NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

"DANGER CLOSE": THE NEED FOR A NATIONWIDE DECONFLICTION AND NOTIFICATION SYSTEM FOR ALL LAW ENFORCEMENT AGENCIES

by

Brian A. Nyhus

December 2020

Co-Advisors: Erik J. Dahl
Christopher Bellavita (contractor)

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE "DANGER CLOSE": THE NEED FOR A NATIONWIDE DECONFLICTION AND NOTIFICATION SYSTEM FOR ALL LAW ENFORCEMENT AGENCIES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brian A. Nyhus	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

To prevent friendly fire incidents and avoid duplication of effort, law enforcement agencies in the United States use multiple deconfliction systems to register investigative targets and notify outside units and agencies of proactive undercover operations. This research reveals that investigators are confused about which of the main systems to use in certain areas and that the use of multiple systems prevents investigators from gathering data on friendly fire incidents and restricts collaboration between agencies that are targeting the same criminals. Having one central deconfliction system for use by federal, state, local, and tribal authorities would make law enforcement officers' jobs safer and would facilitate information sharing among the different units and agencies, leading to greater collaboration and more successful outcomes.

14. SUBJECT TERMS law enforcement deconfliction, information sharing, collaboration, task forces, officer safety	**15. NUMBER OF PAGES** 121
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

"DANGER CLOSE": THE NEED FOR A NATIONWIDE DECONFLICTION AND NOTIFICATION SYSTEM FOR ALL LAW ENFORCEMENT AGENCIES

Brian A. Nyhus
Captain, New York City Police Department
BA, Excelsior College, 2013

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: Erik J. Dahl
Co-Advisor

Christopher Bellavita
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To prevent friendly fire incidents and avoid duplication of effort, law enforcement agencies in the United States use multiple deconfliction systems to register investigative targets and notify outside units and agencies of proactive undercover operations. This research reveals that investigators are confused about which of the main systems to use in certain areas and that the use of multiple systems prevents investigators from gathering data on friendly fire incidents and restricts collaboration between agencies that are targeting the same criminals. Having one central deconfliction system for use by federal, state, local, and tribal authorities would make law enforcement officers' jobs safer and would facilitate information sharing among the different units and agencies, leading to greater collaboration and more successful outcomes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT LANK

LIST OF ACRONYMS AND ABBREVIATIONS

ATF	Bureau of Alcohol, Tabaco, Firearms and Explosives
AUSA	Assistant United States Attorney
CBP	Customs and Border Protection
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DICE	Deconfliction and Internet Coordination Endeavor
DPR	Dread Pirate Roberts (Ross Ulbricht)
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FFL	federal firearms license
HIDTA	High Intensity Drug Trafficking Areas
HSI	Homeland Security Investigations
ICE	Immigration and Customs Enforcement
IRS	Internal Revenue Service
JAG	Ed Byrne Memorial Justice Assistance Grant
MOU	memorandum of understanding
NCIC	National Crime Information Center
NYPD	New York City Police Department
OCDETF	Organized Crime Drug Enforcement Task Force
OIG	Office of the Inspector General
ONDCP	Office of the National Drug Control Policy
PDI	Partner Deconfliction Interface
RISS	Regional Information Sharing Systems
RISSafe	RISS Officer Safety Deconfliction System
SAFETnet	Secure Automated Fast Event Tracking Network
SHIELD	Secure High-Speed Investigative and Event Law Enforcement Deconfliction
SMM	Sex Money Murder gang
SOD	Special Operations Division
SWB	southwest border

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

A deconfliction system's primary purpose is to prevent friendly fire shootings among law enforcement agencies that conduct undercover operations and street enforcement operations. This research seeks to show how a single, nationwide deconfliction system could be implemented for law enforcement agencies in the United States—from the local to the federal—to improve safety, information sharing, and collaboration. To do so, the thesis examines the different deconfliction systems agencies currently use and reveals that the use of multiple systems limits investigators' opportunities to connect with other agencies that are investigating similar targets. This lack of information can limit the investigation's scope and cause an investigator to miss vital evidence, which may mean the investigator fails to arrest the subject. Additionally, the research shows that the use of multiple systems creates dangerous conditions for law enforcement personnel conducting proactive street investigations.

The thesis presents three case studies that show how deconfliction plays a vital role in law enforcement investigations; the way that investigators use the knowledge gained from deconfliction meetings is up to them. The lead agent in Operation Fast and Furious, the first case study presented, deconflicted through personal meetings and the federal deconfliction database, DICE.[1] Because the agent used the proper system to register her subjects, she received a notification when another agent attempted to register the same subject. This facilitated a meeting between the agencies; information the agent received in that meeting provided the evidence the agency needed to obtain a wiretap.[2] While the agent used the deconfliction process correctly and prevented a possible blue-on-blue situation, the agency's flawed investigation failed to capitalize on other information-sharing opportunities, which prolonged the investigation and resulted in the death of a border patrol agent.

[1] U.S. Department of Justice Office of Inspector General, *A Review of ATF's Operation Fast and Furious and Related Matters* (Washington, DC: Department of Justice, 2012), 121, https://oig.justice.gov/reports/2012/s1209.pdf.

[2] U.S. Department of Justice Office of Inspector General, 122.

The second case study examines Ross Ulbricht, who used modern technology to create the Silk Road, an online drug empire that stymied multiple law enforcement agencies for several years. Under his alias, Dread Pirate Roberts (DPR), Ross Ulbricht amassed a multimillion-dollar fortune while facilitating drug sales worldwide, all while remaining completely anonymous. Law enforcement agencies investigated Ulbricht and his website early on, but were only able to arrest low-level dealers. Then, as a result of a deconfliction meeting at the Department of Justice attended by all the agencies investigating the Silk Road, the investigation began to progress.[3] Collaboration between multiple federal law enforcement agencies led investigators to identify Ross Ulbricht as DPR and allowed law enforcement to seize the Silk Road website.

The final case study examines Sex Money Murder, a Bloods gang that dealt drugs and death throughout the Bronx, and nationally, while making millions of dollars. In law enforcement's fight against the gang, collaboration between the New York City Police Department gang team, the North Carolina State Police, and the Bureau of Alcohol, Tobacco, Firearms and Explosives led to two federal convictions against gang leader Peter Rollack and the incarceration of the gang's other members. The three agencies developed the evidence and provided the testimony that saw Rollack face the death penalty for his acts of violence. While the agencies' collaboration did not come about because of deconfliction, a notification from the National Crime Information Center facilitated their initial information sharing.[4]

The information sharing that leads to positive outcomes, however, is stymied when agencies use disparate systems. And without a policy or mandate for law enforcement agencies to participate in deconfliction systems, the systems are even less effective. The continued use of multiple systems despite evidence that shows the danger of poor integration gives the impression that the system organizers, along with the federal partners, do not care about officer safety. A standard deconfliction system offers safety benefits,

[3] Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind behind the Silk Road* (New York: Portfolio/Penguin, 2018), 239.

[4] Seth Ferranti, *Street Legends,* vol. 1 (Gorilla Convict Publications, 2010), 249.

increased information sharing, and collaboration; these benefits outweigh the main possible drawback, corruption.

Changing the deconfliction environment will be a complicated task that will require multiple agencies to work together and to combine different databases. To alleviate some of the problems identified in this thesis, however, the law enforcement community must reduce deconfliction down to two systems and strongly push their universal use. Everyone who participates in the investigative effort would benefit from the elimination of information silos. For law enforcement to be successful, agencies must work together and share information; while deconfliction systems help keep officers safe, they also bring agencies together. The implementation of the incremental changes described in this thesis will increase officer safety during field operations, increase collaboration across multiple agencies, and reduce waste in funding and investigative overlap. These changes can occur if the members of the governing boards for the High Intensity Drug Trafficking Areas (HIDTA) and Regional Information Sharing System (RISS) are willing to accept that the deconfliction monopoly they participate in is dangerous to law enforcement officers and needs to be addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As we all know, this program is difficult. But the circumstances that occurred in 2020 made it even more difficult. It goes without saying that I would like to thank my friends and family for all of the support they gave me throughout the eighteen months of this master's degree program. They endured my long absences both during the in-residencies (when we had them) and the distance-learning sessions so I could achieve this goal. This program allowed me to meet some fantastic cohort members (too numerous to mention) who were always willing to provide support and advice when needed. We will always have Room 300, till they took it away from us.

I would especially like to thank my thesis team, who were able to get me over the finish line with a finished draft that I am proud to have written. Noel, my writing coach, bore the brunt of my unintelligible first drafts with a tremendous amount of patience and grace, and helped transform my work into the acceptable product it became. Chris Bellavita, who approached me during the Executive Leaders Program and encouraged me to apply to this program, believing that I could contribute to the group learning during the class. Chris also graciously agreed to be my thesis advisor along with Erik Dhal, neither of whom knew what it would entail to get me to think logically.

I would like to thank my chief, Chris McCormack, who knew that this program would be beneficial for me, my career, and the department. Additionally, thanks to all my coworkers, who endured the frequent absences that this program necessitates. They all stepped up and filled in for me so the work of keeping New York City safe would continue.

Finally, I would like to thank my mother, Catherine, who supported me throughout this, along with my good friends Caroline, Dana, John, and Danny, all of whom helped my family out when I could not be there for them because of the obligation to this program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A deconfliction system's primary purpose is to prevent friendly fire shootings among law enforcement agencies that conduct undercover operations and street enforcement operations. The use of these systems, which began in the late 1980s, has expanded from investigations involving narcotics to those involving violent street gangs, nationwide economic scams, and human trafficking cases.[1] In law enforcement, there are two types of deconfliction: target and event deconfliction. Target deconfliction is the process of registering subjects of an investigation with a central database along with their vehicles, residences, and other identifying information. This process informs other agencies about a possible conflict with their investigations if they attempt to register the same subjects, gives investigators case ownership, and informs other units that there is an active investigation. The other type of deconfliction, known as event deconfliction, takes place when an agency plans an enforcement operation, such as a search warrant or an undercover drug sale, at a particular location. The investigator registers the location to prevent other agencies from planning an enforcement operation at the same place.

There are two significant problems with deconfliction in law enforcement: first, there are multiple systems in use and they are not interconnected; second, some agencies do not use the systems at all. Without a nationwide system for all agencies, law enforcement personnel in undercover operations face increased risk, and agencies that could benefit from joint investigative targets are inhibited from communicating. Police Chief James Hurley of Leicester, Massachusetts, offers an example. When Hurley was supervising a multiagency task force on an undercover drug buy, he discovered that the drug dealer being investigated was actually an undercover officer from another county,

[1] Tom Carr, Kent Shaw, and Jack Killorin, "Event Deconfliction Avoids Operational Conflicts, Saves Lives, and Solves Cases," *Police Chief*, February 1, 2017, https://www.policechiefmagazine.org/event-deconfliction-avoids-operational-conflicts/.

which forced Hurley to cancel the operation.[2] During a meeting after the operation, the other department's supervisor admitted that he did not know about deconfliction.[3]

In the United States, a law enforcement agency's location dictates the deconfliction system it uses—if it uses one at all. These systems operate under funding from the federal government, but, as mentioned, the systems are not interconnected. Currently, there are seven national or regional formal deconfliction systems, operated or funded by four separate government agencies. According to the Department of Justice, these multiple systems have led to confusion among law enforcement agencies and have prevented them from sharing case information and collaborating on investigations.[4] The use of a central database shared by task forces across the United States has improved information sharing and helped to increase arrests of pedophiles. Such a single database might offer solutions for a deconfliction systems. As such, this thesis asks: How can a single, nationwide deconfliction system for federal, state, local, and tribal law enforcement agencies improve safety, information sharing, and collaboration?

A. LITERATURE REVIEW

This literature review examines the available published material about deconfliction in law enforcement and explores whether a single national system might increase information sharing and collaboration. The first section of the review focuses on the importance of collaboration in law enforcement, and particularly what experts have identified is needed for successful collaboration. The second section focuses on information sharing in the law enforcement community and examines whether it has improved since 9/11. This review contains reports from the federal government, academic journals, and published theses.

---

[2] Carr, Shaw, and Killorin.

[3] Carr, Shaw, and Killorin.

[4] Eileen Larence, *Combating Child Pornography: Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective*, GAO-11-334 (Washington, DC: Government Accountability Office, 2011), 30, https://www.gao.gov/products/GAO-11-334.

1. Collaboration

In the aftermath of 9/11, the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) called for increased information sharing and cooperation among all levels of government.[5] Almost twenty years after the attacks and the publishing of the 9/11 Commission's report, scholars and law enforcement experts argue that although information sharing and collaboration in the law enforcement community have improved, there is still a long way to go.[6] In particular, experts believe that three factors are important for increasing collaboration among law enforcement agencies: trust, resources, and clarity about roles and responsibilities.

Interagency collaboration depends on trust between agencies and, more importantly, among workers. As Renee Graphia Joyal defines it in *Criminal Justice Studies*, "Trust refers to the degree that one agency or person has that another agency or person is both competent and honest."[7] She further states that trust-based relationships generate reciprocity, genuineness, and confidence in other workers and agencies.[8] Trust between these parties ensures that the information they exchange is timely and accurate and that it will not be misused.[9] Government mandates for collaborative agreements can evolve if the participants show that they are willing to foster positive relationships and attempt to collaborate as they work to resolve their problems.[10] E. Madalina Busuioc strengthens this reasoning, showing that a lack of trust among the collaborating agencies in Europol is one of the reasons that the agency has had difficulty achieving success.[11]

---

[5] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W. W. Norton & Company, 2004), 263.

[6] Renee Graphia Joyal, "How Far Have We Come? Information Sharing, Interagency Collaboration, and Trust within the Law Enforcement Community," *Criminal Justice Studies* 25, no. 4 (December 2012): 357, https://doi.org/10.1080/1478601X.2012.728789.

[7] Joyal, 366.

[8] Joyal, 366.

[9] Andreas Riege, "Three-Dozen Knowledge-Sharing Barriers Managers Must Consider," *Journal of Knowledge Management* 9, no. 3 (2005): 24, https://doi.org/10.1108/13673270510602746.

[10] Joyal, "How Far Have We Come," 362.

[11] E. Madalina Busuioc, "Friend or Foe? Inter-agency Cooperation, Organizational Reputation, and Turf," *Public Administration* 94, no. 1 (March 2016): 42, https://doi.org/10.1111/padm.12160.

Europol's member agencies focus on reputation and public perception; protecting their "turf" is more important than building trust among partner agencies.[12] In a Government Accountability Office report, J. Christopher Mihm also identified trust as foundational to positive working relationships between participants, as it helps bridge institutional and cultural differences.[13]

The literature also identifies availability of resources as an integral part of collaboration. Janet Weiss believes that if groups do not secure resources at the start of a collaborative effort, the process will grind to a halt and the effort will lose whatever participants it has.[14] Resource sharing and financial support are two of the main reasons that agencies participate in collaborative efforts.[15] Without sufficient funding, the team may be unable to complete their work and some team members may leave due to strains on their departments. Even though Weiss claims some agencies may participate when funding is unavailable, funding is a reliable indicator of successful collaboration.[16] Collaboration may also fail when team members cannot participate on a regular schedule or become overworked and incapable of completing their tasks.[17]

Finally, collaboration among agencies improves when each agency's roles and responsibilities are clearly defined. Mihm states that an agreed-upon process for decision making and clarity of roles in a memorandum of understanding will lead to a successful

---

[12] Busuioc, 43.

[13] J. Christopher Mihm, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, DC: Government Accountability Office, 2012), 14, https://www.gao.gov/products/GAO-12-1022.

[14] Janet A. Weiss, "Pathways to Cooperation among Public Agencies," *Journal of Policy Analysis and Management* 7, no. 1 (1987): 111, https://doi.org/10.2307/3323353.

[15] Russell M. Frazier, "A Cannon for Cooperation: A Review of the Interagency Cooperation Literature," *Journal of Public Administration and Governance* 4, no. 1 (2014): 10, https://doi.org/10.5296/jpag.v4i1.4870; Frederick M. Kaiser, *Interagency Collaborative Arrangements and Activities: Types, Rationales, Considerations*, CRS Report No. R41803 (Washington, DC: Congressional Research Service, 2011), 12, https://www.hsdl.org/?view&did=5216.

[16] Weiss, "Pathways to Cooperation among Public Agencies," 99.

[17] Mary Atkinson, Paul Doherty, and Kay Kinder, "Multi-agency Working: Models, Challenges and Key Factors for Success," *Journal of Early Childhood Research* 3, no. 1 (February 2005): 116, https://doi.org/10.1177/1476718X05051344.

collaborative effort.[18] Clearly defined roles can also mitigate conflict among team members over different policy ideas.[19] Everyone must understand their specific role in the group, the roles that specific agencies perform, and the limitations placed on team members by their agencies.[20] However, as Busuioc has shown, even with a consensus, it may be challenging to get all participating agencies to cooperate completely. For example, even though Europol was created by convention in 1995 and funded by the European Union, it still sees poor cooperation and information sharing between member offices.[21]

2. Barriers to Information Sharing

Like collaboration, poor information sharing among law enforcement and government agencies was acknowledged as a contributing factor to the 9/11 attacks.[22] Scholars and practitioners suggest that overcoming institutional and cultural differences, fostering trust among partner agencies, and improving technology improves information sharing. Improved information sharing, in turn, leads to greater collaboration on complex issues and increased resources. Writing for the *Journal of Knowledge Management*, Andreas Riege similarly describes a triad of barriers to information sharing: individual, organizational, and technological.[23] Individual barriers that prohibit information sharing include time—which is needed to identify who needs the information—and lack of trust—e.g., that other agencies will misuse or take credit for the information.[24]

As it pertains to the first element in Riege's triad—individual barriers Lambert notes that some officers fail to share information because they believe the information they

---

[18] Mihm, *Managing for Results*, 18.

[19] Kaiser, *Interagency Collaborative Arrangements and Activities*, 17.

[20] Atkinson, Doherty, and Kinder, "Multi-agency Working," 120.

[21] Busuioc, "Friend or Foe," 46.

[22] Rahul Bhaskar and Yi Zhang, "Knowledge Sharing in Law Enforcement: A Case Study," *Journal of Information Privacy and Security* 3, no. 3 (July 2007): 45, https://doi.org/10.1080/15536548.2007.10855821.

[23] Riege, "Three-Dozen Knowledge-Sharing Barriers," 23.

[24] Riege, 24.

possess is not a priority.[25] As Rick Brown indicates, however, a significant amount of modern police work now involves reviewing data to uncover criminal connections that may go beyond local jurisdictions.[26] For information sharing to work, members of all law enforcement agencies must be able to collect and refer pertinent information to the agency or unit where it is needed. Law enforcement agencies are also constrained by legal factors; for instance, they cannot share sealed records and officers must not violate people's civil liberties when they obtain or share information.[27] Paul Hendriks shows that information sharing provides a link between the individual workers who gather information and those at the level of the organization where the information becomes useful.[28] In law enforcement circles, that information leads to arrests and crime prevention. Many in the profession do not understand, however, that information sharing is also a component of ordinary policing.[29]

Rahul Bhaskar and Yi Zhang's case study explores the factors that influence information sharing in law enforcement. They state that people are reluctant to share information without strong personal motivation and that these motivations are influenced by internal and external factors.[30] Internal motivating factors include benefits, or power, that an individual may gain from sharing the information.[31] Some may have a specific reason for sharing information, for instance, to solve an investigation. If investigators fail to share information about a hard case, the investigation may never be resolved; the desire to solve the investigation may cause a determined investigator to overcome the personal

---

[25] Lambert, "Addressing Challenges to Homeland Security Information Sharing," 1258.

[26] Rick Brown, "Understanding Law Enforcement Information Sharing for Criminal Intelligence Purposes," *Trends and Issues in Crime and Criminal Justice*, no. 566, (December 2018): 1.

[27] Steven Chermak et al., "Law Enforcement's Information Sharing Infrastructure: A National Assessment," *Police Quarterly* (February 19, 2013): 228, https://doi.org/10.1177/1098611113477645.

[28] Paul Hendriks, "Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing," *Knowledge and Process Management* 6, no. 2 (June 1999): 91.

[29] David E. Lambert, "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model," *Criminal Justice Policy Review*, July 18, 2018, 1251, https://doi.org/10.1177/0887403418786555.

[30] Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 48.

[31] Bhaskar and Zhang, 48.

barrier of hoarding information.[32] One external factor that affects information sharing is establishing and building relationships with other agencies and officials, including building trust with particular officials in coordinating agencies.[33] Other external factors include recognition or rewards from coworkers and supervisors and increased solidarity among those involved with the information-sharing effort.[34]

Organizational barriers that lead to a lack of information sharing (the second element in Riege's triad) include poor leadership or direction when communicating the benefits of information sharing, and competition with other agencies.[35] Riege states that an organization's structure, such as a hierarchical structure, may limit sharing, as can an organization's culture.[36] To overcome cultural influences, agencies must integrate their goals and strategy. Senior management is responsible for communicating the company's goals to all employees so they understand and support the mission.[37] In their case study, Bhasker and Zhang found that law enforcement traditionally does not encourage information sharing, relying instead on jurisdictional and legal restrictions to enforce a "need to know" attitude.[38]

Likewise, David Lambert states that information silos negatively affect information sharing. Some individuals and agencies will hoard information and hide behind cultural barriers that dissuade information sharing.[39] Agencies will "silo" or "stovepipe" and refuse to share information because they feel that the organization requesting the information is

---

[32] Bhaskar and Zhang, 53.

[33] Bhaskar and Zhang, 48.

[34] Sirkka L. Jarvenpaa and D. Sandy Staples, "Exploring Perceptions of Organizational Ownership of Information and Expertise," *Journal of Management Information Systems* 18, no. 1 (May 31, 2001): 157, https://doi.org/10.1080/07421222.2001.11045673.

[35] Riege, "Three-Dozen Knowledge-Sharing Barriers," 25.

[36] Riege, 26, 30.

[37] Riege, 26.

[38] Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 55.

