REORGANIZING FOR HOMELAND SECURITY:
DOES CENTRALIZATION IMPROVE INFORMATION-SHARING?

by
Alexandra L. Rosen

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Government

Baltimore, Maryland
August, 2019

ABSTRACT

In the wake of the terror attacks of September 11, 2001, President George W. Bush signed into law the Homeland Security Act of 2002 (Public Law 107-296), which formally authorized the creation of the Department of Homeland Security (DHS). The Homeland Security Act of 2002 centralized twenty-two federal agencies with a diverse array of missions into a unified, integrated cabinet-level department. DHS was explicitly designed to rectify the conditions that enabled the September 11 terror attacks to take place. Thus, DHS's centralized organizational structure was intended to facilitate information-sharing and coordination among the numerous government agencies with a stake in the homeland security mission. These structural reforms were based on the premise that a centralized bureaucratic model is more apt to foster inter-agency coordination than is a decentralized bureaucratic model.

This paper examines the degree to which the creation of the Department of Homeland Security resolved the information-sharing challenges that ultimately resulted in the events of September 11. Chapter 1 evaluates the foremost theoretical perspectives on information-sharing to answer the following questions: *What is information? What does information-sharing mean? How does information-sharing happen? How is information-sharing measured?* Chapter 2 examines how bureaucracy contributes to, and at times exacerbates, the myriad factors that inhibit information-sharing efforts among Department of Homeland Security component agencies. Chapter 3 assesses DHS's response to the terror attack in San Bernardino, California on December 2, 2015 as a case study to illustrate how the Department of Homeland Security's centralized bureaucratic model enables and encourages its component agencies to pursue their parochial self-interests at the detriment of the Department's overarching mission.

All three chapters provide critical insight into the ways in which the Department of Homeland Security's organizational structure institutionalizes interagency competition, thereby reinforcing factors that impede and discourage effective information-sharing. Self-interest ultimately, is what undercuts the unity of effort that the centralization of twenty-two disparate agencies was intended to foster. This paper concludes that structural reform alone is insufficient—the Department of Homeland Security must supplement its centralized organizational structure with an incentives system to promote effective, timely, and generous information-sharing among component agencies.

Keywords: information-sharing, Department of Homeland Security, centralization

Thesis Reviewers:

Michael E. Siegel, Ph.D.

Thomas H. Stanton, J.D.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

1. AMO – Air and Marine Operations
2. APG – Agency Priority Goals
3. BCIS – Bureau of Citizenship and Immigration Services
4. CBP – Customs and Border Protection
5. CIA – Central Intelligence Agency
6. DHS - Department of Homeland Security
7. FBI – Federal Bureau of Investigation
8. FDNS – Fraud Detection and National Security Directorate
9. FEMA – Federal Emergency Management Agency
10. FPS – Federal Protective Service
11. FY – Fiscal Year
12. GAO – Government Accountability Office
13. GEOINT – Geospatial Intelligence
14. HSDN – Homeland Security Data Network
15. HSI – Homeland Security Investigations
16. HSIN – Homeland Security Information Network
17. HUMINT – Human Intelligence
18. I&A – Office of Intelligence and Analysis
19. IC – Intelligence Community
20. ICE – Immigration and Customs Enforcement
21. IMINT – Imagery Intelligence
22. INS – Immigration and Naturalization Service
23. IRC – Inland Regional Center
24. ISIS – Islamic State of Iraq and Syria
25. IT – Information Technology
26. JTF – Joint Task Force
27. JTTF – Joint Terrorism Task Force
28. MASINT – Measurement and Signature Intelligence
29. NPPD – National Protection and Programs Directorate
30. ODNI – Office of the Director of National Intelligence
31. OIG – Office of Inspector General
32. OMB – Office of Management and Budget
33. OSINT – Open-source Intelligence
34. PIO – Performance Improvement Officer
35. POE – Port of Entry
36. PMDF – Performance Measure Definition Form
37. PPBE – Planning, Programming, Budgeting, and Execution
38. SIGINT – Signals Intelligence
39. TCO – Transnational Criminal Organization
40. TSA – Transportation Security Administration
41. USCG – U.S. Coast Guard
42. USCIS – U.S. Citizenship and Immigration Services
43. USSS – U.S. Secret Service

INTRODUCTION

Intelligence failures are predictably followed by calls for structural reform. Likewise, calls for structural reform are predictably focused on improving information-sharing among intelligence organizations. The structural reforms mandated by the National Security Act of 1947 (Public Law 253) were largely intended to rectify the conditions that prompted the Pearl Harbor intelligence failure. However, despite the landmark structural improvements achieved through the National Security Act of 1947, the United States experienced another intelligence failure on September 11, 2001.

On September 11, 2001 nineteen al-Qaeda militants hijacked four airplanes and carried out suicide attacks against targets in the United States. The terrorists crashed two planes into the World Trade Center in New York City, one plane into the Pentagon near Washington, D.C., and one plane in a field in Pennsylvania. The attacks caused the deaths of 2,996 people and the injuries of more than 6,000 others. It was deadliest terrorist act in U.S. history and the most devastating foreign attack on American soil since Pearl Harbor. Moreover, like Pearl Harbor, the September 11 terror attacks represented an intelligence failure characterized by inadequate coordination and insufficient information-sharing. The September 11 intelligence failure is colloquially referred to as a failure to 'connect the dots.'

Similar to how the United States responded to the attacks on Pearl Harbor with structural reforms, the United States also pursued a massive organizational overhaul in the wake of the September 11 terror attacks. On November 25, 2002, President George W. Bush signed into law the Homeland Security Act of 2002 (Public Law 107-296), which formally authorized the creation of the Department of Homeland Security (DHS).

The Homeland Security Act of 2002 centralized twenty-two federal agencies with a diverse array of missions into a unified, integrated cabinet-level department. Importantly, the structural reforms were based on the premise that a centralized bureaucratic model is more apt to prevent strategic surprise and foster coordination than is a decentralized bureaucratic model. Theoretically, centralization, if supported by consistent information-sharing activities, can help decision-makers create a more precise and comprehensive picture of complex threats that involve multiple agencies or departments.

President Bush articulated the need for a centralized bureaucratic structure with homeland security as its primary mission, arguing that "the changing nature of the threats facing America requires a new government structure to protect against invisible enemies that can strike with a wide variety of weapons" (Bush, 2002). The Department of Homeland Security was explicitly designed to facilitate information-sharing and coordination among the numerous government agencies with a stake in the homeland security mission. Moreover, the structure of DHS was intended to reflect the dynamic environment in which it operates. Like the National Security Act of 1947, the Homeland Security Act of 2002 imposed structural reforms upon the U.S. national security apparatus to rectify the conditions that prompted an egregious intelligence failure.

While the centralization of homeland security activities under one bureaucratic umbrella presumably offers enhanced coordination, reduced redundancies, and increased output, larger bureaucratic structures are not necessarily apt to govern the unique priorities and organizational cultures of each component agency. Thus, it is reasonable to question the degree to which the creation of the Department of Homeland Security resolved the information-sharing challenges that ultimately resulted in the events of

September 11. This paper provides critical insight into the structural reforms prescribed by the Homeland Security Act of 2002 as well as subsequent changes. Ultimately, this paper demonstrates that the current organizational structure of the Department of Homeland Security discourages information-sharing among the Department's 22 component agencies, and specifically among those agencies responsible for immigration enforcement functions.

The utility of information-sharing has been a topic of academic research for decades, and it continues to receive attention across a range of academic disciplines. Recent scholarly work identifies specific factors that promote effective information-sharing in organizational settings. However, factors influencing inter- and intra-organizational information-sharing efforts are more complex and interrelated when multiple entities or government agencies are involved, such as the homeland security enterprise. As such, the information-sharing literature is limited in that it does not consider the interplay between factor relationships in a sufficiently inclusive theoretical framework. The next three chapters offer substantive research and knowledge from personal experience to answer the following question: *How does the organizational structure of the Department of Homeland Security influence information-sharing among component agencies?*

Chapter 1 provides the framework for this thesis with a literature review discussing how various academic disciplines apply unique theoretical lenses to the study of information-sharing. To better assess how information is shared among and within organizations, as well as across organizational boundaries, it is necessary to conduct a systematic review of predominant theoretical frameworks. This systematic review evaluates key themes and patterns that emerge across academic disciplines to inform a comprehensive, multi-theoretical information-sharing framework. This chapter examines the foremost theoretical perspectives on information-sharing to answer the following questions: *What is information? What does information-sharing mean? How does information-sharing happen? How is information-sharing measured?*

The literature acknowledges that 'information' is a very broad concept, and there is currently no consensus on its boundaries and definition (Willem and Buelens, 2007). Generally, information manifests in two forms: tangible and intangible. It is important to highlight this distinction because the literature suggests that people's attitudes toward information-sharing can be influenced by the form of the information (Feldman and March, 1981; Constant et al., 1994). We can gain more clarity about the relative value and utility of information when the concept is evaluated from four perspectives: (1) information as knowledge, (2) information as a commodity, (3) information as power, and (4) information as intelligence. These distinctions reflect four important facets of information, all of which have important implications in the homeland security context.

To significantly improve information-sharing explanatory power, it is important to discuss information-sharing as an integration of disciplines, including organizational behavior and theory, information systems, psychology, sociology, economics, and strategy. Specifically, the focus is placed on seven predominant theories in the information-sharing literature: (1) theory of reasoned action, (2) transaction cost economics, (3) relational governance theories, including social exchange theory and economic exchange theory, (4) social capital theory, (5) contingency theory, (6) resource dependency theory, and (7) resource based view, including knowledge-based view. The numerous aforementioned theories address factors and conditions that influence information-sharing within and across organizations. It is worthwhile to note that these factors and conditions are often divergent, complementary, or overlapping, and that they each provide a nuanced explanation of a complex and multi-layered process.

Furthermore, the literature presents the information-sharing process through three perspectives: (1) interpersonal, (2) intra-organizational, and (3) inter-organizational (Yang and Maxwell, 2011). When evaluating information-sharing in public organizations, and especially in the homeland security domain, it is important to consider how the three perspectives of information-sharing are both interrelated and, at times, interdependent. Moreover, interpersonal information-sharing behaviors become more complicated when they are embedded within the contexts of intra- and inter-organization information-sharing. Individual attitudes and predilections may interface with organizational factors, such as competition and collaboration, which can either encumber or promote intra- and inter-organizational information-sharing. Unlike information-sharing within a single organizational unit, cross-boundary information-sharing efforts are far more complicated and multifaceted due to the diversity of missions and interests involved. This is particularly important in the context of the Department of Homeland Security, as its component agencies often have overlapping or divergent missions and priorities.

Although information-sharing has attracted considerable attention from researchers and is widely accepted as an approach to improve organizational performance, there is a remarkable absence of research dedicated to measuring the effectiveness of information-sharing efforts. Fundamentally, the success of information-sharing endeavors cannot be measured simply by the successful transmission of information across organizational boundaries; it is also important to assess whether the information is absorbed and utilized effectively within the organization that acquired it (Jackson, 2014; Yang and Maxwell, 2011). Information-sharing is multi-dimensional, and its complexity demands an equally multifaceted evaluation process. The results of the structured review in chapter 1 enable a more informed and multi-dimensional discussion of information-sharing in chapters 2 and 3.

In chapter 2, the focus shifts to examining how bureaucracy contributes to, and at times exacerbates, the myriad factors that inhibit information-sharing efforts among Department of Homeland Security component agencies. These factors highlight the enduring difficulty of harmonizing the twenty-two disparate agencies that comprise the Department of Homeland Security and give credence to the notion that centralization fosters a culture of competition rather than collaboration.

Chapter 2 begins with a discussion of how the Department of Homeland Security's centralized bureaucratic structure is intended to support the Department's primary mission and departmental objectives with regard to information-sharing. The Department of Homeland Security is unique because its components balance the interdependent cultures of law enforcement, domestic intelligence, emergency preparedness, and emergency response to facilitate a robust homeland security enterprise. However, the Department of Homeland Security is particularly vulnerable to contradictory organizational objectives due to the sheer diversity of component objectives, which range from short-term emergency response to long-term intelligence gathering. Notwithstanding these contradictory priorities, the gravity of the overarching homeland security mission demands seamless interoperability between component agencies.

Despite the theoretical benefits of a centralized Department of Homeland Security, centralization imposes large transaction costs on component agencies as they merge and modify their respective activities (Cohen et al., 2006). These costs can inadvertently foster competition between components operating in similar or overlapping regulatory environments. Ultimately, persistent barriers to effective information-sharing are compounded by a bureaucratic model that institutionalizes interagency competition. Five key categories of factors that stymie information-sharing activities among DHS component agencies are identified: (1) lack of information technology interoperability, (2) incongruity of classification standards, (3) overlapping agency jurisdictions and missions, (4) overreliance on outcome-centric metrics to quantify achievement, and (5) correlation between perceived agency performance and annual budget appropriations. The Department of Homeland Security must develop structures and processes that address the aforementioned factors and provide incentives or rewards for collaboration, consultation, and support for implementing key goals.

Chapter 3 examines the Department of Homeland Security's response to the terror attack in San Bernardino, California on December 2, 2015, as a case study to test the information-sharing and bureaucracy theoretical frameworks established in chapters 1 and 2. This case study provides substantive insight into the overarching research question: *How does the organizational structure of the Department of Homeland Security influence information-sharing among component agencies?* Chapter 3 illustrates how the Department of Homeland Security's centralized bureaucratic model enables and encourages component agencies to pursue their parochial self-interests at the detriment of the Department's overarching mission.

This case study features a clear example of an information-sharing failure between two DHS component agencies on hierarchical parity within the broader DHS organizational structure: Immigration and Customs Enforcement (ICE) and U.S. Citizenship and Immigration Services (USCIS). In the aftermath of the terror attack in San Bernardino, USCIS took three deliberate actions to prevent ICE from obtaining information critical to the ongoing investigation: (1) USCIS delayed ICE's entry into the USCIS facility; (2) USCIS prohibited ICE from arresting, detaining, or interviewing anyone in the USCIS facility; and (3) USCIS did not share a tangible copy of Mariya Chernykh's A-file with ICE agents. An analysis of these three actions illustrates how the present organizational structure of the Department of Homeland Security does not incentivize information-sharing between component agencies.

Government agencies must be coerced to share information because bureaucracies are explicitly designed to counteract inter-organizational information-sharing. Institutional features of the U.S. federal government, such as regulations, oversight mechanisms, and organizational cultures, are intended to frustrate integration and prevent organizations from becoming too powerful. Arguably, the multiple layers of bureaucracy inherent in DHS's organizational structure stifle opportunities for information-sharing between component agencies like USCIS and ICE because components have relatively little incentive to overcome the 'institutional features of the U.S. federal government' (Peled, 2014) that frustrate coordination. This problem is compounded by the fact that no specific department-level group is responsible for oversight of overarching component immigration challenges, such as information-sharing (Roth, 2017). Without incentives or an oversight body to encourage cross-component information-sharing, it is unsurprising that the Department of Homeland Security has difficulty coercing USCIS and ICE, and all the other components more broadly, to share information voluntarily.

In the wake of the devastating terror attacks that occurred on September 11, 2001, President George W. Bush recognized that the evolving threat landscape necessitated a more agile, unified government structure that could better protect the homeland and the American people. The Department of Homeland Security was explicitly designed to facilitate cooperation and coordination among the numerous government agencies with a stake in the homeland security mission. Moreover, the structure of DHS was intended to reflect the dynamic environment in which it operates. However, since its inception, the Department of Homeland Security has been largely unable to overcome the same problems that both preceded and prompted its creation. This case study answers the overarching research question with a chilling conclusion: The Department of Homeland Security's organizational structure creates a disincentive for cross-component collaboration and information-sharing. Self-interest, ultimately, is what undermines the unity of effort that the centralization of twenty-two disparate agencies was intended to foster.

CHAPTER 1: A Multi-Theoretical Perspective

I. Introduction

Information-sharing is an important approach to increasing organizational efficiency and fostering innovation. The utility of information-sharing has been a topic of academic research for decades, and it continues to receive attention across a range of academic disciplines. The literature is as vast as it is multidisciplinary, and each discipline applies a unique theoretical lens to the study of information-sharing. To better assess how information is shared among and within organizations, as well as across organizational boundaries, it is critical to first conduct a systematic review of predominant theoretical frameworks. This systematic review evaluates key themes and patterns that emerge across academic disciplines to inform a comprehensive, multi-theoretical information-sharing framework. Chapter 1 examines the foremost theoretical perspectives on information-sharing to answer the following questions: *What is information? What does information-sharing mean? How does information-sharing happen? How is information-sharing measured?* Leaders of massive government agencies, such as the Department of Homeland Security, can improve their approach to information-sharing by studying the meaning of information (implicit versus explicit knowledge), the four ways in which information assumes a relative value (power, knowledge, commodity, and intelligence), the concept of "reasoned action," as well as the concept of "transactions." The results of this structured review will enable a more informed and multi-dimensional discussion of information-sharing in chapters 2 and 3.

II. What is Information?

In the dictionary, ‘information’ is defined as “facts provided or learned about something or someone” (“Information,” n.d.). This definition is sufficient for a rudimentary conceptualization of information, but it fails to capture the variety and nuance of what is being exchanged in an information-sharing partnership. The literature acknowledges that information is a very broad concept, and there is currently no consensus on its boundaries and definition (Willem and Buelens, 2007). Generally, information manifests in two forms: tangible and intangible. Tangible information can be thought of as a document, email, or software program, and intangible information can be thought of as a skill, experience, or memory (Constant et al., 1994). It is important to highlight this distinction because the literature suggests that people’s attitudes toward information-sharing can be influenced by the form of the information (Feldman and March, 1981; Constant et al., 1994). Form, therefore, is a critical variable in the larger conversation about the relative value of information in information-sharing exchanges (Klischewski and Scholl, 2008; Nonaka and Takeuchi, 1995; Scholl, 1999).

From a macro perspective, information must be a nebulous concept because the value of information can be defined only relative to its user (Marchand, 1990). Furthermore, the meaning of information is subject to change over time, so its value and utility can vary even for the same user (Ballou et al., 2003). That said, we can gain more clarity about the relative value and utility of information when the concept is examined from a micro perspective. This involves a meticulous consideration of the context in which the information is exchanged between individuals and across organizational entities. The following sections examine four ways in which information assumes a relative value: (1) information as knowledge, (2) information as a commodity, (3) information as power, and (4) information as intelligence. These distinctions reflect four important facets of information, all of which have important implications in the homeland security context which will be discussed in subsequent chapters.

a. Information as Knowledge

Like information, knowledge is an ambiguous concept. When discussing knowledge, the literature creates two distinctions: explicit and implicit knowledge (Polanyi, 1966; Van Den Hooff and De Ridder, 2004). Information is considered to be explicit knowledge that can be articulated and translated into a tangible form outside of the human mind (Stenmark, 2002; Zhang and Dawes, 2006). However, researchers point out that information-sharing is not only limited to the exchange of tangible, explicit knowledge and information. Rather, information-sharing also encompasses tacit (implicit) knowledge (Polanyi, 1966; Klischewski and Scholl, 2008; Nonaka and Takeuchi, 1995; Scholl, 1999; Van Den Hooff and De Ridder, 2004). The seminal work of Polanyi (1966) clarifies that explicit knowledge is objective, rational, and can be expressed in words, numbers, formulas, or charts. In contrast, implicit knowledge is subjective, experience-based, and difficult to communicate. Implicit knowledge can be better understood as know-how, or “practical understanding that enables a firm to perform various operations” (Sanchez and Heene 1997, p. 178).

Understandably, the practical differences between explicit and implicit knowledge influence the relative ease with which knowledge can be transferred. Explicit knowledge is easier to communicate and thus easier to share (Cress and Kimmerle, 2006). On the other hand, implicit knowledge is embedded in individuals' cognition and thus entrenched within organizational units (Birkinshaw, Nobel, and Ridderstrale, 2002; Szulanski 2000; Willem and Buelens, 2007). As such, individuals are a critical source of implicit knowledge and information within organizations. Through their experiences in the organization's key processes, individuals create, organize, and amass knowledge (Jarvenpaa and Staples, 2001). The knowledge worker therefore possesses a valuable trove of organizational information that is not easily communicated or expressed. Even with the codification of information, implicit knowledge and expertise reside within the individual and are not accessible for broader consumption unless the individual makes the information available (Bock et al., 2005).

b. Information as a Commodity

Information and knowledge sharing have become increasingly important to researchers and practitioners because organizations are now thought to operate in a knowledge economy (Haas and Hansen, 2007). In a knowledge economy, the transfer and exchange of information is a source of competitive advantage and a driver of organizational innovation. Many public-sector organizations create knowledge as their core product, provide knowledge to the public as their main activity, or employ workers to develop knowledge as their primary responsibility (Starbuck, 1992; Willem and Buelens, 2007). In this environment, the quality of information is relevant to its value as a commodity because the transmission and exchange of information takes on a more transactional role. The source, timeliness, relevance, accuracy, and volume of information influence the utility of transactions in a knowledge economy.

Despite the transactional qualities of an information-sharing framework, it can be problematic to refer to knowledge as a commodity because individuals do not view information as a monolithic, undifferentiated resource (Constant et al., 1994). Simply, there is a correlation between the form of information and its psychological meaning to the information possessor. As such, the value of information is inextricably linked to its form, manner of presentation, processors, and channel of communication (Feldman and March, 1981). Although individuals view tangible information products as a commodity in the context of a rational-economic exchange, they do not view expertise as a commodity in the same context (Constant et al., 1994; Jarvenpaa and Staples, 2001). Rather, individuals associate expertise with personal identity and inner qualities. Expertise is "deeply rooted in an individual's action and experience, as well as in the ideals, values, or emotions he or she embraces" (Nonaka and Takeuchi, 1995, p. 8).

This raises a dilemma about information as a commodity: knowledge workers create, organize, and amass tangible information goods and services, but organizations own these products. Additionally, organizations expect employees to extract utility from these products to benefit the organization as a whole (Constant et al., 1994). However, because expertise is associated with a knowledge worker's personal identity and self-worth, the issue of ownership presents a challenging issue. The question of whether organizations can reasonably expect or mandate knowledge workers to share expertise presents an additional layer of ambiguity to this dilemma. For example, some believe that that professional codes of conduct, intellectual property laws, and standard business practices are not sufficient to govern ownership of expertise and that organizations should explicitly address this issue through their organizational culture and through precise policies (Jarvenpaa and Staples 2001).

c. Information as Power

Given that information has value, information is an incredible source of power. Power can be defined as “the capacity of an individual, or group of individuals, to modify the conduct of other individuals or groups in the manner which he desires, and to prevent his own conduct being modified in the manner in which he does not” (Blau, 1964, p. 115). Recognizing that the transfer and exchange of information is a source of competitive advantage in a knowledge economy (Haas and Hansen, 2007), individuals may seek to control information to protect their own self-interests rather than the interests of the organization (Jarvenpaa and Staples, 2001). Regarded as one of the most, if not the most, important organizational asset, knowledge should be carefully managed to avoid power games (Argote et al., 2003; Teece, 1998). Power games involve the unjust use of power to elevate value, influence, or status (Willem and Buelens, 2007). Because owning information within an organization translates to owning power within an organization (Ardichvill et al., 2003; Kolekofski and Heminger, 2003; Marks et al., 2008), information can be hoarded as an asset to strategically enhance individual status and identity (Constant et al., 1994). According to this perspective, information can be understood as a form of property, which when surrendered, diminishes an individual’s influence within the organization (Yang and Maxwell, 2011; Ardichvill et al., 2003; Marks et al., 2008).

d. Information as Intelligence

An article published by Central Intelligence Agency's (CIA) journal, *Studies in Intelligence*, offers the following guidance for defining the term, 'intelligence': "Formulating a brief definition of so broad a term as intelligence is like making a microscopic portrait of a continent, and the product of this effort is likely to have less value than the process of arriving at it" (Bimfort, 1958, p. 75). Quoting the 1955 task force on intelligence of the second Herbert Hoover Commission, Former CIA Director Allen W. Dulles presented the following definition: "Intelligence deals with all the things which should be known in advance of initiating a course of action" (Dulles, 2006, p. 1). In effect, intelligence provides a predictive advantage to an organization, enabling it to act preemptively and make strategic decisions (Phythian and Gill, 2018).

