr}(a) - \text{Pr}(e)) / (1 - \text{Pr}(e))$$

- Step 1: Calculate Pr_a (the relative observed agreement among raters).
- Step 2: Find the probability that the raters would randomly both say Yes.
- Step 3: Calculate the probability that the raters would randomly both say No.
- Step 4: Calculate Pr_e (the hypothetical probability of chance agreement).
- Step 5: Insert calculations into the formula and solve.

3.6 Data Analysis

ATLAS.ti, version 8 was selected as the ideal automated tool to support qualitative data analysis for this study. The ability to code significant amounts of data and the flexibility to modify, search, and visualize data with relative ease situates ATLAS.ti.8 as a valuable tool. ATLAS.ti uses coding to support analysis through interpretation of similarities, differences, categories, themes, concepts and ideas. This researcher supports the process by creating comparisons to build and refine categories, to define conceptual similarities, and to discover patterns. The results of this analysis are discussed in Chapter IV.

3.7 Method

In identifying the meta-synthesis studies, a rigorous six-step process served as the method of synthesizing and interpreting data across a pool of qualitative studies. This study implements the process outlined by Thunder and Berry (2016; p 321).

1. Identify a specific research meta-question,

2. Conduct a comprehensive search,
3. Select initial relevant studies,
4. Appraise the quality of initially selected studies,
5. Synthesize findings of selected studies using qualitative techniques, and
6. Present synthesis findings across the studies to address the research meta-question.

The six steps of meta-synthesis.

Step 1: Identify specific research questions and sub-questions. The qualitative research question for this meta-synthesis must encompass the purpose of the study by identifying the central phenomenon to be examined. More importantly, the meta-synthesis research question must also be a meta-question, which means the question must have already been the subject of qualitative research (Thunder & Berry, 2016). The meta-question serves as the underpinning of analysis and synthesis because it steers the selection of literature for synthesizing (Erwin, Brotherson, & Summers, 2011). While it is not necessary for the meta-question to mirror the research question from previous relevant studies, it should draw an association that facilitates further investigation that can help answer to the question. The goal here is to balance breadth and scope when developing the qualitative research question. The researcher conducting this meta-synthesis posed a research meta-question that was previously studied and could be answered through the analysis of existing, relevant qualitative research studies. Through meta-synthesis, the researcher intends to further understand the phenomenon within the existing collective body. An important aspect to understand is the uniqueness of qualitative meta-question development. Upon examination of multiple qualitative studies, variations in their description of the phenomenon may materialize. As an iterative process, the meta-question for this study may require revision (Thunder & Berry, 2016).

Step 2: Conduct a comprehensive literature search. The second step involves the search and retrieval of relevant primary studies. Primary studies formulate the pragmatic grounding for the subsequent synthesis. Two central components comprise this step: 1) Developing a comprehensive search strategy, and 2) Defining search terms (Cooper, 2010; Card, 2012). The development of a comprehensive search strategy involves the reliance on multiple search modes that include searches through electronic databases, manual searches of printed sources, consultation with subject matter experts, and open electronic searches. As Lemire (2017) reminds us, “the most important threat to the validity of any research synthesis is the failure to conduct a sufficiently exhaustive search” (p.35).

The specification of relevant and effective search terms for the electronic search is equally important. Search terms should carefully balance the potential for false positives or failing to identify and include relevant studies. What is important to understand here is there is no single approach for achieving this balance. The “criteria for inclusion and exclusion of articles may need to be fluid and flexible because the procedures for screening may change as the researchers learn more about populations, models, and various defining characteristics of the interventions they are locating” (Erwin, Brotherson, & Summers, 2011, p. 192). The only solution is to approach the search process as an iterative, trial-and-error process, merging back and forth between electronic searches and refinement of search terms and strategies. Despite the iterative nature of the search process, the final search procedure is still to be systematic and documented for the purpose of transparency and possible replication (Bronson & Davis, 2012). Thus, the development of a search and retrieval log, tracking and detailing the number of manuscripts (duplicate and unique records) identified by source, is recommended as a sufficient search and retrieval process (Appendix D) (Lemire, 2017).

The studies used for this research will rely on data collected through interviews, focus groups, observations, and document analyses from previously conducted qualitative studies. A comprehensive search of relevant literature supports data collection efforts. This comprehensive literature search differs from a comprehensive literature review in that it is a systemic, iterative process that requires the researcher maintain records of search parameters, retrieval processes, decision points, and validation of data. Consolidation of this information serves as a research audit trail and a guide for future replication. Four key factors (topical, population, temporal, and methodological) ensure the precise selection and recall ability of relevant data. With the researcher defining the parameters for these factors, their effectiveness is contingent upon the researcher's knowledge of the subject area. Therefore, the researcher must possess a comprehensive understanding of the subject matter in order to define, describe, and defend such parameters. The first factor, topical, is directly linked to the research meta-question. The researcher initially develops a working definition consistent with personal knowledge of the research area. The definition is dynamic, allowing for revisions as unanticipated findings arise. The second factor is population. Similar to the topical factor, this factor is also defined in concert with personal knowledge of the research area and the researcher must be able to define, describe, and defend the population selected for the study. Third, the temporal factor deals with the time-based aspect for research data by establishing acceptable chronological windows for data retrieval and collection. Fourth, the methodological factor aids in determining what constitutes qualitative research that this study encompasses. As previously stated, meta-synthesis assimilates the discoveries and conclusions of previous qualitative research; accordingly, the studies used in this meta-synthesis must have used qualitative methodologies (Thunder & Berry, 2016).

Step 3: Select initial relevant studies. Initial inclusion/exclusion vetting involved a two-stage process. The first stage in the selection process reviewed the title and abstract of each retrieved citation to decide its relevance. Initial reviews of titles and abstracts were conducted using a standardized title and abstract screening tool (Appendix E). During the second stage, a more detailed review sought to identify the presence of key factors to support coding using a content validation log (Appendix F). During this stage, a designation of [include, unsure, or discard] was applied to each study. Published data labeled as “unsure” underwent additional screening using a standardized research question and factors screening tool (Appendix G). This process eliminated many of the articles found during the literature search.

During this process, some sources were read in their entirety. The benefit in this step is the researcher’s flexibility to revise or redefine the inclusion/exclusion criteria. The researcher should systematically record all decisions, criteria changes, and search modifications. Recording this information also allows the researcher to confirm their audit trail and replicability by completing double searches. Figure 13 visually displays the various decision points encountered during the search, retrieval, and validation process.

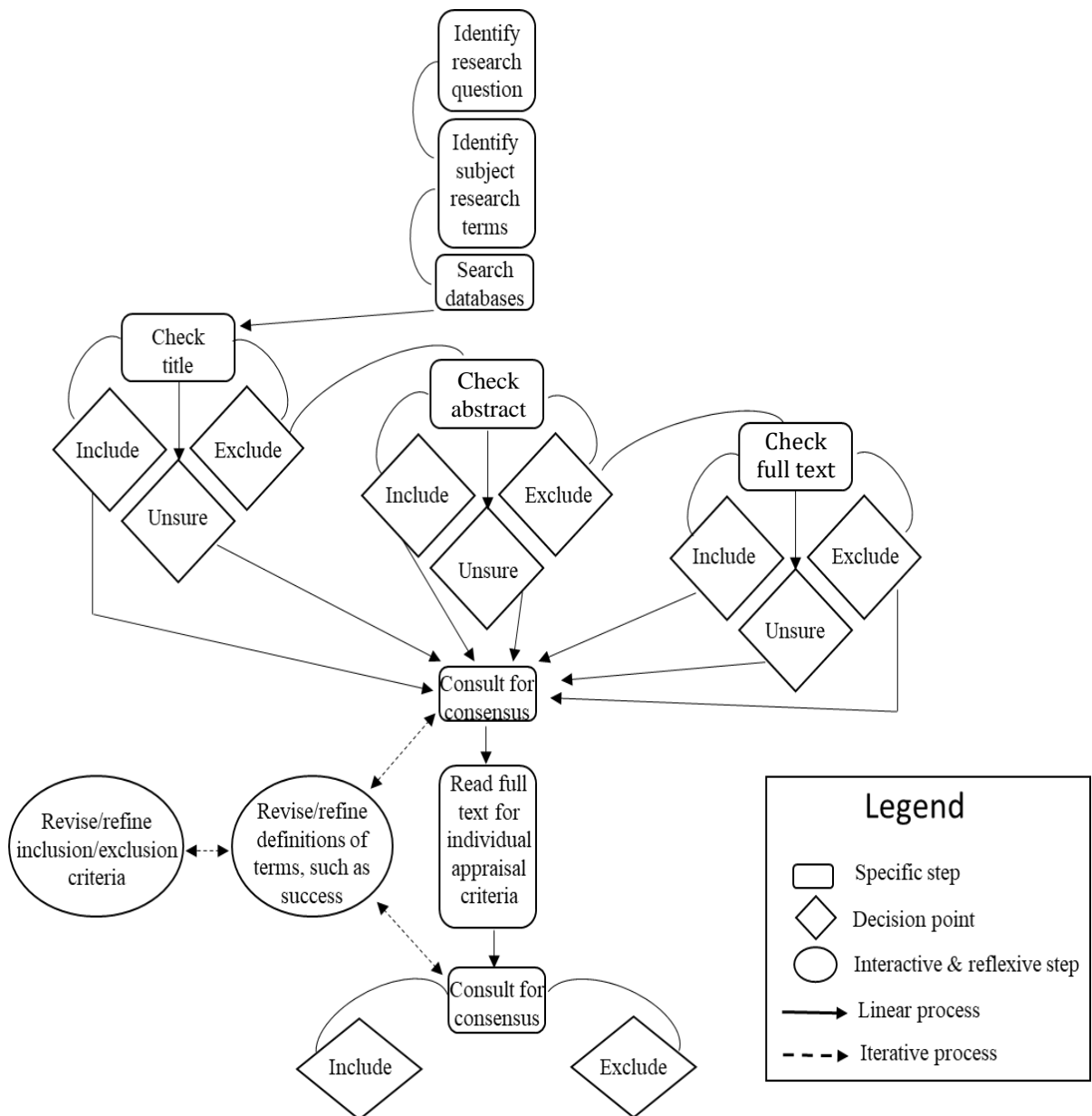


Figure 13. Search, retrieval, and validation process.

Inclusion/exclusion criteria. Central to Step 3 is the formulation of clear inclusion/exclusion criteria. These criteria may include outcomes of interest (e.g., topical, temporal, population, methodological). The definition of the inclusion/exclusion criteria in tandem with the formulation of the research questions collectively serve to delineate the boundaries of the synthesis and in effect the conclusions drawn. Thus, the definition of these boundaries should be carefully defined for the research questions and established prior to any

analyses of any identified studies (Lemire, 2017). In this step, a key determination of what studies to include that must be made. This is accomplished through comparing studies with established boundaries that can include research purpose, data collection techniques, and the research stated findings. The researched may also elect to reevaluate the quality of research used for the meta-synthesis (Erwin, Brotherson, & Summers, 2011).

Published data must meet inclusion/exclusion criterion provided in Appendix H. First, publications must have occurred from 2003-2018. Second, the published data must focus on some aspect of information security culture or unauthorized disclosures. Third, the published study must be an empirical qualitative study. Fourth, the studies must present the results and findings. Fifth, the target population should be identified. The overarching aim of this initial relevance appraisal is two-fold:

- 1) Identify obviously irrelevant studies (i.e., false positives), and
- 2) Categorize the remaining manuscripts according to their analytical purpose in the synthesis.

To minimize the risk of excluding a potentially relevant study on the basis of an abstract, one should always err on the side of inclusion, even if the potential relevance of the manuscript appears faint. The worst error at this stage of the synthesis is for the researcher to exclude a useful study (Lemire, 2017; Polanin, 2013).

All forms of results, findings, and analysis techniques were considered. Although differing types of published data were considered, preference to key factors of a comprehensive information security culture - leadership support, security policy, and SETA – remained. To help maintain a focus and relevance to this study, published data failing to meet 80% of screening questions were excluded. Remaining studies selected in accordance with exclusion

criteria established the sampling frame. Any study identified as erroneously included in the sampling frame was removed (Polanin, 2013). This step concludes with a final selection of studies to support the meta-synthesis (Erwin, Brotherson, & Summers, 2011).

Step 4: Appraise the quality of initially selected studies. This step describes the approach for identifying study similarities through the use of comparison parameters. These parameters may consist of study purpose, research questions, data collection, analysis, and findings. A tool for appraising and rating content was developed to track comparisons to support an audit trail and synthesis. The typology used considered the study type, classification of findings, and the ability to support the transformation of data (Erwin, Brotherson, & Summers, 2011). Upon conclusion of the initial selection of studies, the researcher individually appraised each study for quality and compared the studies.

Individual appraisal. The individual appraisals involve the reading and evaluation of each study using a systematic but dynamic, intra-report reading guide. The purposes of individual appraisal are to (Thunder & Berry, 2016):

- 1) Determine whether reports meet your inclusion criteria,
- 2) Ensure that your inclusion criteria require no further modification, and
- 3) Familiarize yourself with the informational content, methodological orientation, style, and form of each report (p 325).

Conducting individual appraisals is a unique opportunity to validate comparability among qualitative studies. Each relevant qualitative study provides a unique contribution to understanding the phenomenon. Qualitative studies “should include the basic quality criteria for methodological aspects such as research problem, purpose, and question; data collection techniques; data analysis; report of findings; and implications and conclusions” (Thunder &

Berry, 2016, p. 328). It is acceptable to formulate additional inclusion and exclusion criteria during this process. The tool for appraising the quality of qualitative research in this step is adapted from Erwin, Brotherson and Summers (2011) and Thunder and Berry (2016). Figure 14 depicts the adapted checklist that is divided into four criteria, each with its own indicators.

	Possible Points	Study #3	Study #5	Study #7	Study #9	Study #10	Study #12
1. Research problem and purpose	2						
a) Problem is stated clearly and related to research literature							
b) There is a clear statement of research purpose and/or question							
2. Method: Data collection and analysis	6						
a) Study is methodology qualitative							
i. Sampling plan and data collection are appropriate to the question							
ii. Data analysis plan is consistent with design and purpose							
b) Described the participants/subjects of the study and how selected							
c) Researchers show an awareness of their influence on the study and its participants (e.g., described experiences and/or assumptions with which the researcher entered the research)							
d) Data collection procedures are fully described (interviews, focus groups, document analysis)							
e) Steps/process of data analysis is clear with examples							
f) Techniques for credibility and trustworthiness described and used correctly							
3. Findings	5						
a) Interpretation of data are plausible and/or substantiated with data							
b) Overall findings address the purpose of the study							
c) Ideas (e.g., themes, categories, concepts) are precise, well developed, and linked to each other							
d) Results offer new information about or insight into the target phenomenon							
e) Quotes provide support/evidence for each theme/concept presented							
4. Discussion and implication	2						
a) Returned to research questions proposed at the beginning and discuss interpretation and significance of findings							
b) Recommendations for intended audience and future research issues							
Total points	15	0	0	0	0	0	0

Figure 14. Appraisal criteria for assessing quality of qualitative research process.