[39] David E. Lambert, "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model:," *Criminal Justice Policy Review*, July 18, 2018, 1259, https://doi.org/10.1177/0887403418786555.

less competent.[40] Some organizations only share with locally known agencies, or only regionally or federally.[41] Lambert has found that silos can also form within an agency, either between different departments or between people who are deemed to have lower status in the organization; these silos in both cases cause "institutional friction" and prevent reciprocity of information.[42] Overcoming such cultural issues requires not only technology but also an openness to learning. Key managers and leaders must encourage behavioral awareness and interconnectivity among people and organizations.[43] Clear directives about the department's mission from leadership will routinize information sharing. While Lambert discovered these issues with police organizations, Tom Ruddy has observed similar issues with non-law-enforcement or nongovernment organizations.[44]

For the final element in his triad, Riege notes that technological factors also constrain effective information sharing. Bashkar and Zhang also found that technology can both increase and inhibit information sharing.[45] Hendriks agrees that the use of proper technology allows people and agencies to reduce the temporal and spatial barriers to effective information sharing.[46] Without proper technology, Riege emphasizes, people often cannot share information.[47] Bhaskar and Zhang further this idea, stating that technology that does not fit the requirements for the agency will have limited use.[48] Other technological barriers that inhibit information sharing include poor systems integration, poor compatibility between systems, and improper training on systems.[49] Additionally, when people do not understand the advantages of new technology over existing systems,

---

[40] Lambert, "Addressing Challenges to Homeland Security Information Sharing," 1260.

[41] Lambert, 1260.

[42] Lambert, 1259.

[43] Ruddy, "Taking Knowledge from Heads," 37.

[44] Ruddy.

[45] Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 50.

[46] Hendriks, "Why Share Knowledge," 91.

[47] Riege, "Three-Dozen Knowledge-Sharing Barriers," 29.

[48] Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 50.

[49] Riege, "Three-Dozen Knowledge-Sharing Barriers," 29.

they are less likely to use the new technology.[50] The authors agree that with proper utilization of technology, information sharing will improved.

Lambert also highlights technological factors with information sharing. He states that leadership must continuously communicate that effectively sharing information through proper deconfliction platforms will, for example, allow police officers to identify burglars or map out robbery patterns.[51] Information sharing in this environment will also provide feedback on crime issues and improve two-way communication.[52] As Hendriks states, however, if people are not motivated to share information, it is also likely that they are not motivated by the information-sharing tools available to them.[53] Sharon Dawes believes that harnessing such technology can improve the accuracy and timeliness of information; she opines that information is essential for problem solving, and that timely, accurate information improves decision making, placing the organization in a better position to respond to the situation.[54]

In addition to its benefits for information sharing, technology can also act as a catalyst for organizational change.[55] When organizations define strategies that support use of particular programs, employees begin to accept the programs as a routine part of the job; in doing so, information sharing increases.[56] Riege argues that organizations must integrate infrastructure that supports various technologies as well as employees' work-related needs. If organizations promote improper technology that does not work for the employees, they may form a barrier to sharing.[57]

---

[50] Riege, 29.

[51] Lambert, "Addressing Challenges to Homeland Security Information Sharing," 1271.

[52] Lambert, 1271.

[53] Hendriks, "Why Share Knowledge," 91.

[54] Sharon S. Dawes, "Interagency Information Sharing: Expected Benefits, Manageable Risks," *Journal of Policy Analysis & Management* 15, no. 3 (Summer 1996): 379, https://doi.org/10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F.

[55] Eric Tsui, "The Role of IT in KM: Where Are We Now and Where Are We Heading?" *Journal of Knowledge Management* 9, no. 1 (2005): 3.

[56] Tsui, 3.

[57] Riege, "Three-Dozen Knowledge-Sharing Barriers," 30.

Successful information sharing occurs when organizations finds a successful balance of technology, process, and content.[58] For example, a 2011 Government Accountability Office report reveals an increase in arrests for child pornography cases after the creation of a specific database for investigations into the distribution of child pornography.[59] The creation of a single peer-to-peer central database fostered communication among investigators in separate jurisdictions, allowing them to share evidence and case information.[60] The investigators, the database, and the system all had a single goal: to apprehend people who trade child pornography. The new system allowed them to share information and achieve that goal.

3. Conclusion

Because there is little information or research on deconfliction systems, it is difficult to draw conclusions about how the different deconfliction systems perform. A greater understanding of such systems is necessary to determine if they are providing the benefits that they advertise, including keeping officers safe and reducing duplication of effort. This thesis examines the current deconfliction systems in use by law enforcement and determines if they function as designed while supporting law enforcement. It also seeks to determine if the current use of multiple systems, coupled with inconsistent policies by law enforcement agencies, confuses officers and agents, reducing information sharing and collaboration and increasing the dangers to law enforcement.

B. RESEARCH DESIGN

This thesis examines how a national deconfliction system will increase safety for law enforcement agencies while improving information sharing and collaboration in investigations. The first step is to understand the deconfliction process and why it is necessary for law enforcement. Although published information on deconfliction is scarce, published U.S. government reports and articles, as well as a previously published thesis,

58 Tsui, "The Role of IT in KM," 3.

59 Larence, *Combating Child Pornography*, 28.

60 Larence, 30.

are the basis for this research. It does not use surveys, interviews, focus groups, or personally collected data, as there is little information on deconfliction in law enforcement. The result is a recommended plan of action and the development of a new deconfliction system that will increase law enforcement safety and collaboration. Using policy analysis and policy options analysis, the thesis specifically looks at how, through the deconfliction system, agencies in different parts of the country could become aware of other agencies investigating the same target. The thesis also evaluates studies and policy recommendations in law enforcement sources; law enforcement understands that cooperation is necessary to combat growing criminal threats.

This thesis uses program evaluation and case study analysis to examine collaboration in the following law enforcement investigations:

- Operation Fast and Furious: the failed gunwalking scandal at the Department of Alcohol, Tobacco, Firearms and Explosives (ATF) that resulted in the death of a U.S. Border Patrol agent.

- Ross Ulbricht: known as the Dread Pirate Roberts of the Silk Road, Ulbricht was arrested for selling drugs on the dark web through the combined efforts of the Federal Bureau of Investigation (FBI), Department of the Treasury, and Homeland Security Investigations.

- Sex Money Murder: the Bloods street gang that dealt narcotics along the Eastern Seaboard and ruthlessly killed anyone who got in their way. Gang members were arrested through the combined efforts of the New York City Police Department (NYPD), the ATF, and North Carolina State Police.

These cases highlight that through the combined efforts of multiple agencies, law enforcement can target and destroy significant drug trafficking organizations. The case studies also analyze the increased use of federal task forces, which lead to better cooperation among law enforcement agencies. The thesis uses the case studies to examine the possible ramifications of increased information sharing and collaboration in law

enforcement and the dangers that agencies and investigators must avoid. The final goal of this thesis is to develop a proof of concept to evaluate the effectiveness of the proposed deconfliction system.

Ultimately, this thesis examines the deconfliction environment in law enforcement and attempts to analyze how it can be improved to facilitate better information sharing and collaboration. The following chapters define event and target deconfliction, and describe the multiple systems that facilitate the deconfliction process. Additionally, the cases studies show how use of the deconfliction systems have enabled some law enforcement agencies to share information and collaborate on investigations that may have failed without outside agency assistance. The final chapter provides an analysis of the current deconfliction environment and three possible options to improve the process.

II. LAW ENFORCEMENT AND DECONFLICTION

The United States has law enforcement entities at the federal, state, local, and tribal levels, all of which have responsibilities that, at times, intersect another agency's area of responsibility. The vast number of agencies and the numerous officers they employ complicate investigations and increase the need for deconfliction. This chapter examines the benefits and drawbacks of the deconfliction systems agencies use today. The use of disparate systems and the absence of proper policies from executives can lead to confusion, can prevent information sharing, and can break down trust in law enforcement.

The federal government is the largest single law enforcement employer. Over 132,000 people work as federal officers in 83 separate agencies.[61] The principal functions of federal law enforcement agencies include prevention, detection, and investigation of crimes and the apprehension of criminals.[62] The federal government's primary law enforcement agencies are the Department of Justice (DOJ) and the Department of Homeland Security (DHS). According to the Bureau of Justice Statistics, the DOJ and DHS combined employ 70 percent of the federal law enforcement officers. The remaining 30 percent fall under the federal government's separate agencies, including the Department of Agriculture, Bureau of Prisons, and Department of Energy.[63] According to the Office of Personnel Management, in 2019, 82,000 agents, or 62 percent of the workforce, were federal investigators.[64]

Over 17,000 other law enforcement agencies operate at the state, local, and tribal levels.[65] According to the Uniformed Crime Reporting program maintained by the FBI, in

---

[61] Conner Brooks, *Federal Law Enforcement Officers, 2016 - Statistical Tables*, NCJ 251922 (Washington, DC: Bureau of Justice Statistics, October 2019, 3, https://www.bjs.gov/index.cfm?ty=pbdetail&iid=6708.

[62] Brooks, 1.

[63] Brooks, 5.

[64] Brooks, 6.

[65] Duren Banks et al., *National Sources of Law Enforcement Employment Data*, NCJ 249681 (Washington, DC: Bureau of Justice Statistics, April 2016), 3, https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5600.

2016, over 750,000 people were employed in the United States as sworn law enforcement officers. Sworn employees are armed personnel who can enforce the laws of their government, such as state police, county sheriffs, local police, and tribal police.[66] Another 325,000 people are employed as non-sworn officers assisting law enforcement.[67]

Because of the large number of law enforcement officers and the diverse agencies, deconfliction is essential for officer safety and agency collaboration. As previously mentioned, deconfliction is the limited sharing of information among law enforcement agencies to identify common investigative targets or activity.[68] Law enforcement agencies in the United States employ two types of deconfliction: target deconfliction for investigations and event deconfliction for enforcement activities. Target deconfliction identifies investigations with the same criminal subjects, and event deconfliction notifies law enforcement agencies of planned enforcement events.[69] The notification methods range from regional or national computer databases at the local, state, and federal level to direct person-to-person contact with an outside law enforcement agency. These systems are operated and maintained by different law enforcement agencies and are supported by funding from the federal government through grant programs.

One program, the High Intensity Drug Trafficking Areas (HIDTA) program, operates two sub-programs: Case Explorer, a deconfliction and records management system, and the Secure Automated Fast Event Tracking Network (SAFETnet). While funded by HIDTA, these two systems are used regionally throughout the United States; law enforcement agencies can choose which system to use.[70] The Regional Information

---

66 Banks et al., 2.

67 Banks et al., 2.

68 "DOJ and DHS OIGs Release a Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations," Department of Homeland Security Office of Inspector General, August 1, 2019, 1, https://www.oig.dhs.gov/news/press-releases/2019/08012019/doj-and-dhs-oigs-release-joint-review-law-enforcement-cooperation-southwest-border-between-federal-bureau.

69 Department of Homeland Security Office of Inspector General, 1.

70 David Maurer, *Office of National Drug Control Policy: Lack of Progress on Achieving National Strategy Goals*, GAO-16-257T (Washington, DC: Government Accountability Office, December 2, 2015), 17, https://www.gao.gov/products/GAO-16-257T.

Sharing Systems (RISS) Program operates RISSSafe, which is similar to Case Explorer and SAFETnet but offers only event deconfliction.[71] Law enforcement agencies may also use the El Paso Intelligence Center's system, the Deconfliction Internet Connectivity Endeavor (DICE), or the Special Operations Division (SOD), all of which are operated by the Drug Enforcement Agency (DEA).

A. THE THREE MAIN DECONFLICTION SYSTEMS

The High Intensity Drug Trafficking Areas (HIDTA) program maintains two of the three primary deconfliction systems used by law enforcement, Case Explorer and SAFETnet. The HIDTA program was formed under the Office of National Drug Control Policy (ONDCP) in 1988 when Congress passed the Anti-Drug Abuse Act.[72] The HIDTA program's goal is to provide funding, assistance, and investigative support to federal, state, local, and tribal law enforcement agencies to combat drug trafficking and distribution.[73] The HIDTA program targets drug production and trafficking by:

- Coordinating and sharing information with law enforcement agencies at all levels of government;
- Increasing and facilitating intelligence-sharing among federal, state, local, and tribal law enforcement;
- Assisting law enforcement in designing programs to counter the drug threat in their communities; and
- Coordinating across multiple law enforcement agencies to reduce the drug supply locally and nationally.[74]

HIDTA is a regionally based program that uses the county as the geographic unit of inclusion. Individual executive boards comprising law enforcement representatives assist the local law enforcement agencies with additional funding for investigations provided by the ONDCP.[75] The local executive boards have a great deal of discretion in

---

[71] Maurer, 18.

[72] Kristin Finklea, *High Intensity Drug Trafficking Program (HIDTA) Program*, R45188 (Washington, DC: Congressional Research Service, 2018), 4, https://crsreports.congress.gov/product/pdf/R/R45188.

[73] Finklea, 2.

[74] Finklea, 1.

[75] Finklea, 2.

determining how to tailor their policies to fight narcotics issues in the region. Regional HIDTAs span every state as well as Puerto Rico and the U.S. Virgin Islands.[76] The HIDTAs operate with a great deal of autonomy from each other and from the ONDCP to design drug control policies that fit their specific regions and to spend their funds as they see fit. The autonomy of the separate HIDTAs has led to the funding of duplicate programs in the deconfliction environment: the Case Explorer system and SAFETnet.

1. Case Explorer

One of the two deconfliction systems developed and maintained by HIDTA is the Case Explorer system, which matches data between cases and organizations to determine if there is overlap. Released in 2005 by the Washington/Baltimore HIDTA, Case Explorer is a web-based case management, criminal intelligence, and deconfliction system, as well as an information-sharing tool for law enforcement that allows agents and officers to register information in the system about investigative targets and planned enforcement events for deconfliction.[77] If investigators receive a registration number back from Case Explorer, there is no conflict with any other investigation or planned operation; the registration number allows the investigator to move forward. However, investigators receive a conflict notification when they attempt to register a target already registered to someone else, or when they plan an event in proximity to an existing operation. The conflict notification contains the contact information of the already registered investigator. While the system was designed and built by the Washington/Baltimore HIDTA, Case Explorer is open to all twenty-nine HIDTAs in the country and to the law enforcement agencies that they serve at the federal, state, local, and tribal levels.[78] It also provides enterprise case management functions to help investigators build and develop cases on their targets.[79]

---

[76] Finklea, 3.

[77] Case Explorer Law Enforcement Software for Police Training, accessed April 15, 2020, http://caseexplorer.net/; Maurer, *Office of National Drug Control Policy*, 17.

[78] Case Explorer Law Enforcement Software for Police Training.

[79] Case Explorer Law Enforcement Software for Police Training.

2. SAFETnet

The Secure Automated Fast Event Tracking Network (SAFETNet) is the other deconfliction system operated by HIDTA and is more secure then Case Explorer because it contains no specific case information. The New York/New Jersey HIDTA created SAFETnet in 2001; it was the first online computer database for event and target deconfliction in the United States. SAFETnet is a decentralized system used in multiple locations throughout the country and is open for use by all law enforcement agencies.[80] While SAFETnet is a deconfliction system, it differs from Case Explorer because it does not provide case management functions. The system does operate, however, in the same manner as Case Explorer: the user inputs the relevant information about a person or location into the system, and the user receives a registration number if no conflicts exist. If the system finds a conflict, the user receives a point of contact for the other investigator. The investigator who finds the conflict is responsible for speaking with the owner of the registration. Because SAFETNet is not a records management system, no relevant case information is stored in the system outside of the investigative targets and event locations; this provides greater case security.

3. RISSafe

Local law enforcement agencies realized they needed a way to share information about the growing and sophisticated organized criminal organizations that crossed the city, state, and county jurisdictions.[81] Since 1973, the Regional Information Sharing Systems (RISS) Program, created by the Bureau of Justice Administration (BJA), has done just that, providing technical support for criminal investigations to enhance officer safety.[82] RISS is a collection of local and state police departments that collect, analyze, and distribute law

---

[80] Maurer, *Office of National Drug Control Policy*, 17.

[81] Arnold Jones, *Statement of Arnold P. Jones, Senior Associate Director General Government Division Before the Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations on, Regional Information Sharing Systems* (Washington, DC: Government Accountability Office, March 26, 1985).

[82] "RISS Overview," Regional Information Sharing Systems, accessed April 15, 2020, https://www.riss.net/about-us/.

enforcement intelligence and information relevant to the region.[83] Operated with funds and grants from the BJA, RISS has six regional centers—which cover all fifty states—and a technical support center locally managed by a policy board or executive committee.[84] The executives of each RISS center form the RISS National Policy Group and are responsible for strategic planning and nationwide organization.[85]

RISS provides many distinct functions for law enforcement employing different operational mechanisms, and one of RISS's primary functions is to operate the RISS Officer Safety Deconfliction System (RISSafe).[86] RISSafe was created in 2009 and is the third primary deconfliction system for law enforcement. RISSafe is a web-based system that automatically informs the submitting officer of an event conflict. The RISS watch center also receives a notification about the event conflict and attempts to deconflict the operation to ensure officer safety. The RISS watch center operates 24 hours a day, 365 days a year to assist with event deconfliction and provide support for law enforcement. RISSafe, unlike Case Explorer and SAFETNet, tracks data only for officer safety event deconfliction, such as search warrants, controlled buys, or surveillances.[87]

B. THE EL PASO INTELLIGENCE CENTER

The El Paso Intelligence Center (EPIC) assists law enforcement with timely intelligence analysis on threats to the United States that originate in the Western Hemisphere; while it was created to perform an all-threat mission, it focuses on drug interdiction[88] EPIC is a DEA-led organization with twenty-seven partner law enforcement agencies that focus on narcotics, drugs, human trafficking, and weapons trafficking along

---

[83] Jones, *Statement of Arnold P. Jones*.

[84] Regional Information Sharing Systems, "RISS Overview."

[85] Regional Information Sharing Systems.

[86] Regional Information Sharing Systems.

[87] Regional Information Sharing Systems.

[88] Department of Justice Office of the Inspector General, *Follow-up Review of the Drug Enforcement Administration's El Paso Intelligence Center* (Washington, DC: Department of Justice, 2017), 1, https://oig.justice.gov/reports/2017/e1701.pdf.

the southwest border (SWB).[89] A primary component of EPIC is the twenty-four-hour watch center, which operates seven days a week. The watch center responds to requests from law enforcement officers and alerts from the Law Enforcement Inquiries and Alerts (LIEA) system, an information exchange system maintained by the DEA.[90] One function of the watch section is tactical intelligence, entering lookouts and detections. The watch section personnel connect personnel who enter a lookout on the same person or vehicle.[91] EPIC also hosts SAFETNet for the SWB region and the National Virtual Pointer System, which allows EPIC to search multiple databases to conduct event and target deconfliction.[92] An officer or agent can request these actions by calling the center for assistance.

C. DICE

Created in 2010, the Deconfliction Internet Connectivity Endeavor (DICE) is a DEA-maintained deconfliction database for use by participating federal, state, local, and tribal law enforcement.[93] All DOJ and DHS agencies are mandated to use DICE to deconflict any case-related information, telephone numbers, email addresses, license plates, and IP addresses.[94] DICE operates in the same manner as RISSSafe, Case Explorer, and SAFETnet: the system generates a conflict if the information entered into the system matches current information. The system notifies the investigator if there is a conflict.[95] DOJ and DHS also require agents to use local and regional deconfliction systems when

89 Department of Justice Office of the Inspector General, 1.

90 "Law Enforcement Inquiry and Alerts," Data.gov, accessed May 15, 2020, https://catalog.data.gov/dataset/law-enforcement-inquiry-and-alerts.

91 Department of Justice Office of the Inspector General, *Follow-up Review*, 22.

92 Department of Justice Office of the Inspector General, 30.

93 Douglas Coleman, *Stopping the Flow of Illicit Drugs in Arizona by Leveraging State, Local and Federal Information Sharing* (Washington, DC: House of Representatives, 2012), 3.

94 Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 6.

95 Alejandro Mayoraks, *Department Policy Regarding Investigative Data and Event Deconfliction*, Policy Directive 045–04 (Washington, DC: Department of Homeland Security, October 18, 2016), 2, https://www.dhs.gov/sites/default/files/publications/mgmt/law-enforcement/mgmt-dir_045-04-dept-policy-regarding-investigative-data-event-deconfliction.pdf.

practical, since law enforcement agencies at the state, local, and tribal levels may not use DICE for deconfliction purposes.[96]

D. SPECIAL OPERATIONS DIVISION

To coordinate investigations of large-scale drug trafficking organizations, the DEA created the Special Operations Division (SOD) The SOD is a multiagency coordination center designed to identify overlapping investigations into transnational drug trafficking organizations and enhance deconfliction and communications among the agencies.[97] SOD oversees the deconfliction and information sharing among twenty government agencies. This oversight allows the DEA to deconflict classified and sensitive information and connect cases in different parts of the country and the world.[98] If SOD discovers a connection between separate cases, supervisors in charge of the investigations will connect these cases at coordination meetings.

E. PARTNER DECONFLICTION INTERFACE

When it became clear that the fractured nature of the three main deconfliction systems was a safety issue, the Criminal Intelligence Coordinating Council (CICC) began exploring ways to integrate the systems. The CICC serves as a voice for all law enforcement agencies by facilitating the sharing of intelligence to prevent criminal activity.[99] In 2013, the CICC, including members of HIDTA, RISS, DEA, and BJA, formed an event deconfliction policy group.[100] The policy group determined that, to keep officers safe, all law enforcement agencies must conduct event deconfliction using one of the three universally recognized deconfliction systems: Case Explorer, SAFETnet, or

96 Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 6.

97 Department of Homeland Security Office of Inspector General, 17.

98 Department of Homeland Security Office of Inspector General, 17.

99 "Intelligence," Office of Justice Programs, accessed May 22, 2020, https://it.ojp.gov/global/working-groups/cicc.