Given the complexity and multifaceted nature of the term, 'information,' and the intentionally narrow scope of this study, intelligence is intended to mean information products (such as strategic assessments or subject profiles) that are shared among and between U.S. government agencies whose missions primarily involve homeland security. While the strategic importance of intelligence as a network of organizations and information as a process are central to homeland security, the focus should be on intelligence as a product (Lowenthal, 2006). In this context, intelligence can be thought of as the tangible result of the processes by which certain types of information are required, requested, collected, analyzed, and disseminated (Lowenthal, 2006). Intelligence is not merely a data dump; it offers value in that the information has been analyzed and packaged for a specific customer (Steiner, 2015). The process of evaluation is key to this process. The potential user must assess the quality of the information before deciding to transform and use it as an intelligence product. In this paper, the intelligence customer is the homeland security professional who receives and uses the intelligence product to make decisions about a course of action.

Intelligence collection is an essential and preliminary step in the creation of intelligence products (Ganor, 2005; Lowenthal, 2006; Steiner, 2015; Clark, 2017). There are six basic intelligence collection disciplines that yield intelligence products for customers ("What is intelligence?," n.d.). The most familiar type of collection is human intelligence (HUMINT), which refers to information collected by human sources about a target's intentions and capabilities. In the homeland security context, many federal, state, and local law enforcement agencies are major HUMINT collectors. Law enforcement agencies rely heavily on human sources, referred to as confidential informants, to provide intelligence that can be used to disrupt terrorist plots (Steiner, 2015). In addition to HUMINT, there are five forms of technical intelligence collection techniques: signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), open-source intelligence (OSINT), and geospatial intelligence (GEOINT). Technical collection methods are the best way to gather enormous quantities of information on enemy capabilities and fixed terrorism targets (Steiner, 2015). Fundamentally, the deployment of intelligence collection disciplines is driven by the nature of and our access to the target. As such, intelligence products can either be based on a single type of collection (single-source) or based on all available types of collection (all-source) ("What is intelligence?," n.d.).

From the customer's perspective, intelligence products can be categorized into three levels that correspond with either short-term or long-term goals: (1) tactical intelligence, (2) operational intelligence, and (3) strategic intelligence (Steiner, 2015). Tactical intelligence refers to intelligence used for planning or directing individual operations in the short-term. This form of intelligence enables tactical units to achieve a positional advantage over their adversaries (Clark, 2017). Law enforcement agencies consider tactical intelligence to mean any information that directly leads to an arrest or builds a case against a subject. Tactical intelligence involves specific details like dates, times, locations, weapons, and methods that facilitate immediate utility (Ganor, 2005). Operational intelligence refers to intelligence that may be relevant in pursuit of long-term goals like arrests or prosecutions. This form of intelligence focuses on the capabilities and intentions of adversaries and is required for the planning and execution of specific operations (Clark, 2017). The key distinction is that operational intelligence has no immediate utility. Strategic intelligence is highly sought after by policymakers who make decisions concerning long-term national and international issues. Strategic intelligence can be thought of as the intelligence in support of a broader strategy, including the identities of high-value subjects, motives, hierarchies, ideologies, and methods (Ganor, 2005).

III. What Does Information-Sharing Mean?

Information-sharing within and across organizations improves organizational performance and efficiency (Lesser and Storck, 2001), promotes competitive advantage (Argote and Ingram, 2000; Grant, 1996; Kogut and Zander, 1992; Nonaka and Takeguchi, 1995), fosters organizational learning (Argote, 1999), and stimulates innovation (Powell et al., 1996). As such, the concept has received considerable attention from researchers and practitioners alike. Recent scholarly work endeavors to identify specific factors that promote effective information-sharing in organizational settings. However, factors influencing inter- and intra-organizational information-sharing efforts are more complex and interrelated when multiple entities or government agencies are involved (Yang and Maxwell, 2011). As such, the information-sharing literature is limited in that it does not consider the interplay between factor relationships in a sufficiently inclusive theoretical framework.

In asking the fundamental question, *What does information-sharing mean?*, it is beneficial to integrate the predominant theoretical lenses from a variety of academic disciplines to significantly improve information-sharing explanatory power. Compared to a single-theory framework, a multi-theory framework can provide more comprehensive insights into intra- and inter-organizational information-sharing because it is better suited to perceive multi-faceted influential factors (Yang and Maxwell, 2011). Since information-sharing behaviors are influenced not only by personal motivations but also by contextual forces (Yoo and Torrey, 2002), the study of information-sharing should be envisioned as an integration of disciplines, including organizational behavior and theory, information systems, psychology, sociology, economics, and strategy. In the following paragraphs, the predominant theories underpinning the diverse array of information-sharing literature are presented to support an integrated theoretical analysis of homeland security information-sharing in chapters 2 and 3.

a. Theory of Reasoned Action

The theory of reasoned action was introduced by Fishbein and Ajzen (1975) as an improvement over information integration theory. The theory of reasoned action assumes that individuals are rational and will make systematic use of the information available to them (Fishbein and Ajzen, 1975; Bock and Kim, 2001). The theory is widely accepted in social psychology to explain human behavior and can be a useful model to explain information-sharing behaviors in organizations (Davis et al., 1989). Critically, the theory of reasoned action assumes that information-sharing behavior occurs at the individual level (Bock and Kim, 2001). Additionally, it suggests that performance of a behavior can be predicted by three elements: (1) attitude toward the behavior, (2) subjective norms, and (3) behavioral intention (Fishbein and Ajzen 1975; Jolaee, 2014). The literature proposes that subjective norms are likely to affect behavioral intentions both directly and indirectly through attitude (Bock et al., 2005; Kim and Lee, 1995; Koys and Decotiis, 1991; Kurland, 1995; Mathieson, 1991; Thompson et al., 1991).

The theory of reasoned action is an important lens that contributes to our collective understanding of why knowledge workers engage or choose not to engage in information-sharing behaviors. This is key because the literature suggests that information-sharing is unnatural, and that hoarding information and looking suspiciously upon information from others is a natural human tendency (Davenport, 1996; Bock and Kim, 2001). Importantly, numerous studies suggest that the degree of an individual’s positive feelings about information-sharing significantly impacts their intent to share information (Kuo and Young, 2008; Kolekofski and Heminger, 2003; Bock et al., 2005; Pavlou and Fygenson, 2006). Taken a step further, the significant positive relationship between attitude and information-sharing intention means that individuals share information when they have positive attitudes about information-sharing (Jolaee, 2014; Bock and Kim, 2001).

b. Transaction Cost Economics

Transaction cost economics considers the factors that govern economic transactions (Williamson, 1985). Inherent in this theoretical framework is the assumption that individuals are opportunistic and will choose to share information when such an approach can reduce uncertainty and when transaction costs are low (Tan et al., 2010). The variables of uncertainty and transaction costs are important to a broader understanding of what may motivate individuals to share information. On the other hand, transaction cost economics can also explain why partners would be motivated to withhold information. As such, information-sharing is most likely to occur when individuals perceive that incentives exceed costs (Kelley and Thibaut, 1978).

Even when information-sharing is framed in the context of contributing to a collective good, the decision is ultimately a calculation of the perceived costs and benefits (Jian and Jeffres, 2006; Marks et al., 2008). Assuming that individuals are rational and self-interested, they will seek to maximize individual benefits and minimize individual costs (Jian and Jeffres, 2006; Draaijer, 2008). Given the value of information as an asset or capital, partners may use the advantage strategically to control the behaviors of their partners (Kim et al., 2006). Uncertainty and transaction costs maintain information asymmetry and limit opportunities for partners to exploit the exchange relationship and act opportunistically (Klein et al., 2007; Yigitbasioglu, 2010). The transaction cost economics literature suggests that formal structures, like contracts and government institutions, reduce the possibility of opportunism by limiting uncertainty in transactions (Tan et al., 2010; Porterfield et al., 2010; Grover and Saeed, 2007). In addition to equitable compensation, formal structures could integrate incentives or penalties to institutionalize the importance of information sharing (Grover and Saeed, 2007; Porterfield et al., 2010).

c. Relational Governance Theories, Including Social Exchange Theory and Economic Exchange Theory

Relational governance theories conceptualize information-sharing as a necessarily reciprocal activity that serves, primarily, to improve transactional relationships (Nyaga et al., 2010). Such relationships create a framework for enhanced inter-organizational cooperation, which could eventually lead to increased organizational efficiencies (Wei et al., 2012). Recent studies suggest that information-sharing between organizations is heavily influenced by good inter-organizational relationships based on core features like trust, commitment and shared vision (Li and Lin, 2006). The core supposition of relational governance theory is that partners are operating in an environment of trust where the benefits of information-sharing unquestionably outweigh the benefits of opportunism (Kim et al., 2006). The environment of trust, demonstrated through mutual reliance or interdependency, is reinforced by informal structures, such as social controls (Patnayakuni et al., 2006). Relational governance theories assign considerable, and arguably disproportionate, emphasis to the benefits of mutual reliance with the expectation of mutual gains (Nyaga et al., 2010).

Because information-sharing can be understood as a distinct type of social interaction among individuals, it is important to consider theories that explain the social interaction of people, such as social exchange theory and economic exchange theory. Organization theorists and behavioralists have challenged the assumptions underlying economic theories like transaction cost economics as being too narrowly focused on opportunism. (Jones, 1983; Perrow, 1981). Conversely, according to the economic exchange theory, individuals will behave by rational self-interest. Thus, information-sharing will occur when expected rewards exceed perceived costs (Bock and Kim, 2001; Kelley and Thibaut, 1978; Constant, et al., 1994). Additionally, researchers argue that social exchange theory may be a more useful theoretical lens for the examination of inter- and intra-organizational alliances (Graham, 1988). Specifically, several researchers found that social networks help to generate positive attitudes about the sharing of information and knowledge within an organization. (Kim and Lee, 2006; Kolekofski and Heminger, 2003; Reagans and McEvily, 2003). Some social exchange theorists suggest that transaction cost economics could be supplemented by social context to provide a more comprehensive analysis of organizational relationships (Cook and Emerson, 1978).

Constant et al. (1994) suggest that social exchange and economic exchange theories are similar in that they both consider reciprocity to be an important motivational factor in promoting information-sharing behaviors within organizations. Furthermore, rational economic transactions, such as information-sharing, are embedded in social relations that generate trust and discourage opportunism (Granovetter, 1985). Like economic theories, social exchange theory predicts that information-sharing behaviors adhere to a cost-benefit framework. Both theories could be useful if exercised in tandem because social exchange theory also investigates intangible costs and intangible benefits (Hung and Chuang, 2009). However, an important distinction is that economic exchange theory primarily concerns extrinsic benefits, such as monetary rewards or promotions, while social exchange theory primarily concerns intrinsic benefits, such as feelings of gratitude or trust (Blau, 1964; Bock and Kim, 2001).

d. Social Capital Theory

Social capital theory, like social exchange theory, is often used to explain information-sharing behavior within and across organizations. The term ‘social capital’ refers to the resources embedded within, available through, and derived from networks of individuals, communities, networks, or societies (Nahapiet and Ghoshal, 1998; Chang and Chuang, 2011). In the context of information-sharing, social capital theory suggests that social capital is a necessary condition for the exchange of information (Hung and Chuang, 2009; Kankanhalli et al., 2005). Nahapiet and Ghoshal (1998), examine social capital through three categories: the structural, relational, and cognitive dimensions of social capital. The structural dimension describes the configuration of linkages between people or units and focuses on the broader patterns of relationships found within organizations (Mäkelä, 2007; Chang and Chuang, 2011). The relational dimension denotes the nature of the linkages between people or units and includes elements such as trust, norms, identity, obligations, and expectations (Mäkelä, 2007; Chang and Chuang, 2011). The cognitive dimension is characterized by shared paradigms, codes, languages, and systems of meaning that facilitate a common understanding or perspective within a social network (Tsai and Ghoshal, 1998; Mäkelä, 2007; Chang and Chuang, 2011).

While social exchange theory can be used to identify cost and benefit factors affecting the information-sharing framework, social capital theory can supplement the examination to account for the moderating influence of contextual social capital factors (Kankanhalli et al., 2005; Constant et al., 1994). Specifically, contextual social capital factors like trust, norms, and identification impact the conditions for information-sharing (Cohen and Prusak 2001; Nahapiet and Ghoshal, 1998) and can either strengthen or weaken the effects of cost and benefit factors on information-sharing behavior (Kankanhalli et al., 2005). A pivotal study by Chow and Chan (2008) empirically analyzes the influence of social capital on organizational information-sharing. They found that higher levels of social networks and shared goals directly influence attitudes and subjective norms about information-sharing, and indirectly influence intentions to share information (Chow and Chan, 2008).

e. Contingency Theory

Contingency theory suggests that the structures and processes that facilitate information-sharing are influenced by internal and external environments. Thus, organizational design should mirror the environment in which it operates (Woodward, 1965; Lawrence and Lorsch, 1967; Thompson, 1967; Galbraith, 1974; Persson, 1978, 1995; Donaldson, 2001; Butterman et al., 2008; Flynn et al., 2010). Although information-sharing yields numerous organizational benefits, it can concurrently increase transaction risk and uncertainty, as higher degrees of transparency can inadvertently invite opportunistic behavior (Yigitbasioglu, 2010). Contingency theory states that such uncertainty can detract from an organization’s incentive to share information, and that the amount of uncertainty and rate of change in an environment impact the development of internal organizational structures and mechanisms (Lawrence and Lorsch, 1967; Yigitbasioglu, 2010). The underlying assumption in contingency theory is that organizations perform better when they share information in favorable environments compared to when they share information in unfavorable environments (Wong et al., 2012).

One of the distinct benefits of this theory is that it prescribes an adaptive approach to information-sharing, rather than a one-size-fits-all approach (Stock et al., 2000; Grover and Saeed, 2007; Caridi et al., 2010). In effect, there is no universal or optimal way to structure an organization or to make decisions because organizational effectiveness is contingent on the influence of internal and external variables like technology, culture, and the environment (Bastian and Andreas, 2012). Critics of contingency theory point out that internal and external variables are constantly evolving, and that an organization only remains in fit temporarily until contingency variables lead the organization into misfit once again. Though the theory claims that organizations in fit experience higher performance than those in misfit, critics argue that the contingency variables themselves change so that the organizational structural change does not effectively produce fit (Donaldson, 2001, 2006; Abba et al., 2018).

f. Resource Dependence Theory

Like contingency theory, resource dependence theory recognizes the influence of external factors on organizational behaviors (Hillman et al., 2009). Resource dependence theory acknowledges that organizations are dependent on the external environment for sustained access to resources and therefore act to reduce environmental uncertainty (Pfeffer and Salancik, 1978). The theory also suggests that organizations will seek to diversify access to resources to maintain their autonomy and decrease their dependency on external factors (Donaldson, 2001). However, organizations cannot be truly autonomous because they are constrained by a network of interdependencies with other organizations (Pfeffer, 1987). As such, organizational attempts to manage external interdependencies are never completely successful and inevitably produce new patterns of external dependence and interdependence (Hillman et al., 2009; Pfeffer, 1987).

A critical element of organizational efforts to manage external dependencies and resource uncertainties is the concept of power, which refers to control over vital resources (Ulrich and Barney, 1984). Resource dependence theory posits that organizations will often attempt to assert control over resources to both reduce others' power and increase their own power over others (Hillman et al., 2009). In the context of information-sharing, the degree to which organizations are dependent on their partners for resources may explain such organization's willingness to share information. (Patnayakuni et al., 2006). As such, the intensity of information-sharing practices between organizations should reflect the level of dependency asymmetry. (Vijayasarathy, 2010; Yigitbasioglu, 2010). Dependency asymmetry may exacerbate power imbalances between partners and introduce an avenue for opportunism at the detriment of the exchange relationship (Yigitbasioglu, 2010).

g. Resource-Based View, Including Knowledge-Based View

The resource-based theoretical lens considers how an organization's distinctive competencies can be important sources of heterogeneity that uniquely contribute to the organization's competitive advantage (Mahoney and Pandian, 1992; Ramanujam and Varadarajan, 1989). The resource-based view assigns considerable importance to an organization's resources, which can be defined as anything thought of as a strength or weakness of a given organization (Wernerfelt, 1984). In the context of information-sharing, information is an organization's most valuable resource and can be used to generate increased rents (Peteraf, 1993). The generation of rents is the focal point of analysis for determining an organization's competitive advantage (Porter and Millar, 1985). Notably, the resource-based view prioritizes the ownership of inimitable resources, like information, to maintain a competitive advantage and underplays opportunities for rent generation through collaborative endeavors (Peteraf, 1993).

An increasing interest in knowledge as a strategic resource led scholars to develop the knowledge-based version of the resource-based view. According to the knowledge-based view of an organization (Grant, 1996; Spender, 1996), knowledge enhances the coordinative and integrative capabilities of organizations and is the cornerstone of an organization's competitive advantage. As such, knowledge is a focal point of analysis in determining an organization's value. The knowledge-based theory emphasizes the content of organizational activities, such as information-sharing, as an important indicator of performance (Argote et al., 2003). Additionally, the theory suggests that organizations are social communities that specialize in the creation, development, and exchange of information (Kogut and Zander, 1996; Reagans and McEvily, 2003). However, the issue of information ownership is again problematic as knowledge is created, organized, and amassed by knowledge workers who apply knowledge to carry out their responsibilities (Nonaka and Konno, 1998; Bock et al., 2005).

Critics of the resource-based theoretical lens argue that an emphasis on insularity and resource protection neglects to consider the impact of integration with external resources to improve internal routines and processes (Barney et al., 2011). While traditional perspectives of the resource based-view envision organizations as independent, autonomous organizations (Barney, 1991; Dierickx and Cool, 1989; Wernerfelt, 1984), more recent literature examines the competitive advantages of organizations participating in networked environments (Lavie, 2006; Kogut, 2000). Lavie's (2006) extension of Barney's (1991) framework of resource-based competitive advantage is instructive because he introduces social network theories to analyze the impact of network structure on organizational performance. Lavie's (2006) research suggests that organizations can extract value from resources that are not owned or controlled through participation in a social network.

The numerous aforementioned theories and literatures address factors and conditions that impact information-sharing within and across organizations. It is worthwhile to note that these factors and conditions are often divergent, complementary, or overlapping, and that they each provide a nuanced explanation of an admittedly complicated process. The assessments of homeland security information-sharing in chapters 2 and 3 will synthesize prior research across academic disciplines to examine how contextual factors and underlying motivational forces affect information-sharing.

This will provide a more comprehensive and diverse framework to evaluate information-sharing efficacy in the homeland security context.

IV. How Does Information-Sharing Happen?

Technological advances have significantly enhanced the capacity to share information within and across organizations. Information can be transferred from the possessor to the recipient through a variety of mechanisms, including by telephone, fax, email, web-enabled portals, and face-to-face contact, among many others (Kembro et al., 2014). A significant amount of research has been dedicated to the challenges associated with integrating heterogeneous information systems with inconsistent data structures (Atabakhsh et al., 2004; Chen et al., 2007; Dawes, 1996; Gil-Garcia et al., 2007; Klischewski and Scholl, 2008; Lam, 2005; Pardo et al., 2004; Zhang and Dawes, 2006). While technological capabilities can pose significant challenges to information-sharing within and across organizations (Fedorowicz et al., 2007; Lam, 2005), researchers claim that such challenges pale in comparison to challenges in organizational structure and policy (Atabakhsh et al., 2004; Brazelton and Gorry, 2003; Landsbergen and Wolken, 2001). Moreover, technology interoperability in the information-sharing context presents a research topic of its own and is out of the scope of this paper.

The literature presents the information-sharing process through three perspectives: (1) interpersonal, (2) intra-organizational, and (3) inter-organizational (Yang and Maxwell, 2011). Each perspective contributes to a broader discussion about personal motivations and contextual forces (Yoo and Torrey, 2002) that ultimately influence how and why organizations share information. These perspectives provide a necessary foundation for discussions in chapters 2 and 3 about how homeland security information is shared between component agencies of the Department of Homeland Security and among other relevant government agencies.

When evaluating information-sharing in public organizations, it is important to consider how the three perspectives of information-sharing are both interrelated and, at times, interdependent. Interpersonal relationships are social associations among individuals, and research at the interpersonal level focuses on individual behaviors such as motivations of, approaches to, and channels for, an individual to share information with others (Yang and Maxwell, 2011). In a seminal study, Bock et al. (2005) suggest that interpersonal relationships, characterized as mutual social exchange relationships, are important in driving information-sharing intentions and behaviors. The correlation also has value in reverse: information-sharing behavior is employed as an approach to strengthen social associations between information givers and receivers (Marshall and Bly, 2004; Yang and Maxwell, 2011). The knowledge management literature depicts this relationship as a cycle in which trust and information-sharing are both an antecedent and a consequence of each other (Piderit et al., 2011). Strong interpersonal relationships are a necessary element of social exchange theory and economic exchange theory, which both consider reciprocity to be an important motivational factor in promoting information-sharing behaviors within and across organizations.

However, interpersonal information-sharing behaviors become more complicated when they are embedded within the contexts of intra- and inter-organization information-sharing. Information-sharing between two individuals acting alone is fundamentally different than information-sharing between two individuals who are influenced by their social and organizational context (Constant et al., 1994). Individual attitudes and predilections may interface with organizational factors, such as competition and collaboration, which can either encumber or promote intra- and inter-organizational information-sharing. This provides critical insight for research into larger, bureaucratic information-sharing frameworks. Information-sharing among and between agencies within a single, centralized organization can ultimately become entrenched in an even broader inter-organizational framework. (Dawes, 1996; Gil-Garcia et al., 2007, 2009; Klischewski and Scholl, 2006; Pardo and Tayi, 2007; Zhang and Dawes, 2006). This is especially pertinent for research about homeland security information-sharing, which, by the nature of its gravity, must occur in a timely, precise, and generous manner.

This is challenging for research into intra- and inter-organizational information sharing because all three perspectives must be considered both individually and collectively. The consideration should ideally include factors that are unique to each perspective and an examination of how those unique factors interface within the comprehensive information-sharing environment. As the network of participating organizations grows, the factors influencing inter-organizational information-sharing become more diversified and complex (Gil-Garcia et al., 2005). Unlike information-sharing within a single organizational unit, cross-boundary information-sharing efforts are far more complicated and multifaceted due to the diversity of missions and interests involved. This becomes problematic when individuals and organizations have conflicting or divergent motivations (Klischewski and Scholl, 2008).

V. How is Information-Sharing Measured?

Although information-sharing has attracted considerable attention from researchers and is widely accepted as an approach to improve organizational performance, there is a remarkable absence of research dedicated to measuring the effectiveness of information-sharing efforts. Furthermore, debates about the value and efficacy of information-sharing efforts are stunted without clear data to inform empirical assessments. This is especially pertinent to the sharing of tacit information, which may not be readily observable or trackable (Yi, 2009). Objective and defensible approaches to measure the impacts of information-sharing efforts would allow for future comparisons of the costs associated with supporting such efforts (Jackson, 2014).

The economics literature provides a theoretical foundation for efforts to quantify and measure information-sharing. Researchers have examined how the value of information can be evaluated in the context of business decisions. This approach is convenient because performance outcomes in the private sector are primarily concerned with monetary profit, which is easily quantifiable. Information-sharing measurement techniques involve efforts to quantify how decision quality improves with access to additional information (McCarthy, 1956; Feltham, 1968). Additionally, ‘options thinking’ describes how access to more information changes the relative attractiveness of different choices that could be made, as well as the entire decision space within which choices are made (Conrad, 1980; Felli and Hazen, 1997). Outcome measures in business focus on how information affects decision quality, and how decision quality in turn impacts monetary profits (Jackson, 2014).

Fundamentally, evaluation efforts measure the degree to which a desired outcome was achieved. At the core of this premise is the existence of a ‘desired outcome’ that can be clearly articulated. In the context of information-sharing, ‘desired outcomes’ are difficult to quantify for a variety of reasons (Jackson, 2014). The success of information-sharing endeavors cannot be measured simply by the successful transmission of information across organizational boundaries; it is also important to assess whether the information is absorbed and utilized effectively within the organization that acquired it (Jackson, 2014; Yang and Maxwell, 2011). Furthermore, the sharing of different forms of information involves different social costs and benefits, and evaluation efforts should ideally consider employees’ perspectives on information-sharing (Constant et al., 1994). Outcome-centric evaluation measures place a disproportionate emphasis on the products of information-sharing and largely ignore the processes that yielded the successful transfer (Yi, 2009; Huysman and de Wit, 2002).

