



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**CULTIVATING DECISION ADVANTAGE:
HOW CBP CAN INTEGRATE INTELLIGENCE
TO IMPROVE BORDER SECURITY**

by

John W. Siffermann

September 2023

Thesis Advisor:
Second Reader:

Erik J. Dahl
Rodrigo Nieto-Gomez

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE CULTIVATING DECISION ADVANTAGE: HOW CBP CAN INTEGRATE INTELLIGENCE TO IMPROVE BORDER SECURITY			5. FUNDING NUMBERS	
6. AUTHOR(S) John W. Siffermann				
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) Customs and Border Protection (CBP) seeks to integrate intelligence to use the information it collects more strategically. CBP's Office of Field Operations (OFO) can anticipate emerging threats at ports of entry but is limited in its ability to capitalize on existing data to thwart criminal networks. This thesis explores how OFO can effectively integrate intelligence to improve border security by collecting, analyzing, and disseminating information in a more strategic manner. Using a case study approach to adopt best practices, and acknowledging disparate roles and responsibilities, this study assesses the domestic intelligence services of the United Kingdom, Australia, and Germany to understand how each coordinates intelligence activity. As a result, this thesis identifies best practices for OFO to consider; specifically, this thesis recommends two possible frameworks for OFO to shape port intelligence units at ports of entry. As CBP seeks to integrate intelligence, OFO can contribute to its strategic goal by standardizing port intelligence units within a desk officer or task-sharing system; each system integrates intelligence, cultivates decision advantage, and fosters analytically driven collection. This thesis concludes that standardizing port intelligence effectively integrates intelligence and positions CBP to make meaningful contributions to the intelligence enterprise and accomplish mission goals.				
14. SUBJECT TERMS U.S. Customs and Border Protection, Office of Field Operations, CBP, OFO, border search, electronic devices, intelligence, information sharing, desk officer, task sharing, MI5, ASIO, BfV			15. NUMBER OF PAGES 95	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**CULTIVATING DECISION ADVANTAGE:
HOW CBP CAN INTEGRATE INTELLIGENCE
TO IMPROVE BORDER SECURITY**

John W. Siffermann
Supervisory CBP Officer, Office of Field Operations,
U.S. Customs and Border Protection, Department of Homeland Security
BS, Western Illinois University, 2011

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
September 2023**

Approved by: Erik J. Dahl
Advisor

Rodrigo Nieto-Gomez
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Customs and Border Protection (CBP) seeks to integrate intelligence to use the information it collects more strategically. CBP's Office of Field Operations (OFO) can anticipate emerging threats at ports of entry but is limited in its ability to capitalize on existing data to thwart criminal networks. This thesis explores how OFO can effectively integrate intelligence to improve border security by collecting, analyzing, and disseminating information in a more strategic manner. Using a case study approach to adopt best practices, and acknowledging disparate roles and responsibilities, this study assesses the domestic intelligence services of the United Kingdom, Australia, and Germany to understand how each coordinates intelligence activity. As a result, this thesis identifies best practices for OFO to consider; specifically, this thesis recommends two possible frameworks for OFO to shape port intelligence units at ports of entry. As CBP seeks to integrate intelligence, OFO can contribute to its strategic goal by standardizing port intelligence units within a desk officer or task-sharing system; each system integrates intelligence, cultivates decision advantage, and fosters analytically driven collection. This thesis concludes that standardizing port intelligence effectively integrates intelligence and positions CBP to make meaningful contributions to the intelligence enterprise and accomplish mission goals.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH QUESTION	3
C.	LITERATURE REVIEW	3
1.	Intelligence Defined	4
2.	Intelligence Partnerships.....	5
3.	American Intelligence.....	7
4.	Border Intelligence.....	9
D.	RESEARCH DESIGN	11
E.	THESIS OUTLINE.....	12
II.	CBP OFFICE OF FIELD OPERATIONS	13
A.	BORDER SEARCH AUTHORITY	13
B.	INTELLIGENCE CYCLE.....	15
1.	Collection	16
2.	Analysis	20
3.	Dissemination	23
C.	LIMITATIONS.....	23
1.	Disparate Responsibilities and Competing Priorities.....	24
2.	Insufficient Intelligence Structures	25
3.	Public Awareness	27
D.	CONCLUSION	28
III.	COMPARATIVE ANALYSIS OF MI5, ASIO, AND BFV	31
A.	UNITED KINGDOM SECURITY SERVICE	31
1.	History.....	32
2.	Structure	33
3.	Priorities.....	35
4.	Intelligence Activity	35
B.	AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION.....	37
1.	History.....	38
2.	Structure	39
3.	Priorities.....	40
4.	Intelligence Activity	42

C.	FEDERAL OFFICE FOR THE PROTECTION OF THE CONSTITUTION	44
1.	History.....	44
2.	Structure	45
3.	Priorities.....	46
4.	Intelligence Activity	49
D.	CONCLUSION	50
1.	Threat Prioritization.....	50
2.	Structural Approach.....	51
3.	Transparency.....	51
IV.	FINAL ANALYSIS	53
A.	KEY FINDINGS	53
1.	OFO Capabilities and Limitations	53
2.	MI5, ASIO, and the BfV	54
B.	RECOMMENDATIONS.....	55
1.	Desk Officer System.....	55
2.	Task-Sharing System	58
C.	FINAL THOUGHTS AND FUTURE RESEARCH.....	61
	LIST OF REFERENCES.....	63
	INITIAL DISTRIBUTION LIST	73

LIST OF FIGURES

Figure 1.	CBP Intelligence Cycle.....	16
Figure 2.	Desk Officer System	57
Figure 3.	Task-Sharing System	59

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Office of Field Operations and United States Border Patrol	14
----------	--	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACAS	Air Cargo Advanced Screening
AFI	Analytical Framework for Intelligence
APIS	Advance Passenger Information System
ASIO Act	Australian Security Intelligence Organisation Act 1979
ASIO	Australian Security Intelligence Organisation
ASPI	Australian Strategic Policy Institute
A-TCET	Anti-Terrorism Contraband Enforcement Team
ATS	Automated Targeting System
ATU	Advanced Targeting Unit
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
CBP	Customs and Border Protection
CONTEST	Counterterrorism Strategy
DHS	Department of Homeland Security
DO	Desk Officer
FBI	Federal Bureau of Investigation
FVEY	Five Eyes
GCHQ	Government Communications Headquarters
HUMINT	human intelligence
I&A	Intelligence and Analysis
IC	Intelligence Community
IGIS	Inspector-General of Intelligence and Security
IIR	Independent Intelligence Review

MI5	Security Service
MOU	memorandum of understanding
NADIS WN	Intelligence Information System and Knowledge Network
OFO	Office of Field Operations
ONI	Office of National Intelligence
PAU	Passenger Analytical Unit
PCS	Passport Control Secondary
PERT	Passenger Enforcement Rover Team
PIA	Privacy Impact Assessments
PIR	Priority Intelligence Requirement
PLA	People's Liberation Army
PRC	People's Republic of China
RIPA	Regulation of Investigatory Powers Act 2000
SIS	Secret Intelligence Service
SSA	Security Service Act 1989
TRP	Threat Review and Prioritization
TTRT	Tactical Terrorism Response Team
UKIC	United Kingdom Intelligence Community
UPAX	Unified Passenger
USBP	United States Border Patrol

EXECUTIVE SUMMARY

Customs and Border Protection (CBP) seeks to integrate intelligence to capitalize on the information it collects and cultivate decision advantage within its frontline ranks. CBP places significant emphasis on strengthening its ability to recognize and confront threats impacting the United States by extending intelligence capabilities to the field.¹ The Office of Field Operations (OFO)—a CBP component—is capable of integrating intelligence by leveraging its authorities and embracing its access to valuable information. Despite CBP’s potential to collect, analyze, and disseminate tactical and strategic intelligence, several factors impede OFO’s ability to integrate intelligence to improve border security. Disparate responsibilities, competing priorities, insufficient intelligence structures, and a lack of public awareness impact OFO’s evolution toward intelligence. Exploring those perceived problems assists OFO as it navigates mission priorities with increased and integrated intelligence roles.

This thesis explores how OFO can effectively integrate intelligence to improve border security by collecting, analyzing, and disseminating information in a more strategic manner. Considering CBP’s desire to expand intelligence capabilities to improve border security, a case study approach helps understand contemporary OFO practices and recognize deficiencies in its ability to coordinate intelligence. Comparative research identifies how intelligence agencies abroad coordinate intelligence; specifically, the domestic intelligence apparatuses of the United Kingdom (MI5), Australia (ASIO), and Germany (BfV) provide a potential path forward for OFO. Although the role of OFO expands beyond intelligence responsibilities, understanding the functionality of various established intelligence agencies provides context to adopt best practices.

OFO can contribute to CBP’s strategic intelligence goals and empower personnel in various roles. However—due to the size of OFO and the scope of its mission—disparate responsibilities and competing priorities impact its ability to translate the information it

¹ Customs and Border Protection, *CBP Strategy 2021–2026* (Washington, DC: Customs and Border Protection, 2020), 25, <https://www.cbp.gov/sites/default/files/assets/documents/2020-Dec/CBP-Strategy-2021-2026.pdf>.

collects into actionable intelligence. Similarly, insufficient intelligence structures and a lack of public awareness about CBP's mission impede OFO's ability to transcend the limits of its capabilities. Therefore, despite the authorities and tools in place to play to the edge, OFO must improve its ability to coordinate intelligence and cultivate decision advantage.

Researching established intelligence agencies—like MI5, ASIO, and the BfV—proves beneficial for OFO to integrate intelligence into operations. By studying each agency, OFO can learn and adapt best practices to coordinate intelligence effectively. The history, structure, and priorities of MI5, ASIO, and the BfV provide insight into the intricacies of the intelligence profession. In particular, intelligence frameworks help the surveyed agencies structure intelligence and pursue the greatest threats to their homelands. Similarly, each intelligence agency values transparency differently; however, research identifies that increased transparency has a positive impact on garnering strategic legislative support. Overall, a case study approach of established intelligence agencies reveals best practices that emerged from threat prioritization, structural approach, and transparency. By adapting best practices and leveraging its tools and authorities, OFO can emerge as an agency capable of cultivating decision advantage and contributing to tactical and strategic intelligence objectives.

Upon evaluating each intelligence agency, and considering CBP's strategic goal to integrate intelligence, OFO should establish intelligence units at designated ports of entry. However, merely prioritizing port intelligence does not sufficiently integrate intelligence. By adopting structured intelligence frameworks, OFO can efficiently coordinate intelligence to improve agency outcomes and contribute to the broader intelligence enterprise. One takeaway from the case studies is MI5's intelligence structure, which features a desk officer at the center of the intelligence cycle.² OFO can adopt a modified structure in which CBP officers fulfill the entire intelligence cycle, including collection efforts. In a desk officer system, a group of CBP officers comprise a port intelligence unit;

² Paul Jonathan Smith, "Counterterrorism in the United Kingdom," in *Module III: The UK's Counterterrorism Structure and the Pursuit of Terrorists* (Monterey, CA: Center for Homeland Defense & Security, August 3, 2023), https://www.chds.us/coursefiles/comp/lectures/comp_CT_in_the_UK_mod03/script.pdf.

in that unit, officers are responsible for collecting, exploiting, analyzing, and disseminating information and intelligence. The desk officer system bridges gaps between collection and analysis; it further streamlines the ability to disseminate actionable intelligence to consumers quickly. By structuring port intelligence in a desk officer system, enforcement units focus on interdiction, primarily driven by port intelligence.

The other framework for OFO to consider is an adaptation of the BfV intelligence structure known as federal task-sharing. In Germany, the BfV oversees the activity of each state's domestic intelligence service; OFO can modify the task-sharing system to satisfy tactical and strategic intelligence needs at ports of entry.³ In the task-sharing system, port intelligence units feature a central intelligence body with intelligence officers embedded in various specialized work units. Like the desk officer system, CBP officers comprise the task-sharing system; however, port intelligence officers are not responsible for collection efforts. The central body coordinates strategic intelligence while the embedded port intelligence officers focus on tactical intelligence to improve team outcomes. The task-sharing system emphasizes analytically driven collection—which is considered the ideal state for collectors—by streamlining the dissemination of relevant information.⁴

The recommended frameworks for OFO to structure port intelligence serve to integrate intelligence effectively. Such integration improves OFO's ability to use the information it collects more strategically. Establishing and structuring intelligence units at CBP ports of entry will help OFO evolve as an agency capable of contributing to the intelligence enterprise; furthermore, embracing intelligence capabilities will strengthen OFO's ability to cultivate the necessary decision advantage to improve border security.

³ “The German Domestic Intelligence Services,” Bundesamt für Verfassungsschutz, accessed November 2, 2021, https://www.verfassungsschutz.de/EN/home/home_node.html.

⁴ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 9th ed. (Thousand Oaks, CA: CQ Press, 2022), 81.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It is a privilege to conclude this chapter of my life. The Naval Postgraduate School Center for Homeland Defense and Security provided me with avenues to critically assess a myriad of homeland security issues. I am sincerely grateful for the guidance from Dr. Erik J. Dahl as my advisor; your encouragement and honest feedback motivated me to refine the scope of my research and produce meaningful analyses. I am also grateful for the support that Dr. Rodrigo Nieto-Gomez provided as my second reader. Furthermore, the CHDS faculty and staff were crucial to my analytical development; my gratitude extends to the instructors, writing coaches, library staff, operations coordinators, technology specialists, thesis processors, and thesis whisperers.

The culmination of this educational journey was preparing a thesis to improve the operational readiness of Customs and Border Protection. CBP continually affords me unique opportunities to enhance border security and protect the United States. I am grateful for the time, support, and trust that CBP bestowed upon me over the last 18 months. I am particularly thankful for the patience and guidance provided by my chain of command, colleagues, and mentors throughout this process.

I cannot imagine the NPS CHDS experience without Cohort 2201/02. We shared similar highs and lows, joy and agony, comfort and stress. While we found solace in each other's experiences, it was the love and support of our families that truly sustained us.

Pursuing this degree would not have been possible without the unwavering love and support of my wife, Ashley. We started a family during this academic journey, and I could not have completed it without her leadership. Thank you for being my main source of encouragement, determination, and resilience. You were equally dedicated to this journey and centered me when I conjured doubt and uncertainty.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Customs and Border Protection (CBP) seeks to integrate intelligence to capitalize on the information it collects and cultivate decision advantage within its frontline ranks. In its recently published strategy, CBP places significant emphasis on strengthening its ability to recognize and confront threats impacting the United States by extending intelligence capabilities to the field.¹ Such emphasis is outlined in a five-year strategy “to transform CBP into threat-based, intelligence and data-driven, and operationally-focused agency that enhances national security through innovation, intelligence, collaboration, and trust.”² A CBP component capable of embracing intelligence functions might be the Office of Field Operations (OFO). Although the search authority of OFO remains strictly at ports of entry, 26,000 officers process more than a million international travelers each day and the nexus to potentially actionable intelligence is vast.³ At international airports, OFO can anticipate who is traveling into and out of the United States, allowing time to conduct security vetting and analysis. The capacity to analyze information is augmented by border search authority, which officers can leverage for significant collection opportunities. Despite the potential to transcend the border agency’s limits in collecting, analyzing, and disseminating tactical and strategic intelligence, several factors impede OFO’s ability to integrate intelligence to improve border security.

Even though OFO has placement and access to collect meaningful information, coordinating intelligence activity is not a core function. Although OFO has grown over the last twenty years, work assignments still revolve around the facilitation of travel and

¹ Customs and Border Protection, *CBP Strategy 2021–2026* (Washington, DC: Customs and Border Protection, 2020), 25, <https://www.cbp.gov/sites/default/files/assets/documents/2020-Dec/CBP-Strategy-2021-2026.pdf>.

² Customs and Border Protection, 25.

³ Staffing is based on FY22 and passenger processing is based on FY19; “On a Typical Day in Fiscal Year 2022, CBP...,” July 21, 2023, <https://www.cbp.gov/newsroom/stats/typical-day-fy2022>; “On a Typical Day in Fiscal Year 2019, CBP...,” May 11, 2022, <https://www.cbp.gov/newsroom/stats/typical-day-fy2019>.

interdiction.⁴ The occupational requirements of a CBP officer (Series 1895) include interviewing and examining documents, determining admissibility, eliciting information, searching for contraband, examining cargo, and apprehending violators of applicable laws.⁵ Missing from the Series 1895 job description is coordinating intelligence; yet, CBP hopes to expand intelligence capabilities to increase the field's understanding of evolving threats.⁶ According to an OIG report, OFO estimates that 85 percent of its funding for drug enforcement is dedicated to interdiction; 15 percent is dedicated to intelligence.⁷ Therefore, OFO will struggle to integrate intelligence until it is a core function of CBP officers.

The lack of enhanced intelligence expertise among CBP officers hinders effective intelligence collection, analysis, and dissemination. Foundational to advanced intelligence collection are intellectual curiosity, critical thinking, and decision-making.⁸ Furthermore, the sensitive and unique nature of intelligence can take as long as a decade to gain the necessary skills to conduct effective analysis.⁹ Although CBP employs robust analytical systems like the Analytical Framework for Intelligence (AFI), systems are of little use if the information is not properly collected, analyzed, and disseminated.¹⁰ Underestimating the complexity of intelligence training ultimately suspends OFO from embracing its capabilities and integrating intelligence.

⁴ “Careers: Office of Field Operations,” Customs and Border Protection, accessed July 13, 2023, <https://www.cbp.gov/careers/ofo>.

⁵ “Customs and Border Protection Series 1895,” Office of Personnel Management, accessed August 3, 2023, <https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/1800/customs-and-border-protection-series-1895/>.

⁶ Customs and Border Protection, *CBP Strategy 2021–2026*, 25.

⁷ Office of Inspector General, *Review of U.S. Customs and Border Protection's Fiscal Year 2022 Detailed Accounting Report for Drug Control Funds*, OIG-23-10 (Washington, DC: Department of Homeland Security, 2023), 9.

⁸ Dan Harris, “The Consequences of Eroding Human Intelligence Collection,” The Cipher Brief, Summer 2016, https://www.thecipherbrief.com/column_article/the-consequences-of-eroding-human-intelligence-collection.

⁹ Charles Nemfakos et al., *Workforce Planning in the Intelligence Community: A Retrospective* (Santa Monica, CA: RAND Corporation, 2013), 63, https://www.rand.org/pubs/research_reports/RR114.html.

¹⁰ Mario Medina, *Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI)*, DHS/CBP/PIA-010(a) (Washington, DC: Department of Homeland Security, 2016), <https://www.dhs.gov/sites/default/files/2022-10/privacy-pia-cbp010%28a%29-afi-october2022.pdf>.