100 Carr, Shaw, and Killorin, "Event Deconfliction," 6.

RISSafe.[101] And to provide maximum coverage nationwide, the three systems would need to become interconnected.[102]

In May 2015, HIDTA and RISS announced the Partner Deconfliction Interface (PDI), the interconnection of the three systems for only event deconfliction; the PDI does not include target deconfliction. The PDI connected all systems except SAFETnet in New York City .[103] With the PDI, a submission into one deconfliction system will return results from the other two systems. The goal was to have as many law enforcement agencies as possible connecting through the systems, and to avoid the need to mandate use of one system over the others. In its first five months, the PDI reportedly processed over 159,000 target deconflictions in the combined systems.[104] However, because the PDI is limited to event deconfliction, there remains an issue with investigative targets.

F. CURRENT PROBLEMS WITH DECONFLICTION

In addition to the multiple deconfliction systems in use across the country, collaboration and information sharing across law enforcement agencies are also inhibited by inconsistent agency deconfliction practices, a lack of agency policy, and jurisdictional conflicts. These issues have diminished trust between agencies and discouraged interagency agreements that seek to avoid duplication of efforts, which increases the likelihood that officers will compromise an investigation.[105] Furthermore, the variety of methods used for deconfliction has led to confusion and has negatively affected officer safety. Some agencies believe that information regarding specific investigations is too sensitive to be included in deconfliction systems and that inclusion in the system may jeopardize the investigation.[106]

---

[101] Carr, Shaw, and Killorin, 6.

[102] Carr, Shaw, and Killorin, 8.

[103] The Police Foundation, "Best Practices in Event Deconfliction," CALEA, October 2016, 3, https://www.calea.org/sites/default/files/2019-02/EventDeconfliction_PoliceFoundation.pdf.

[104] Maurer, "Office of National Drug Control Policy," 20.

[105] Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 6.

[106] Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 18.

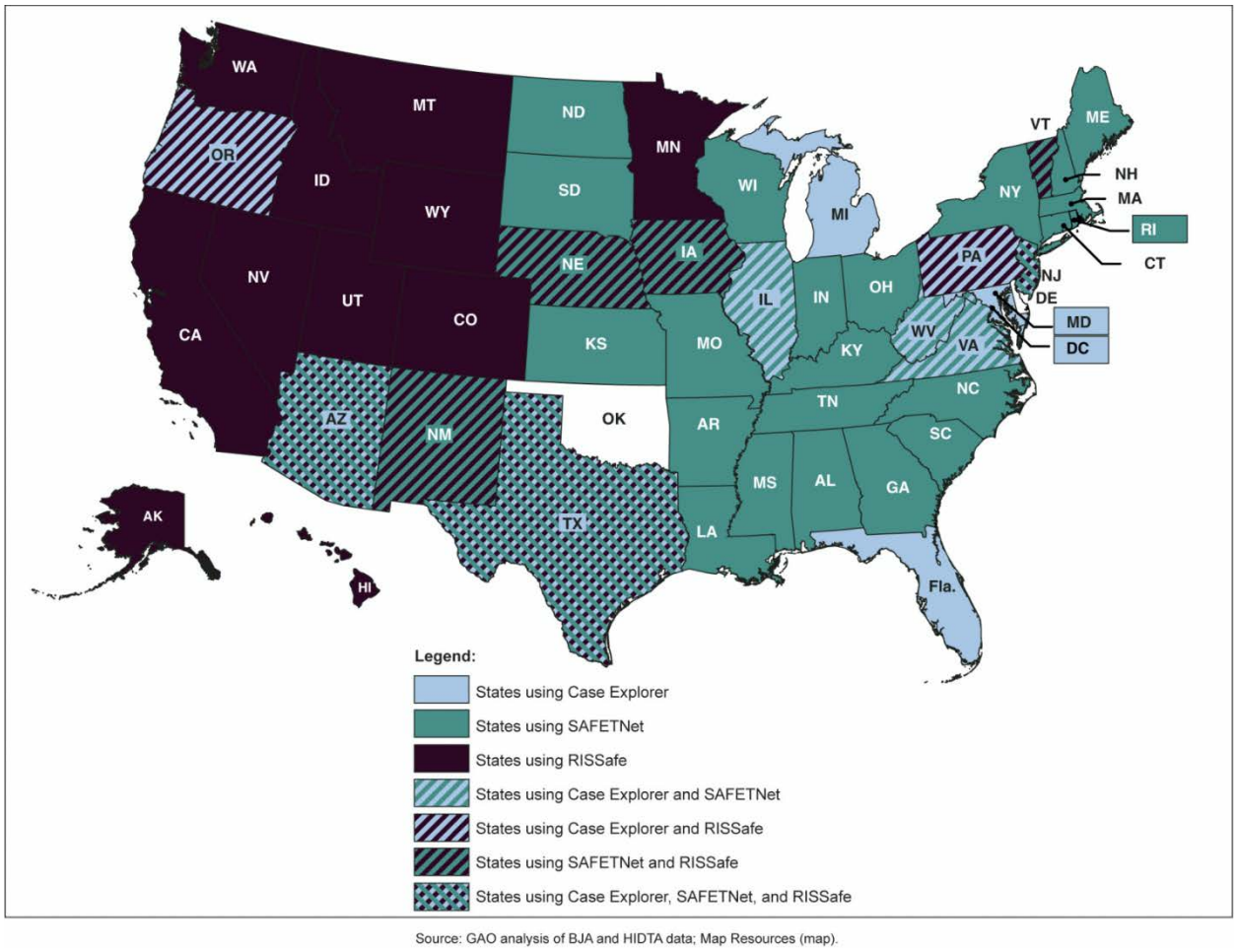
This section highlights the confusion caused by the current use of multiple deconfliction systems and the cascading issues with information sharing and a lack of institutional trust among law enforcement agencies. It also discusses problems with including information from sensitive investigations in deconfliction systems, and possible issues with corrupt police officers and agents.

1. Deconfliction Systems by State

While law enforcement agencies and associations—including the DOJ, DHS, and International Association of Chiefs of Police—realize that event deconfliction can save lives, not everyone participates.[107] Each law enforcement agency decides whether it wants to participate in the system that is available in its region of the country; no federal authority mandates participation in any deconfliction system. The map in Figure 1 breaks down the different deconfliction systems available by state. It is telling that Texas, New Mexico, and Arizona, which are in the SWB region, all use multiple systems for deconfliction, as this region deals with the most substantial flow of narcotics into the United States, and the use of multiple systems breeds inefficiency.[108]

[107] The Police Foundation, "Best Practices in Event Deconfliction," 1.

[108] Liana Rosen, *International Drug Control Policy: Background and U.S. Responses* (Washington, DC: Congressional Research Service, March 16, 2015), 6, https://fas.org/sgp/crs/row/RL34543.pdf.



Source: GAO analysis of BJA and HIDTA data; Map Resources (map).

Figure 1. Deconfliction Systems by State[109]

No agency at any level of government has direct oversight of deconfliction systems and their use. Without such oversight, it is not possible to analyze the threats to law enforcement safety in blue-on-blue situations. Oversight and analysis would also allow agencies to identify duplication of efforts and help them reduce operational inefficiencies.[110]

109 Source: Eileen Larence, *Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*, GAO-13-471 (Washington, DC: Government Accountability Office, 2013), 30, https://www.gao.gov/products/GAO-13-471.

110 Larence, 30.

2. Sensitive Information and Corruption Issues

Despite their necessity for officer safety and collaboration, some agencies resist deconfliction systems because they believe the systems may compromise their investigation. FBI agents, for example, have refused to deconflict public corruption cases.[111] Agents believe that since public corruption investigations may involve multiple subjects, some being members of law enforcement, the investigation may be compromised if the subject accesses the system.[112] Additionally, due to the sensitivity of their nature and the systems' lack of security, investigations related to national security and investigations that are classified investigations may not be included in deconfliction systems.

Deconfliction systems can also be exploited by corrupt law enforcement officers who are looking to target known money or drug traffickers for robberies. If the deconfliction system returns the corrupt officer a registration number, meaning there is no conflict with another investigation, the officer knows that his robbery of this person may go unnoticed and will not be exposed. A corrupt law enforcement officer may also use target deconfliction to protect a drug dealer or other criminal by holding registration on the dealer. If the corrupt officer holds the deconfliction on a drug dealer, he will be alerted if another officer tries to open an investigation on that dealer; he can then prevent the other investigation or alert the dealer about the investigation.

3. Joint Investigation by the Department of Justice and Department of Homeland Security

The Offices of the Inspector General (OIG) for DOJ and DHS released a joint report that highlights the lack of cooperation between the FBI and Homeland Security Investigations (HSI) at the SWB. The joint OIG report defines cooperation as "deconflicting investigative targets to avoid duplicative investigations, deconflicting law enforcement operations to promote officer safety, and sharing relevant investigative

[111] Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 18.

[112] Department of Homeland Security Office of Inspector General, 18.

information."[113] The investigators used anonymous surveys and interviews of agents assigned to the region to gather data for the report.[114] The report shows that inconsistent deconfliction practices, a lack of guidance from the agencies, and a misunderstanding of different agencies' federal authority have led to a decrease in information sharing, collaboration, and, most importantly, trust between the two agencies.[115]

The vast SWB region presents significant challenges to law enforcement, and effective information sharing and deconfliction is paramount. The SWB spans nearly 2,000 miles and is the main conduit for narcotics smuggling into the United States. Almost 3,000 federal agents from the FBI and HSI conduct investigations in this region of the United States.[116] Despite their distinct missions, both agencies share some overlapping authority in certain criminal matters, such as narcotics smuggling and human trafficking. Their investigations may cross jurisdictions, so information sharing and collaboration are essential in identifying overlapping investigations. The high concentration of personnel from these two agencies is exacerbated by the other federal, state, and local law enforcement agencies.

The agent surveys from the report provide a better picture of how law enforcement agencies are cooperating with each other and the obstacles they encounter. Survey respondents answered questions about their experiences with target deconfliction, event deconfliction, and information sharing.[117] The survey generated 980 responses from the 2,948 agents in the SWB region. Of the 980 agents who participated in the survey, 363 (37 percent) had at least one experience with cooperation failure.[118] According to the report, 207 out of the 363 agents who experienced at least one deconfliction failure felt that the most significant impact was a loss of trust in the other agency.[119] Only 343 (35 percent)

[113] Department of Homeland Security Office of Inspector General, 1.

[114] Department of Homeland Security Office of Inspector General, 3.

[115] Department of Homeland Security Office of Inspector General, 2.

[116] Department of Homeland Security Office of Inspector General, 1.

[117] Department of Homeland Security Office of Inspector General, 8.

[118] Department of Homeland Security Office of Inspector General, 8.

[119] Department of Homeland Security Office of Inspector General, 8.

of the agents believed that the FBI and HSI had a good working relationship at the SWB.[120] Likewise, 416 (43 percent) of the respondents were comfortable sharing information with the other agency. This is similar to the results for operational deconfliction, 511 or (53 percent), and target deconfliction, 482 (50 percent).[121] These survey responses may be skewed by the answers from agents that work in a task force setting. Agents in co-located, task forces reported more of an increase in cooperation and information sharing than agents working just with their own agency. The task force agents attribute this increase to the shared mission aspect of the task force and the personal relationships with their coworkers.[122]

The report shows that even in a target-rich environment like the SWB, target and enforcement overlaps are common. Agents will independently develop information on an investigative subject. Agents reported target overlaps with another agency in 44 percent of cases, and almost one-third (29 percent) of agents reported enforcement operation overlap.[123] The significant occurrences of overlap in both targets and operations indicate the necessity for a robust deconfliction system policy. Survey respondents indicated that they would take steps to deconflict properly if made aware of the conflict.[124] Besides the loss of trust in the agency or its personnel, agents reported that the failure to deconflict and share information resulted in lower morale, prolonged investigations, compromised confidential sources, and compromised agent safety.[125]

Although the FBI and HSI have policies that address deconfliction procedures, their policies can lead to confusion for the agents. In response to the joint OIG report, the FBI concurred with the recommendation to review its deconfliction procedures for the SWB. The FBI also plans to replace its regional policy procedure with an agency-level policy due

[120] Department of Homeland Security Office of Inspector General, 9.

[121] Department of Homeland Security Office of Inspector General, 9.

[122] Department of Homeland Security Office of Inspector General, 12.

[123] Department of Homeland Security Office of Inspector General, 10.

[124] Department of Homeland Security Office of Inspector General, 10.

[125] U Department of Homeland Security Office of Inspector General, 15.

to the multi-jurisdictional nature of FBI investigations.[126] Considering the need for uniformity with its deconfliction policy, Immigration and Customs Enforcement (ICE), which is HSI's parent agency, stated that investigations may extend beyond the SWB and may affect multiple offices, and regional deconfliction policy may restrict information sharing and affect investigations and officer safety.[127] The policy mandates that all agents use DEA's DICE system as well as the local or regional systems, regardless of their assignment and geographic location.[128]

The survey highlighted several issues needed to improve deconfliction and information sharing between the FBI and HSI. A clear agency policy needs to be developed for deconfliction and sharing information.[129] A proper policy from each agency is also necessary and must be conveyed and understood by all the federal investigators. Also necessary to increase information sharing and deconfliction compliance are improvements to information sharing systems, alignment of investigative procedures, and compliance with established deconfliction protocols.[130] This policy, coupled with the proper technology, can significantly benefit law enforcement. The surveys complied with the report provide an understanding of agency interactions and the shortfalls of current policies and systems.

G. CONCLUSION

Proper deconfliction in law enforcement is necessary for officer safety and information sharing, and complex investigations require cooperation among multiple agencies. The current use of multiple deconfliction systems among the vast number of law enforcement officers and agencies is inefficient and, without policy governing their use, officers are confused about how and when to use deconfliction. As the joint OIG survey indicates, failure to properly deconflict investigations also causes officers to lose trust in

[126] Department of Homeland Security Office of Inspector General, 62.

[127] Department of Homeland Security Office of Inspector General, 68.

[128] Department of Homeland Security Office of Inspector General, 69.

[129] Department of Homeland Security Office of Inspector General, 8.

[130] Department of Homeland Security Office of Inspector General, 9.

each other and in other agencies. This loss of trust leads to a breakdown in information sharing and collaboration, which harms investigations and leads to conflicting cases and competition. A single deconfliction system may bridge some of these gaps and allow for greater cooperation.

The following chapters examine several high-profile investigations that were affected by deconfliction issues. They highlight how communication between agencies as a result of a deconfliction meeting can improve information sharing and collaboration on investigations. One case review shows that the refusal to cooperate, share information, and collaborate with other agencies increases the risk to the general public and can cause grave danger.

III. OPERATION FAST AND FURIOUS

Operation Fast and Furious was an ATF-led investigation of firearms trafficking into Mexico, undertaken to arrest drug cartels leaders. The investigation attempted to track the firearms and the subjects through a Title III federal wiretap warrant. A primary component of the investigation was for law enforcement to allow the firearms to leave the United States and enter Mexico without interdiction; investigators hoped this would help them identify all members of the operation. As such, they allowed drug cartel agents to purchase nearly 2,000 high-powered firearms.

Deconfliction meetings between agencies to discuss crossover investigative targets can facilitate information sharing; in the case of Operation Fast and Furious, it resulted in the creation of a dedicated task force. Even with these meetings, however, information sharing still requires all parties to act honestly. If task force members do not share all their information with other members, or if they limit team members' involvement, the investigation will not be successful.

While some agencies worked well together on this investigation, there were many instances of failure to share information, turf protection, and refusal to collaborate. Agents also used technology to limit information sharing and therefore inhibit other agencies' investigations. Operation Fast and Furious eventually led to the death of Border Patrol Agent Brian Terry, who was killed by a firearms trafficker armed with one of the 2,000 guns in question.

This case review of Operation Fast and Furious was compiled from government reports from the DOJ and DHS, and it highlights successful examples of information sharing, deconfliction, and collaboration; more importantly, however, it highlights failures in these areas. This case study does not examine the investigative methodology unless it was affected by the agents and supervisors who refused to share information or deconflict with an outside agency. The investigation's failures were caused by the strategy of the case agent; the deconfliction system's use and meetings did result in information sharing and collaboration.

A. EVENTS[131]

One suspicious firearm purchase set in motion the investigation that would become known as Operation Fast and Furious. On October 31, 2009, a local federal firearms license (FFL) holder notified the ATF's Phoenix Field Division about a suspicious firearm purchase, which initiated the investigation. The buyer, Jacob Chambers, had purchased six AK-47-style firearms at one time, with cash. The FFL holder reported this suspicious purchase, and the notification to the ATF led to the case against Jacob Chambers et al., which would become Organized Crime Drug Enforcement Strike Force Operation Fast and Furious.[132] Other FFL holders alerted the ATF to additional suspicious firearms sales made from November 1 through November 6 by new subjects. Although the lead case agent established an official case as required by ATF guidelines, she and her supervisors decided on a course of action that would prove very dangerous to the citizens of Mexico and to U.S. law enforcement.[133] During the next month, using conventional investigative techniques, suspect surveillance, and information supplied by the FFL holders, the ATF agents established a connection between the different straw buyers and possible stash locations.[134]

The ATF and the FFL holders in the Phoenix area already had a friendly relationship marked by reporting of suspicious purchases. To thoroughly investigate the organization and the cartel connection, the ATF capitalized on this relationship and requested that the FFL holders fulfill any firearms purchase request, thus allowing the numerous firearms to go to Mexico. The FFLs then notified the ATF team in advance of the purchases, allowing the ATF to conduct surveillance on the purchasers. One cooperating FFL holder allowed the ATF to install surveillance cameras in his store so the

131 For a condensed timeline of events, see Appendix A.

132 The only federal reporting requirement at this time for an FFL was the sale of multiple handgun purchases to the same person in 5 days. The FFL holders did not need to report the sale of multiple long guns until July 2011. Department of Justice Office of Inspector General, *A Review of ATF's Operation Fast and Furious and Related Matters* (Washington, DC: Department of Justice, 2019), 109, https://oig.justice.gov/reports/2012/s1209.pdf.

133 Department of Justice Office of Inspector General, 111.

134 Department of Justice Office of Inspector General, 109.

ATF could remotely monitor transactions.[135] The FFL holders' cooperation was instrumental to the investigation.

However, the ATF's investigation strategy was inconsistent with a standard policy: The lead case agent and her supervisors chose not to interdict the firearms because they believed this course of action would alert the traffickers and financers to a law enforcement investigation.[136] Case agents conducted surveillance and identified additional suspects and stash locations but did not perform any proactive policing. Although the lead agent and the supervisors decided that a Title III wiretap investigation would allow them to identify the cartel connected to the firearms, this type of investigation was time-consuming; it prolonged the investigation and, moreover, differed from standard ATF methods.[137] The ATF's common investigative technique was to have the investigator conduct a "knock and talk" to interview the straw buyer and attempt to obtain a confession, then use the straw buyer as a cooperator against the trafficker.[138] The lead case agent and her supervisors felt that these arrests would not be fruitful, however, because they would not take down the entire organization.[139]

The Phoenix Field Division created a new team, Team VII, that brought in agents from other states for the investigation, and law enforcement authorities along both sides of the SWB started recovering firearms trafficked into Mexico. On November 20, 2009, in the Naco, Sanora, region, Mexican soldiers arrested three individuals and recovered forty-two firearms, nineteen of which were bought by Fast and Furious subjects earlier in the month.[140] This weapons seizure identified additional Fast and Furious subjects, and members of the HSI interviewed the arrested individuals from that seizure. To protect their investigation and avoid alerting the gun traffickers who were being investigated, the

---

[135] Department of Justice Office of Inspector General, 228.

[136] House Committee on Oversight and Government Reform, *The Fast and Furious: The Anatomy of a Failed Operation Part I of III* (Washington, DC: U.S. Congress, 2012), 20, https://azmemory.azlibrary.gov/digital/collection/feddocs/id/2276/.

[137] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 215.

[138] Department of Justice Office of Inspector General, 121.

[139] Department of Justice Office of Inspector General, 122.

[140] Department of Justice Office of Inspector General, 112.

Special Agent in Charge for ATF Phoenix Field Division advised HSI to stop its investigation and not interview other people arrested for firearms trafficking.[141] The ATF scheduled a deconfliction meeting with HSI for November 30, 2009. Deconfliction meetings between the two agencies were routine, as investigations between the agencies frequently overlapped. During the deconfliction meeting, HSI agreed to stop their firearms trafficking investigations related to the Naco, Mexico, seizures, as the Assistant United States Attorney supported the ATF's investigation.[142] HSI Phoenix assigned one special agent to the investigation to assist the ATF and promote information sharing between the two agencies.

To track the firearms in an investigation and control the release of the information, the ATF records information about firearms purchases electronically. As part of her investigation, the lead agent entered the serial numbers of the firearms into the ATF Suspect Guns Database. ATF agents use the Suspect Gun Database to track firearms they believe have been trafficked or purchased by straw buyers.[143] To prevent other law enforcement agencies from talking to subjects of her investigation, the lead agent for Fast and Furious requested that the National Tracing Center not release any information related to her firearms without her approval.[144]

The lead case agent used agency deconfliction systems to protect other agents and determine whether other investigations involved her targets. In November 2009, the lead ATF agent requested that a DEA analyst run six telephone numbers related to Fast and Furious subjects in its DICE deconfliction system.[145] This initial request by the lead agent led to negative results for deconfliction.[146] On December 14, 2009, a DEA agent conducting a narcotics investigation with the FBI received information from his Title III

---

[141] Department of Justice Office of Inspector General, 112.

[142] Department of Homeland Security Office of Inspector General, *DHS Involvement in OCDETF Operation Fast and Furious*, OIG-13-49 Revised (Washington, DC: Department of Homeland Security, 2013), 18.

[143] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 16.

[144] Department of Justice Office of Inspector General, 114.

[145] Department of Justice Office of Inspector General, 121.