One point is allotted for each indicator, with a maximum total of 15 points. The point distribution for overall standards of quality and credibility is as follows:

11–15 points: High overall standards

6–10 points: Moderate overall standards

0–5 points: Low overall standards.

Comparative appraisal. This step involves the creation of cross-case graphics and summaries of the carefully chosen studies. “The purpose of comparative appraisal is to prepare for synthesizing findings, to notice initial trends and patterns, and to include items directly relevant to the integration of findings you want to produce” (Thunder & Berry, 2016, p. 331). The comparison appraisal also allows for the identification of missing information, confirming negative cases, and duplicate reports. Since all studies vary in context, a crosswalk display may be used to identify variances, such as participants, experiences, time periods, and focus. The patterns in these contexts are significant because they can narrow or broaden the participants’ lenses. This comparative appraisal supported supports analysis, coding, and integration of findings (Thunder & Berry, 2016).

Step 5: Synthesize findings of selected studies using qualitative techniques. The findings sections from each article serve as the primary data for meta-synthesis. The data for the meta-synthesis include a minimum of each article’s entire findings sections, and may also include salient aspects of the discussion section. These data are extracted into a single document for coding and recorded by the researcher. The researcher’s selected method for analysis is informed by the purpose of the study, the theoretical framework of the study, and the type of meta-synthesis. The data analysis process for a single-study qualitative research is the same process and meta-synthesis. The following steps should be observed during Step 5.

1. Code, categorize, and compare data to develop a general theory of success.
2. Re-read and re-code to refine and verify coding and to assure consistency.
3. Sort the data by codes and reread, looking for themes within each code to see if there were dimensions that required the data to be further discriminated.

The First coding cycle estimates effect sizes and focuses on relevant background information from each study on:

- 1) Publication information (author name, publication year);
- 2) Study features
- 3) Type of control (e.g., treatment as usual or a specific alternative program)
- 4) Study design (e.g., experimental or quasi experimental), and
- 5) Program design features (e.g., the absence or presence of specific program factors)

According to Lemire (2017), the specific codes used are contingent on the nature of the study and the research questions. Individual effect sizes for each study are assessed. The primary purpose is to obtain a standardized effect size for each salient outcome and comparison, as determined by the scope of the synthesis. Coding also determines the overall effectiveness of the program under study by gauging the degree of unexplained variation between the studies, and assesses the presence, or influence of publication bias. Publication bias pertains to reviews that solely rely on published studies. The potential bias emerges from non-significant findings being less likely to be published, or reported in publications, as compared with significant findings. (Lemire, 2017).

In advancing the analyses, attention is given to the unexplained variation among primary studies. Examining the amount of unexplained variation is important for several reasons. First, the presence of large amounts of unexplained variation jeopardizes the accuracy of the effect size estimates, as reflected in widened confidence intervals. Secondly, unexplained variation affects the ability to meaningfully interpret the combined effect size estimate. This is because the unexplained variation may be due to cross-study variations in program design features,

contextual conditions, target group characteristics, or other pertinent particularities, that in some way affect the effectiveness of the programs being studied (Lemire, 2017).

Step 6: Present synthesis findings across the studies to address the research Meta-question. The use of visual displays to reflect meta-summary findings is not uncommon (Thunder & Berry, 2016; Erwin, Brotherson, & Summers, 2011). Researchers produce visual displays with information derived from the classifying and placing of data into categories. Visual displays can also include representative quotes from gathered data to provide clarity and defining qualities of findings (Thunder & Berry, 2016). The final synthesized findings encompassing the collective body of work should answer the central question and sub-questions. With the finished products of synthesis, this researcher is able to present evidence-based findings that can be used to drive federal government policy and practice.

3.8 Risks and Benefits

There is no known risk associated with this study. Alternatively, the benefits are vast in the continued promulgation, application, and enforcement of information security culture.

3.9 Ethical Assurances

Delaware State University's Institutional Review Board approval (Appendix I) is required prior to initiating any data collection process or procedure. However, the design of this study is sufficient for an exemption. Meta-modeling did not pose any additional risk of harm to participants. The information gathered for this meta-synthesis is maintained on a personally owned laptop computer. The computer is password protected and files are encrypted. The laptop operates on a secure network that is password protected and requires a physical connection. Automatic virus scans and threat protection programs are implemented weekly to identify any potential malware or other IS risks. The information used for this research shall be

destroyed following dissertation acceptance, upon which time the researcher will destroy all physical and digital study related documents. The laptop hard drive used for this research shall undergo one of the below processes by an approved tool that meets one of the below procedures:

Degaussing: “Procedure using an approved device to reduce the magnetization of a magnetic storage media to zero by applying a reverse (coercive) magnetizing force rendering any previously stored data unreadable and unintelligible. Degaussing is also called demagnetizing” (IA BBP, 2009).

Destruction (of HDDs): “Destruction of a HDD is the process of physically damaging or destroying the drive so that it is not usable in a computer, and so that no known exploitation method can retrieve data from it” (IA BBP, 2009).

Purge (Sanitize): “Process of rendering stored information unrecoverable. Purge removes data from an IS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. An IS must be disconnected from all external networks before purging takes place” (IA BBP, 2009).

3.10 Assumptions

This study assumes the data collected from selected studies are reliable and provide a valid cross-section of the federal government. The development of this research design weighs heavily on the concept of voluntary and anonymous participation in the studies selected for this research. Adequate protections for participant concerns of confidentiality and anonymity were addressed in each selected study, thus no additional protections were necessary for this study. There are three fundamental study assumptions concerning anonymity and validity of data collected from in selected studies:

Assumption 1. Participant responses to survey questions would be honest.

Assumption 2. One survey would be completed by each participant.

Assumption 3. The description of anonymity provided to participants allows for the level of trust needed for truthful participation.

Assumption 4. Efforts were made not to alienate any particular group taking part in any of the selected studies.

Assumption 5. The reasonable assurance that all participants from selected studies have received their information security training, as mandated by federal government and they possess some degree of information security awareness, thus possess some degree of understanding and awareness of the organization's information security culture.

Assumption 6. The inclusion exclusion/criteria I sufficient for allowing the number of studies needed for this research.

Assumption 7. Studies selected for this research allow for the identification of extensive sub-codes that support the identification of emerging themes.

3.11 Summary

The purpose of this meta-synthesis is to explore and analyze the factors of leadership support, security policy, and SETA on federal government information security culture. This chapter introduced the research design and its rationale. The types of meta-synthesis were highlighted and a rationale for selecting a meta-synthesis was discussed. The participants for this study derive from a population of approximately 2.8 million personnel. Through the use of a six-step meta-synthesis process and various coding tools, data was analyzed across a broad number of qualitative studies that enables synthesis which generates new data and offers insight of information security culture. With no need for human interaction or participant data collection, any risk is negligible.

CHAPTER IV: FINDINGS

4.1 Introduction

This meta-synthesis sought to identify themes across multiple qualitative studies while focusing on the three key components of information security culture within the federal government. Through a 6-step meta-synthesis process, emphasis was placed on preserving the sense of original accounts through the selection of key metaphors and organizers. Multiple sources were explored using refined search parameters. Selected studies were screened and rated for inter-rater agreement and inter-rater reliability. The semantical networked coding of resulting themes that emerged in the areas of leadership support, security policy, and SETA will provide meaningful insight for organizations within the federal government to improve on the organizational information security culture, while reducing the number of unauthorized disclosures. This chapter will discuss the inter-rater agreement, inter-rater reliability, semantic coding, and findings. The central question and sub-questions for this study are:

Central question: What is the information security culture within the federal government?

Sub-questions: This meta-synthesis is guided by the below sub-questions.

- 1: What are workforce perceptions of leadership support and federal government information security culture?
- 2: What are workforce perceptions of security policy and federal government information security culture?
- 3: What are workforce perceptions of SETA and federal government information security culture?

4: What relationship exists between leadership support, security policy, and SETA within the federal government?

4.2 Literature Search

Sources. The selection of studies for this research underwent a rigorous process. The strategy developed for this comprehensive literature search utilized multiple means. To ensure sufficiency, both traditional and non-traditional scholarly sources were surveyed. Traditional scholarly databases (i.e., Elsevier, ERIC, JSTOR, MIS ProQuest, SAGE, and Springer) constituted the primary search effort. With the federal government managing its internal academic and professional development programs, it was appropriate that additional checks within the federal government academic arena occur within the following databases:

- National Defense University (<https://www.ndu.edu/Libraries.aspx>)
- U.S. Army War College Library (<http://usahec.polarislibrary.com/polaris/Search/>)
- U.S. Army Combined Arms Research Library (<http://cgsc.contentdm.oclc.org/cdm/>)
- U.S. Naval Academy Library (<https://www.usna.edu/Library/>)
- U.S. Naval War College Library (<https://www.usnwc.edu/Learning-commons>)

Search parameters. The literature review for this study provided the foundation for determining the initial set of search criterion. A continued consciousness of the importance of maintaining an emphasis on defining search parameters that target pertinent studies while reducing false positives was recognized early in the search process. Numerous revisions and combinations of words and phrases across multiple databases was a necessary, but time-consuming effort. A positive and reassuring aspect of this effort was noted with presence of some studies across multiple databases. These revisions broadened parameters that eventually

facilitated the initial identification of a sufficient number of studies for initial consideration for this meta-synthesis. The following phrases served as the final set of search parameters:

- Civil service
- Defense contractor
- Department of Defense
- Federal employee
- Federal government
- Information security
- Insider threat
- Leadership support
- Military (by branch)
- Security behavior
- Security compliance
- Unauthorized disclosure
- Security culture
- Security education, training and awareness
- Security incidents
- Security policy

Inclusion/exclusion criteria. Determinations for establishing inclusion/exclusion criteria positioned around the study's purpose, central question, and sub-questions. This carefully defined criteria established the synthesis boundaries. Although some of the references were located in multiple databases, the added redundancy afforded an increased level of assurance. However, a concern arose when an insufficient number of studies was identified during Step 3 of the meta-synthesis process. A decision was made to extend the window of data collection another 5 years, from 2008 to 2003. This modification resulted in identification of a sufficient number of studies for potential for inclusion. An evaluation of the selected studies based on search parameters and inclusion/exclusion criteria is presented in Table 13.

Table 13

Inclusion/Exclusion Evaluation Matrix

Author / Date	Study #	Qualitative Study	Between 2003-2018	Information Security Culture	Results / Findings	Military / Federal / Contractor
Abraham, S. (2011)	1	X	X	X	X	
Aburto, R. (2014)	2	X	X		X	X
Armstead, S. K. (2017).	3	X	X		X	X
Chander, M., Jain, S., & Shankar, R. (2013)	4		X	X	X	X ²
Charest, K. M. (2013)	5	X	X	X	X	X
Cook, J. L. (2015)	6		X	X	X	X
Cornely, D. D. (2003)	7	X	X	X	X	X
Dempsey, M. E., Carter, A. B. (2015)	8	X	X	X		X
Edwards, G. (2011)	9	X	X	X	X	X
Farah, J. (2004)	10	X	X	X	X	X
Glaspie, H. W., Karwowski, W. (2018)	11	X	X	X	X	X
Grant, R. L. (2017)	12	X	X	X	X	X
Harris, M. A. (2010)	13	X	X	X	X	
Hodge, T. D. (2018)	14	X	X	X	X	X
Krasley, P. F. (2011)	15	X	X	X	X	X
Lopez, R. H. (2012)	16	X	X	X	X	X ²
Lutkenhaus, J. (2014)	17	X	X	X		X
Macioce, G. E. (2003)	18	X ¹	X	X	X	X
McDaniel, E. A. (2013)	19	X	X	X		X
McIntosh, B. (2011)	20	X	X	X	X	X
Price, J. D. (2014)	21	X	X	X	X	X
Rotvold, G. (2008)	22	X	X	X	X	X
Stewart, H., Jürjens, J. (2017)	23	X	X	X	X	
Stroup, J. W. (2014)	24	X	X	X	X	X
Tanoh, R. A. (2017)	25	X	X	X	X	X
Tinoco, J., & Arnaud, A. (2013)	26	X	X	X	X	X
Veseli, I. (2011)	27	X ¹	X	X	X	
Williams, K. L. (2014)	28	X	X		X	X

1 - Both qualitative and quantitative.

2 - Participants were a mix of government, private sector and non-profit organizations.

Literature search. To ensure transparency and possible replication, a search and retrieval log captured results of the literature search. In addition to including the four key factors (topical, population, temporal, and methodological) identified by Thunder and Berry (2016) that facilitate recall ability of relevant data, additional categories (abstracts, research questions, information security factors, factors and citations) were added. The literature search results are captured in the search and retrieval log (Appendix D).

Study Selection. While the initially selected studies may have met the established 80% inclusion/exclusion criteria, research questions or findings were not always congruent with this study focus - leadership support, security policy, and SETA. During the first stage of study selection, initial reviews of titles and abstracts were conducted using a title and abstract screening tool (Appendix E). Although cursory, the first stage served as a method of quick delineation for grouping studies. During the second stage, a more detailed review sought to identify the presence of key factors to support coding. The work in this stage resulted in a research question and factors screening tool (Table 14). There were 28 studies selected for this research. Not all studies addressed the factors that are the focus of this research. Four (#'s 8, 11, 17, & 19) of the 28 studies did not have clearly identified research questions. Four (#'s 17, 18, 20, & 26) of the studies did not contain findings relevant to this research focus. There were 51 combined occurrences of factors specific to this research among the findings of the 28 selected studies (15 - leadership support, 20 - security policy, and 16 – SETA). Studies then underwent a screening process to ensure an alignment of research questions among studies.

Table 14

Research Question Screening Tool

Study #	Research Questions (Y/N)	Information Security Culture Factors		
		Leadership Support	Security Policy	SETA
1	Yes	X	X	
2	Yes		X	
3	Yes			X
4	Yes ¹	X	X	X
5	Yes		X	X
6	Yes		X	
7	Yes	X	X	X
8	No		X	X
9	Yes	X	X	
10	Yes	X	X	X
11	No	X	X	X
12	Yes			X
13	Yes	X	X	X
14	Yes	X	X	
15	Yes			X
16	Yes	X	X	
17	No			
18	Yes			
19	No			X
20	Yes			
21	Yes	X	X	
22	Yes			X
23	Yes	X	X	
24	Yes	X	X	X
25	Yes	X	X	X
26	Yes ¹			
27	Yes			X
28	Yes		X	X

1 - Identified as research parameters or dimensions instead of research questions.

Decision point. A major decision point arose during the literature search process.

Although several combinations of search criteria across multiple databases were executed, the application of the initially selected parameters failed to yield sufficient results. This researcher was faced with three options:

1) Amend the sources selected: Amendments to the sources selected would have been counter-productive. Sources were specifically selected because of their relevance to scholarly, peer-reviewed research and their relationship to the federal government. Changes to the selected sources would not have significantly increased the probability of literature saturation.

2) Adjust the search parameters: Adjusting search parameters would have been a time-consuming process that was impractical for this study completion timeline. Also, there was little to no assurance that additional variations of multiple searches would result in identifying a sufficient number of acceptable studies. A decision to forego the risk associated with the time needed to conduct multiple searches and maintain current search parameters was made.