It is unclear how the extension of intelligence capabilities will be implemented by and structured by OFO. Although CBP states that the development of a “world-class CBP Intelligence Training Academy” is essential to meet rapidly expanding intelligence needs, missing from its strategy is how CBP intelligence activity will be modeled for individual components with disparate responsibilities and competing priorities.¹¹ A likely candidate from which OFO can adopt frameworks is the United States Intelligence Community (IC); however, it is essential not to overlook the importance of acquiring a comprehensive understanding of the operations of various intelligence agencies worldwide.

CBP’s pursuit of an operationally focused and intelligence-driven workforce is important; however, several factors impede OFO’s ability to evolve.¹² The main objective of this thesis is to resolve the stated problems by examining OFO’s intelligence capabilities at international airports and exploring how those capabilities can be embraced to improve border security. Such exploration will assist OFO as it prepares to navigate mission priorities with increased and integrated intelligence roles. The desired outcome is to establish OFO as an agency capable of making valuable contributions to the broader intelligence enterprise while maintaining the integrity of existing policies and procedures.

B. RESEARCH QUESTION

How can OFO effectively integrate intelligence to improve border security by collecting, analyzing, and disseminating information in a more strategic manner?

C. LITERATURE REVIEW

The following literature examines intelligence definitions, intelligence and information-sharing partnerships, American intelligence, and border intelligence. The review examines key components of the main research question to navigate areas for improvement. These works also provide the background needed for my research, which addresses how OFO can embrace capabilities to integrate intelligence into frontline operations.

¹¹ Customs and Border Protection, *CBP Strategy 2021–2026*, 25.

¹² Customs and Border Protection.

1. Intelligence Defined

It is important to preface an examination of intelligence activity by defining intelligence and explaining its purpose. Mark Lowenthal defines intelligence as a process of requesting, collecting, analyzing, and providing national security-related information to policymakers.¹³ Lowenthal simplifies intelligence as 1) asking a question and 2) collecting information to answer that question.¹⁴ Godfrey and McGlynn broadly define intelligence as “the ability to obtain and apply knowledge and skills.”¹⁵ Their definition is an echo of Robert Steele, who describes intelligence as a process that produces tailored actionable knowledge.¹⁶ The authors’ definitions relate intelligence to a process, as opposed to a finished product.

The intelligence process involves several components that contribute to a finished product. According to Lowenthal, seven components comprise the intelligence cycle: requirements, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback.¹⁷ The collection component is key to effective intelligence; however, Lowenthal warns us that collection efforts complicate the task of finding meaningful intelligence because more haystacks do not equate to more needles.¹⁸ Furthermore, according to Erik Dahl, effective intelligence hinges on two assumptions; that intelligence provides an accurate assessment of a situation, and that the assessment is adequately conveyed to decision-makers with a high level of receptivity.¹⁹ To the former assumption, information improperly exploited or analyzed is identical to information not

¹³ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 9th ed. (Thousand Oaks, CA: CQ Press, 2022), 9–10.

¹⁴ Lowenthal, 48.

¹⁵ Patrick McGlynn and Godfrey Garner, *Intelligence Analysis Fundamentals* (Boca Raton, FL: CRC Press, 2018), 2, <https://doi.org/10.4324/9781351249355>.

¹⁶ Robert D. Steele, *The New Craft of Intelligence, Personal, Public, & Political: Citizen’s Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption* (Oakton, VA: OSS International Press, 2002), 11.

¹⁷ Lowenthal, *Intelligence*, 73–74.

¹⁸ Lowenthal, 79.

¹⁹ Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 20.

collected.²⁰ To the latter assumption, intelligence is of little use until it is received by its consumers.²¹ Therefore, as Steele suggests, dissemination can be viewed as strategic communication; it is the cart carrying the message.²² Therefore, intelligence must be properly collected, analyzed, and disseminated in a manner that cultivates decision-making.

The authors effectively define intelligence, explain its purpose, and provide insight into the elusiveness of collecting, analyzing, and disseminating meaningful intelligence. Missing from the authors' examinations is how intelligence ought to be conducted. Although an answer to that may vary across intelligence professions, Michael Hayden offers his perspective. According to Hayden, intelligence must be played to the edge; by playing to the edge, operators use all the tools and authorities available, similar to professional athletes using the entire field of play.²³ Playing to the edge is an illuminating concept; agencies must embrace their intelligence capabilities to produce actionable knowledge and provide decision advantage. Falling short of playing to the edge detracts from collecting, analyzing, and disseminating meaningful intelligence.

2. Intelligence Partnerships

Intelligence starts from the bottom up. Bruce Hoffman states, “prevention comes first from the cop on the beat.”²⁴ A similar argument is made by Stefanie Fisher; she recognizes an increasing need for region-specific intelligence and argues that local intelligence units are an integral part of the broader counterterrorism fight.²⁵ In other

²⁰ Lowenthal, *Intelligence*, 80.

²¹ Erik J. Dahl, “Why Won’t They Listen? Understanding Policy Maker Receptivity toward Intelligence” (paper presented at the International Studies Association Annual Conference, Montreal, March 2011), 1, <https://hdl.handle.net/10945/58528>; Lowenthal, *Intelligence*, 20.

²² Robert David Steele, *Information Operations: All Information, All Languages, All the Time*, 2nd ed. (Concord, CA: OSS International Press, 2006), 32.

²³ Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016), xiv.

²⁴ Bruce Hoffman, *Inside Terrorism*, 3rd ed. (New York: Columbia University Press, 2017), 179.

²⁵ Stefanie Fisher, “The Fight against Terrorism—the Need for Local Police Units in the United States’ Intelligence Community,” *Journal of Military and Strategic Studies* 17, no. 1 (2018): 189–90, <https://jmss.org/article/view/58212>.

words, local police units have much to offer intelligence consumers; therefore, effective intelligence requires information sharing. Carter et al. argue that limited participation among information-sharing partners reduces intelligence capabilities.²⁶ Similarly, Pickering and Fox insist that data and information sharing, along with collaborative efforts, are essential to reduce linkage blindness—a concept that authors explain as the inability to communicate or share information that could otherwise connect dots.²⁷ In other words, the production of intelligence is useless without effective distribution and engagement at all levels of government.

Although the benefits of sharing information are well-studied, effective sharing can be evasive. David Lambert explains how complex information sharing is because it involves multiple stakeholders, competing priorities, lack of experience, and a tendency to “silo” intelligence.²⁸ Through the lens of John Kotter’s *Leading Change* principles, Lambert argues that gaining buy-in from partnering agencies requires establishing a sense of urgency across organizations; doing so requires effective leadership to drive permanent change.²⁹ He also sees short-term “wins” as catalysts capable of causing strategic change since agencies tend to mimic the success of others, so long as those wins demonstrate a direct improvement to agency performance.³⁰ Therefore, information-sharing is more than just sharing information; it requires full participation, organizational support, and that priorities align with or complement each other.

Scholars comprehensively identify best practices to improve intelligence practices and enhance information-sharing. Such practices include adopting analytic standards and

²⁶ Jeremy G. Carter et al., “Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment While Safeguarding Privacy,” *Journal of Police and Criminal Psychology* 32, no. 1 (March 2017): 23, <https://doi.org/10.1007/s11896-016-9199-4>.

²⁷ Jordan C. Pickering and Andrew M. Fox, “Enabling Collaboration and Communication across Law Enforcement Jurisdictions: Data Sharing in a Multiagency Partnership,” *Criminal Justice Policy Review* 33, no. 7 (August 2022), 735, 750, <https://doi.org/10.1177/08874034211066756>.

²⁸ David E. Lambert, “Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter’s Leading Change Model,” *Criminal Justice Policy Review* 30, no. 8 (October 2019), <https://doi.org/10.1177/0887403418786555>.

²⁹ Lambert, 1263-64.

³⁰ Lambert, 1268.

encouraging full participation among information-sharing partners. Improving intelligence and information-sharing helps mitigate linkage blindness and prevent agencies from failing to connect the dots.

3. American Intelligence

Christian Beckner argues that the Office of Intelligence and Analysis (I&A) has struggled to fulfill its intended purpose as the nexus of intelligence and is not considered a prominent member of the IC.³¹ I&A is the intelligence arm of the Department of Homeland Security (DHS) and has been criticized for its inability to influence and integrate intelligence-related activities across DHS components.³² Additionally, it experiences challenges communicating its function to Congress and the public, which results in doubt and uncertainty about its role in intelligence.³³ Beckner suggests reducing the size and responsibilities of I&A; he argues it should be modeled after the Bureau of Intelligence and Research at the Department of State and the Office of Intelligence and Analysis at the Department of Treasury, both of which are considerably smaller than I&A.³⁴ In such exploration, the author examines which members of the IC would serve as appropriate models for I&A.

A number of experts argue that the Intelligence Community's organizational structure, analytical deficiencies, and fear of failure hinder its effectiveness in producing intelligence and anticipating threats. Habeck and Stimson assess that disparate organizational structures within the Intelligence Community support individual missions, not cooperation and collaboration.³⁵ The authors criticize the Intelligence Community for its lack of analytical diversity cultivated by groupthink, confirmation biases, and cultural

³¹ Christian Beckner, "Reassessing Homeland Security Intelligence: A Review of the DHS Office of Intelligence and Analysis," Center for a New American Security, May 25, 2021, <https://www.cnas.org/publications/reports/reassessing-homeland-security-intelligence>.

³² Beckner.

³³ Beckner.

³⁴ Beckner.

³⁵ Mary Habeck and Charles D. Stimson, *Reforming Intelligence: A Proposal for Reorganizing the Intelligence Community and Improving Analysis* (Washington, DC: Heritage Foundation, 2016), <https://www.hsdl.org/c/abstract/?docid=795261>.

norms.³⁶ Also problematic is a failure to encourage expertise, which promotes generalization rather than specialization.³⁷ The authors are also critical of the Central Intelligence Agency; in particular, its historical fear of failure results in an inability to learn from mistakes.³⁸ Overall, the authors argue for a more adaptable Intelligence Community, capable of evolving with emerging threats.

The Federal Bureau of Investigation (FBI) establishes its most severe and impactful threats through an annual process known as Threat Review and Prioritization (TRP); however, the TRP process is reactive and may be an insufficient process to anticipate emerging threats. Tromblay argues that the TRP compounds the FBI's oldest problems, mainly grounded in a state of reactivity.³⁹ According to Tromblay, the FBI is affected by prematurely closed cases that eliminate collection opportunities and bureaucratic expectations that change from one Presidential administration to the next.⁴⁰ Tromblay argues that the focus of TRP is not informed by proactively disrupting emerging threats, but rather focuses on reacting to threats that have already fully manifested within the FBI realm.⁴¹ Therefore, the FBI is challenged to identify strategies to implement proactive intelligence initiatives to predict and anticipate emerging threats.

Treating intelligence as a discipline may help improve agency outcomes. To improve the performance of agencies tasked with intelligence functions, scholars find value in advancing analysis toward a professional discipline with analytical standards, principles, and guidelines.⁴² According to Reinhold, Russo, and Eisenfeld, such transformation may

³⁶ Habeck and Stimson.

³⁷ Habeck and Stimson.

³⁸ Habeck and Stimson.

³⁹ Darren E. Tromblay, "The Threat Review and Prioritization Trap: How the FBI's New Threat Review and Prioritization Process Compounds the Bureau's Oldest Problems," *Intelligence and National Security* 31, no. 5 (2016): 762, <https://doi.org/10.1080/02684527.2015.1105496>.

⁴⁰ Tromblay.

⁴¹ Tromblay.

⁴² Derek Reinhold, Charles Russo, and Beth Eisenfeld, "Analytical Standards in the Intelligence Community: Are Standards Professionalized Enough?," *Journal of Strategic Security* 14, no. 1 (2021): 106, <https://doi.org/10.5038/1944-0472.14.1.1923>.

align intelligence analysis more closely with professions like medicine and law.⁴³ The authors argue that standards and oversight, which are needed to advance intelligence as a maturing profession, would facilitate better analysis.⁴⁴ Reinhold et al., therefore, see analytical standardization as a necessary advancement for intelligence analysis. Rather than focusing on individual components of the intelligence process, the authors argue that improving outcomes requires a fundamental change in intelligence analysis. Agencies cannot expect to produce effective intelligence without analytic standards.

Ample research identifies deficiencies and challenges across the Intelligence Community. Although the Intelligence Community has a wide range of experience producing tactical and strategic intelligence, some challenges include overwhelming responsibilities, organizational structures that impede robust analysis, and bureaucratic conflicts that limit proactive intelligence. There is little research, however, about intelligence practices outside of the Intelligence Community; such exploration may provide a more unique perspective for CBP as it seeks to expand its intelligence enterprise. As CBP is at the forefront of emerging threats and has a range of methods to exploit such threats, it may benefit by looking beyond its borders to other well-established intelligence agencies, instead of conforming to how the United States Intelligence Community operates.

4. Border Intelligence

A review of CBP and its role in intelligence is the necessary context for an assessment of its historic and current challenges. Christopher Hall argues that the Department of Homeland Security (DHS) is unable to generate and collect intelligence effectively.⁴⁵ However, he finds value in quasi-intelligence agencies like CBP, despite their historical inexperience in intelligence collection and fusion aspects.⁴⁶ Hall claims that because CBP has not played a significant role inside the IC, it contributes to overall

⁴³ Reinhold, Russo, and Eisenfeld, 113-16.

⁴⁴ Reinhold, Russo, and Eisenfeld, 118.

⁴⁵ Christopher E. Hall, "Has the Department of Homeland Security (DHS) Outlived Its Usefulness?" (master's thesis, Naval Postgraduate School, 2012), <https://hdl.handle.net/10945/27839>.

⁴⁶ Hall.

ineffectiveness in intelligence within DHS. In other words, CBP is capable of coordinating intelligence; however, its inexperience with traditional intelligence practices negatively impacts the intelligence process.

A number of news stories have criticized CBP and its role in intelligence. Alleged violations invite scrutiny and raise doubts about CBP's ability to balance enforcement with intelligence while protecting civil liberties; furthermore, perceived incidents and stories that reflect poorly on the agency negatively impact CBP's ability to expand intelligence roles.⁴⁷ Nevertheless, some welcome the prospect of increased intelligence roles within CBP. Thomas Barnett sees such mission creep as a needed transformation, as opposed to the status quo in which CBP surrenders intelligence functions to other government agencies with greater political influence.⁴⁸ Barnett claims that CBP's role as an enabler and regulator of international trade and travel is threatened in an age of globalization and political polarization.⁴⁹ The author also acknowledges CBP's inexperience in advanced information sharing and risk management, as demonstrated by the agency's strategic goal to improve those areas.⁵⁰ Although CBP is ultimately at the mercy of legislative decision-making, it must transcend its capabilities beyond current practices.

Increased intelligence roles at the border, where travelers surrender to many Fourth Amendment exceptions, can be challenging because of strict sharing policies and international relations. Despite such challenges, Richard Best Jr. argues that a role for intelligence agencies exists in border security; although, he offers recommendations to be successful.⁵¹ Intelligence must not detract from traditional intelligence missions or be

⁴⁷ See, for example: Jana Winter, "Operation Whistle Pig: Inside the Secret CBP Unit with No Rules That Investigates Americans," Yahoo News, December 11, 2021, <https://news.yahoo.com/operation-whistle-pig-inside-the-secret-cbp-unit-with-no-rules-that-investigates-americans-100000147.html>; Karl Jacoby, "Why the CBP's Presence at the DC Protests Should Alarm All of Us," Politico, June 10, 2020, <https://www.politico.com/news/magazine/2020/06/10/cbp-protests-border-zone-312151>.

⁴⁸ Thomas P.M. Barnett, "Capability Gaps Threatening CBP's Present and Future Operations," *Homeland Security Affairs* 15 (September 2019): 3, <https://www.hsaj.org/articles/15389>.

⁴⁹ Barnett, 4.

⁵⁰ Barnett, 9.

⁵¹ Richard A. Best Jr., *Securing America's Borders: The Role of the Intelligence Community*, CRS Report No. R41520 (Washington, DC: Congressional Research Service, 2010), 11, <https://sgp.fas.org/crs/intel/R41520.pdf>.

duplicative, nor should it infringe on U.S. persons' civil liberties or negatively impact U.S.-Canadian and U.S.-Mexican relations.⁵² With those issues in mind, Best Jr. acknowledges the benefits of intelligence in preventing narcotics smuggling and terrorist activity.⁵³ Although the role intelligence serves in border security is mostly classified, designated ports of entry are hubs where officers and agents can collect information about nefarious actors and illicit organizations against U.S. interests.

Existing literature identifies deficiencies in CBP's ability to conduct effective intelligence; however, research is broad in scope. Insufficient exists to highlight the unique capabilities of the Office of Field Operations; and much less, how those capabilities are amplified in airport environments. Regardless, authors are generally wary of how increased intelligence roles at the border could impact American citizens.

D. RESEARCH DESIGN

In light of CBP's desire to expand intelligence capabilities to improve border security, a case study approach will be utilized to understand how OFO can embrace its intelligence capabilities. First, an overview of OFO will attempt to identify contemporary practices and recognize deficiencies in its ability to coordinate intelligence. This part of the analysis will include a historical review of the agency and its performance in intelligence activity. Such analysis will employ inductive reasoning to understand whether current intelligence practices can be improved to enhance border security. Second, given traditional challenges faced by the United States Intelligence Community, comparative government research will attempt to identify how domestic intelligence agencies abroad coordinate intelligence. The study will focus on the British Security Service (MI5), the Australian Security Intelligence Organisation (ASIO), and the Federal Office for the Protection of the Constitution (BfV) to evaluate a potential path forward for OFO. This research will intend to shed light on how each of the studied agencies coordinates intelligence; such research will attempt to provide a deeper understanding of relative practices for OFO to adopt and implement in accordance with existing CBP policies. Both

⁵² Best Jr.

⁵³ Best Jr.

sections rely on existing research, which includes reviewing journal and news articles, policies and procedures, and information from government websites. Such sources will provide additional insight into research gaps to ultimately answer why and how OFO needs to embrace its intelligence frameworks to evolve as an agency capable of improving border security.

This thesis recognizes the disparate roles and responsibilities of established intelligence agencies compared to OFO; furthermore, existing laws and policies may prevent OFO from adopting certain aspects of traditional intelligence activity. However, this thesis aims to synthesize contemporary approaches to intelligence to propel OFO as agency officials define its role within the intelligence enterprise. Considering CBP aspires to improve intelligence capabilities among frontline personnel, it is reasonable to evaluate agencies that employ intelligence professionals. Importantly, this thesis does not advocate collecting more information than OFO already collects; it focuses on how OFO can improve collection, analysis, and dissemination practices to provide tactical- and strategic-level decision advantage. The scope of this research is limited to OFO at international airports; it will not address other components of CBP, nor will it address functions unrelated to intelligence.