[146] Department of Justice Office of Inspector General, 122.

wiretap investigation that one of his subjects met a person about a firearms deal.[147] During surveillance, the DEA agent observed his subject with a person he later identified as Jacob Chambers, the Fast and Furious investigation's original subject.[148] Computer and deconfliction checks conducted by the DEA agent showed that an ATF agent registered Jacob Chambers; because of this conflict, the DEA and FBI set up a separate deconfliction meeting with the ATF.

The DEA and the ATF held a deconfliction meeting to discuss the crossover between the two investigations. During the meeting, the DEA provided the ATF with all the information that they had on Manual Celis-Acosta, the ATF's current main subject.[149] Celis-Acosta was in contact with the DEA investigation subject and discussed the sale of firearms and money transfers.[150] The ATF did not act on the information provided by the DEA about Celis-Acosta because they claim the DEA asked them not to. The DEA refutes this explanation, however, because the subject was only tangentially related to the DEA case and would not affect their investigation. While the ATF did not contact or investigate Celis-Acosta, the DEA's information was essential to the ATF's wiretap warrants, issued later on, in March 2010.[151] The DEA information would have shortened the investigation and reduced the danger to the public, as it would have prevented the need for the Title III investigation.[152]

The pace of the firearms purchases began to worry some of the FFL holders. On December 17, 2009, the FFL holder who had sold the most guns during the investigation requested a meeting with the ATF agents because of the unprecedented number of firearms purchased. At the meeting, the ATF agents assured the FFL holder that they were surveilling the subjects and doing everything possible to retrieve the firearms.[153] During

147 Department of Justice Office of Inspector General, 122.

148 Department of Justice Office of Inspector General, 122.

149 Department of Justice Office of Inspector General, 122.

150 House Committee on Oversight and Government Reform, *The Fast and Furious*, 35.

151 Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 123.

152 Department of Justice Office of Inspector General, 426.

153 Department of Justice Office of Inspector General, 129.

the meeting, the ATF agents asked the FFL holder to record phone conversations with the subjects and asked if they could install a surveillance camera in the store to monitor the sales.[154] Being assured that the ATF was doing what it could to interdict the guns and prevent them from going to Mexico, the FFL holder agreed to their request.

One week after the deconfliction meeting, the DEA provided the ATF case agent with information about a transfer of firearms between Celis-Acosta and another party heading to Mexico. The DEA did not act on this information because it did not have a narcotics component in the exchange.[155] The ATF case agent also did not act on the DEA's information because, being so close to Christmas, there were not enough agents to conduct the surveillance for the exchange, and the ATF agent did not believe the subject was going to meet with the other party for the firearms exchange. This information, about the Christmas gun shipment provided by the DEA, was the most substantial evidence in the investigation tying Celis-Acosta to the Mexican cartels, but the ATF did not act on it.

Specific federal investigations are deemed a higher priority and receive a special designation. In February 2010, the ATF submitted the Fast and Furious investigation for Organized Crime Drug Enforcement Task-Force (OCDETF) approval.[156] The OCDETF designation provided the case investigators with increased funding, additional resources, and personnel, along with greater prestige for the agency. The OCDETF proposal submitted to the review committee indicated that the Fast and Furious investigations were being handled by a multiagency task force led by the ATF, with additional personnel provided by HSI, the DEA, the Internal Revenue Service (IRS), and the local police department as task force officers.[157] Because of the OCDETF designation, Team VII moved its offices to the OCDETF Strike Force headquarters, giving the team greater access to other agencies and information for their investigation.

---

[154] Department of Justice Office of Inspector General, 228.

[155] Department of Justice Office of Inspector General, 124.

[156] House Committee on Oversight and Government Reform, *The Fast and Furious*, 53.

[157] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 148.

Celis-Acosta had several interactions with the police, but the ATF did not attempt to gain his cooperation against the cartels. On May 29, 2010, the Lukeville, Arizona, Port of Entry Customs and Border Protection (CBP) stopped Celis-Acosta and found him in possession of an AK-47 drum-style magazine and seventy-four rounds of ammunition. A computer check by the CBP officer indicated that Celis-Acosta was the subject of an investigation, and he contacted the lead case agent.[158] The agent responded to the location to interview Celis-Acosta but did not obtain any useful information. Upon Celis-Acosta's release from the location, the agent provided him with her phone number, but he never called her.

In March 2010, the ATF received approval for the Title III wiretap warrant for the Fast and Furious subjects. In applying for the warrant, the ATF used the information the DEA had supplied during the deconfliction meeting in December 2009.[159] The ATF renewed the Title III warrant every thirty days until August 2010. During that time, the ATF continued its same investigative strategy and allowed firearms trafficking into Mexico without interdiction, out of fear that interdicting the firearms shipments would cause the subject to change phone numbers.[160] During the Title III wiretap monitoring, the ATF did not identify any additional subjects and received no new information about their existing subjects, other than the information provided by the DEA in December. In August the ATF discontinued Title III because it added no value to the investigation. The ATF continued with the investigation for several more months even though ATF headquarters in Washington, DC, requested an exit strategy.[161]

By December 2010, almost 2,000 firearms had been allowed to enter Mexico and the operation had identified dozens of subjects and the main trafficker. On December 14, 2010, in the Rio Rico region of Arizona, Border Patrol Agent Brian Terry was killed in a shootout with Mexican smugglers. The weapon that killed Agent Terry, and another gun

158 Department of Justice Office of Inspector General, 178.

159 House Committee on Oversight and Government Reform, *The Fast and Furious*, 55.

160 Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 160.

161 Department of Justice Office of Inspector General, 266.

found at the scene, had been purchased by Fast and Furious straw buyers in the very early stages of the Fast and Furious investigation.[162] As a result of Terry's murder, the ATF conducted an emergency case takedown; in January 2011, they arrested twenty members of the straw buying ring. The indictment of the ring members did not contain additional evidence obtained during the Title III investigation.[163] Although law enforcement recovered 567 of the nearly 2,000 firearms trafficked into Mexico, the Fast and Furious investigative team only recovered 105 firearms.[164] Police and federal agents recovered the remaining 462 firearms while conducting their regular duties, usually at crime scenes or as the result of search warrants or car stops—putting their lives in great danger.[165]

B. DECONFLICTION

At the beginning of the Fast and Furious investigation, the ATF conducted several target deconfliction meetings with other law enforcement agencies. These deconfliction meetings allowed the agencies to exchange information and reassign personnel to help with the investigation. The first deconfliction meeting took place between ATF and HSI over the Naco, Mexico, firearms seizure; because this seizure occurred in Mexico, HSI had jurisdiction to investigate under the Arms Export Control Act.[166] During the deconfliction meeting, the ATF took the lead on the investigation and HSI assigned an agent to assist with deconfliction and information sharing. The HSI special agent in charge agreed to this because he had been instructed by his leadership at Immigration and Customs Enforcement (ICE), his parent agency, to foster a better working relationship with the ATF. To facilitate this cooperation, in June 2009, ICE and ATF signed a memorandum of understanding (MOU) that mandated the sharing of information between the two agencies and the correction of disputes at the lowest management level.[167] The direction by management

---

[162] House Committee on Oversight and Government Reform, *The Fast and Furious*, 13.

[163] House Committee on Oversight and Government Reform, 114.

[164] Department of Homeland Security Office of Inspector General, *DHS Involvement*, 4.

[165] Department of Homeland Security Office of Inspector General, 4.

[166] Authority of U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection Officers, 22 CFR § 127.4 (2005).

[167] Department of Homeland Security Office of Inspector General, *DHS Involvement*, 22.

and the creation of official agreements facilitating information sharing among agencies echoes Riege's work, which describes senior management's responsibility to foster communication to achieve its goals.[168] The MOU between the two agencies also served to overcome the traditional law enforcement need-to-know mentality described by Bhasker and Zhang; MOUs can help reduce turf wars between agencies, allowing the agencies to build trust.[169]

Because the DICE deconfliction systems were used properly, both the ATF and DEA were alerted that Jacob Chambers was connected to the agencies' separate investigations. The deconfliction meeting took place because the agents correctly followed procedures and used their deconfliction systems. The lead ATF agent had all the telephone numbers for her subject researched in DICE by a DEA analyst, which resulted in no conflict for the subjects. A short while later, the DEA agent, working on a separate investigation, identified a new person who was talking to his drug suspect about firearms. The agent again followed the procedure and submitted the new subject's information into DICE, which conflicted with the ATF agent's registration. The proper use of the DICE system prevented a possible event conflict and promoted information sharing between the two agencies.

Because both the ATF and DEA agents properly deconflicted their subjects, they were able to meet in person and share their case information. The deconfliction meeting provided the ATF agent with the name of the chief firearms trafficker for the Fast and Furious investigation. While the ATF did not use this information, the exchange was a positive result of proper deconfliction policies. The meeting also allowed the agents to properly deconflict the information they provided DEA. The DEA asked the ATF to inform them if they were going to take action against the individual discussed.

168 Riege, "Three-Dozen Knowledge-Sharing Barriers," 26.

169 Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 55.

C. INFORMATION SHARING

Operation Fast and Furious was able to begin in the first place thanks to information sharing between the FFL holders and the ATF. In 2009, the sale of multiple long guns in a short period did not require a notification to the ATF; however, because FFL holders in Arizona had a good working relationship with the ATF and a concern for public safety, they provided a constant stream of information to the ATF. The notifications about planned purchases and the installation of real-time surveillance cameras in the store underscore how much the FFL holders helped the ATF. One FFL holder stated that he participated in the operation because of the number of friends he had in law enforcement.[170] Another created a worksheet for his employees to use when an identified straw buyer made a purchase; it contained all of the information about the transaction, and it was faxed it to the ATF.[171]

As the investigation continued, the FFL holders became concerned about the number of firearms purchased and the length of the investigation.[172] The ATF insisted, however, that the information derived from the sales was essential to the investigation, so the FFL holders continued cooperating, even though some felt it was becoming dangerous.[173] One FFL holder even recorded phone conversations with a straw buyer for the ATF to use as evidence. The FFL holders, all the while, believed that the ATF was interdicting the weapons; the ATF did not inform the FFL holders that they were allowing the guns to walk. The ATF implied they were doing everything possible to seize the firearms and prevent them from going to Mexico. Had they not, the FFL holders might have refused to sell the firearms to the straw buyers and abruptly ended the investigation.[174]

The ATF agent's reluctance to use the DEA's information shows a lack of trust in the agency, or at least the agent. Upon learning of the deconfliction issue on the case, the

---

[170] John Dodson, *The Unarmed Truth: My Fight to Blow the Whistle and Expose Fast and Furious* (New York: Threshold Editions, 2013), 74.

[171] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 228.

[172] Department of Justice Office of Inspector General, 130.

[173] Department of Justice Office of Inspector General, 128.

[174] Department of Justice Office of Inspector General, 227.

DEA talked to the lead ATF agent. The DEA provided information about the main trafficker, Celis-Acosta, and the Christmas weapons transfer, neither of which the ATF used. The ATF agent may have refused initially to use the DEA information because of institutional friction; both the DEA and the ATF targeted Mexican drug cartels and did not want the competition. The DEA agent provided pertinent information to the ATF in hopes that doing so would build trust with the agent for future information exchanges.

The DEA, HSI, and CBP voluntarily shared information with the ATF at the deconfliction meetings in November and December 2009. The ATF, however, actively tried to prevent information about the case from being shared with the other agencies. Technology was used to hinder information sharing when the lead ATF agent used the Suspect Guns Database to block information about the recovered firearms. The improper use of technology, or the use of the incorrect technology, is a barrier to effective information sharing, according to Riege.[175] Registering the firearms in the Suspect Gun Database allows law enforcement to trace firearms recovered at a crime scene or from a seizure to their original point of sale. To protect her investigation, the lead agent would not release any information about the recovered firearms; she would state to any requestor that it was part of an ongoing ATF investigation. By not releasing this information to the outside agencies, the Fast and Furious investigation's true scope was unknown to other agencies. CBP notified the lead case agent of Celis-Acosta's arrest on May 29, 2010, which allowed the lead agent to interview him. While the agent acted on the information very quickly, she did not obtain Celis-Acosta's cooperation or even arrest him for the firearms trafficking.

Also listed with the firearm information in the Suspect Guns Database is the related case information and case number. The case agents list their name and contact information to allow direct communication about a possible case connection. This is designed to save the investigator time; it allows instant access to the history of the firearm without running a full check through the National Tracing Center.[176] This information will also allow the person requesting the eTrace to have direct contact with the other ATF agent assigned to

[175] Riege, "Three-Dozen Knowledge-Sharing Barriers," 23.

[176] House Committee on Oversight and Government Reform, *The Fast and Furious*, 25.

the case.[177] Direct contact allows both investigations to proceed, allows the ATF to see how vast the trafficking network is, and helps the requestor determine the origin of the gun. Investigators not assigned to the ATF must contact the National Tracing Center to obtain the case agent's information.[178]

D. COLLABORATION

The ATF created a new investigative team, Team VII, to conduct Operation Fast and Furious, and for the first time a firearms trafficking investigation received an OCDETF designation.[179] OCDETF-funded cases increase collaboration and information sharing because they include more law enforcement agencies in a task force setting; the ATF agents controlled the investigative information provided to those agencies and limited their involvement.[180] According to a report by the DHS OIG, the ATF supervisors did not allow the HSI agent to participate in internal meetings regarding the investigation, even though the HSI agent was named co-lead; the ATF excluded him from attending specific case meetings, preventing him from offering his ideas.[181] By controlling the information to outside agencies, the ATF allowed many high-powered firearms to reach the hands of violent criminals, leading to the death of Border Patrol Agent Terry.

Although collaboration between agencies may be necessary for an investigation, it does not always work. The HSI agent was assigned to Fast and Furious to facilitate deconfliction and information sharing about seizures.[182] The special agent in charge stated that his other reason for assigning the HSI agent was that ICE asked HSI to cooperate with ATF on investigations in the region.[183] During this portion of the investigation, executives,

---

[177] eTrace is an internet-based system run by the ATF through the National Tracing Center. It allows federal, state, local, and tribal agencies to determine an initial firearms point of sale history.

[178] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*, 114.

[179] An OCDETF designation combines resources and experience of several agencies to target criminal drug trafficking organizations.

[180] Department of Homeland Security Office of Inspector General, *DHS Involvement*, 9.

[181] Department of Homeland Security Office of Inspector General, 52.

[182] Department of Homeland Security Office of Inspector General, 19.

[183] Department of Homeland Security Office of Inspector General, 1.

on several occasions, fostered collaborative work environments by adding resources and agents to the investigation. The meeting between HSI and ATF was an attempt to overcome turf protection—a barrier to collaboration, according to Busuioc.[184] The need for additional resources and the addition of the HSI agent outweighed the ATF's reluctance to work collaboratively on the investigation. Additionally, the MOU between the ATF and ICE, and the instructions from ICE executives to work with the ATF, reflect Riege's statement that senior management needs to communicate its goals to employees if employees are to buy into the information sharing.[185]

Unfortunately, this assignment of an HSI agent to the investigation did not help HIS produce any significant information. To protect its investigation, the ATF fought against collaboration with HSI. For instance, the ATF case agent did not provide the HSI agent with information about the Naco, Mexico, gun seizure, and they limited his surveillance assignments to restrict his knowledge of the investigation. Without full information and with limited surveillance duties, the agent was not able to pass information to the HSI field office in Arizona. To improve its access to information about the Fast And Furious investigation, the HSI field office assigned a senior special agent to act as a liaison. Although this agent was an expert in firearms trafficking in the SWB region, the ATF did not give the agent specifics about the investigation, choosing to build silos. These actions increased the barriers to information sharing and collaboration between the two agencies, breeding an us-versus-them culture.

E. CONCLUSION

Operation Fast and Furious had many flaws; in the end, the flaws proved fatal for Border Patrol Agent Brian Terry. Although some key features of information sharing and collaboration were championed, others were ignored and abused. ATF investigators ignored information provided by other agencies because of a lack of trust. Even when the ATF collaborated with outside agencies in a task force environment, the ATF limited information sharing and the other agencies' participation in the case. The ATF also used

184 Busuioc, "Friend or Foe?"

185 Riege, "Three-Dozen Knowledge-Sharing Barriers," 26.

technology designed to facilitate information sharing to prevent law enforcement, and the public, from learning the number of firearms it allowed to travel into Mexico.

Conversely, the FBI, DEA, and HSI attempted to facilitate information sharing during the investigation. All of the agencies participated in deconfliction meetings with the ATF about the recovered firearms and possible case subjects. The special agent in charge for HSI Arizona supplied an agent to the ATF in hopes of better communication between the two agencies, following executives' instructions to collaborate with the ATF. The DEA and FBI provided information from their investigation regarding a Fast and Furious subject they had identified during a normal deconfliction process, and about a man who was eventually identified as the primary subject. ATF agents failed to respond to the DEA's information about a weapons shipment, which may have ended the case long before Terry's death. A combination of institutional friction, abuse of technology, and groupthink unnecessarily prolonged the investigation.

IV. ROSS ULBRICHT AND THE SILK ROAD

The internet has allowed criminals to expand their illegal activities in ways never thought possible. Because of the internet, child pornography exploded: over 70 million files are shared each year.[186] The internet has also become fertile ground for identity theft, with cases increasing by more than 100 percent between 2010 and 2015.[187] Dealing drugs, however, was initially more difficult on the internet because sellers and buyers needed to exchange money for the product, and buyers could not trust the dealers or keep their identities safe from law enforcement. This case study examines the Silk Road, a dark website where people could sell almost anything illegal. The investigation of the website presented new challenges to law enforcement that would require them to share information among investigative groups across the country and eventually collaborate and target the organization's leader.

This case study focuses on the investigation into the Silk Road website by the federal agencies—HSI, FBI, and IRS—whose collaboration led to the identification of its founder, Ross Ulbricht. This chapter discusses how Ulbricht built the Silk Road and an online drug empire and highlights the difficulties law enforcement encountered during the investigation thanks to the technology that allowed the website to succeed. The chapter also discusses a meeting organized by the DOJ that gave all the investigative agencies a chance to present their evidence. Without the information sharing facilitated by this meeting, the Silk Road would have continued operating and Ulbricht might never have been identified or prosecuted by the DOJ

186 "The Intersection of Technology and Child Sexual Abuse," Thorn, accessed July 25, 2020, https://www.thorn.org/child-sexual-exploitation-and-technology/.

187 "Identity Theft," Federal Bureau of Investigation, accessed July 25, 2020, https://www.fbi.gov/investigate/white-collar-crime/identity-theft.

A. EVENTS[188]

In January 2011, twenty-six-year-old Ross Ulbricht launched the Silk Road, a website hidden on the dark web and designed for contraband material transactions—the eBay of drugs. Ulbricht, known to site users as the Dread Pirate Roberts (DPR), envisioned a libertarian society where people could indulge in any drug they wished without government interference. A former doctoral candidate in physics at Penn State University, he capitalized on new technologies such as Tor, Bitcoin, and the dark web to covertly launch his new enterprise. The website allowed users to distribute drugs worldwide, upending typical drug distribution models and avoiding law enforcement efforts to stop the illegal flow of drugs. Even with the immense popularity of the website and calls from Congress for its seizure, law enforcement could not identify who, or where, DPR was. It took the combined efforts of multiple law enforcement agencies, sharing information and working together, to identify and apprehend DPR.

Ulbricht believed that the street dealing of narcotics leads to violent crime and user victimization, with most drug deals happening in poor neighborhoods, and with users at risk of violence and arrest by law enforcement. If he could develop a way to distribute drugs to people that kept the end user safe from violence and arrest, he believed society would improve. The Silk Road website, a marketplace for the distribution of illegal narcotics to anyone in the world, intended to do just that; its chat room and customer feedback system developed into a large online community that allowed for the free trade of information on how to buy, sell, and ingest drugs, and on which dealers were the most reputable and had the best product. It also provided Ulbricht a platform to discuss his libertarian beliefs.[189]

The key to the Silk Road's secrecy was its security measures, which protected the users and vendors while hampering law enforcement's efforts. The Silk Road operated on the dark web, a large portion of the internet that is not accessible through conventional

[188] For a condensed timeline of events, see Appendix B.

[189] Eileen Ormsby, *Silk Road* (Sydney: Pan Macmillan Australia, 2014), 54.

search engines like Google Chrome or Safari, which search only the clearnet.[190] Access to the dark web is only possible with specific search engines that hide the user's information. To access the Silk Road on the dark web, users need to download and use Tor, a search engine initially designed by the United States Navy to protect overseas operatives and political dissidents by masking the user's IP address.[191] Using Tor on the dark web, a person in New York, for example, can appear to be in South Africa. Tor became available to the general public in 2004 and is widely used to protect illegal online activities.[192] The site users are protected from law enforcement surveillance because investigators can only conduct word and phrase searches on clearnet search engines.[193]

To increase site security, Ulbricht required customers to use the new, anonymous cryptocurrency Bitcoin. Created in 2009, Bitcoin is a peer-to-peer electronic payment system that cuts out a third-party money manager like a bank or credit card company, which must report suspicious transactions to law enforcement for investigation.[194] The blockchain records all Bitcoin transactions on anonymous public ledgers between buyers and sellers; the ledger allows the seller to verify that that the buyer did not already spend the electronic currency.[195] Because the blockchain is a public record, investigators can

---

190 Clearnet is the accessible portion of the internet by conventional search engines. It is the portion of the internet that hosts most commercial websites. Wesley Lacson and Beata Jones, "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road," *International Journal of Cyber Criminology* 10, no. 1 (January 2016): 41, https://doi.org/10.5281/zenodo.58521.

190 Lacson and Jones, 42.

190 Lacson and Jones, 42.

190 Lacson and Jones, 45.

190 Declaration of Purpose, 31 U.S.C. 5311 §1020.302 (a) (i).

190 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, 2, accessed March 1, 2020, https://bitcoin.org/bitcoin.pdf.

190 Clearnet is the accessible portion of the internet by conventional search engines. It is the portion of the internet that hosts most commercial websites. Bilton, *American Kingpin*, 45.