3) Modify the inclusion/exclusion criteria: The inclusion/exclusion criteria and research questions collectively delineate the boundaries of this meta-synthesis (Lemire, 2017). While these boundaries were already defined, a slight revision to the inclusion/exclusion criteria expanded the data collection range from ten to fifteen years. The addition of five years yielded a sufficient number of studies to meet the desired effect.

4.3 Inter-Rater Agreement

The assessment of inter-rater agreement provides a way of quantifying the degree of agreement between two or more raters who make independent ratings about the features of a set of subjects. A 3-point Likert scale (1 = No Relevance, 2 = Moderate Relevance; 3 = High

Relevance) measured agreement between Rater A and Rater B. All 28 studies for this research were independently rated and the results are reflected in the below inter-rater agreement table.

Table 15

Inter-Rater Agreement Table

Study #	Rater A	Rater B	Agreement (Yes/No)
1	1	2	No
2	1	2	No
3	3	3	Yes
4	1	2	No
5	3	3	Yes
6	1	1	Yes
7	3	3	Yes
8	1	1	Yes
9	3	3	Yes
10	3	3	Yes
11	1	1	Yes
12	3	3	Yes
13	3	3	Yes
14	3	3	Yes
15	3	3	Yes
16	3	3	Yes
17	1	1	Yes
18	1	2	No
19	1	1	Yes
20	2	2	Yes
21	2	2	Yes
22	3	3	Yes
23	1	2	No
24	3	3	Yes
25	3	3	Yes
26	1	1	Yes
27	1	2	No
28	3	2	No

Note: 1 - No Relevance, 2 - Moderate Relevance; 3 - High Relevance

Rater A and Rater B showed agreement on 21 of the 28 (75%) total studies. Rater A rated 12 studies as having “No Relevance” (43%), 2 studies with “Moderate Relevance” (7%), and 14 studies as having “High Relevance” (50%). Rater B rated 6 studies as having “No Relevance” (21%), 9 studies with “Moderate Relevance” (32%), and 13 studies as having “High Relevance” (46%).

The overall inter-rater agreement among studies selected as “High Relevance” by raters was 13 of 14 (93%). There were 6 rater agreements of “No Relevance”, 2 rater agreements of “Moderate Relevance”, and 13 rater agreements of “High Relevance”. Rater A and Rater B ratings for 7 studies were in disagreement. Table 16 reflects the inter-rater agreement matrix. Inter-rater agreement was calculated using the approach described by Zaiontz (2018).

Table 16

Inter-Rater Agreement Matrix

		Rater A			Total	Percent
		No Relevance	Moderate Relevance	High Relevance		
Rater B	No Relevance	6	0	0	6	21%
	Moderate Relevance	6	2	1	9	32%
	High Relevance	0	0	13	13	46%
Total		12	2	14	28	
Percent		43%	7%	50%		

4.4 Inter-Rater Reliability

Cohen's Kappa (1960) measured the observed level of agreement between raters while accounting for agreement that would be expected by chance. As stated in Chapter 3, rater responses of "No Relevance" and "Moderate Relevance" were counted in the "No" category of the inter-rater reliability rating matrix. Raters assigning "No Relevance" and "Moderate Relevance" to any single study resulted in removal of that study for coding purposes. Only studies with mutual rater agreement of "High Relevance" were considered for inclusion into the "Yes" column/row of the inter-rater reliability rating matrix and for coding purposes. Cohen's Kappa was determined by calculating the marginal frequencies of each rater's ratings utilizing the inter-rater reliability rating matrix in Table 17.

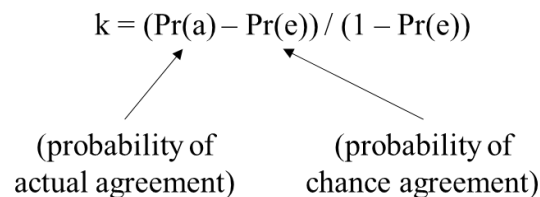
Table 17

Inter-Rater Reliability Rating Matrix

		Coder A		Total
		Yes	No	
Coder B	Yes	13	0	13
	No	1	14	15
	Total	14	14	28

As noted in Chapter III, the below formula was used to solve for Cohen's Kappa.

$$k = (\text{Pr}(a) - \text{Pr}(e)) / (1 - \text{Pr}(e))$$


(probability of actual agreement) (probability of chance agreement)

In order to solve for Kappa, observed [actual] and expected [chance] agreements must be determined. Supporting calculations are annotated for each step in the process.

Step 1: Calculate $Pr_{(a)}$ (the relative observed agreement among raters).

13 studies were rated Yes by both.

14 studies were rated No by both.

So, $Pr_{(a)} = \text{number in agreement} / \text{total} = (13 + 14) / 28 = 0.96$.

Step 2: Find the probability that the raters would randomly both say Yes.

Rater A said Yes to 14/28 studies, or 50% (0.50).

Rater B said Yes to 13/28 studies, or 46% (0.46).

The total probability of the raters both saying Yes randomly is: $0.50 * 0.46 = 0.23$.

Step 3: Calculate the probability that the raters would randomly both say No.

Rater A said No to 14/28 studies, or 50% (0.50).

Rater B said No to 15/28 studies, or 58% (0.53).

The total probability of the raters both saying No randomly is: $0.50 * 0.53 = 0.27$.

Step 4: Calculate $Pr_{(e)}$ (the hypothetical probability of chance agreement).

Add your answers from Step 2 and 3 to get the overall probability that the raters would randomly agree.

$Pr_{(e)} = 0.23 + 0.27 = 0.50$.

Step 5: Insert calculations into the formula and solve:

$$k = (Pr_{(a)} - Pr_{(e)}) / (1 - Pr_{(e)})$$

$$k = (0.96 - 0.50) / (1 - 0.50)$$

$$k = (.46) / (.50)$$

$k = 0.92$, which indicates near perfect agreement.

4.5 Semantic Coding

ATLAS.ti 8 supported the semantic coding process for this study. Codes are used as classification devices at different levels of abstraction in order to create sets of related information units for the purpose of comparison (ATLAS.ti 8, 2018). In this research, semantic coding was used to classify quotations according to study factors (information security culture, leadership support, security policy, and SETA), which formed the networks for emerging themes. Through semantic coding, distinct concepts that shared common meanings were coded using an abstract compilation of selected content to create semantic domains [nodes] for each factor. Mutually exclusive concepts were identified and assigned opposing semantic nodes. Quotations [sub-nodes] were then selected based on key words or phrases and assigned to a node in order to populate networks within each factor. The creation of networks supports the conceptualizing of factorial structures that are visually displayed in the proceeding text. Semantic coding of the 13 studies used in this research resulted in the identification of 4 networks consisting of 36 total nodes (5 - information security culture, 13 - leadership support, 7 - security policy, and 10 - SETA). Finally, there were 398 total sub-nodes selected from all studies. The number of sub-nodes derived from each study ranged from 2 to 45, with the average per study being 11. The coding document depicted in Table 18 provides the total sub-node counts by study and code. While Table 18 is intended to provide a consolidated view of the network, node, and sub-node totals by grouping, it does not provide a real perspective for the complexity involved once linkages are established based on relationships. A view of the consolidated network diagram (Figure 15) provides a more detailed graphic of networks, nodes, sub-nodes, and their relationships. To make it easy for the reader to understand, the proceeding text will address sub-nodes and findings by individual network.

Table 18

Code Document Table

Newtork	Node	Study #3	Study #5	Study #7	Study #9	Study #10	Study #12	Study #13	Study #14	Study #15	Study #16	Study #22	Study #24	Study #25	Total
Information Security Culture	Behavior		2	1										3	6
	Change			1			1							4	6
	Resources			2										1	3
	Teamwork				2		9			1	9		2	3	26
	Workload		2												2
Leadership Support	Accountability						7		1					8	16
	Awareness					2									2
	Behavioral Controls		1		2						1			12	16
	Communication			3	1						6			6	16
	Communication (Employee)										4				4
	Decision making				3									1	4
	Empowerment													4	4
	Involvement	3	1												4
	Management Controls					6	1						3	5	15
	Perceptions				1						23			1	25
	Policy Acceptance				4								1	1	6
	Staff					2					1			2	5
	Incentives									4					4
Security Policy	Classification				4										4
	Compliance		2									2		5	9
	Effectiveness		2	1							2	4		2	11
	Governance				13	1		1			2	3	1	4	25
	Social Impact				5										5
	Transparency				2							1		2	5
	Behavior				2							3		5	10
SETA	Approach, Socio-Technical				2		1	3				1	1	2	10
	Behavior													15	15
	Benefit								3					1	13
	Challenges						17		4	3					24
	Content	3	1							3		1		4	12
	Effectiveness	6	1	2										5	14
	Employee Awareness					5	1			1				7	14
	Feedback			1			3			1		1			6
	Objectives, Goals, & Expectations						12								12
	Training and Delivery Approach	7	1				17		3	9		3		5	45
Total		19	13	11	47	11	68	4	11	22	48	19	8	117	398

The consolidated network diagram (Figure 15) provides a detailed view of networks, nodes, sub-nodes, and their relationships. To make it easy for the reader to understand, the proceeding text will discuss findings for each network and the nodes within that network. Groundedness and density levels are presented for each node. Groundedness levels for each node equates to the

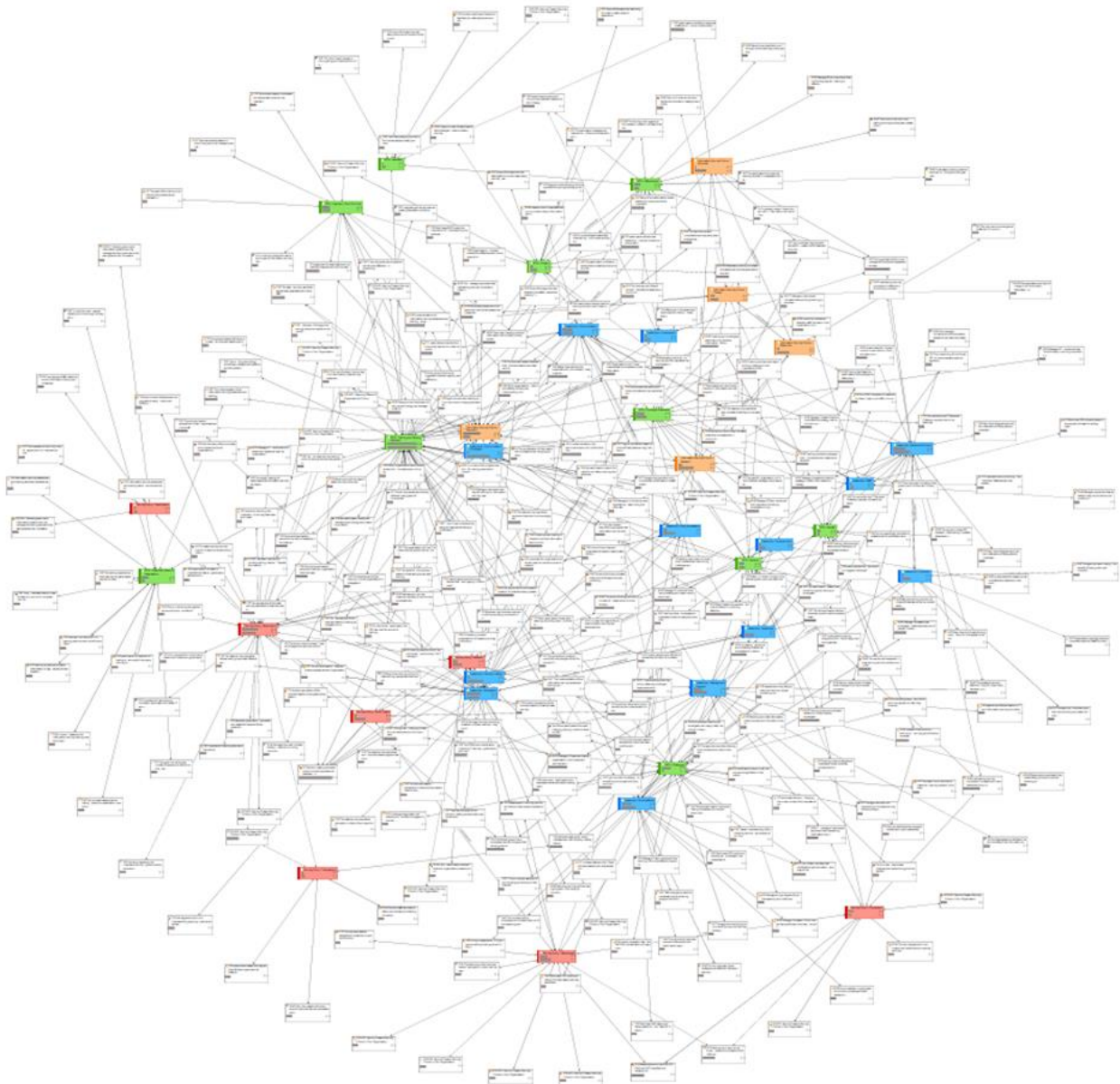


Figure 15. *Consolidated network diagram*

total number of sub-nodes that were extracted from selected studies. Codes with a higher degree of groundedness signify a higher frequency of reporting and a greater probability of evidence. Density levels for each node equates to the total number of relationships with other nodes. Codes with a higher degree of density are indicate nodes with a higher number of related structures and suggest a greater degree of theoretical significance.

Information security culture network. Semantic coding for the information security culture network resulted in 5 nodes and 43 total sub-nodes. Groundedness for the five nodes ranged from 2 to 26 (2 – Workload, 3 – Resources, 6 – Behavior, 6 – Change, and 26 - Teamwork). Density levels for all information security culture nodes ranged from 2 to 4. Figure 16 depicts the coding results and relationships of the information security culture network.

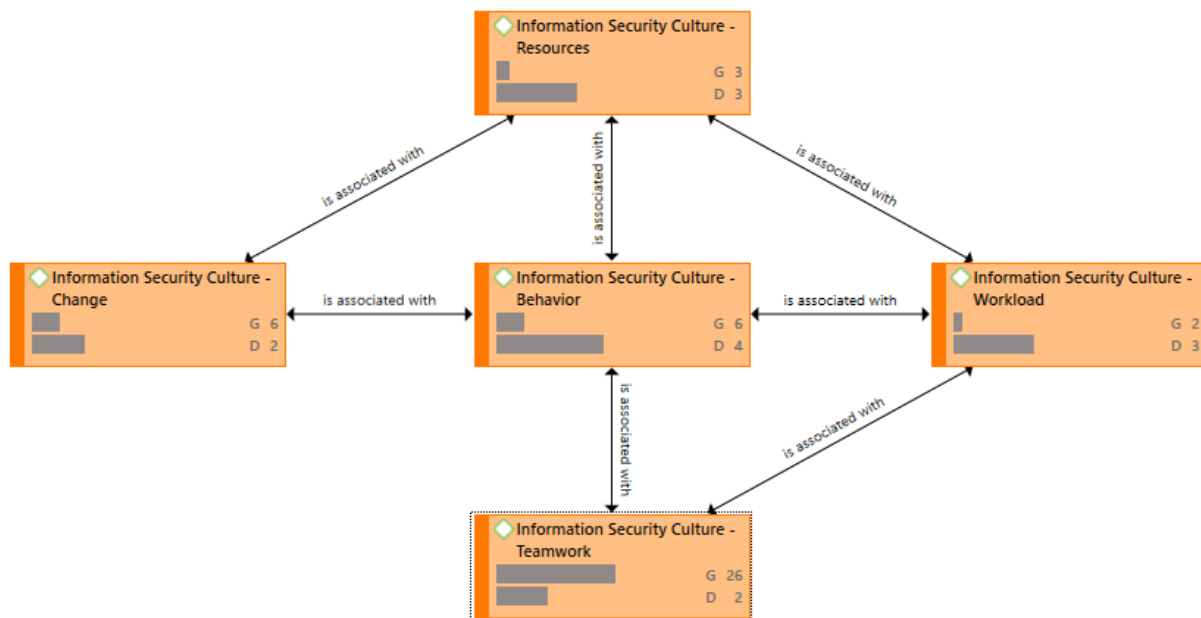


Figure 16. *Information security culture network.*

Behavior. The findings for the behavior node indicate leadership support and SETA have the greatest influence on end-user threat-response behaviors associated with information security

culture. Training was noted as an effective and accepted method of controlling behavior and providing employees with comprehensive measures necessary to safeguard organizational information. However, high organizational tempo and heavy workloads tend to create conflicts between end-user behaviors and information security requirements. Weak and inconsistent application of security policies also create barriers that impede operations. While leadership and subject matter experts within organizations were aware of [and able to recite] security policy, there was little attention to address negative end-user behavior. Another finding that emerged was leadership and subject matter expert disagreement with some information security requirements. Leaders and subject matter experts contribute to organizational security culture and their disagreement with policy serves as an influencing factor for information security policy compliance throughout the organization.