Despite this significant challenge, researchers have developed systematic ways of assessing the effects of information-sharing programs and processes to determine such programs’ and processes’ relative value. Jackson (2014) categorizes these methods according to their assessments of four key effects: (1) the process, referring to whether a program or process is established or functioning effectively, (2) output, referring to what products or services the program or process is intended to produce, (3) outcomes, referring to how such products or services affect the organization’s desired outcome, and (4) efficiency, referring to whether the costs of the aforementioned products or services are higher than those of alternative mechanisms to produce the same outcome. The flexibility of this methodology allows for its application in a variety of information-sharing environments.

VI. Conclusion

Information-sharing involves more than the simple transmission of information from one entity to another. Rather, it is a process of exchanging and processing information in a way that enables the knowledge of one entity to be integrated into another. Information-sharing is multi-dimensional, and its complexity demands an equally multifaceted examination from multiple theoretical perspectives. This chapter presented the predominant theoretical lenses that researchers have used to explain how individuals and organizations share information. This structured effort demonstrates how the study of information-sharing should be envisioned as an integration of disciplines, including organizational behavior and theory, information systems, psychology, sociology, economics, and strategy. Chapter 1 addressed fundamental questions that underpin information-sharing activities, including: *What is information? What does information-sharing mean? How does information-sharing happen? How is information-sharing measured?* Chapter 2 builds upon this foundation to assess how bureaucracy contributes to, and at times exacerbates, the myriad factors that inhibit information-sharing efforts among Department of Homeland Security component agencies.

CHAPTER 2: Bureaucracy and Homeland Security

I. Introduction

In response to the terror attacks on September 11, 2001, Congress passed the Homeland Security Act of 2002 and formally authorized the establishment of the Department of Homeland Security (DHS). In his proposal to create the Department of Homeland Security, President George W. Bush articulated that "America needs a single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future" (Bush, 2002). President Bush proposed to integrate twenty-two federal agencies with a diverse array of missions into a single department to rectify the federal government's uncoordinated and inadequate response to the September 11 attacks and protect the nation against emerging terrorist threats. However, while the centralization of homeland security activities under one bureaucratic umbrella presumably offers enhanced coordination, reduced redundancies, and increased output, larger bureaucratic structures are not necessarily apt to govern the unique interests and organizational cultures of each component.

Thus, it is reasonable to question the degree to which the creation of the Department of Homeland Security resolved the information-sharing challenges that ultimately resulted in the events of September 11, 2001. *This chapter will examine how bureaucracy contributes to, and at times exacerbates, the myriad factors that inhibit information-sharing efforts among Department of Homeland Security component agencies.* First, this chapter evaluates how the Department of Homeland Security's centralized bureaucratic structure supports the Department's primary mission and departmental objectives with regard to information-sharing. Then, the discussion shifts to address how persistent barriers to effective information-sharing are compounded by a bureaucratic model that institutionalizes interagency competition. Applied and understood in tandem, these factors highlight the enduring difficulty of harmonizing the twenty-two disparate agencies that comprise the Department of Homeland Security and give credence to the notion that centralization fosters a culture of competition rather than collaboration. The historical evolution of the Department of Homeland Security since 2002 has not effectively produced a single, unified homeland security structure that accomplishes the original goals of the agency, which, as articulated in the Department's authorizing legislation, call for information-sharing and coordination among the 22 government agencies with a stake in the homeland security mission. The barriers to effective information-sharing, including lack of information interoperability, incongruity of classification standards, overlapping agency jurisdictions and missions, and overreliance on outcome-centric metrics to qualify achievement have proved more powerful than the rhetorical dedication to common mission and purpose.

II. Background

The mission of the Department of Homeland Security is to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016). DHS expounds its mission by defining five departmental objectives: (1) prevent terrorism and enhance security, (2) secure and manage our borders, (3) enforce and administer our immigration laws, (4) safeguard and secure cyberspace, and (5) ensure resilience to disasters ("Our Mission," 2016). The diversity of these objectives is a testament to the diversity of threats facing the homeland, the wide-ranging nature of the homeland security enterprise, as well as the variation of missions among component agencies. Importantly, when agencies were transferred to the nascent Department of Homeland Security, they retained their legacy mandates and absorbed new homeland security statutory responsibilities. Thus, the new bureaucratic structure forced these agencies to reorient their limited resources to accommodate for both sets of mandates and reconcile conflicting organizational goals (Cohen et al., 2006). In this sense, centralization resulted in twenty-two unique agencies with split loyalties between legacy missions and new homeland security responsibilities. Today, these split loyalties reinforce cultural differences and competing interests among component agencies.

The bureaucracy literature contends that as a bureaucratic organization expands both vertically and horizontally, the formal, hierarchical structure of bureaucracy can create barriers that impede information-sharing efforts (Creed et al., 1996; Tsai, 2002; Argote et al., 2000; Willem and Buelens, 2007; Yang and Maxwell, 2011). The multiplicity of external forces that exert control over the activities and priorities of DHS component agencies results in a complex network of governance (Fountain, 2013). Competing or contradictory demands from authority figures such as component chiefs, the DHS Cabinet Secretary, Congressional policymakers, and the President of the United States may frustrate DHS component agencies' abilities to faithfully carry out policy and operations. It is worth noting that the different components of DHS report to a plethora of different congressional authorities. More than 100 congressional committees, subcommittees, and caucuses conduct oversight of the Department of Homeland Security, and each entity can have contradictory expectations and priorities for the Department. This convoluted network of governance creates forces, such as competition and differing organizational cultures, which impede information-sharing across component agencies. In addition to competing interests and goals, component agencies can also have different authority figures, which may detract from collaboration, mutual aid arrangements, and resource sharing (Caudle, 2005). The Department of Homeland Security is particularly vulnerable to contradictory organizational objectives due to the sheer diversity of component objectives, which range from short-term emergency response to long-term intelligence gathering. Despite these contradictory priorities, the gravity of the overarching homeland security mission demands seamless information-sharing activities between component agencies.

Compared to other Cabinet-level Departments, the Department of Homeland Security is unique because its components balance the interdependent cultures of law enforcement, domestic intelligence, emergency preparedness, and emergency response to facilitate a robust homeland security enterprise. As such, information-sharing among and within DHS components can involve communications, notifications, and alerts before, during, and after an emergency (Jackson, 2014). The scope of this paper focuses on information-sharing before an emergency, or “left of boom,” which is a military idiom that refers to efforts to disrupt and dismantle militant networks before such networks can manufacture and plant bombs. The term “left of boom” was popularized by Doug Laux, a former case officer for the Central Intelligence Agency (CIA), who used it in his memoir to describe the intelligence activities that precede and ideally prevent terrorist plots (Laux and Pezzullo, 2016). In the context of homeland security information-sharing, activities left of boom are generally carried out by DHS components whose organizational missions require intelligence and/or law enforcement activities, such as U.S. Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and the U.S. Secret Service (USSS) (Jackson et al., 2009). Additionally, the DHS Office of Intelligence and Analysis (I&A) is responsible for the timely dissemination of information among DHS components and other public and private partners to keep the homeland safe, secure, and resilient ("Office of Intelligence and Analysis," 2018).

Former Federal Bureau of Investigation (FBI) Director Robert Mueller articulates the importance of the symbiosis of intelligence collection and law enforcement activities in the homeland security effort: "Splitting the law enforcement and the intelligence functions would lead both agencies fighting the war on terrorism with one hand tied behind their backs. The distinct advantage we gain by having intelligence and law enforcement together would be lost in more layers and greater stovepiping of information, not to mention the difficulty of transitioning safely to a new entity while terrorists seek to do us harm" ("Law Enforcement and the Intelligence Community," 2004). Law enforcement operations, such as the USSS' efforts to combat money laundering and ICE's investigations into antiquities theft, increasingly involve domestic intelligence activities. The evolution of traditional law enforcement operations to what is colloquially referred to as 'intelligence-led policing' indicates that domestic intelligence is a burgeoning asset in the homeland security enterprise (Jackson et al., 2009).

Several DHS components, including the Federal Emergency Management Agency (FEMA), CBP, TSA, USCIS, ICE, and the USSS comprise the "domestic IC" (Marks, 2010, p. 124). Members of the domestic Intelligence Community (IC) collect tactical intelligence for consumption within their respective agencies. Government agencies responsible for law enforcement, border protection, intelligence, and military functions contribute to the domestic IC through the prevention and mitigation of threats (Howitt and Pangi, 2003; Falkenrath, 2001; Caudle, 2005). In effect, each agency is responsible for a certain domain of the homeland security enterprise and has the appropriate resources to collect information within that domain (Jackson et al., 2009). However, the proliferation of intelligence activities in different domains of the domestic IC has generated uncertainty about the roles and responsibilities of each agency within the broader homeland security effort, as well as concerns about data quality. DHS's comprehensive intelligence capabilities and sizeable law enforcement workforce support an intelligence-driven approach to homeland security operations, but such a diverse network of autonomous components makes the creation of uniform standards and common practices to facilitate the sharing of high-quality information very difficult (Jackson et al., 2009).

Though the creation of the Department of Homeland Security was intended to resolve the intelligence failures associated with September 11, many scholars question whether the massive centralization of twenty-two disparate agencies under one, unified homeland security bureaucracy achieved this goal. Centralization certainly offers certain benefits that help to streamline information-sharing activities, but Peled (2014) argues that government agencies must be coerced to share information because bureaucracies are explicitly designed to counteract inter-organizational information-sharing. He maintains that the institutional features of the U.S. federal government, such as regulations, oversight mechanisms, and organizational cultures, are intended to frustrate integration and prevent organizations from becoming too powerful (Peled, 2014). Moreover, information flows are strictly regulated in the bureaucratic model, which further restricts opportunities for integration (Wheatley, 2006; Yang and Maxwell, 2011). On the other hand, some scholars consider centralization to be beneficial for improving coordination, reducing redundancies, and increasing efficiencies (Cohen et al., 2006).

Despite the theoretical benefits of a centralized Department of Homeland Security, centralization imposes large transaction costs on component agencies as they merge and modify their respective activities (Cohen et al., 2006). These costs can inadvertently foster competition between components operating in similar or overlapping regulatory environments. Bureaucratic rivalries within a larger organization are counterproductive when one entity seeks to promote itself over others, and individual bureaucrats who lose power and authority are less likely to adopt new goals and interests associated with the reorganization (Cohen et al., 2006). The literature acknowledges that government officials are selfish actors who primarily seek to increase their agency's reputation and autonomy (Kraemer and King, 1986; Ardichvill et al., 2003; Constant et al., 1994; Jarvenpaa and Staples, 2001; Jian and Jeffres, 2006; Kolekofski and Heminger, 2003; Marks et al., 2008; Yang and Maxwell, 2011; Peled, 2014).

III. Barriers to Effective Information-Sharing

In spite of the Department of Homeland Security's centralized organizational structure, several persistent barriers impede effective information-sharing between component agencies. These barriers can be organized into five key categories: (1) Lack of information technology interoperability, (2) Incongruity of classification standards, (3) Overlapping agency jurisdictions and missions, (4) Overreliance on outcome-centric metrics to quantify achievement, and (5) Correlation between perceived agency performance and annual budget appropriations. The following paragraphs illustrate how these categories of factors are intimately related to the Department's organizational design and give credence to the notion that centralization fosters a culture of competition rather than collaboration.

a. Lack of Information Technology Interoperability

Electronic data systems are not integrated between DHS component agencies. Because DHS components have unique missions, their information technology (IT) systems have adapted to cater to the specific needs of analysts and personnel in the field. As such, the evolution of systems and databases may be helpful for individual components, but may be incompatible with the data systems of other agencies. The bureaucracy literature suggests that agency leaders invest in data integration only if it furthers their own agency's interests (Krause and Douglas, 2005; Schneider and Ingram, 1990; Peled, 2014). For example, TSA maintains the No-Fly List and Selectee List, two databases that accumulate passenger data and restrict access to commercial air travel (Jackson et al, 2009). The information in these databases can be helpful for a number of other component agencies whose missions involve protecting the border in some capacity, including the USCG, CBP, ICE, and USCIS. Unfortunately, department-wide IT interoperability is unrealistic because datasets are often duplicated, fragmented, or simply inaccessible to individuals outside of the organization (Peled, 2014).

The Office of Inspector General recently audited DHS's data strategy and found that as of April 2017, DHS was in the process of implementing only four of 23 strategic objectives in its Enterprise Data Strategy ("Improvements Needed to Promote DHS Progress toward Accomplishing Enterprise-Wide Data Goals," 2017). Enterprise data is data created, managed, or maintained within DHS that is common to, or shared among, multiple DHS entities. ("Directive Number 103-01: Enterprise Data Management Policy," 2014). The report highlights DHS's inadequate progress in executing policies that would otherwise improve agency data quality, enable digital information-sharing across components, secure data platforms, and build a data workforce. While technological capabilities can pose significant challenges to information-sharing efforts within and across organizations (Fedorowicz et al., 2007; Lam, 2005), researchers claim that such challenges pale in comparison to challenges in organizational structure and policy (Atabakhsh et al., 2004; Brazelton and Gorry, 2003; Landsbergen and Wolken, 2001).

Additionally, synchronized IT systems inundate DHS analysts with too much information. In an attempt to facilitate database interoperability, DHS implemented a number of IT systems to simplify information-sharing among components and federal, state, local, and tribal partners. The Homeland Security Information Network (HSIN) is a Web-based information portal for sensitive but unclassified information. The Homeland Secure Data Network (HSDN) is similar to HSIN but transmits classified information (Jackson et al., 2009). In theory, HSIN and HSDN provide appropriate DHS personnel with critical homeland security information, but in practice, the systems conflate helpful intelligence and irrelevant intelligence in an overwhelming amount of data. Enhancing information-sharing has traditionally translated to increasing the volume of information moving through a system, but little thought has been given to the quality of the information (Jackson et al., 2009). Although false-positives and other data quality issues can arise in smaller organizations, the diversity inherent in a larger network with disparate authorities and responsibilities could produce significant complications (Jackson et al., 2009). If end users are unable to effectively identify and utilize actionable intelligence, it undermines the original intent of the synchronized IT systems.

b. Incongruity of Classification Standards

Classification methodologies vary across departments and agencies. The literature suggests that inter-organizational information-sharing can be encumbered by policies that prevent government agencies from sharing certain public safety and/or national security information (Dawes, 1996; Gil-Garcia et al., 2007; Gil-Garcia and Pardo, 2005; Yang and Maxwell, 2011). As national security threats evolve, it is imperative that coordination between DHS component agencies, law enforcement personnel, first responders, and key stakeholders is rapid and reliable. Many government agencies classify information according to different standards, and the lack of continuity renders effective information-sharing very difficult, if not impossible. In many instances, law enforcement personnel and first responders who could make the most use of timely intelligence do not have access to it. The means do exist whereby knowledge can be shared without needlessly endangering sources or methods, but these systems must be refined to work more efficiently (Cilluffo, 2002).

Additionally, the process of obtaining a security clearance is tedious, lengthy, and expensive, which further limits the scope of audiences eligible to consume classified intelligence. According to the Office of the Director of National Intelligence (ODNI), the total number of initial security clearance case investigations pending for more than four months increased from 2,526 in Fiscal Year (FY) 2015 to 3,707 in FY 2016. Furthermore, in FY 2016, 2,361 security clearance determinations for U.S. government employees took longer than one full year to complete ("Fiscal Year 2016 Annual Report on Security Clearance Determinations," 2016). This is frustrating for government employees who cannot perform their job functions without a clearance, as well as the tens of thousands of state, local, and tribal first responders who neither need nor want a clearance (Marks, 2010). Variations in classification methodology coupled with the arduous security clearance process inhibit the seamless, dynamic flow of information across the homeland security enterprise.

Furthermore, the over-classification of material prohibits seamless collaboration, even among personnel in varying positions of trust. It is logical and necessary to limit the dissemination of certain information that may jeopardize U.S. national security interests. While an overabundance of caution seems appropriate, it often has an adverse effect on the coordination of homeland security efforts. In theory, classification decisions are guided by established standards, but in practice, the classification system is sometimes used inappropriately and even promiscuously, classifying material too highly or, in some cases, classifying material that does not deserve to be classified (Lowenthal, 2006). The practice of designating unclassified information as security-sensitive is problematic because there is no standardized definition of security-sensitive, no uniform understanding about how to control the classification, no consensus about its implications for U.S. national security, and no avenues for redress or adjudication (Carafano and Heyman, 2004).

The instinct to classify material imprisons valuable information within exclusive, compartmentalized communities. In FY 2016, 366,948 security clearances were approved at the Confidential or Secret level and 227,946 were approved at the Top Secret level. These figures represent a 6.9% reduction in the number of security clearances approved between FY 2016 and FY 2015 ("Fiscal Year 2016 Annual Report on Security Clearance Determinations," 2016). To put these figures in perspective, the Department of Homeland Security alone employed around 240,000 individuals in FY 2015 ("Budget in Brief: Fiscal Year 2015," 2015). Given the disproportionately small number of security clearance holders, the over-classification of material results in a largely uninformed homeland security enterprise. If critical information is blockaded by bureaucratic hurdles and unable to reach frontline personnel in a timely manner, it begs the question: *Are the Department of Homeland Security's activities truly informed by a risk-based evaluation of intelligence?*

c. Overlapping Agency Jurisdictions and Missions

Many DHS components predate the creation of the Department and thus have their own internal collection, analysis, and dissemination practices, which reinforce established organizational cultures. Prevalent in the bureaucracy literature is the idea that horizontal structures of bureaucracy, such as departmentalization, create obstacles to information-sharing between different component agencies because of varying functional mandates, processes, and expectations (Argote et al., 2000; Willem and Buelens, 2007, Yang and Maxwell, 2011). Twenty-one out of twenty-two DHS component agencies predate the creation of the Department of Homeland Security, and each component has a distinct organizational culture and set of norms around the collection, processing, storage, analysis, and delivery of intelligence. This has problematic implications because, as recognized in the relevant literature, information-sharing can become more complex when participating entities' organizational cultures, norms, origins, and values are inconsistent (Drake et al., 2004; Gil-Garcia et al., 2007; Kellogg et al., 2006; Lam, 2005; Pardo et al., 2004; Yang and Maxwell, 2011). Importantly, perceptions about individual benefits and organizational interests are developed and maintained through organizational cultures and values (Jian and Jeffres, 2006; Yang and Maxwell, 2011). Thus, organizational members' attitudes and collective behaviors regarding information-sharing are closely linked to organizational cultures and values (Constant et al., 1994; Jian and Jeffres, 2006).

As the Department of Homeland Security matured, individual components largely retained their respective identities and procedural norms. Researchers acknowledge that organizations have greater difficulty pursuing a common objective when they have diverse organizational values (Atabakhsh et al., 2004; Fedorowicz et al., 2007; Kim and Lee, 2006; Ring and Perry, 1985; Yang and Maxwell, 2011). The lack of cultural continuity among component agencies is further exacerbated by DHS's lack of a centralized authority structure. Over the last three years, DHS has attempted to formalize intra-component cooperation through its "One DHS" and "Unity of Effort" initiatives, but the Office of Inspector General reported little evidence of proactive efforts by leadership to view the organization holistically, to forcefully communicate the need for cooperation among components, and to establish programs or policies that ensure unity, even though such effort is a necessary precondition to unified action ("Major Management and Performance Challenges Facing the Department of Homeland Security," 2017). These bureaucratic challenges hinder DHS's ability to operate as a single entity, hampering the Department's broader efforts to accomplish the homeland security mission effectively.

Furthermore, component agencies are hesitant to share information that may jeopardize a source or method. Law enforcement agents and officers err on the side of caution when an informant's identity is concerned, and for good reason. It often takes months or years for agencies to develop a productive relationship with informants, and most law enforcement and intelligence organizations are not willing to expose all their intelligence beyond their own employees. The recent Chelsea Manning and Edward Snowden cases provide strong justification for this practice, as information-sharing partners can exploit the exchange relationship and act opportunistically (Steiner, 2015).

While the fear of leakers is rationally grounded in recent events and institutional memory, there are other justifications for withholding information that highlight significant mistrust among DHS component agencies. For example, an ICE informant may have information that the USCG needs for a tangential criminal case. If ICE allows the USCG to solicit information from their informant, that individual may subsequently become the crux of the USCG's criminal case and must testify in court, jeopardizing any future work with ICE. This anecdote highlights a critical tension between case-based approaches to law enforcement investigations and intelligence investigations—while the case-based approach to law enforcement investigations is primarily concerned with prosecutions and convictions, the intelligence investigations approach continually revisits lines of analysis (Jackson et al., 2009). These inherently oppositional approaches create unnecessary divisions in trust and loyalty among DHS components and illustrate how bureaucratic competition within the same mission area can make intelligence partners less willing to share analytic products, much less raw information (Jackson et al., 2009).

Likewise, CBP, ICE, TSA, and the USCG share a primary mission to protect the border, and all four agencies compete with each other to achieve this mission, to a certain degree. Efforts to protect the homeland are contingent upon a robust border security strategy that prevents the movement of illicit substances and bad actors while facilitating the lawful flow of commerce and peoples. The variance among ports of entry (POEs), which include the land, sea, and air domains, necessitates the expertise of multiple DHS component agencies to effectively secure the border. In part, the creation of the Department of Homeland Security was intended to consolidate key border security agencies from various Cabinet departments to better integrate the efforts of agencies with overlapping missions (Carafano and Heyman, 2004). However, the centralized bureaucratic structure arguably had an inverse effect—the number of agencies responsible for border, immigration, and transportation security increased to eight, the missions of such agencies were not clearly delineated, and the interdependent responsibilities of ICE and CBP were formally separated without sufficient justification (Carafano and Heyman, 2004).

Although current domestic intelligence efforts necessitate reliable interagency coordination, bureaucratic competition among agencies operating in the same regulatory environment can reduce the likelihood that individuals will share intelligence products

(Jackson et al., 2009). While CBP, ICE, TSA, and the USCG collectively work to prevent a myriad of threats from entering and infiltrating the United States, the reality is that these component agencies are forced to compete with each other to fulfill their individual target performance goals. Despite the fact that CBP, ICE, TSA, and the USCG secure different border domains, DHS does not tailor border security performance metrics to a large enough degree to reflect the nuances of each agency's mission.

For example, CBP is primarily responsible for safeguarding the homeland at and in between POEs. One aspect of this responsibility includes preventing the illegal flow of people and contraband across about 7,000 miles of land border and, in partnership with the USCG, about 95,000 miles of shoreline (Steiner, 2015). Such a daunting task would ideally involve seamless cooperation in the land and maritime domain, but CBP and the USCG compete with each other in an attempt to reach their respective target metrics for interdictions, seizures, apprehensions, etc. per fiscal year. In addition to the USCG, CBP also shares performance metrics with ICE. ICE conducts offensive law enforcement investigations and operations to supplement the primary defensive role of CBP at the border (Steiner, 2015). Additionally, CBP also competes with TSA in their shared responsibility of preventing terrorist exploitation of international passenger and commercial cargo transportation systems (Steiner, 2015).

ICE, CBP, and the USCG all rely on intelligence to support their respective law enforcement responsibilities. However, this becomes problematic when intelligence is valued as a competitive advantage rather than a communal asset (Peled, 2014; Yang and Maxwell, 2011). Through the perspective of transaction cost economic theory, incentives can influence whether information is withheld or shared across organizational boundaries

(Pardo and Tayi, 2007). There are costs associated with gathering information, such as time, resources, and personnel. If the benefits of sharing information do not outweigh the costs incurred in the collection process, there is often little incentive for agencies to share their information with other agencies (Chau et al., 2001; Pardo and Tayi, 2007; Yang and Maxwell, 2011). Furthermore, considering that ICE, CBP, and the USCG all compete with each other to maximize their respective number of interdictions, arrests, disruptions, etc. per fiscal year, there is little incentive for these components to share border security intelligence.

d. Overreliance on Outcome-Centric Metrics to Quantify Achievement

DHS budget requests are heavily influenced by outcome-driven metrics. Components leverage their respective numbers of apprehensions, arrests, detentions, removals, seizures, disruptions, interdictions, etc. to justify budget increases, indirectly prompting fierce competition among agencies to act independently in order to secure recognition of achievement. The Department of Homeland Security's mission is to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016). Due to the gravity of this mission and the persistence of the evolving terrorist threat, Congress appropriates billions of dollars each fiscal year to support DHS's component agencies. Justified as the most important mission that any government can provide to its people ("Budget in Brief: Fiscal Year 2018," 2017) the Department of Homeland Security's nearly $65 billion budget per fiscal year is intended to fund unceasing agility and vigilance on the behalf of the American people. However, it is difficult to evaluate the efficacy of homeland security efforts because prevention, protection, response, and recovery are heavily focused on risk management rather than quantifiable outcomes (Jackson, 2014). The fact that terrorists have been unable to replicate the devastation caused by the September 11 attacks does not necessarily imply a robust homeland security enterprise, nor does it imply money aptly spent. Instead, it could indicate that the terror threat is not nearly as severe as we understand it to be. While I do not personally agree with this sentiment, it does rightfully challenge the value that DHS provides to the American people.