191 Lacson and Jones, "The 21st Century DarkNet Market," 42.

192 Lacson and Jones, 42.

193 Lacson and Jones, 45.

194 Declaration of Purpose §1020.302 (a) (i)

195 Nakamoto, "Bitcoin," 2.

trace all transactions a person has made if they know the person's account number. Bitcoin allowed the Silk Road to flourish and the Silk Road symbiotically launched Bitcoin's acceptance as a currency.

While the Silk Road was growing quietly in the dark web community, it would soon gain worldwide notoriety. To spread the word about the website while remaining anonymous, Ulbricht—using the screenname Altoid—posted to a website for psychedelic mushrooms called Shroomery.com, asking if its users had heard about the Silk Road.[196] This post and another post on a website called Bitcoin talk, also from Altoid, were the first mentions of the Silk Road recorded on the internet. To publicize his philosophical views and explain how the government was wrong to deny people access to drugs, Ulbricht also cooperated anonymously with the website Gawker. Adrien Chen, an experienced blogger for the site, published his article on June 1, 2011, entitled "The Underground website Where You Can Buy Anything," announced the Silk Road to the world.[197] Publicity from the article generated thousands of new sales on the Silk Road, making Ulbricht very wealthy and drawing the federal government's attention. Senator Charles Schumer of New York and Senator Joseph Manchin of West Virginia called on the DOJ and DEA to shut down the site.[198]

Law enforcement was aware of the Silk Road website, however, before the Gawker article was published. During the winter of 2011, rookie HSI Chicago Agent Jared Der-Yeghiayan began looking into the Silk Road from the evidence recovered at the Chicago International Mail Center. The Silk Road's vendors exploited the international mail system to deliver its drugs; Der-Yeghiayan compared seized drug shipments from the mail facility to images of drugs advertised on the Silk Road to identify and arrest customers, who he

196 Bilton, *American Kingpin*, 45.

197 Adrian Chen, "Underground website Lets You Buy Any Drug Imaginable," Wired, June 1, 2011, https://www.wired.com/2011/06/silkroad-2/.

198 "Schumer Pushes to Shut Down Online Drug Marketplace," NBC New York, May 31, 2016, https://www.nbcnewyork.com/news/local/schumer-calls-on-feds-to-shut-down-online-drug-marketplace/1920235/.

then compelled to work with law enforcement.[199] This strategy eventually allowed law enforcement to confirm that Ross Ulbricht was DPR.

Chicago was not the only city investigating the Silk Road. In March 2011, HSI Baltimore formed the Marco Polo task force with the DEA to investigate and dismantle the Silk Road, using an undercover operation online to amass evidence. A key component of the investigation was the arrest of a Silk Road dealer who, when forced to cooperate with law enforcement, helped investigators target other dealers on the site.[200] Additionally, the DEA agent assigned to the investigation posed online as a Dominican drug dealer using the screenname Nob, and contacted DPR directly. Nob became friendly with DPR through multiple online chats, during which he advised DPR about how to avoid government investigations and how to obtain fake identification so he could hide his true identity if he needed to flee the country.[201] Nob did not document all of these conversations in case files. Because of this close relationship, DPR agreed to help facilitate a kilo sale of cocaine for Nob, which resulted in the arrest of Silk Road employee Curtis Green. Green would later present evidence against DPR and the Silk Road and serve as the principal witness for the Maryland U.S. Attorney's Office in its John Doe indictment of DPR. Nob, however, was having financial troubles in his personal life; his relationship with DPR led to several illegal transactions and his eventual arrest and conviction.[202]

Because HSI led two of the early Silk Road investigations, in the spring of 2012 the Chicago and Baltimore field offices held a contentious deconfliction meeting in Chicago.[203] During the meeting, the HSI Baltimore contingent declared that it would take the lead on the investigation because of the cooperating dealer. A heated discussion about the investigation ensued, which prevented the teams from sharing information or agreeing

199 Bilton, *American Kingpin*, 87.

200 Ian Duncan, "Fall of Online Drug Bazaar Silk Road Began with Tip to Md. Agents," *Baltimore Sun*, November 18, 2013, https://www.baltimoresun.com/maryland/baltimore-city/bs-xpm-2013-11-18-bs-md-ci-inside-silk-road-20131118-story.html.

201 Bilton, *American Kingpin*, 166.

202 Bilton, 94.

203 Bilton, 110.

to collaborate. The supervisors and prosecutors protected their own agents and their separate investigations; the supervisors yielded that they would deconflict targets when necessary, but they would not work together.[204]

One of the greatest contributions to the Silk Road investigation came from the FBI New York Field Office. The field office's cyber crimes squad started its investigation of the Silk Road by analyzing the computer traffic on the site, ignoring the dealers and customers who used it.[205] As the lead investigator for the FBI explained, his team was able to discover the location of the Silk Road server because, even though the server operated on the Tor network, the programmer (Ulbricht) did not configure the website's applications for Tor. This meant that when customers logged into the website, their IP addresses were leaked.[206] This allowed the FBI to determine that the Silk Road server was leased from a web hosting company and located in Iceland.[207] With the assistance of the Reykjavík Metropolitan Police, the FBI received a copy of the imaged server on July 29, 2013, allowing the team to begin their forensic examination.[208]

The multiple investigations into the Silk Road still had not identified DPR, nor were they able to take down the website. To rectify this situation and analyze all evidence from the different investigative agencies, the DOJ called for a deconfliction meeting in July 2013. In addition to analyzing the evidence from all the investigations, the DOJ planned to use the meeting to determine which unit would lead the investigation and which U.S. attorney's office would prosecute. The meeting was hosted by a chief from the DOJ Criminal Division and required the different investigators and prosecutors to present their evidence. Each unit spoke in turn; however, HSI Baltimore refused to supply any information, stating its case had already gone to a grand jury for the John Doe

204 Bilton, 110.

205 United States of America v. Ross Ulbricht, No. 1:14-cr-00068KBF (S.D. of New York) (September 5, 2014).

206 United States of America v. Ross Ulbricht, at 2.

207 United States of America v. Ross Ulbricht, at 5.

208 United States of America v. Ross Ulbricht, at 5.

indictment.[209] Additionally, before the meeting, HSI Baltimore warned Agent Der-Yeghiayan not to talk about his evidence out of fear that the FBI would attempt to take over his investigation.[210]

Unlike HSI Baltimore, however, the other teams at the meeting did share information. At the end of the meeting, the FBI informed the room that its team had a copy of the Silk Road server. As a result of the deconfliction meeting, the FBI decided that it would work with HSI Chicago to identify DPR and seize the Silk Road website. The sharing of the server information allowed other agencies to seek FBI assistance with their separate investigations. Gary Alford, an IRS-Criminal Investigator assigned to the DEA Strike Force, went to the FBI to analyze the server for his separate money-laundering investigation into the Silk Road. While at the FBI office, he and Der-Yeghiavan discovered that the server was once accessed from a bistro in San Francisco, indicating that DPR lived in or had visited San Francisco. Upon learning this, Alford informed the FBI agent that he had a possible subject in San Francisco. However, the FBI agent did not have faith in the information.

Also as a result of the deconfliction meeting, Der-Yeghiayan went to New York to work undercover with the FBI; by arresting dealers and monitoring Silk Road discussion forums, they able to identify DPR and, more importantly, secure his laptop. While Der-Yeghiayan was engaging in such discussions, he became friends with a person named Cirrus. Der-Yeghiayan located Cirrus's address and performed a knock and talk to discuss her activity on the illegal website.[211] As a result of this meeting Cirrus agreed to work with the investigators and allowed them to impersonate her on the website. Because Cirrus was a paid administrator for the Silk Road, this gave investigators access to all of the discussion forums.[212] Der-Yeghiayan took over Cirrus's account and monitored system

---

[209] Bilton, 240.

[210] Bilton, 238.

[211] A knock and talk is a police investigative tactic where they will speak with a person who they know is involved in criminal activity and try to gain their cooperation to target a more significant target that the person is working with.

[212] Bilton, *American Kingpin*, 246.

administrators' discussions, allowing him to see when DPR was accessing the server. Cirrus also gave Der-Yeghiayan screenshots of DPR's posts so Agent Der-Yeghiayan could understand Cirrus's history on the site and identify DPR by his writing style.[213]

Meanwhile, as his site became increasingly popular, Ulbricht became increasingly paranoid. Following Nob's advice, Ulbricht prepared to leave the country. In July 2013, to facilitate his life of obscurity, Ulbricht ordered nine fake driver's licenses from a vendor on the Silk Road.[214] The new IDs were intercepted by CBP and handed over to DHS for an investigation. On July 26, 2013, two agents from DHS went to the address listed on the fake ID envelopes to talk to the person who had purchased them. The agents met and interviewed Ulbricht and explained that they were not there to arrest him but wanted to know how he obtained the fake IDs. Ulbricht calmly explained that he was very protective of his privacy and had bought them on the Silk Road, explaining how to access it and use Bitcoin.[215] After positively identifying Ulbricht through his Texas driver's license, the agents ended the interview, returned to their office, and documented the interview with Ulbricht's real name and address on the report.

In late July, when the Marco Polo Task force learned that the FBI had the Silk Road server, the DEA's undercover agent, Nob, became anxious. For the previous few months, Nob had been communicating with DPR using pretty good protection (PGP) encryption and had not been documenting the conversations.[216] Nob encrypted these conversations because he was sharing case information with DPR in exchange for Bitcoin, and the DEA agent was fearful that non-encrypted information about his conversations with DPR might be on the server. The DEA agent attempted to gain access to the server, but the FBI denied him.[217] When he learned that the FBI had discovered DPR's identity, he tried to obtain the identity from the U.S. attorney who was prosecuting the Baltimore investigation so he

---

213 Bilton, 246.

214 Bilton, 254.

215 Bilton, 254.

216 United States of America v. Carl Mark Force IV et al., No. 3–15–70370 (N.D. California) (March 25, 2015).

217 Bilton, *American Kingpin*, 289.

could warn DPR to destroy his computer.[218] Nob (a DEA agent), along with a Secret Service agent, was eventually arrested for wire fraud, money laundering, and government property theft.

Meanwhile, when the FBI did not accept Alford's information about a possible subject in San Francisco, Alford began to investigate the lead again. Alford approached the Silk Road investigation differently; he used Google searches to examine all internet posts that mentioned the Silk Road, which led him to the post by Altoid on the Shroomery website on January 27, 2011.[219] Alford reviewed all of Altoid's posts online, on one of which included Altoid's email address, rossulbricht@gmail.com.[220] Next, Alford discovered a post—made from the username Ross Ulbrich—asking for help with Tor coding; after the post, the user changed his name on the site to Frosty.[221] Further Google searches revealed information about Ulbricht's education and libertarian views.

After the FBI refused his assistance, Alford conducted a new computer check to see if Ulbricht had any contact with the police. The new search revealed the report from DHS agents describing the fake IDs and their intended recipient, Ross Ulbricht. This information lead Alford to believe that Ulbricht was a target. With the new information provided by Alford, the Assistant United States Attorney (AUSA) discovered that Ulbricht's apartment in San Francisco was only a few hundred feet from the San Francisco bistro that the FBI identified in its investigation. During a conference between the investigators and the AUSA, the FBI agent who had examined the Silk Road server stated that DPR named the server Frosty—the same name Ulbricht had used in his inquiry about Tor. Der-Yeghiayan compared the writing style of DPR's Silk Road posts to Ulbricht's public posts on Facebook and discovered that they used similar phrases writing patterns.[222]

---

[218] United States of America v. Carl Mark Force IV et al., at 18.

[219] Nathaniel Popper, "The Tax Sleuth Who Took Down a Drug Lord," *New York Times*, December 25, 2015, https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html.

[220] Popper.

[221] Popper.

[222] Bilton, *American Kingpin*, 277.

With the new information provided by Alford, the FBI made Ross Ulbricht the lead suspect in the Silk Road investigation. Surveillance of Ulbricht in San Francisco confirmed his computer activity coincided with DPR's. The information provided by the three different agencies, working together, led to Ulbricht's arrest and the seizure of the Silk Road on October 2, 2013.[223]

After years of separate investigations by multiple agencies, the takedown of the Silk Road and arrest of DPR were the result of collaboration and information sharing. The DOJ's deconfliction meeting to improve the disparate investigative efforts was the catalyst. During its time on the dark web, the Silk Road generated almost $1.2 billion in sales and earned Ulbricht $80 million in commission, which the U.S. government seized through forfeiture.[224] The dismantling of the organization resulted in arrests of several hundred people in forty-three different countries. Consequently, the collaboration between the agencies magnified the individual work done by the investigators.

B. DECONFLICTION

In response to lawmakers' challenges to seize the Silk Road website and arrest the operator, several federal agencies began investigations into the site. HSI in Chicago and Baltimore conducted Silk Road investigations, along with the DEA's Strike Force and the FBI in New York. While these investigations had some success separately, it was their information sharing and collaboration that led to the seizure of the Silk Road. Two primary deconfliction meetings took place during the Silk Road investigation. The first one was between the HSI Baltimore and Chicago offices. The meeting, which was attended by management and the AUSAs prosecuting the investigation, achieved nothing, as institutional friction and competition between the two offices prevented any form of collaboration. Each office wanted the prestige that came with arresting DPR and taking down the Silk Road. Instead of mandating that their agents work together, the separate supervisors supported their agents in protecting their evidence, fostering a turf war rather

223 Popper, "The Tax Sleuth."

224 Matthew Goldstein, "Silk Road Case Began with Hunt for a John Doe," *New York Times*, March 21, 2014, https://dealbook.nytimes.com/2014/03/21/silk-road-case-began-with-hunt-for-a-john-doe/.

than a working relationship over the investigation. The deconfliction meeting may even have hampered the investigations; the agents developed no new leads and hoarded information.

The second deconfliction meeting, mandated by the DOJ, had a different result: it led directly to the arrest of DPR. Although the HSI Baltimore Marco Polo task force refused to share information to protect its investigation and indictment, the DOJ bureau chief convinced the other agencies to talk freely about their evidence, the most significant being that the FBI had the Silk Road server. The units' willingness to share their information allowed others to see new evidence and overcome turf wars. Importantly, the DOJ deconfliction meeting facilitated collaboration between the FBI and HSI Chicago, and allowed IRS Agent Alford from the DEA Strike Force to review the evidence. Had the three agencies not worked together, it might have taken months longer to identify DPR.

C. INFORMATION SHARING

The information sharing between the different agencies was key to solving the Silk Road investigations. However, institutional friction, turf battles, and egos prevented exchange of evidence that may have allowed one of the agencies to arrest DPR sooner. As Bashkar and Zheng indicate, management must communicate to employees that information sharing is necessary.[225] During the first deconfliction meeting between the Chicago and Baltimore HSI offices, however, the managers in the room prevented the sharing of information between the two agencies, and a turf battle started over the investigation. Baltimore believed that it was weeks away from DPR's arrest and did not need Chicago's help; Chicago thought Baltimore's investigation strategy would not work and did not understand the size of the Silk Road customer base.[226] During the DOJ's deconfliction meeting, HSI Baltimore again refused to disclose any of its information, claiming that doing so would affect its current grand jury proceedings on the case. HSI Baltimore also attempted to influence HSI Chicago without providing any evidence during the deconfliction, citing a lack of trust with the FBI.

[225] Bhaskar and Zhang, "Knowledge Sharing in Law Enforcement," 49.

[226] Bilton, *American Kingpin,* 111.

There were several instances of individual agents, too, refusing to share information. The FBI agent in charge of the Silk Road investigation refused to acknowledge the IRS agent's contributions to the investigation; the FBI agent did not think a lower-status agency like the IRS could contribute anything significant to the investigation.[227] Thus, the IRS agent refused to offer the information to the FBI, prolonging the investigation. Moreover, to protect his criminal actions, the DEA agent assigned to the Marco Polo task force did not inform his supervisors about all the conversations he had had with DPR, limiting the information in the case.

The information sharing between Agent Alford and the FBI, however, led directly to the identification of Ross Ulbricht as DPR. Alford overcame the FBI's disinterest in his information by showing the AUSA assigned to the case his strategy for identifying Ulbricht as a possible subject. The strength of this evidence built trust between Alford and the AUSA, which allowed the FBI to target Ulbricht with surveillance and confirm his identity as DPR. At the deconfliction meeting, Agent Der-Yeghiayan provided all the information he possessed about how to identify mail packages originating from Silk Road vendors, helping to get the drugs off the street. By impersonating Cirrus, the Silk Road employee, he allowed the FBI to identify the other Silk Road employees and confirm that Ulbricht was DPR.

The seizure of the Silk Road server posed a problem for the corrupt DEA agent who was posing as Nob. The DEA agent was providing DPR with case-related information and teaching him how to hide from the government in exchange for Bitcoin. Nob feared that some of his corrupt conversations with DPR may have been saved on the Silk Road server and would implicate him.[228] The actions of this corrupt undercover DEA agent show the dangers of too much information sharing. When the FBI informed the audience at the deconfliction meeting that it had the Silk Road server, it unwittingly informed the corrupt agent, who then tried to protect himself. The agent tried to gain access to the server to see if it contained any unencrypted files of his conversations with DPR. The FBI Agent in

[227] Popper, "The Tax Sleuth."

[228] Bilton, *American Kingpin*, 288.

charge of the investigation refused Nob's request, however, informing him that he needed permission from his supervisor to view the server information.[229]

D. COLLABORATION

Although the deconfliction meeting facilitated information sharing and led to the collaboration needed to identify and arrest DPR, early attempts at collaboration were not very fruitful. HSI Baltimore created the Marco Polo task force to investigate the Silk Road and try to identify DPR. Even though agents from the HSI, along with the DEA, made some arrests and online contact with DPR himself through discussion forums, these actions did not contribute to the other efforts to arrest DPR. Conversely, the Marco Polo task force attempted to prevent the Chicago investigation from moving forward during its deconfliction meeting so they could garner the credit for arresting DPR and seizing the website.

The first collaboration that affected the Silk Road investigation was between the DEA Strike Force, the FBI in New York, and HSI Chicago. The combined resources of the three investigative efforts led to the discovery of the bistro in San Francisco that accessed the Silk Road's server. Seeing that the server was accessed by a person in San Francisco led Alford to reexamine a person of interest from the area, Ulbricht. When Alford presented his new information to the AUSA, they discovered that the computer was named Frosty. The FBI's seizure of the server, coupled with the information provided by Der-Yeghiayan in his undercover role, helped confirm the information provided by Alford. Each agent used the other agency's information to develop his evidence further and identify DPR. Although Alford identified Ulbricht as a possible subject in March 2012, the lack of additional evidence prevented further investigation. The FBI's additional information about the server access in San Francisco and the DHS report about the fake IDs provided the additional evidence needed to investigate Ulbricht further.

Each team approached the investigation of the Silk Road differently, allowing it to develop different evidence. The FBI approached the investigation by looking for the server,

[229] Bilton, 289.

HSI targeted the mail shipments and the recipients to gain cooperation and access through employees, and Alford's DEA Strike Force conducted a money laundering investigation. Ultimately, the evidence produced by the different investigations, when analyzed together, provided enough information to identify Ulbricht as DPR.

E. CONCLUSION

When Ross Ulbricht created the Silk Road, he used the newest technology to keep himself and his buyers anonymous. Ulbricht capitalized on Bitcoin, the dark web, and Tor to prevent his arrest for over two years and created a new distribution model for drugs. It took the combined efforts of multiple law enforcement agencies—and missteps by DPR—to develop the evidence that identified Ulbricht and led to his arrest. The first deconfliction meeting between the HSI Chicago and Baltimore field offices failed because of ego and institutional friction. The second deconfliction meeting, hosted by the DOJ, forced information sharing between the different agencies. The meeting brought about the collaboration between the FBI in New York and HSI Chicago, but the critical component was when Agent Alford learned about the access to the Silk Road server in San Francisco from the FBI; this information prompted him to review past subjects, which uncovered additional evidence and made Ulbricht a subject. Alford's ability to identify DPR shows that significant information in an investigation can be provided by any person or agency. The relevance of that information will not be known until it is reviewed by all participants, and the only way that can happen is if all parties are aware of the information.

V. SEX MONEY MURDER

In the early 1990s, violence-plagued the streets of New York City; 1990 started the decade with 2,245 murders.[230] The crack epidemic turned most low-income neighborhoods into war zones, with gangs battling for territory to deal drugs. The residents of the Soundview Housing Developments in the Bronx saw the rise of one the most violent of these gangs. In 1992, Peter "Pistol Pete" Rollack, a teenage drug dealer, formed Sex Money Murder (SMM), a street gang whose drug-dealing empire would span several states and use violence and murder to protect its business. Rollack's influence and control were so significant that he was still able to control SMM from his prison cell after being sentenced on federal drug charges. With this power, Rollack would order executions from his jail cell of anyone he felt might testify against him.

This case study focuses on the collaboration of North Carolina State Police, a special gang task force in the New York City Police Department, and the ATF, which produced the evidence and testimony needed to sentence Rollack to life in prison. Although the investigation into Rollack and SMM took place before deconfliction was widely used in law enforcement, the National Crime Information Center database was used to list Rollack as a wanted felon, which allowed the police form North Carolina to indict him for drug trafficking. After the North Carolina indictment, the multiple law enforcement agencies began sharing information; together, they uncovered an even greater number of violent crimes committed by Rollack and his gang. This collaboration allowed law enforcement to charge senior members of SMM with violating the RICO statutes; the gang members then either cooperated with the federal government or were convicted.

230 Christina Sterbenz, "New York City Used to Be a Terrifying Place," Business Insider, July 12, 2013, https://www.businessinsider.com/new-york-city-used-to-be-a-terrifying-place-photos-2013-7.