Change. Change within the federal government is known for being an arduous and time-consuming process. Findings in the change node revealed that organizational ineffectiveness and lack of change stems from years of stagnation. Some employees question the efforts needed to affect change and view potential change in terms of whether the amount of time, resources, and effort needed is worth the desired change. Others viewed the removal or reassignment of the employees as a more viable option. One reason for this ineffectiveness was noted as a reluctance to recognize “significant training program concepts affected by organizational culture” (Grant, 2017, p. 103). Also, this “reluctance to recognize and address the effects of organizational culture upon implementation of information security awareness and training programs has allowed the lag in priority to persist” (Grant, 2017, p. 103). Individual experience, openness to change, and leadership involvement were identified as influences of information security culture. The balancing of these items throughout the workforce promotes a positive culture. The findings

indicate training programs are considered an effective resource for enlisting employee compliance and for protecting organizational assets and safeguarding organizational information if properly implemented. A key aspect of successful SETA programs is the feedback from employees. However, employees' failure to actively provide the feedback necessary to improve their organizational information security culture was identified as a weakness. Specifically, ineffective implementation of requirements "prevented the successful integration of a security program into the culture" of large federal organizations (Harris, 2010, p. 171).

Workload and resources. The uniqueness of organizations within the federal government and varying degrees of leadership involvement emerged as a significant influence on employee compliance behavior. In the workload and resources nodes, heavy and increasing workload was a noted source of conflict between employees and compliance intent behavior. Weaknesses in the communication and allocation of resources was also a concern. Varying organizational mission requirements and multiple levels of semi-autonomous leadership approaches also create operating differences throughout the workforce. In addition, Charest (2013) noted variations in leadership, there exists disparity in the "level of understanding and appreciation for the current information security threat environment" among leaders (p. 137).

Teamwork. The concept of teamwork is well established at all levels within the federal government. Two general themes emerged within the teamwork node: 1) acknowledgement of the requirement for a SETA program and trained employees to meet policy requirements, and 2) the overwhelming need for leaders and security specialists to work jointly toward achieving goals. The findings in the information security teamwork node indicate an employee willingness to assist peers with security training to avoid the consequences associated with non-compliance. Additionally, leaders believe a lack of security specialists' capability and its potential negative

impact to organizational security. This may be due to leader perceptions that non-sensitive work environments do not have a need for high levels of security protocols. Alternatively, from the security specialists' perspective, leaders and end-users view security protocols as interfering with mission requirements. Findings in this area indicate room for improvement. Leaders and security specialists share common goals, but do not possess a good understanding of each other's perspective. There was overwhelming agreement "that information security strategy must be in alignment or closely linked to the overall business governance". The findings contend that "such an alignment of strategy would enhance information security performance and reduce loss of critical knowledge" (Stroup, 2014, p. 123).

Leadership support network. Semantic coding for the leadership support network resulted in 13 nodes and 121 total sub-nodes. Groundedness for the 13 nodes varied from 2 to 25 (2 – Awareness, 4 – Communication, 4 – Empowerment, 4 – Involvement, 4 – Incentives, 5 – Staff, 4 – Decision Making, 6 – Policy Acceptance, 15 – Management Controls, 16 – Accountability, 16 – Behavioral Controls, 16 – Communication, and 25 - Perceptions). Density levels for leadership support nodes ranged from 2 to 4. Figure 17 depicts the coding results and relationships of the leadership support network.

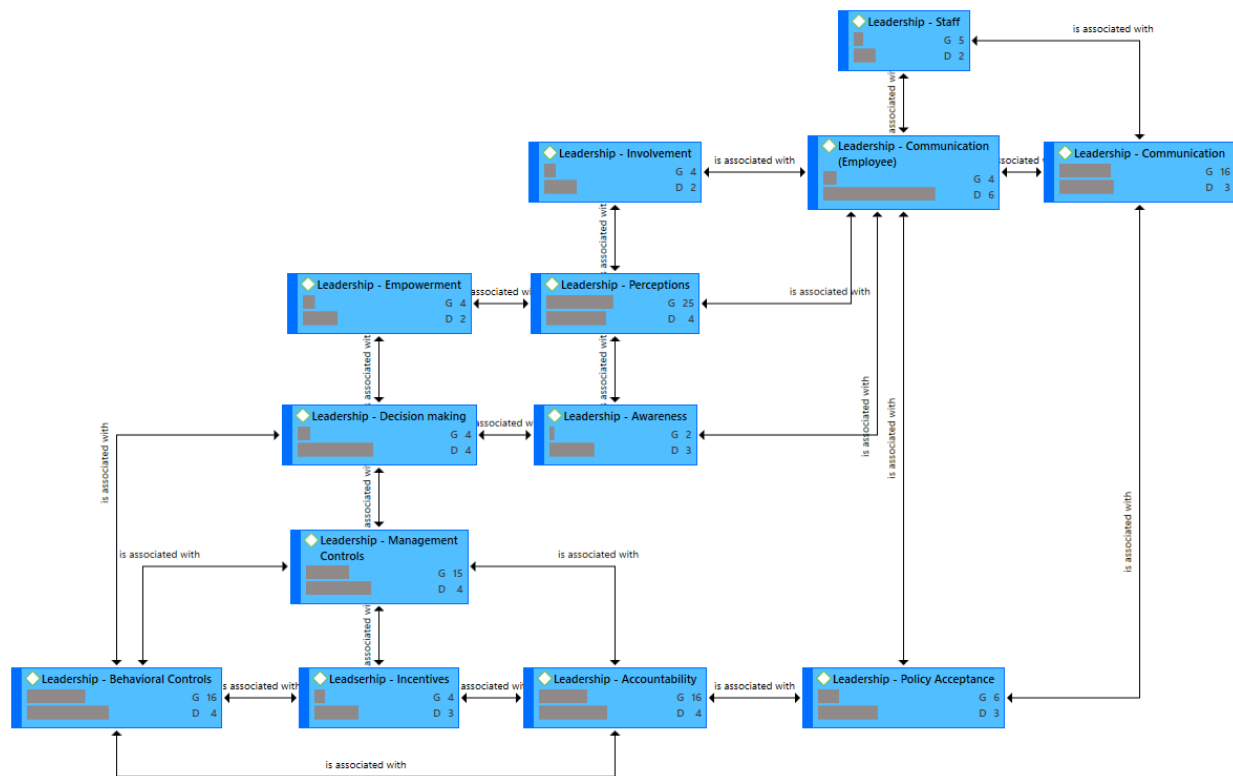


Figure 17. *Leadership support network.*

Accountability. The findings in the accountability node clearly held that all levels of the workforce view accountability as a key component of information security culture. There was widespread acceptance for holding employees accountable, in writing. Concurrently, many of the responses for holding employees accountable were linked to employees having received their required training and their signed acknowledgement of acceptable use policies. There was overwhelming consensus of the desire to complete required training and not face the consequences. Another finding highlighted a desire by both managers and employees to receive information on those who were held accountable. They believed the information could effectively educate other employees on the results of counterproductive behavior, thus reducing the likelihood of similar behaviors.

Behavioral control. Behavioral control node findings revealed two key themes. The first addressed the need for leaders to understand how changes to security controls affect employee behavior. The second addressed a need to control security compliance by providing more training and increasing controls to lessen counterproductive behavior. While there was acknowledgement that some controls were too restrictive, it was generally viewed as an acceptable alternative that provided the desired security levels. Managers believed that being armed with effective strategies and solutions would better equip them for engaging and maintaining an open dialogue with employees.

Communication. Leaders must communicate to engagement in discussions about the organization. The communication node findings highlighted three themes. The first theme discusses the importance of leaders being able to engage in discussions about information security controls. This involves not only understanding the needs of the organization, but also being empathetic to the needs and concerns of the organization's security professionals. The second theme addresses the inability of leaders to understand the technical language used by security professionals. "Communication between the two groups is challenging due to the objectives and language barriers" (Lopez, 2012, p. 104). The third theme provides acknowledgement of a weakness in communication between leaders and security professionals. Leaders can communicate the business aspects of an organization while security professionals communicate the technical aspects of securing such information. However, both groups will have to reach a common ground that enables an understanding of mission goals/objectives and how best to achieve them without implementing overly restrictive security controls. Of note, security professionals acknowledge intentionally not providing senior managers with information for fears of increasing communication barriers. As a result of these communication challenges,

the security professional “perspective regarding data security is negative because business leaders and end users perceive data security as interference or unavoidable to conduct business.” (Lopez, 2012, p. 107).

Decision-making. A single theme emerged from the decision-making node. Leadership decisions should consider all available information and be supported by a synthesis of behavioral, cultural, and social influences. Leadership decision-making involving empowerment should consider social influences and their potential impacts early in the process.

Involvement. In the involvement node, “managerial involvement appeared to have the greatest influence on end-user threat-response behaviors as evidenced by the responses from the end-user population” (Charest, 2013: p. 137). The findings indicate wide support for leadership involvement and empowerment. While employees believe that leadership involvement is necessary to ensure the completion of training is, there also exists a perception that leadership involvement is a joint commitment between leaders and employees. An important note in these findings is the perception that leadership involvement provides credibility by endorsing training. However, there was a notable low regard for leaders who appear during the actual training event, as opposed to the preparations/planning and actual training.

Empowerment. Empowering employees requires leadership trust and the confidence that employees will do the right thing. The findings that emerged in the empowerment node centered on leadership empowering employees on their use of information systems. This move away from leadership involvement and toward empowerment invokes the creativity that encourages employees to think “outside the box” (Tanoh, 2017, p. 98). The findings indicate that innovativeness desired by leaders is best achieved by allowing employees some degree of control

over their daily work tasks. Doing so provides a sense of ownership and results in positive employee perceptions.

Management control. Management controls are an important part of information security culture. Controls can be in the form of policies, training, audits, or making resources/access available to employees. Findings in the management control node reveal agreement among employees that robust information security policy across the federal government can implement successful controls that do not conflict with innovation or operations. However, there was disagreement throughout the federal government on the actual effectiveness of governance in managing information security. Workers at all levels perceive that maintenance of an information security program promotes security controls for employees and improves performance. The findings made a distinction in that the blocking of non-malicious devices and websites is perceived as too restrictive.

Perceptions. Leadership perceptions can drive policy, influence culture, and affect training. A recurring theme throughout the perceptions node revealed leaders' perspectives on the causes of conflicts and misunderstandings with security professionals. A lack of common understanding of goals and communication challenges emerged as the two primary drivers of leader perceptions. Misalignment of goals creates a lack of understanding for safeguarding assets and material. Leaders appear to "understand loss of revenue, ...but they don't understand why some things will cause a loss of revenue" (Lopez, 2012, p. 99). A supporting theme was that leaders working in unclassified or non-sensitive environments believe the securing of data is a lesser priority. While the findings indicate that leaders recognize the importance of security professionals, they remain hesitant to increase security controls - most leaders have not experienced an unauthorized disclosure.

Policy acceptance. The federal government is a policy driven organization that codifies its technical and procedural security requirements. The policy acceptance node highlighted continuing attempts by adversaries to gain access to sensitive and classified information necessitates that leaders develop and implement strategies to contend with these threats. The policy acceptance findings revealed the need for leaders to assess second and third order behavioral effects of implementing increased controls. Leadership should remain open to new techniques or approaches of governance, while decision-making processes include a synthesis of its impacts to the workforce. While federal government standards at times may drive industry standards, adopting industry techniques or approaches may occur.

Staff. Although separate from leadership, staff personnel also play a role in promoting and setting the tone for information security culture. Findings from the leadership staff node revealed that half of the population admitted having little to no knowledge of the implementation of security practices. Furthermore, they specifically acknowledged having no knowledge of 1) current information security policies, 2) existing risk assessments, and 3) incident handling procedures. While managers understood that setting the example was both a manager and staff responsibility, no connection materialized between leadership expectations and staff knowledge.

Incentives. Incentives are a great method of rewarding employees. When employees feel their work is acknowledged and rewarded, they are prone to go the extra mile. Findings from the incentives node revealed organizations were not providing a reason for employees improving their security posture or establishing and clarifying meaningful incentives for acknowledging outstanding security performance. Providing monetary and non-monetary incentives can affect security culture change. Advertising these incentives in exchange for compliance and notification of violations is appreciated by employees.

Security policy network. Semantic coding for the security policy network resulted in 7 nodes and 69 total sub-nodes. Groundedness for the 7 nodes varied from 4 to 25 (4 – classification, 5 – social impact, 5 – transparency, 9 – compliance, 10 – behavior, 11 – effectiveness, and 25 – governance). Density levels for leadership support nodes ranged from 1 to 4. Figure 18 depicts the coding results and relationships of the security policy network.