E. THESIS OUTLINE

This chapter provides the foundational background to explore effective intelligence practices, especially as they relate to CBP's strategic goals to improve border security capabilities. Chapter II delivers the background for CBP border search authority with a focus on OFO in airport settings. It further provides an assessment of collection, analysis, and dissemination practices before identifying respective limitations. Chapter III is dedicated to comparative research and explores the domestic intelligence practices of the United Kingdom, Australia, and Germany. Such analysis highlights the best practices of each organization to potentially implement as CBP seeks to embrace its own intelligence capabilities. The thesis concludes with Chapter IV, which presents recommendations and an implementation plan for CBP leadership to consider.

II. CBP OFFICE OF FIELD OPERATIONS

This chapter assesses the CBP Office of Field Operations (OFO) and its ability to coordinate intelligence. Although “border security” alludes to securing the land borders separating the United States from Mexico and Canada, border security operations expand to international airports which serve as the functional equivalent to an international border.⁵⁴ By extension, about half of the designated ports of entry in the United States are international airports and one-third of border crossings occur at international airports.⁵⁵ Accordingly, this chapter focuses on OFO at “air” ports of entry, rather than “land” ports of entry; such analysis will provide a different perspective on border security and the role intelligence can serve in operations. Throughout this chapter, it is important to conceptualize OFO through intelligence frameworks—rather than as a traditional law enforcement agency—to provide the necessary context regarding the complexity of OFO and its capability to produce tactical and strategic intelligence for broader homeland security issues.

This chapter serves as the landscape for subsequent chapters and is broken into three sections: 1) An overview of OFO and its unique search authority; 2) An assessment of how OFO operates within the intelligence cycle; and 3) An evaluation of limitations that impede effective intelligence activity. The three sections will provide context to understand OFO’s intelligence capabilities while exploring limitations that require attention.

A. BORDER SEARCH AUTHORITY

OFO is just one component of CBP; another component with separate responsibilities and authorities is the United States Border Patrol (USBP). The two CBP

⁵⁴ Hillel R. Smith and Kelsey Y. Santamaria, *Searches and Seizures at the Border and the Fourth Amendment*, CRS Report No. R46601 (Washington, DC: Congressional Research Service, 2020), 20, <https://crsreports.congress.gov/product/pdf/R/R46601/2>.

⁵⁵ According to GSA, 167 of the 328 ports of entry are land ports of entry. “Land Ports of Entry and the Bipartisan Infrastructure Law,” U.S. General Services Administration, accessed April 21, 2023, <https://www.gsa.gov/real-estate/gsa-properties/land-ports-of-entry/bipartisan-infrastructure-law-construction-projects>; “Traveler and Conveyance Statistics,” Customs and Border Protection, July 18, 2023, <https://www.cbp.gov/newsroom/stats/travel>.

components are important to border security but are commonly confused. An important distinction is that OFO employs CBP officers, whereas USBP employs agents; however, both components adhere to CBP policy since CBP is the overarching agency. Table 1 provides a brief overview of their distinct responsibilities and authorities.

Table 1. Office of Field Operations and United States Border Patrol

United States Customs and Border Protection	
Office of Field Operations	United States Border Patrol
Officers work at ports of entry.	Agents patrol in between and around ports of entry.
Authority remains at the port of entry.	Authority extends 100 miles beyond the border. ⁵⁶
Officers conduct searches at the border and its functional equivalent—such as international airports, seaports, and mail facilities—without probable cause. ⁵⁷	Agents must establish probable cause to search people and conveyances beyond verifying citizenship and making plain-view observations at checkpoints. ⁵⁸

OFO operates with border search authority, an exception to the Fourth Amendment that typically protects against unreasonable search and seizure. Such an exception is significant for OFO to operate efficiently and effectively, especially related to thwarting criminal networks; for example, it would be impractical for OFO to establish probable cause to search for narcotics in luggage belonging to an international traveler. Border search authority is affirmed in the Code of Federal Regulations (19 CFR 162.6), which states, “All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs

⁵⁶ “Legal Authority for the Border Patrol,” June 29, 2023, https://help.cbp.gov/s/article/Article-1084?language=en_US.

⁵⁷ Smith and Santamaria, *Searches and Seizures at the Border and the Fourth Amendment*, 20.

⁵⁸ Customs and Border Protection, “Legal Authority for the Border Patrol.”

officer.”⁵⁹ Several court rulings uphold such authority in favor of the sovereign’s interest to protect itself by examining persons and property crossing into the United States from foreign countries.⁶⁰ Border search authority extends beyond interviews and baggage exams and can, under certain circumstances in accordance with CBP policy, include searches of electronic devices; therefore, OFO is positioned to acquire troves of information from individuals during routine searches when justified under the law.

B. INTELLIGENCE CYCLE

CBP adopts an intelligence cycle comprised of seven phases: planning and direction, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback.⁶¹ Figure 1 provides a visual depiction of the intelligence cycle CBP adopts. Although all components of the intelligence cycle serve an important role in coordinating intelligence, three components are primarily explored in relation to OFO frontline personnel. Specifically, the following subsections—collection, analysis, and dissemination—explore the role CBP officers play in collecting, analyzing, and disseminating information and intelligence.

⁵⁹ Search of Persons, Baggage, and Merchandise, 19 C.F.R. § 162.6 (1972), <https://www.ecfr.gov/current/title-19/chapter-I/part-162/subpart-A/section-162.6>.

⁶⁰ See, for example: *United States v. Ramsey*, 431 U.S. 606 (1977) dealt with searching international mail; *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985) and *United States v. Flores-Montano*, 541 U.S. 149 (2004) dealt with government’s compelling interest to prevent the entry of illegal narcotics; *United States v. Cotterman*, 709 F.3d 952 (2013) dealt with searching electronic devices without a warrant.

⁶¹ Customs and Border Protection, *Air and Marine Operations Vision 2025* (Washington, DC: Department of Homeland Security, 2016), 8, <https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/AMO%20Vision%202025.pdf>.



Figure 1. CBP Intelligence Cycle⁶²

1. Collection

Planning and direction feed the intelligence cycle; specifically, intelligence requirements dictate collection efforts. Policymakers determine which issues need to be addressed by setting intelligence priorities.⁶³ The results of CBP’s planning and direction are Priority Intelligence Requirements (PIR), which are intended to guide collection strategies.⁶⁴ However, not all data collection serves specific intelligence priorities. For

⁶² Source: Customs and Border Protection, *Air and Marine Operations Vision 2025*, 8.

⁶³ “How the IC Works,” Office of the Director of National Intelligence, accessed April 15, 2019, <https://www.intelligence.gov/how-the-ic-works>.

⁶⁴ Customs and Border Protection, *Air and Marine Operations Vision 2025*, 8.

example, CBP integrates biographic and biometric data collection at ports of entry.⁶⁵ Implementing facial recognition technology is a primary way that OFO collects information from international travelers; according to CBP, “...biometric facial comparison technology standardizes, automates, and enhances manual processes by making them more efficient, accurate, and secure.”⁶⁶ Although CBP credits facial recognition with creating a seamless travel process, it also serves as the foundation for data collection.⁶⁷ Furthermore, officers are trained to collect information through interviews and submit a brief report based on interactions with international travelers.⁶⁸ Therefore, OFO is able to collect troves of information from potential threat actors.

a. Passenger and Cargo Collection

For targeted data collection in passenger and cargo environments, OFO deploys specialized teams in furtherance of the various laws CBP enforces. The surveyed collection methods are strategies for collecting valuable information to improve border security and potentially answer PIRs. The following is a non-exhaustive list of specialized teams in OFO tasked with collection; there are many other teams that serve an important role in border security. Additionally, the responsibilities of each team may vary based on staffing and locality.

- Tactical Terrorism Response Team (TTRT) researches information and interviews individuals to mitigate possible threats to national security.⁶⁹ According to CBP, “TTRT officers are immersed in the current and

⁶⁵ Customs and Border Protection, “CBP Access: September 2022,” June 12, 2023, <https://www.cbp.gov/about/congressional-resources/cbp-access/september-2022>.

⁶⁶ “Statement for the Record on Assessing CBP’s Use of Facial Recognition Technology,” Customs and Border Protection, August 29, 2022, <https://www.cbp.gov/about/congressional-resources/testimony/statement-record-assessing-cbps-use-facial-recognition-technology>.

⁶⁷ Customs and Border Protection.

⁶⁸ Jacqueline Russell-Taylor, *Privacy Impact Assessment Update for the TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative*, DHS/CBP/PIA-009(a) (Washington, DC: Department of Homeland Security, 2011), 2, <https://www.dhs.gov/publication/tecs-system-cbp-primary-and-secondary-processing-tecs-national-sar-initiative>.

⁶⁹ *Denying Terrorists Entry to the United States: Examining Visa Security: Hearing before the Task Force on Denying Terrorists Entry to the United States*, 115th Cong. 1, (2017), 18, <https://www.govinfo.gov/content/pkg/CHRG-115hhrg27293/pdf/CHRG-115hhrg27293.pdf>.

developing threat picture through the continuous review of information, and are responsible for the examination of travelers...suspected of having a nexus to terrorism.”⁷⁰ Kevin McAleenan—former CBP Commissioner—elaborates that TTRT officers use their instincts to identify potential threats to national security.⁷¹

- Passenger Enforcement Rover Team (PERT) is responsible for identifying and interdicting high-risk passengers attempting to bring contraband, including narcotics, into the United States.⁷² PERT is trained to select travelers for “cold-stop” examinations based on observational techniques and staying current on concealment trends and methods.⁷³
- Passport Control Secondary (PCS) processes violations of the Immigration and Nationality Act which may result in administrative or criminal adverse actions, including a determination of inadmissibility to the United States.⁷⁴ Typical adverse actions include Expedited Removals, Visa Waiver Refusals, Notices to Appear, and Expedited Removal with

⁷⁰ H.R., *Denying Terrorist Entry to the United States*.

⁷¹ Brian Dodwell and Paul Cruickshank, “A View from the CT Foxhole: An Interview with Kevin McAleenan, Commissioner of U.S. Customs and Border Protection,” *CTC Sentinel* 11, no. 8 (September 2018): 9–14, <https://ctc.westpoint.edu/view-ct-foxhole-interview-kevin-mcaleenan-commissioner-u-s-customs-border-protection/>.

⁷² Richard M. Stana, *Border Security: Additional Steps Needed to Ensure That Officers Are Fully Trained*, GAO-12-269 (Washington, DC: Government Accountability Office, 2011), 30, <https://www.gao.gov/products/gao-12-269>.

⁷³ “Passenger Enforcement Rover Team,” American Council on Education, accessed July 19, 2023, <https://www.acenet.edu/National-Guide/Pages/Course.aspx?org=U.S.+Customs+and+Border+Protection&cid=9713cf9c-271f-ec11-b6e6-000d3a34f821&oid=92099b28-9016-e811-810f-5065f38bf0e1>.

⁷⁴ Stana, *Border Security*, 30.

Credible Fear.⁷⁵ Therefore, during an adverse action, considerable derogatory information may be captured and documented.⁷⁶

- Anti-Terrorism Contraband Enforcement Team (A-TCET) conducts inbound and outbound inspections for contraband in passenger and cargo environments.⁷⁷ A-TCET has counterterrorism objectives, but CBP estimates that almost 70 percent of its officers' efforts are devoted to drug enforcement.⁷⁸

b. Digital Data Collection

OFO routinely searches electronic devices at the border. Digital searches are a longstanding practice to collect information and are considered essential to border security.⁷⁹ According to CBP, digital searches are “driven by [its] mission to protect the American people and enforce the nation’s laws in this digital age.”⁸⁰ Such searches are helpful in combatting terrorist activity, child pornography, export violations, intellectual property rights violations, and visa fraud.⁸¹ Considering the level of intrusiveness of a digital search—compared to a luggage exam—CBP implemented a policy that outlines how officers can search electronic devices.

⁷⁵ Executive Director Admissibility and Passenger Programs, “Providing Inadmissible Travelers with Documentation of an Adverse Action” (official memorandum, Washington, DC: Customs and Border Patrol, 2012), https://www.cbp.gov/sites/default/files/assets/documents/2022-May/Providing%20Inadmissible%20Travelers%20with%20Documentation%20of%20an%20Adverse%20Action_Redacted.pdf.

⁷⁶ Executive Director Admissibility and Passenger Programs.

⁷⁷ Stana, Border Security, 31.

⁷⁸ Office of Inspector General, *Review of U.S. Customs and Border Protection’s Fiscal Year 2022*, 9.

⁷⁹ Customs and Border Protection, *Border Search of Electronic Devices*, CBP Directive No., 3340-049A (Washington, DC: Customs and Border Protection, 2018), <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf>.

⁸⁰ “CBP Releases Statistics on Electronic Device Searches,” Customs and Border Protection, April 11, 2017, <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0>.

⁸¹ Customs and Border Protection.

The Border Search of Electronic Devices directive (CBP Directive 3340–049A) outlines when, where, and how officers can search electronic devices.⁸² As part of CBP’s border search authority, and depending on the level of suspicion that an enforceable law has been violated, an electronic search may be conducted as a cursory review—also referred to as a basic search—or it may involve connecting the device to external equipment to copy its contents for analysis.⁸³ Regardless of the level of intrusiveness, electronic devices must be disconnected from cellular and Wi-Fi networks before a search begins.⁸⁴ By disabling connectivity, officers can only review what is physically stored on a device, which restricts the officer from searching content in the mobile cloud and otherwise beyond the border. Accessing mobile cloud content would be like an officer finding a key during a luggage exam, driving to the traveler’s house, using the key to open a lock box, and searching its contents. Although digital searches are more intrusive than a luggage exam, the policy prevents officers from conducting searches beyond the port of entry. Strict adherence to policy is paramount for officers to use electronic devices as key sources of intelligence.

2. Analysis

In the land border environment, CBP officers are generally unable to predict who will arrive at a port of entry; in the airport environment, however, officers benefit from advanced notice. The Advance Passenger Information System (APIS) provides officers with flight manifest data on all passengers and crew members, thus permitting advanced analysis.⁸⁵ Similarly, the Air Cargo Advance Screening (ACAS) system provides officers with relevant information to conduct risk assessments of incoming shipments.⁸⁶ Both systems store advanced data that allows officers in analytical roles to anticipate who and

⁸² Customs and Border Protection, *Border Search of Electronic Devices*.

⁸³ Customs and Border Protection.

⁸⁴ Customs and Border Protection.

⁸⁵ “APIS: Advance Passenger Information System,” For Travel Industry Personnel, July 24, 2023, <https://www.cbp.gov/travel/travel-industry-personnel/apis2>.

⁸⁶ Dennis McKenzie, *Privacy Impact Assessment for the Air Cargo Advance Screening (ACAS)*, DHS/CBP/PIA-061 (Washington, DC: Department of Homeland Security, 2019), 2, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-acas-061-october2019.pdf>.

what is crossing United States borders. Two teams with analytical roles are identified below; however, there are other teams in OFO tasked with analytical functions.

- Passenger Analytical Unit (PAU) screens passengers arriving to or departing the United States.⁸⁷ Responsibilities include analyzing flight manifests to coordinate enforcement exams.⁸⁸ Officers use automated systems to target high-risk passengers and identify potential threats.⁸⁹ PAU works closely with enforcement teams, including A-TCET and PERT.⁹⁰
- Advanced Targeting Unit (ATU) identifies cargo that is at risk for containing weapons of mass destruction, narcotics, and other contraband; although automated systems may assign a risk score to some containers, officers in ATU may identify additional cargo for inspection.⁹¹ In contrast to PAU, officers assigned to ATU target high-risk commercial shipments.⁹²

CBP officers use various systems to process, exploit, and analyze the data provided by APIS and ACAS. The primary system for data analysis is the Automated Targeting System (ATS), which provides information based on travel patterns to help officers make decisions. According to DHS, “ATS is a decision support tool that compares traveler,

⁸⁷ “Customs-Trade Partnership against Terrorism (CTPAT) Session” Customs and Border Protection, September 9, 2020, <https://www.cbp.gov/sites/default/files/assets/documents/2020-Sep/CBP%20Virtual%20Trade%20Week%20Biographies-%20CTPAT%20Session%20-%20Wed.%20Sept%209%202020.pdf>; Customs and Border Protection, *Traveler Verification Service Standard Operating Procedure* (Washington, DC: Department of Homeland Security, 2017).

⁸⁸ Customs and Border Protection, *Facial Debarkation: Sea Innovation, Mobility, Biometric Advancement*, FOIA CBP 000194 (Washington, DC: Department of Homeland Security, 2020), <https://www.cbp.gov/sites/default/files/assets/documents/2022-Mar/Second%20Interim%20Response%20%2820-cv-02213-NRB%29.pdf>.

⁸⁹ Stana, Border Security, 30.

⁹⁰ Office of Inspector General, *Review of U.S. Customs and Border Protection’s Fiscal Year 2022*, 9.

⁹¹ Vivian C. Jones and Audrey Singer, *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*, CRS Report No. R43014 (Washington, DC: Congressional Research Service, 2015), 28, <https://crsreports.congress.gov/product/pdf/R/R43014/14>.

⁹² Stana, Border Security, 31.

cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments.”⁹³ ATS compares existing information with patterns that require additional scrutiny, known as targeting rules.⁹⁴ The data retained in ATS is used to select cargo and conveyances for inspection to fulfill border security objectives.⁹⁵ Unified Passenger (UPAX) technology is an updated version of ATS and consolidates information from disparate systems; UPAX also modernizes the visual presentation of relevant information.⁹⁶ For cargo analysis, officers in analytical roles typically use ATS to analyze cargo arriving in the United States; conversely, officers will use the Exodus Accountability Referral System to analyze cargo departing the United States.⁹⁷ Expertise in analytical systems further expands OFO’s ability to analyze information related to passengers and cargo shipments.

Open-source methods are another way for OFO to analyze relevant information. The Publicly Available Information Group provides “advanced open-source and social media research and analysis support to CBP...for strategic and tactical targeting, vetting, and analysis missions and operations.”⁹⁸ For example, access to open-source systems helps OFO exploit and analyze relevant traveler information on social media platforms.⁹⁹ According to CBP, “Information found in social media will enhance the vetting process and may be used to...validate legitimate travel...and identify potential threats.”¹⁰⁰ Aside

⁹³ Mario Medina, *Privacy Impact Assessment Update for the Automated Targeting System*, DHS/CBP/PIA-006(e) (Washington, DC: Department of Homeland Security, 2017), 2, <https://www.dhs.gov/sites/default/files/2022-10/privacy-pia-cbp010%28a%29-afi-october2022.pdf>.

⁹⁴ Medina, 2.

⁹⁵ McKenzie, *Privacy Impact Assessment for the Air Cargo Advance Screening (ACAS)*, 12.

⁹⁶ Medina, *Privacy Impact Assessment Update for the Automated Targeting System*, 12.