A. EVENTS[231]

Growing up, Rollack idolized the Italian mafioso who brutally executed competitors; to ensure success and safety in the drug-dealing business, he knew he needed to control the Soundview Houses where he lived and not allow any competition.[232] In September 1991, Rollack and the other teenage members that would eventually form SMM began a drug war with the other dealers in the Soundview Houses.[233] The battle with the rival drug dealers lasted until November 3, 1991, when an associate of Rollack murdered a rival drug dealer in view of multiple witnesses.[234] The brazen acts of violence caused the older dealers to flee, leaving the Soundview Houses to Rollack and his dealers.

In the summer of 1992, Rollack officially started referring to his group of drug dealers and enforcers as Sex Money Murder. Their main goal was to make as much money as possible from dealing drugs, and they would murder anyone who tried to stop them.[235] Members of SMM had a strict code that did not tolerate police cooperation; they would kill anyone suspected of snitching, regardless of their rank in SMM. The snitching rule applied to everyone in the community, not just SMM's members. Rollack's violence extended beyond this rule, however. While visiting the annual Harlem Week Festival in August 1993, Rollack killed Keenyon Jenkins over a gambling debt owed to a friend. Then, on April 8, 1994, Rollack killed Karlton Hines, another local drug dealer, who Rollack had thought disrespected him in public. When Rollack killed Hines, a witness escaped without injury; to ensure the witness did not cooperate with the police, Rollack killed him too.[236]

To increase profits, Rollack expanded his organization into other housing developments. David "Twin" Mullins, who controlled the drug deals in the neighboring Castle Hill Houses, became a lieutenant in SMM and obtained his supply of drugs from

---

231 For a condensed timeline of events, see Appendix C.

232 Green, *Sex Money Murder*, 23.

233 Green, 92.

234 Green, 109.

235 Green, 136.

236 Green, 186.

Rollack.[237] SMM also expanded the drug empire outside New York City, with members moving to Kingston and Buffalo, New York, to establish SMM chapters and sell drugs. More significantly to Rollack and SMM, however, was their new relationship with an interstate trafficker, Savon Codd, who had a car with hidden stash boxes that could hold kilos of cocaine, money, and guns, which he used to transport the contraband between states.[238] Rollack and Codd expanded their interstate dealings to parts of North and South Carolina, significantly increasing the size of the SMM drug empire. They eventually established satellite gangs in multiple states, ultimately making SMM more powerful.[239]

Interstate trafficking was extremely lucrative for SMM. In October 1994, Rollack, Codd, and other members of SMM embarked on a trip in a Nissan Quest minivan containing a stash box loaded with drugs and weapons. The purpose of the trip was to "re-up," or resupply, the satellite locations and pick up the money from the previous drug sales. The SMM members traveled to Pittsburgh, then eventually North Carolina. In North Carolina, Rollack met with an associate in Rockingham, and the two men got in a dispute over a money shortage. Rollack gave the associate twenty-four hours to obtain the remaining money, or he would kill him and his family.[240] On October 21, 1994, while waiting for the associate at a fast-food restaurant, the police received an anonymous tip about a Nissan minivan transporting drugs and stopped Rollack and the SMM members.[241] After a canine detected drugs in the vehicle, the police removed Rollack and the SMM members to the station house, where Rollack and the others provided the police with fake identification and were released without the van so that the police could perform a more extensive search[242] During the more extensive search of the vehicle, the police discovered

---

[237] Green, 155.

[238] Green, 157.

[239] United States v. Rollack, No. 98–4272 (United States Court of Appeals for the Fourth Circuit) (May 2, 2014).

[240] United States v. Rollack, at 2.

[241] United States v. Rollack, at 3.

[242] United States v. Rollack, at 3.

the drugs and arrested Rollack and the others before they could return home.[243] When the police ran the fake IDs, they found no warrants and released the group on bail.

Rollack was not so lucky, however, during the Harlem Week Festival in August 1996, when he was arrested for possession of a firearm and the homicides of two rival drug dealers. While incarcerated in the Rikers Island jail complex and awaiting trial for the homicides, Rollack joined the United Blood Nation—an umbrella organization of the Bloods street gangs. The Bloods had a structural organization, a code of conduct, and connections in the prison system throughout the state—which protected the incarcerated members of the Bloods from the Spanish prison gangs.[244] Rollack's induction automatically made all members of SMM Bloods gang members as well, including his satellite operations in other states. United Blood Nation subsets provided protection and prestige in the members' criminal world, both inside and outside of prison.[245]

The violent acts committed by the SMM members instilled fear in the community, preventing cooperation with the police. Although he was free of the homicide charges—the witnesses had not cooperated with the investigation—Rollack received a sentence of two to four years for weapon possession. Additionally, on December 16, 1996, Rollack was indicted by the Western District of North Carolina for the October 1994 drug arrest.[246] The North Carolina State Police identified Rollack's fingerprints through the Nationwide Criminal Information Center (NCIC) after his arrest in New York City.[247] Rollack was moved to a jail in North Carolina to stand trial for the federal narcotics charges. Even while incarcerated in North Carolina, Rollack controlled the SMM members by coded letters sent through the mail, sending instructions to form a legal fund and continue growing the criminal empire in his absence.[248]

---

[243] United States v. Rollack, at 3.

[244] Green, *Sex Money Murder*, 217.

[245] Green, 219.

[246] United States v. Rollack, at 2.

[247] Ferranti, *Street Legends*, 249.

[248] United States v. Rollack, No. 90 F. Supp. 263 (Southern District of New York) (December 20, 1999).

While incarcerated in North Carolina, Rollack continued ordering murders as well. Rollack believed that several SMM members were cooperating with the police, violating his and the Bloods' snitching ordinance. For example, although David "Twin" Mullin was a high-ranking member of SMM, Rollack believed he was responsible for his arrest at the Harlem Week Festival and ordered his murder through a coded letter sent from prison.[249] While playing a Thanksgiving Day football game in front of thirty people at the Soundview Houses, SMM members killed Mullins and Efrin Solar and injured three other people.[250] In response to this public act of violence, the NYPD tasked a newly formed gang unit to investigate the homicides and SMM.[251]

Because of the public nature of the Thanksgiving Day homicides, the police asked other agencies for help with the investigation. The NYPD gang unit worked with the North Carolina State Police and the ATF to uncover evidence linking Rollack to the Thanksgiving Day homicides and the current drug trial. Members of the North Carolina State Police and the NYPD traveled from state to state to interview witnesses and informants. As a result of these interviews, the police gained cooperation from the associate Rollack had threatened to kill in October 1994. The interviews also allowed investigators to learn about the size of the SMM drug empire and, more importantly, the murders associated with Rollack.

To secure Rollack's conviction, the NYPD and the other agencies needed to prove to the jury that, even from a prison in North Carolina, Rollack was able to have people executed without question. The communication between Rollack and SMM was key to the prosecution. On December 17 and December 29, 1997, ATF agents obtained warrants allowing law enforcement to intercept the mail between Rollack and SMM members.[252] Members of the NYPD's gang team traveled to North Carolina and testified in court as experts on the Bloods gang, its hierarchy, and its code of honor. Additionally, the NYPD explained how Rollack controlled SMM through the mail with a coded language developed

[249] United States v Peter Rollack, No. S4 97 Cr. 1293 (MCG).

[250] Green, *Sex Money Murder*, 258.

[251] Green, 265.

,[252] United States v. Rollack, at 3.

by the Bloods and used to prevent law enforcement from developing intelligence on gang activities.[253] The testimony by the NYPD, the letters obtained from the search warrant, the evidence recovered from the minivan, and the cooperator's testimony resulted in Rollack's conviction and a forty-year prison sentence.

During Rollack's drug trafficking trial, the NYPD gang team, with assistance from the ATF and Southern District of New York U.S. Attorney's Office, targeted Rollack and the remaining SMM members with an organized crime (RICO Act) investigation. Additionally, the U.S. Attorney for the Southern District filed a notice with the court that it would seek the death penalty for Rollack.[254] Thanks to the evidence developed with help from the North Carolina State Police, the NYPD charged Rollack with six murders committed during his time as head of SMM. Members of the NYPD traveled to North Carolina to work with the State Police and the Charlotte Police Department, interviewing witnesses and gathering evidence. While the trial used some of the existing evidence from the North Carolina drug trafficking conviction to target all of SMM, it was the investigators' work during their trips to North Carolina and other states to gain cooperators against Rollack that secured his conviction. The letters used to convict Rollack for narcotics trafficking also described how SMM should expand its drug business and provide for the gang financially; the testimony by the cooperators described how Rollack killed or ordered the deaths of at least six people to keep control of his empire.[255] In November 2000, Rollack pleaded guilty, taking a deal that prevented him from receiving the death penalty. Rollack received life plus 105 years for his SMM leadership. Because law enforcement knew Rollack would still be able to control SMM from prison, a unique condition of his incarceration was that he received limited contact with the outside.[256]

[253] United States v. Rollack, at 4.

[254] United States v. Peter Rollack, at 1.

[255] United States v. Rollack, at 6.

[256] Green, *Sex Money Murder*, 322.

B. DECONFLICTION

The SMM investigation predated the creation of the SAFETEnet and Case Explorer deconfliction systems and occurred when deconfliction was not universal. Although law enforcement did not use a deconfliction system during the investigation, the NCIC system allowed for information sharing between the North Carolina State Police and the NYPD. When police arrested Rollack and other SMM members in North Carolina on October 21, 1994, they provided the arresting officers with fake IDs and were released on bond to return to New York. Their true identities would not be known until the FBI returned the fingerprints. When Rollack and the SMM members did not return to North Carolina, law enforcement issued a felony warrant in the NCIC.[257] Police discovered Rollack's outstanding warrant from North Carolina for firearms possession in August 1996, when the FBI confirmed his fingerprints among the evidence. Therefore, the discovery of the outstanding warrant led to communication between the NYPD and the North Carolina State Police regarding the drug trafficking charges. The notification allowed the State Police to indict Rollack and arrest him shortly after he was released from jail.

The use of a deconfliction system could have resulted in a faster arrest, however. When Rollack was arrested in North Carolina in October 1994 for drug possession, he had already gained a reputation in the Bronx for the violence perpetrated by SMM and the volume of drugs that he sold. In April 1993, the police arrested Rollack for narcotics possession in Kingston, New York. If the Kingston Police had registered Rollack in a system during this arrest, the North Carolina State Police would have contacted them in regards to that arrest. That communication could have led the State Police to indict Rollack several years earlier. Additionally, if the NYPD members had been investigating Rollack in 1993 or early 1994 and registered him in a deconfliction system, it would have provided another point of contact for the North Carolina State Police. Either of these registrations might have allowed for Rollack's indictment before the summer of 1997.

257 "National Crime Information Center (NCIC)," Federal Bureau of Investigation, accessed August 6, 2020, https://www.fbi.gov/services/cjis/ncic.

C. INFORMATION SHARING

Critical information sharing between the agencies included the notification between the NYPD and the North Carolina State Police about Rollack's arrest from the NCIC hit after Rollack's arrest at the Harlem Week Festival. Because of the notification from the NYPD, the State Police were able to draw up federal trafficking charges against Rollack. Rollack's resulting incarceration in North Carolina was devastating to his organization, as Rollack lost direct contact with his lieutenants and was forced to communicate by mail. The handwritten letters left a trail of evidence detailing his instructions to SMM. Although Rollack wrote the letters in code, they were not destroyed; eventually the letters were used as evidence at his trial to show his control of the organization.

Key to Rollack's prosecution, too, was convincing the jury that he was the head of SMM and that the contraband discovered in the minivan belonged to him. In 1997, during the trial, the Bloods gang was new to the East Coast and was not widely known outside major metropolitan cities. When SMM became an official Bloods set in 1996, the gangs in North Carolina also became Bloods sets and operated under the Bloods code. The NYPD provided knowledge and expertise about the Bloods to the North Carolina State Police, allowing them to understand how the gang operated. Also, the NYPD's testimony, translating the coded letters to the jury, allowed the prosecutors to show, in Rollack's words, that he was in charge of SMM.

D. COLLABORATION

It took the combined efforts of multiple police agencies and two separate federal prosecutors' offices to develop the evidence needed to convict Rollack and the other SMM members. The close interaction between the NYPD gang team and the North Carolina State Police developed the information needed to convict Rollack and sentence him to life in prison. The NYPD provided the prosecutors in North Carolina with the information that Rollack communicated with SMM using coded letters. This information allowed the ATF to obtain the warrants to seize Rollack's correspondence, which provided the proof of Rollack's role in the organization when the NYPD translated them for the jury.

The NYPD travel to North Carolina to interview cooperators and additional subjects in the investigation greatly enhanced the cooperation and the strength of the evidence against Rollack. While conducting these interviews, the NYPD discovered the number of homicides and shootings that Rollack had committed. With the assistance of the North Carolina State Police and Investigators from the Southern District of New York, the NYPD gang unit was able to identify six homicide victims. The combined efforts of the different agencies, in conjunction with several SMM cooperators, secured Rollack's conviction.

E. CONCLUSION

It took the combined efforts of multiple law enforcement agencies to identify and convict Peter Rollack for his acts of violence while he ruled his drug empire. Although the investigation into SMM took place before deconfliction was commonplace, the North Carolina State Police's use of the NCIC computer system to alert law enforcement of wanted felons led to Rollack's arrest. The information sharing about the arrest and the testimony provided by the NYPD gang unit members about the coded letters used to instruct the SMM were integral to the conviction. Additionally, the information developed by the NYPD during trips to interview cooperators provided the evidence needed to charge Rollack and the SMM members with the RICO statute for additional prosecution. Furthermore, the investigation conducted by the NYPD provided the evidence and the witnesses to charge Rollack with six counts of homicide, which forced Rollack to plead guilty to his charges to avoid the death penalty.

The investigation of SMM, along with the Silk Road and Operation Fast and Furious, shows that different agencies develop separate evidence during investigations, and very rarely does one unit uncover the entire picture of the criminal organization. Information sharing between them allows for a better understanding of the organization, can strengthen the evidence, and identify cooperators. Additionally, as the trust builds between the different agencies, they will work together in a more significant collaborative effort maximizing their resources and capitalizing on their information.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

This thesis posed the question: Can a single, nationwide deconfliction system for federal, state, local, and tribal law enforcement increase safety, information sharing, and collaboration? As of this writing, no federal, regional, or state authority has mandated deconfliction systems for all law enforcement agencies. Additionally, agencies decide which deconfliction system to use based on regional and personal preferences. As stated in an earlier chapter of this thesis, some states use multiple systems, even in the same region, which leads to confusion when law enforcement officers register targets and plan operational events.[258] Furthermore, not all law enforcement agencies have access to every deconfliction system, resulting in information gaps between agencies that put officers' lives in danger.

This chapter presents a policy options analysis that weighs the current state of deconfliction in law enforcement against two other possible options, drawing on examples from the case studies to illustrate what went well or could have gone better vis-à-vis the status quo. The policy options analysis judges the possible options based on the following criteria, and as shown in Table 1: deconfliction, which covers ease of use of the systems and officer safety; information sharing; collaboration between agencies; oversight of the system, which encompasses the use of the system by all agencies and the ability to monitor officer safety and duplication of effort; and funding, which deals with the waste of federal funding to maintain the multiple systems currently in use. The chapter concludes with a set of recommendations for policymakers in expanding the consistent use of deconfliction systems. Based on these inconsistencies and gaps, the current use of deconfliction systems may not be the best application of technology.

[258] See Chapter II.

Table 1. Policy Options: Status Quo, Two Systems, SHIELD

	Status Quo	**Two Systems**	**SHIELD**
DECONFLICTION	Fair	Good	Good
Ease of use	Fair	Good	Good
Officer safety	Fair	Good	Good
INFORMATION SHARING	Low	Good	Good
COLLABORATION	Low	Good	Good
OVERSIGHT	Low	Fair	Good
Mandate	Low	Fair	Good
Duplication of effort	Low	Good	Good
FUNDING	Low	Good	Low

The case studies in this thesis illustrated how the use of deconfliction systems and the investigative meetings that followed improved the evidence in the cases through information sharing and collaboration. Chapter III examined the failed ATF investigation Operation Fast and Furious, which showed how the current use of deconfliction alerted two separate federal agencies about a common target, leading to the sharing of vital information; however, the information was improperly used and resulted in a federal agent's death. In the Silk Road investigation, examined in Chapter IV, the information disclosed during deconfliction meetings led rapidly to the arrest of Ross Ulbricht and the seizure of the Silk Road website. Finally, Chapter V's Sex Money Murder case study explored how the collaboration between the NYPD, the North Carolina State Police, and the ATF developed the evidence to send Peter Rollack to federal prison for life. All three case studies show that when law enforcement personnel discover investigations into the same criminals and are willing to share information, they can keep officers safer and improve collaboration, which the current deconfliction systems limit.

A. OPTION 1: STATUS QUO

The first option is to keep the existing, mismatched deconfliction systems and optional participation by law enforcement agencies. Despite its limitations, does, to an extent, keep officers safe while allowing for some information sharing and collaboration. Moreover, to address the issue of the multiple systems, in 2016 the National Criminal Intelligence Resource Center (NCICC), under the BJA, announced the interconnection of SAFETnet, Case Explorer, and RISSafe for event deconfliction with the Partner Deconfliction Interface (PDI), which allows a user to access the other systems, but only for event deconfliction.[259] However, the three systems' interconnection through the PDI does not include the federal deconfliction database, DICE, so investigators must still check multiple systems to ensure that investigative targets are free of conflict. Also, the New York/New Jersey HIDTA SAFETnet does not participate in the PDI, thus reducing the system's effectiveness. While the PDI provides only event deconfliction for its users, it does improve officer safety and reduce the number of computer checks required for law enforcement.

Compounding the issue, neither DOJ nor DHS has called for the mandatory use of even one deconfliction system by all law enforcement agencies. While the federal government requires the use of DICE, it does not require the nearly 17,000 law enforcement agencies in the country to use any of the available deconfliction systems. Some agencies, like HSI and the FBI, have issued policies to compel their investigators to use the local region's deconfliction system and the federal DICE system.[260] The Policy Event Deconfliction Group—an advisory board that oversees deconfliction and comprises members of the DEA, BJA, and the Office of the Program Manager, Information Sharing Environment (PM-ISE)—liaises with participating agencies to answer technical questions and develop policy on the systems requirements, though not on the system's usage.[261]

---

259 "Officer Safety Event Deconfliction: Frequently Asked Questions," National Criminal Intelligence Resource Center, April 2016, 2, https://www.ncirc.gov/Deconfliction/Documents/Event_Deconfliction_FAQs.pdf.

260 Department of Homeland Security Office of Inspector General, "Law Enforcement Cooperation on the Southwest Border," 6.

261 National Criminal Intelligence Resource Center, "Officer Safety Event Deconfliction," 4.

Nevertheless, the body of advisors does not have the authority to force any law enforcement agency to participate. However, even if the systems' use were mandated, compliance with that mandate would be difficult to monitor or measure.

Furthermore, there is little or no oversight for the use of deconfliction systems, be they federal, regional, or statewide. Without a unit or agency monitoring the deconfliction systems, law enforcement cannot obtain data to improve officer safety by preventing blue-on-blue incidents. Law enforcement agencies might lack information because they may not report a blue-on-blue incident, or they may only record the incident in one system. As pointed out in a Government Accountability Office report, the federal government currently does not hold entities funded by the DOJ, DHS, and ONDCP accountable for the lack of coordination.[262] When investigators discover an overlap through deconfliction, members might share information about the subject and target the organization together, facilitating a quicker resolution. Alternatively, when they discover a conflict, one investigator might turn his investigation over to the other investigator if he has more persuasive evidence against the subject. Oversight of the deconfliction systems will law enforcement agencies throughout the country to use the systems more fruitfully and will allow for increased data on safety issues, which will benefit the investigators.

Some components of the federal government acknowledge the risks of multiple deconfliction systems. As previously discussed, in 2019, the DOJ and DHS's combined OIG offices issued a report on law enforcement cooperation between the FBI and HSI along the southwest border (SWB).[263] This report recommendations for improving cooperation between the two agencies; the majority of these recommendations dealt with developing written policies on how the agents should deconflict with each other. Additional recommendations included training the agents assigned to the SWB to ensure that they know about the other agency's deconfliction policy. While the recommendations mention the FBI and HSI, they leave out the DEA, ATF, or any other federal, state, local, or tribal law enforcement agency that conducts operations along the SWB.

---

[262] Larence, *Information Sharing*, i.

[263] See Chapter II.

Funding also contributes to the inefficiencies associated with the deconfliction environment's current makeup. The three regional deconfliction systems are all funded by the federal government. Funding for SAFETnet and Case Explorer comes from the same agency, HIDTA, which receives funding from the Office of National Drug Control Policy RISS receives its funding from the Bureau of Justice Administration. The use of multiple systems funded by taxpayer dollars to provide the same service is wasteful. Additionally, along with the federal government's funding comes oversight of the agency to ensure that the money is spent correctly per grant requirements. The funding of multiple systems is an additional waste of resources that could be applied elsewhere.

The following subsections detail how the criteria for the policy options were used to gauge the current deconfliction systems, and to show how the two proposed options would have helped or hindered investigations based on the case studies.

1. Deconfliction

Members of law enforcement are aware of the shortcomings of the current deconfliction setup. They must check multiple databases and hold meetings to further deconflict with other agencies, which consumes time and manpower. In Operation Fast and Furious, the lead agent for the investigation correctly listed her targets in the DICE system, which led to a conflict with the DEA over a joint target; the deconfliction meeting between the two agencies avoided a possible friendly fire situation and led to the sharing of vital information. However, while deconfliction registration and meetings were successful, the agent needed an analyst from the DEA to input the information into the system, as she did not have access to it. Requiring assistance from another agency may lead to further investigation delays, increasing the dangers to law enforcement. The outside investigator might challenge the reliability of the other agency or may see that agency as a competitor for the casework and try to steal the investigation.

2. Information Sharing

The use of the DICE system illustrates how different agencies can share information when a conflict in the system brings them together. In Operation Fast and Furious, upon learning about the conflict with the DEA, the lead ATF agent scheduled a

meeting to discuss their cases; this meeting led to a significant exchange of information between the agencies. During the meeting, the ATF identified a drug trafficking subject for the DEA. The DEA provided significant information from its investigation, too, which eventually helped the ATF obtain a Title III eavesdropping warrant for the investigation—a priority for the investigator.