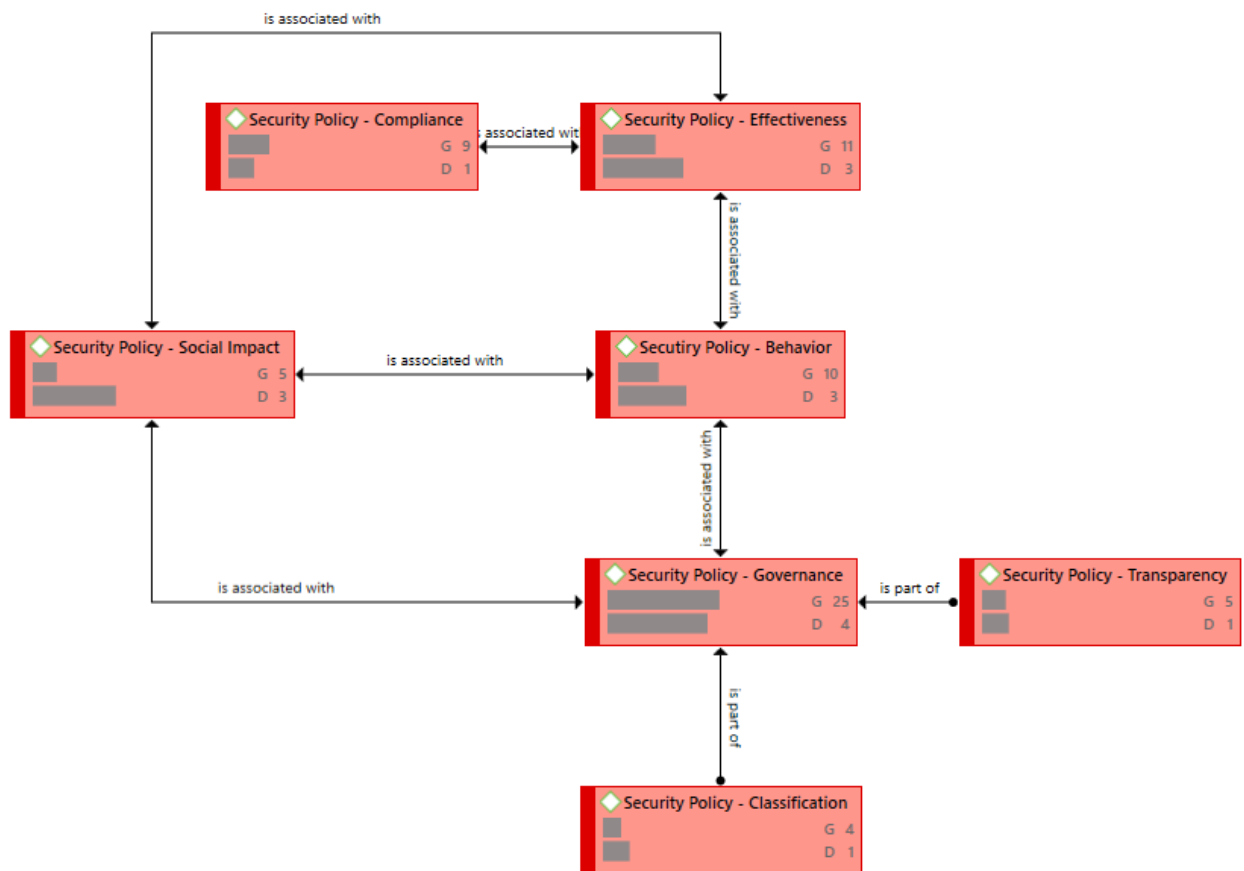


Figure 18. *Security policy network.*

Classification. The federal government’s information classification system serves to protect data. Findings from the classification node revealed significant importance on appropriately classifying information that is shared with partners. There was also a low degree of confirmation that information sharing was not hindered by over classification of information.

However, there was significant agreement of the importance of the current classification system that assigns information at its various levels (Confidential, Secret, and Top Secret).

Compliance. The security policy compliance node is one of the greatest behavioral challenges facing the federal government. Findings from the compliance node indicated only 41.8 percent of employees were aware of the consequence for security violations and 9.8 percent of employees were unaware of any penalties associated with security violations. One reason for these modest numbers may be that only 48.4 percent of those surveyed were aware of incident reporting policies and only 38.6 percent of those that offer training cover incident reporting. Another 40 percent of those surveyed do not have any security awareness training. Employee motivators for compliance include individual motivation, personal responsibility and the importance placed on such information. The findings indicate leadership support in maintaining and supporting the information security program through training increases end-user awareness helps reduce counterproductive security behavior. An important finding was the admission that some employees knowingly violate policy for the sake of convenience.

Effectiveness. The security policy effectiveness node can serve as a measure of organizational security culture. Findings from the effectiveness node provide a leader perception that policies are only effective if they are followed. The leader approach to ensure effectiveness was through efficient controls and additional SETA. The two themes that emerged were weaknesses in security policies and barriers that prevent operations and a lack of policy clarity and consistency. A noted challenge of measuring policy appropriateness is the possibility of non-reporting of security incidents. The reason for non-reporting is that employees may not be aware of what constitutes a breach or are unclear of security reporting procedures. It is difficult for organizations to know if their security programs are effective if they are not measured.

According to the findings, assessment and evaluation are suitable methods of determining security program effectiveness.

Governance. Security policy governance improves security outcomes by providing oversight for policies that can create favorable security conditions. Findings from the governance node highlight the importance of a governance framework that remains neutral in its conveyance, but can mediate or enforce compliance if needed. The below key themes emerged in this node:

- 1) Creating balance and transparency.
- 2) Regulating open and closed systems.
- 3) Avoiding over quantification of control measures.
- 4) Avoiding over classification to protect information.

There was also a perception that governance processes are weakened due to a lack of small group representation. Security policy governance also requires organizations be open to new practices and procedures of governance, and needs employee trust to be successful. Employees, however, were in agreement that strong governance is acceptable if it does not stifle innovation or adversely affect business operations.

Transparency. Security policy transparency allows those impacted to be part of the policy strategy and decision-making process. Leaders, employees, and stakeholders are all affected by security policy and their lack of involvement may impact policy acceptance and compliance. According to the transparency node findings, employees stated the degree they felt there was a lack of balance and transparency in government was average. There was also an average to high perception of a lack of transparency, lack of openness, and unfairness. Most employees also acknowledged that policies were easily accessible and not overly restrictive. The

creation of a work environment with fair and equitable policies and treating employees with dignity and respect will engage employee involvement.

Social impact. The social response resulting from security policy implementation requires leadership attention. Findings from the social impact node call for leaders to consider social impacts when implementing security policy. They also call for leaders to assess the behavioral, cultural, and social influences that could affect employee behavior early in the policy process. According to the findings, there exist situations where major social impacts cannot be fully addressed until external factors are adjusted.

Behavior. Findings derived from the behavior node indicate the most common methods of training include in-person, on-line, and e-mail. A common theme that emerged was that employees view compliance as a job responsibility and rewards should not serve as a motivator for compliance. The findings noted that although organizations implement security policies to control employee behavior, they still experience counterproductive behaviors that do not align with security policies. The best approach to addressing security behavior seems to be through training on security policies that is aligned with the work environment and work-related behaviors of the employees.

SETA network. Semantic coding for the SETA network resulted in 10 nodes and 165 total sub-nodes. Groundedness for the 10 nodes varied from 6 to 45 (6 – feedback, 10 – socio-technical, 12 – content, 12 – objectives, goals, and expectations, 13 – benefit, 14 – effectiveness, 14 – employee awareness, 15 – behavior, 24 – challenges, and 45 – training and delivery approach). Density levels for SETA nodes ranged from 1 to 8. Figure 19 depicts the coding results and relationships of the SETA network.

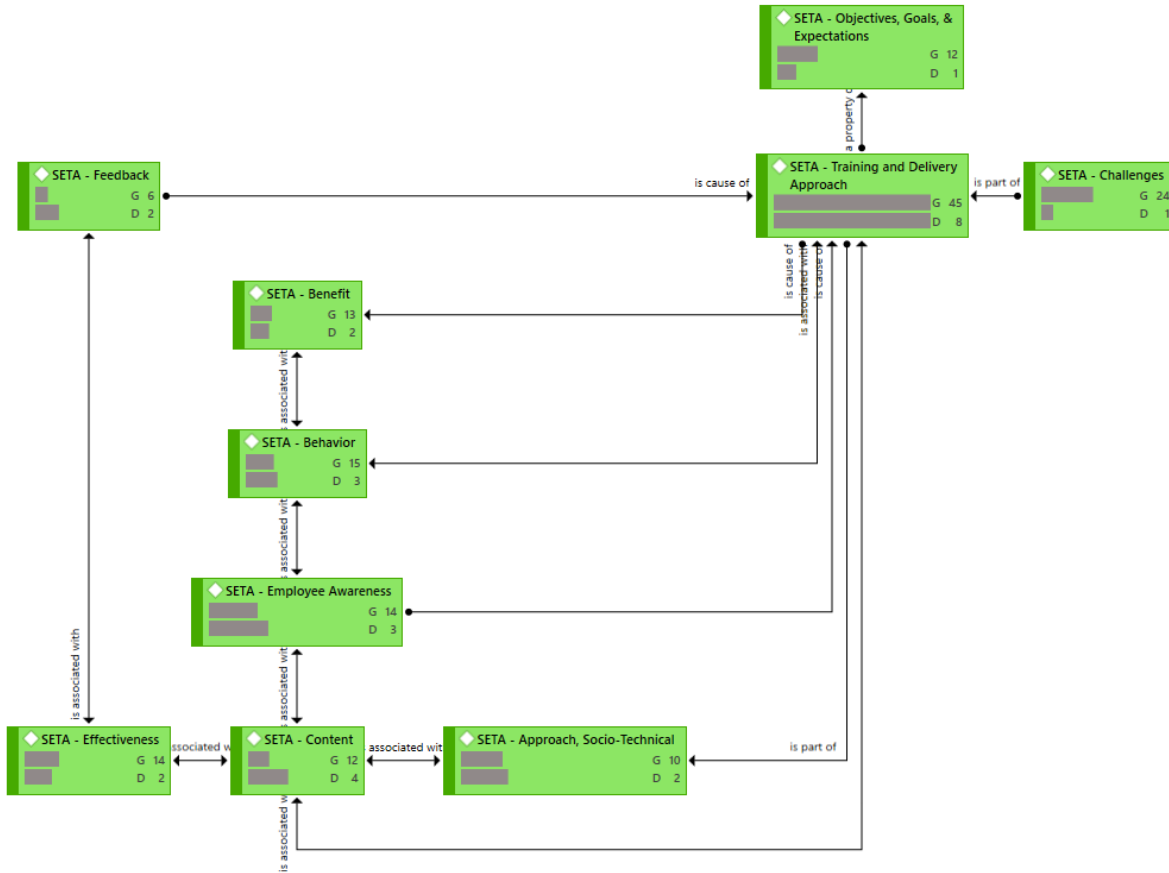


Figure 19. *SETA network*

Socio-technical. Findings from the socio-technical node reveal designers and developers of security technology can leverage what is known about people and their perceptions to provide a more effective security culture. The goal of this training approach is to influence the values of the managers in regard to what they believe are the best ways of maximizing information security. If the nature and scope of their values are influenced to be socio-technical, then their value-based security objectives for protecting information systems will also be socio-technical. In order to change the nature and scope of information security training to socio-technical, information security policy must change its nature and scope to sociotechnical.

Behavior. Within the behavior note, there was overwhelming consensus by all employees and leaders that regular sessions of information security training are the most effective method of diminishing counterproductive behavior. Training not only increases understanding of what comprises counterproductive security behaviors, it also informs employees of the adverse actions associated with such behaviors. A secondary theme called for tighter controls that are also focused on diminishing the likelihood of employees engaging in such behaviors. Those controls were from strong passwords, access control measures, unauthorized software, and end-user privileges.

Benefit. Findings derived from the benefit node reveal that any physical or technical control intended to prevent security violations was considered a benefit of the SETA program. There was a clear distinction between benefits for military, civilians, and defense contractors. Servicemembers viewed certifications as a way of making more money after leaving the military. Federal civilians appeared less motivated, as completion of SETA requirements did not appear to increase career value. Defense contractors associated SETA benefits with salary increases and employment opportunities. Also, while there was agreement in the area of security certifications, there appeared to be no relationship between certifications and risk reduction or return on investment. Overall employee benefits were in the areas of increased awareness, aligning work behaviors, influencing attitudes, and protection of organizational assets.

Challenges. The challenges node brought to light three key themes (resource availability, training credibility, and employee engagement). First, resource constrained environments within the federal government pose a unique set of challenges. A review of the SETA challenges node reveals resources as one of the greatest obstacles. Specifically, the availability of time, employees, and work hours needed to create, prepare and implement SETA aspects is difficult.

Second, the findings indicated training credibility as a training challenge. There was an employee perception that training content should be tailored to the audience and the facilitator be knowledgeable. There was also evidence that employees expected updated training that reflected the current operational environment. Perceived shortcomings in either area by employees was cause to question training credibility. A third theme noted was efforts to keep employees engaged during training. A contributing factor to maintaining employee attention noted that many of those who work technical or engineering jobs feel they are as smart as security professionals and they are sometimes reluctant to listen to the training program. Another related theme highlighted organizational imposed time constraints that prevented the delivery of all training.

Content. SETA content can vary, but the most frequently addressed topics include policies, password protection, workstation security, viruses, remote access, sensitive and classified information, and inappropriate use. However, findings from the content node revealed some shared concerns about content: 1) not allotting the appropriate time for planned training, 2) failing to incorporate SME information to supplement delivery topics, and 3) no attempt to connect with the audience. While security training was highlighted as an effective method of allowing employees to adhere to policies, the type of training may affect the outcome. The findings indicate that simulation training only provided general awareness. Employees acknowledge the training value, but believed tailoring to specific nuances of different environments would have a greater impact on employees.

Effectiveness. The effectiveness of training is diminished when employees scroll through online training slides just to get them completed, but do not read the material. The effectiveness node highlighted training as an effective method of allowing employees to adhere to security

policies when using information systems. There were perceptions that the employee shares responsibility for the effectiveness of training with leadership. Participants felt the employee has a sense of accountability and the responsibility to absorb the material. Alternatively, the leader must engage the employee to show involvement in the process.

Employee awareness. Findings from the SETA employee awareness node revealed there are differing levels of SETA awareness throughout the federal government workforce, but overall awareness was weak. Security professionals possess a greater awareness of information security in their organizations. Program managers were shown to possess a greater knowledge of risks associated with information systems. Employees not in security or management positions were found to possess lower levels of awareness in their agencies. Regardless of the organization, employees who were involved with security programs within their organization possessed a higher degree of security awareness. There were also distinctions in level of SETA awareness between military, government civilians, and defense contractors. Military and government civilians were the groups most likely to receive initial security training.

Feedback. Soliciting feedback is an important way of assessing program effectiveness. Findings from the feedback node reveal that some organizations frequently solicited feedback on how to best present material. However, organizations were not taking the time to assess whether current delivery methods were successful or whether to use the feedback received for continual process improvement. A potential weakness highlighted the concern that employees are not actively involved in providing feedback and improving security of their work and workplace.

Objectives, goals, and expectations. Establishing objectives, goals, and expectations is indicative of a focused SETA program. Findings from the objectives, goals, and expectations node reveal an association with performance appraisals. Some employee performance appraisals

were tied to a security objective, and indirectly related to pay increases. The accessibility, accuracy, content, and frequency of SETA was shown to reduce the number of security incidents. Although employees liked the idea of being provided contact information for security related questions, they believed that training needed to change from rote to interactive.

Training and delivery approach. The training and delivery approach sub-node proved to be the most robust of all sub-nodes. The findings call for SETA programs to consider employee levels of access to classified information and levels of experience when developing the training approach. There was also a call for federal government compliance driven SETA programs to integrate organizational culture as a matter of usefulness. However, there was acknowledgement that organizational cultures which promote innovation will require additional training resources to mirror such innovation in order to maintain employee attention. From a technology perspective, SETA training and delivery approaches that leverage technology were viewed as a means of enhancing training capabilities and enabling employees to feel a sense of connectedness with the workforce. Embedding security training and policy into machine configurations was viewed as reducing the probability of security violations. The distributed and centralized delivery formats and techniques for SETA focused on the threat and the potential for harm to the individual, the organization. There was positive employee appreciation when a change in delivery from traditional slide presentations occurred. Overall, agencies used multiple delivery methods and attempted to provide some form of the required initial, continual, and annual security-awareness to employees.