⁹⁷ Medina, *Privacy Impact Assessment Update for the Automated Targeting System*; James Dinkins, *Privacy Impact Assessment for the Exodus Accountability Referral System (EARS)* (Washington, DC: Department of Homeland Security, 2010), 8, https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_ears.pdf.

⁹⁸ Department of Homeland Security, *U.S. Customs and Border Protection: Budget Overview Fiscal Year 2018 Congressional Justification* (Washington, DC: Department of Homeland Security, 2018), 124, <https://www.dhs.gov/sites/default/files/publications/CBP%20FY18%20Budget.pdf>.

⁹⁹ “Frequently Asked Questions: Privacy and Security,” Customs and Border Protection, accessed August 4, 2023, <https://esta.cbp.dhs.gov/faq?lang=en>.

¹⁰⁰ Customs and Border Protection.

from exploiting and analyzing social media accounts, open-source search platforms can also help identify images, tattoos, symbols, and logos. Indeed, open-source systems provide officers with another avenue to identify, disrupt, and mitigate potential threats.

3. Dissemination

OFO utilizes a system to store intelligence and information products. Intelligence is disseminated and consumed through the Analytical Framework for Intelligence (AFI), a consolidated system for officers to research, analyze data, and develop intelligence products.¹⁰¹ AFI indexes information from various government systems, allowing officers to search multiple databases simultaneously.¹⁰² According to DHS, “AFI improves the efficiency and effectiveness of CBP’s research and analysis process by providing a platform for the research, collaboration, approval, and publication of finished intelligence products.”¹⁰³ Intelligence products in AFI can provide context about current and emerging threats; according to DHS, AFI is also used for “sharing finished intelligence products...with DHS employees who have a need to know in the performance of their official duties and who have appropriate clearances or permissions.”¹⁰⁴ After OFO publishes an intelligence product, and depending on permissions to view it, anyone with a need-to-know can view the product. Because any DHS employee with appropriate access to AFI can view intelligence products, a variety of personnel can use a published product to plan or direct operations. Therefore, AFI serves as a medium to disseminate intelligence and relevant information products to consumers.

C. LIMITATIONS

Despite various opportunities to collect information, and platforms to analyze and disseminate intelligence, OFO can improve how it embraces its capabilities to coordinate

¹⁰¹ Medina, *Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI)*, 2.

¹⁰² Medina, 3.

¹⁰³ Medina, 5.

¹⁰⁴ Jim Gleason, *Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)*, DHS/CBP/PIA-010 (Washington, DC: Department of Homeland Security, 2012), 2, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.

intelligence. OFO stresses the need to use the information it collects in a more strategic manner; specifically, OFO prioritizes the ability to visualize and extract value from data.¹⁰⁵ OFO seeks to leverage its authority, data holdings, intelligence capabilities, and information-sharing partnerships to improve agency outcomes and build a workforce capable of utilizing actionable intelligence.¹⁰⁶ According to CBP, it will take “an enterprise-wide approach to...empower personnel in various roles to access and explore scenarios, potential outcomes, and relationships that exist within available data.”¹⁰⁷ Although CBP hires Intelligence Research Specialists to execute “all-source intelligence compilation, analysis, production, and dissemination,” specialists can only analyze what is collected; furthermore, CBP’s goal is to integrate intelligence so that officers and agents can also analyze, produce, and disseminate intelligence.¹⁰⁸ However, several factors appear to limit OFO’s ability to leverage its authority and integrate intelligence into frontline operations; limitations include disparate responsibilities and competing priorities, insufficient intelligence structures, and public awareness about CBP’s mission.

1. Disparate Responsibilities and Competing Priorities

Disparate responsibilities and competing priorities affect OFO’s ability to evolve beyond traditional practices and emerge as an agency driven by intelligence. A disconnect exists between collection and analysis, and even more so between passenger and cargo operations. As previously outlined, several specialized units focus on the collection or analysis of passengers or cargo. Such separation hinders analytically driven collection efforts. Lowenthal identifies analytically driven collection as the ideal state, in which collectors act in response to analytic needs rather than collecting information independently.¹⁰⁹ CBP officers are trained to enforce laws, not necessarily to collect

¹⁰⁵ Customs and Border Protection, *CBP Strategy 2021–2026*, 23.

¹⁰⁶ Customs and Border Protection, 25.

¹⁰⁷ Customs and Border Protection, 23.

¹⁰⁸ “Careers: Intelligence Research Specialist,” September 28, 2022, <https://www.cbp.gov/careers/professional/0132-intelligence-research-specialist>.

¹⁰⁹ Lowenthal, *Intelligence*, 81.

information based on existing intelligence needs.¹¹⁰ Consequently, the components of the intelligence cycle remain disconnected as some teams collect information, some interdict contraband, and others analyze data. Such disparate responsibilities impact the ability to integrate intelligence into OFO frontline operations.

Competing priorities overshadow other concerns pertaining to border security. Border security expands beyond historical foreign terrorist threats and includes emerging national security concerns, like domestic violent extremism, espionage and foreign interference, and transnational criminal organizations. However, when specialized teams have siloed responsibilities, the ability to identify broader threats is marginalized. For example, although the primary mission of A-TCET is anti-terrorism, almost 70 percent of its efforts are geared toward drug enforcement.¹¹¹ Similarly, OFO estimates that 85 percent of funding for drug enforcement is dedicated to interdiction and only 15 percent is dedicated to intelligence.¹¹² A disproportionate focus on interdiction—like collection—complicates the task of finding meaningful intelligence.¹¹³ The disconnect between priorities exists across most teams previously discussed: TTRT focuses on terrorism; PERT focuses on drugs; PCS focuses on immigration. A failure to intersect priorities limits OFO’s ability to recognize nuances in the ever-expanding threat landscape. Indeed, OFO will struggle to transcend the limits of its intelligence capabilities if disparate responsibilities and competing priorities are not addressed.

2. Insufficient Intelligence Structures

OFO lacks robust intelligence structures to coordinate intelligence effectively; perhaps that is the reason CBP seeks to extend intelligence capabilities to the field. Part of CBP’s initiative to foster intelligence integration is to improve analytical capabilities.¹¹⁴ Lowenthal argues that intelligence requires collection to be an analytically driven effort,

¹¹⁰ Office of Personnel Management, “Customs and Border Protection Series 1895.”

¹¹¹ Office of Inspector General, *Review of U.S. Customs and Border Protection’s Fiscal Year 2022*, 9.

¹¹² Office of Inspector General.

¹¹³ Lowenthal, *Intelligence*, 79.

¹¹⁴ Customs and Border Protection, *CBP Strategy 2021-2026*, 11.

through which collection and analysis amalgamates.¹¹⁵ To promote intelligence integration and improve analytical capabilities, CBP intends to develop an intelligence academy; however, training 26,000 CBP officers is a difficult task.¹¹⁶ Although CBP states that the delivery of intelligence training will include satellite training sites and mobile training teams, courses also hinge on virtual training, which is statistically less effective than in-person participation.¹¹⁷ The development of an intelligence training academy with virtual coursework requires measures to ensure participant engagement and methods to avoid “Zoom fatigue.”¹¹⁸ Although virtual training may be the most efficient way to train many officers from different field offices simultaneously, the absence of well-defined intelligence structures increases the risk of conducting mass training with limited impact.

Despite OFO’s capability to vet potential threats and analyze information with advanced systems like APIS, ATS, and AFI, officers are not trained as analysts. Analytical systems, like ATS and AFI, may provide officers with opportunities to analyze information more efficiently; however, mere access to a system does not cultivate effective analysis. Although OFO has access to various tools to assist with exploitation and analysis, the ability to connect the dots and thwart contemporary threats requires sophisticated intelligence analysis that provokes imagination and intellectual curiosity.¹¹⁹ The importance of effective exploitation and analysis cannot be overstated; poorly analyzed information threatens homeland security and leaves decision-makers vulnerable to information directly in front of them.

OFO is limited in its ability to disseminate intelligence effectively. Lowenthal points out that identifying requirements, conducting collection, and processing information are meaningless tasks if analysts cannot generate reports that meet the needs of

¹¹⁵ Lowenthal, *Intelligence*, 81.

¹¹⁶ Customs and Border Protection, *CBP Strategy 2021-2026*, 25.

¹¹⁷ Customs and Border Protection, 25; Gregory Gross et al., “In-Person or Virtual Training?: Comparing the Effectiveness of Community-Based Training,” *American Journal of Distance Education* 37, no. 1 (2023): 66, <https://doi.org/10.1080/08923647.2022.2029090>.

¹¹⁸ Gross et al., “In-Person or Virtual Training?,” 72-73.

¹¹⁹ Harris, “The Consequences of Eroding Human Intelligence Collection.”

policymakers.¹²⁰ The same can be said about dissemination; after all, intelligence is of little use until it is received by its consumers.¹²¹ Merely distributing information and intelligence does not sufficiently satisfy the dissemination component of the intelligence cycle. Although AFI serves as a hub for CBP intelligence, publishing an intelligence product does not satisfy the dissemination phase. As Steele might describe it, AFI is the cart that delivers intelligence to consumers.¹²² Accordingly, the existence of AFI does not satisfy the assumption that intelligence is an accurate assessment, nor that it will be adequately conveyed to decision-makers. Considering improper analytical training and ineffective dissemination affect how future collection efforts are dictated, a lack of intelligence structures are ports of entry impacts how OFO can integrate intelligence within its frontline ranks.

3. Public Awareness

OFO, and DHS generally, can improve the public's awareness about the teams it deploys to protect America and its borders. DHS issues Privacy Impact Assessments (PIA) when new systems are deployed to the field; PIAs notify the public about the information DHS collects, why DHS collects it, and how DHS will use, share, safeguard, and store it.¹²³ However, the public is largely unaware of the specialized work units within OFO. This is problematic for several reasons. If someone wanted more information about TTRT, for example, an open-source search would indicate the counterterrorism team is a "highly secretive unit" that "interrogate [s] innocent travelers."¹²⁴ It is important to note that such presumptions are uninformed. Particular tools, methods, and techniques are understandably safeguarded; nevertheless, there is a need to communicate the specialized teams that exist

¹²⁰ Lowenthal, *Intelligence*, 74.

¹²¹ Dahl, "Why Won't They Listen?," 1.

¹²² Steele, Information Operations, 32.

¹²³ "Privacy Impact Assessments," Department of Homeland Security, August 18, 2024AD, <https://www.dhs.gov/privacy-impact-assessments>.

¹²⁴ Daniella Silva, "ACLU Sues CBP over 'Highly Secretive' Teams Detaining Travelers," NBC News, December 19, 2019, <https://www.nbcnews.com/news/us-news/aclu-sues-cbp-over-highly-secretive-teams-detaining-travelers-n1104166>.

within OFO and the purpose they serve. A failure to do so may lead the public to formulate its own conclusions about the objectives of various teams.

The benefits of improved awareness extend internally to CBP personnel and law enforcement partners. A lack of awareness increases the risk that officers and agents may interpret sharing obligations differently than the information-sharing expectations.¹²⁵ Being more transparent can help foster the reciprocal sharing of information and help fulfill the intended purpose of the partnership.¹²⁶ CBP's increased involvement with the Joint Terrorism Task Force, for example, has led to better awareness of respective functions and capabilities.¹²⁷ However, such partnerships rely on formal memorandums of understanding (MOU) to establish information-sharing guidelines.¹²⁸ For new partnerships—and informal ones—transparency is necessary to provide context and awareness of OFO's roles and responsibilities, resulting in collaboration and trust.¹²⁹ Therefore, increased awareness about OFO's capabilities, and the specialized teams it deploys, can have a positive impact on agency outcomes and interagency cooperation.

D. CONCLUSION

OFO explores ways to expand its intelligence enterprise to improve border security. Simply, OFO wants to make better use of readily available information by integrating intelligence and expanding capabilities to frontline operations. Officers have the tools to collect, analyze, and disseminate information; however, intelligence integration is limited by disparate responsibilities and competing priorities, insufficient intelligence structures, and public awareness of CBP operations. The next chapter explores how foreign agencies structure intelligence and prioritize threats. Such exploration may provide a path for OFO

¹²⁵ Inspectors General et al., *Review of Domestic Sharing of Counterterrorism Information*, OIG-17-49 (Washington, DC: Department of Justice, 2017), 10, <https://oig.justice.gov/sites/default/files/reports/OIG-17-49-Mar17.pdf>.

¹²⁶ Inspectors General et al., 11.

¹²⁷ Inspectors General et al., 11.

¹²⁸ Inspectors General et al., i.

¹²⁹ Inspectors General et al., 11.

to overcome the limitations identified in this chapter and achieve its strategic goal of integrating intelligence into frontline operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COMPARATIVE ANALYSIS OF MI5, ASIO, AND BFV

This chapter surveys the intelligence capabilities, frameworks, and priorities of the British Security Service (MI5), the Australian Security Intelligence Organisation (ASIO), and the German Federal Office for the Protection of the Constitution (BfV). Each intelligence agency has unique approaches to intelligence and prioritizes threats differently, primarily based on historical precedence and geographical positioning in the world. Importantly, the disparate priorities set by each agency drive respective intelligence activity; similarly, the priorities outlined in this chapter also impact homeland security in the United States. As CBP seeks to leverage its authority, data holdings, intelligence capabilities, and information-sharing partnerships, this chapter surveys best practices associated with the intelligence agencies that have vast experience countering threats that similarly impact United States border security and its broader homeland security landscape. Therefore, the purpose of this chapter is not meant to make a direct comparison between OFO and well-established intelligence agencies; rather, this chapter attempts to identify working concepts for OFO to adopt as it seeks to embrace intelligence capabilities to improve border security. Although coordinating intelligence is not the sole mission of CBP, its desire to improve intelligence capabilities warrants the following comparative research.

For each of the three agencies, the chapter will begin with a brief overview of the agency's history, followed by an examination of its structure and mission priorities in relation to domestic security. Each agency's history, structure, and threat priorities provide insight into how they coordinate intelligence to protect their countries from threats. Throughout the chapter, the reader should be able to identify how each agency values transparency, structures intelligence, and prioritizes threats. At the conclusion of the chapter, the best practices of each agency will be identified to serve OFO as it seeks to integrate intelligence into frontline operations.

A. UNITED KINGDOM SECURITY SERVICE

United Kingdom's Security Service (MI5) serves to protect the United Kingdom from domestic and international threats. It is the primary intelligence agency tasked with

protecting national security, safeguarding economic well-being, and acting in support of police and law enforcement to prevent serious crime.¹³⁰ Importantly, MI5's work is "guided by the government's overall strategy to counter threats to the UK's national security."¹³¹ How MI5 coordinates intelligence is influenced by its history, structure, and priorities.

1. History

MI5 conducted and coordinated intelligence activity long before it was publicly acknowledged and statutorily established as an intelligence agency. Despite conducting intelligence activity since 1909, MI5 was not recognized as an official intelligence apparatus until 1952. Known as the Maxwell Fyfe Directive, the then Security Service was tasked with "the Defence of the Realm as a whole, from external and internal dangers arising from attempts at espionage and sabotage, or from actions of persons and organisations whether directed from within or without the country, which may be judged to be subversive to the State."¹³² However, it was not until 1989 that legislation provided statutory footing for MI5.¹³³ Although many suspected that a more public-facing stance would cause a reduction of secrecy, David Bickford—former legal director of MI5—argued that society would prosper if secrecy were diminished to a necessary minimum.¹³⁴ Furthermore, according to Bickford, "law enforcement and intelligence agencies [would] amalgamate."¹³⁵ Therefore, legislation provided needed transparency—and structure—for

¹³⁰ UK Cabinet Office, *National Intelligence Machinery* (London: UK Cabinet Office, 2010), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf.

¹³¹ "MI5 Protects the UK against Threats to National Security," Security Service MI5, accessed July 20, 2023, <https://www.mi5.gov.uk/what-we-do>.

¹³² David Maxwell Fyfe, "The Directive to the Director General of the Security Service" (Undercover Policing Inquiry, September 24, 1952), <https://www.ucpi.org.uk/wp-content/uploads/2023/01/UCPI0000034262.pdf>.

¹³³ Philip Davies, "Review: Step Changes and Learning Curves in the History of British Intelligence," *Contemporary European History* 22, no. 4 (2013): 691, <https://www.jstor.org/stable/43299411>.

¹³⁴ David Bickford, "The Accountability of the Security and Intelligence Agencies with Particular Regard to the Security Service," Parliament Select Committee on Home Affairs, June 21, 1999, <https://publications.parliament.uk/pa/cm199899/cmselect/cmhaff/291/291ap03.htm>.

¹³⁵ Bickford.

MI5 to coordinate intelligence, effectively share information, and pursue criminal and terrorist activity. The following legislation helped legitimize and refine the scope of MI5:

- The Security Service Act 1989 (SSA) legally provisioned MI5 to obtain warrants and established procedures for investigation.¹³⁶ The SSA was later amended in 1996 to give MI5 the additional role of supporting police and other law enforcement agencies with the prevention of serious crimes; however, in 2006, MI5 suspended such activity to focus on counterterrorism.¹³⁷
- The Regulation of Investigatory Powers Act 2000 (RIPA) regulates how MI5 intercepts, acquires, and uses intelligence.¹³⁸ Specifically, RIPA governs the use of technical surveillance and covert human intelligence sources.¹³⁹
- The Investigatory Powers Act 2016 provides a framework for the investigatory powers of British intelligence agencies, like MI5; specifically, the act relates to how communications can be obtained, intercepted, and retained.¹⁴⁰

2. Structure

The United Kingdom Intelligence Community (UKIC) consists of three main agencies. In addition to MI5, the Secret Intelligence Service (SIS or MI6) and the Government Communications Headquarters (GCHQ) play a major role in national security

¹³⁶ UK Public General Acts, “Security Service Act 1989,” Pub. L. No. 1989, § 5 (1989), <https://www.legislation.gov.uk/ukpga/1989/5/contents>.

¹³⁷ Chris Northcott, “The Role, Organization, and Methods of MI5,” *International Journal of Intelligence and CounterIntelligence* 20, no. 3 (2007): 473–75, <https://doi.org/10.1080/08850600701249758>.

¹³⁸ UK Public General Acts, “Regulation of Investigatory Powers Act 2000,” Pub. L. No. 2000, § 23 (2000), <https://www.legislation.gov.uk/ukpga/2000/23/introduction>.

¹³⁹ UK Public General Acts, “Regulation of Investigatory Powers Act 2000.”

¹⁴⁰ Home Office, *Report on the Operation of the Investigatory Powers Act 2016* (London: Home Office, 2023), <https://www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016>.

and are collectively known as the Agencies.¹⁴¹ Generally, SIS conducts foreign intelligence operations and GCHQ specializes in signals intelligence and cyber security.¹⁴² The work of UKIC members contributes to the decision-making process of the Joint Intelligence Committee and the Joint Intelligence Organisation, which serve to provide all-source assessments for policymakers while supporting collaboration and intelligence capabilities.¹⁴³ Therefore, MI5 is just one contributor to the United Kingdom's national strategy.