Each fiscal year, the Department of Homeland Security provides a budget justification to Congress to explain its funding priorities and to highlight its contributions to the homeland security enterprise. Each component agency communicates their respective successes to Congress to justify their added value in the context of the overarching DHS mission. However, intelligence expert Gregory F. Treverton (2008) acknowledges that there are significant problems with the data that DHS components offer to rationalize their efficacy: First, it is difficult to quantify the level of effort going into counterterrorism intelligence, as assets support multiple activities. Second, the extent of the domestic terrorist threat is impossible to know with any precision, so it is difficult to measure effectiveness against the threat. Third, the complexity of the domestic intelligence enterprise makes it difficult to determine how capable the country is overall at collecting, analyzing, and acting on intelligence information. The pervasiveness of unknown or unquantifiable factors severely limits the scope of relevant and appropriate metrics to evaluate homeland security efforts. Thus, it is unsurprising that many DHS components utilize the same outcome-centric law enforcement metrics to quantify their successes.

The often-overlooked problem with regard to outcome-centric metrics like drug seizures, illegal migrant apprehensions, explosive detections, etc. is that these metrics foster competition in a domain that would be better suited for collaboration. It is objectively unproductive for the USCG to compete with CBP to interdict a panga boat carrying cocaine from Colombia, or for the USSS to compete with ICE to investigate a currency counterfeiting scheme in China. The Department of Homeland Security simply does not have enough resources or manpower to entertain these overlapping efforts. In the private sector, corporations use per-share profits as a reliable success metric, but there is no comparable data for DHS, nor is it easy to achieve a consensus on what the outcome measures should be and how they might be measured (Jenkins, 2006).

e. Correlation Between Perceived Agency Performance and Annual Budget Appropriations

The Planning, Programming, Budgeting, and Execution (PPBE) process forces component agencies to place an extraordinary emphasis on performance targets, which diverts necessary resources away from other critically important missions and discourages collaboration among components with similar objectives. The Department of Homeland Security's Annual Performance Report is a critical nexus between the Department's priorities and subsequent funding decisions. The *Annual Performance Report: Fiscal Years 2016-2018* presents the Department's performance measures and applicable results aligned to DHS missions, provides the planned performance targets for FY 2017 and FY 2018, and includes information on the Department's Strategic Review and Agency Priority Goals (APGs) ("Annual Performance Report: Fiscal Years 2016-

2018," 2017). The Annual Performance Report is organized around missions and goals identified in the Department's FY 2014-2018 Strategic Plan, which incorporate the five previously mentioned departmental objectives: (1) Prevent terrorism and enhance security, (2) Secure and manage our borders, (3) Enforce and administer our immigration laws, (4) Safeguard and secure cyberspace, and (5) Ensure resilience to disasters ("Our Mission," 2016). The DHS performance community, led by the Chief Operating Officer (COO), the Performance Improvement Officer (PIO), the Deputy PIO (DPIO), and the Assistant Director for Performance Management, employ a tool called the Performance Measure Definition Form (PMDF) to annually assess the breadth and scope of publically reported performance metrics. These performance metrics are cited directly for the Department's PPBE process and the corresponding Performance Budget. The budgeting and programming phases occur concurrently during the PPBE process, and the principal outputs of the budgeting phase are the budget justification materials for the Office of Management and Budget (OMB) and Congress. The inextricable link between the performance community's annual assessments of DHS's performance metrics and the fiscal year budget process should not be underestimated nor overlooked. Arguably the nexus between perceived agency performance and budget appropriations increases the transaction costs associated with information-sharing because the possession of information is considered to enhance agency performance.

The performance metrics that inform the PPBE process for DHS agencies involved in the domestic IC are largely outcome-centric and emphasize law enforcement functions, such as apprehensions, arrests, detentions, removals, seizures, disruptions, and interdictions. As such, components with overlapping jurisdictions and regulatory environments may be more inclined to pursue their own parochial self-interests and act independently rather than prioritize collaborative efforts. The following examples from the *Annual Performance Report: Fiscal Years 2016-2018* highlight the unintended consequences of DHS's outcome-centric performance metric assessment process:

i. ICE aims to disrupt and dismantle transnational criminal organizations (TCOs) and is assessed with the following metrics: "Percent of significant drug investigations that resulted in a disruption or dismantlement," "Percent of significant transnational gang investigations that resulted in a disruption or dismantlement," and "Percent of significant child exploitation or child sex trafficking investigations that resulted in a disruption or dismantlement." In FY 2016, ICE was unable to reach the target percent of drug investigations that resulted in a disruption or dismantlement because the agency had reallocated its finite resources to address another timely and equally important issue: the opioid epidemic. ICE dedicated a sizeable proportion of its counter-drug resources, which otherwise would have been utilized to combat TCO activities, to focus on the public health crisis caused by increasing abuse of heroin and fentanyl ("Annual Performance Report: Fiscal Years 2016-2018," 2017). Outcome-centric performance metrics force component agencies to prioritize certain objectives unconditionally, irrespective of emergent threats to the nation's security and well-being. Because of the budget implications of the PPBE process, component agencies like ICE are not inclined to divest significant resources from activities that correspond with APGs, even when such divestments would directly enhance the nation's security. The combination of finite resources and inflexible performance metrics results in fragmented homeland security activities, as agencies are forced to reconcile competing priorities against the backdrop of an evolving threat environment.

ii. Although the USSS is primarily responsible for investigating and preventing counterfeiting, “the agency’s investigative mission has evolved from enforcing counterfeiting laws to safeguarding the payment and financial systems of the United States from a wide range of financial and computer-based crimes” (“The Investigative Mission,” n.d.). Today, the U.S. Secret Service plays a critical role in securing the nation’s critical infrastructure, especially in the realms of cyber, banking, and finance. As such, the USSS’s performance metrics reflect the agency’s ability to meet certain objectives related to financial cybercrimes, including: “Amount of dollar loss prevented by Secret Service cyber investigations (in millions),” “Terabytes of data forensically analyzed for criminal investigations,” and “Number of cyber mitigation responses.” Although the USSS’s investigative mission necessarily expanded to include cybersecurity, the agency competes with the National Protection and Programs Directorate (NPPD) to protect the nation’s critical infrastructure and with ICE to combat cybercrimes. The quantity and sophistication of cybercrimes targeting U.S. financial institutions requires a whole-of-government approach, but the outcome-centric nature of the USSS’s performance metrics discourages the agency from pursuing collaborative activities with other component agencies. Because the USSS, NPPD, and ICE operate in overlapping jurisdictions and regulatory environments, they compete with each other to achieve their respective performance targets. Although the information yielded by USSS investigations would be valuable to all three component agencies, it is unsurprising that USSS would forego information-sharing activities to protect its own self-interests. If the theory of transaction cost economics and the theory of reasoned action are applied in tandem to explain why the USSS would be inclined to withhold information, it becomes clear that bureaucratic competition imposes large transaction costs on information-sharing relationships.

iii. CBP, ICE, the USCG, and USCIS all play a key role in preventing the illicit movement of people and goods across our nation's borders while promoting lawful entry and exit ("Border Security," 2017). The applicable performance metrics, including "Rate of interdiction effectiveness along the Southwest Border between ports of entry," "Percent of detected conventional aircraft incursions resolved along all borders of the United States," and "Number of smuggled outbound weapons seized at the ports of entry" are all used to gauge CBP's effectiveness, though they clearly necessitate a whole-of-government approach. The USCG is evaluated by the metric, "Migrant interdiction effectiveness in the maritime environment," which fuels unnecessary competition with CBP's Air and Marine Operations (AMO). Both the USCG and CBP's AMO are responsible for interdictions, yet both sets of performance metrics neglect to incentivize collaborative capacity between the two agencies.

Recognizing the significant overlap between the operational responsibilities of CBP, ICE, the USCG, and USCIS and the necessity of seamless cross-component coordination to achieve Departmental objectives, Secretary Jeh Johnson commissioned three DHS Joint Task Forces (JTF) on November 20, 2014, in furtherance of a Department-wide Southern Border and Approaches Campaign Plan (Johnson, 2014). Joint Task Force East became responsible for the southern maritime border and approaches, Joint Task Force West became responsible for the Southwest land border and the West Coast, and Joint Task Force Investigations became responsible for investigations in support of both geographic Task Forces. Importantly, Secretary Johnson directed CBP, ICE, the USCG, and USCIS to "realign personnel and stand up headquarters capabilities within each Joint Task Force" (Johnson, 2014, p. 3). Secretary Johnson also harmonized component agency priorities and performance objectives by explicitly directing the Directors of the JTFs to conduct operations consistent with the following lines of effort: (1) Reduce the terrorism risk to the Nation; (2) Combat transnational criminal organizations; (3) Prevent exploitation of legal flows at ports of entry; (4) Counter illegal flows at maritime approaches and in between ports of entry; (5) Manage lawful flows of people and goods in transit; and (6) Disincentivize illegal border behavior (Johnson, 2014). These JTFs were designed to counteract inter-agency competition between components with a stake in border security and "facilitate awareness about cross-component, cross-geographic homeland security issues" ("Drug Control: Certain DOD and DHS Joint Task Forces Should Enhance Their Performance Measures to Better

Assess Counterdrug Activities," 2019, p. 12). Arguably, Secretary Johnson recognized that overlapping jurisdictions and missions in the realm of border security do not make our borders safer when corresponding performance metrics stoke rivalries among component agencies that would otherwise leverage each other's resources and personnel to facilitate a unity of effort.

IV. Conclusion

The Department of Homeland Security was established in the aftermath of the September 11 terror attacks, but its bureaucratic structure has not adapted to the new realities presented by the diversity of threats to the homeland. Reflecting the evolving threat landscape, the Department of Homeland Security's mission to safeguard the country against terrorism has also expanded to include securing our borders, enforcing our immigration laws, safeguarding cyberspace, and ensuring resilience to disasters. Because DHS's success is contingent upon effective collaboration between many different federal, state, local, tribal, public, private, and international partners, DHS must develop structures and processes that provide incentives and rewards for collaboration, consultation, and support for implementing key goals.

Critical to this whole-of-government approach is the remediation of factors that inhibit effective information-sharing, the establishment of an incentives system to encourage information exchanges, and the adoption of a more fluid intelligence discipline that transmits information to end users more quickly. A re-examination of the Department's bureaucratic model could address key problems that inhibit information-sharing, such as the lack of information technology interoperability, the incongruity of classification standards, overlapping agency jurisdictions and missions, the overreliance on outcome-centric metrics to quantify achievement, and the correlation between perceived agency performance and annual budget appropriations. The Department of Homeland Security has an obligation to strengthen the homeland security enterprise, and that must begin with a unified and integrated Department.

CHAPTER 3: Case Study

I. Introduction

Following the terror attack in San Bernardino, California on December 2, 2015, the federal government initiated an extensive investigation to determine whether other terror attacks were imminent. Despite the urgency and gravity of the federal investigation, two component agencies within the Department of Homeland Security (DHS) failed to share pertinent information with each other in a timely manner, jeopardizing the safety and security of the American public. U.S. Citizenship and Immigration Services (USCIS) and Immigration and Customs Enforcement (ICE), which share responsibility for enforcing U.S. immigration laws, were unable to coordinate during an emergency situation and accomplish what DHS was originally designed to facilitate—a more unified and streamlined homeland security apparatus.

This chapter examines the Department of Homeland Security's response to the terror attack in San Bernardino, California on December 2, 2015 as a case study to test the information-sharing and bureaucracy theoretical frameworks established in chapters 1 and 2. This case study features a clear example of an information-sharing failure between two DHS component agencies on hierarchical parity within the broader DHS organizational structure. This information-sharing failure is instructive because USCIS took three deliberate actions to prevent ICE from obtaining critical information, demonstrating unambiguous intent to stymie inter-organizational information-sharing: (1) USCIS delayed ICE's entry into the USCIS facility; (2) USCIS prohibited ICE from arresting, detaining, or interviewing anyone in the USCIS facility; and (3) USCIS did not share a tangible copy of Mariya Chernykh's A-file with ICE agents. The concept of intent is a central focus of this case study because it illustrates how the present structural design of the Department of Homeland Security does not incentivize information-sharing between component agencies. The actions of at least two DHS component agencies in the wake of the December 2, 2015 terror attacks demonstrate the strength of current bureaucratic realities in protecting the "turf," prerogatives, practices of each agency, and the absence of true cooperation or collaboration. This conclusion is demonstrated in the three specific actions that took place after the attacks.

For historical context, this chapter begins with a brief description of the evolution of the Department of Homeland Security's organizational structure. Importantly, the dismantlement of the Immigration and Naturalization Service (INS) and the delineation of DHS's immigration enforcement functions across three separate component agencies created new bureaucracies where none had existed previously. Next, this chapter examines the contemporary relationship between USCIS and ICE with a particular focus on persistent management problems that inhibit coordination and information-sharing efforts. A substantial amount of analysis is dedicated to USCIS's Fraud Detection and National Security Directorate (FDNS), which was created to facilitate the Joint USCIS-ICE Anti-Fraud Strategy, an institutionalized interagency process for addressing immigration benefit fraud. The complexity inherent in administering and enforcing our nation's lawful immigration system requires an integrated approach, but, as this chapter illustrates, the distinct priorities and investigative capabilities of FDNS and ICE detract from overarching departmental objectives.

Ultimately, this case study examines why USCIS would be inclined to withhold information from ICE in the wake of a devastating terror attack and provides substantive insight into the following question: *How does the organizational structure of the Department of Homeland Security influence information-sharing among component agencies?* Building upon chapters 1 and 2, this chapter assesses how the Department of Homeland Security's centralized bureaucratic model enables and encourages its component agencies to pursue their parochial self-interests at the detriment of the Department's overarching mission. These theoretical frameworks provide critical insight into the ways in which the Department of Homeland Security's organizational structure institutionalizes interagency competition, thereby reinforcing factors that impede and discourage effective information-sharing.

II. Limitations

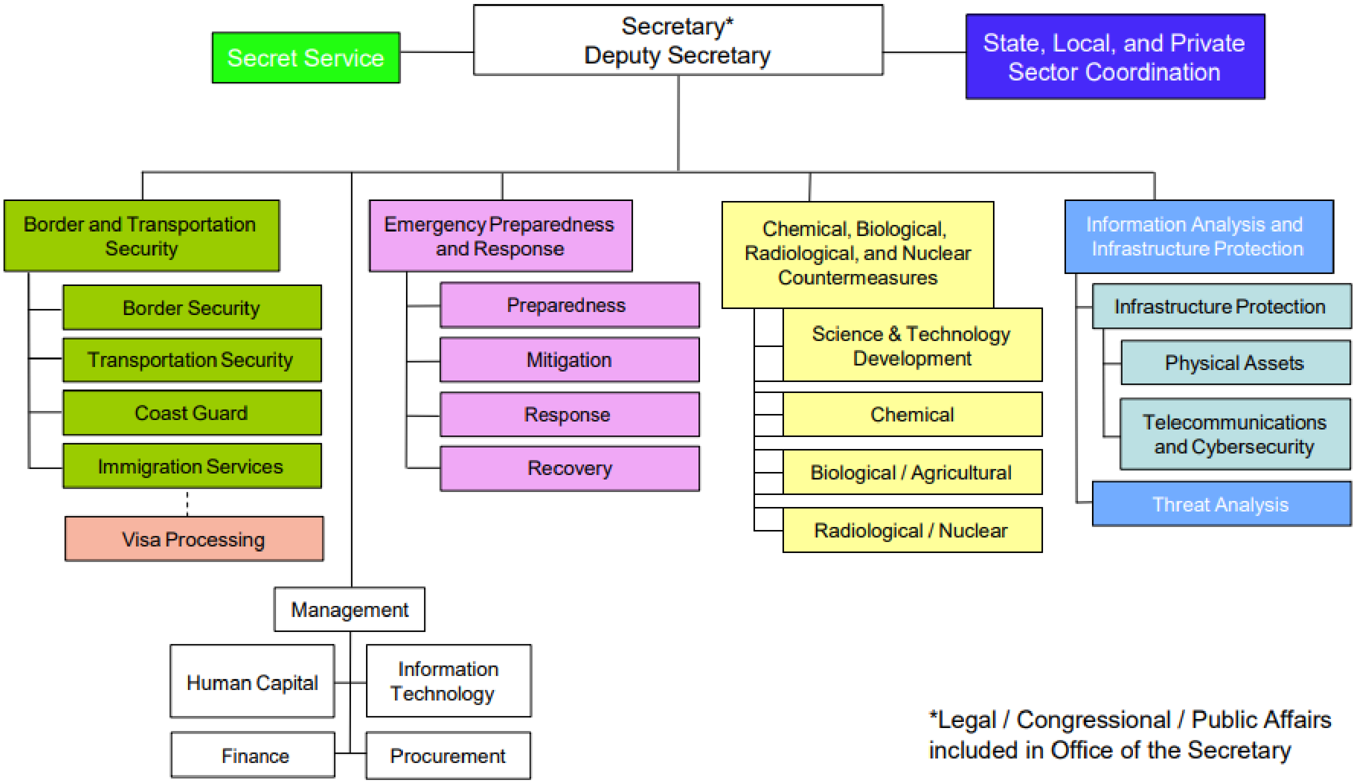
Before discussing the merits of this case study, it is important to first acknowledge the limitations of this particular topic and methodology. Given the sensitive nature of the Department of Homeland Security's mission and associated activities, a large amount of data related to information-sharing practices is classified and therefore inaccessible. Moreover, the relevant reports and audits published by oversight agencies like the Office of Inspector General (OIG) and the Government Accountability Office (GAO) are similarly limited in what they can publicly disclose in an unclassified setting. While the conclusions drawn by the OIG and the GAO are helpful in bolstering the theories underpinning this case study, the analyses set forth in this chapter are admittedly devoid of quantifiable data that would otherwise give credibility to the main argument.

While I am confident that my work and educational experiences have prepared me for this undertaking, I would be remiss if I did not acknowledge the scope of the information I simply do not know. For example, I cannot comment definitively on the organizational culture of a component agency that I have never personally worked for. Nor can I confidently assert that the reports and other publications issued by the Department of Homeland Security accurately portray the entirety of what they purport to explain. What is not included in government documents can arguably be as important as the information the author chooses to include. Realistically, it does not behoove an executive branch agency to issue a report that would erode public trust or prompt Congressional oversight. It is important to consider that Article I Section 9 of the U.S. Constitution gives Congress the power to determine both the size and composition of appropriations that fund executive branch agencies. Because of the financial influence that Congress has over executive branch agencies, one can reasonably conclude that the Department of Homeland Security would be incentivized to issue reports that characterize its activities in a positive light.

Another limitation of this case study stems from the absence of research dedicated to measuring the effectiveness of information-sharing efforts, as discussed in chapter 1. Given that information is an ambiguous concept and that information can exist in both explicit and implicit forms, there is no uniform approach or metric to evaluate the efficacy of information-sharing practices. Aside from objective observations about whether information-sharing did or did not occur in a specific context, there are limited avenues by which one can assess information exchanges (or the lack thereof) in an empirical way. Moreover, the value of information-sharing endeavors cannot be measured simply by the successful transmission of information across organizational boundaries; it is also important to assess whether the information is absorbed and utilized effectively within the organization that acquired it (Jackson, 2014; Yang and Maxwell, 2011). Fundamentally, information is shared not for its own sake but in the pursuit of a mission. Therefore, in this case study, effective information-sharing among DHS component agencies is defined as an activity that helps to “ensure a homeland that is safe, secure, and resilient against terrorism and other hazards” (“Our Mission,” 2016).

III. Background

Fourteen months after the September 11, 2001 terror attacks, Congress passed the Homeland Security Act of 2002 to further coordinate and unify national homeland security efforts. The Homeland Security Act (Public Law 107-296) formally established the Department of Homeland Security as a Cabinet-level department with a primary mission of protecting the American homeland. As outlined in President George W. Bush’s proposal (Bush, 2002), the organizational structure of the Department of Homeland Security was initially designed to reflect four key departmental objectives: (1) Border and Transportation Security; (2) Emergency Preparedness and Response; (3) Chemical, Biological, Radiological and Nuclear Countermeasures; and (4) Information Analysis and Infrastructure Protection. The following organizational chart (*Figure 1*) from President Bush’s proposal illustrates the hierarchy of the nascent homeland security bureaucracy:



Secret Service
Secretary*
Deputy Secretary
State, Local, and Private Sector Coordination
Border and Transportation Security
Border Security
Transportation Security
Coast Guard
Immigration Services
Visa Processing
Emergency Preparedness and Response
Preparedness
Mitigation
Response
Recovery
Chemical, Biological, Radiological, and Nuclear Countermeasures
Science & Technology Development
Chemical
Biological / Agricultural
Radiological / Nuclear
Information Analysis and Infrastructure Protection
Infrastructure Protection
Physical Assets
Telecommunications and Cybersecurity
Threat Analysis
Management
Human Capital
Information Technology
Finance
Procurement
*Legal / Congressional / Public Affairs included in Office of the Secretary

Figure 1. DHS Organizational Chart (June 2002).
Source: Bush, G. W. (2002). The Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/book_0.pdf

The duties and responsibilities of several former agencies were transferred to the Department of Homeland Security, resulting in the most substantial reorganization of the federal government since the 1940s ("Management Challenges Remain in Transforming Immigration Programs," 2004). Importantly, responsibility for immigration enforcement functions was transferred from the Department of Justice's INS to the Department of Homeland Security. The Homeland Security Act of 2002 effectively dismantled the INS and separated the agency into three new components within DHS: USCIS, ICE, and U.S. Customs and Border Protection (CBP). The following diagram (*Figure 2*) illustrates the transfer of immigration functions from INS to DHS:

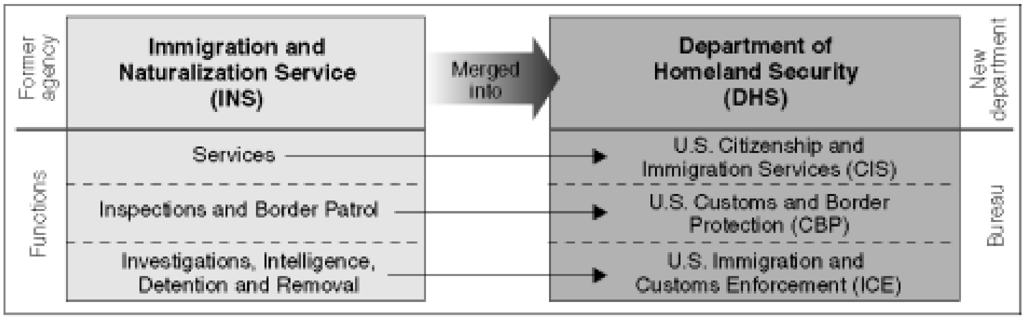

Former agency
Immigration and Naturalization Service (INS)
Merged into
Department of Homeland Security (DHS)
New department
Functions
Services
Inspections and Border Patrol
Investigations, Intelligence, Detention and Removal
U.S. Citizenship and Immigration Services (CIS)
U.S. Customs and Border Protection (CBP)
U.S. Immigration and Customs Enforcement (ICE)
Bureau

Figure 2. Reorganization of INS into DHS (May 5, 2005).
Source: U.S. Government Accountability Office. (2005). Department of Homeland Security: Addressing Management Challenges That Face Immigration Enforcement Agencies. Retrieved from https://www.gao.gov/assets/120/111634.pdf

In 2004, the GAO reported that USCIS, ICE, and CBP were continuing to experience management challenges that were previously pervasive within INS. Importantly, these challenges persisted in spite of the decentralization of INS's immigration authorities across three separate component agencies. According to the report, these INS management challenges included "a lack of clearly defined priorities and goals; difficulty determining whom to coordinate with, when to coordinate, and how to communicate; and inadequately defined roles resulting in overlapping responsibilities, inconsistent program implementation, and ineffective use of resources" ("Addressing Management Challenges That Face Immigration Enforcement Agencies," 2005, p. 1). In fact, the GAO issued seven reports from 1997 to 2002 that identify persistent management challenges impeding INS's ability to effectively enforce immigration law.[1]

[1] See Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy, (Washington, D.C.: June 19, 2002); Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems, (Washington, D.C.: Jan. 31, 2002); INS's Southwest Border Strategy: Resource and Impact Issues Remain after Seven Years, (Washington, D.C.: Aug. 2, 2001); Immigration Benefits: Several Factors Impede Timeliness of Application Processing, (Washington, D.C.: May 4, 2001). Alien Smuggling: Management and Operational Improvements Needed to Address Growing Problem, (Washington, D.C.: May 1, 2000); Criminal Aliens: INS's Efforts to Identify and Remove Imprisoned Aliens Continue to Need Improvement, (Washington, D.C.: Feb., 25, 1999); and Criminal Aliens: INS' Efforts to Identify and Remove Imprisoned Aliens Need to be Improved, (Washington, D.C.: July 15, 1997)

Soon after Michael Chertoff was sworn in as the second Secretary of the Department of Homeland Security in 2005, he initiated a “comprehensive review of the Department’s organization, operations, and policies” (“The Department of Homeland Security Appropriations,” 2005). This review, known as the Second Stage Review or 2SR, involved an evaluation of DHS’s organizational structure to assess whether the Department's policies, operations, and structures aligned in the best way to address present and future threats (“Department Six-point Agenda,” 2015). The 2SR produced a Six-point agenda for the Department of Homeland Security, which proposed realigning the DHS organizational structure to maximize mission performance (“Department Six-point Agenda,” 2015). Despite concerns about the disaggregation of DHS’s immigration responsibilities across multiple agencies, Secretary Chertoff retained the three separate immigration component agencies in the new organizational structure (Wasem, 2007). In his 2SR remarks on July 13, 2005, Secretary Chertoff explained that a flatter bureaucracy would improve DHS’s “ability to coordinate and carry out operations,” and announced that “all seven primary operational components of this Department will have a direct line to the Secretary” (“U.S. Department of Homeland Security Second Stage Review Remarks,” 2005). Accordingly, Secretary Chertoff eliminated the Border and Transportation Security Directorate (BTS) and elevated CBP and ICE to hierarchical parity with the Transportation Security Administration (TSA), the U.S. Secret Service (USSS), USCIS, the Federal Emergency Management Agency (FEMA), and the U.S.