The Silk Road investigation, too, illustrated the usefulness of deconfliction meetings. When the FBI informed the other agencies about the Silk Road server's seizure, outside agencies could review the information at their offices. During an office visit, the IRS-CI learned that someone had accessed the Silk Road server from San Francisco, the home city of a possible suspect, Ross Ulbricht. The IRS-CI presented this information to the AUSA assigned to the case with enough collaborating information from the other investigators to allow them to surveil and target Ulbricht. However, the announcement of the server seizure also alerted the corrupt DEA agent assigned to the HSI Baltimore task force that he was in danger of being discovered. The agent attempted to access the server and learn DPR's identity to warn him and protect his criminal actions. The sharing of this information in a public forum almost compromised the investigation and allowed for DPR's escape. If the deconfliction landscape's current makeup continues to exist unchanged, law enforcement agencies will still face gaps in information sharing and collaboration and will continue to face a safety threat when sharing information in a meeting. During the Silk Road investigation, most of the separate investigators might not have known about the other cases had it not been for the deconfliction meeting—the vehicle for sharing information. That meeting allowed all stakeholders to address the lack of information sharing among the agencies and develop their evidence, thus overcoming the deconfliction systems' shortcomings.

3. Collaboration

Investigators miss opportunities to collaborate on investigations because they do not know about other agencies' activities. During Operation Fast and Furious, HSI and ATF held a deconfliction meeting regarding a firearms seizure made by HSI in Naco, Mexico. To foster better cooperation between the two agencies, HSI agreed to stop its

firearms investigation and supply one agent to the ATF team; the HSI agents' role was to facilitate information sharing between them. The HSI special agent in charge agreed to this arrangement because of a memorandum of understanding that stipulated an increase in information sharing; it was necessary to settle disputes at the lowest supervisory levels. However, the information provided to the agent was limited. The HSI agent was given routine tasks and excluded from meetings. The use of multiple systems led to information gaps and missed communications among the agencies; streamlining the process would have led to greater collaboration.

While the status quo is an option, it does not help improve information sharing and collaboration. Law enforcement agencies are left with the multiple systems and information gaps that can lead to safety issues for investigators. Even if the PDI is expanded to include target deconfliction, issues will still arrive due to lack of oversight and inconsistent use. Additionally, overlapping investigations by multiple waste resources, and funding must go into the multiple systems. For these reasons, law enforcement should consider changing their current deconfliction system.

B. OPTION 2: TWO SYSTEMS

The second option considered here is for law enforcement to simplify the deconfliction picture by reducing the number of systems down to two. If all law enforcement agencies—federal, state, local, and tribal—used only one of the interconnected regional systems—either SAFETnet, Case Explorer, or RISSafe—and the federal government's DICE system, it would increase safety. This option would provide investigators with the information on both event and target deconfliction and would no longer require the PDI. A reduction in the number of systems would limit confusion among law enforcement agencies about which system individual states use. Additionally, consolidating input to two systems would increase the amount of information therein, greatly benefiting law enforcement. Moreover, the increased information would allow for greater communication and information sharing among agencies.

Additionally, RISS and HIDTA could require the agencies to implement a self-inspection program that would require them to audit the systems periodically to ensure

proper use. The requirement of a self-inspection program under the terms of use for the system ensures compliance from the law enforcement agency. With all the deconfliction events and targets entered into one of the two systems, it would be easier to study the information and determine the number of enforcement operation failures and investigative overlap. An essential problem with this deconfliction option is that, while it would reduce investigative conflicts, it would not resolve them completely. The investigators would still need access to two separate systems to conduct their checks. Additionally, this option does not address the problem of requiring all law enforcement agencies to use the systems. It still makes deconfliction an option for each agency.

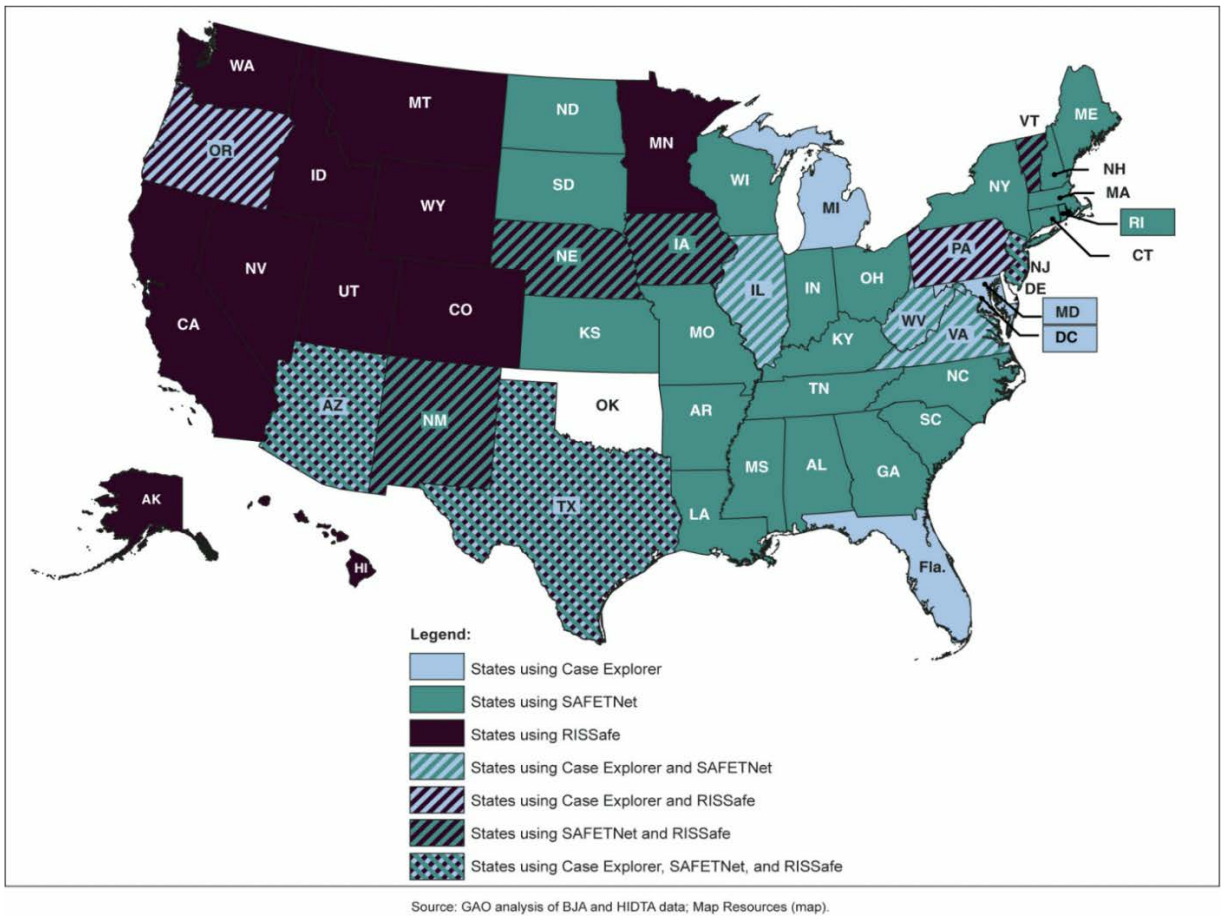
This policy option would also allow the agencies to audit the systems for misuse, training, and investigative overlap. The DOJ's OIG could oversee the DICE system, as the DEA is under the DOJ. Since RISS and HIDTA developed and maintained their systems, they could provide some oversight in conjunction with the agencies that use the systems. RISS or HIDTA could monitor the systems for suspicious activity and notify the appropriate agency if discovered.

As stated previously, the funding for the three systems comes from multiple government organizations. HIDTA funds Case Explorer and SAFETnet from the ONDCP, and the RISSafe system receives funding from the BJA, while the DEA funds DICE. Reducing the deconfliction environment down two systems, one regional system and the federal system, will also reduce the amount of money spent on the other two systems, leaving more money for other criminal justice programs, like community outreach or officer training.

1. Deconfliction

The use of only one regional system nationwide would have made increased safety in the SWB region during Operation Fast and Furious. The Fast and Furious investigation tracked firearms purchases as they moved from Phoenix, Arizona, to Mexico; the traffickers needed to transport the weapons through at least one additional county in the state before they reached the Mexican border. Arizona is one of the states that uses all three regional deconfliction systems: RISSafe, SAFETnet, and Case Explorer (see Figure 2,

which is a replication of Figure 1). Although the reduction to one system used by all the agencies would have increased law enforcement's safety and ensured proper notifications to the lead case agent, it only would have done so if law enforcement officers used the system to register the events.



Source: GAO analysis of BJA and HIDTA data; Map Resources (map).

Figure 2. Deconfliction Systems by State (Replicated from Figure 1 for Your Convenience)[264]

2. Information Sharing

As shown in the Silk Road case study, the HSI Chicago office and Baltimore Office learned of each other's investigations through their case management systems, not through

264 Source: Larence, *Information Sharing*, 30.

a registration conflict. The system design allowed agents to read other agents' case files, with the agent being alerted by an email. Because of this design, agents viewed each other's reports about their investigative status and eventually held a deconfliction meeting in Chicago to discuss their progress. The use of the deconfliction systems to initiate contact and share information would increase the integrity of the investigations and investigators' safety. A notification through a registration conflict only results in the person learning that someone else is interested in a subject; it does not contain any investigative facts. The investigator would only divulge any pertinent case information through direct communication. While this form of direct communication will increase the investigation's security, it relies on investigators' willingness to discuss the case with someone else and not hoard the information.

3. Collaboration

The reduction down to one regional system would allow either the BJA or HIDTA to redirect the funds used for their regional system maintenance to other programs. HIDTA helps local law enforcement agencies target and dismantle narcotics organizations in specific regions around the country. Defunding one or both of their regional systems would allow the agency to fund additional task forces and provide assistance to the state and local police. Similarly, the BJA could use RISS's funds, instead, to enhance its mission of developing collaboration and partnerships through its grant programs. While the funds may not be substantial, this policy option would still end the unnecessary, duplicative systems.

C. OPTION 3: SHIELD

The third option is to build an entirely new database to address all the complex deconfliction issues identified in this thesis. Because current deconfliction methods in the United States are insufficient, the Secure High-Speed Investigative and Event Law Enforcement Deconfliction (SHIELD) database, conceived by this author, and its accompanying policy would replace the existing systems. All law enforcement agencies would participate in the system, which would come with an oversight unit to measure compliance. SHIELD would also assess officer safety and duplicative work and allow registered users to communicate about possible investigative conflicts at the lowest level.

Additionally, to capitalize on the existing technology, the users would submit and register subjects and events from the field through agency smartphones. Along with the greater oversight, this system would be more easily monitored for misuse of information regarding sensitive cases.

The SHIELD database would be the only system in the United States for law enforcement to register investigative targets and planned operational events. Investigators would register a person, vehicle, address, or other identifiable information about an investigative target or planned enforcement event in the system and receive ownership of the registration. If a conflict occurs from the registration, both the registered owner and the person attempting the registration would be alerted with an email from the system containing each investigator's contact information. The dual email alert would allow direct communication between the investigators, who could then share information, facilitating collaboration.

Furthermore, the SHIELD database would increase the security of an investigation. Supervisors would receive notifications when another investigator attempts to register a designated sensitive investigation subject, enhancing the case's security. If an investigator tries to register the subject of a sensitive investigation (e.g., terrorism, public corruption, high-profile person), the system send an email to the supervisor and to the investigator who initially registered the subject. The supervisor must contact the other investigator's supervisor to discuss the subject and the investigator's evidence. The supervisors would then confer before interviewing the investigators; if either investigator does not have valid evidence for registering the subject in SHIELD, the supervisor in charge of the sensitive investigation can notify internal affairs. This notification system helps reduce inquiries into sensitive investigations and prevents possible exploitation by corrupt law enforcement officials. A single deconfliction system alleviates the need to monitor multiple systems and allows law enforcement to register updates, increasing safety.

Law enforcement officers need easy access to the deconfliction system to obtain information in real time. The SHIELD comes with state-of-the-art mobile technology, allowing law enforcement to increase the safety for personnel during operational events. Investigators can access the SHIELD database in the field through an agency- or

department-issued smartphone, which is connected to the system through a protected virtual private network—thus allowing investigators to register an event location during undercover operations. Undercover narcotics or gun buys are complicated operations in which the safety of the undercover officer is paramount. During some undercover buys, the drug dealer will meet up with the undercover and move to another location, either by car or on foot, to improve the security of the transaction and to look for the police. Having access to the SHIELD system through a smartphone will allow the investigator to register the drug buy's new location. The event registration will increase the undercover's safety by alerting other agencies about the operation if they attempt to register an event.

To ensure participation from all law enforcement agencies on the state, local, and tribal levels, the DOJ and DHS should make access to federal criminal justice and homeland security federal grants contingent upon participation in the system. The Ed Byrne Memorial Justice Assistance Grant (JAG) Program, for instance, provides federal grants for a range of criminal justice services to nonfederal law enforcement agencies.[265] Just as the federal government proposed penalties on states that would not raise the legal drinking age to twenty-one in 1984, they could penalize law enforcement agencies for not participating in the SHIELD database. For instance—and although doing so may require congressional approval—if the state, local, and tribal agencies fail to participate in the SHIELD database, they would see a 10 percent reduction in funds through the JAG. Tying the use of the SHIELD database to grant funding gives a powerful incentive for all law enforcement agencies to use the system.[266]

The SHIELD deployment would alleviate most of the issues identified in the joint FBI and HSI OIG report mentioned previously in this thesis; but it would reach further, as it would apply to all law enforcement agencies, not just the FBI and HSI. Because the SHIELD system would mandate use by all law enforcement agencies and have set

265 The Public Health and Welfare, 42 USC § 3751(a).

266 The Organized Crime Drug Enforcement Task Force puts similar limits on their funding to state and local agencies. Any funds provided by OCDETF for overtime must be earned by a full-time task force officer working on an OCDETF case. Additionally, funding for overtime cannot be used for the purchase of information or equipment.

procedures governing its use, it would eliminate the need for MOUs between agencies, making it easier for them to share information and work together.

The government would need a full-time agency to ensure that all law enforcement agencies are using the system correctly and in compliance with the money received from the JAG. This oversight group would collect information about the system's use, like the number of blue-on-blue incidents prevented by event deconfliction each year, which would allow them to analyze the incidents and issues training memos. An oversight agency can also enhance coordination and reduce investigative overlap, facilitating more efficient use of resources. An office composed of members from both the DOJ and DHS OIG should assume these duties; this combined office would have the authority to investigate all the federal components that use SHIELD. This new unit could also refer smaller investigations to the appropriate internal investigative unit when it involves non-criminal issues or improper use of the system for the state, local, and tribal levels of law enforcement.

While it may be costly to develop the SHIELD database, it could potentially save money for the government in the long run. After the initial investment to build and deploy the system, the government would need only to maintain one deconfliction system, not the multiple systems that are currently in use. This option will allow for more money to be allocated to the public for other criminal justice programs, just on a larger scale.

1. Deconfliction

During Operation Fast and Furious, the use of multiple deconfliction systems complicated the investigation and increased the dangers to law enforcement. The lead case agent needed a DEA analyst to register data in the DICE system, which forced her to rely on another agency to accomplish her work. Access to the SHIELD database would have allowed her to complete the registration herself; any other agent would have then been notified if they entered conflicting data into the system. This would be more efficient and would ensure that the subjects are properly registered. Additionally, with the registration in a single system, there would have been fewer dangers for law enforcement in Arizona.

2. Information Sharing

During the Silk Road investigation, multiple agencies and task forces across the country were conducting simultaneous independent investigations, some of them unaware of the parallel investigations. Registration of the subjects in the SHIELD database would have led to notifications among the different investigators, which would have allowed the investigators to discuss their evidence; this information sharing could have led to significant improvements in the case before the DOJ held the mandatory deconfliction meeting. The exchange of information could have led to faster collaboration among the agencies, allowing for a quicker end to the investigation and the illegal Silk Road activities.

3. Collaboration

In the Sex Money Murder investigation, multiple agencies had to collaborate to convict Rollack. After Rollack was arrested and released in North Carolina, he returned to New York and never left the city again. While the State Police issued a warrant for Rollack's arrest and listed it in the NCIC system, they did not notify the NYPD about Rollack's North Carolina crimes. If the State Police had registered Rollack in the SHIELD database, they would have received a notification when the NYPD member attempted to register him in New York. The notification would have allowed the agencies to work together sooner, targeting Rollack and the other SMM members. An earlier arrest would have saved lives and improved the quality of life in the Soundview Houses of the Bronx, which was plagued by the crack epidemic and SMM violence.

D. HYPOTHETICAL SCENARIO

This section presents how a hypothetical law enforcement operation would play out with each of the policy options proposed in this thesis. The scenario itself describes the status quo, and the following paragraphs describe the remaining two options: the two-systems approach and SHIELD.

(1) The Scenario and the Status Quo

Using an undercover agent, HSI is planning a drug buy from a known drug dealer along the SWB in Texas. The lead agent prepares the undercover agent's operation plan,

listing all the computer checks he conducted on the dealer. To ensure the undercover agent's safety, the agent has registered all available information about the dealer in the federal DICE system; additionally, because of the number of law enforcement agencies that operate along the SWB, the agent has registered the dealer and the proposed buy location in all three regional systems, RISSSafe, Case Explorer, and SAFETnet. At the meeting location, the dealer tells the undercover agent that the drugs are at a different location, and he must follow him to complete the transaction. The dealer is driving a previously unknown vehicle, which the agent has not registered. The unknown vehicle and the new buy location increase the dangers to the undercover agent, who must decide if the operation is worth the dangers before proceeding. To ensure the undercover agent's safety, the lead agent asks another agent to check the new car and location, which will take the agent some time. After learning that there are no conflicts, the drug transaction proceeds without further delays.

(2) Two Systems

If the scenario were conducted using the DICE and SAFETnet systems only, the workload of the lead agent would be reduced: he would only need to conduct searches in two databases to register the subject and the event. However, the agent would still need to have another agent in the office register the new car and buy location while they were in the field. That said, the agent would have been able to conduct those searches faster because he would only need to search two systems.

(3) SHIELD

If the scenario were conducted with use of the SHIELD database, the planning and operation would be less complicated and more secure. Instead of conducting multiple database inquiries while planning the undercover buy, the agent would have only needed to access the SHIELD database to register the event. Additionally, when the dealer arrived in an unknown car and changed the buy location, the agent or a member of his field team could have registered the car and the new location from the field, ensuring the undercover agent's safety by confirming that no other agency was investigating the dealer or planning an event at the new buy location.

E. RECOMMENDATION

The analysis in this thesis shows that the current deconfliction model hinders information sharing and creates safety issues for law enforcement. Considering the complexity of the various deconfliction systems and their importance to law enforcement personnel, a wholesale change to the deconfliction environment—the SHIELD option—might prove difficult, as the system will come with a new set of requirements and policy. This option would also require congressional legislation and the creation of a new oversight body, which may prove too time-consuming or challenging. The new database itself may also be costly and time-consuming to create, particularly considering the FBI spent almost $500 million and over ten years creating its current management system.[267]

The option to limit deconfliction to two systems may therefore be the most logical move for the law enforcement community. The continued use of the DEA's DICE system in conjunction with the expansion of either SAFETnet, Case Explorer, or RISSafe is feasible and provides the most significant benefit to law enforcement. With only two systems to access and search for deconfliction targets and events, investigators would have greater confidence that their operations are safe from other law enforcement personnel and that no one else is targeting their subjects. The reduction down to two systems would also allow for some monitoring and auditing to improve officer safety and identify waste. This option would incur no additional cost for design and deployment, and allows the funding for the discontinued systems to be reallocated. Additionally, the increased information in the systems would help law enforcement better navigate the increasingly complex criminal environment. Universal use, however, is necessary for successful information sharing and collaboration. This option, by itself, does not improve participation among the agencies; this issue needs to be address by the law enforcement community through training.

To compel agencies to use the systems, and to use them properly, the law enforcement community will need support from the DOJ and the DHS. A mandate requiring the use of the systems by all agents will help overcome current reluctance and

267 "F.B.I. Computer System Is Late and Over Budget, Report Says," *The New York Times*, October 20, 2010, https://www.nytimes.com/2010/10/21/us/21brfs-FBICOMPUTERS_BRF.html.

press enforcement at state, local, and tribal levels. If organizations like the International Associations of Chiefs of Police and the Police Executive Research Forum request that member agents or agencies use the systems, they can also help increase public knowledge about the systems and their use.

With greater participation and only two systems, it will be easier to collect data collection for safety reports of investigative overlap. The agencies that operate the systems will be able to monitor the systems more closely, allowing them to generate reports based on safety issues. Also, the agencies will be able to identify how often multiple agencies target the same people and monitor resources. While the internal report generating would not be as robust as it would be with an OIG monitoring the system, the reports will still be significantly more comprehensive than anything currently generated.

The reduction down to one regional system will also address the waste of resources; no longer would law enforcement need to fund three-separate regional deconfliction systems. Money allocated by either the ONDCP or the BJA that supports the three systems could be redirected to, or instance, counter-drug programs and treatment programs.

F. CONCLUSION

This research asked how a single, nationwide deconfliction system for federal, state, local, and tribal law enforcement might increase safety, information sharing, and collaboration. The thesis examined how the different deconfliction systems law enforcement currently uses lead to confusion and safety issues, and how they limit investigators' opportunities to connect with other agencies investigating similar targets, which can cause them to miss vital evidence that might lead to the subject's arrest. Additionally, multiple systems increase the dangers to law enforcement personnel who are conducting proactive street investigations.

As shown in the case studies, deconfliction plays a vital role in law enforcement investigations; how the investigators use the knowledge gained from deconfliction meetings is up to them. The lead agent in Operation Fast and Furious deconflicted through

personal meetings and the federal deconfliction database, DICE.[268] Because the agent used the proper system to register her subjects, she received a notification when another agent attempted to register the same subject. The conflict allowed the agencies to meet, and the information the ATF received during the meeting helped them obtain the Title III wiretap.[269] While the ATF used the deconfliction process correctly and prevented a possible blue-on-blue situation, they failed to capitalize on the information provided by the other agency, which prolonged the investigation and resulted in the death of a Border Patrol agent.

Ross Ulbricht used modern technology to create the Silk Road online drug empire that stymied multiple law enforcement agencies for several years. During the website's life, law enforcement agencies investigated Ulbricht under his pseudonym, DPR, but were only able to arrest low-level dealers on the site. As a result of a deconfliction meeting at the DOJ, however, all the agencies investigating the Silk Road began to make progress; their collaboration led investigators to identify Ulbricht as DPR and seize the Silk Road website.[270]

The Sex Money Murder gang dealt drugs and death across the Bronx while making millions of dollars, eventually exporting their drugs and violence around the country. Collaboration between the NYPD gang team, the North Carolina State Police, and the ATF, however, led to two federal convictions against gang leader Peter Rollack and the incarceration of other members of SMM. Together, the three agencies were able to develop the necessary evidence and testimony to see Rollack face the death penalty. While the agencies' collaboration did not come about because of deconfliction, the NCIC notification allowed for the initial notification and information sharing between the agencies.[271] The investigators convicted Rollack for drug trafficking in North Carolina and also discovered his connection to multiple homicides, forcing him to take a life-sentence plea.[272]

---

[268] Department of Justice Office of Inspector General, *ATF's Operation Fast and Furious*.

[269] Department of Justice Office of Inspector General, 122.

[270] Bilton, *American Kingpin*.

[271] Ferranti, *Street Legends*, 249.

[272] Green, *Sex Money Murder*, 312.

With multiple deconfliction systems in use, and with no policy or mandate for law enforcement agencies to participate in the systems, deconfliction is not as effective as it could be. In creating the PDI, the HIDTA and RISS governing boards acknowledged that the separate deconfliction systems are inefficient and dangerous. If the boards of HIDTA and RISS, along with the federal partners, cared about officer safety, however, they would address the current problems with deconfliction to simplify—and make mandatory—the system's use. Realistically, there is no significant downside to the proper use of a deconfliction system; there are only safety benefits, increased information sharing, and collaboration. These benefits outweigh the one possible drawback, corruption.

While the SHIELD database, with proper oversight and incentives for use, would be the ideal method to solve the current deconfliction issue, its creation would be complicated. However, if law enforcement agencies choose to reduce the number of deconfliction systems down to two—one regional system and the federal system—the less complicated model, combined with a strong push by the law enforcement community for universal use, would alleviate some of the problems identified in this thesis. The elimination of information silos, first and foremost, would benefit everyone who participates in investigative efforts. For law enforcement to be successful, agencies need to work together and share information; while deconfliction systems help keep officers safe, they also bring agencies together. The implementation of incremental improvements to the system will increase officer safety during field operations, increase collaboration across agencies, and reduce waste in funding and investigative overlap. These small changes can occur if the federal law enforcement agencies, along with the governing boards for HIDTA and RISS, collectively address this issue with police fraternal organizations across the country.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. OPERATION FAST AND FURIOUS TIMELINE

October 2009	ATF Phoenix Field Office establishes Group VII, the lead investigative unit.
October 31	Group VII is notified by an FFL holder of the purchase of a suspicious firearm by Jacob Chambers..
November 1–4	Group VII learns of three additional purchase incidents made by new subjects at several FFL holders locations.
November 18	Group VII connects the different individuals through surveillance and officially opens the investigation.
November	Jamie Avila is identified as a subject of the investigation.
November 20	Group VII learns of the Mexican seizure of forty-two firearms in the Naco, Sonora, region of Mexico. Several identified subjects purchased these firearms. HSI agents from ICE interview the arrested subjects.
November 30	ATF hosts a deconfliction meeting with ICE. ATF takes the lead on the investigation and ICE agrees to assign an HSI agent to the case.
November	All identified firearms are entered into the Suspect Gun Database by case agents. The lead case agent submits six phone numbers to DEA for deconfliction in the DICE system.
December 1	Group VII identifies 341 firearms from local FFL holders, purchased by as many as 15 subjects.
December 9	Firearms purchased during the investigation begin to be recovered by Mexican authorities from cartel members.
December 11	Manual Celis-Acosta is identified as a subject.
December 14	A DEA analyst attempts to register Jacob Chambers's phone number and discovers a conflict with ATF. They schedule a deconfliction meeting for December 15.
December 15	At the deconfliction meeting, the DEA states that Celis-Acosta is dealing with a subject, Manual Marquez. The DEA gives the ATF permission to approach Celis-Acosta, but only if the ATF is present. The ATF does not act on this information. The DEA

	provides the ATF with information that will allow the DEA to obtain a Title III wiretap warrant.
December 17	The ATF and the first FFL holder hold a meeting to discuss the number of firearms sold. The FFL holder is concerned about the number of guns sold and officer safety, and that he is implicating himself in the case. The ATF informs the FFL holder that they are doing everything possible to recover the firearms.
December 22	The DEA informs the ATF about a transfer between Celis-Acosta and another person in El Paso, Texas. The ATF does not conduct surveillance due to manpower constraints.
December	By the end of December 2009, the nineteen subjects of Operation Fast and Furious have purchased 690 firearms.
January 4, 2010	Group VII decides to obtain a Title III wiretap warrant for several subjects in the investigation.
January 16	Jamie Avia purchases the firearm that will kill Border Patrol Agent Brian Terry.
February	Operation Fast and Furious is designated an OCDETF investigation.
March 16	Group VII starts intercepting subjects' phone calls.
April–August	Subjects continue to purchase firearms and traffic them to Mexico. Group VII continues to conduct surveillance but does not interdict any firearms.
May 29, 2010	The CBP arrests Celis-Acosta at the Lukeville, Arizona, border crossing. The lead case agent interviews Celis-Acosta but does not arrest him or ask him to cooperate against the cartel.
August 2	The ATF Title III wiretap warrant ends; no additional subjects or evidence is discovered during the wiretap period.
August	ATF begins to move toward an indictment of the subjects.
December 14	Border Patrol Agent Terry is killed near Rio Rico, Arizona.
December 15	ATF learns that a Fast and Furious firearm killed Terry.
January 25, 2011	The U.S. Attorney's Office of Arizona indicts thirty-four defendants in connection with Operation Fast and Furious.

APPENDIX B. SILK ROAD TIMELINE

January 23, 2011	Ross Ulbricht creates the Silk Road on the dark web.
January 27	An account is created on Shroomery.com under the name Altoid, later discovered to be Ross Ulbricht; the user asks people if they have heard about the Silk Road.
January 28	A message is posted in Bitcointalk, asking if users have heard about the Silk Road.
June 1	Adrian Chen's Gawker article is published online.
June 5, 2011	Senators Charles Schumer and Joe Manchin ask the DOJ and DEA to investigate the Silk Road.
October 11	Altoid, posts on Bitcointalk to request help with a Bitcoin startup.
October 13	HSI Agent Jared Der-Yeghiayan opens Operation Dime Store to investigate drug seizures at the O'Hare Airport Mail Facility.
November	HSI agents in Baltimore take over the seller account of a Silk Road vendor. The vendor becomes a cooperator.
November	The Marco Polo task force is formed in Baltimore.
February 2, 2012	A deconfliction meeting is held between HSI Chicago and the Marco Polo task force.
March 3	Ulbricht creates an account under the username on the Stack Overflow message board under the name Frosty.
March 4	DEA Agent Carl Mark Force begins talking with DPR as "Nob."
January 13, 2013	Marco Polo members arrest a Silk Road employee during a controlled delivery of drugs; the employee agrees to work with law enforcement.
March 16	A question is posted to Stackoverflow about how to program with curl. After the post, the user changes his name to Frosty.
May 26	IRS CI uncovers the first mention of the Silk Road by Altoid posted on Shroomery.com.

June 1	The IRS CI investigator discovers the Altoid post asking for programming help and that it is connected to the email address rossulbricht@gmail.com.
June 12	The FBI discovers the Silk Road server's location in Iceland and asks local authorities to image the device.
July	Der-Yaghiayan begins impersonating Silk Road employee Cirrus.
July 10	CBP discovers nine fake IDs in the mail that were ordered by Ross Ulbricht.
July 13	A deconfliction meeting occurs at the DOJ with members of the Marco Polo task force, HSI Chicago, FBI, and DEA Strike Force from New York.
July 26	Ulbricht is interviewed by DHS agents about the fake IDs.
July 29	The FBI receives an imaged copy of the Silk Road server from the Reykjavik Metropolitan Police.
August	The corrupt undercover DEA agent tries to sell information to DPR about the investigation to protect the agent's identity.
September 10	The IRS CI explains to the AUSA and other investigators why he thinks Ulbricht is DPR.
Late September	Members of the FBI begin to conduct surveillance on Ulbricht in San Francisco to confirm that his computer usage time coincides with DPR's posts on the Silk Road website.
October 2	DPR is arrested in San Francisco by members of the FBI, HSI, and IRS.

APPENDIX C. SEX MONEY MURDER TIMELINE

1992	Peter Rollack forms the Sex Money Murder gang in the Soundview Public Housing Development in the Bronx.
August 16, 1993	Rollack kills Keenyon Jenkins at the Harlem Week Festival over a gambling dispute with David Mullin.
April 8, 1994	Rollack kills Karlton Hines on Boston Road in the Bronx over a show of disrespect and attempts to kill Carlos Mestre.
June 1994	Rollack kills Anthony Dunkley in the Bronx over a dispute.
July 17, 1994	Rollack kills Carols Mestre to prevent his cooperation with the police about the Hines murder.
October 21, 1994	Rollack, David Gonzales, and Savon Codd, are arrested in Rockingham, North Carolina, on charges of drug and firearms possession, and then released.
August 9, 1996	Rollack is arrested at Grant's Tomb for criminal possession of a weapon and for the murder of Hines.
Fall 1996	Rollack and SMM become an official Bloods set.
Fall 1996	Rollack is sentenced to two to six years for weapons possession.
December 16, 1996	Rollack is indicted for narcotics trafficking stemming from his October 1994 North Carolina arrest.
November 27, 1997	David Mullin and Efrin Solar are killed while playing football at the Soundview Housing Complex, under orders from an incarcerated Rollack.
January 2, 1997	Rollack is transferred to North Carolina to await trial.
February 6, 1997	Rollack's trial begins.
February 1998	Rollack and ten other members of SMM are indicted in the Southern District of New York for RICO charges concerning the gang's criminal activities.
March 31, 1998	Rollack is convicted in North Carolina.
January 2000	Rollack is sentenced to life plus 105 years for leading SMM.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Atkinson, Mary, Paul Doherty, and Kay Kinder. "Multi-agency Working: Models, Challenges and Key Factors for Success." *Journal of Early Childhood Research* 3, no. 1 (February 2005): 7–17. https://doi.org/10.1177/1476718X05051344.

Banks, Duren, Joshua Hendricks, Matthew Hickman, and Tracey Kyckelhahn. *National Sources of Law Enforcement Employment Data*. NCJ 249681. Washington, DC: Bureau of Justice Statistics, April 2016. https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5600.

Baskar, Rahul, and Yi Zhang. "Knowledge Sharing in Law Enforcement: A Case Study." *Journal of Information Privacy and Security* 3, no. 3 (July 2007): 45–68. https://doi.org/10.1080/15536548.2007.10855821.

Bilton, Nick. *American Kingpin: The Epic Hunt for the Criminal Mastermind behind the Silk Road*. New York: Portfolio/Penguin, 2018.

Brooks, Conner. *Federal Law Enforcement Officers, 2016 - Statistical Tables*. NCJ 251922. Washington, DC: Bureau of Justice Statistics, October 2019. https://www.bjs.gov/index.cfm?ty=pbdetail&iid=6708.

Brown, Rick. "Understanding Law Enforcement Information Sharing for Criminal Intelligence Purposes." *Trends and Issues in Crime and Criminal Justice*, no. 566 (December 2018): 1.

Busuioc, E. Madalina. "Friend or Foe? Inter-agency Cooperation, Organizational Reputation, and Turf." *Public Administration* 94, no. 1 (March 2016): 40–56. https://doi.org/10.1111/padm.12160.

Carr, Tom, Kent Shaw, and Jack Killorin. "Event Deconfliction Avoids Operational Conflicts, Saves Lives, and Solves Cases." *Police Chief*, February 1, 2017. https://www.policechiefmagazine.org/event-deconfliction-avoids-operational-conflicts/.

Chen, Adrian. "Underground website Lets You Buy Any Drug Imaginable." Wired, June 1, 2011. https://www.wired.com/2011/06/silkroad-2/.

Chermak, Steven, Jeremy Carter, David Carter, Edmund F. McGarrell, and Jack Drew. "Law Enforcement's Information Sharing Infrastructure: A National Assessment," *Police Quarterly* (February 19, 2013): 211–244. https://doi.org/10.1177/1098611113477645.

Coleman, Douglas. *Stopping the Flow of Illicit Drugs in Arizona by Leveraging State, Local and Federal Information Sharing.* Washington, DC: House of Representatives, 2012.

Data.gov. "Law Enforcement Inquiry and Alerts." Accessed May 15, 2020. https://catalog.data.gov/dataset/law-enforcement-inquiry-and-alerts.

Dawes, Sharon S. "Interagency Information Sharing: Expected Benefits, Manageable Risks." *Journal of Policy Analysis & Management* 15, no. 3 (Summer 1996): 377–94. https://doi.org/10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F.

Department of Homeland Security Office of Inspector General. *DHS Involvement in OCDETF Operation Fast and Furious*. OIG-13-49 Revised.(Washington, DC: Department of Homeland Security, 2013.

Department of Homeland Security Office of Inspector General. "DOJ and DHS OIGs Release a Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations." August 1, 2019. https://www.oig.dhs.gov/news/press-releases/2019/08012019/doj-and-dhs-oigs-release-joint-review-law-enforcement-cooperation-southwest-border-between-federal-bureau.

Department of Justice Office of the Inspector General. *Follow-up Review of the Drug Enforcement Administration's El Paso Intelligence Center*. Washington, DC: Department of Justice, 2017. https://oig.justice.gov/reports/2017/e1701.pdf.

Department of Justice Office of Inspector General. *A Review of ATF's Operation Fast and Furious and Related Matters*. Washington, DC: Department of Justice, 2019. https://oig.justice.gov/reports/2012/s1209.pdf.

Dodson, John. *The Unarmed Truth: My Fight to Blow the Whistle and Expose Fast and Furious*. New York: Threshold Editions, 2013.

Duncan, Ian. "Fall of Online Drug Bazaar Silk Road Began with Tip to Md. Agent," *Baltimore Sun*, November 18, 2013. https://www.baltimoresun.com/maryland/baltimore-city/bs-xpm-2013-11-18-bs-md-ci-inside-silk-road-20131118-story.html.

Federal Bureau of Investigation. "Identity Theft." Accessed July 25, 2020. https://www.fbi.gov/investigate/white-collar-crime/identity-theft.

Federal Bureau of Investigation. "National Crime Information Center (NCIC)." Accessed August 6, 2020. https://www.fbi.gov/services/cjis/ncic.

Ferranti, Seth. *Street Legends*, vol. 1. Gorilla Convict Publications, 2010.

Finklea, Kristin. *High Intensity Drug Trafficking Program (HIDTA) Program*. R45188. Washington, DC: Congressional Research Service, 2018. https://crsreports.congress.gov/product/pdf/R/R45188.

Frazier, Russell M. "A Cannon for Cooperation: A Review of the Interagency Cooperation Literature." *Journal of Public Administration and Governance* 4, no. 1 (2014). https://doi.org/10.5296/jpag.v4i1.4870.

Goldstein, Matthew. "Silk Road Case Began with Hunt for a John Doe." *New York Times*, March 21, 2014. https://dealbook.nytimes.com/2014/03/21/silk-road-case-began-with-hunt-for-a-john-doe/.

Green, Jonathan. *Sex Money Murder: A Story of Crack, Blood, and Betrayal*. New York: W. W. Norton & Company, 2019.

Hendriks, Paul. "Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing." *Knowledge and Process Management* 6, no. 2 (June 1999): 91–100.

House Committee on Oversight and Government Reform. *The Fast and Furious: The Anatomy of a Failed Operation Part I of III*. Washington, DC: U.S. Congress, 2012. https://azmemory.azlibrary.gov/digital/collection/feddocs/id/2276/.

Jenpaa, Sirkka L., and D. Sandy Staples. "Exploring Perceptions of Organizational Ownership of Information and Expertise." *Journal of Management Information Systems* 18, no. 1 (May 31, 2001): 151–83. https://doi.org/10.1080/07421222.2001.11045673.

Joyal, Renee Graphia. "How Far Have We Come? Information Sharing, Interagency Collaboration, and Trust within the Law Enforcement Community." *Criminal Justice Studies* 25, no. 4 (December 2012): 357–70. https://doi.org/10.1080/1478601X.2012.728789.

Kaiser, Frederick M. *Interagency Collaborative Arrangements and Activities: Types, Rationales, Considerations*. CRS Report No. R41803. Washington, DC: Congressional Research Service, 2011. https://www.hsdl.org/?view&did=5216.

Lacson, Wesley, and Beata Jones. "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road." *International Journal of Cyber Criminology* 10, no. 1 (January 2016): 40–61. https://doi.org/10.5281/zenodo.58521.

Lambert, David E. "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model:" *Criminal Justice Policy Review*, July 18, 2018. https://doi.org/10.1177/0887403418786555.

Larence, Eileen. *Combating Child Pornography: Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective*. GAO-11-334. Washington, DC: Government Accountability Office, 2011. https://www.gao.gov/products/GAO-11-334.

Larence, Eileen. *Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*. GAO-13-471. Washington, DC: Government Accountability Office, 2013. https://www.gao.gov/products/GAO-13-471.

Maurer, David. *Office of National Drug Control Policy: Lack of Progress on Achieving National Strategy Goals*. GAO-16-257T. Washington, DC: Government Accountability Office, December 2, 2015. https://www.gao.gov/products/GAO-16-257T.

Mayoraks, Alejandro. *Department Policy Regarding Investigative Data and Event Deconfliction*. Policy Directive 045–04. Washington, DC: Department of Homeland Security, October 18, 2016. https://www.dhs.gov/sites/default/files/publications/mgmt/law-enforcement/mgmt-dir_045-04-dept-policy-regarding-investigative-data-event-deconfliction.pdf.

Mihm, J. Christopher. *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*. GAO-12-1022. Washington, DC: Government Accountability Office, 2012. https://www.gao.gov/products/GAO-12-1022.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin, accessed March 1, 2020. https://bitcoin.org/bitcoin.pdf.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W. W. Norton & Company, 2004.

National Criminal Intelligence Resource Center. "Officer Safety Event Deconfliction: Frequently Asked Questions." April 2016. https://www.ncirc.gov/Deconfliction/Documents/Event_Deconfliction_FAQs.pdf.

NBC New York. "Schumer Pushes to Shut Down Online Drug Marketplace." May 31, 2016. https://www.nbcnewyork.com/news/local/schumer-calls-on-feds-to-shut-down-online-drug-marketplace/1920235/.

The New York Times. "F.B.I. Computer System Is Late and Over Budget, Report Says." October 20, 2010. https://www.nytimes.com/2010/10/21/us/21brfs-FBICOMPUTERS_BRF.html.

Office of Justice Programs. "Intelligence." Accessed May 22, 2020. https://it.ojp.gov/global/working-groups/cicc.

Ormsby, Eileen. *Silk Road*. Sydney: Pan Macmillan Australia, 2014.

The Police Foundation. "Best Practices in Event Deconfliction." CALEA, October 2016. https://www.calea.org/sites/default/files/2019-02/EventDeconfliction_PoliceFoundation.pdf.

Popper, Nathaniel. "The Tax Sleuth Who Took Down a Drug Lord." *New York Times*, December 25, 2015. https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html.

Riege, Andreas. "Three-Dozen Knowledge-Sharing Barriers Managers Must Consider." *Journal of Knowledge Management* 9, no. 3 (2005): 18–35. https://doi.org/10.1108/13673270510602746.

Regional Information Sharing Systems. "RISS Overview." Accessed April 15, 2020. https://www.riss.net/about-us/.

Ruddy, Tom. "Taking Knowledge from Heads and Putting It into Hands." *Knowledge & Process Management* 7, no. 1 (January 2000): 37–40. https://doi.org/10.1002/(SICI)1099-1441(200001/03)7:1<37::AID-KPM81>3.0.CO;2-X.

Rosen, Liana. *International Drug Control Policy: Background and U.S. Responses*. Washington, DC: Congressional Research Service, March 16, 2015. https://fas.org/sgp/crs/row/RL34543.pdf.

Sterbenz, Christina. "New York City Used to Be a Terrifying Place." Business Insider, July 12, 2013. https://www.businessinsider.com/new-york-city-used-to-be-a-terrifying-place-photos-2013-7.

Thorn. "The Intersection of Technology and Child Sexual Abuse. Accessed July 25, 2020. https://www.thorn.org/child-sexual-exploitation-and-technology/.

Tsui, Eric. "The Role of IT in KM: Where Are We Now and Where Are We Heading?" *Journal of Knowledge Management* 9, no. 1 (2005): 3–6.

U.S. Department of Justice Office of Inspector General. *A Review of ATF's Operation Fast and Furious and Related Matters*. Washington, DC: Department of Justice, 2012. https://oig.justice.gov/reports/2012/s1209.pdf.

Weiss, Janet A. "Pathways to Cooperation among Public Agencies." *Journal of Policy Analysis and Management* 7, no. 1 (1987): 94–117. https://doi.org/10.2307/3323353.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California