Unique to MI5 is a system that streamlines how intelligence is collected and used to support investigations, counter threats, advise stakeholders, and assist other agencies. British intelligence features a Desk Officer System; a Desk Officer (DO) is tasked with investigating one or several targets and coordinates the appropriate collection method, such as physical or technical surveillance, based on the necessity of the collection method and its proportionality to the threat.¹⁴⁴ DOs receive and disseminate intelligence to further their investigation, fill intelligence gaps, and provide actionable intelligence.¹⁴⁵ Therefore, DOs are more than analysts; they are also investigators and serve as subject matter experts of a specific target. Indeed, the Desk Officer System is beneficial to an overall intelligence product; however, the system requires the DO to be adequately trained and intellectually curious. As the quarterback of intelligence, the DO is centrally responsible for disseminating a complete and comprehensive intelligence product; therefore, the DO must ensure that information is appropriately collected, analyzed, and disseminated effectively.

¹⁴¹ UK Cabinet Office, *National Intelligence Machinery*, 1.

¹⁴² Home Office, "Secret Intelligence Service," UK Government, October 13, 2015, <https://www.gov.uk/government/organisations/secret-intelligence-service>; "Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber-Intelligence Agency," *Journal of Military and Strategic Studies* 20, no. 3 (2021): 2, <https://jmss.org/article/view/72868>.

¹⁴³ Home Office, "Joint Intelligence Organisation," GOV.UK, accessed August 4, 2023, <https://www.gov.uk/government/groups/joint-intelligence-organisation>.

¹⁴⁴ Paul Jonathan Smith, "Counterterrorism in the United Kingdom," in *Module III: The UK's Counterterrorism Structure and the Pursuit of Terrorists* (Monterey, CA: Center for Homeland Defense & Security, August 3, 2023), https://www.chds.us/coursefiles/comp/lectures/comp_CT_in_the_UK_mod03/script.pdf.

¹⁴⁵ Smith, "Counterterrorism in the United Kingdom."

3. Priorities

The mission priorities for MI5 are broken into four main categories. According to MI5, “the main threats to national security that MI5 counters are terrorism, espionage, cyber threats and the proliferation of weapons of mass destruction.”¹⁴⁶ The counterterrorism mission is a broad priority and includes efforts to disrupt international terrorism, Northern Ireland-related terrorism, Right Wing Terrorism, and Left, Anarchist, and Single-Issue Terrorism.¹⁴⁷ Although espionage, cyber threats, and weapons of mass destruction are legitimate threats to the United Kingdom, the counterterrorism mission reigns supreme. The United Kingdom’s counterterrorism strategy (CONTEST) includes an approach to unite public and private sectors, communities, citizens, and foreign partners to counter all forms of terrorism.¹⁴⁸ According to CONTEST, its four ‘P’ framework is a proven and reliable:

- Prevent: to stop people becoming terrorists or supporting terrorism.
- Pursue: to stop terrorist attacks.
- Protect: to strengthen our protection against a terrorist attack.
- Prepare: to mitigate the impact of a terrorist attack.¹⁴⁹

Although CONTEST is not specific to MI5—the strategy is a national response—it certainly positions MI5 to prioritize terrorism over espionage, cyber threats, and the proliferation of weapons of mass destruction.

4. Intelligence Activity

MI5 generally conducts the following activity: gathering, analyzing, and assessing intelligence; countering sources of threats; advising government officials and other stakeholders of threats and appropriate security measures; and assisting other agencies in

¹⁴⁶ Security Service MI5, “What We Do.”

¹⁴⁷ “Introduction to Counter-Terrorism,” Security Service MI5, accessed August 2, 2023, <https://www.mi5.gov.uk/counter-terrorism>.

¹⁴⁸ Secretary of State for the Home Department, *CONTEST: The United Kingdom’s Strategy for Countering Terrorism* (London: Her Majesty’s Stationery Office, 2018), 7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

¹⁴⁹ Secretary of State for the Home Department, *CONTEST*, 8.

combatting threats.¹⁵⁰ Although MI5 does not have the authority to make arrests, it does work closely with law enforcement agencies to provide them with the necessary information to coordinate arrests and take preventative measures.¹⁵¹ Without executive powers, information-sharing is an integral part of MI5 intelligence activity to protect the United Kingdom from threats.

MI5 gathers information by means of human intelligence (HUMINT) and surveillance. Although HUMINT is a category of intelligence by which information is collected covertly or overtly from human sources, MI5 places great emphasis on covert—or clandestine—methods.¹⁵² Surveillance, either physical or technical, is the other primary collection method employed by MI5.¹⁵³ Physical surveillance is the direct observation of people, while technical surveillance includes intercepting communications and tapping phones.¹⁵⁴ Importantly, collection methods must be necessary for national security and proportionate to the threat.¹⁵⁵ Ensuring that collection methods are necessary and proportionate is an important criterion considering how transparent MI5 is about its collection methods. Despite the secrecy associated with intelligence activity, MI5's collection methods are disclosed on its website, including the use of eavesdropping devices; such transparency about collection efforts helps normalize intelligence activity.¹⁵⁶

The British intelligence cycle supports MI5 activity. Chris Northcott explains that the work of MI5 falls into four main categories, which include investigating, acting, advising, and assisting:

- Investigating – collecting, collating, analyzing, and assessing secret intelligence pertinent to the threat.
- Acting – countering the threats.

¹⁵⁰ UK Cabinet Office, *National Intelligence Machinery*, 10–11.

¹⁵¹ UK Cabinet Office, 11.

¹⁵² “How MI5 Gather Intelligence,” Security Service MI5, accessed August 4, 2023, <https://www.mi5.gov.uk/gathering-intelligence>.

¹⁵³ Davies, “Step Changes and Learning Curves.”

¹⁵⁴ Security Service MI5, “How MI5 Gather Intelligence.”

¹⁵⁵ Security Service MI5, “How MI5 Gather Intelligence.”

¹⁵⁶ Security Service MI5, “How MI5 Gather Intelligence.”

- Advising – keeping the government and others informed about the threats, and advising on the correct countermeasures, including protective security.
- Assisting – supporting other agencies, organizations, and governments.¹⁵⁷

The raw information that MI5 collects and analyzes must be used, stored, or discarded; though, a considerable amount of intelligence is too vague on its own.¹⁵⁸ Therefore, MI5 may store seemingly insignificant intelligence to connect the dots later. Importantly, MI5 must decide when collected information requires further analysis and when it is no longer needed; such insight and experience provide context to coordinate intelligence specific to investigating, acting, advising, or assisting.

MI5 works closely with law enforcement agencies to act on the intelligence it produces. Because MI5 does not hold executive powers, it provides other agencies with recommendations to take enforcement action against individuals who pose a threat to national security.¹⁵⁹ Therefore, according to former Director of MI5 Jonathan Evans, the relationship with the police is crucial.¹⁶⁰ Echoed by Bruce Hoffman, prevention of terrorist events from materializing “comes first from the cop on the beat.”¹⁶¹ Part of MI5’s success lies in the recognition of the vital intelligence role that police play. Such recognition transcends partnerships beyond MOUs and facilitates robust frameworks that promote the receptive consumption of tactical and strategic intelligence.

B. AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

Similar to MI5, the Australian Security Intelligence Organisation (ASIO) plays a crucial role in protecting Australia from both domestic and international threats. It collects

¹⁵⁷ Northcott, “The Role, Organization, and Methods of MI5,” 471.

¹⁵⁸ Northcott, 472.

¹⁵⁹ Northcott, 467.

¹⁶⁰ Smith, “Counterterrorism in the United Kingdom.”

¹⁶¹ Hoffman, *Inside Terrorism*, 179.

intelligence to investigate, uncover, and understand threats to Australia.¹⁶² ASIO has less experience in the intelligence profession than MI5, and perhaps the least of the Five Eyes (FVEY) intelligence network.¹⁶³ Although Australia was initially considered a junior member of FVEY, at least compared to the United States and the United Kingdom, its history is important to contextualize how it has evolved in recent years, particularly in relation to its structure, priorities, and intelligence activity.¹⁶⁴

1. History

ASIO was established in 1949 following serious security leaks by the Commonwealth Investigation Service—previously responsible for Australian intelligence—that left the United States and the United Kingdom wary of sharing information.¹⁶⁵ However, despite already coordinating intelligence for decades, ASIO was not publicly acknowledged until 1978.¹⁶⁶ The following legislation helped legitimize and refine the scope of ASIO:

- The First Hope Royal Commission (1974-1977) articulated principles for Australian intelligence activity, including separating ASIO’s collection and intelligence assessments from the law enforcement community.¹⁶⁷ Therefore, the commission prohibited ASIO from having executive powers, similar to MI5.

¹⁶² Department of the Prime Minister and Cabinet, *ASIO Corporate Plan 2022-26* (Canberra: Department of the Prime Minister and Cabinet, 2022), 12, https://www.transparency.gov.au/sites/default/files/reports/2022-23_australian_security_intelligence_organisation_corporate_plan.pdf.

¹⁶³ FVEY is an intelligence network and alliance between the United States, United Kingdom, Canada, New Zealand, and Australia. Andrew O’Neil, “Australia and the ‘Five Eyes’ Intelligence Network: The Perils of an Asymmetric Alliance,” *Australian Journal of International Affairs* 71, no. 5 (2017): 530, <https://doi.org/10.1080/10357718.2017.1342763>.

¹⁶⁴ O’Neil, 536.

¹⁶⁵ “National Intelligence Community History,” Office of National Intelligence, accessed June 8, 2023, <https://www.oni.gov.au/national-intelligence-community/about-the-NIC/history>.

¹⁶⁶ Office of National Intelligence.

¹⁶⁷ Office of National Intelligence.

- The Second Hope Royal Commission (1984) resulted in stronger measures to enhance transparency and accountability among Australian intelligence agencies.¹⁶⁸ The second commission ensured that the recommendations of the First Hope Royal Commission had been implemented while also establishing oversight committees.
- The Australian Security Intelligence Organisation Act 1979 (ASIO Act) outlines the purpose and scope of ASIO activity.¹⁶⁹ It stipulates that ASIO is accountable for the protection of Australia and its inhabitants from various security threats, including “espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia’s defense system, acts of foreign interference, and the protection of Australia’s territorial and border integrity from serious threats.”¹⁷⁰

Indeed, the Royal Hope Commissions were foundational for ASIO to emerge as an intelligence organization; additionally, the ASIO Act provides the necessary statutory footing for ASIO to conduct intelligence activity.

2. Structure

In 2017, an independent intelligence review resulted in the restructuring of Australian intelligence agencies. Specifically, the 2017 Independent Intelligence Review (IIR) focused “on how key aspects of Australia’s security environment, and nature of security threats, has changed, and whether the Australian Intelligence Community was appropriately structured and resourced to serve Australia’s national interests.”¹⁷¹ The IIR’s

¹⁶⁸ Office of National Intelligence.

¹⁶⁹ “About ASIO,” Australian Security Intelligence Organisation, accessed June 8, 2023, <https://www.asio.gov.au/about>.

¹⁷⁰ Australian Government, “Australian Security Intelligence Organisation Annual Report 2020-21: Overview of ASIO,” February 18, 2022, <https://www.transparency.gov.au/annual-reports/australian-security-intelligence-organisation/reporting-year/2020-21-20>.

¹⁷¹ Parliament of Australia, “Advisory Report on the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020: Timeline of Reviews,” February 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IntegrityMeasuresBill/Report/section?id=committees%2Freportjnt%2F024737%2F78649.

major recommendation was to create the Office of National Intelligence (ONI) to enhance coordination and strategy integration specific to individual agency capabilities.¹⁷² The ONI was created to lead the development and implementation of intelligence priorities, evaluate the performance of the agencies, and implement workforce planning to enhance data sharing and collaborative analysis.¹⁷³ The IIR was not specific to ASIO; however, the broad scope of the review—focusing on creating a collaborative network—impacted how ASIO shares information and communicates with other agencies.

3. Priorities

ASIO's intelligence priorities have shifted recently to favor countering espionage and foreign interference over terrorism. As recently as September 2021, ASIO prioritized countering terrorism over other threats; in an annual report, ASIO drafted five key priorities: counterterrorism; counterespionage and foreign interference; border security; ASIO's reform program, and; governance and accountability.¹⁷⁴ When those priorities were written, the national terrorism threat level in Australia was 'probable,' which indicated that an intention and capability to conduct a terrorist attack existed.¹⁷⁵ Since then, however, ASIO's intelligence priorities have shifted away from counterterrorism and become more focused on disrupting espionage and foreign interference. In a threat assessment delivered in February 2023, Director-General Mike Burgess describes the threat landscape as complex, challenging, and changing.¹⁷⁶ By describing the Australian security environment this way, Burgess identifies espionage and foreign interference as

¹⁷² Parliament of Australia.

¹⁷³ Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Canberra: Government of Australia, 2017), 7, <https://www.pmc.gov.au/sites/default/files/resource/download/2017-Independent-Intelligence-Review.pdf>.

¹⁷⁴ Australian Government, "Overview of ASIO."

¹⁷⁵ Australian Government, "Australian Security Intelligence Organisation Annual Report 2020-21: Terrorism in Australia," February 18, 2022, <https://www.transparency.gov.au/annual-reports/australian-security-intelligence-organisation/reporting-year/2020-21-29>.

¹⁷⁶ Mike Burgess, "Director-General's Annual Threat Assessment 2023," Australian Security Intelligence Organisation, February 21, 2023, <https://www.asio.gov.au/director-generals-annual-threat-assessment-2023>.

emerging threats surpassing traditional terrorism. According to Burgess, espionage is deliberate and damaging:

- Espionage takes away sovereign choices and options.
- Espionage steals the advantages of significant investment in research and development.
- Espionage damages the economy and literally sends businesses bankrupt.
- Espionage undermines our ability to defend ourselves militarily.
- Espionage is a reconnaissance tool to shape disinformation campaigns used in our community.
- Espionage can enable sabotage, foreign interference, and more espionage.
- Espionage is a thousand different effects that chip away at the base of our sovereignty.¹⁷⁷

Downgrading terrorism was a remarkable decision. Burgess emphasized the prioritization of espionage and foreign interference by lowering the terrorism threat level from probable to possible, marking the first time since 2014 that it had been lowered.¹⁷⁸ Indeed, Burgess' publicly addressed threat assessment was an opportunity to demonstrate ASIO's new intelligence priorities; Burgess went as far as describing the recent removal of 'nests' and 'hives' of spies and drawing an analogy to the Cold War era.¹⁷⁹ Although Burgess describes the new threat landscape as complex, challenging, and changing, he is confident about ASIO's capabilities to collect, assess, and disrupt emerging threats.¹⁸⁰ Burgess' confidence in coordinating intelligence to address the new priority suggests a shift in resources to thwart developing threats.

Counterespionage is not only a priority for the Australian Security Intelligence Organisation (ASIO) but also for national security stakeholders. The Australian Strategic Policy Institute (ASPI), a prominent think tank, plays a crucial role in providing expert and

¹⁷⁷ Burgess, "Director-General's Annual Threat Assessment 2023."

¹⁷⁸ "Australian National Security," Australian Government, accessed November 28, 2022, <https://www.nationalsecurity.gov.au/>.

¹⁷⁹ Burgess, "Director-General's Annual Threat Assessment 2023."

¹⁸⁰ Burgess.

timely advice on emerging threats to both Australian and global partners.¹⁸¹ A significant overlap in priorities exists between ASIO and ASPI regarding countering China's espionage and foreign interference activities. ASPI's reports on China's universities, particularly the China Defence Universities Tracker, highlights the potential risks associated with People's Republic of China (PRC) universities, which could be leveraged by the People's Liberation Army (PLA) for surveillance, human rights violations, or military objectives.¹⁸² The PRC's efforts to advance its military capabilities to achieve the "great rejuvenation of the Chinese nation" raises concerns for countries like Australia, which is geographically positioned as a target for espionage and foreign interference.¹⁸³ ASIO benefits from partnerships with private entities like ASPI, which provides valuable insights and research on China's defense and intelligence links. The PRC's extensive reach and influence through universities and organizations reinforce the gravity of the espionage and foreign interference threats identified by ASIO, validating their prioritization for Australia's national security.

4. Intelligence Activity

Although ASIO is transparent about the threats facing Australia and its citizens, it is less transparent about its methods to counter those threats. An annual report from the Inspector-General of Intelligence and Security (IGIS) discloses that "ASIO collects information using a variety of intelligence methods including the use of human sources, special powers authorised by the Attorney-General, authorised liaison relationships, and open sources."¹⁸⁴ Some collection strategies, as IGIS reiterates in a more recent report, are

¹⁸¹ "About Us," Australian Strategic Policy Institute, accessed July 13, 2023, <http://www.aspi.org.au/about-aspi>.

¹⁸² Alex Joske, *The China Defence Universities Tracker: Exploring the Military and Security Links of China's Universities* (Barton ACT, Australia: Australian Strategic Policy Institute, 2019), <http://www.aspi.org.au/report/china-defence-universities-tracker>.

¹⁸³ Department of Defense, *Military and Security Developments Involving the People's Republic of China: 2022* (Washington, DC: Department of Defense, 2022), <https://www.defense.gov/CMPR/>.

¹⁸⁴ Inspector-General of Intelligence and Security, *Inspector-General of Intelligence and Security Annual Report 2016–17* (Canberra: Inspector-General of Intelligence and Security), accessed August 6, 2023, <https://www.igis.gov.au/sites/default/files/minisite/static/0ba68540-aa4c-476e-a41b-3e5ce1a567e6/site/index.html>.

“highly sensitive and cannot be disclosed in a public report.”¹⁸⁵ ASIO’s collection methods are understandably safeguarded, especially considering that ASIO strives to assure its allies that it can keep secrets.¹⁸⁶ Therefore, an important aspect of Australian statecraft is protecting *how* ASIO conducts intelligence.¹⁸⁷ Still, ambiguity about how ASIO coordinates intelligence is constant.

Although ASIO does not publicize how it conducts intelligence activity, its key activities can be inferred through public addresses. In 2020, Director-General Burgess delivered his first annual threat assessment.¹⁸⁸ In that address, Burgess said that the relentless advances in technology impact ASIO’s ability to monitor threats and protect Australians; he elaborated that “encrypted communications impact intelligence coverage in nine out of [ten] priority counterterrorism cases.”¹⁸⁹ Therefore, one can surmise that communications intelligence is integral for ASIO to identify threats. In 2023, Burgess stated that ASIO assesses open-source materials and information gathered through investigative and operational activity; that information is evaluated through robust structured analytical techniques to contest assumptions.¹⁹⁰ Although ASIO does not publish its intelligence methods, Burgess provides some insight into its collection efforts and the importance of structured analysis.