Coast Guard (USCG). The following organizational chart (*Figure 3*) illustrates the structure of the Department of Homeland Security after the 2SR reorganization:

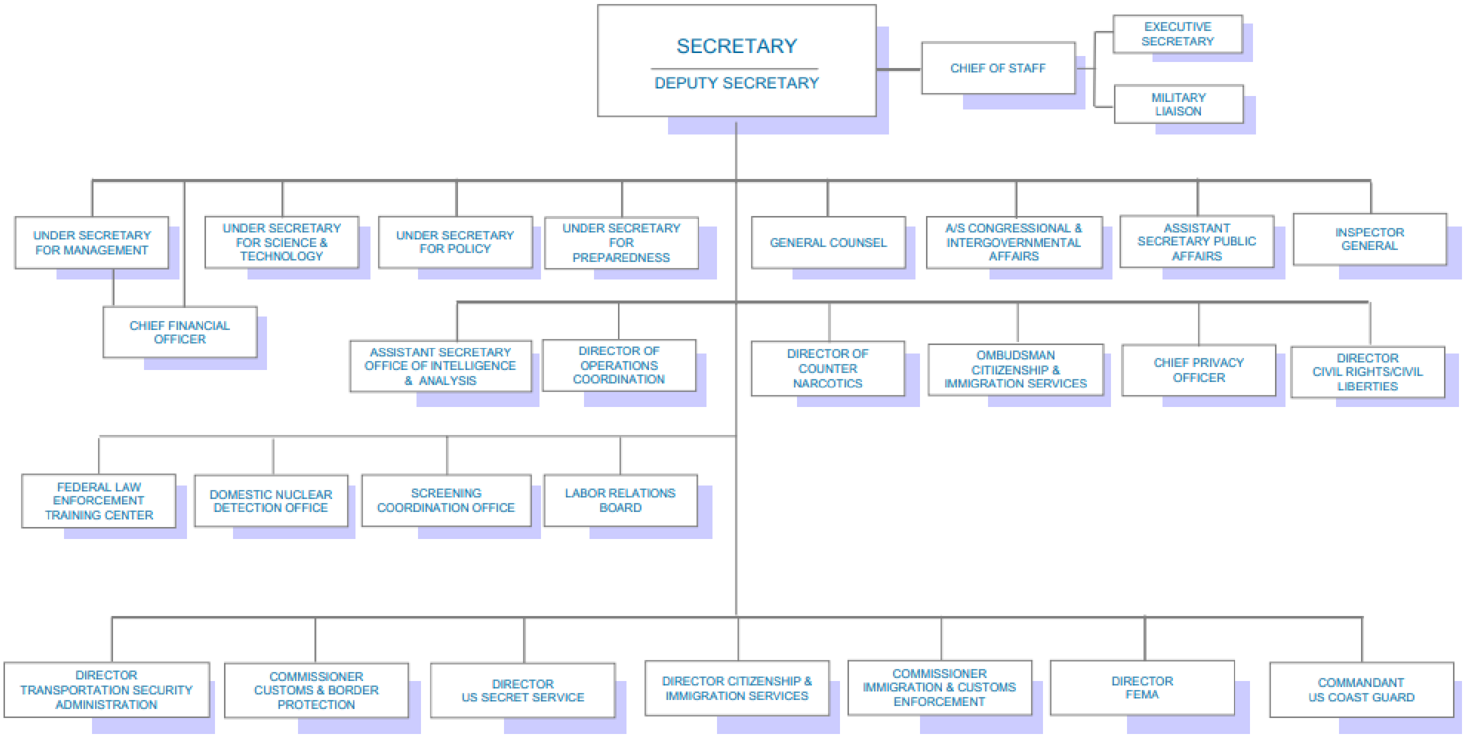

SECRETARY
DEPUTY SECRETARY
CHIEF OF STAFF
EXECUTIVE SECRETARY
MILITARY LIAISON
UNDER SECRETARY FOR MANAGEMENT
UNDER SECRETARY FOR SCIENCE & TECHNOLOGY
UNDER SECRETARY FOR POLICY
UNDER SECRETARY FOR PREPAREDNESS
GENERAL COUNSEL
A/S CONGRESSIONAL & INTERGOVERNMENTAL AFFAIRS
ASSISTANT SECRETARY PUBLIC AFFAIRS
INSPECTOR GENERAL
CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OFFICE OF INTELLIGENCE & ANALYSIS
DIRECTOR OF OPERATIONS COORDINATION
DIRECTOR OF COUNTER NARCOTICS
OMBUDSMAN CITIIZENSHIP & IMMIGRATION SERVICES
CHIEF PRIVACY OFFICER
DIRECTOR CIVIL RIGHTS/CIVIL LIBERTIES
FEDERAL LAW ENFORCEMENT TRAINING CENTER
DOMESTIC NUCLEAR DETECTION OFFICE
SCREENING COORDINATION OFFICE
LABOR RELATIONS BOARD
DIRECTOR TRANSPORTATION SECURITY ADMINISTRATION
COMMISSIONER CUSTOMS & BORDER PROTECTION
DIRECTOR US SECRET SERVICE
DIRECTOR CITIZENSHIP & IMMIGRATION SERVICES
COMMISSIONER IMMIGRATION & CUSTOMS ENFORCEMENT
DIRECTOR FEMA
COMMANDANT US COAST GUARD

Figure 3. DHS Organizational Structure After 2SR (July 27, 2005).
Source: U.S. Department of Homeland Security. (2008). Brief Documentary History of the Department of Homeland Security: 2001-2008. Retrieved from https://www.hsdl.org/?view&did=37027

Structurally, the reorganization streamlined the chain of command for all three operational components with immigration enforcement functions. The Director of USCIS, the Commissioner of ICE[2], and the Commissioner of CBP all serve with the same rank under the Secretary of the Department of Homeland Security. In a sense, the 2SR reorganization recreated the cohesiveness of the INS by placing USCIS, ICE, and

[2] Immigration and Customs Enforcement (ICE) is currently led by a Director, not a Commissioner.

CBP on the same lateral plane. However, the delineation of immigration responsibilities across three separate agencies means that no single agency has full responsibility or accountability for overarching immigration policy. The question remains, *Does this bifurcation of responsibility yield a more focused and concerted approach to specific immigration functions, or does it complicate the chain of command and foster competition between component agencies with distinct yet interrelated priorities?*

IV. The Contemporary Relationship Between USCIS and ICE

The organizational structure that resulted from the 2SR largely mirrors the organizational structure of the Department of Homeland Security today. Although USCIS and ICE are both vestiges of the INS, both agencies have evolved over time and adopted their own respective cultures and priorities. Since 2003, USCIS and ICE have operated independently to accomplish their distinct missions. The mission statements of both agencies reflect their unique areas of responsibility within the broader concept of immigration enforcement. USCIS "administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values" ("Mission Statement," 2018). ICE's mission is to "protect America from the cross-border crime and illegal immigration that threaten national security and public safety" ("What We Do," 2018). Both agencies are charged with ensuring the integrity of our nation's immigration system, but recent evidence shows that USCIS and ICE do not always coordinate efforts to achieve successful immigration management.

In 2017, the Department of Homeland Security Office of Inspector General (OIG) conducted an audit "to determine whether DHS fosters collaboration and unity of effort department-wide to enforce and administer immigration law and policy" (Roth, 2017, p. 12). The OIG concluded that ICE and USCIS continue to experience immigration enforcement and administration challenges despite departmental efforts to establish a "Unity of Effort," as described in chapter 2. Importantly, the OIG determined that both agencies' persistent management problems are directly correlated with the organizational structure of the Department of Homeland Security. According to the audit, "Challenges related to the evaluation of immigration outcomes, the affirmative asylum application process, and cross-component coordination difficulties existed because no specific department-level group is responsible for addressing overarching component immigration challenges" (Roth, 2017, p. 3).

The central difference between the organizational structure of the INS and the organizational structure of DHS's immigration responsibilities today is the decentralization of authority and oversight. In a sense, the organization of the Department of Homeland Security's immigration functions encourages individual agencies to prioritize their respective responsibilities at the detriment of broader, departmental goals. Prevalent in the bureaucracy literature is the idea that horizontal structures of bureaucracy, such as departmentalization, create obstacles to information-sharing between different component agencies because of varying functional mandates, processes, and expectations (Argote et al., 2000; Willem and Buelens, 2007; Yang and Maxwell, 2011). When the Homeland Security Act of 2002 decentralized INS's immigration enforcement and administration responsibilities and reorganized those functions within a new centralized structure, USCIS and ICE inherited distinct yet critically interrelated elements of that broader authority. Now, both components must balance their own respective priorities as well as the Department's overarching immigration authority with finite resources and manpower.

Although the OIG contends that the management challenges experienced by USCIS and ICE are linked to the organizational changes brought on by the Homeland Security Act of 2002, the OIG stipulates that "Nothing in the Act would prohibit greater cross-component coordination and unity of effort with respect to immigration" (Roth, 2017, p. 3). While the OIG correctly points out that the provisions within the Homeland Security Act in and of themselves do not directly impair unity of effort, the Act fundamentally decentralized the Department's immigration authorities and created new bureaucracies where none had existed previously. As such, it is reasonable to question whether the Department's immigration responsibilities are best served by a centralized immigration agency like INS or a decentralized network of three separate immigration bureaucracies like USCIS, ICE, and CBP.

With regard to the relationship between bureaucracy and information-sharing, scholars like Peled (2014) argue that government agencies must be coerced to share information because bureaucracies are explicitly designed to counteract inter-organizational information-sharing. He maintains that the institutional features of the U.S. federal government, such as regulations, oversight mechanisms, and organizational cultures, are intended to frustrate integration and prevent organizations from becoming too powerful (Peled, 2014). Moreover, information flows are strictly regulated in the bureaucratic model, which further restricts opportunities for integration (Wheatley, 2006;

Yang and Maxwell, 2011). Arguably, the multiple layers of bureaucracy inherent in DHS's organizational structure stifle opportunities for information-sharing between component agencies like USCIS and ICE because components have relatively little incentive to overcome the 'institutional features of the U.S. federal government' (Peled, 2014) that frustrate coordination. This problem is compounded by the fact that no specific department-level group is responsible for oversight of overarching component immigration challenges, such as information-sharing (Roth, 2017). Without incentives or an oversight body to encourage cross-component information-sharing, it is unsurprising that the Department of Homeland Security has difficulty coercing USCIS and ICE to share information voluntarily.

To counteract cross-component coordination hurdles posed by DHS's centralized bureaucratic structure, USCIS established the Fraud Detection and National Security (FDNS) Directorate to "ensure immigration benefits are not granted to individuals who pose a threat to national security or public safety, or who seek to defraud our immigration system" ("Fraud Detection and National Security Directorate," 2015). Previously, there were no formal cross-component strategies or institutionalized processes for addressing benefit fraud (Skinner, 2007). In a 2005 Conference Report, Congress articulated its intent that FDNS would be responsible for "developing, implementing, directing, and overseeing the joint CIS[3]-ICE anti-fraud initiative, and conducting law enforcement/background checks on every applicant, beneficiary, and petitioner prior to granting any immigration benefits" (Conf. Rep. No. 108-774, 2004, p. 74). Accordingly, FDNS and ICE established a formal partnership and implemented a Joint Anti-Fraud

[3] CIS is another acronym for USCIS.

Strategy through FDNS. USCIS describes this partnership as a necessary division of interrelated responsibilities: “FDNS pursues administrative inquiries into most application and petition fraud, while ICE conducts criminal investigations into major fraud conspiracies” (“Fraud Detection and National Security Directorate,” 2015). The Joint Anti-Fraud Strategy promotes a balanced and coordinated operation that distinguishes USCIS’s administrative authority from ICE’s investigative authority.

In 2010, FDNS was elevated to Directorate status, which significantly raised the profile of fraud detection and national security work within USCIS. This structural change was intended to prompt operational enhancements and improve “the integration of the FDNS mission in all facets of the agency’s work” (“Fraud Detection and National Security Directorate,” 2015). As the prominence of FDNS dramatically increased, its mission of detecting, deterring, and combatting fraud evolved to place greater emphasis on national security challenges and threats to public safety in the immigration benefits process (“Annual Report 2018,” 2018). For example, former USCIS Director Leon Rodriguez described FDNS’s work as fulfilling “the USCIS mission of enhancing both national security and the integrity of the legal immigration system” (“The Security of U.S. Visa Programs,” 2016). FDNS supports these new priorities by, among other things, “acting as USCIS’s primary conduit for information sharing and collaboration with other governmental agencies” (“Privacy Impact Assessment,” 2014, p. 2). As USCIS’s principal liaison to law enforcement and intelligence partners involved in combatting immigration benefit fraud, FDNS plays a critical role in determining what information is shared with ICE and when such information-sharing exchanges occur. The discretion afforded by this responsibility will be apparent in the following case study.

V. San Bernardino Terror Attack

On December 2, 2015, Sayed Rizwan Farook and his wife, Tashfeen Malik, carried out an Islamic State of Iraq and Syria (ISIS)-inspired attack at the Inland Regional Center (IRC) in San Bernardino, California that left 14 people dead and 22 injured. Following the attack, authorities initiated a broad federal investigation to determine "the identity of those involved or whether further attacks were planned" (Roth, 2016, p. 2). Soon after, law enforcement personnel discovered that Enrique Marquez, Farook's friend and long-time neighbor, purchased the Oracle Rifle and the Smith and Wesson Rifle that Farook had used in the attack (*United States of America v. Enrique Marquez Jr.*, 2015).

At approximately 12:20 p.m. on December 3, 2015, the San Bernardino Joint Terrorism Task Force (JTTF) provided crucial information regarding Marquez's location to Homeland Security Investigations (HSI), the investigative arm of ICE (Roth, 2016). The JTTF developed information that Marquez's wife, Mariya Chernykh, had an appointment at 12:30 p.m. on December 3, 2015, at the San Bernardino USCIS facility (Roth, 2016). The JTTF believed that Marquez would accompany Chernykh, a Russian national attempting to adjust her immigration status, to the USCIS facility. Following up on the information from the JTTF, HSI dispatched a team of five agents dressed in tactical gear to the USCIS facility (Roth, 2016).

At approximately 12:30 p.m., the HSI agents arrived at the USCIS facility and informed the Federal Protective Service (FPS) of their official purpose. The FPS guards "advised the HSI agents that they had to stay in the lobby until the Field Office Director approved their entry," (Roth, 2016, p. 3) despite the urgency of the matter. The HSI agents waited in the lobby for approximately 15 to 20 minutes before they were escorted to a conference room. The HSI agents waited an additional 10 minutes before the USCIS Field Office Director arrived to meet with them (Roth, 2016).

Although HSI vocalized concerns that Marquez could be connected to the prior day's terror attack and that he could be in the USCIS building with weapons and explosives, the Field Office Director insisted that she contact her superiors for guidance before permitting the agents to enter the building. Citing USCIS policy, the Field Office Director told the HSI agents that they were "not allowed to arrest, detain, or interview anyone in the building" (Roth, 2016, p. 4). The agents also spoke with the FDNS Acting Chief, Los Angeles, who relayed the same message over the phone (Roth, 2016).

After HSI's futile attempt to enter the USCIS facility, the agents requested a copy of Chernykh's Alien Registration File, or A-file. The Field Office Director refused to give the HSI agents Chernykh's A-file and, according to the agents, was not forthcoming with the material in the file (Roth, 2016). HSI asked for known addresses, but the Field Office Director only confirmed the address provided by the agents (Roth, 2016). The Field Office Director refused to offer more information: "HSI believed that the Field Office Director was not going to cooperate in their effort to locate Marquez, so they left the building and regrouped in the parking lot" (Roth, 2016, p. 5). More than an hour after HSI agents first arrived at the USCIS facility, the Field Office Director agreed to discuss Chernykh's A-file with the HSI agents. Importantly, the Field Office Director refused to give HSI a copy of the file and only allowed the agents to hand-copy information under USCIS supervision (Roth, 2016).

VI. Congressional Oversight

At some point before March 15, 2016, a whistleblower contacted the office of Senator Ron Johnson, the Chairman of the Homeland Security and Governmental Affairs Committee, to inform him of the lack of coordination between USCIS and ICE in the aftermath of the San Bernardino terror attack. Chairman Johnson subsequently invited the Honorable Leon Rodriguez, the Director of USCIS, and the Honorable Sarah Saldaña, the Director of ICE, to testify before the Committee at a hearing titled, *The Security of U.S. Visa Programs*. During the hearing, Chairman Johnson criticized USCIS for failing to facilitate information-sharing processes in the midst of a national security emergency: "So, we had a team, armed up and, potentially, dealing with a terrorist. They had a tip from the FBI that Mr. Marquez might be at the USCIS facility and the officer in charge of USCIS—the officers would not allow HSI into the building and would not give them the A-file. That is not indicating a great deal of cooperation between two different agencies under DHS, whose supposedly top concern is the security of this Nation" ("The Security of U.S. Visa Programs," 2016). Chairman Johnson rightfully points out that the Department of Homeland Security's overarching mission is undermined when component agencies are unable to effectively share information. Senator Chuck Grassley, Chairman of the Judiciary Committee, echoed Chairman Johnson's dismay, stating, "This is a classic example of the left hand not knowing what the right hand is doing in the Obama Administration's Department of Homeland Security… Agents we depend on to keep us safe, especially hours after a terrorist attack in San Bernardino, were blocked by officials within their own agency from conducting a routine law enforcement action to prevent a potentially dangerous situation at a federal building" (Hattem, 2016).

The events that transpired on December 3, 2015 at the San Bernardino USCIS facility triggered widespread criticism of the Department of Homeland Security's ability to carry out its foundational missions, including preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience ("Our Mission," 2016). Luckily, the bureaucratic turf war between two Department of Homeland Security component agencies merely resulted in a delayed investigation as neither Chernykh nor Marquez showed up for the appointment. However, it begs the question, *Is the structure of the Department of Homeland Security conducive to cross-component information-sharing, a critical process underlying the Department's key missions?*

VII. Case Study

In hindsight, we are very lucky that Marquez did not play a bigger role in the terror attack that occurred at the IRC on December 2, 2015. While Marquez and Chernykh's intentions were unknown at the time of ICE's visit to the USCIS facility, HSI's precautionary investigation into Marquez on December 3, 2015 was ultimately warranted. Enrique Marquez was later charged with a variety of terrorism-related offenses and eventually pled guilty to conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a) and false statements in connection with the acquisition of a firearm in violation of 18 U.S.C. § 922(a)(6) (*United States of America v. Enrique Marquez Jr.*, 2017).

Had Marquez and Chernykh conspired with Farook and Malik to carry out additional attacks in San Bernardino, the Department of Homeland Security would have been ill-prepared to connect the dots ‘left of boom.’ Fundamentally, the lack of coordination between USCIS and ICE impeded the Department’s ability to “ensure a homeland that is safe, secure, and resilient against terrorism and other hazards” (“Our Mission,” 2016). Particularly damning is the fact that this information-sharing failure was intentional. USCIS deliberately withheld information from another component agency similarly responsible for immigration and homeland security functions during a national security emergency. As such, the crux of this case study is an examination of the three actions taken by USCIS on December 3, 2015 in San Bernardino that demonstrate an intent to withhold information from ICE. In the following paragraphs, the predominant theories underpinning the diverse array of information-sharing and bureaucracy literature are applied to these actions in the context of the Department of Homeland Security’s broader organizational structure.

USCIS took three distinct actions on December 3, 2015 to prevent ICE from obtaining critical homeland security information in a timely manner: (1) USCIS delayed ICE’s entry into the USCIS facility; (2) USCIS prohibited ICE from arresting, detaining, or interviewing anyone in the USCIS facility; and (3) USCIS did not share a tangible copy of Mariya Chernykh's A-file with ICE agents.

1. USCIS delayed ICE’s entry into the USCIS facility.

When five HSI agents dressed in tactical gear arrived at the USCIS facility and stated their official purpose, they should have been granted permission to enter the building immediately. The agents lost invaluable time when FPS and USCIS confined them to the lobby for 15 to 20 minutes. Moreover, the agents lost an additional 10 minutes while they waited to meet with the Field Office Director in the conference room (Roth, 2016). Especially during a fluid investigation, this type of lackadaisical response from USCIS is both inappropriate and potentially dangerous. The seemingly innocuous issue of timeliness is a symptom of bureaucratic inefficiency and must be examined in the context of the situation.

When HSI initially encountered the FPS contract guards and explained their official purpose, the question of authority prompted a chain reaction among USCIS personnel: First, the FPS guard located the Field Office Director and informed her that "HSI agents were looking to obtain information regarding a Russian female and Hispanic male who may have been connected to the shootings the previous day" (Roth, 2016, p. 3). Next, the Field Office Director contacted her superior, the District Director of USCIS in Los Angeles. The District Director then notified her supervisor, the USCIS Regional Director in Laguna Nigel (Roth, 2016). In the meantime, the HSI agents spoke with the FDNS Acting Chief over the telephone.

The inefficiencies highlighted by this lengthy process illustrate how the formal hierarchical structure of bureaucracy can create barriers that frustrate an organization's information-sharing activities (Creed et al., 1996; Tsai, 2002). In bureaucratic organizations, power and authority are centralized in upper management tiers (Hall and Tolbert, 2004; Kim and Lee, 2006; Yang and Maxwell, 2011). This becomes more complicated when we consider how power and authority are centralized in multi-component organizations, such as the Department of Homeland Security. Kim and Lee (2006) argue that centralization can reduce the likelihood that information-sharing occurs because organizational members have limited decision-making authority and must seek approval from upper management tiers before any action is taken. In context of this case study, four individuals were involved in USCIS's decision-making process: the Field Office Director, the District Director, the Regional Director, and the FDNS Acting Chief. A critical element of homeland security information-sharing is timeliness, and the fact that four individuals in four separate USCIS offices were consulted before a decision was made demonstrates that centralization can prolong vertically imposed bureaucratic processes. In the homeland security information-sharing environment, time simply cannot be compromised because lives are often at stake.

To justify her course of action on December 3, 2015, the Field Office Director insisted that she had the explicit authority to regulate who could enter the USCIS facility, including law enforcement personnel (Roth, 2016). Simply, that is factually incorrect—there is no law, regulation, procedure, or policy to support the Field Office Director's claim. Even if the Field Office Director truly believed that she had such authority, what would motivate her to delay ICE's entry during a national security emergency? The theory of reasoned action is widely accepted in social psychology to explain human behavior and can be a useful model to explain information-sharing behaviors in organizations (Davis et al., 1989). The theory of reasoned action assumes that individuals are rational and will make logical use of the information available to them (Fishbein and Ajzen, 1975; Bock and Kim, 2001). Arguably, a rational individual responsible for ensuring "a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016) would make a reasonable effort to assist federal officers during an ongoing terrorism investigation.

That said, the theory of transaction cost economics builds on the theory of reasoned action and introduces the idea that individuals are both rational and self-interested. Even when information-sharing is framed in the context of contributing to a collective good, the decision is ultimately a calculation of the perceived costs and benefits (Jian and Jeffres, 2006; Marks et al., 2008). The Field Office Director's decision to intentionally delay ICE's entry into the USCIS facility indicates that she perceived the cost of information-sharing to be greater than the benefits it would yield. Since information-sharing behaviors are influenced not only by personal motivations but also by contextual forces (Yoo and Torrey, 2002), it is critical to consider how the organizational culture of USCIS, the operational relationship between USCIS and ICE, and other contextual factors may have influenced the Field Office Director's calculation. If we apply the theory of transaction cost economics and the theory of reasoned action in tandem to explain why USCIS would delay ICE's entry, it becomes clear that bureaucratic competition imposes large transaction costs on information-sharing relationships.

2. USCIS prohibited ICE from arresting, detaining, or interviewing anyone in the USCIS facility.

There is considerable evidence to support the claim that USCIS made a concerted, systemic effort to prevent the HSI agents from ensuring "a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016). On more than one occasion, USCIS officials propagated the false narrative that USCIS policy does not permit law enforcement to arrest, detain, or interview individuals on USCIS property

(Roth, 2016). Pursuant to 19 U.S.C. § 1589a, HSI agents may "make an arrest without a warrant for… a felony, cognizable under the laws of the United States committed outside the officer's presence if the officer has reasonable grounds to believe that the person to be arrested has committed or is committing a felony" (19 U.S.C. § 1589). Given the JTTF's notification to ICE of the location of a person of interest in an ongoing terror investigation, HSI had sufficient legal authority to perform law enforcement functions within the USCIS facility.

Importantly, at least two USCIS Directorates and Program Offices intentionally mischaracterized USCIS's policy and procedure to prevent ICE from carrying out its law enforcement authority during a national emergency. In addition to the Field Office Director, the FDNS Acting Chief played a significant role in USCIS's systematic efforts to maintain information asymmetry over ICE. The Acting Chief's role in the events that transpired on December 3, 2015 is particularly damning because he had previously worked for HSI (Roth, 2016). As a former HSI employee, the FDNS Acting Chief should be knowledgeable about, or at least aware of, HSI's law enforcement authorities. In his interview with the OIG, the Acting Chief denied having any role in the information-sharing failure and stated that "he was well aware that USCIS could not supersede HSI law enforcement authority, nor could USCIS provide direction as to how HSI conducted law enforcement operations" (Roth, 2016, p. 4). The Acting Chief's account was not corroborated by anyone else interviewed by the OIG, and we can reasonably conclude that he lied to cover up a decision that he knew was wrong.

Given that FDNS is "USCIS's primary conduit for information-sharing and collaboration with other governmental agencies" ("Privacy Impact Assessment," 2014, p.

2), why would the Acting Chief knowingly prevent ICE from executing its criminal investigative authority to obtain time-sensitive information? The answer to this question is intricately related to the contemporary relationship between FDNS and ICE. FDNS and ICE work together through the framework of the Joint Anti-Fraud Strategy to detect and prevent immigration benefit fraud. Although the Strategy is intended to delineate "USCIS's administrative authority, responsibility, and jurisdiction from ICE's criminal investigative authority" ("Privacy Impact Assessment," 2014, p. 2), the reality is that USCIS is reluctant to cede its comprehensive investigative authority to ICE even for the sake of national security. In Homeland Security Delegation No. 0150.1 paragraph (I), the Secretary of Homeland Security delegated the following authority to USCIS: "Authority to investigate alleged civil and criminal violations of the immigration laws, including but not limited to alleged fraud with respect to applications or determinations within the Bureau of Citizenship and Immigration Services (BCIS) [predecessor to USCIS] and make recommendations for prosecutions or other appropriate action when deemed advisable" ("DHS Delegation No. 0150.1," 2003). Moreover, Congress explicitly authorized USCIS to "to conduct law enforcement and background checks on every applicant, beneficiary, and petitioner" ("Privacy Impact Assessment," 2014, p. 8) in the 2005 Conference Report. In addition to administrative investigations, USCIS clearly has the statutory authority to conduct criminal investigations in furtherance of its fraud detection mission.

Given that USCIS and ICE have overlapping criminal investigative authorities and jurisdictions with regard to immigration benefit fraud, it is unsurprising that the FDNS Acting Chief was unwilling to relinquish USCIS's authority to ICE. Jackson et al.

(2009) argue that bureaucratic competition among agencies operating in the same regulatory environment can reduce the likelihood that individuals will share information. A closer look at the standard operating procedures governing FDNS's fraud investigation process illustrates why formal information-sharing frameworks are not immune to inter-agency competition. *Figure 4* is a simplified flow chart that shows, among other things, where FDNS's administrative investigations intersect with ICE's criminal investigations:

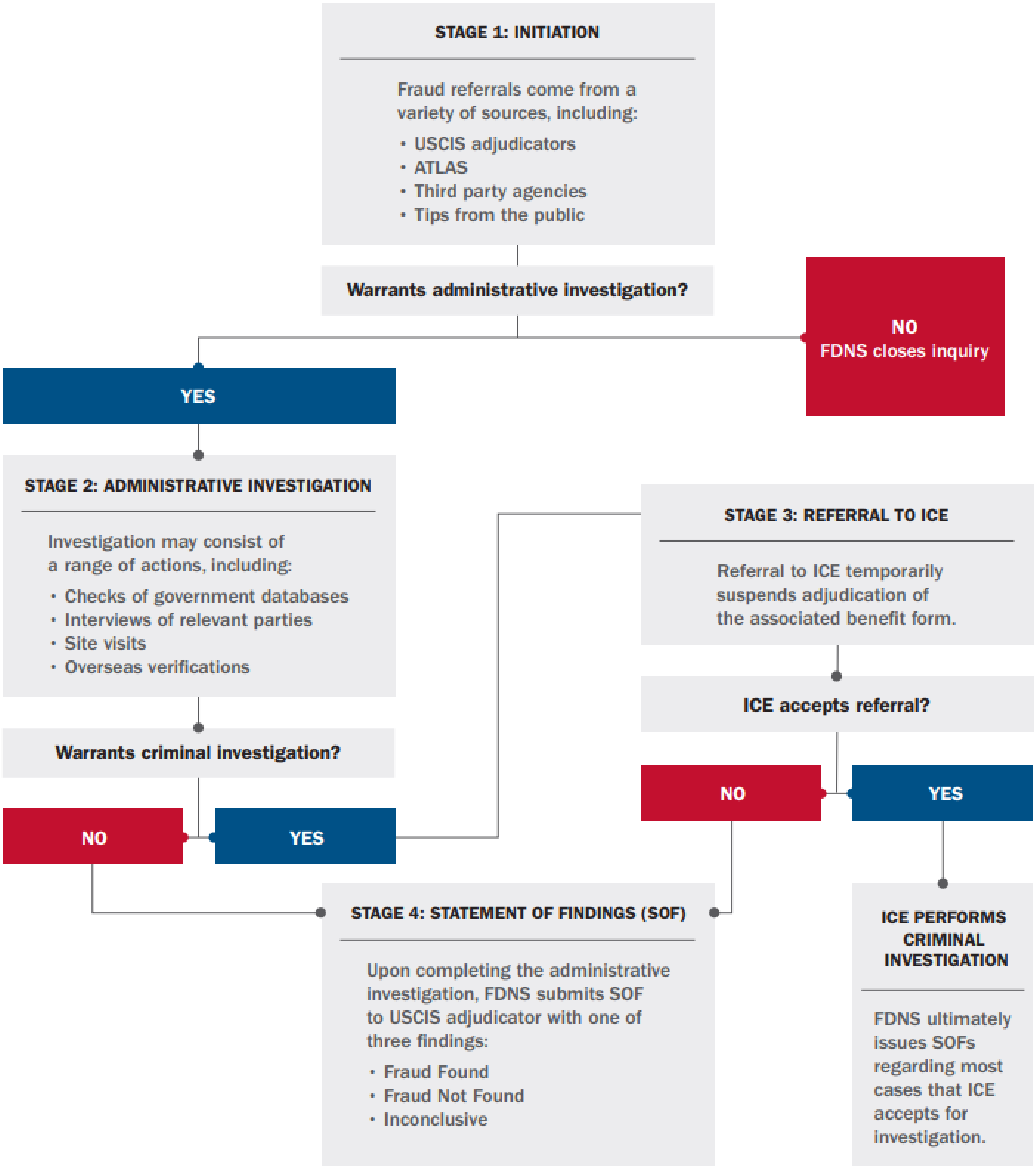

STAGE 1: INITIATION
Fraud referrals come from a variety of sources, including:
• USCIS adjudicators
• ATLAS
• Third party agencies
• Tips from the public
Warrants administrative investigation?
NO
FDNS closes inquiry
YES
STAGE 2: ADMINISTRATIVE INVESTIGATION
Investigation may consist of a range of actions, including:
• Checks of government databases
• Interviews of relevant parties
• Site visits
• Overseas verifications
Warrants criminal investigation?
NO
YES
STAGE 3: REFERRAL TO ICE
Referral to ICE temporarily suspends adjudication of the associated benefit form.
ICE accepts referral?
NO
YES
STAGE 4: STATEMENT OF FINDINGS (SOF)
Upon completing the administrative investigation, FDNS submits SOF to USCIS adjudicator with one of three findings:
• Fraud Found
• Fraud Not Found
• Inconclusive
ICE PERFORMS CRIMINAL INVESTIGATION
FDNS ultimately issues SOFs regarding most cases that ICE accepts for investigation.

Figure 4. FDNS Fraud Investigation Flow Chart (June 28, 2018).
Source: Citizenship and Immigration Services Ombudsman. (2018). Annual Report 2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20%20Annual%20Report%202018.pdf

According to *Figure 4*, if FDNS determines that a fraud referral warrants further investigation, it will initiate an administrative investigation into the implicated case. If FDNS uncovers information during the course of the administrative investigation that justifies a criminal investigation, FDNS refers the case to ICE. The chronology of this process is important because the standard operating procedures "set forth the guidelines for the receipt, documentation, investigation, and recording of the results of investigative action for either criminal investigation referral to ICE or administrative investigation to remain within USCIS" ("The Aftermath of Fraud by Immigration Attorneys," 2012). If FDNS refers a case to ICE for criminal investigation, FDNS must suspend its administrative adjudication of the matter.

In theory, FDNS's administrative investigations should complement (and contrast with) ICE's criminal investigations into suspected immigration benefit fraud. However, in practice, this is not necessarily the case. Dan Cadman, a former INS and ICE official with over 30 years of government experience, recently published an article titled, "Is USCIS Incrementally Recreating the INS?," that provides evidence that USCIS is "quietly building its own investigative corps" (Cadman, 2018). Specifically, Cadman argues that the decentralization of INS's immigration authorities across three separate component agencies catalyzed a power imbalance between USCIS and ICE. The following excerpt from Cadman's article illustrates how the post-INS organizational structure of the Department of Homeland Security fosters competition rather than cooperation between USCIS and ICE:

> The result of stove-piping all three organizations is that USCIS has been unable to actually do much about fraud other than deny applications here and there. The

> agency was left in the unenviable position of having to send referrals to ICE for actual investigation of cases. In the 15 years since the creation of DHS and its organizations, though, ICE has repeatedly shown an unwillingness to accept all but a few referrals, and then only when they appear to constitute large-scale frauds or conspiracies. Of course in the investigative and law enforcement world, sometimes small violations grow into large investigations, but in the absence of anyone to look into the 'small' stuff, that doesn't happen. That ICE expects complex investigative work to be handed to them on a platter defies the logic of bureaucracies, any bureaucracies. Anyone that spends that much effort on something will fight like hell not to give it away (Cadman, 2018).

As a former INS and ICE official, Cadman can credibly comment on the relationship between USCIS and ICE with the advantage of hindsight and personal experience. There are three key points in the above excerpt that provide excellent insight into the organizational cultures of both USCIS and ICE, and perhaps more importantly, that help to explain why USCIS would not be inclined to share information with ICE.

First, Cadman proposes a causal relationship between the disaggregation of the INS and the notion that "USCIS has been unable to actually do much about fraud other than deny applications here and there" (Cadman, 2018). There is merit to this argument, as USCIS must outsource its criminal investigations to agencies with law enforcement authority, such as ICE, in order to accomplish FDNS's fundamental mission. Cadman describes USCIS as being in an "unenviable position" because the agency is relatively powerless to combat serious cases of immigration benefit fraud without its own criminal investigative unit. Furthermore, the importance of the symbiosis of intelligence functions and law enforcement activities in the homeland security effort is highlighted in chapter 2. The same principle applies in this case—splitting the law enforcement functions (criminal investigations) and the intelligence functions (administrative investigations) will lead both agencies fighting the war on terrorism (USCIS and ICE) with one hand tied behind their backs. Former FBI Director Robert Mueller's argument is particularly poignant: "The distinct advantage we gain by having intelligence and law enforcement together would be lost in more layers and greater stovepiping of information" ("Law Enforcement and the Intelligence Community," 2004).

Second, Cadman claims that ICE's reluctance to accept referrals from USCIS fundamentally impairs USCIS's ability to carry out its mission, forcing USCIS to bolster its own investigative capabilities to compensate for ICE's minimal cooperation. FDNS's administrative investigations lay the groundwork for ICE's criminal investigations, which are an integral step in the overarching Joint Anti-Fraud Strategy. Given that ICE has "repeatedly shown an unwillingness to accept all but a few referrals, and then only when they appear to constitute large-scale frauds or conspiracies," (Cadman, 2018) it is unsurprising that USCIS is pursuing other avenues to initiate criminal investigations. From a macro perspective, interagency cooperation is necessary for FDNS, which does not have law enforcement authority, to accomplish its core mission. In theory, the delineated process illustrated by *Figure 4* is designed to ensure consistent detection, documentation, and prevention of immigration benefit fraud ("The Aftermath of Fraud by Immigration Attorneys," 2012). However, in practice, this process is undermined by self-interest. Like all DHS component agencies, ICE has limited resources and is only willing to expend such resources on cases indicating major fraud conspiracies. Furthermore, the chief performance metric used to evaluate HSI's contribution to the overarching ICE mission—"Percent of significant Homeland Security Investigation cases that result in a disruption or dismantlement" ("FY 2017-2019 Annual Performance Report," 2018)—explicitly incentivizes HSI to prioritize large-scale crimes and conspiracies. Fundamentally, HSI's self-interest materially impairs FDNS's ability to "determine whether individuals or organizations filing for immigration benefits pose a threat to national security, public safety, or the integrity of the nation's legal immigration system" ("Fraud Detection and National Security Directorate," 2015).

Third, Cadman offers a compelling explanation for why USCIS would intentionally withhold information from ICE in spite of their necessary partnership. Absent a reliable path to pursue criminal investigations, FDNS began bolstering its own workforce capacity to circumvent ICE's institutional roadblock. Between FY 2012 to FY 2018, FDNS staffing levels grew from 756 authorized positions to 1,548 authorized positions—a nearly 205% spike ("Annual Report 2018," 2018). Additionally, the USCIS Strategic Plan explicitly documents USCIS's intent to strengthen its investigative capabilities. To advance a more systematic approach to mitigating fraud risks, USCIS will "Enhance our technological and analytical capabilities to identify non-obvious relationships and patterns of malfeasance related to immigration benefit fraud and communicate insights to our government partners" ("USCIS Strategic Plan," 2016, p. 5). It is clear that USCIS is seeking to reduce its dependency on ICE by augmenting its own capabilities, indicating that the agency is actively pursuing strategies to make itself more autonomous. The Strategic Plan unambiguously cites USCIS's relationship with ICE under the Joint Anti-Fraud Strategy as a catalyst for this transition, and the Plan specifically confirms that USCIS will “Examine existing models for interagency fraud referrals and explore alternate referral opportunities” (“USCIS Strategic Plan,” 2016, p. 5). Cadman insightfully points out that USCIS’s motivation for advancing its internal investigative capabilities stems from inefficiencies connected to the Department of Homeland Security’s bureaucratic structure: “That ICE expects complex investigative work to be handed to them on a platter defies the logic of bureaucracies, any bureaucracies. Anyone that spends that much effort on something will fight like hell not to give it away” (Cadman, 2018).

The fraught relationship between FDNS and ICE is exacerbated by an organizational structure that arbitrarily separates administrative functions from investigative functions. The complexity inherent in administering and enforcing our nation’s lawful immigration system requires an integrated approach, but the distinct priorities of FDNS and ICE detract from overarching departmental objectives. Moreover, the distinct priorities of FDNS and ICE likely influenced the FDNS Acting Chief’s decision to prohibit ICE from arresting, detaining, or interviewing anyone in the USCIS facility. Considering the fact that FDNS is aggressively bolstering its internal investigative capacity and actively pursuing a strategy to reduce its dependency on ICE, it makes sense that the Acting Chief was unwilling to accommodate HSI’s investigation on December 3, 2015. In the context of information-sharing, the degree to which organizations are dependent on their partners for resources can explain such organization’s willingness to share information (Patnayakuni et al., 2006).

Resource dependence theory acknowledges that organizations are dependent on the external environment for sustained access to resources and therefore act to reduce environmental uncertainty (Pfeffer and Salancik, 1978). In the case of FDNS, we can easily point to its sustained efforts to boost investigative capacity as evidence of its broader strategy to reduce environmental uncertainty. One could also argue that the FDNS Acting Chief prevented HSI from carrying out its law enforcement authorities in an attempt to reduce environmental uncertainty. Because FDNS and ICE operate in overlapping jurisdictions and regulatory environments, they compete for similar resources, such as information and funding. The information-sharing literature acknowledges the connection between resources and power, and scholars contend that owning information within an organization translates to owning power within an organization (Ardichvill et al., 2003; Kolekofski and Heminger, 2003; Marks et al., 2008). More importantly, resource dependence theory suggests that organizations will often attempt to assert control over resources to both reduce others' power and increase their own power over others (Hillman et al., 2009). Arguably, this case study is a premier example of an agency asserting control over resources to maintain a favorable power relationship. On December 3, 2015, the FDNS Acting Chief assumed the unofficial role of information gatekeeper for the express purpose of regulating HSI's access to valuable resources in USCIS's possession. The Acting Chief went so far as to invoke authority he did not have to prevent ICE from gaining a competitive advantage.

The FDNS Acting Chief went to great lengths to preserve USCIS's exclusive access to information about Marquez and Chernykh because information, ultimately, is an important resource and source of power (Pfeffer, 1981). As FDNS continues to fortify its criminal investigative capacity, it will increasingly compete with HSI for power and legitimacy with regard to the Department of Homeland Security's overarching immigration responsibilities. Of all people, the FDNS Acting Chief would be acutely aware of that reality.

3. USCIS did not share a tangible copy of Mariya Chernykh's A-file with ICE agents.

In addition to being denied access to the USCIS facility, the HSI agents were also denied access to Mariya Chernykh's A-file, as well as any other pertinent information about her. The Field Office Director deliberately withheld the A-file from ICE without any legal or procedural reason for doing so. Furthermore, USCIS had previously determined that such law enforcement information-sharing was a “routine use” and thus permissible pursuant to 5 U.S.C. § 552a(b)(7). The OIG concurred and noted that “HSI is, and always has been, able to obtain USCIS immigration files without approval by any particular authority” (Roth, 2016, p. 7). If there was clear precedent indicating that USCIS could share A-files with ICE, why did the San Bernardino terror attack prompt a departure from the norm?

The fact that USCIS and ICE routinely exchange A-files demonstrates that the information-sharing failure that occurred on December 3, 2015 was not due to an innocuous logistical or technological error. Rather, it suggests that the information-sharing failure was a direct result of individual motivations and self-interest. In fact, Chairman Johnson confirmed the influence of individual motivations and self-interest at the highest levels of USCIS hierarchy in the oversight hearing titled, *The Security of U.S. Visa Programs*. Chairman Johnson informed USCIS Director Leon Rodriguez of damning evidence provided by a whistleblower: “By the way, we have been told during the gathering of information process that the decision not to let HSI in came from higher up" ("The Security of U.S. Visa Programs," 2016). When asked to explain the role that USCIS leadership played in the information-sharing failure, Director Rodriguez admitted, "Unfortunately, it all happened so quickly that it was, incorrectly, perceived as our folks trying to, in some way, obstruct what ICE was trying to do" ("The Security of U.S. Visa Programs," 2016). Unconvinced by Director Rodriguez's feeble justification, Chairman Johnson explicitly stated, "It sounds like they were prevented," and ICE Director Sarah Saldaña agreed: "I will say, in all honesty, Senator, that I had a similar reaction when I first heard about the incident" ("The Security of U.S. Visa Programs," 2016). While Director Rodriguez excused the information-sharing failure as a simple error exacerbated by the chaos of the situation, the Chairman of the Homeland Security and Governmental Affairs Committee and the Director of ICE refused to exonerate USCIS leadership on those grounds.

Cress and Kimmerle (2006) posit that information-sharing presents a social dilemma. Social dilemmas are situations where personal interests are inconsistent or incompatible with collective interests. When confronted with a social dilemma, individuals are more likely to prioritize their short-term personal interests than long-term organizational interests (Dawes, 1996; Yang and Maxwell, 2011). If we examine the events that occurred at the IRC through the lens of a social dilemma, we can reasonably conclude that the Field Office Director, the FDNS Acting Chief, and other USCIS employees identified significant costs associated with sharing Chernykh's A-file with ICE. To be clear, USCIS ultimately calculated that such costs outweighed the potential of thwarting an ensuing terror attack. USCIS's willful neglect of its role in ensuring "a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016) in favor of individual interests points to a significant flaw in the Department of Homeland Security's organizational design. Despite the fact that the Department of Homeland Security was specifically designed to encourage information-sharing, there is no institutionalized incentive system to counteract the social dilemma presented by information-sharing.

Many public-sector organizations, such as the Department of Homeland Security, create information as their core product, provide information to the public as their main activity, or employ workers to develop information as their primary responsibility (Starbuck, 1992; Willem and Buelens, 2007). In this environment, the transmission and exchange of information takes on a more transactional role. In spite of the transactional qualities of an information-sharing framework, the issue of ownership presents a challenging problem. Employees create, organize, and amass tangible information goods and services, but organizations ultimately own these products. Moreover, organizations expect employees to extract utility from these products to benefit the organization as a whole (Constant et al., 1994). With respect to Mariya Chernykh's A-file, the information belongs to the Department of Homeland Security and should not have been subject to individual motivations and self-interest. Scholars suggest that the degree to which employees believe in organizational ownership (rather than individual ownership) strongly influences the likelihood that information-sharing occurs (Jarvenpaa and Staples, 2001; Yang and Maxwell, 2011). This case study illuminates how the Department of Homeland Security's organizational structure, which features a complex network of governance, fundamentally undermines the concept of organizational ownership.

The DHS organizational chart depicted in *Figure 3* shows that USCIS employees are governed by two distinct bureaucracies: the USCIS hierarchy and the overarching Department of Homeland Security hierarchy. In terms of chain of command, it is clear that the Secretary of Homeland Security outranks the USCIS Director and is the ultimate authority for all Department and component agency matters. However, most DHS employees rarely interface with Department leadership, are not directly involved in the operations of other component agencies, and do not have a stake in the well-being of other component agencies. In spite of the hierarchical supremacy of the Department's overarching mission and objectives, DHS employees are primarily loyal to the missions and priorities of their respective component agencies.