4.6 Summary

The purpose of this meta-synthesis was to examine information security culture within the federal government through the factors of leadership support, security policy, and SETA and

to synthesize findings to determine emerging themes that identify strengths and weaknesses within the federal government information security culture. A sample of 28 studies was selected to undergo inter-rater agreement and inter-rater-reliability to determine relevance. Thirteen studies were assessed as suitable for this study to identify themes impacting information security culture within the federal government. Textual themes were coded to create a structural network of nodes based on quotations within every study. This chapter presented the emerging themes of selected studies to identify common positive and negative aspects within selected areas of the federal government information security culture. The thematic networks and codes created facilitated a review of the research questions and study factors. Chapter V will address conclusion that are based on those findings.

CHAPTER V: CONCLUSION

5.1 Introduction

Unauthorized disclosures of sensitive and classified information continue within the federal government and the need to protect this information through an effective information security culture is a crucial component of organizational readiness, mission success, and national security. This study implemented a meta-synthesis to examine the information security culture within federal government through the factors of leadership support, security policy, and SETA. This meta-synthesis approach employed a selection and coding process utilizing thirteen specifically selected empirical studies that were relevant to the federal government. The intent was to examine the findings from selected studies in order to identify emerging themes across multiple studies. The research was guided using the central question: “What is the information security culture within the federal government?” To better understand the phenomena of the factors of information security culture, sub-questions were incorporated into this research.

1) What are workforce perceptions of leadership support and federal government information security culture?

2) What are workforce perceptions of security policy and federal government information security culture?

3) What are workforce perceptions of SETA and federal government information security culture?

4) What relationship exists between leadership support, security policy, and SETA within the federal government?

This chapter will examine and discuss the study results derived from the themes which emerged. This chapter will also discuss how this research is grounded in theory and provide its

relationship to the theories identified at the onset of research. A discussion of main findings is provided to emphasize the themes that emerged across multiple studies. The study implications follow and are intended to provide the federal government with an overall theme from which to orient its actions if improvements in information security culture are desired. In support of the implications, recommendations are provided to assist in focusing federal government efforts to improve its overall information security culture. Finally, a new research model is proposed to further this body of knowledge. The model is developed specifically for the federal government, but may be applied to other organizations charged with safeguarding national defense classified information. The model is grounded in theories (GDT, PMT, and POS) that resulted from this study's findings.

5.2 Discussion

This study integrated the key components of leadership support, security policy, and SETA to form a framework for examining the federal government information security culture. The development, implementation, and maintenance of an information security culture is a valuable tool for organizations to educate and prepare employees for implementing behaviors that diminish non-compliance behavior. Information security culture is especially important for organizations whose employees work with sensitive and unclassified information. Therefore, it is important for leaders at all levels of management, staff, and end-users to understand the importance of information security culture and how its factors are employed to ensure the protection of our nation's sensitive and classified information. Research data collection, analysis, and synthesis of sub-codes derived from selected studies served as an essential component of this research framework. From this researcher's perspective, the findings and

themes that emerged provide valuable information and insights about employee experiences concerning security culture from across the federal government.

Grounded theory. This study is well rooted in grounded theory, as it aligns with the grounded theory process of identifying and integrating categories from data. This study also presents a method that provides an explanatory framework that assists in understanding the phenomenon under investigation. Various key strategies were used to identify, refine and integrate categories of grounded theory phenomena. Descriptive labeling of nodes (leadership support, security policy, and SETA) was assigned prior to data analysis. The nodes share central characteristics that allow grouping with a higher-level category (information security culture). Alternatively, the identification of sub-nodes used an analytic process because they allow for a higher level of abstraction and were not developed prior to analysis, but emerged as a result of data analysis. During the coding process, 39 low level categories (sub-nodes) emerged. Since grounded theory aims to identify new context-specific theories, all sub-nodes were grounded in data analysis and coded based on words or phrases contained in the data. Data analysis in grounded theory calls for a line-by-line analysis to ensure a truly grounded product. The coding of pages or large paragraphs should be avoided to prevent less obvious, but equally important, instances or occurrences to emerge.

As previously stated in Chapter I, this research intended to link GDT, the theory of POS, SET, and MT as a basis for examining the security climate within the federal government. From a GDT perspective, SETA programs and policies were found to serve as procedural controls by acting as deterrence instruments to discourage non-compliant behavior. GDT posits the greater the perceived swiftness and certainty of sanctions, the greater the degree of deterrence from the act. Thus, one assumption of GDT is that individuals make rational decisions regarding

compliance or non-compliance based on the associated costs-benefit analysis (Chen, Ramamurthy, & Wen, 2015; D'arcy & Herath, 2011; Yuryna, Lang, Gathegi, & Tygar, 2017). From a GDT perspective, employees do not seem to hold the potential severity and certainty of sanctions in high regard as many acknowledge selective implementation of security protocols. Employee perceptions about leadership accountability as a procedural control was also lacking, negatively impacting employee decisions regarding compliant or non-compliant behavior. The theory of POS addresses employee perceptions about the extent to which organizational support impacts their work efforts. This means, when employees feel the organization values their contributions and cares about their general well-being, they reciprocate with increased dedication and loyalty in their efforts to comply with rules and achieve organizational goals. The potential of issuing of sanctions that occur from policy violations impact the employee's perception of information security culture. Considering POS, empirical findings in this study and its association with building a strong sense of security among employees within the organization, a relationship between SETA and information security culture was established. This relationship was primarily established through a perceived sense of teamwork among employees who encourage others to comply with organizational security training requirements. Alternatively, perceptions about employee care about and well-being are diminished due to a lack of incorporating feedback and a lack of leadership involvement in SETA planning.

In conjunction with POS, SET serves as a theoretical basis for the relationship between POS and compliant behavior. When employees hold POS at high levels, a social exchange occurs in which employees may feel obligated to reciprocate the affective support from organizational leadership by engaging in higher levels of acceptable performance (D'Arcy & Greene, 2014; Dawley, Houghton, & Bucklew, 2010; Newman, Thanacoody, & Hui, 2012). In

the context of information security culture, commitment to higher levels of employee performance will lead to an increased compliance with information security policies. Considering the POS and SET empirical findings and their association with increased commitment to reduce non-compliant behavior, a relationship between leadership support and information security culture is considered moderate. The lack of POS plays a significant role in assessing SET, as both are mutually dependent to some extent.

A review of findings from this study does not provide sufficient evidence from which to draw a relationship with MT from a traditional perspective. MT focuses on the concept of data quantity and concerns merging of insignificant pieces of data that become significant when combined (Rooney, 2017). Initially, MT was cited as a theory regarding its relationship to the collection of information provided through unauthorized disclosures. From a meta-synthesis perspective, MT supports the data collection, analysis, and synthesis process of piecing together information from multiple studies to identify themes as part of a larger picture.

Discussion of findings. The greatest positive influencers on information security culture and end-user threat-response behaviors were leadership support and SETA. However, these influencers are offset by employee conflicts with high organizational tempo, heavy workloads, and leadership disagreement with information security requirements. Both leaders and subject matter experts will need to serve as change agents in order to improve the organizational security culture. The fact that employees actually consider whether positive security change is worth the effort indicates a larger problem within the federal government. From a teamwork perspective, teamwork efforts among employees was generally positive. However, there was an overwhelming need for increased teamwork between leadership and security professionals across

all nodes. The major detractors between leadership and security professionals were seen as misaligned perspectives and ineffective communication between both groups.

Leadership emphasis on individual accountability was noted as having importance at all levels of the federal government. There was also widespread acceptance for leaders holding employees accountable, in writing. The extent of holding employees accountable primarily encompassed meeting training requirements and acknowledgement of acceptable use policies. However, there was little indication of compliance with Executive Order 13526, which requires federal employee performance objectives include the designation and management of classified information as a critical element or item to be rated for performance appraisals. While there were concerns that some controls were too restrictive, it is important to acknowledge that employees commonly accepted security controls as a trade-off in order to achieve the desired security levels. Leadership endorsement of training also provides credibility. However, leaders who are not involved in the planning and only appear for the execution of training lost credibility. From a staff perspective, a noted majority of staff possessed less than a working knowledge of security practices. While lack of knowledge may detract from organizational information security culture, all staff employees are required to receive annual security training and should, therefore, be familiar with security practices.

Approaching from a policy perspective, there is an admitted lack of awareness for the policies, consequences, and penalties associated with security violations, but policies were acknowledged as easily accessible and not overly restrictive. The lack of awareness is compounded by employee admissions that some knowingly violate policy by prioritizing convenience over security. Although employees considered strong governance as acceptable, it was only when such governance did not stifle innovation or adversely affect operations. Also,

policy compliance was seen as a job responsibility and rewards were not expected as a motivator for compliance. The selective compliance with security policy poses a risk for the federal government. Security policy governance can create favorable security conditions. To do so, the leadership must ensure program effectiveness is measured through assessments and evaluation.

There was overwhelming consensus that tighter controls and regular sessions of SETA are the most effective method of diminishing counterproductive behavior. Various delivery methods and numerous areas of security focus necessitate that SETA be tailored to audience needs for the most effectiveness. When SETA is not tailored to the employee's work environment, employees become disengaged and less attentive. One approach to tailoring SETA is through employee feedback. Soliciting feedback is an important way of assessing program effectiveness. However, failing to consider feedback was a noted weakness within federal government. With an overall weakness in SETA, attempts to improving security culture in a resource constrained environment create unique challenges for the federal government.

5.3 Implications

This study's findings are based on scholarly research of federal government participants concerning their experiences and perceptions of information security culture. These perspectives provided the premise for this study's results. The findings and themes revealed in this meta-synthesis were applied to gain a better understanding of federal government information security culture. From this acquired insight, this study seeks to gain greater knowledge concerning the various positive and negative features that constitute the current federal government information security culture. This information can assist equip leaders with implementing more effective information security programs and creating environments that diminish non-compliant behavior.

The first implication of this study concerns federal government information security culture. For the last few years, the federal government has acknowledged a continuing problem with unauthorized disclosures and it certainly has not presented a mechanism to prevent future occurrences. Thus, the implication is for the federal government, at all levels of leadership, to take a genuine interest in actively and intensely engaging in implementing improvements with leadership support, security policy, and SETA.

A second implication addresses leadership accountability. The managing and handling of sensitive and classified information must be clearly stated as a performance objective, as required by executive order and several other governances. Leaders must hold employees accountable, and employees must know they will be held accountable. This study has validated continued employee acknowledgement of non-compliance behavior. Thus, the findings imply that leaders are failing to hold employees accountable. The implication for leaders to meet established requirements by holding employees accountable should stand as a principal goal.

Implication four concerns leadership support. As previously indicated, leadership support plays a significant role in ensuring employee compliance. From the perspective of this researcher, leaders “play the role” in showing leadership support when convenient. From the perspective of leadership support, where there is an absence of IT or security professionals who are responsible for securing this nation’s sensitive and classified information, a different tone emanates from leadership. From this researcher’s perspective drawn from 30+ years of experience, leaders may openly support security policy, but state otherwise behind closed doors.

The final implication five involves the protection of resources essential for maintaining a positive information security culture. Advancements in technology, new and emerging threats, and non-compliant behavior will present continued challenges with protecting sensitive and

classified information. The federal government must simultaneously confront these challenges while planning for future threats to national security. Resources must be budgeted, allocated, and receive the commensurate level of attention as other business-related priorities.

Accordingly, information security strategies should be managed holistically and in parallel with technology, administration, communication, and business architectures, and not as an afterthought or supplemental element of systems or business infrastructure. This study corroborates much of the previous information security culture work. The results of this research deliver an informative assimilation of the mindset of those who manage, lead, and are subject to information security policy. The results provide that insight into the phenomena of information security culture from the perspective of those who are part of that culture.

5.4 Recommendations

Problem solving should be approached from multiple perspectives. The framework used in this study provides governing factors that can be used to further examine specific sectors within the federal government information security culture. The sheer size of the federal government prevents a shotgun approach to solving this problem. Future research should be conducted using this framework to examine the information security culture of organizations that experience the greatest numbers of security incidents. Identifying and isolating the problem areas within the federal government using this approach will help with focusing the resources necessary to contend with such a problem. Additionally, the body of knowledge may benefit from the comparisons which could be conducted between federal government organizations to help gain efficiencies. The themes developed in this research study should also be used to support additional quantitative studies on individual government organizations outside the federal government.

This study revealed strengths and weaknesses within the federal government information security culture. The federal government should promote the strengths found in this research as best business practices. The evidence of teamwork at all levels extends beyond information security culture by improving social exchange, developing relationships, and promoting common goals. The federal government should continue to implement behavior controls through technology and policy. Employees acknowledge that strong governance serves in their best interest by protecting both employees and the organization. With leadership support and SETA as the greatest influence on end-user threat-response behaviors, the federal government should work to create innovative methods of leveraging teamwork to increase the effect of leadership support and SETA on minimizing non-compliant behavior. Forms of leverage may be through increased controls or supplemental training.

A great motivator of compliant behavior is the use of fear appeals. Since the findings highlight a desire by both managers and employees to receive information on those who were held accountable, why not give them what they are asking for? The posting or advertising of adverse actions [with redacted PII] could be leveraged as tools to control behavior. The potential benefit would be three-fold:

- 1) Promote transparency
- 2) Educate employees
- 3) Control non-compliant behavior

Another recommendation addresses accountability. All employees working with classified and sensitive information should have a performance objective that identifies the employee's individual responsibility for safeguarding such information. Considering that some employees knowingly violate policy for the sake of convenience, leadership within the federal

government must implement measures to hold employees accountable for such non-compliant behavior.

There were also some areas of weakness where the federal government should focus on implementing effective strategies to diminish non-compliant security behaviors. High organizational tempo and heavy workloads that exist in many organizations create conflicts between end-user behaviors and information security requirements. Employees also become increasingly frustrated when weak communications and a lack of resources occur. Considering that some employees knowingly violate policy for the sake of convenience, the federal government must implement measures to prevent non-compliant behavior. Security policy was also an area of weakness. Governance controls need to be advertised so that employees are aware of approved security practices, reporting procedures, and consequences for security violations. Although the presence of a SETA program was an overall strength, its weakness lies in the content, delivery and approach that may not be tailored to the specific audience. SETA program improvement could occur when the appropriate feedback is incorporated into the program. A final weakness involves communication among all groups. The primary contributing factor is lack of a common understanding that results from differing perspectives of work focus (business versus technical).

Proposed federal government information security research model. The factors used in constructing this framework represent a first in qualitative research. This researcher was not able to locate any pre-existing quantitative or qualitative research that has utilized the framework developed for this study. Extending the use of this framework into an entity of the federal government may add to the body of knowledge. Conducting this study within the private sector where it is not required to implement an information security program would also produce

interesting findings. To assist in furthering the body of knowledge, this researcher proposes the following research model.