Although ASIO and MI5 have similar responsibilities in their respective countries, they approach intelligence differently; notably, MI5 sees foreign terrorism as the United Kingdom’s greatest threat, whereas ASIO identifies espionage and foreign interference as priorities. The last agency that will be evaluated is Germany’s Federal Office for the

¹⁸⁵ Australian Government, “Analysis,” Office of the Inspector-General of Intelligence and Security Annual Report 2019-20 (Transparency Portal, October 21, 2020), <https://www.transparency.gov.au/annual-reports/office-inspector-general-intelligence-and-security/reporting-year/2019-20-20>.

¹⁸⁶ Burgess, “Director-General’s Annual Threat Assessment 2023.”

¹⁸⁷ Chris Taylor, “The Role of Intelligence in Australian Statecraft,” *The Strategist*, April 21, 2023, <https://www.aspistrategist.org.au/the-role-of-intelligence-in-australian-statecraft/>.

¹⁸⁸ Mike Burgess, “ASIO Director-General’s Annual Threat Assessment,” *The Strategist*, February 24, 2020, <https://www.aspistrategist.org.au/asio-director-generals-annual-threat-assessment/>.

¹⁸⁹ Burgess.

¹⁹⁰ Burgess, “Director-General’s Annual Threat Assessment 2023.”

Protection of the Constitution, which also serves to conduct domestic intelligence and prioritizes a different kind of threat compared to MI5 and ASIO.

C. FEDERAL OFFICE FOR THE PROTECTION OF THE CONSTITUTION

Like MI5 and ASIO, Germany's Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz or BfV) is responsible for domestic intelligence activity. Its mission is concise: Protecting the free democratic basic order.¹⁹¹ The following examination of its history, structure, priorities, and intelligence activity is important to understand how the BfV operates; however, limitations exist when considering best practices to adopt.

1. History

The formation of the BfV is a unique part of world history; it formed in the wake of World War II and was tasked “to collect and disseminate information about subversive activities directed against the Federal Government.”¹⁹² Specifically, the BfV was responsible for protecting Germany's newly drafted Constitution. Western Allies were integral in shaping the authoritative scope of the BfV; Allies prohibited the BfV from possessing police powers.¹⁹³ Germany's intelligence network was purposefully established to prevent another monolithic agency from emerging like the Nazi Gestapo.¹⁹⁴ A major focus for the BfV from the very beginning was the prevention of a coup d'état by left- or right-wing extremists.¹⁹⁵ Therefore, the German-English translation “Federal Office for the Protection of the Constitution” is quite literal.

¹⁹¹ “The German Domestic Intelligence Services,” Bundesamt für Verfassungsschutz, accessed November 2, 2021, https://www.verfassungsschutz.de/EN/home/home_node.html.

¹⁹² “Our History,” Bundesamt für Verfassungsschutz, accessed February 11, 2021, http://www.verfassungsschutz.de/EN/about-us/bundesamt-fuer-verfassungsschutz/our-history/history_node.html.

¹⁹³ Bundesamt für Verfassungsschutz.

¹⁹⁴ Marilyn Gerlach, “Insight - How German History Helps Modern Spies,” Reuters, March 13, 2012, <https://www.reuters.com/article/uk-germany-espionage-idUKBRE82C0CZ20120313>.

¹⁹⁵ Bundesamt für Verfassungsschutz, “Our History.”

The BfV's authorities are rooted in Germany's Constitution. Originally adopted in 1949, The Basic Law for the Federal Republic of Germany was intended to be a provisional framework for the basic organization of Germany following World War II; however, the document contained the necessary features of a constitution.¹⁹⁶ The Basic Law specifies that a central office exists "for the compilation of data for purposes of protection of the constitution and of protection against activities within the federal territory which...endanger the external interests of the Federal Republic of Germany."¹⁹⁷ The BfV was subsequently created in 1950 by the "Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution."¹⁹⁸ The Act served as the basis for the BfV to oversee the intelligence activity of Germany's federal states. A couple of years later, bans on the Socialist Reich Party and the Communist Party of Germany laid the groundwork for the BfV to protect the free democratic basic order of Germany.¹⁹⁹

2. Structure

The BfV distinctly oversees the domestic intelligence services of each of the sixteen federal states. The domestic intelligence services of the federal states are responsible for the collection and analysis of extremist activity within their respective states; they are not subject to the instructions of the BfV.²⁰⁰ Instead, the BfV serves as a central body for domestic intelligence; the BfV supports the domestic intelligence services of each state and collects and analyzes information that spans several states and otherwise implicates the country as a whole.²⁰¹ The effectiveness of German intelligence, especially the BfV, hinges on cooperation and respect. The BfV acknowledges that domestic intelligence

¹⁹⁶ "Constitution of the Federal Republic of Germany," Federal Ministry of the Interior and Community, accessed November 8, 2022, <https://www.bmi.bund.de/EN/topics/constitution/constitutional-issues/constitutional-issues.html>.

¹⁹⁷ Basic Law for the Federal Republic of Germany [Constitution], Art. 87, § 1, https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html.

¹⁹⁸ Bundesamt für Verfassungsschutz, "Our History."

¹⁹⁹ Bundesamt für Verfassungsschutz.

²⁰⁰ Bundesamt für Verfassungsschutz, "The German Domestic Intelligence Services."

²⁰¹ Bundesamt für Verfassungsschutz.

services have their own expertise and access to resources; however, the BfV can help connect with partnering services and foreign partners for additional context and support. The BfV describes its framework for cooperation as federal task sharing; according to the BfV, “domestic intelligence cooperation between the Federation and the sixteen federal states can only be successful in an efficiently organised community in which there is a mutual exchange of all relevant information.”²⁰² Although analytical tools play a major role in ensuring that information and intelligence are shared appropriately across domestic intelligence services, the BfV credits its organizational structure with ensuring the harmonization of intelligence activity.²⁰³ Therefore, relationships are essential for the BfV to coordinate intelligence with the other sixteen domestic intelligence services to protect Germany’s Constitution and its free democratic order.

3. Priorities

Several domestic and international events have shaped the BfV’s intelligence priorities. The Cold War was accompanied by threats of espionage, left-wing extremism, and militant foreigners; as a result, the BfV expanded its area of responsibility to include “extremism by foreigners.”²⁰⁴ Clearly, the BfV evolved beyond its original purpose to prevent coups and subversive activity directed against democracy. The BfV, like most intelligence agencies globally, was further shaped by the terrorist attacks against the United States on September 11, 2001. The 9/11 attacks served as a wake-up call for the BfV and the overall German intelligence enterprise considering three of the hijackers plotted their attack while living in Hamburg. Although German citizens had not yet been directly targeted by Islamic terrorists, Germany responded with a strategy to join the global war on terror.²⁰⁵ Before 9/11, the BfV was primarily focused on domestic threats and paid little attention to foreign threats, despite suffering attacks from Palestinian terrorists in the

²⁰² Bundesamt für Verfassungsschutz, “The German Domestic Intelligence Services.”

²⁰³ Bundesamt für Verfassungsschutz.

²⁰⁴ Bundesamt für Verfassungsschutz, “Our History.”

²⁰⁵ Francis T. Miko and Christian Froehlich, *Germany’s Role in Fighting Terrorism: Implications for U.S. Policy*, CRS Report No. RL32710 (Washington, DC: Congressional Research Service, 2004), 5, <https://fas.org/irp/crs/RL32710.pdf>.

1970s.²⁰⁶ Indeed, the BfV evolved as Germany's threat landscape has diversified; however, the Islamic threat in Germany is waning.

Compared to the Islamic threats that the BfV identified in 2020, the most prevalent threat to Germany's security is far-right extremism. In 2020, the BfV identified 32,000 far-right extremists in Germany and considered 13,000 to be violent or capable of an attack.²⁰⁷ In the same year, the BfV identified 28,290 individuals associated with Islamism—a political ideology—and considered 679 to be violent or capable of an attack.²⁰⁸ In 2018, far-right extremists were responsible for 1,212 attacks; in 2020, followers of Islamism were responsible for 409 attacks.²⁰⁹ Since 1990, far-right extremists have been responsible for 83 murders in Germany; in comparison, Islamic terrorism has resulted in 17 deaths, 12 of which occurred during a single attack in 2016.²¹⁰

The BfV releases an annual report to apprise German citizens of key events from the previous year; although the reports provide transparency, they also serve to put threat groups on notice. The annual Report on the Protection of the Constitution can be seen as a deterrent for individuals considering membership in a group identified as a threat to Germany's constitution and democracy.²¹¹ In each report, the BfV identifies “facts and trends” related to various categories of threats, ranging from politically motivated crime and right-wing extremism to Islamist terrorism and Scientology. For Marcel Schmeer, however, the reports require explanation and legitimation.²¹² Although some transparency

²⁰⁶ Miko and Froehlich, 4; Bundesamt für Verfassungsschutz, “Our History.”

²⁰⁷ “Germany: Extremism and Terrorism,” Counter Extremism Project, accessed August 4, 2023, <https://www.counterextremism.com/countries/germany-extremism-and-terrorism>.

²⁰⁸ Counter Extremism Project.

²⁰⁹ Counter Extremism Project.

²¹⁰ Bojan Pancevski, “On Edge from Attacks, Germany Finds Far-Right Radicals within Security Services,” *Wall Street Journal*, October 11, 2019, <https://www.wsj.com/articles/on-edge-from-attacks-germany-finds-far-right-radicals-within-security-services-11570786206????> Germany counter extremism; Counter Extremism Project, “Germany.”

²¹¹ Marcel Schmeer, “Intelligence for the Masses: The Annual Reports on the Protection of the Constitution in West Germany between Cold War Propaganda and Government Public Relations,” in *Intelligence Agencies, Technology and Knowledge Production: Data Processing and Information Transfer in Secret Services during the Cold War*, ed. Rüdiger Bergien, Debora Gerstenberger, and Constantin Goshler (New York: Routledge, 2022), 249.

²¹² Schmeer, 249.

is necessary, it appears that the BfV goes above and beyond what is expected of an intelligence agency. The annual release of reports about everyday activities borders on arbitrary censorship of opinions.²¹³ Nevertheless, each Report on the Protection of the Constitution provides context to the multitude of threats that the BfV identifies as security risks to Germany's democratic order.

In its latest report, the BfV highlights politically motivated crime and right-wing extremism/terrorism as the top two threats. According to the BfV, a total of 58,916 politically motivated crimes were registered in 2022.²¹⁴ Right-wing followership rose to 38,800 with 14,000 individuals classified as violence-oriented; furthermore, right-wing extremist violent offenses rose almost 4 percent from the previous year.²¹⁵ The report labels entire political parties as right-wing extremists and includes fringe groups with right-wing extremist flavor, such as the Reichsbürger movement.²¹⁶ Although some are skeptical of labeling the Reichsbürger as a “movement” due to their lack of structure, unifying narratives, and conventional leadership, the BfV clearly warns of the potential violence similar groups can pose to democracy.²¹⁷ In December 2022, twenty-five individuals affiliated with Reichsbürger were arrested for allegedly creating a terrorist organization and aiming to overthrow the government.²¹⁸ Indeed, the annual reports published by BfV can provide the necessary context to understand Germany's greatest threats to its democracy.

²¹³ Schmeer, “Intelligence for the Masses,” 250.

²¹⁴ Federal Ministry of the Interior and Community, *Brief Summary 2022 Report on the Protection of the Constitution: Facts and Trends* (Berlin: Federal Ministry of the Interior and Community, 2023), http://www.verfassungsschutz.de/DE/home/hidden_node.html.

²¹⁵ Federal Ministry of the Interior and Community.

²¹⁶ Federal Ministry of the Interior and Community.

²¹⁷ Alexander Ritzmann, “The December 2022 German Reichsbürger Plot to Overthrow the German Government,” *CTC Sentinel* 16, no. 3 (March 2023): 19, <https://ctc.westpoint.edu/the-december-2022-german-reichsbuerger-plot-to-overthrow-the-german-government/>; Federal Ministry of the Interior and Community, *Brief Summary 2022 Report on the Protection of the Constitution: Facts and Trends*.

²¹⁸ Ritzmann, “The December 2022 German Reichsbürger Plot,” 15.

4. Intelligence Activity

Like most intelligence agencies, the BfV leverages various methods to coordinate intelligence and assess risk associated with individuals and groups potentially posing a threat to national security. The BfV uses surveillance and confidential sources to collect intelligence; it also intercepts communications and monitors internet activity.²¹⁹ The BfV “systematically and continuously monitor [s] and analyze [s] relevant websites frequented by terrorists and militant extremists.”²²⁰ Furthermore, social media is a key resource for the BfV to gather information covertly.²²¹ Besides clandestine methods, the BfV regards open-source methods as a major component of effective intelligence; the BfV analyzes news articles, and websites, attends public events, and requests participation in voluntary interviews.²²² Therefore, the BfV does not consider covert or clandestine collection methods as requisites to gather valuable information.

On its website, the BfV is careful not to overlook the importance of analysis. According to the BfV, “Analysis is a distinct area of the German domestic intelligence services’ work, but it is of course not carried out in isolation from information gathering. Instead, the respective units work in close cooperation to fulfill the services’ statutory mission.”²²³ Essentially, the BfV contends that effective intelligence hinges on analytically driven collection; information-gathering units collect the information needed to evaluate existing intelligence more effectively.²²⁴ Additionally, the BfV leverages access to information stored in the Intelligence Information System and Knowledge Network (NADIS WN) which is used—in part—to detect important links between disparate pieces of information; leveraging technology allows the BfV to connect dots that

²¹⁹ “Information Gathering,” Bundesamt für Verfassungsschutz, accessed November 2, 2021, http://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/information-gathering/information-gathering_node.html.

²²⁰ Bundesamt für Verfassungsschutz.

²²¹ Bundesamt für Verfassungsschutz.

²²² Bundesamt für Verfassungsschutz.

²²³ Bundesamt für Verfassungsschutz.

²²⁴ Bundesamt für Verfassungsschutz.

would otherwise remain hidden.²²⁵ Therefore, the BfV finds analysis to be a major component in its approach to conducting and coordinating intelligence; furthermore, the NADIS WN serves as a tool to disseminate intelligence to the sixteen domestic agencies it oversees.

D. CONCLUSION

In conclusion, this chapter provides a historical overview of the structures, priorities, and intelligence activity of MI5, ASIO, and the BfV. Although similarities can be found between each agency, nuances exist that can serve OFO as it seeks to integrate intelligence to improve border security. The following key elements were identified through this chapter's case study analysis: threat prioritization, structural approach, and transparency.

1. Threat Prioritization

Each of the surveyed intelligence agencies has different threat priorities. MI5 focuses on preventing and disrupting terrorism. In contrast, ASIO recently lowered its terrorism threat level from probable to possible. The lowered threat level allows ASIO to focus its efforts on counterespionage and disrupting foreign interference. ASIO benefits from private stakeholders like ASPI who also see espionage as an emerging threat that warrants immediate attention. By restructuring priorities, ASIO can effectively distribute resources to address emerging threats to Australia. Although the BfV has increased its counterterrorism efforts since 9/11, traditional threats of terrorism still take a back seat to right-wing extremism. The BfV has a unique responsibility to protect Germany's Constitution and democratic free order, dating back to its establishment post-World War II. Therefore, the BfV prioritizes right-wing extremism to assure global partners that Germany will not suffer democratic backsliding. As each intelligence agency prioritizes threats differently, resources are allocated more effectively to address respective priorities. Like transparency, structuring threat priorities allows intelligence agencies to justify their activity.

²²⁵ Bundesamt für Verfassungsschutz, "Information Gathering."

2. Structural Approach

Although ASIO is cautious to broadcast its intelligence methodology, MI5 and the BfV provide useful frameworks to structure intelligence. The BfV oversees the domestic intelligence activity of Germany's sixteen federal states. Its federal task-sharing concept relies on significant cooperation and collaboration to share intelligence timely and effectively. Although the BfV does not dictate the domestic intelligence methods of each federal state, it serves as a central body for intelligence in Germany. Therefore, the BfV serves to complement and support the intelligence capabilities of the other sixteen agencies that are tasked with domestic intelligence activity.

MI5 coordinates intelligence through a Desk Officer. In that system, a Desk Officer coordinates all intelligence activity: gathering requirements; collecting information; exploiting and analyzing data; producing actionable intelligence; and disseminating intelligence to decision-makers. The Desk Officer System provides agility to coordinate collection efforts based on existing information; because Desk Officers act as both analysts and investigators, they are aware of intelligence gaps requiring proportionate collection techniques. Intimate knowledge of the target also allows the Desk Officer to arrange targeted collection efforts, so as not to collect information unnecessarily. Lastly, the Desk Officer System prevents the relevant information from being lost in translation or misinterpreted by decision-makers; such ownership of intelligence increases the chance that consumers will be receptive during the dissemination phase.

3. Transparency

By juxtaposing the transparency practices of MI5 and ASIO, it becomes evident that while MI5 openly discloses its collection methods, ASIO maintains a more secretive stance. MI5 seeks to diminish secrecy to a necessary minimum; although such efforts are primarily meant to enhance collaboration and cooperation across intelligence and law enforcement partners, MI5 discloses many of its collection efforts on its website for public awareness. Transparency has allowed MI5 to normalize intelligence activity, especially while contextualizing the threat of terrorism to British citizens. ASIO, however, appears more cautious about how transparent it is, seemingly to protect its information-sharing

relationships with global partners. The BfV is ultra-transparent about the threats Germany faces; in fact, the BfV goes to great lengths to ensure it is not perceived by German citizens as a secret agency. In annual reports about how the BfV protects the Constitution, the BfV identifies key security events and groups that threaten Germany's democracy. The reports are opportunities for the BfV to dissuade individuals from various group memberships. Furthermore, each Report on the Protection of the Constitution is an opportunity to contextualize the danger of right-wing extremism in Germany. Transparency allows each agency to justify its intelligence activity, which is important to foster partnerships and coalitions to address imminent threats.

The manners in which MI5, ASIO, and the BfV prioritize threats, structure intelligence, and pursue transparency may serve as pathways for OFO to embrace its capabilities to integrate intelligence into frontline operations. Although CBP policies and procedures may prevent OFO from replicating the practices of established intelligence agencies, a modified approach to some of their best practices may be an option. The next chapter focuses on developing recommendations and implementation plans considering OFO's capabilities, limitations, and best practices of the various intelligence agencies identified in this chapter.

IV. FINAL ANALYSIS

This chapter serves to present the key findings from previous chapters and identifies a path for CBP to integrate intelligence into frontline operations. This chapter will provide OFO leadership with best practices to consider based on comparative research involving three intelligence agencies with unique histories, structures, and priorities that shape their domestic intelligence footprint. Such consideration will position OFO to integrate intelligence and play to the edge of its capabilities more effectively. At the conclusion of this chapter, future research opportunities will provide avenues to explore additional best practices for OFO to become a key player within the intelligence enterprise.