VIII. Conclusion

In the wake of the devastating terror attacks that occurred on September 11, 2001, President George W. Bush proposed to create the Department of Homeland Security, the most significant transformation of the U.S. government since the 1940s. President Bush recognized that the evolving threat landscape necessitated a more agile, unified government structure that could better protect the homeland and the American people:

> The changing nature of the threats facing America requires a new government structure to protect against invisible enemies that can strike with a wide variety of weapons. Today no one single government agency has homeland security as its primary mission. In fact, responsibilities for homeland security are dispersed among more than 100 different government organizations. America needs a single, unified homeland security structure that will improve protection against

> today's threats and be flexible enough to help meet the unknown threats of the future. (Bush, 2002).

The Department of Homeland Security was explicitly designed to facilitate cooperation and coordination among the numerous government agencies with a stake in the homeland security mission. Moreover, the structure of DHS was intended to reflect the dynamic environment in which it operates. However, since its inception, the Department of Homeland Security has been largely unable to overcome the same problems that both preceded and prompted its creation.

The San Bernardino terror attack is a high-profile case that can be reasonably extrapolated to explain systemic information-sharing challenges within the Department of Homeland Security. In the aftermath of the one of the deadliest terror attacks on U.S. soil since September 11, 2001, USCIS failed to share critical information about a potentially dangerous person of interest with ICE. More importantly, this failure was not merely the result of an administrative error or a technological malfunction. USCIS deliberately withheld information from ICE despite the fact that individuals associated with the person of interest "had committed an atrocity on an unthinkable scale against unarmed innocents" less than 24 hours before (Roth, 2016, p. 6). This case study is illustrative of the ways in which the Department of Homeland Security's organizational structure institutionalizes interagency competition, thereby reinforcing factors that impede and discourage effective information-sharing.

On December 3, 2015, USCIS personnel took three distinct actions to stonewall ICE: (1) USCIS delayed ICE's entry into the USCIS facility; (2) USCIS prohibited ICE from arresting, detaining, or interviewing anyone in the USCIS facility; and (3) USCIS did not share a tangible copy of Mariya Chernykh's A-file with ICE agents. Each of these actions was inconsistent with USCIS policy and procedure, yet each action was sanctioned by a high level USCIS official. In a clear dereliction of duty, the Field Office Director and the FDNS Acting Chief willfully mischaracterized the authorities vested in them by USCIS in pursuit of self-interest. Self-interest, ultimately, is what undermines the unity of effort that the centralization of twenty-two disparate agencies was intended to foster.

This case study illustrates how the Department of Homeland Security's organizational structure creates a disincentive for cross-component collaboration and information-sharing.

CONCLUSION

Chapter 1 determined that the value of information is relative to its user, and that the transfer and exchange of information is a source of competitive advantage in a knowledge economy (Haas and Hansen, 2007). In a knowledge economy, such as the homeland security enterprise, individuals may seek to control information to protect their own self-interests rather than the interests of the organization. Chapter 2 presented a variety of factors—including overlapping missions, interagency competition, and the nexus between performance metrics and budget appropriations—that stymie information-sharing activities among DHS component agencies. These factors are evident in the case study and give credence to the notion that centralization fosters a culture of competition rather than collaboration. Chapter 3 established that DHS employees are primarily loyal to the missions and priorities of their respective component agencies. The Department of Homeland Security's organizational structure institutionalizes interagency competition and sanctions the pursuit of self-interest, thereby creating a disincentive for cross-component collaboration and information-sharing.

The centralized organizational structure of the Department of Homeland Security fundamentally undermines information-sharing efforts among component agencies. Because twenty-one out of twenty-two DHS component agencies predate the creation of the Department of Homeland Security, centralization resulted in a heterogeneous bureaucracy with inconsistent organizational values, organizational priorities, and organizational processes. Centralization also forced component agencies to both retain legacy mandates and adopt broader departmental mandates. In this sense, centralization resulted in twenty-two unique agencies with split loyalties between organizational priorities and departmental responsibilities. Thus, as evidenced by this case study, DHS's centralized organizational structure enables component agencies to pursue their parochial self-interests at the detriment of the Department's overarching mission. Absent an incentive to prioritize departmental objectives over individual interests, component agencies will continue to align resources and information-sharing activities with self-interest. Self-interest ultimately, is what undercuts the unity of effort that the centralization of twenty-two disparate agencies was intended to foster.

Furthermore, because information-sharing presents a social dilemma, self-interest directly impacts a component agency's willingness to share information. When confronted with a social dilemma, individuals are likely to favor short-term personal interests over long-term organizational interests (Dawes, 1996; Yang and Maxwell, 2011). Accordingly, the case study demonstrates how the centralized organizational structure of the Department of Homeland Security is overshadowed by component agency self-interest. USCIS's willful neglect of its role to ensure "a homeland that is safe, secure, and resilient against terrorism and other hazards" ("Our Mission," 2016) in favor of personal interests points to a significant flaw in the Department of Homeland Security's organizational design. Despite the fact that the Department of Homeland Security was specifically designed to encourage information-sharing, there is no institutionalized incentive system to counteract the social dilemma presented by information-sharing. Assuming that individuals are rational and self-interested, even when information-sharing is framed in the context of contributing to a collective good, the decision is ultimately a calculation of the perceived costs and benefits (Jian and Jeffres, 2006; Marks et al., 2008).

Because DHS's success depends on critical relationships with many different federal, state, local, tribal, public, private, and international partners, DHS must develop structures and processes that provide incentives and rewards for collaboration, consultation, and support for implementing key goals. Critical to this whole-of-government approach is the remediation of factors that inhibit effective information-sharing, the establishment of an incentives system to encourage information exchanges, and the adoption of a more fluid intelligence discipline that transmits information to end users more quickly. To conclude, I offer five recommendations to aid in the establishment of an incentives system:

1. Develop Performance Metrics that Measure Inter-Agency Collaboration

The Department of Homeland Security's outcome-centric performance metrics do not adequately capture the extent to which cross-component collaboration and information-sharing efforts are successful. The relative success of information-sharing endeavors cannot be measured simply by the successful transmission of information across organizational boundaries; it is also important to assess whether the information is absorbed and utilized effectively within the organization that acquired it (Jackson, 2014; Yang and Maxwell, 2011). To incentivize inter- and intra-organizational information-sharing, the Secretary of Homeland Security should create metrics for each component agency that measure the degree to which inter-agency collaboration solves major problems. The Secretary should seek to emulate the information-sharing metrics that govern the three DHS JTFs because such performance measures are "intended to better reflect the JTFs' coordination activities and contributions" ("Drug Control: Certain DOD and DHS Joint Task Forces Should Enhance Their Performance Measures to Better Assess Counterdrug Activities," 2019, p. 25).

DHS JTF performance metrics have evolved significantly since FY 2017 to prioritize "strategic-level coordination" among component agencies and no longer focus on outcome-centric activities, "such as the amounts of drugs seized, arrests made, and currency seized" ("Drug Control: Certain DOD and DHS Joint Task Forces Should Enhance Their Performance Measures to Better Assess Counterdrug Activities," 2019, p. 25). Moreover, the evolution of JTF information-sharing measures critically addressed the self-interest and personal motivations that otherwise guide component agency activities: "For example, a new JTF performance measure developed for fiscal year 2018 included the number of leads that the JTFs provided to a partner law enforcement agency, DHS component, or foreign government partner for interdiction or investigative action." The following DHS JTF FY 2018 metrics should be used as guidance for broader DHS applicability:

- Number of operations executed against TCOs with assistance or coordination limited to DHS components
- Number of joint intelligence products initiated or enhanced in alignment with the JTF operational priorities
- Number of supportive efforts provided to or in response to a partner agency, component, or foreign partner that are for awareness only
- Number of supportive efforts provided to a partner agency, component, or foreign partner that are for interdiction or investigative action

- Number of individuals who satisfactorily completed a joint training event provided by their respective JTF
- Number of marketing efforts provided to stakeholders regarding JTF capabilities, capacities, or processes for awareness, collaboration, cooperation, and relationship building ("Drug Control: Certain DOD and DHS Joint Task Forces Should Enhance Their Performance Measures to Better Assess Counterdrug Activities," 2019, p. 26).

By assigning performance value to inter-agency information-sharing processes, information-sharing will become an activity that correlates directly with broader organizational success. Furthermore, "Task force officials reported that the task forces coordinated effectively with each other when they had shared purposes and overlapping or shared geographical boundaries. Because outcome-centric evaluation measures place a disproportionate emphasis on the products of information-sharing and largely ignore the processes that yielded the successful transfer (Yi, 2009; Huysman and de Wit, 2002), the DHS JTF performance metrics quantify inter-agency collaboration as the desired outcome.

2. Foster a Cooperative and Social Work Environment

The degree to which an individual views his or her relationship with colleagues as cooperative or competitive can significantly influence information-sharing behaviors. Steinel, Utz, and Koning (2010) compared the impacts of incentives based on group-performance and incentives based on individual performance. They determined that cooperatively motivated individuals were more likely to share information with others and competitively motivated individuals were more likely to withhold information from others. Ultimately, cooperative work environments and cooperative interpersonal relationships incentivize reciprocal information-sharing behaviors. Recent studies suggest that information-sharing between organizations is heavily influenced by good inter-organizational relationships based on core features like trust, commitment and shared vision (Li and Lin, 2006).

Moreover, in addition to cooperation, scholars have noted the importance of social relationships as a motivational mechanism (Kim and Lee, 2006; Reagans and McEvily, 2003). Interpersonal interactions are thought to have an indirect influence on individual motivation to share and receive information (Geen, 1991). Information-sharing is a fundamentally social process, and individuals engaging in information exchanges are likely to be motivated by social factors that emerge from the process and relationship. Specifically, several researchers found that social networks help to generate positive attitudes about the sharing of information and knowledge within an organization. (Kim and Lee, 2006; Kolekofski and Heminger, 2003; Reagans and McEvily, 2003). Highly social work environments bolster the relationships needed to motivate people to engage in helping and sharing behavior (Smith and McKeen).

3. Integrate Standard Operating Procedures

Processes, best practices, and standard operating procedures are key pillars of an organization’s culture, and incorporating information-sharing into such routines can help solidify its role in the organization. Supplementing these processes with metrics that evaluate information-sharing efficacy can also motivate employees to prioritize collaborative behavior. Standard operating procedures reflect organizational values, and embedding the importance of information-sharing in routine business practices can promote collaborative behaviors in both the organizational culture and the workplace (Smith and McKeen). Training is another avenue by which the value of information-sharing can be emphasized. If employees are taught the appropriate protocols and understand the behaviors that are expected of them, they will be more motivated to replicate the behavior (Smith and McKeen).

4. Focus on Culture

Organizational culture is an effective motivator because it can powerfully influence human behavior (Smith and McKeen). Work environments that integrate information-sharing into functional culture will provide platforms for individual growth as well as organizational growth. When an organizational culture promotes fairness, affiliation, and innovation, it can positively influence an individual's intentions to share information (Bock et al., 2005). Moreover, organizational culture is intimately related to social networks, as social interactions can influence or drive changes in organizational culture (Smith and McKeen). Organizational culture also shapes the degree to which information-sharing resonates in the hearts and minds of people in the organization (Smith and McKeen). Concerted efforts to develop new organizational culture mechanisms can also foster greater information-sharing capacity. Fundamentally, if the organizational culture embraces information-sharing as a central activity, individuals will be more likely to engage in such activities. To incentivize people to change their behavior, the organizational culture must offer a compelling vision of how information-sharing will improve the future (Smith and McKeen).

5. Embolden Managers to be Motivators

Motivating staff is a daunting task, but a concerted effort to influence mid-level managers can help transform organizational cultures. Managers play a critical role in stimulating and sustaining information-sharing activities (Smith and McKeen). Moreover, managers have a considerable amount of influence within their respective organizations and are in positions to modify organizational processes. Motivating mid-level managers to share information can function as a force multiplier because employees look to managers to lead by example. Additionally, managers are in an optimal position within the organization to recognize subordinates for exhibiting good information-sharing behavior. Managers' opinions have significant value, and consistent communication from managers about the impact that information-sharing activities have on organizational performance will motivate employees to continue to prioritize such behaviors.

Structural reform alone is insufficient—the Department of Homeland Security must supplement its centralized organizational structure with an incentives system to promote effective, timely, and generous information-sharing among component agencies. Importantly, the incentives system must be embedded within each component agency's standard processes and procedures to ensure that information-sharing is engrained in each agency's organizational culture. Because the institutional features of the U.S. federal government, such as regulations, oversight mechanisms, and organizational cultures, are intended to frustrate cross-component information-sharing efforts, the Department of Homeland Security must overhaul these institutional features to incentivize collaborative activities. By developing performance metrics that measure inter-agency collaboration, fostering a cooperative and social work environment, integrating standard operating procedures, focusing on culture, and emboldening managers to be motivators, DHS leadership can counteract the powerful influence that self-interest has on component objectives. As evidenced by this paper, self-interest, ultimately, is what undercuts the unity of effort that the centralization of twenty-two disparate agencies was intended to foster.

If the Department of Homeland Security's centralized organizational structure is supplemented with an incentives system that encourages components to prioritize departmental objectives over individual interests, the Department's information-sharing capacity will become one of its greatest assets. The key to a "single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future" (Bush, 2002) is unencumbered information-sharing among Department of Homeland Security component agencies.

WORKS CITED

Abba, M., Yahaya, L., & Suleiman, N. (2018) Explored and Critique of Contingency Theory for Management Accounting Research. *Journal of Accounting and Financial Management ISSN*, *4*(5), 40-50.

Ardichvill, A., Page, V., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge sharing communities or practice. *Journal of Knowledge Management*, *7*(1), 64−77.

Argote, L. (1999). *Organizational Learning: Creating, Retaining & Transferring Knowledge*. Norwell, MA: Kluwer Academic Publishers.

Argote, L., McEvily, B., & Reagans, R. (2003). Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes. *Management Science*, *49*(4), v-582.

Argote, L. & Ingram, P. (2000). Knowledge Transfer: A Basis for Competitive Advantage in Firms. *Organizational Behavior and Human Decision Processes*, *82*(1), 150-169.

Argote, L., Ingram, P., Levine, J. M., & Moreland, R. L. (2000). Knowledge transfer in organizations: Learning from the experience of others. *Organizational Behavior and Human Decision Processes*, *82*(1), 1-8.

Atabakhsh, H., Larson, C., Petersen, T., Violette, C., & Chen, H. (2004). Information sharing and collaboration policies within government agencies. In *International Conference on Intelligence and Security Informatics* (pp. 467-475). Tucson, AZ: Springer, Berlin, Heidelberg.

Ballou, D., Madnick, S., & Wang, R. (2003). Special Section: Assuring Information Quality. *Journal of Management Information Systems, 20*(3), 9-11.

Bansemer, J. (2006). *Intelligence Reform: A Question of Balance*. Air University Press, 107-138.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120.

Barney, J. B., Ketchen Jr., D. J., & Wright, M. (2011). The future of resource-based theory: revitalization or decline?. *Journal of Management*, *37*(5), 1299-1315.

Bastian, H., & Andreas, W. (2012). A Bibliometric View on the Use of Contingency Theory in Project Management Research. *Project Management Journal*, *43*(3), 4-23.

Bimfort, M. T. (1958). A Definition of Intelligence. *Studies in Intelligence*, *2*(4), 75-78.

Birkenshaw, J., Nobel, R., & Ridderstrale, J. (2002). Knowledge as a Contingency Variable: Do the Characteristics of Knowledge Predict Organization Structure?. *Organizational Science*, *13*(3), 274-289.

Blau, P. M. (1964). *Exchange and power in social life*. New York: John Wiley.

Bock, G. W., & Kim, Y. G. (2001). Breaking the Myths of Rewards: An Exploratory Study of Attitudes about Knowledge Sharing. *Pacific Asia Conference on Information Systems 2001 Proceedings*, 1112-1125.

Bock, G. W., Zmud, R. W., Kim, Y. G., & Lee, J.N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social–psycho- logical forces, and organizational climate. *MIS Quarterly*, *29*(1), 87−111.

Brazelton, J., & Gorry, G. A. (2003). Creating a knowledge-sharing community: if you build it, will they come?. *Communications of the ACM*, *46*(2), 23-25.

Bush, G. W. (2002). The Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/book_0.pdf

Buttermann, G., Germain, R., & Iyer, K. N. (2008). Contingency theory “fit” as gestalt: An application to supply chain management. *Transportation Research Part E: Logistics and Transportation Review*, *44*(6), 955-969.

Carafano J. J., & Heyman, D. (2004) *DHS 2.0: Rethinking the Department of Homeland Security*. Washington, DC: The Heritage Foundation.

Caridi, M., Crippa, L., Perego, A., Sianesi, A., & Tumino, A. (2010). Do virtuality and complexity affect supply chain visibility?. *International Journal of Production Economics*, *127*(2), 372-383.

Caudle, S. (2005). Homeland Security: Approaches to Results Management. *Public Performance & Management Review*, *28*(3), 352-375.

Chang, H. H., & Chuang, S. S. (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. *Information & Management*, *48*(1), 9-18.

Chau, M., Atabakhsh, H., Zeng, D., & Chen, H. (2001). Building an infrastructure for law enforcement information sharing and collaboration: Design issues and challenges. *Paper presented at the National Conference on Digital Government*.

Chen, Z., Gangopadhyay, A., Holden, S. H., Karabatis, G., & McGuire, M. P. (2007). Semantic integration of government data for water quality management. *Government Information Quarterly*, *24*(4), 716-735.

Chertoff, M. (2005). U.S. Department of Homeland Security Second Stage Review Remarks. Ronald Reagan Building, Washington, DC. Retrieved from http://www.dhs.gov/dhspublic/display?theme=44&content=4597&print=true

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & Management*, *45*(7), 458-465.

Cilluffo, F. J., Marks, R. A., & Salmoiraghi, G. C. (2002). The Use and Limits of U.S. Intelligence. *The Washington Quarterly, 25*(1), 61-74.

Clark, R. M. (2017). *Intelligence Analysis: A Target-Centric Approach*. Thousand Oaks, CA: Sage Publications.

Cohen, D., & Prusak, L. (2001). *In Good Company: How Social Capital Makes Organizations Work*. Boston, MA: Harvard Business School Press.

Cohen, D. K., Cuéllar, M. F., & Weingast, B. R. (2006). Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates. *Stanford Law Review*, *59*(3), 673-759.

Complaint, United States of America v. Enrique Marquez Jr., No. 5:15mJ498 (C.D. Cal., filed on Dec. 17, 2015)

Conrad, J. M. (1980). Quasi-option value and the expected value of information. *The Quarterly Journal of Economics*, *94*(4), 813-820.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's Mine Is Ours, or Is It? A Study of Attitudes about Information Sharing. *Information Systems Research, 5*(4), 400-421.

Cook, K. S., & Emerson, R. M. (1978). Power, Equity and Commitment in Exchange Networks. *American Sociological Review*, *43*(5), 721-739.

Creed, W., Douglas, E., & Miles, R. (1996). Trust in Organizations: A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls. In R. M. Kramer, & T. R. Tyler (Eds.), *Trust in Organizations: Frontiers of Theory and Research* (pp. 16-38). Thousand Oaks, CA: Sage Publications.

Cress, U., & Kimmerle, J. (2006). Information exchange with shared database as a social dilemma: The effect of metaknowledge, bonus systems, and costs. *Communication Research*, *33*(5), 370−390.

Davenport, T. H. (1996). Some principles of knowledge management. *Strategy & Business*, *1*(2), 34-40.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982-1003.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management*, *15*(3), 377−394.

Dierickx, I., & Cool, K. (1989). Asset stock accumulation and sustainability of competitive advantage. *Management Science*, *35*(12), 1504-1511.

Donaldson, L. (2001). *The contingency theory of organizations*. Thousand Oaks, CA: Sage Publications.

Donaldson, L. (2006). The contingency theory of organizational design: Challenges and opportunities. In Burton, R. M., Håkonsson, D. D., Eriksen, B., & Snow, C. C. (Eds.) *Organization Design* (pp. 19-40). Boston, MA: Springer.

Draaijer, R. (2008). *Why Share? An empirical investigation of knowledge contribution within electronic networks of practice.* The Netherlands: University of Twente Enschede.

Drake, D. B., Steckler, N. A., & Koch, M. J. (2004). Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures. *Social Science Computer Review*, *22*(1), 67-84.

Dulles, A. (2006). *The Craft of Intelligence*. Guilford: The Lyons Press.

Falkenrath, R. A. (2001). Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack. *International Security*, *25*(4), 147-186.

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2007). A collaborative network for first responders: Lessons from the CapWIN case. *Government Information Quarterly*, *24*(4), 785-807.

Feldman, M., & March, J. (1981). Information in Organizations as Signal and Symbol. *Administrative Science Quarterly, 26*(2), 171-186.

Felli, J. C., & Hazen, G. B. (1997). Sensitivity analysis and the expected value of perfect information. *Medical Decision Making*, *18*(1), 95-109.

Feltham, G. A. (1968). The value of information. *The Accounting Review*, *43*(4), 684-696.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An Introduction to Theory and Research*. Reading, MA: Addison Wesley.

Flynn, B. B., Huo, B., & Zhao, X. (2010). The impact of supply chain integration on performance: A contingency and configuration approach. *Journal of Operations Management*, *28*(1), 58-71.

Fountain, J. (2013). *Implementing Cross-Agency Collaboration: A Guide for Federal Managers*. Washington, DC: IBM Center for the Business of Government.

Fraud Detection and National Security Directorate. (2014). Privacy Impact Assessment. DHS/USCIS/PIA-013-01. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdns-november2016_0.pdf

Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, *4*(3), 28-36.

Ganor, B. (2005). *The Counter-Terrorism Puzzle: A Guide for Decision Makers*. New York, NY: Transaction Publishers.

Geen, R. G. (1991). Social motivation. *Annual Review of Psychology*, *42*(1), 377-399.

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems*, *16*(2), 121−133.

Gil-Garcia, J. R., Chun, S., & Janssen, M. (2009). Government information sharing and integration: Combining the social and the technical. *Information Polity*, *14*(1/2), 1-10.

Gil-García, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly*, *22*(2), 187-216.

Graham, J. L. (1988). Deference given the buyer: Variations across twelve cultures. *Cooperative Strategies in International Business*, 473-85.

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology*, *91*(3), 481-510.

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109-122.

Grover, V., & Saeed, K. A. (2007). The impact of product, market, and relationship characteristics on interorganizational system integration in manufacturer-supplier dyads. *Journal of Management Information Systems*, *23*(4), 185-216.

Haas, M. R. & Hansen, M. T. (2007). Different knowledge, different benefits: Toward a productivity perspective on knowledge sharing in organizations. *Strategic Management Journal*, *28*(11), 33–53.

Hall, R. H., & Tolbert, P. S. (2004). *Organizations: Structures, Processes, and Outcomes* (9th ed). New York: Prentice Hall.

Hattem, J. (2016). Homeland Security field office failed in San Bernardino aftermath, says report. *The Hill*. Retrieved from https://thehill.com/policy/national-security/282091-watchdog-report-finds-fault-in-aftermath-of-san-bernardino-shooting

Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource Dependence Theory: A Review. *Journal of Management*, *35*(6), 1404-1427.

Howitt, A. M., & Pangi, R. L. (2003). *Countering Terrorism: Dimensions of Preparedness*. Cambridge, MA: Massachusetts Institute of Technology Press.

Hung, Y. C., & Chuang, Y. H. (2009). Factors affecting knowledge sharing behavior: a content analysis of empirical findings. In *International Conference of Pacific Rim Management, July*.

Huysman, M. H., & de Wit, D. H. (2002). *Knowledge Sharing in Practice*. Norwell, MA: Kluwer Academic Publishers.

Information. Def. 1. (n.d.). In *Oxford English dictionary*. Retrieved from https://en.oxforddictionaries.com/definition/information

Jackson, B. A. (2014). *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts*. Santa Monica, CA: Rand Corporation.

Jackson, B. A., Noricks, D., & Goldsmith, B.W. (2009). Current Domestic Intelligence Efforts in the United States. In Schaefer, A. G., Noricks D., Goldsmith B. W., Lester G., Goulka J., Wermuth M. A., Libicki, M. C., & Howell, D. R. (Eds.), *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency* (pp. 49-78). Santa Monica, CA: RAND Corporation.

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems*, *18*(1), 151−183.

Jenkins, W. O. (2006). Collaboration over Adaptation: The Case for Interoperable Communications in Homeland Security. *Public Administration Review, 66*(3), 319-321.

Jian, G., & Jeffres, L. (2006). Understanding Employees' Willingness to Contribute to Shared Electronic Databases. *Communication Research*, *33*(4), 1-20.

Johnson, J. (2014). Memorandum for DHS Leadership: Southern Border and Approaches Campaign. Retrieved from https://www.dhs.gov/sites/default/files/publications/14_1120_memo_southern_border_campaign_plan.pdf

Jolaee, A., Nor, K., Khani, N., & Mdyusoff, R. (2014). Factors affecting knowledge sharing intention among academic staff. *International Journal of Educational Management*, *28*(4), 413-431.

Jones, G. R. (1983) Transaction costs, property rights and organizational culture: An exchange perspective. *Administrative Science Quarterly*, *28*, 454-467.

Kankanhalli, A., Tan, B., & Wei, K. (2005). Contributing Knowledge to Electronic Knowledge Repositories: An Empirical Investigation. *MIS Quarterly, 29*(1), 113-143.

Keller, K., Yeung, D., Baiocchi, D., & Welser, W. (2013). Barriers to Information Sharing. In *Facilitating Information Sharing Across the International Space Community: Lessons from Behavioral Science*, 3-10.

Kelley, H. H., & Thibaut J. W. (1978). *Interpersonal Relations: A Theory of Interdependence*. New York: John Wiley & Sons.

Kellogg, K. C., Orlikowski, W. J., & Yates, J. (2006). Life in the trading zone: Structuring coordination across boundaries in postbureaucratic organizations. *Organization Science*, *17*(1), 22-44.

Kembro, J., Selviaridis, K., & Näslund, D. (2014). Theoretical perspectives on information sharing in supply chains: A systematic literature review and conceptual framework. *Supply Chain Management: An International Journal*, *19*(5/6), 609-625.

Kim, Y. B., & Lee, B. H. (1995). R and D project team climate and team performance in Korea. *R and D Management*, *25*(2), 179-196.

Kim, S., & Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review*, *66*(3), 370−385.

Kim, S., Cavusgil, T., & Cantalone, R. J. (2006). Information System Innovations and Supply Chain Management: Channel Relationships and Firm Performance. *Journal of the Academy of Marketing Science*, *34*(1), 40-54.

Klein R., Raj, A. & Straub, D.W. (2007). Competitive and cooperative positioning in supply chain logistics relationships. *Decision Sciences*, *38*(4), 611-646.

Klischewski, R., & Scholl, H. J. J. (2006). Information quality as a common ground for key players in e-government integration and interoperability. *Paper presented at the Hawaii International Conference on System Sciences (HICSS-37)*, Hawaii.

Klischewski, R., & Scholl, H. J. (2008). Information quality as capstone in negotiating e-Government integration, interoperation and information sharing. *Electronic Government, an International Journal*, *5*(2), 203−225.

Kogut, B. (2000). The network as knowledge: Generative rules and the emergence of structure. *Strategic Management Journal*, *21*(3), 405-425.

Kogut, B., & Zander, U. (1992). Knowledge of the Firm, Integration Capabilities and the Replication of Technology. *Organization Science*, 3, 383-397.

Kogut, B., & Zander, U. (1996). What firms do? Coordination, identity, and learning. *Organization Science*, *7*(5), 502-518.

Kolekofski, K. E., Jr., & Heminger, A. R. (2003). Beliefs and attitudes affecting intentions to share information in an organizational setting. *Information Management*, *40*, 521−532.

Koys, D. J., & Decotiis, T. A. (1991). Inductive measures of psychological climate. *Human Relation*, *44*(3), 265-285.

Kraemer, K. L., & King, J. L. (1986). Computing and public organizations. *Public Administration Review*, *46*(Special Issue: Public Management Information Systems), 488-496.

Krause, G. A., & Douglas, J. W. (2005). Institutional design versus reputational effects on bureaucratic performance: Evidence from US government macroeconomic and fiscal projections. *Journal of Public Administration Research and Theory*, *15*(2), 281-306.

Kuo, F., & Young, M. (2008). Study of the intention-action gap in knowledge sharing practices. *Journal of the American Society for Information Science and Technology*, *59*(8), 1224-1237.

Kurland, N. B. (1995). Ethical intentions and the theories of reasoned action and planned behaviour. *Journal of Applied Social Psychology*, *25*(4), 297-313.

Lam, W. (2005). Barriers to e-Government integration. *Journal of Enterprise Information Management*, *18*(5/6), 511−530.

Landsbergen Jr, D., & Wolken Jr, G. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. *Public Administration Review*, *61*(2), 206-220.

Lavie, D. (2006). The competitive advantage of interconnected firms: An extension of the resource-based view. *Academy of Management Review*, *31*(3), 638-658.

Lawrence, P. R., & Lorsch, J. W. (1986). Organization and environment: Managing differentiation and integration (Harvard Business School Classics).

Laux, D., & Pezzullo, R. (2016). *Left of Boom: How a Young CIA Case Officer Penetrated the Taliban and al-Qaeda*. New York, NY: St. Martin's Press.

Law Enforcement and the Intelligence Community: Hearing before the National Commission on Terrorist Attacks Upon the United States (2004) (Testimony of the Honorable Robert Mueller).

Lesser, E. L., & Storck, J. (2001). Communities of practice and organizational performance. *IBM Systems Journal*, *40*(4), 831-841.

Li, S., & Lin, B. (2006). Accessing Information Sharing and Information Quality in Supply Chain Management. *Decision Support Systems*, *42*(3), 1641-1656.

Lowenthal, M. (2006). *Intelligence: From Secrets to Policy* (3rd ed.). United States: CQ Press.

Mahoney, J. T., & Pandian, J. R. (1992). The resource-based view within the conversation of strategic management. *Strategic Management Journal*, *13*(5), 363-380.

Mäkelä, K. (2007). Knowledge Sharing through Expatriate Relationships: A Social Capital Perspective. *International Studies of Management & Organization*, *37*(3), 108-125.

Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005, and for Other Purposes, Conference Report to accompany H.R. 4567, Report No. 108-774 (2004).

Marchand, D. (1990). Infotrends: A 1990s Outlook on Strategic Information Management. *Information Management Review*, *5*(4), 23-32.

Marks, P., Polak, P., McCoy, S., & Galletta, D. (2008). Sharing Knowledge. *Communications of the ACM*, *51*(2), 60−65.

Marks, R. A. (2010). *Spying in America in the Post 9/11 World: Domestic Threat and the Need for Change.* Santa Barbara, CA: Praeger.

Marshall, C. C., & Bly, S. (2004, June). Sharing encountered information: Digital libraries get a social life. In *Proceedings of the 4th ACM/IEEE-CS Joint Conference on Digital libraries* (pp. 218-227). ACM.

Mathieson, K. (1991). Predicting user intentions, comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173-191.

McCarthy, J. (1956). Measures of the value of information. *Proceedings of the National Academy of Sciences*, *42*(9), 654-655.

Nahapiet, J., & Ghoshal, S. (1998). Social Capital, Intellectual Capital, and the Organizational Advantage. *Academy of Management Review*, *23*(2), 242-266.

Nonaka, I., & Konno, N. (1998). The concept of "Ba": Building a foundation for knowledge creation. *California Management Review*, *40*(3), 40-54.

Nonaka, I., & Takeuchi, H. (1995). *The Knowledge Creating Company*. New York: Oxford University Press.

Nyaga, G.N., Whipple, J. M., & Lynch, D. F. (2010). Examining supply chain relationships: Do buyer and supplier perspectives on collaborative relationships differ?. *Journal of Operations Management*, *28*(2), 101-114.

Office of the Director of National Intelligence. (2016). Fiscal Year 2016 Annual Report on Security Clearance Determinations. Retrieved from https://www.odni.gov/files/documents/Newsroom/FY16-Report-Security-Clearance-Determinations-PubRelease-20171017.pdf

Office of the Director of National Intelligence. (n.d.). What is intelligence?. Retrieved from https://www.dni.gov/index.php/what-we-do/what-is-intelligence

Pardo, T. A., Cresswell, A. M., Dawes, S. S., & Burke, G. B. (2004). Modeling the social & technical processes of interorganizational information integration. *Paper presented at the Hawaii International Conference on System Sciences (HICSS-37)*, Hawaii.

Pardo, T., & Tayi, G. (2007). Interorganizational information integration: A key enabler for digital government. *Government Information Quarterly*, *24*(4), 691-715.

Patnayakuni, R., Rai, A., & Seth, N. (2006). Relational antecedents of information flow integration for supply chain coordination. *Journal of Management Information Systems*, *23*(1), 13-50.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behaviour. *MIS Quarterly*, *30*(1) 115-143.

Patnayakuni, R., Rai, A., & Seth, N. (2006). Relational antecedents of information flow integration for supply chain coordination. *Journal of Management Information Systems*, *23*(1), 13-50.

Peled, A. (2014). *Traversing digital Babel: Information, e-government, and exchange*. Cambridge, MA: Massachusetts Institute of Technology Press.

Perrow, C. (1981). Markets, hierarchies and hegemony: A Critique of Chandler and Williamson. In A. Van de Ven & J. Joyce (Eds.) *Perspectives in Organisation Design and Behaviour* (pp. 371-386). New York: Wiley.

Persson, G. (1978). Organisation design strategies for business logistics. *International Journal of Physical Distribution & Materials Management*, *8*(6), 287-297.

Persson, G. (1995). Logistics process redesign: Some useful insights. *The International Journal of Logistics Management*, *6*(1), 13-26.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: a resource-based view. *Strategic Management Journal*, *14*(3), 179-191.

Pfeffer, J. (1987). A resource dependence perspective on interorganizational relations. In M. S. Mizruchi, & M. Schwartz (Eds.), *Intercorporate relations: The structural analysis of business* (22-55). Cambridge, UK: Cambridge University Press.

Pfeffer, J. (1981). *Power in organizations*. Boston, MA: Putnam.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence approach*. New York: Harper and Row Publishers.

Phythian, M., & Gill, P. (2006). *Intelligence in an Insecure World*. Cambridge, MA: Polity Press.

Piderit, R., Flowerday, S., & Von Solms, R. (2011). Enabling information sharing by establishing trust in supply chains: A case study in the South African automotive industry. *South African Journal of Information Management*, *13*(1), 1-8.

Plea Agreement for Defendant Enrique Marquez, Jr., United States of America v. Enrique Marquez Jr., No. 5:15mJ498 (C.D. Cal., filed on Feb. 14, 2017).

Polanyi, M. (1966). *The Tacit Dimension*. Chicago, IL: The University of Chicago Press.

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, *63*(4), 149-152.

Porterfield, T. E., Bailey, J. P. & Evers, P. T. (2010). B2B eCommerce: an empirical investigation of information exchange and firm performance. *International Journal of Physical Distribution & Logistics Management*, *40*(6), 435-455.

Powell, W. W., Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational Collaboration and the Locus of Innovation: Networks of Learning in Biotechnology. *Administrative Science Quarterly*, *41*(1), 116-145.

Quigley, N. R., Tesluk, P. E., Locke, E. A., & Kathryn M. (2007). A Multilevel Investigation of the Motivational Mechanisms Underlying Knowledge Sharing and Performance. *Organization Science*, *18*(1), 71-88.

Ramanujam, V., & Varadarajan, P. (1989). Research on corporate diversification: A synthesis. *Strategic Management Journal*, *10*(6), 523-551.

Reagans, R., & McEvily, B. (2003). Network structure and knowledge transfer: The effects of cohesion and range. *Administrative Science Quarterly*, *48*(2), 240−267.

Ring, P. S., & Perry, J. L. (1985). Strategic management in public and private organizations: Implications of distinctive contexts and constraints. *Academy of Management Review*, *10*(2), 267−287.

Roth, J. (2016). December 3, 2015 – San Bernardino Incident Memorandum. Retrieved from https://www.oig.dhs.gov/assets/Mga/OIG-mga-060116.pdf

Roth, J. (2017). DHS Needs a More Unified Approach to Immigration Enforcement and Administration. Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-07-Oct17.pdf

Sanchez, R., & Heene, A. (1997). *Strategic Learning and Knowledge Management*. Chichester, England: John Wiley.

Schneider, A., & Ingram, H. (1990). Behavioral assumptions of policy tools. *The Journal of Politics*, *52*(2), 510-529.

Scholl, H. J. (1999). Knowledge management and the vital organization. In R. Berndt (Ed.), *Management Strategien 2000*. Berlin, Germany: Springer.

Skinner, R. L. (2007). Review of the USCIS Benefit Fraud Referral Process. Retrieved from file:///C:/Users/arosen/Downloads/481729%20(1).pdf

Smith, H. A., & McKeen, J. D. (2003). Instilling a knowledge-sharing culture. *Queen's Centre for Knowledge-Based Enterprises*, *20*(1), 1-17.

Spender, J.C. (1996). Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal*, *17*(S2), 45-62.

Starbuck, W. (1992). Learning by Knowledge-Intensive Firms. *Journal of Management Studies*, *29*(6), 713-740.

Steiner, J. E. (2015). *Homeland Security Intelligence*. Thousand Oaks, CA: Sage Publications.

Stenmark, D. (2002). Information vs. knowledge: The role of Intranets in knowledge management. *Paper presented at the Hawaii International Conference on System Sciences (HICSS-35), Big Island, Hawaii.*

Stock, G. N., Greis, N. P., & Kasarda, J. D. (2000). Enterprise logistics and supply chain structure: The role of fit. *Journal of Operations Management*, *18*(5), 531-547.

Szulanski, G. (2000). The Process of Knowledge Transfer: A Diachronic Analysis of Stickiness. *Organizational Behavior and Human Decision Processes, 82*(1), 9-27.

Tan, K. C., Kannan, V. R., Hsu, C. C., & Keong G. L. (2010) Supply chain information and relational alignments: Mediators of EDI on firm performance. *International Journal of Physical Distribution & Logistics Management*, *40*(5), 377-394.

Teece, D. (1998). Capturing Value from Knowledge Assets: The New Economy, Markets for Know-How, and Intangible Assets. *California Management Review*, *40*(3), 55-79.

The Aftermath of Fraud by Immigration Attorneys, House of Representatives, 112th Cong. (2012) (Testimony of Sarah Kendall)

The Department of Homeland Security Appropriations: Hearing before the Committee on Appropriations, House of Representatives, 109th Cong. (2005)

The Security of U.S. Visa Programs: Hearing before the Committee on Homeland Security and Government Affairs, Senate, 114th Cong. 13 (2016)

Thompson, J. D. (1967). *Organizations in Action: Social Science Bases of Administration*. New York: McGraw-Hill Book Company.

Thompson, R. L., Higgins, C.A. & Howell, J.M. (1991). Personal computing, toward a conceptual model of utilization. *MIS Quarterly*, *15*(1), 125-143.

Treverton, G. F. (2008). *Reorganizing U.S. Domestic Intelligence: Assessing the Options*. Santa Monica, CA: RAND Corporation.

Tsai, W. (2002). Social structure of “coopetition” within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization Science*, *13*(2), 179-190.

Tsai, W., & Ghoshal, S. (1998). Social Capital and Value Creation. *Academy of Management Journal*, *41*(4), 464-476.

Ulrich, D., & Barney, J. B. (1984). Perspectives in organizations: Resource dependence, efficiency, and population. *Academy of Management Review*, *9*(3), 471-481.

U.S. Citizenship and Immigration Services. (2018). About Us. Retrieved from https://www.uscis.gov/aboutus

U.S. Citizenship and Immigration Services. (2015). Fraud Detection and National Security Directorate. Retrieved from https://www.uscis.gov/about-us/directorates-and-program-offices/fraud-detection-and-national-security/fraud-detection-and-national-security-directorate

U.S. Citizenship and Immigration Services. (2016). USCIS Strategic Plan: FY 2017–2021. Retrieved from https://www.uscis.gov/sites/default/files/USCIS/About%20Us/Budget%2C%20Planning%20and%20Performance/USCIS_2017-2021_Strategic_Plan.pdf

U.S. Citizenship and Immigration Services Ombudsman. (2018). Annual Report 2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20%20Annual%20Report%202018.pdf

U.S. Department of Homeland Security. (2017). Annual Performance Report: Fiscal Years 2016-2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20FY%202016-2018%20APR.pdf

U.S. Department of Homeland Security. (2018). Annual Performance Report: Fiscal Years 2017-2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20FY%202017-2019%20APR_0.pdf

U.S. Department of Homeland Security. (2017). Border Security. Retrieved from https://www.dhs.gov/border-security

U.S. Department of Homeland Security. (2008). Brief Documentary History of the Department of Homeland Security: 2001-2008. Retrieved from https://www.hsdl.org/?view&did=37027

U.S. Department of Homeland Security. (2003). Delegation to the Bureau of Citizenship and Immigration Services. Delegation Number 0150.1. Retrieved from https://www.hsdl.org/?view&did=234775

U.S. Department of Homeland Security. (2015). Department Six-point Agenda. Retrieved from https://www.dhs.gov/department-six-point-agenda

U.S. Department of Homeland Security. (2014). Directive Number 103-01: Enterprise Data Management Policy. Retrieved from https://www.dhs.gov/office-intelligence-and-analysis

U.S. Department of Homeland Security. (2015). Budget in Brief: Fiscal Year 2015. Retrieved from https://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf

U.S. Department of Homeland Security. (2017). Budget in Brief: Fiscal Year 2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf

U.S. Department of Homeland Security. (2018). Office of Intelligence and Analysis. Retrieved from https://www.dhs.gov/office-intelligence-and-analysis

U.S. Department of Homeland Security. (2016). Our Mission. Retrieved from https://www.dhs.gov/our-mission

U.S. Department of Homeland Security Office of Inspector General. (2017). Improvements Needed to Promote DHS Progress toward Accomplishing Enterprise-Wide Data Goals. Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-101-Aug17.pdf

U.S. Department of Homeland Security Office of Inspector General. (2017). Major Management and Performance Challenges Facing the Department of Homeland Security. Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-11-Nov17.pdf

U.S. Government Accountability Office. (2019). Drug Control: Certain DOD and DHS Joint Task Forces Should Enhance Their Performance Measures to Better Assess Counterdrug Activities. Retrieved from https://www.gao.gov/assets/710/700187.pdf

U.S. Government Accountability Office. (2005). Department of Homeland Security: Addressing Management Challenges That Face Immigration Enforcement Agencies. Retrieved from https://www.gao.gov/assets/120/111634.pdf

U.S. Immigration and Customs Enforcement. (2018). What We Do. Retrieved from https://www.ice.gov/overview

U.S. Secret Service. (n.d.). The Investigative Mission. Retrieved from https://www.secretservice.gov/investigation/

Van den Hoof, B., & De Ridder, J. (2004). Knowledge sharing in context: The influence of organizational commitment, communication climate and CMC use on knowledge sharing. *Journal of Knowledge Management*, *8*(6), 117-130.

Vijayasarathy, L. R. (2010). Supply integration: An investigation of its multi-dimensionality and relational antecedents. *International Journal of Production Economics*, *124*(2), 489-505.

Wasem, R. E. (2007). Toward More Effective Immigration Policies: Selected Organizational Issues. *Congressional Research Service*. Retrieved from https://trac.syr.edu/immigration/library/P1623.pdf

Wei, H.-L., Wong, C. W. Y. & Lai, K. H., (2012). Linking inter-organizational trust with logistics information integration and partner cooperation under environmental uncertainty. *International Journal of Production Economics*, *139*(2), 642-653.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171-180.

Wheatley, M. J. (2006). *Leadership and the new science: Discovering order in a chaotic world*. San Francisco, CA: Berrett-Koehler Publishers.

Willem, A., & Buelens, M. (2007). Knowledge sharing in public sector organizations: The effect of organizational characteristics on interdepartmental knowledge sharing. *Journal of Public Administration Research and Theory*, *17*(4), 581−606.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York: The Free Press.

Wong, C. W., Lai, K. H., & Cheng, T. C. E. (2011). Value of information integration to supply chain management: roles of internal and external contingencies. *Journal of Management Information Systems*, *28*(3), 161-200.

Woodward, J. (1965). *Industrial Organization: Theory and Practice*. London: Oxford University Press.

Yang, T., & Maxwell, T. A., (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164-175.

Yi, J. (2009). A measure of knowledge sharing behavior: Scale development and validation. *Knowledge Management Research & Practice*, *7*(1), 65-81.

Yigitbasioglu, O.M. (2010). Information sharing with key suppliers: A Transaction Cost Theory Perspective. *International Journal of Physical Distribution & Logistics Management*, *40*(7), 550-578.

Yoo, Y., & Torrey, B. (2002). National culture and knowledge management in a global learning organization. In C. W. Choo & N. Bontis (Eds.), *The Strategic Management of Intellectual Capital and Organizational Knowledge* (pp. 421-434). New York: Oxford University Press.

Zhang, J., & Dawes, S. S. (2006). Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks. *Public Performance & Management Review*, *29*(4), 433-466.

Alexandra Rosen

EXPERIENCE

American Trucking Associations **Arlington, VA**
Customs, Immigration, & Cross-Border Operations Manager *Jan. 2019 - Present*

- Formulate and execute policy on behalf of ATA members engaged in cross-border and international business
- Liaise with U.S., Canadian, and Mexican government agencies dealing with customs, immigration, security, and trade policy
- Coordinate with cross-border motor carriers in the U.S., Canada, and Mexico; state trucking associations; and state, provincial, and national trucking associations in Canada and Mexico
- Serve as staff liaison for ATA's Supply Chain Security Policy Committee
- Engage with Members of Congress to advocate for ratification of the U.S.-Mexico-Canada Agreement (USMCA)
- Appointed to the Transportation Security Administration's Surface Transportation Security Advisory Committee as a voting member

U.S. House of Representatives, Committee on Homeland Security **Washington, D.C.**
Professional Staff Member *March 2018 – Dec. 2018*

- Advised the Chairman of the Subcommittee on Transportation and Protective Security, Rep. John Katko (R-NY), on Transportation Security Administration and U.S. Secret Service policy matters
- Coordinated policy communications between the Committee Chairman, Subcommittee Chairmen, Department of Homeland Security personnel, Congressional staff, and stakeholders in the development and advancement of legislation
- Led policy negotiations and conference process with Senate counterparts to codify the FAA Reauthorization Act of 2018
- Drafted 11 formal memoranda, 13 opening statements, 11 question series, and other relevant materials for Full Committee and Subcommittee hearings

Legislative Assistant / Clerk
May 2017 – March 2018

- Conducted oversight of U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and the U.S. Coast Guard
- Specialized in transportation security, border security, and maritime security

Staff Assistant
Oct. 2016 – May 2017

- Assisted Full-Committee staff with hearings, bill markups, and briefing preparations

U.S. Department of Justice, Child Exploitation and Obscenity Section **Washington, D.C.**
Legal Intern *June 2016 – Aug. 2016*

- Audited the Tor Network to determine if the operational costs outweighed the investigative benefits
- Drafted memoranda regarding child sexual abuse, extraterritorial sexual exploitation of children, and parental kidnapping

U.S. Department of Justice, Office of International Affairs **Washington, D.C.**
Legal Intern *June 2015 – Aug. 2015*

- Drafted formal letters in both English and Spanish to South American dignitaries and U.S. officials

EDUCATION

Johns Hopkins University **Washington, D.C.**
GPA: 4.0 │ MA: Government │ Concentrations: Security Studies and Political Communication
Sept. 2017 - Aug. 2019

Bucknell University **Lewisburg, PA**
GPA: 3.93 │ BA: History, Spanish, and English │ Summa Cum Laude │ Phi Beta Kappa
Aug. 2012 – May 2016

LEADERSHIP

Bucknell Student Government **Lewisburg, PA**
Executive President *Jan. 2015 – Dec. 2015*

- Served as the official liaison to the Board of Trustees and the President of Bucknell University

American Security Project **Washington, D.C.**
Women in Security Leadership Fellow *Jan. 2017 – Jan. 2018*

- Authored reports on visa overstays, cybersecurity, and national security to be published and publicly affiliated with ASP

The Woodrow Wilson Center **Washington, D.C.**
Foreign Policy Fellow *Feb. 2017 – May 2017*

- Debated current U.S. foreign policy concerns with a bipartisan and bicameral cohort of Congressional staffers

Women in Government Relations **Washington, D.C.**
Judy Schneider Fellow *Jan. 2019 – Dec. 2019*

- Fellowship is aimed at mentoring and emboldening the next generation of talented, ethical, savvy, and passionate female advocates.