The situation. A preponderance of literature reviewed for this research cites a lack of leadership emphasis, loosely followed security policy, and ineffective SETA programs as sources of unauthorized disclosures in large organizations (GAO, 2015). Failure to follow security procedures, non-compliance with established policy, and dysfunctional SETA programs emerge as key contributors to unauthorized disclosures. In a study addressing the relationship between information security and leadership practices, Rutherford (2014) provides further validation that human error exceeds technical defense as a primary failure point. No single study has sought to explore these three areas when examining information security culture.

The problem. Research in this area is of great value, as furthering the body of knowledge will increase the overall safety and security of American citizens. Within recent years, consequences of unauthorized disclosures to the federal government have included significant unexpected costs, reduced resource availability, strained international relationships, and lost lives. The amount of resources invested in consequence management of unauthorized disclosures sometimes surpasses the damage from the incident itself. To prevent the occurrence of future security incidents, a better understanding of information security culture within the federal government is needed to assist in further refining and implementing organizational information security programs. While significant research exists addressing the information security culture within the private sector, a paucity of research exists addressing the information security culture within the federal government.

The solution. A proposed research model will contribute to new understanding of previous research. The research model is derived from the theoretical framework of GDT, PMT,

and POS as a basis for examining the security climate within the federal government. GDT and PMT support the security policy and SETA factors. GDT posits the greater the perceived swiftness and certainty of sanctions, the greater the degree of deterrence from the act. Thus, one assumption of GDT is that individuals make rational decisions regarding compliance or non-compliance based on the associated costs-benefit analysis. PMT proposes that people protect themselves based on four factors: the perceived severity of a threatening event, the perceived probability of the occurrence, or vulnerability, the efficacy of the recommended preventive behavior, and the perceived self-efficacy. POS closely aligns with the leadership support factor and explains how employee perceptions about the extent to which they receive organizational support impact their work efforts. The federal government information security culture model consists of three factors (leadership support, security policy, and SETA) (Figure 20). A significant review of literature supports the use of these factors as significant aspects for examining federal government information security culture. Sub-factors are derived from this study's semantic coding process. The sub-factors are provided as a point of reference for future researchers to categorize data.

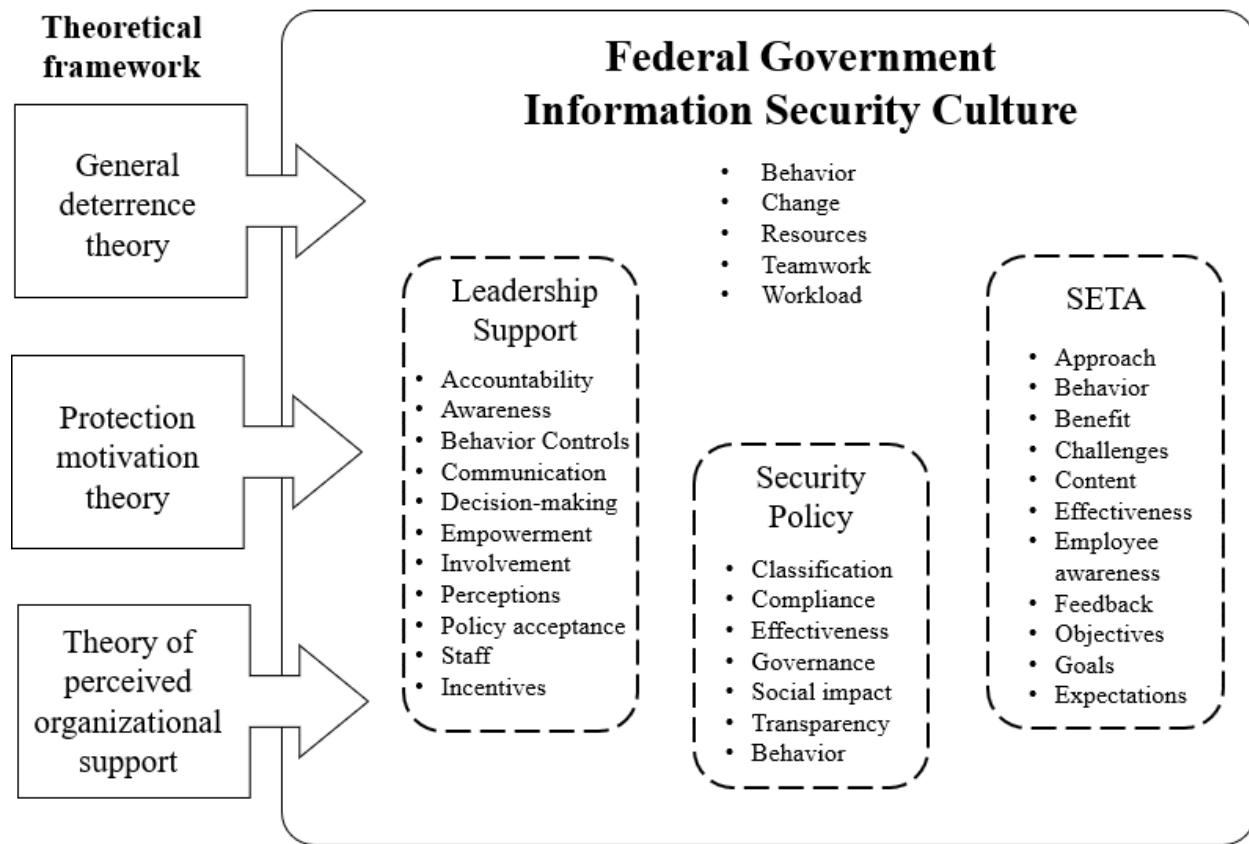


Figure 20. *Proposed federal government information security culture model*

5.5 Conclusion

The meta-synthesis design employed in this qualitative research assisted in gaining insight into the federal government information security culture. The research problem focused on examining the relationships between information security culture and its three factors (leadership support, security policy, and SETA). A goal of this study was to identify and better understand key items in each factor that draw an association with unauthorized disclosures. An opposing goal was to examine management and governance principles intended to shape information security culture and their environments. This study was grounded in general deterrence theory, social exchange theory, and the theory of perceived organizational support, with the central and sub-questions evolving from an exhaustive literature search. The final set of

data collected for this research consisted of 13 empirical studies that underwent a rigorous screening process. As a result of semantic coding, themes emerged that provided an in-depth understanding of the federal government information security culture from the perspectives of service-members, civilians, and defense contractors. The themes provided strengths that highlighted best business practices, as well as weaknesses that afforded insight into potential vulnerabilities. As an important note, the themes, findings and discussion that emerged from this study may not be generalizable, thus caution should be observed if attempting to apply solely to any particular federal entity.

This study separates itself from other studies in this knowledge area, as it concludes by presenting a new research model supported by a theoretical framework. This proposed model is intended for primary use within the public sector, but may be applicable in some private sector organizations. The factors of federal government information security culture emerged as a result of a comprehensive literature review and meticulous meta-synthesis process. Future use of this proposed model will further the body of knowledge and benefit the federal government.

References

- Aftergood, S. (2010). National security secrecy: How the limits change. *Social Research*, 77(3), 839-852, 1052. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/815414815?accountid=10458>
- Al Sabbagh, B., Al Ameen, C., Watterstam, T. & Kowalski, S. (2012). A prototype For HI2Ping information security culture and awareness training. *Proceedings of International Conference on e-Learning and e-Technologies in Education (ICEEE)*, 32–36.
- Aloul, F. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology (JAIT)*, 3(3), 176-183.
- Altermatt, B. (2007). Reliability analysis: Internal consistency reliability. Unpublished instrument. Retrieved from https://psych.hanover.edu/classes/ResearchMethods/Readings/Reliability_Analysis.pdf
- Army Regulation 25-2. (2009). Information assurance
- Army Regulation 380-10. (2009). Foreign Disclosure and Contacts with Foreign Representatives
- Army Regulation 380-5. (2000). Department of the Army information security program
- Bakken, T. (2013). The prosecution of newspapers, reporters, and sources for disclosing classified information: The government's softening of the first amendment. *The University of Toledo Law Review*, 45(1), 1.
- Barton, P. F. (2016). *Unauthorized disclosures and press publication of classified intelligence information: A case study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10109620).

- Berberoglu, A. (2018). Impact of organizational climate on organizational commitment and perceived organizational performance: Empirical evidence from public hospitals. *BMC Health Services Research*, 18 doi:<http://dx.doi.org/10.1186/s12913-018-3149-z>
- Bronson, D. E. and Davis, T. S. (2013). *Finding and evaluating evidence: Systematic reviews and evidence-based practice*. Oxford University Press.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Card, N. A. (2012). *Applied meta-analysis for social science research*. New York, NY: The Guilford Press.
- Castellano, N. E. (2017). Where the sunshine meets the shade: Using FOIA exemption 4 to protect confidential compliance information after the 2016 FOIA improvement act. *Public Contract Law Journal*, 46(3), 589-622. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1918883896?accountid=10458>
- Center for Development of Security Excellence (2018). *Insider Threat Case Studies*. Retrieved from: <https://www.cdse.edu/resources/case-studies/insider-threat.html>
- Central Intelligence Agency (2018). Freedom of Information Act Electronic Reading Room. Retrieved from: <https://www.cia.gov/library/readingroom/document/cia-rdp94b00280r001200100015-9>

- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security*, 1(3), 18-41. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/203675978?accountid=10458>
- Chandran, A. (2015). The classified information procedures act in the age of terrorism: Remodeling CIPA in an offense-specific manner. *Duke Law Journal*, 64(7), 1411.
- Chen, Y., Ramamurthy, R., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, 55(3), 11-19. Retrieved from <https://search.proquest.com/docview/1674250399?accountid=10458>
- Classified Information Procedures Act, 18 U.S.C. § 1-16 (1980).
- Cohen, J. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20, 213-220, 1960.
- Cooper, H. (2010). *Research synthesis and meta-analysis—a step-by-step approach (4th ed.)*. Thousand Oaks, CA: Sage Publications.
- Creswell, J (2013) *Qualitative Inquiry and Research Design; Choosing Among Five Approaches (3rd ed)*, Los Angeles, CA: Sage Publication.
- Creswell, J. (2014) *Research Design; Qualitative, Quantitative, and Mixed Methods Approaches (4th ed)*, Los Angeles, CA: Sage Publication.
- Creswell, J. (2015). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research (5th ed)*. Boston, MA: Pearson.

- Creswell, J. W. & Creswell, D. J. (2018) *Research Design; Qualitative, Quantitative, and Mixed Methods Approaches (5th ed)*. Los Angeles, CA: Sage Publication.
- Da Veiga A. & Martins, N. (2014). Information Security Culture: A Comparative Analysis of Four Assessments. *Proceedings at the European Conference on Information Management and Evaluation (ECIME)*. Ghent, Belgium. doi: 10.13140/2.1.3221.8885.
- Da Veiga A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, 49, 162 - 176.
- Da Veiga, A. & Martins, N. (2014). The Value of Using a Validated Information Security Culture Instrument. *Proceedings at the European Conference on Information Management and Evaluation (ECIME)*, Ghent, Belgium. doi: 10.13140/2.1.2283.9049
- Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information and Computer Security*, 24(2), 139-151. Retrieved from <https://search.proquest.com/docview/1826442794?accountid=458>
- Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196. Retrieved from <https://search.proquest.com/docview/207388846?accountid=10458>
- Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review*, 13(1), 37-58, 101-102. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1881414624?accountid=10458>

- D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474-489. doi:10.1108/IMCS-08-2013-0057
- D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658. doi:http://dx.doi.org.desu.idm.oclc.org/10.1057/ejis.2011.23
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98,155,157. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/208155167?accountid=10458>
- Dawley, D., Houghton, J. D., & Bucklew, N. S. (2010). Perceived organizational support and turnover intention: The mediating effects of personal sacrifice and job fit. *The Journal of Social Psychology*, 150(3), 238-57. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/741063922?accountid=10458>
- Defense Intelligence Agency (29 Jan 2014), Senate Select Committee on Intelligence. *DIA Director Flynn: Unauthorized Disclosures Have "Caused Grave Damage to Our National Security"*. Retrieved from <http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/567078/dia-director-flynn-unauthorized-disclosures-have-caused-grave-damage-to-our-nat/>
- Defense Manpower Data Center (DMDC), DoD Personnel, Workforce Reports & Publications, (August 2018). Retrieved from https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp

Department of Defense (DoD), Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy (ODASD (MC&FP)), *2015 Demographics: Profile of the military community*, Retrieved from <http://download.militaryonesource.mil/12038/MOS/Reports/2015-Demographics-Report.pdf>

Department of the Army Memorandum. (2009). Implementation of Information Assurance Best Business Practice (IABBP).

Director of National Intelligence. (2015). National Counterintelligence and Security Center. *2015 Annual Report on Security Clearance Determinations*. Retrieved from <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2016/item/1603-2015-annual-report-on-security-clearance-determinations>

Director of National Intelligence. (2016). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Director of National Intelligence. (2017). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf>

Director of National Intelligence. (2018). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>

- Donahue, S. E. (2011). *Assessing the impact that organizational culture has on enterprise information security incidents* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3486968)
- Dubouloz, CJ, King, J., Ashe, B., Paterson, B., Chevrier, J., Moldoveanu, M., (2010). The process of transformation in rehabilitation: What does it look like? *International Journal of Therapy and Rehabilitation*, 17(11), 604-615
- Erwin, J. E., Brotherson, M. J., & Summers, J. A. (SEP 2011) Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. *Journal of Early Intervention* 33(3), 186-200. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1033.8634&rep=rep1&type=pdf>
- Escaleras, M., Lin, S., & Register, C. (2010). Freedom of information acts and public sector corruption. *Public Choice*, 145(3-4), 435-460.
doi:<http://dx.doi.org.desu.idm.oclc.org/10.1007/s11127-009-9574-0>
- Eustace, A., & Martins, N. (2014). The role of leadership in shaping organizational climate: An example from the fast-moving consumer goods industry. *SA Journal of Industrial Psychology*, 40(1), 1-13. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1530409768?accountid=10458>
- Exec. Order No. 13526, 75 F.R. 707-731 (2009).
- Exec. Order No. 13556, 75 F.R. 68675-68677 (2010).

- Fitzpatrick, W. M., & DiLullo, S. A. (2013). International trade secret protection: Global issues and responses. *Competition Forum*, 11(2), 21-46. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1756027032?accountid=10458>
- Francois, M. T. (2016). *A quantitative study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10252444)
- Freedom of Information Act, 5 U.S.C. § 552 (1996).
- Fujii, S., Sato, M., Yamauchi, T., & Taniguchi, H. (2016). Evaluation and design of function for tracing diffusion of classified information for file operations with KVM. *The Journal of Supercomputing*, 72(5), 1841-1861. doi:10.1007/s11227-016-1671-5
- Grande, T. (2015). Calculating and interpreting Cohen's Kappa in Excel [Software and training video]. Unpublished instrument. Retrieved from <https://www.youtube.com/watch?v=AfgFyzGGlto>
- Guo, Y., Kopec, J.A, Cibere, J., Li, C. L., & Goldsmith, C. H., (2016). Population survey features and response rates: A randomized experiment. *American Journal of Public Health*, 106(8), 1422-1426.
doi:<http://dx.doi.org.desu.idm.oclc.org/10.2105/AJPH.2016.303198>
- Hallgren, K. A. (2012). Computing Inter-Rater Reliability for Observational Data: An Overview and Tutorial. *Tutorials in Quantitative Methods for Psychology*, 8(1), 23–34.

- Hamstra, M. R., Sassenberg, K., Van Yperen, N. W., & Wisse, B. (2014). Followers feel valued—When leaders' regulatory focus makes leaders exhibit behavior that fits followers' regulatory focus. *Journal of Experimental Social Psychology*, 51, 34-40.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. doi:10.1016/j.dss.2009.02.005
- Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? an empirical approach for the causes of non-compliance. *Online Information Review*, 41(1), 2-18. doi:10.1108/OIR-11-2015-0358
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69-79. doi:10.1016/j.im.2013.10.001
- Iljins, J., Skvarciany, V., & Gaile-Sarkane, E. (2015). Impact on organizational climate through organizational culture factors. case study of latvia and lithuania. *Trendy Ekonomiky a Managementu*, 9(24), 9-17. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1770210025?accountid=10458>
- ISO/IEC 27002 (2013), Information Technology – Security Techniques – Code of Practice for Information Security Management, ISO/IEC 27002.
- Jaffer, J. (2010). The mosaic theory. *Social Research*, 77(3), 873-0_3. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/815414808?accountid=10458>. Retrieved from [https://search-proquest-](https://search-proquest-com.desu.idm.oclc.org/docview/815414808?accountid=10458)

com.desu.idm.oclc.org/abicomplete/docview/815414808/C5477FDF44EF465CPQ/3?accountid=10458

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518-555. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/889977041?accountid=10458>

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture - state-of-the-art review between 2000 and 2013. *Information and Computer Security*, 23(3), 246-285. Retrieved from <https://search.proquest.com/docview/1786146076?accountid=10458>

Kasner, A. J. (2015). National security leaks and constitutional duty. *Stanford Law Review*, 67(1), 241-283. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1661722557?accountid=10458>

Lemire, S. T. (2017). Meta-modeling social programs: Methodological reflections on a practical application. UCLA. ProQuest ID: Lemire_ucla_0031D_15949. Merritt ID: <https://escholarship.org/uc/item/2nc16490>

Littell, J. H., Corcoran, J., & Pillai, V. K. (2008). *Systematic reviews and meta-analysis*. Oxford, England: Oxford University Press."

- Liu, C. (2015). Types of employee perceptions of information security using Q methodology: An empirical study. *International Journal of Business and Information*, 10(4), 557-575.
Retrieved from <https://search.proquest.com/docview/1779514165?accountid=458>
- Livanis, E. (2016). Financial aspects of cyber risks and taxonomy for the efficient handling of these risks. *Proceedings at the Varazdin Development and Entrepreneurship Agency (VADEA)*. Varazdin, Croatia. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1854280427?accountid=10458>
- Lutkenhaus, J. (2014). Prosecuting leakers the easy way: 18 U.S.C. § 641. *Columbia Law Review*, 114(5), 1167-1208. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1792171800?accountid=10458>
- MacDougall, I. (2014). CIPA creep: The classified information procedures act and its drift into civil national security litigation. *Columbia Human Rights Law Review*, 45(2), 668.
- Maxwell, L. (2015). Truth in public: Chelsea manning, gender identity, and the politics of truth-telling. *Theory & Event*, 18(1), 1. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1650149075?accountid=10458>
- Mayer, P., Gerber, N., McDermott, R., Volkamer, M., & Vogt, J. (2017). Productivity vs security: Mitigating conflicting goals in organizations. *Information and Computer Security*, 25(2), 137-151. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1908738496?accountid=10458>
- Meyer, C. (2014). A brief tutorial on inter-rater agreement. Retrieved from <https://dkpro.github.io/dkpro-statistics/inter-rater-agreement-tutorial.pdf>

- Millar, S. A. (2006). Privacy and security: Best practices for global security. *Journal of International Trade Law & Policy*, 5(1), 36-49. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1011918818?accountid=10458>
- Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication & Ethics in Society*, 14(3), 254-271. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1826809344?accountid=10458>
- Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, 27(5), 644-667. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1660745086?accountid=10458>
- New research: Most companies fault employees for data breaches. (2011). *International Journal of Micrographics & Optical Technology*, 29(4), 6-7. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1030743317?accountid=10458>
- Newman, A., Thanacoody, R., & Hui, W. (2011) The effects of perceived organizational support, perceived supervisor support and intra-organizational network resources on turnover intentions: A study of Chinese employees in multinational enterprises. *Personnel Review*, 41(1), 56-72. Retrieved from: doi.org/10.1108/00483481211189947
- Overstreet, K.E. (2017). *Organization development and U.S. institutions of higher education: a thematic meta-synthesis of approaches and practice* (Doctoral dissertation). Retrieved from <https://pqdtopen.proquest.com/doc/1886474521.html?FMT=AI>

- Papandrea, M. (2014). Leaker traitor whistleblower spy: National security leaks and the first amendment. *Boston University Law Review*, 94(2), 449-544. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1529055968?accountid=10458>
- Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010, October). Human Factors and Information Security: Individual, Culture and Security Environment. Retrieved from U.S. Department of Defense: <http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf>
- Paterson, B.L., Dubouloz, C.J., Chevrier, J., Ashe, B., King, J., & Moldoveanu, M. (2009). Conducting qualitative meta-synthesis research: Insights from a meta-synthesis project. *International Journal of Qualitative Methods* 8(3). Retrieved from <https://doi.org/10.1177/160940690900800304>
- Pierce, R. E. (2012). *Key factors in the success of an organization's information security culture: A quantitative study and analysis* (Doctoral dissertation). Retrieved from <https://search.proquest.com/docview/1143268791?accountid=10458>
- Polanin, J. R. (2013). *Addressing the Issue of Meta-Analysis Multiplicity in Education and Psychology* (Doctoral Dissertation). Retrieved from http://ecommons.luc.edu/luc_diss/539
- Poortman, C. L., & Schildkamp, K. (2012). Alternative quality standards in qualitative research? *Quality and Quantity*, 46(6), 1727-1751.
doi:<http://dx.doi.org.desu.idm.oclc.org/10.1007/s11135-011-9555-5>
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.
doi: 10.2307/25750704

Radsan, A. J. (2010). Remodeling the classified information procedures act. *Cardozo Law Review*, 32(2), 437.

Revitalizing privacy and trust in a data-driven world: Key findings from the global state of information security survey. (2018). *Cybersecurity and Privacy*. Retrieved from <https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf>

Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816-826. doi:10.1016/j.cose.2009.05.008

Rooney, J. L. (2017). Going postal: Analyzing the abuse of mail covers under the fourth amendment. *Vanderbilt Law Review*, 70(5), 1627-1662. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1952349342?accountid=10458>

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, 23(3), 241-255. doi:<http://dx.doi.org.desu.idm.oclc.org/10.1057/ejis.2014.7>

Rutherford, A. J. (2014). *Information security, leadership practices inventory, and their relationship*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3634729)

Schneider, B., Ehrhart, M. G., & Macey, W.H. (2011). Organizational climate research: Achievements and the road ahead. In N. M. Ashkanasy, C. P. M. Widerson, & M. F. Peterson (Eds.), *the Handbook of Organizational Culture and Climate* (2nd ed.). California: Sage Publications, Inc.

- Scully, T. (2014). The cyber security threat stops in the boardroom. *Journal of business continuity & emergency planning*, 7(2), 138-148.). Retrieved from
- Shapiro, J. (2007). Strictly confidential. *Foreign Policy*, (161), 72-73. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/224029925?accountid=10458>
- Shelton, D. C. (2014). *Reasons for non-compliance with mandatory information assurance policies by a trained population* (Doctoral dissertation). Retrieved from: <http://pqdtopen.proquest.com/doc/1752642751.html?FMT=AI>
- Sheskin, D. Handbook of Parametric and Nonparametric Statistical Procedures. 3rd ed., CRM Press, 2004.
- Snilstveit, B., Oliver, S., and Vojtkova, M. (2012). Narrative approaches to systematic review and synthesis of evidence for international development policy and practice. *Journal of Development Effectiveness*, 4(3), p 409-429. doi: 10.1080/19439342.2012.710641
- Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, 17(2), 179-186. doi:<http://dx.doi.org/10.1007/s10799-015-0252-2>
- The surveillance state and its discontents. (2013). *Foreign Policy*, 74, 64-67. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1468593963?accountid=10458>
- Thunder, K. & Berry, R. Q., (2016). The Promise of Qualitative Meta-synthesis for Mathematics Education. *Journal for Research in Mathematics Education*, 47(4), 318–337. Retrieved from <https://www.nctm.org/Publications/Journal-for-Research-in-Mathematics->

Education/2016/Vol47/Issue4/Research-Commentary_-The-Promise-of-Qualitative-Metasyntesis-for-Mathematics-Education/

U.S. Department of Justice. (2018). FOIA search: DoD FOIA requests received, processed, and pending 2013-2017, Retrieved from <https://www.foia.gov/>

U.S. Department of Justice. (2018). Frequently asked questions: What are FOIA exemptions? Retrieved from <https://www.foia.gov/faq.html>

U.S. DoD Directive 5205.16, Change 2, (2017). The DoD Insider Threat Program. Retrieved from <http://www.esd.whs.mil/Directives/issuances/dodd/>

U.S. DoD Manual 5200.01-V1, Change 1, (2018). *DoD Information Security Program: Overview, Classification, and Declassification*. Retrieved from <http://www.esd.whs.mil/Directives/issuances/dodm/>

U.S. DoD Manual 5200.01-V2, Change 2, (2013). *DoD Information Security Program: Marking of Classified Information*. Retrieved from <http://www.esd.whs.mil/Directives/issuances/dodm/>

U.S. DoD Manual 5200.01-V3, Change 2, (2013). *DoD Information Security Program: Protection of Classified Information*. Retrieved from <http://www.esd.whs.mil/Directives/issuances/dodm/>

U.S. DoD Manual 5200.01-V4, Change 1, (2018). *DoD Information Security Program: Controlled Unclassified Information (CUI)*. Retrieved from <http://www.esd.whs.mil/Directives/issuances/dodm/>

U.S. Government Accounting Office, Report to Congressional Committees. (2015, Jun). *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems* (Publication No. GAO-15-544). Retrieved from <https://www.gao.gov/assets/680/670570.pdf>

U.S. Government Accounting Office, Report to Congressional Committees. (2017, Feb). *High-Risk Areas: Progress on Many High-Rick Areas, While Substantial Efforts Needed on Others*. (Publication No. GAO-17-317). Retrieved from <https://www.gao.gov/assets/690/682765.pdf>

U.S. Government Accounting Office, Report to Congressional Committees. (2017, Sep). *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*. (Publication No. GAO-17-549). Retrieved from <https://www.gao.gov/assets/690/687461.pdf>

Under Secretary of Defense Memorandum, (12 JAN 2018). *Security Executive Agent Directive 4: National Security Adjudicative Guidelines*. Retrieved from http://ogc.osd.mil/doha/SEAD4_20170608.pdf

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 679-722. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1619352586?accountid=10458>

- Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25-35. doi:10.1016/j.dss.2016.09.013
- Weaver, J. M. (2017). Security of classified information: One standard or many? *International Journal of Public Leadership*, 13(1), 9-12, <https://doi.org/10.1108/IJPL-07-2016-0028>
- Wibowo, K., & Batra, M. M. (2010). Information insecurity in the globalization era: Threats, governance, and survivability. *Competition Forum*, 8(1), 111-120. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/760989964?accountid=10458>
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816. doi:10.1016/j.chb.2008.04.005
- Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, 26(4), 401-419. doi:10.1108/ITP-12-2012-0147
- Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organizational culture, procedural countermeasures, and employee security behavior. *Information and Computer Security*, 25(2), 118-136. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/1908738391?accountid=10458>
- Zaiontz, C. (2019). Real statistics using excel: Cohen's Kappa. Unpublished instrument. Retrieved from <http://www.real-statistics.com/reliability/cohens-kappa/>

Zamaray, O. S. (2010). The Obama administration's blanket FOIA policy is no comfort to federal contractors: The need for executive branch guidance on exemption 4 within the "openness regime". *Public Contract Law Journal*, 39(3), 617-639. Retrieved from <https://search-proquest-com.desu.idm.oclc.org/docview/615891137?accountid=10458>

APPENDICES

Appendix A

Appointment Affidavits

(Position to which Appointed)

(Date Appointed)

(Department or Agency)

(Bureau or Division)

(Place of Employment)

I, , do solemnly swear (or affirm) that—

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this day of , 2

at

(City)

(State)

(SEAL)

(Signature of Officer)

Commission expires

(If by a Notary Public, the date of his/her Commission should be shown)

(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Appendix B

Inter-Rater Agreement Table

Study #	Coder A	Coder B	Agreement (Y/N)
1			
2			
3			
4			
5			
...			

Note: 1 - No Relevance, 2 - Moderate Relevance; 3 - High Relevance

Appendix C

Inter-Rater Reliability Rating Matrix

		Coder A		
		Yes	No	Total
Coder B	Yes			
	No			
	Total			

Search and Retrieval Tracking Log

[illegible]

Appendix E

Title and Abstract Screening Tool

Questions	Retain (Y/N)	Explanation (if needed)
Title:		
1. Does the title of the study indicate a study focus on an information security?		
2. Does the title of the study indicate the study is quantitative?		
Abstract:		
1. Does the abstract discuss information security culture?		
2. Does the abstract report the results of an analysis?		
3. Are findings reported in the abstract?		

Appendix F

Content Validation Log

Artifact	Population	Title	Abstract	Research Questions	Findings / Results	Include, Unsure, or Discard (I, U, D)
1						
2						
3						
4						
5						
...						

Appendix G

Research Question & Factors Screening Tool

Study #	Research Questions (Y/N)	Research Questions		
		Leadership Support	Security Policy	SETA
1				
2				
3				
4				
5				
....				

Appendix H

Inclusion / Exclusion Criteria

Inclusion	Exclusion
Qualitative studies	Quantitative studies
Between 2003 – 2018	Mixed-methods studies
Information security culture	Case studies
Results and findings	Reviews or summaries of literature
DoD (military, civilian, contractor)	Calls for research
	Policy documents
	Book reviews
	Op-ed pieces
	Non U.S. DoD setting/context

Appendix I

IRB Exemption



DELAWARE STATE UNIVERSITY

Institutional Review Board – Human Subjects Protection Committee

November 10, 2018

Mr. Calvin Simpson
Department of Education
Delaware State University
1200 N. DuPont Hwy
Dover, DE 19901

Mr. Simpson,

Delaware State University's Institutional Review Board (IRB)-Human Subjects Protection Committee has reviewed your project **"A non-experimental meta-synthesis of leadership support, security policy, and security education, training and awareness, on Department of Defense workforce Information security culture"**. After review of application, the Committee has **granted** an exemption from the IRB as it meets a Category of Exempt Research specified in 45 CFR 46.101(b).

Contact the Office of Sponsored Programs at 302-857-6834 if you have any questions or concerns.

Sincerely,

Dr. Brian Friel
Chairperson, Human Subjects Committee (IRB)

ckh