A. KEY FINDINGS

The second chapter surveyed OFO's capabilities, specifically in relation to collection, analysis, and dissemination. The chapter identified three major limitations to integrating intelligence: disparate responsibilities and competing priorities, insufficient intelligence structures, and an absence of transparency. The third chapter examined three experienced foreign intelligence agencies tasked with domestic intelligence activity; each agency's history, structure, and priorities provided context to how they coordinate intelligence. By studying how seasoned intelligence agencies operate, OFO may discover ways to overcome its limitations to intelligence integration.

1. OFO Capabilities and Limitations

OFO is capable of contributing to CBP's strategic intelligence goals and empowering personnel in various roles. Specifically at international airports, OFO can anticipate threats before they arrive and depart the United States. By leveraging its border search authority and advanced passenger and cargo systems, CBP officers can produce meaningful intelligence for tactical and strategic consumers. However, OFO is limited by several factors that prevent it from capitalizing on its ability to coordinate intelligence effectively.

Due to the size of OFO and the scope of its mission, many ports of entry deploy specialized teams to focus on specific mission areas. Although officers on specialized teams often develop the necessary skills and expertise for their areas of responsibility, the disparate nature of enforcement and analysis detracts from intelligence integration. OFO must implement structured frameworks to coordinate intelligence. Although CBP desires to integrate intelligence, disparate specialized knowledge, competing priorities, and insufficient intelligence structures prevent OFO from expanding its capabilities. Internal and external awareness of OFO operations also limits intelligence integration. Internally, awareness improves how officers and information-sharing partners understand their respective roles, responsibilities, and capabilities. External awareness improves how lawmakers and the public understand OFO's role in border security.

2. MI5, ASIO, and the BfV

The domestic intelligence agencies of the United Kingdom, Australia, and Germany, namely MI5, ASIO, and BfV, were chosen for examination due to their alignment with OFO's homeland security mission. Although CBP does not seek to emulate traditional intelligence activity, the experiences of these established agencies hold value. Therefore, a study of MI5, ASIO, and BfV was conducted to understand how their history, structure, and priorities shape intelligence activities. Through case studies, best practices emerged in threat prioritization, structural approach, and transparency.

MI5 focuses on countering terrorist threats through the CONTEST strategy, which encompasses prevention, pursuit, protection, and preparation. ASIO has recently shifted its priorities from terrorism to espionage and foreign interference, aided by external resources like ASPI. The BfV, after participating in the global war on terror, refocused its sights on safeguarding Germany's democratic order and identifies right-wing extremism as the major threat. These distinct priorities showcase agency evolution in response to evolving threats. Coordination methods also differ; MI5 employs Desk Officers to centralize intelligence processes, while the BfV acts as the hub for German domestic intelligence and supports various state-level services. Additionally, transparency varies among agencies, with MI5 emphasizing reduced secrecy over time, the BfV prioritizing transparency to

dissuade group membership, and ASIO striking a balance due to security concerns. Although the three agencies prioritize threats, coordinate intelligence, and value transparency differently, these findings establish the basis for recommendations.

B. RECOMMENDATIONS

Considering that CBP seeks to integrate intelligence by extending capabilities to the field, the overarching recommendation of this thesis is to establish intelligence units at ports of entry. Like TTRT, A-TCET, PERT, PCS, PAU, and ATU, ports of entry can standardize intelligence units across the country to cultivate decision advantage. Port intelligence units will facilitate a needed shift toward analytically driven collection and bridge the gap created by disparate responsibilities and competing priorities. Although CBP's Intelligence Research Specialists provide analytical support, port intelligence units will streamline intelligence at ports of entry. However, merely establishing port intelligence units does not achieve intelligence integration; structure is required.

This section is divided into two main recommendations to structure port intelligence at designated ports of entry. Each recommendation serves as a framework for OFO to structure port intelligence and is based on the research presented in this thesis. Importantly, either recommendation can be implemented with existing personnel; however, positions at ports of entry must be allocated from other work units to create port intelligence units. Lastly, leadership roles are essential to foster collaboration, drive permanent change, and ensure that port intelligence activity is structured and compliant with existing CBP policies.²²⁶

1. Desk Officer System

The first framework for OFO to consider is the desk officer system. The proposed desk officer system is an adaptation of the MI5 intelligence structure and puts the CBP officer at the center of the intelligence cycle. In this system, CBP officers assigned to port intelligence units are responsible for satisfying local and national intelligence needs; specifically, they are tasked with planning and direction, collection, exploitation, analysis,

²²⁶ Lambert, "Addressing Challenges to Homeland Security," 1263-64.

and dissemination of tactical and strategic intelligence. The desk officer system amalgamates disparate responsibilities and competing priorities while prioritizing the coordination of intelligence to thwart criminal networks. Considering that smuggling methods and their indicators are similar for narcotics and terrorism, collecting data to thwart criminal networks is not mutually exclusive.²²⁷ Therefore, the desk officer system combines expertise from specialized units to collect, exploit, and analyze information to counter all threats to border security. Because one officer is responsible for all components of the intelligence cycle, the CBP officer collects in response to evolving analytic needs. Furthermore, the desk officer system improves the timely dissemination of relevant information to feed enforcement operations because the officer is working alongside the intended consumers. Ultimately, the desk officer system integrates intelligence by allowing the CBP officer to advance through each phase of the cycle efficiently and take ownership of intelligence. Figure 2 demonstrates the responsibilities of a CBP officer within the desk officer system.

²²⁷ Office of Inspector General, *Review of U.S. Customs and Border Protection's Fiscal Year 2022*, 9.

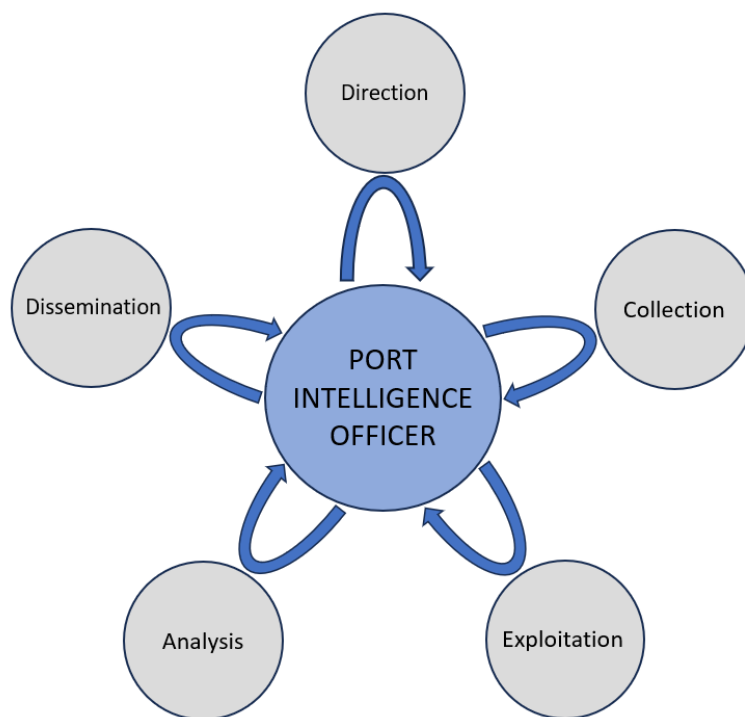


Figure 2. Desk Officer System²²⁸

a. Characteristics

Within the desk officer system, officers assigned to port intelligence units are directed by CBP Priority Intelligence Requirements and local management's intelligence needs. Such requirements dictate initial collection efforts, followed by relevant exploitation and analysis. The officer can subsequently collect additional information based on preliminary exploitation and analysis and develop finished intelligence products for dissemination to decision-makers. Although AFI is a designated platform to publish finished intelligence products, port intelligence units streamline the dissemination and consumption of intelligence with regular briefings to port personnel. In this system, the mission focus of teams like TTRT, A-TCET, PERT, and PCS blend to coordinate strategic intelligence to dismantle criminal networks. The desk officer system does not replace the need for specialized teams to interdict contraband; instead, it focuses on deploying intelligence officers to connect the dots through various intelligence disciplines to give

²²⁸ Adapted from Smith, "Counterterrorism in the United Kingdom."

CBP a strategic advantage. Key characteristics of a port intelligence unit in the desk officer system include:

- A group of CBP officers who collect, exploit, analyze, and disseminate information and intelligence in response to Priority Intelligence Requirements and local policymaker needs.
- The coordination of intelligence to disrupt and dismantle threat networks through strategic collaboration and partnership with port personnel, law enforcement partners, and intelligence professionals.
- Effective communication of evolving border security threats to frontline personnel and policymakers through established sharing platforms and regular in-person briefings.

b. Implementation

Considering the scope and complexity of CBP's mission, adapting an intelligence unit under the desk officer system would be substantial. To appropriately staff a port intelligence unit, port leadership must evaluate local tactical and strategic intelligence needs, and assess how many CBP officers are needed to collect, exploit, analyze, and disseminate intelligence to fill those gaps. The intelligence needs of a large port of entry, like Chicago O'Hare International Airport, may be more complex than smaller ports of entry. Therefore, the staffing of port intelligence units may vary across the United States. However, senior port management should consider the size of a port intelligence unit based on short-term and long-term intelligence needs.

2. Task-Sharing System

The other framework for OFO to consider—as opposed to the desk officer system—is the task-sharing system. The proposed task-sharing system is an adaptation of the BfV intelligence structure. Similar to how the BfV supports the intelligence network of several states within Germany, port intelligence units will support the intelligence needs of specialized teams within OFO. In the task-sharing system, port intelligence units feature a

central intelligence body with intelligence officers embedded in various specialized work units. In this system, port intelligence units deploy intelligence officers to specialized teams like TTRT, PERT, A-TCET, PCS, PAU, and ATU. The intelligence officer designated to support each team provides officers with information and intelligence to cultivate decision advantage and foster analytically driven collection. The central intelligence body is responsible for building and sustaining strategic intelligence partnerships and facilitating the mutual exchange of information and resources between intelligence officers. Unlike the BfV—which does not direct the activity of the 16 domestic intelligence services in Germany—the central intelligence body at a port of entry has operational control over the intelligence officers assigned to specialized teams. Figure 3 demonstrates the responsibilities of a CBP officer within the task-sharing system.

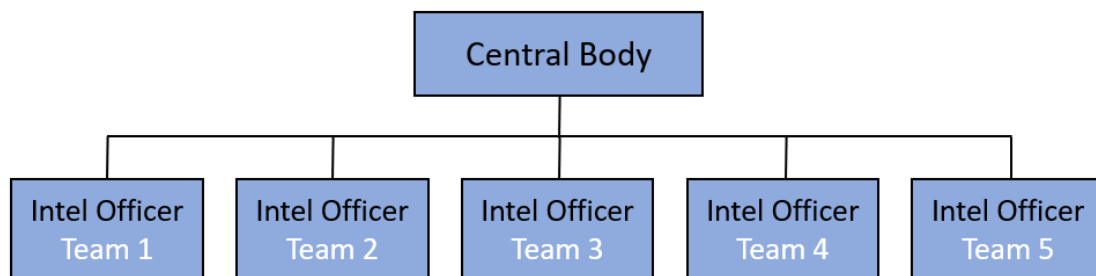


Figure 3. Task-Sharing System

a. Characteristics

Within the task-sharing system, officers assigned to specialized teams operate as collectors.²²⁹ Intelligence officers exploit and analyze the information that is collected by specialized teams. Based on open-source and classified information, intelligence officers feed relevant information to their assigned specialized teams to fuel enforcement activity. Additionally, intelligence officers conduct pre- and post-encounter analyses of arriving or departing targets. The overarching central body communicates threat information to policymakers and intelligence partners, particularly when a threat or trend expands beyond

²²⁹ In the Desk Officer System, strategic collection is the responsibility of the intelligence officer.

the scope of a single port of entry. Through the task-sharing system, intelligence and interdiction coalesce to improve team, port, and agency outcomes by facilitating data-driven decisions. Key characteristics of a port intelligence unit in the task-sharing system include:

- A central intelligence body comprised of CBP officers and supervisory personnel, which
 - Oversees the activity of intelligence officers embedded in various specialized teams at a port of entry.
 - Fosters strategic information- and intelligence-sharing partnerships to cultivate decision advantage.
 - Communicates information and intelligence that impacts the decision-making process of more than one specialized team.
 - Provides resources and operational support for intelligence officers assigned to specialized teams, while ensuring the harmonization of port intelligence activity through cooperation and collaboration.
- Port intelligence officers who are embedded in specialized teams at ports of entry, and who are primarily responsible for
 - Providing specialized team members with local and national intelligence requirements to guide their collection efforts.
 - Exploiting, analyzing, and disseminating information and intelligence based on team members' collection efforts.
 - Providing team members with relevant and actionable intelligence to enhance analytically driven collection.

b. Implementation

Implementing an intelligence unit with task-sharing characteristics would be less complicated than adopting the desk officer system. Since port intelligence units are not responsible for the collection component, the staffing requirements are reduced; however, port management must still consider tactical and strategic intelligence needs. The exploitation, analysis, and dissemination of intelligence by the central body and embedded port intelligence officers will enable the collection methods of specialized teams. Therefore, port management may consider the tasks of a port intelligence unit to be more manageable in the task-sharing system than in the desk officer system. In either system, however, advanced training is critical to ensure that port intelligence is effective.

C. FINAL THOUGHTS AND FUTURE RESEARCH

Establishing intelligence units staffed with CBP officers at ports of entry is a solution to some of the limitations previously identified. However, the main recommendations transcend establishing a new work unit and focus on structuring port intelligence for consistency and effective integration. Structuring port intelligence units in a desk officer or task-sharing system alleviates OFO's limitations caused by disparate responsibilities and competing priorities; furthermore, structuring intelligence refines the scope and role of a CBP officer assigned to port intelligence. Nevertheless, this thesis identified other limitations that are not mitigated by adopting either of the recommended frameworks.

CBP must consider its desired level of transparency and assess whether current training supports enhanced development in intelligence methods; however, both considerations are understandably safeguarded. The studied intelligence agencies—MI5, ASIO, BfV—have varying levels of transparency. MI5 has emphasized the importance of transparency, while ASIO prioritizes the appearance that it can keep secrets. Although transparency about how CBP integrates intelligence may be in the public's interest, it can also be damaging to national security; therefore, finding the right level of transparency is challenging. To the latter consideration, training techniques are also safeguarded.

However, CBP should evaluate current training methods to ensure that its officers and agents are qualified to embrace increased intelligence roles.

Additional research may also provide CBP with diverse options to consider. First, this research focused on just three professional intelligence agencies; expanding research to other established intelligence organizations could reveal additional useful practices. Second, although integrating intelligence intends to improve border security, CBP's homeland security mission is complex; OFO's access to valuable information may provide additional context to American intelligence agencies. If OFO considers structuring port intelligence units under a desk officer or task-sharing system, additional research may shed light on what role, if any, CBP could officially play in the United States Intelligence Community.

CBP seeks to integrate intelligence to capitalize on the information it collects to cultivate decision advantage within its frontline ranks. This thesis sought to identify how OFO can integrate intelligence to achieve that goal and improve border security by collecting, analyzing, and disseminating information in a more strategic manner. Although OFO is capable of significant contributions to the intelligence enterprise, it is limited by internal factors. Through structured analysis of established agencies tasked with domestic intelligence collection, this thesis provides recommendations for OFO to consider. Establishing and structuring intelligence units at CBP ports of entry will help OFO overcome some of its current limitations and evolve as an agency capable of contributing to the intelligence enterprise more effectively; furthermore, adopting either the desk officer or task-sharing system as an intelligence framework would encourage CBP officers to play to the edge of their capabilities and cultivate the necessary decision advantage to improve border security.

LIST OF REFERENCES

- American Council on Education. "Passenger Enforcement Rover Team." Accessed July 19, 2023. <https://www.acenet.edu/National-Guide/Pages/Course.aspx?org=U.S.+Customs+and+Border+Protection&cid=9713cf9c-271f-ec11-b6e6-000d3a34f821&oid=92099b28-9016-e811-810f-5065f38bf0e1>.
- Australian Government. "Office of the Inspector General of Intelligence and Security Annual Report 2019–20: Analysis." October 21, 2020. <https://www.transparency.gov.au/annual-reports/office-inspector-general-intelligence-and-security/reporting-year/2019-20-20>.
- . "Australian National Security." Accessed November 28, 2022. <https://www.nationalsecurity.gov.au/>.
- . "Australian Security Intelligence Organisation Annual Report 2020–2: Overview of ASIO," February 18, 2022. <https://www.transparency.gov.au/annual-reports/australian-security-intelligence-organisation/reporting-year/2020-21-143>.
- . "Australian Security Intelligence Organisation Annual Report 2020–21, February 18, 2022: Terrorism in Australia." <https://www.transparency.gov.au/annual-reports/australian-security-intelligence-organisation/reporting-year/2020-21-29>.
- Australian Security Intelligence Organisation. "About ASIO." Accessed June 8, 2023. <https://www.asio.gov.au/about>.
- . "Australian Security Intelligence Organisation Annual Report 2020–21, February 18, 2022: Transparency." <https://www.transparency.gov.au/annual-reports/australian-security-intelligence-organisation/reporting-year/2020-21-142>.
- Australian Strategic Policy Institute. "About Us." Accessed July 13, 2023. <http://www.aspi.org.au/about-aspi>.
- Barnett, Thomas P.M. "Capability Gaps Threatening CBP's Present and Future Operations." *Homeland Security Affairs* 15 (September 2019): 1–14. <https://www.hsaj.org/articles/15389>.
- Beckner, Christian. "Reassessing Homeland Security Intelligence: A Review of the DHS Office of Intelligence and Analysis." Center for a New American Security, May 25, 2021. <https://www.cnas.org/publications/reports/reassessing-homeland-security-intelligence>.

- “Behind the Enigma: The Authorized History of GCHQ, Britain’s Secret Cyber-Intelligence Agency.” *Journal of Military and Strategic Studies* 20, no. 3 (2021): 1–12. <https://jmss.org/article/view/72868>.
- Best Jr., Richard A. *Securing America’s Borders: The Role of the Intelligence Community*. CRS Report No. R41520. Washington, DC: Congressional Research Service, 2010. <https://sgp.fas.org/crs/intel/R41520.pdf>.
- Bickford, David. “The Accountability of the Security and Intelligence Agencies with Particular Regard to the Security Service.” Parliament Select Committee on Home Affairs, June 21, 1999. <https://publications.parliament.uk/pa/cm199899/cmselect/cmhaff/291/291ap03.htm>.
- Bundesamt für Verfassungsschutz. “Information Gathering.” Accessed November 2, 2021. http://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/information-gathering/information-gathering_node.html.
- . “Our History.” Accessed February 11, 2021. http://www.verfassungsschutz.de/EN/about-us/bundesamt-fuer-verfassungsschutz/our-history/history_node.html.
- . “The German Domestic Intelligence Services.” Accessed November 2, 2021. https://www.verfassungsschutz.de/EN/home/home_node.html.
- Burgess, Mike. “ASIO Director-General’s Annual Threat Assessment.” *The Strategist*, February 24, 2020. <https://www.aspistrategist.org.au/asio-director-generals-annual-threat-assessment/>.
- . “Director-General’s Annual Threat Assessment 2023.” Australian Security Intelligence Organisation, February 21, 2023. <https://www.asio.gov.au/director-generals-annual-threat-assessment-2023>.
- Carter, Jeremy G., David L. Carter, Steve Chermak, and Edmund McGarrell. “Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment While Safeguarding Privacy.” *Journal of Police and Criminal Psychology* 32, no. 1 (March 2017): 11–27. <https://doi.org/10.1007/s11896-016-9199-4>.
- Counter Extremism Project. “Germany: Extremism and Terrorism.” Accessed August 4, 2023. <https://www.counterextremism.com/countries/germany-extremism-and-terrorism>.
- Customs and Border Protection. *Air and Marine Operations Vision 2025*. Washington, DC: Department of Homeland Security, 2016. <https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/AMO%20Vision%202025.pdf>.
- . “APIS: Advance Passenger Information System.” July 24, 2023. <https://www.cbp.gov/travel/travel-industry-personnel/apis2>.

- . *Border Search of Electronic Devices*. CBP Directive No., 3340–049A. Washington, DC: Customs and Border Protection, 2018. <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf>.
- . “Careers: Intelligence Research Specialist.” September 28, 2022. <https://www.cbp.gov/careers/professional/0132-intelligence-research-specialist>.
- . “Careers: Office of Field Operations.” Accessed July 13, 2023. <https://www.cbp.gov/careers/oyo>.
- . “CBP Access: September 2022.” June 12, 2023. <https://www.cbp.gov/about/congressional-resources/cbp-access/september-2022>.
- . “CBP Releases Statistics on Electronic Device Searches.” April 11, 2017. <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0>.
- . *CBP Strategy 2021–2026*. Washington, DC: Customs and Border Protection, 2020. <https://www.cbp.gov/sites/default/files/assets/documents/2020-Dec/CBP-Strategy-2021-2026.pdf>.
- . “Customs-Trade Partnership against Terrorism (CTPAT) Session.” September 9, 2020. <https://www.cbp.gov/sites/default/files/assets/documents/2020-Sep/CBP%20Virtual%20Trade%20Week%20Biographies-%20CTPAT%20Session%20-%20Wed.%20Sept%209%202020.pdf>.
- . *Facial Debarkation: Sea Innovation, Mobility, Biometric Advancement*. FOIA CBP 000194. Washington, DC: Department of Homeland Security, 2020. <https://www.cbp.gov/sites/default/files/assets/documents/2022-Mar/Second%20Interim%20Response%20%2820-cv-02213-NRB%29.pdf>.
- . “Frequently Asked Questions: Privacy and Security.” Accessed August 4, 2023. <https://esta.cbp.dhs.gov/faq?lang=en>.
- . “Legal Authority for the Border Patrol.” June 29, 2023. https://help.cbp.gov/s/article/Article-1084?language=en_US.
- . “On a Typical Day in Fiscal Year 2019, CBP....” May 11, 2022. <https://www.cbp.gov/newsroom/stats/typical-day-fy2019>.
- . “On a Typical Day in Fiscal Year 2022, CBP....” July 21, 2023. <https://www.cbp.gov/newsroom/stats/typical-day-fy2022>.

- . “Statement for the Record on Assessing CBP’s Use of Facial Recognition Technology.” August 29, 2022. <https://www.cbp.gov/about/congressional-resources/testimony/statement-record-assessing-cbps-use-facial-recognition-technology>.
- . “Traveler and Conveyance Statistics.” July 18, 2023. <https://www.cbp.gov/newsroom/stats/travel>.
- . *Traveler Verification Service Standard Operating Procedure*. Washington, DC: Department of Homeland Security, 2017.
- Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.
- . “Why Won’t They Listen? Understanding Policy Maker Receptivity toward Intelligence.” Paper presented at the International Studies Association Annual Convention, Montreal, March 2011. <https://hdl.handle.net/10945/58528>.
- Davies, Philip. “Review: Step Changes and Learning Curves in the History of British Intelligence.” *Contemporary European History* 22, no. 4 (2013): 687–97. <https://www.jstor.org/stable/43299411>.
- Department of Defense. *Military and Security Developments Involving the People’s Republic of China: 2022*. Washington, DC: Department of Defense, 2022. <https://www.defense.gov/CMPR/>.
- Department of Homeland Security. “Privacy Impact Assessments.” August 18, 2022. <https://www.dhs.gov/privacy-impact-assessments>.
- . *U.S. Customs and Border Protection: Budget Overview Fiscal Year 2018 Congressional Justification*. Washington, DC: Department of Homeland Security, 2018. <https://www.dhs.gov/sites/default/files/publications/CBP%20FY18%20Budget.pdf>.
- Department of the Prime Minister and Cabinet. *2017 Independent Intelligence Review*. Canberra: Government of Australia, 2017. <https://www.pmc.gov.au/sites/default/files/resource/download/2017-Independent-Intelligence-Review.pdf>.
- . *ASIO Corporate Plan 2022–26*. Canberra: Department of the Prime Minister and Cabinet, 2022. https://www.transparency.gov.au/sites/default/files/reports/2022-23_australian_security_intelligence_organisation_corporate_plan.pdf.
- Dinkins, James. *Privacy Impact Assessment for the Exodus Accountability Referral System (EARS)*. Washington, DC: Department of Homeland Security, 2010. https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_ears.pdf.

Dodwell, Brian, and Paul Cruickshank. “A View from the CT Foxhole: An Interview with Kevin McAleenan, Commissioner of U.S. Customs and Border Protection.” *CTC Sentinel* 11, no. 8 (September 2018): 9–14. <https://ctc.westpoint.edu/view-ct-foxhole-interview-kevin-mcaleenan-commissioner-u-s-customs-border-protection/>.

Executive Director Admissibility and Passenger Programs. “Providing Inadmissible Travelers with Documentation of an Adverse Action.” Official memorandum. Washington, DC: Customs and Border Patrol, 2012. https://www.cbp.gov/sites/default/files/assets/documents/2022-May/Providing%20Inadmissible%20Travelers%20with%20Documentation%20of%20an%20Adverse%20Action_Redacted.pdf.

Federal Ministry of the Interior and Community. *Brief Summary 2022 Report on the Protection of the Constitution: Facts and Trends*. Berlin: Federal Ministry of the Interior and Community, 2023. http://www.verfassungsschutz.de/DE/home/hidden_node.html.

———. “Constitution of the Federal Republic of Germany.” Federal Ministry of the Interior and Community. Accessed November 8, 2022. <https://www.bmi.bund.de/EN/topics/constitution/constitutional-issues/constitutional-issues.html>.

Fisher, Stefanie. “The Fight against Terrorism—the Need for Local Police Units in the United States’ Intelligence Community.” *Journal of Military and Strategic Studies* 17, no. 1 (2018): 189–208. <https://jmss.org/article/view/58212>.

Fyfe, David Maxwell. “The Directive to the Director General of the Security Service.” Undercover Policing Inquiry. September 24, 1952. <https://www.ucpi.org.uk/wp-content/uploads/2023/01/UCPI0000034262.pdf>.

General Services Administration. “Land Ports of Entry and the Bipartisan Infrastructure Law.” U.S. General Services Administration. Accessed April 21, 2023. <https://www.gsa.gov/real-estate/gsa-properties/land-ports-of-entry/bipartisan-infrastructure-law-construction-projects>.

Gleason, Jim. *Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)*. DHS/CBP/PIA-010. Washington, DC: Department of Homeland Security, 2012. https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.

Gross, Gregory, Rui Ling, Brad Richardson, and Nayong Quan. “In-Person or Virtual Training?: Comparing the Effectiveness of Community-Based Training.” *American Journal of Distance Education* 37, no. 1 (2023): 66–77. <https://doi.org/10.1080/08923647.2022.2029090>.

- Habeck, Mary, and Charles D. Stimson. *Reforming Intelligence: A Proposal for Reorganizing the Intelligence Community and Improving Analysis*. Washington, DC: Heritage Foundation, 2016. <https://www.hsdl.org/c/abstract/?docid=795261>.
- Hall, Christopher E. “Has the Department of Homeland Security (DHS) Outlived Its Usefulness?” Master’s thesis, Naval Postgraduate School, 2012. <https://hdl.handle.net/10945/27839>.
- Harris, Dan. “The Consequences of Eroding Human Intelligence Collection.” The Cipher Brief, November 2, 2016. https://www.thecipherbrief.com/column_article/the-consequences-of-eroding-human-intelligence-collection.
- Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.
- Hoffman, Bruce. *Inside Terrorism*. 3rd ed. New York: Columbia University Press, 2017.
- Home Office. “Joint Intelligence Organisation.” GOV.UK. Accessed August 4, 2023. <https://www.gov.uk/government/groups/joint-intelligence-organisation>.
- . *Report on the Operation of the Investigatory Powers Act 2016*. London: Home Office, 2023. <https://www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016>.
- . “Secret Intelligence Service.” UK Government, October 13, 2015. <https://www.gov.uk/government/organisations/secret-intelligence-service>.
- Inspector-General of Intelligence and Security. *Inspector-General of Intelligence and Security Annual Report 2016–17*. Canberra: Inspector-General of Intelligence and Security. Accessed August 6, 2023. <https://www.igis.gov.au/sites/default/files/minisite/static/0ba68540-aa4c-476e-a41b-3e5ce1a567e6/site/index.html>.
- Inspectors General, Intelligence Community, Department of Homeland Security, and Department of Justice. *Review of Domestic Sharing of Counterterrorism Information*. OIG-17-49. Washington, DC: Department of Justice, 2017. <https://oig.justice.gov/sites/default/files/reports/OIG-17-49-Mar17.pdf>.
- Jacoby, Karl. “Why the CBP’s Presence at the DC Protests Should Alarm All of Us.” Politico, June 10, 2020. <https://www.politico.com/news/magazine/2020/06/10/cbp-protests-border-zone-312151>.
- Jones, Vivian C., and Audrey Singer. *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*. CRS Report No. R43014. Washington, DC: Congressional Research Service, 2015. <https://crsreports.congress.gov/product/pdf/R/R43014/14>.

- Joske, Alex. *The China Defence Universities Tracker: Exploring the Military and Security Links of China's Universities*. Barton, ACT, Australia: Australian Strategic Policy Institute, 2019. <http://www.aspi.org.au/report/china-defence-universities-tracker>.
- Lambert, David E. "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model." *Criminal Justice Policy Review* 30, no. 8 (October 2019): 1250–78. <https://doi.org/10.1177/0887403418786555>.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 9th ed. Thousand Oaks, CA: CQ Press, 2022.
- Marilyn Gerlach. "Insight – How German History Helps Modern Spies." Reuters, March 13, 2012. <https://www.reuters.com/article/uk-germany-espionage-idUKBRE82C0CZ20120313>.
- McGlynn, Patrick, and Godfrey Garner. *Intelligence Analysis Fundamentals*. Boca Raton, FL: CRC Press, 2018. <https://doi.org/10.4324/9781351249355>.
- McKenzie, Dennis. *Privacy Impact Assessment for the Air Cargo Advance Screening (ACAS)*. DHS/CBP/PIA-061. Washington, DC: Department of Homeland Security, 2019. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-acas-061-october2019.pdf>.
- Medina, Mario. *Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI)*. DHS/CBP/PIA-010(a). Washington, DC: Department of Homeland Security, 2016. <https://www.dhs.gov/sites/default/files/2022-10/privacy-pia-cbp010%28a%29-afi-october2022.pdf>.
- . *Privacy Impact Assessment Update for the Automated Targeting System*. DHS/CBP/PIA-006(e). Washington, DC: Department of Homeland Security, 2017. <https://www.dhs.gov/sites/default/files/2022-10/privacy-pia-cbp010%28a%29-afi-october2022.pdf>.
- Miko, Francis T., and Christian Froehlich. *Germany's Role in Fighting Terrorism: Implications for U.S. Policy*. CRS Report No. RL32710. Washington, DC: Congressional Research Service, 2004. <https://fas.org/irp/crs/RL32710.pdf>.
- Nemfakos, Charles, Bernard D. Rostker, Raymond E. Conley, Stephanie Young, William A. Williams, Jeffrey Engstrom, Barbara Bicksler et al. *Workforce Planning in the Intelligence Community: A Retrospective*. Santa Monica, CA: RAND Corporation, 2013. https://www.rand.org/pubs/research_reports/RR114.html.
- Northcott, Chris. "The Role, Organization, and Methods of MI5." *International Journal of Intelligence and CounterIntelligence* 20, no. 3 (2007): 453–79. <https://doi.org/10.1080/08850600701249758>.

- Office of Inspector General. *Review of U.S. Customs and Border Protection's Fiscal Year 2022 Detailed Accounting Report for Drug Control Funds*. OIG-23-10. Washington, DC: Department of Homeland Security, 2023.
- Office of National Intelligence. "National Intelligence Community History." Accessed June 8, 2023. <https://www.oni.gov.au/national-intelligence-community/about-the-NIC/history>.
- Office of Personnel Management. "Customs and Border Protection Series 1895." Accessed August 3, 2023. <https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/1800/customs-and-border-protection-series-1895/>.
- Office of the Director of National Intelligence. "How the IC Works." Accessed April 15, 2019. <https://www.intelligence.gov/how-the-ic-works>.
- O'Neil, Andrew. "Australia and the 'Five Eyes' Intelligence Network: The Perils of an Asymmetric Alliance." *Australian Journal of International Affairs* 71, no. 5 (2017): 529–43. <https://doi.org/10.1080/10357718.2017.1342763>.
- Pancevski, Bojan. "On Edge from Attacks, Germany Finds Far-Right Radicals within Security Services." *Wall Street Journal*, October 11, 2019, <https://www.wsj.com/articles/on-edge-from-attacks-germany-finds-far-right-radicals-within-security-services-11570786206>.
- Parliament of Australia. "Advisory Report on the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020: Timeline of Reviews." February 2022. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IntegrityMeasuresBill/Report/section?id=committees%2Freportjnt%2F024737%2F78649.
- Pickering, Jordan C., and Andrew M. Fox. "Enabling Collaboration and Communication across Law Enforcement Jurisdictions: Data Sharing in a Multiagency Partnership." *Criminal Justice Policy Review* 33, no. 7 (August 2022): 732–55. <https://doi.org/10.1177/08874034211066756>.
- Reinhold, Derek, Charles Russo, and Beth Eisenfeld. "Analytical Standards in the Intelligence Community: Are Standards Professionalized Enough?" *Journal of Strategic Security* 14, no. 1 (2021): 106–21. <https://doi.org/10.5038/1944-0472.14.1.1923>.
- Ritzmann, Alexander. "The December 2022 German Reichsbürger Plot to Overthrow the German Government." *CTC Sentinel* 16, no. 3 (March 2023): 15–20. <https://ctc.westpoint.edu/the-december-2022-german-reichsburger-plot-to-overthrow-the-german-government/>.

- Russell-Taylor, Jacqueline. *Privacy Impact Assessment Update for the TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative*. DHS/CBP/PIA-009(a). Washington, DC: Department of Homeland Security, 2011. <https://www.dhs.gov/publication/tecs-system-cbp-primary-and-secondary-processing-tecs-national-sar-initiative>.
- Schmeer, Marcel. "Intelligence for the Masses: The Annual Reports on the Protection of the Constitution in West Germany between Cold War Propaganda and Government Public Relations." In *Intelligence Agencies, Technology and Knowledge Production: Data Processing and Information Transfer in Secret Services during the Cold War*, edited by Rüdiger Bergien, Debora Gerstenberger, and Constantin Goshler, 249–73. New York: Routledge, 2022.
- Secretary of State for the Home Department. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. London: Her Majesty's Stationery Office, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.
- Security Service MI5. "How MI5 Gather Intelligence." Accessed August 4, 2023. <https://www.mi5.gov.uk/gathering-intelligence>.
- . "Introduction to Counter-Terrorism." Accessed August 2, 2023. <https://www.mi5.gov.uk/counter-terrorism>.
- . "MI5 Protects the UK against Threats to National Security." Accessed July 20, 2023. <https://www.mi5.gov.uk/what-we-do>.
- Silva, Daniella. "ACLU Sues CBP over 'Highly Secretive' Teams Detaining Travelers." NBC News, December 19, 2019. <https://www.nbcnews.com/news/us-news/aclu-sues-cbp-over-highly-secretive-teams-detaining-travelers-n1104166>.
- Smith, Hillel R., and Kelsey Y. Santamaria. *Searches and Seizures at the Border and the Fourth Amendment*. CRS Report No. R46601. Washington, DC: Congressional Research Service, 2020. <https://crsreports.congress.gov/product/pdf/R/R46601/2>.
- Smith, Paul Jonathan. "Counterterrorism in the United Kingdom." In *Module III: The UK's Counterterrorism Structure and the Pursuit of Terrorists*. Monterey, CA: Center for Homeland Defense & Security, 2023. https://www.chds.us/coursefiles/comp/lectures/comp_CT_in_the_UK_mod03/script.pdf.
- Stana, Richard M. *Border Security: Additional Steps Needed to Ensure That Officers Are Fully Trained*. GAO-12-269. Washington, DC: Government Accountability Office, 2011. <https://www.gao.gov/products/gao-12-269>.

- Steele, Robert D. *The New Craft of Intelligence, Personal, Public, & Political: Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption*. Oakton, VA: OSS International Press, 2002.
- Steele, Robert David. *Information Operations: All Information, All Languages, All the Time*. 2nd ed. Concord, CA: OSS International Press, 2006.
- Taylor, Chris. "The Role of Intelligence in Australian Statecraft." *The Strategist*, April 21, 2023. <https://www.aspistrategist.org.au/the-role-of-intelligence-in-australian-statecraft/>.
- Tromblay, Darren E. "The Threat Review and Prioritization Trap: How the FBI's New Threat Review and Prioritization Process Compounds the Bureau's Oldest Problems." *Intelligence and National Security* 31, no. 5 (2016): 762–70. <https://doi.org/10.1080/02684527.2015.1105496>.
- UK Cabinet Office. *National Intelligence Machinery*. London: UK Cabinet Office, 2010. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf.
- Winter, Jana. "Operation Whistle Pig: Inside the Secret CBP Unit with No Rules That Investigates Americans." Yahoo News. December 11, 2021. <https://news.yahoo.com/operation-whistle-pig-inside-the-secret-cbp-unit-with-no-rules-that-investigates-americans-100000147.html>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE