NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CARROT OR STICK—A MULTIPLE CASE STUDY OF ANTI-CORRUPTION AND INCENTIVE-BASED PROGRAMS AND LESSONS LEARNED

by

Cesar Garcia

January 2022

Co-Advisors:	Robert L. Simeral (contractor) Lauren Wollman (contractor) Carolyn C. Halladay

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
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** January 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CARROT OR STICK—A MULTIPLE CASE STUDY OF ANTI-CORRUPTION AND INCENTIVE-BASED PROGRAMS AND LESSONS LEARNED			**5. FUNDING NUMBERS**
6. AUTHOR(S) Cesar Garcia			
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)			

U.S. Customs and Border Protection (CBP) is responsible for protecting all U.S. borders. CBP protects all air, land, and seaports, as well as the areas on the border between the official ports of entry. Drug trafficking organizations and human trafficking organizations continually target gaps in CBP's infrastructure, practices, and methodologies to exploit any shortfalls. Outside of technology and infrastructure gaps, CBP employees themselves are targets for criminal organizations. Criminal organizations look to corrupt current employees or insert a member of the criminal organization as a new employee to further their criminal enterprise.

This thesis investigates the human element in insider threats and employee corruption, as well as whether current nontechnology-based CBP tactics to combat insider threats and employee corruption requires additional fortifications. One incentive-based and one anti-corruption program are studied to determine if those programs can benefit CBP. CBP has a unique and challenging operational environment. This thesis addresses the unique operating environment encountered by CBP and provides recommendations to fill the gaps in current nontechnology-based insider threat and anti-corruption methodologies used in CBP.

14. SUBJECT TERMS U.S. Customs and Border Protection, CBP, corruption, employee corruption, incentives			**15. NUMBER OF PAGES** 99
			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

THIS PAGE INTENTIONALLY LEFT BLANK

CARROT OR STICK—A MULTIPLE CASE STUDY OF ANTI-CORRUPTION AND INCENTIVE-BASED PROGRAMS AND LESSONS LEARNED

Cesar Garcia
Assistant Special Agent in Charge, U.S. Customs and Border Protection,
Department of Homeland Security
BS, Strayer 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
January 2022

Approved by: Robert L. Simeral
Co-Advisor

Lauren Wollman
Co-Advisor

Carolyn C. Halladay
Co-Advisor

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

U.S. Customs and Border Protection (CBP) is responsible for protecting all U.S. borders. CBP protects all air, land, and seaports, as well as the areas on the border between the official ports of entry. Drug trafficking organizations and human trafficking organizations continually target gaps in CBP's infrastructure, practices, and methodologies to exploit any shortfalls. Outside of technology and infrastructure gaps, CBP employees themselves are targets for criminal organizations. Criminal organizations look to corrupt current employees or insert a member of the criminal organization as a new employee to further their criminal enterprise.

This thesis investigates the human element in insider threats and employee corruption, as well as whether current nontechnology-based CBP tactics to combat insider threats and employee corruption requires additional fortifications. One incentive-based and one anti-corruption program are studied to determine if those programs can benefit CBP. CBP has a unique and challenging operational environment. This thesis addresses the unique operating environment encountered by CBP and provides recommendations to fill the gaps in current nontechnology-based insider threat and anti-corruption methodologies used in CBP.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMO	air and marine officer
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BPA	border patrol agent
CBP	Customs and Border Protection
CBPO	Customs and Border Protection officer
CERT	computer emergency response team
CIA	Central Intelligence Agency
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
DOJ/OIG	Department of Justice/Office of Inspector General
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
HSAC	Homeland Security Advisory Council
IA	internal affairs
IAB	Internal Affairs Bureau
IC	intelligence community
IOD	Investigative Operations Division
IRB	Institutional Review Board
IT	information technology
JIC	Joint Intake Center
NBPC	National Border Patrol Council
NTEU	National Treasury Employee Union
NYPD	New York Police Department
OCDETF	Organized Crime Drug Enforcement Task Force
ONDCP	Office of National Drug Control Policy
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
OTD	Office of Training and Development
PERSEREC	Personnel Security Research Center

POE	port of entry
QSI	quality step increases
SAC	Special Agents in Charge
SSBI	single scope background investigation
USCS	U.S. Customs Service
VAP	Voluntary Assistance Program

EXECUTIVE SUMMARY

The Homeland Security Act of 2002 provided the legislation to establish the Department of Homeland Security (DHS), which gathered all federal agencies involved in such security under one umbrella.[1] Various legacy immigration and customs agencies merged to create the U.S. Customs and Border Protection (CBP) within this DHS umbrella. CBP's mission is to protect and secure the U.S. border against terrorist attacks, the importation of dangerous contraband, and illegal entry of criminals, terrorists, foreign intelligence officers, and undocumented aliens. CBP employs more than 60,000 personnel and has over 45,000 sworn law enforcement officers, the largest of any U.S. law enforcement entity.[2] In this way, CBP serves a vital defense function.

Like many organizations, CBP is vulnerable to employee misconduct and corruption;[3] however, border agency vulnerabilities extend beyond these known and expected improprieties. A 2012 Government Accountability Office study reported arrests of CBP employees for misconduct, such as domestic violence or driving under the influence from fiscal years 2005 to 2012, and 144 former or current CBP employee arrests or indictments for corruption-related activities, such as smuggling of aliens or drugs.[4]

[1] U.S. Customs and Border Protection, *Vision and Strategy 2020*, CBP Publication Number 0215-0315 (Washington, DC: Department of Homeland Security, 2015), 6, https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf.

[2] Homeland Security Advisory Council, *Final Report of the CBP Integrity Advisory Panel* (Washington, DC: Department of Homeland Security, 2016), 12, https://www.dhs.gov/sites/default/files/publications/HSAC%20CBP%20IAP_Final%20Report_FINAL%20(accessible)_0.pdf.

[3] *Merriam-Webster* defines misconduct as "intentional wrongdoing; specifically: deliberate violation of law or standard especially by a government official." *Merriam-Webster*, s.v. "misconduct," accessed September 5, 2017, https://www.merriam-webster.com/dictionary/misconduct. Cornell Law School defines corruption as "a government official, whether elected, appointed, or hired, who asks, demands, solicits, accepts, or agrees to receive anything of value in return for being influenced in the performance of their official duties." "Public Corruption," Information Institute, accessed April 12, 2018, https://www.law.cornell.edu/wex/public_corruption.

[4] Government Accountability Office, *Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct*, GAO-13-59 (Washington, DC: Government Accountability Office, 2012), 2, http://www.gao.gov/assets/660/650505.pdf.

Literature regarding insider-threat mitigation mainly deals with these risks in the cyber realm, but a corrupt CBP officer or agent working at a port of entry (POE) would not necessarily gain access to classified databases or generate intelligence reports, as only approximately 22% of the CBP workforce has a security clearance.[5] Most CBP employees with a security clearance work in management, intelligence units, or special operations. Instead, the corrupt CBP officers would more likely allow persons or items to enter the country without inspection. To do so, they would likely inspect either the driver but not the vehicle or passengers. This tactic obviously does not require access to classified databases nor does it leave a cyber-trail; therefore, a computer algorithm tracking access to unauthorized databases will fail to identify the act.

The CBP Office of Professional Responsibility (OPR), or internal affairs (IA), investigates and fights employee corruption and misconduct, but it does not have a policy either to identify or mitigate insider threats proactively. Rather, OPR manages insider threats reactively through two methods: (1) OPR waits until a source of information provides intelligence regarding criminal activity or misconduct, and (2) OPR waits until an employee triggers an information technology (IT) mechanism that reveals criminal activity or misconduct. The flaw with a reactive approach is that the incident, and thus the damage, has already occurred. A proactive approach mitigates insider threats by identifying cues, actions, or triggers associated with corruption before a crime is committed.

Effective solutions to mitigate corruption are those that incentivize employees to report crimes and programs that recruit employees as surreptitious "eyes and ears" within an organization. The New York Police Department (NYPD) Voluntary Assistance Program (VAP) is an exceptional program in which employees act as an Internal Affairs Bureau (IAB) force multiplier. The VAP recruits employees who volunteer to act as the "eyes and ears" within the organization. VAP participants work their regularly assigned posts but also report findings of corruption to their assigned handlers. All VAP participants' identities are kept confidential, even to other VAP participants and IAB staff. Only the VAP participants' handlers and IAB management know their identities. Maintaining the participants'

[5] Information obtained through the researcher's duties and operational knowledge of CBP.

identities confidential is important for the safety of the participants, as well as to ensure operational viability for continued operational deployments.

Crime Stoppers is also a unique program that provides financial incentives to report crimes while protecting the identity of the reporting party. The program is exceptional because it provides anonymity and a monetary incentive for persons who might otherwise not feel the moral obligation to provide information or who might fear reprisal for cooperating with law enforcement.

CBP will benefit from the adoption of incentive programs. The challenge is to determine whether existing approaches are scalable and how much modification they would require for the unique CBP environment. CBP is a federal law enforcement organization composed of approximately 60,000 employees with jurisdiction throughout the United States. CBP employees are represented by three different labor unions with whom negotiations to enact such approaches would be necessary. Labor unions do not affect the CBP mission or the integrity of CBP personnel. However, any change identified as a change in work environment or established past practice typically requires labor contract re-negotiation. Lastly, CBP has employees stationed throughout the world where U.S. laws may not apply. CBP employees stationed abroad must still follow CBP's policies and procedures, but criminal statutes vary from country to country that can possibly hamper criminal prosecution or extradition for criminal acts committed outside the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank my wife for her support, encouragement, and steadfast determination to keep me on track. I would also like to thank my family and friends who provided constant encouragement throughout this process. Many hours of family life and family commitments were sacrificed in favor of time spent working on this project. Without all of you, this thesis would not have been possible.

My thanks are extended to Customs and Border Protection for supporting and endorsing my participation in this program. I am grateful for the opportunity. I cannot forget my most fierce advocate, Dr. Michael Larrañaga. Without your support and endorsement, this lifelong dream would not be a reality.

Lastly, I would like to thank my thesis co-advisors, Captain (Ret.) Robert Simeral, Dr. Lauren Wollman, and Dr. Carolyn Halladay. Without your guidance, and mostly your patience, this thesis would never have become a reality. Thank you very much for all your time and guidance. Your boundless advice and support helped me take an abstract idea and craft it into a coherent thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The Homeland Security Act of 2002 provided the legislation to establish the Department of Homeland Security (DHS), which married all federal agencies involved in such security under one umbrella.[1] Various legacy immigration and customs agencies merged to create the U.S. Customs and Border Protection (CBP) within this DHS umbrella. CBP's mission is to protect and secure the U.S. border against terrorist attacks, against the importation of dangerous contraband, and the illegal entry of criminals, terrorists, foreign intelligence officers, and undocumented aliens. CBP employs more than 60,000 personnel and has over 45,000 sworn law enforcement officers, the largest of any U.S. law enforcement entity.[2] In this way, CBP serves a vital defense function.

Like many organizations, CBP is vulnerable to employee misconduct and corruption;[3] however, border agency vulnerabilities extend beyond these known and expected improprieties. A 2012 Government Accountability Office (GAO) study reported arrests of CBP employees for misconduct, such as domestic violence or driving under the influence from fiscal years 2005 to 2012, and 144 former or current CBP employee arrests or indictments for corruption-related activities, such as smuggling of aliens or drugs.[4]

[1] U.S. Customs and Border Protection, *Vision and Strategy 2020*, CBP Publication Number 0215-0315 (Washington, DC: Department of Homeland Security, 2015), 6, https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf.

[2] Homeland Security Advisory Council, *Final Report of the CBP Integrity Advisory Panel* (Washington, DC: Department of Homeland Security, 2016), 12, https://www.dhs.gov/sites/default/files/publications/HSAC%20CBP%20IAP_Final%20Report_FINAL%20(accessible)_0.pdf.

[3] *Merriam-Webster* defines misconduct as "intentional wrongdoing; specifically: deliberate violation of law or standard especially by a government official." *Merriam-Webster*, s.v. "misconduct," accessed September 5, 2017, https://www.merriam-webster.com/dictionary/misconduct; Cornell Law School defines corruption as "a government official, whether elected, appointed, or hired, who asks, demands, solicits, accepts, or agrees to receive anything of value in return for being influenced in the performance of their official duties." "Public Corruption," Information Institute, accessed April 12, 2018, https://www.law.cornell.edu/wex/public_corruption.

[4] Government Accountability Office, *Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct*, GAO-13-59 (Washington, DC: Government Accountability Office, 2012), 2, http://www.gao.gov/assets/660/650505.pdf.

Within the agency, employee misconduct occurs more often than criminal corruption, but employee criminal corruption is arguably a more serious threat to the homeland than employee misconduct. Literature regarding insider-threat mitigation mainly deals with these risks in the cyber realm, but a corrupt CBP officer or agent working at a port of entry (POE) would not necessarily gain access to classified databases or generate intelligence reports, as approximately only 22% of the CBP workforce has a security clearance.[5] Most CBP employees with a security clearance work in management, intelligence units, or special operations. As a result, the corrupt CBP officers could easily allow persons or items to enter the country without inspection. To do so, they would either likely inspect the driver but not the vehicle or passengers. This tactic obviously does not require access to classified databases nor does it leave a cyber-trail; therefore, a computer algorithm tracking access to unauthorized databases will fail to identify such an act.

The CBP Office of Professional Responsibility (OPR), or internal affairs (IA), investigates and fights employee corruption and misconduct, but it does not have a policy either to identify or mitigate insider threats proactively. Rather, OPR manages insider threats reactively through two methods: (1) OPR waits until a source of information provides intelligence regarding criminal activity or misconduct, and (2) OPR waits until an employee triggers an information technology (IT) mechanism that reveals criminal activity or misconduct. The flaw with a reactive approach is that the incident, and thus the damage, has already occurred. A proactive approach much more quickly mitigates insider threats by identifying cues, actions, or triggers associated with corruption.

Effective solutions to mitigate corruption are those that incentivize employees to report crimes and programs that recruit employees as surreptitious "eyes and ears" within an organization. The New York Police Department (NYPD) Voluntary Assistance Program (VAP) is an exceptional program in which employees act as an Internal Affairs Bureau (IAB) force multiplier. The VAP, created after the Commission to Investigate Allegations of Police Corruption and the Anti-Corruption of Procedures of the Police Department, also

[5] Information obtained through the researcher's duties and operational knowledge of CBP.

known as the Mollen Commission, published recommendations in 1994.[6] In this way, the NYPD institutionalized an incentive program to root out corruption.

The VAP recruits employees who volunteer to act as the "eyes and ears" within the organization. VAP participants work their regularly assigned posts but also report findings of corruption to their assigned handlers. All VAP participants' identities are kept confidential, even to other VAP participants and IAB staff. Only the VAP participants' handlers and IAB management know their identity. Maintaining the participants' identities confidential is important for the safety of the participants, as well as to ensure operational viability for continued operational deployments. The program is significant because it institutionalizes and formalizes the rooting out of corruption in a systematic and regular way.

Crime Stoppers is also a unique program that provides financial incentives to report crimes while protecting the identity of the reporting party. The program is exceptional because it provides anonymity and a monetary incentive for persons who might otherwise not feel the moral obligation to provide information or fear reprisal for cooperating with law enforcement. Greg MacAleese, an Albuquerque, NM, police officer, founded Crime Stoppers in 1976.[7] Officer MacAleese created the program because of the lack of information regarding an ongoing murder investigation. Now, Crime Stoppers is an international program with approximately 1,148 programs worldwide.[8] Information provided to Crime Stoppers has led to 965,163 arrests, 1,501,776 solved cases, $2,122,776,681 worth of personal property recovered, and $8,976,384,548 in drug seizures worldwide.[9] Literature on incentive-driven corruption-mitigating strategies, psychology-based game theory, and social dilemma studies demonstrate that incentive strategies result

[6] Harold Baer Jr. and Joseph P. Armao, "The Mollen Commission Report: An Overview," *New York Law School Law Review* 40 (1995): 2.

[7] Dennis P. Rosenbaum, Arthur J. Lurigio, and Paul J. Lavrakas, "Enhancing Citizen Participation and Solving Serious Crime: A National Evaluation of Crime Stoppers Programs," *Crime & Delinquency* 35, no. 3 (July 1, 1989): 401–420, https://doi.org/10.1177/0011128789035003006.

[8] Jeff Walsh, "Crime Stoppers," in *Encyclopedia of Law Enforcement*, ed. Larry E. Sullivan et al., (Thousand Oaks, CA: SAGE, 2018), 122–123, http://sk.sagepub.com/reference/lawenforcement.

[9] "About Us," Crime Stoppers International, accessed April 7, 2018, https://csiworld.org/about-us.

in an increase in reported misconduct and corruption as compared to non-incentive driven crime reporting programs.[10]

CBP might benefit from the adoption of incentive programs. The challenge is to determine whether existing approaches are scalable and how much modification they would require for the unique CBP environment. CBP is a federal law enforcement organization composed of approximately 60,000 employees with jurisdiction throughout the United States. CBP employees are represented by three different labor unions with whom negotiations to enact such approaches would be necessary. Labor unions do not affect the CBP mission or the integrity of CBP personnel. However, any change identified as a change in work environment or established past practice typically requires labor contract re-negotiation. Lastly, CBP has employees stationed throughout the world where U.S. laws may not apply. CBP employees stationed abroad must still follow CBP's policies and procedures, but criminal statutes vary from country to country that can possibly hamper criminal prosecution or extradition for criminal acts committed outside the United States.

B. RESEARCH QUESTION

How can CBP leverage successful non-cyber centric programs to detect and prevent corruption?

C. LITERATURE REVIEW

This literature review focuses on information available regarding counterintelligence methods used to detect, deter, and mitigate insider threats within U.S. law enforcement and the intelligence community (IC), specifically within CBP. The review also uses information regarding human behavior and psychological markers indicative of insider threats. This review is of non-law enforcement sensitive and non-classified sources, government reports, professional journals, and books written by members of the IC and psychological experts.

[10] Stephen E. G. Lea and Paul Webley, "Money as Tool, Money as Drug: The Biological Psychology of a Strong Incentive," *Behavioral and Brain Sciences; New York* 29, no. 2 (April 2006): 161–165, ProQuest.

1. Understanding Insider Threats

Employees are a critical asset within an organization; however, employees who become insider threats present a significant risk to an agency's mission and operations. An important question that must be asked regarding insider threats is "Why does an employee become an insider threat?" Michael Sulick, former head of the Central Intelligence Agency's (CIA's) Directorate of Operations, argues that employees become insider threats for money, improvement of their self-image, revenge, romance, adventure, ideological sympathy, globalization resulting in conflicting allegiances, greed, or loyalty to a cause.[11] In this way, critical assets can be transformed into threats. Ceresola asserts that both structural and institutional factors and individual factors cause corruption.[12] More transparent organizations are less prone to corruption and more restrictive organizations are more prone to corruption, where arguably the organizational structure determines if the organization is susceptible to corruption. Beyond the structure of the organization, some employees engage in corruption regardless of the structural influence. Employees who believe they are above the rules and believe the chances of being caught are low are more likely to engage in corruption.

Traditional insider threat mitigation strategies typically employ negative incentives (disincentives) to compel employees to act in the best interests of the organization. Negative incentives range from infractions, sanctions, admonishments, to criminal charges. Research indicated that when relied on excessively, negative incentives could lower morale and cause unintended consequences. However, positive incentives foster employee cooperation through extrinsic (money) or intrinsic (dedication) measures to act in the best interest of the organization. Stated differently, employees who feel as though they have organizational support are more prone to report corrupt acts.

[11] Michael J. Sulick, *American Spies: Espionage against the United States from the Cold War to the Present* (Washington, DC: Georgetown University Press, 2013), 7.

[12] Ryan G. Ceresola, "The U.S. Government's Framing of Corruption: A Content Analysis of Public Integrity Section Reports, 1978–2013," *Crime, Law and Social Change; Dordrecht* 71, no. 1 (February 2019): 49, ProQuest.

An organization must prioritize the need to understand who poses an insider threat to conduct operations effectively. According to a RAND Corporation conference proceedings document, organizations must understand, define, and find methods to mitigate the risks associated with potential breaches of security.[13] Per Greitzer et al., one method to mitigate insider threat risks is psychosocial models. They argue that psychosocial models that analyze behaviors associated with an increased risk of a person becoming an insider threat can identify certain traits exhibited by insider threats.[14] Such psychosocial models define several risk indicators, such as disregard for authority, disgruntlement, and anger management issues, and assign each indicator a level or psychosocial risk. Cole and Ring contend that besides psychosocial tools, technology can identify warning signs through word use analysis.[15] However, word use analysis requires the examination of computer keystrokes and word usage in analytical intelligence documents. Employees strictly engaged in law enforcement activities do not routinely create intelligence analysis documents. According to CBP, employees whose duties reside strictly in law enforcement write police and incident reports and rarely stray from those types of documents.[16] Literature regarding state and local law enforcement officers either arrested or convicted of crimes does not yield any link to the release of intelligence documents nor list any CBP officers or agents either arrested or indicted for unauthorized disclosure of classified material.[17] This situation gives CBP few tools to predict such warning signs.

[13] Richard C. Brackney and Robert H. Anderson, *Understanding the Insider Threat: Proceedings of a March 2004 Workshop* (Santa Monica, CA: RAND, 2004).

[14] Frank L. Greitzer et al., “Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis,” *e-Service Journal* 9, no. 1 (2013): 106–138, https://muse.jhu.edu/article/548560/summary.

[15] Eric Cole and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*, 1st. ed. (Rockland, MA: Syngress, 2006), 209, 215.

[16] “Border Patrol Agent Duties,” U.S. Customs and Border Protection, accessed November 27, 2017, https://www.cbp.gov/careers/frontline-careers/bpa/duties.

[17] Graham H. Turbiville, “Silver over the Border: U.S. Law Enforcement Corruption on the Southwest Border,” *Small Wars & Insurgencies* 22, no. 5 (December 2011): 835–859, http://www.tandfonline.com/doi/abs/10.1080/09592318.2011.620811.

Scholars agree that understanding why a person engages in insider threat activity gives employers a proactive edge in identifying persons who display an increased psychosocial risk. As per CBP and Police Integrity Lost, arrests of local, state, and CBP law enforcement officers demonstrated that front line agents and officers do not typically create or handle classified intelligence reports.[18] Strategies to identify insider threats proactively generally discuss IC personnel who create or handle classified information rather than front line law enforcement staff, despite the fact that the latter do handle and generate proprietary, personably identifiable, and law enforcement sensitive information.

2. Defending against Insider Threats

The goal of any agency or employer is proactively to identify and mitigate employees with intent to cause the agency harm. Lowenthal argues that to identify and mitigate such threats, the agency must develop methods and policies to defend against them.[19] Employees already inside an agency have various reasons for engaging in insider threat activity. According to Catrantzos, different types of insider threats include the malicious insider, trust betrayer, infiltrator, recruited asset, and disgruntled employee.[20] While Catrantzos does focus on why actors either engage in corruption or espionage, the focus should rather be on the individuals, their positions in the organization, and how the actors obtained those positions (e.g., through infiltration, as a recruited asset).[21] The literature discusses numerous methodologies—including but not limited to background checks, polygraphs, analytical software, and techniques used in the IC—available to employers to defend against insider threats.

According to Dahl, intelligence gathering provides strategic level warning intelligence and mitigates insider attacks; however, warning intelligence is not necessarily

[18] Homeland Security Advisory Council, *Final Report of the CBP Integrity*, 8–11.

[19] Mark M. Lowenthal, *Intelligence; From Secrets to Policy*, 7th ed. (Washington, DC: CQ Press, 2016), 239, 310.

[20] Nicholas Catrantzos, "No Dark Corners: Defending against Insider Threats to Critical Infrastructure" (master's thesis, Naval Postgraduate School, 2009), 1, http://www.dtic.mil/docs/citations/ADA508935.

[21] Catrantzos, 1–4.

the same as operational information.[22] Grabo and Goldman state that warning intelligence can either provide information regarding imminent, immediate future, near future, and foreseeable attacks or threats but infrequently produces actionable intelligence.[23] Grabo and Goldman assert that intelligence only provides decision makers with the best and earliest information to make an informed judgement that an action is hostile, and thus only provides tactical intelligence.[24] Steps must be taken to create a tangible intelligence product. According to the *Homeland Security Advisory Council Final Report* of the CBP Integrity Advisory Panel, properly analyzed and processed warning intelligence will likely produce more than just information; the product provides actionable intelligence.[25] Researchers agree that when agencies obtain actionable intelligence, the agencies can defend their infrastructure and technology better.

The "No Dark Corners" concept, an array of defenses to configure job roles to reduce the probability of a single person occupying a sensitive area undetected or without the possibility of being alone, discusses proactive measures that can be used to defend critical infrastructure.[26] Corporate sentinels, random audits, background checks, and technologically based monitoring can be used to defend against insider threats.

Literature available on the topic of defending against insider threats focuses on infrastructure and technology. The infrastructure and technology discussed in the literature are not typically available to law enforcement personnel on patrol. According to the House Homeland Security Committee's Subcommittee on Border and Maritime Security, it is challenging and costly to add improvements to infrastructure in remote areas or private

[22] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 21, 23.

[23] Cynthia Grabo and Jan Goldman, *Handbook of Warning Intelligence: Assessing the Threat to National Security*, 1st ed. (Lanham, MD: Scarecrow Press, 2010), 2–3, 30.

[24] Grabo and Goldman, 2, 13.

[25] Homeland Security Advisory Council, *Final Report of the CBP Integrity*, 15–19.

[26] Catrantzos, "No Dark Corners," 2.

property to deter insider threats.[27] As per Catrantzos, infrastructure improvements to public service buildings and technology may not be as challenging.[28] However, research into what infrastructure improvements to remote areas or private property may mitigate insider threats is important to this topic in CBP's context because CBP employees routinely work in austere environments or on private property, such as ranches and farms.

3. The Human Element in Insider Threat Detection and Mitigation

Traditional IC methodologies and counterintelligence techniques play an important role in the literature. Infrastructure and technology employee monitoring are an important tool in detecting and mitigating insider threats.[29] Not much discussion however has resulted concerning such tools used outdoors or across large geographic areas where supervisor contact is limited.

According to Lowenthal, leveraging IC data collection and counterintelligence tactics can provide intelligence that detects and mitigates insider threats.[30] Sims and Gerber argue that to leverage IC techniques and counterintelligence tactics, IC professionals must reinvent themselves to meet the demands of the ever-evolving threat.[31] An example of a non-traditional counterintelligence tactic is the NYPD's VAP.[32] The VAP unit recruits cadets while at the police academy to work their regular patrol duties and report corruption or misconduct to the IAB.

[27] *Keeping Pace with Trade, Travel, and Security: How Does CBP Prioritize and Improve Staffing And Infrastructure?: Hearing before the Subcommittee on Border and Maritime Security*, House of Representatives, 114th Cong., 2nd sess., April 19, 2016, 23–24, https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg22756/pdf/CHRG-114hhrg22756.pdf.

[28] Catrantzos, "No Dark Corners," 2–5.

[29] Cole and Ring, *Insider Threat*, 42, 58.

[30] Lowenthal, *Intelligence*, 239, 310.

[31] Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 70, 97.

[32] Gary T. Marx, "When the Guards Guard Themselves: Undercover Tactics Turned Inward," *Policing and Society* 2, no. 3 (April 1992): 151–172, http://www.tandfonline.com/doi/abs/10.1080/10439463.1992.9964639.

Cole and Ring argue that insider threat case studies and their findings will determine what technology and what processes work best in which environments.[33] Lowenthal reasons that the overall process of intelligence gathering, analysis, and dissemination, specifically the use of counterintelligence methods, and the external indicators and problems associated with counterintelligence operations, must be studied and understood.[34] After managers and decision makers study and understand the IC, they will find it challenging to create counterintelligence policies to combat insider threats as no single method or process exists that is completely successful in all scenarios.

4. IC and Counterintelligence Use to Combat Insider Threats within Customs and Border Protection

No CBP insider threat programs, policies, or procedures proactively target insider threats. According to a GAO report for Congress, CBP conducts pre-employment polygraph exams, pre-employment background investigations, and periodic re-investigations for employees in certain positions.[35] No literature demonstrates a proactive approach to combat current employees engaged in insider threat activities other than typical IA investigations that investigate employees after an allegation is made against the particular employee. Reports and data regarding countrywide police officer arrests are available and provide a solid benchmark to determine why employees engage in corruption or misconduct (insider threats).

5. Human Behavior and Psychological Markers

Insider threat research began in the United States in the 1990s, and studies identified psychological markers that indicate an increased risk for damaging behavior.[36] Additional studies corroborated initial findings that persons who engage in retaliatory behavior, such as abusing sick leave, wasting material, or damaging equipment, are prone

[33] Cole and Ring, *Insider Threat*, 17.

[34] Lowenthal, *Intelligence*, 232.

[35] Government Accountability Office, *Border Security*, 3, 6.

[36] William R. Claycomb et al., *Chronological Examination of Insider Threat Sabotage: Preliminary Observations* (Pittsburgh, PA: Carnegie Mellon University, 2012), 17.

to psychological breaches of contract.[37] Puleo argues that persons engage in criminal acts because of greed, revenge, ideological differences, sympathy for a cause, and recognition of power indicating that reasons for criminal behavior derive from human emotions.[38] The Defense Personnel Security Research Center (PERSEREC) notes that differences in ethical conventions originating from cultural differences may be the cause of conflict and misunderstanding between employees and staff with different cultural, ethnic, or political and social differences.[39] Arguably, these ethical and cultural contextual differences can directly influence insider risk. To mitigate the risk, policies and practices should be modified as required by cultural settings; however, care must be taken not to confuse personnel and undermine the effectiveness of the policy.[40]

Carnegie Mellon University computer emergency response team (CERT) and PERSEREC's analysis of insider sabotage models identified stressful events, such as organizational sanctions as factors that increase the likelihood of sabotage or espionage.[41] Therefore, psychological, cultural, and political stressors are arguably influential factors that when combined with psychological markers increase the likelihood of a person becoming an insider threat.

However, Greitzer et al. argue that no psychosocial evaluation methods can predict risks for insider threats and that any evaluation methods must be coupled with security techniques to achieve an effective security package.[42] Hence, employee evaluation models are more effective in mitigating insider threats from materializing when partnered with

[37] Frank L. Greitzer et al., *Identifying At-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats*, PNNL-19665 (Washington, DC: Department of Energy, 2010), 2.3, http://www.osti.gov/servlets/purl/1000159-1JPnC7/.

[38] Anthony J. Puleo, "Mitigating Insider Threat Using Human Behavior Influence Models" (master's thesis, Air Force Institute of Technology, 2006), 121.

[39] Eric D. Shaw, Lynn F. Fischer, and Andrée E. Rose, *Insider Risk Evaluation and Audit*, Technical Report 09-02 (Monterey, CA: Department of Defense, 2009), 6, http://www.dtic.mil/docs/citations/ADA563910.

[40] Shaw, Fischer, and Rose, 8.

[41] Claycomb et al., *Chronological Examination of Insider Threat*, 7.

[42] Greitzer et al., *Identifying At-Risk Employees*, 2.4.

additional security layers, such as security protocols and a better-trained workforce to report anomalous actions or behavior indicative of an insider threat.

6. Leadership Acceptance of Counterintelligence Program

According to Dahl, acceptance of a counterintelligence program by government officials is challenging to achieve.[43] Government leaders do not like to fail and that can cause some to be risk averse. A risk management plan with the risks versus rewards of certain actions or inactions must be developed. As per a 2013 DHS, Office of Inspector General (OIG) report, the most concerning insider threat concerns are unauthorized use and disclosure of classified or unclassified information, critical information technology network interruption, and border security breaches through malfeasance or nonfeasance.[44] Personnel must receive clear and consistent messaging regarding their roles and responsibilities from managers and supervisors in CBP for mitigating insider threats. Policies and procedures are already in place within CBP to identify unauthorized access and disclosure of classified or unclassified information, as well as security to IT networks. Due to the sensitive nature of internal investigations, exact figures on the effectiveness are not available. Every CBP employee knows that all activity on CBP networks are tracked and analyzed for suspicious activity. The IT-based security safeguards are thus particularly effective. However, CBP employees can deliberately circumvent operational procedures to allow unauthorized persons or material to enter the United States without the use of CBP networks. CBP's Standards of Conduct policy requires every CBP employee to report allegations of misconduct immediately. OPR conducts an in-depth analysis of subjects with frequent OPR contact to ensure illicit activity is not ongoing. Nevertheless, the lack of a plan, policy, or procedure in place to combat insider threats proactively who have not had any previous contact with OPR threatens CBP. Individuals who want to breach the gap in border security by facilitating the flow of terrorists, narcotics, or other undocumented individuals through the U.S. border, can proceed unencumbered. Studies and research must

[43] Dahl, *Intelligence and Surprise Attack*, 157.

[44] Department of Homeland Security, *U.S. Customs and Border Protection Has Taken Steps to Address Insider Threat, but Challenges Remain*, OIG-13-118 (Washington, DC: Office of the Inspector General, 2013), 6, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-118_Sep13.pdf.

be conducted to determine what, if any, IC methodologies can mitigate employee insider threats.

7. Additional Literature

Literature obtained from NYPD interviews and Crime Stoppers research facilitated the case study research and subsequent policy recommendations in this thesis.[45] Operational NYPD data including policy, policy implementation data, metrics, challenges, legal issues, and statistical data added to the overall policy plan. Crime Stoppers data regarding crime clearance rates, monetary returns, and incentive programs aided in crafting the dual-prong policy plan.[46]

D. RESEARCH DESIGN

This research consists of two case studies, the NYPD VAP and the Crime Stoppers Program. This research identified and examined key structural, strategic, and operational elements of those programs. The research extracted the components and lessons applicable to CBP through replication or modification.

The two programs are exceptional outlier cases.[47] The VAP and Crime Stoppers programs were selected because of their innovative proactive approaches to mitigate crime and corruption. Both programs are large, established, and high profile enough to allow close and detailed study. An incentive program, such as the Crime Stoppers model, which allows employees to remain anonymous, has worked with civilians, and the framework may be used in the CBP environment. Implementing a Crime Stoppers-like program that allows employees to provide information anonymously to CBP's Office of Professional Responsibility (OPR) with a possible monetary incentive, should the information the anonymous employee provides lead either to an arrest or conviction, is a viable option.

[45] Jeffrey Liss, email message to author, February 7, 2018.

[46] "History," Crime Stoppers USA, accessed March 29, 2021, https://www.crimestoppersusa.org/history/.

[47] Robert K. Yin, *Case Study Research: Design and Methods*, 5th ed. (Thousand Oaks, CA: SAGE, 2013), 15.

Implementation of a policy creating a proactive program, such as the NYPD VAP is a viable option for CBP. The VAP is an exceptional program that consists of frontline police personnel who voluntarily provide information to personnel within NYPD's IAB. The VAP is unique because participants work their regular assigned posts but also report findings of corruption to their assigned IAB handlers.

VAP research relied on internal documents and sources with cooperation from an NYPD VAP supervisor and a senior investigator. Specifically, the NYPD shared information regarding the VAP creation, VAP design and structure, performance metrics, possible improvements, and challenges faced. The NPS Institutional Review Board (IRB) determined that the interviews with NYPD VAP principals provided by email to the author did not warrant IRB approval. Crime Stoppers research relied on academic literature, program evaluations, legal briefs, and Crime Stoppers International documents.

E. OVERVIEW

Chapter II provides the reader with background information on the U.S. Customs Service (USCS), the predecessor to CBP. The chapter provides the reader with historical research of corruption and misconduct within the USCS and CBP. The chapter informs the reader of CBP new-employee vetting procedures and compares the CBP polygraph program to other federal agencies while reviewing the efficacy of the polygraph.

Chapter III is a case study of the Crime Stoppers program and psychological research on incentive-based reporting studies and programs. Chapter III addresses social dilemma studies and explores whether incentive-based programs unknowingly drive people to report fictitious crimes to receive monetary incentives.

Chapter IV is a case study of the NYPD's VAP and psychological research into psychological markers that demonstrate whether a person is prone to commit criminal acts. Lastly, the chapter discusses whether peer reporting mitigates insider threats.

Chapter V makes recommendations for a hybrid program that encompasses both an incentive-based reporting model and a peer-reporting model to mitigate corruption and misconduct. The chapter analyzes challenges and costs associated with implementation. It also presents conclusions of a fully implemented carrot-and-stick hybrid program. The chapter summarizes the research and assesses the importance of the constant evolution required to ensure the program is successful.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MISCONDUCT IN CBP AND CURRENT MITIGATION STRATEGIES

Like most large law enforcement entities, CBP suffers from employee misconduct, ranging from administrative policy violations to serious criminal acts. Pre-employment vetting and polygraph examinations decrease the chances of hiring persons with questionable backgrounds. However, once employed, methodologies to ensure employees continue to avoid and prevent misconduct would enhance the likelihood of deterrence or apprehension. Changing culture that accepts misconduct as an unavoidable aspect of law enforcement is a challenging endeavor but not an impossible task. Changing this culture begins with understanding the agency's roots. This chapter presents the history of corruption within CBP, discusses vetting and backgrounds checks, and determines the historical effectiveness of pre- and post-employment polygraphs.

The USCS was the first federal law enforcement agency created by the newly formed United States of America and established by the First Congress in 1789.[48] Unfortunately, corruption in USCS was present almost from its inception, and for almost 100 years, appointments and promotions within USCS were made according to the "spoils system."[49] The spoils system doled out civil service positions according to political loyalty and favoritism, and prominent families and political supporters benefitted the most from it. Similarly, most early American police departments were infamously corrupt.[50] The local political district head selected the local police administrator, which triggered effortless manipulation by the polity.[51] The local district head generally controlled the gambling and prostitution, the local tavern, and local gangs, which thus resulted in having a foothold on policing and crime all at once.[52] Regrettably, corruption and misconduct of

[48] U.S. Customs and Border Protection, *Vision and Strategy 2020*, 6.

[49] "History," U.S. Customs Museum Foundation, accessed August 8, 2017, http://customsmuseum.org/history/.

[50] Gary Potter, "The History of Policing in the United States," EKU Online, accessed August 8, 2017, http://plsonline.eku.edu/sites/plsonline.eku.edu/files/the-history-of-policing-in-us.pdf.

[51] Potter.

[52] Potter.

U.S. law enforcement officers and agents continues to this day.[53] CBP is no exception to rank-and-file misconduct and corruption. Regrettably, no national databases allow for the study, research, and analysis of either police corruption or crime.[54] Nevertheless, this practice means it must be actively thwarted.

A 2011 Organized Crime Drug Enforcement Task Force (OCDETF) budget provided a succinct overview of the U.S. law enforcement corruption problem and its impact:

> Magnifying the problem is the documented presence of corrupt border officials who facilitate a wide range of illegal activities along the Southwest Border. Resource-rich cartels employ a variety of methods in order to target and recruit U.S. Border Patrol agents, Customs and Border Protection officers, and local police officers who can facilitate organized crime. The corrupt officials assist the cartels by providing intelligence and participating in moving weapons, drugs, aliens, and other contraband across the US-Mexican border. Corruption within U.S. law enforcement, coupled with extensive corruption among Mexican government, military, and law enforcement officials, facilitates the operations of the cartels.[55]

As previously mentioned, a 2012 GAO study indicated that CBP employees were reported and arrested for misconduct, such as domestic violence or driving under the influence for fiscal years 2005 to 2012, and 144 former or current CBP employee were arrested or indicted for corruption-related activities, such as smuggling aliens or drugs.[56] The majority of the allegations of corruption or misconduct against CBP employees occurred along the southwest border because this area represents a key transit route for undocumented migrants and illegal drugs.[57] Arguably, the majority of corruption or misconduct allegations occur on the southwest border because a large majority of CBP employees is stationed along that area compared to the northern border.

[53] Philip Matthew Stinson et al., *Police Integrity Lost: A Study of Law Enforcement Officers Arrested: Final Technical Report* (Bowling Green, OH: Criminal Justice Program, Department of Human Services, College of Health & Human Services, Bowling Green State University, 2016).

[54] Stinson et al., 14.

[55] Turbiville, "Silver over the Border," 835–859.

[56] Government Accountability Office, *Border Security*, 2.

[57] Government Accountability Office, 2.

In 2016, the White House Office of National Drug Control Policy (ONDCP) released a *National Southwest Border Counternarcotics Strategy* to highlight the most important issues in U.S. policy.[58] The strategy addresses corruption along the southwest border and requires agencies to report corruption to the FBI's Border Corruption Task Force. Namely, the strategy increases the focus on connections between public corruption and threats to U.S. national security. The involvement of the ONDCP demonstrates the importance of combatting criminal corruption and misconduct along the southwest border.

A. CRIMINAL CORRUPTION IN CBP

CBP law enforcement officers and agents enforce hundreds of U.S. laws and regulations. CBP's main task is to keep terrorists and their weapons out of the United States while facilitating lawful trade and travel. CBP law enforcement personnel include CBP officers (CBPOs), border patrol agents (BPAs), and air and marine officers (AMOs). CBPOs work at official POEs in and around the country. BPAs work between the POEs. BPAs detect and apprehend persons and illicit goods illegally entering the country between the POEs. AMOs include pilots and boat operators who work in concert with BPAs to apprehend persons and illicit goods illegally entering the country. The three types of CBP law enforcement personnel work in different environments. Each environment provides unique opportunities for corrupt employees either to allow items or individuals to enter the country without inspection. For example, a CBPO may allow a vehicle to enter the country without proper inspection while not triggering any IT safeguards by simply not inspecting the passengers in that vehicle. BPAs patrolling in an austere desert may allow persons carrying narcotics by not patrolling their assigned areas. Lastly, AMO personnel on patrol in the maritime environment may allow a boatload of narcotics to pass by avoiding an established smuggling route. Even though these are hypothetical scenarios, a corrupt employee can easily allow items or persons to enter without drawing either much suspicion from peers or supervisors.

[58] Office of National Drug Control Policy (ONDCP), *National Southwest Border Counternarcotics Strategy* (Washington, DC: Office of the President of the United States, 2016), 1, https://obamawhitehouse.archives.gov/sites/default/files/ondcp/policy-and-research/southwest_strategy-3.pdf.

All federal law enforcement agents and officers undergo background and vetting procedures that disqualify persons with questionable backgrounds or criminal history. Although these background checks and vetting generally disqualify persons not fit for employment as federal law enforcement officers, some may slip through the cracks. Research and analysis in this thesis demonstrates a corrupt employee does not just take a single path to criminalization. Some employees begin their careers with no intention to commit criminal acts but are somehow corrupted along the way. Some employees are infiltrators who enter into law enforcement with the intent to cause harm for nefarious reasons. Failures in employee vetting, non-reporting by peers, and lack of on–the-job-supervision are some contributing factors. Arguably, no pre-employment vetting system is foolproof.

To combat corruption and misconduct, CBP implemented pre-employment polygraph examinations in 2008. CBP randomly polygraphed law enforcement candidates from 2008 to 2013. However, only approximately 25 percent of the new employee candidate pool received a polygraph examination.[59] CBP uses a full-scope polygraph combining lifestyle, national security, and counterintelligence questions.

CBP candidates who did not receive a polygraph examination underwent a single scope background investigation (SSBI). CBP still has several thousand employees who never received a polygraph. Those hired before 2008 did not receive a polygraph and only a small percentage of the employees hired from 2008 to 2013 received one.

Due to the national security position held by CBP law enforcement officers and agents, corruption within its ranks can have devastating outcomes. A corrupt CBP employee turning a blind eye might theoretically allow terrorists or terrorist weapons into the country that could have a devastating impact deep in the interior of the country. CBPOs and BPAs have allowed either persons or items into the country in exchange for money, sex, or drugs. No one really knows what these corrupt employees allowed into the United States because the employees themselves do not know what they allowed to enter. High profile CBP corruption cases bring this concern to light. The significant cases that follow

[59] Author was assigned to CBP HQ at the time the CBP polygraph program was implemented.

highlight criminal corruption within CBP ranging from an employee whose goal was to work with a smuggling organization when he applied to join CBP, to employees who for an unknown reason engaged in criminal activity after several years of service in CBP.

1. Some Examples of Corrupt CBP Employees

- In 2009, CBPO Luis F. Alarid, who worked in San Diego, California, was convicted for allowing drugs and illegal immigrants through his inspection lane at a POE.[60] Alarid earned over $200,000 for his illicit acts. Investigators involved in the case believed that Alarid planned to work for smugglers when he applied to join CBP.[61]

- In February 2016, Douglas, Arizona POE employee, CBPO Johnny Acosta, received an eight-year prison sentence for bribery and drug smuggling.[62] Authorities arrested Acosta attempting to flee into Mexico. Acosta accepted over $70,000 in bribes and allowed over a ton of marijuana into the United States.

- In January 2016, Supervisory BPA Eduardo Bazan, who worked in McAllen, Texas, was accused of assisting a drug organization in smuggling cocaine.[63] Bazan admitted to receiving over $8,000 to help the drug smuggling organization.

- In 2017, BPA Joel Luna, who worked in Hebbronville, Texas, was charged with murder and engaging in organized criminal activity.[64] Luna

[60] Randal C. Archibold, “Mexican Cartels Look to Turn Border Agents—With Some Success,” *New York Times*, sec. U.S., December 17, 2009, https://www.nytimes.com/2009/12/18/us/18corrupt.html.

[61] Archibold.

[62] Ron Nixon, “The Enemy within: Bribes Bore a Hole in the U.S. Border,” *New York Times*, sec. U.S., December 28, 2016, https://www.nytimes.com/2016/12/28/us/homeland-security-border-bribes.html.

[63] Nixon.

[64] Jeremy Raff, “The Border Patrol’s Corruption Problem,” *The Atlantic*, May 5, 2017, https://www.theatlantic.com/politics/archive/2017/05/not-one-bad-apple/525327/.

> was acquitted of the murder charge but was convicted on two counts of engaging in organized criminal activity.

Review of records demonstrates that employees were either charged or convicted of corruption vary in years of service. Of the CBP employees either arrested or convicted for acts of corruption between 2004 and 2015, 49 had five years or less of service, 43 had six to 10 years of service, 30 had 11 to 19 years of service, 11 had 20 years or more of service, and seven had an unknown number of years in service.[65] The pattern demonstrates that a large number of employees convicted of corruption did not undergo pre-employment polygraph examinations because they were not required at the time of their employment. Research into misconduct and criminality rates specifically for employees hired after mandatory pre-employment polygraphs is not available. Even though a polygraph or periodic re-investigation cannot predict whether a person will become corrupt after employment, an analysis of agencies within the Department of Justice (DOJ) discussed later does show a correlation between lower corruption rates and pre- and post-employment polygraphs.

2. Status Quo—Current CBP Law Enforcement Employee Vetting Process

All CBP law enforcement employees hired after 2013 must pass an SSBI and a polygraph. Though an SSBI qualifies CBP employees for security clearances, the general uniformed CBP workforce carries only a law enforcement sensitive clearance; specialty, plain clothes (non-uniformed), and intelligence units are generally granted a secret or top-secret clearance. Due to the sensitive nature of this information, exact numbers of CBP employees with security clearances are not available.

A typical five-year periodic re-investigation consists of criminal records checks, credit bureau reports, commercial databases containing public civil records, foreign travel databases, and co-worker interviews. CBP does not use any other proactive screening tool to mitigate the risk of incumbent employee corruption and misconduct.

[65] "Cracks in the Wall: When Border Watchdogs Turn Criminal," *The Texas Tribune*, July 7, 2016, https://apps.texastribune.org/bordering-on-insecurity/when-border-watchdogs-turn-criminal/.

Nevertheless, undergoing a pre-employment background check does not mean the check itself was completed. From 2008 to the writing of this thesis, 22 Office of Personnel Management (OPM) background investigators and two record inspectors were convicted of falsifying reports of investigation.[66] The background investigators generated false reports indicating they interviewed references, reviewed sources, and records regarding the subjects of the investigations. However, the background investigators did not conduct the interviews or obtain the records. The agencies requesting the background investigations used and relied upon the false reports generated by the background investigators for employment and security clearance purposes. Positions filled with the incomplete or false investigative background checks included positions with access to classified information, national security, and positions of public trust.[67] The convictions were a stark reminder that simply having a completed SSBI does not guarantee an applicant was properly vetted prior to employment and demonstrated a need for an ongoing vetting process.

To guarantee an ongoing vetting process within CBP, the Homeland Security Advisory Council (HSAC) *Final Report of the CBP Integrity Advisory Panel* recommended the expansion of the CBP polygraph program to include targeted and random post-employment polygraphs.[68] The HSAC report suggests ongoing monitoring:

> We believe that integrity could be enhanced further by periodic random and targeted polygraph examinations on a post-hire basis of CBP law enforcement personnel. The FBI and the agencies in the U.S. intelligence community (e.g., CIA, DIA, NSA) currently conduct post-hire polygraphs during their 5-year periodic security investigation and some random polygraphs for on-board employees.[69]

In keeping with this sentiment, a bill introduced in July 2017 titled, "Integrity in Border and Immigration Enforcement Act" requires CBP to administer post-employment

[66] "Former Background Investigator for Federal Government Pleads Guilty to Making a False Statement," Department of Justice, accessed August 11, 2017, https://www.justice.gov/usao-dc/pr/former-background-investigator-federal-government-pleads-guilty-making-false-statement-6.

[67] Department of Justice.

[68] Homeland Security Advisory Council, *Final Report of the CBP Integrity*, 19.

[69] Homeland Security Advisory Council, 19.

polygraphs to law enforcement personnel.[70] To date, the bill has passed in neither the Senate nor the House and has not become law.[71] It is unknown why the bill has not passed the Senate or the House and become law. Thus, incumbent CBP employees do not receive a post-hire polygraph examination and only undergo a periodic re-investigation every five years of employment. As discussed later in this thesis, post-hire polygraph examinations will not completely eliminate corruption or misconduct. However, the research indicated that agencies within the DOJ that require incumbent polygraph tests reported less corruption cases than CBP.

3. Other Agencies that Employ Polygraph Testing

Components within the DOJ conduct polygraph examinations for a variety of reasons. The components use polygraphs during pre-employment and personnel security vetting to investigate criminal, administrative (IA and misconduct), and security violations, ensure witness security, and provide sex offender treatment, foreign counterintelligence and counterterrorism investigations, as well as operational support in examining or vetting foreign task force members and validating intelligence sources.[72] Thus, the DOJ uses polygraphs to find a host of problems.

A 2006 DOJ/OIG documented the four DOJ components that operate their own polygraph programs and administer post-employment polygraph tests during misconduct investigations.[73] The four components are the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and the DOJ/OIG. "From FY 2002 through 2005, the four polygraph units conducted 149 specific-issue polygraph examinations of employees who were subjects, witnesses, or complainants in investigations of personal misconduct in the

[70] "S. 1560: Integrity in Border and Immigration Enforcement Act," GovTrack, accessed August 7, 2017, https://www.govtrack.us/congress/bills/115/s1560/text.

[71] Richard Durbin, "S.1560—Integrity in Border and Immigration Enforcement Act," Congress.gov, last modified July 13, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1560.

[72] Department of Justice Office of the Inspector General, *Polygraph Examinations in the Department of Justice* (Washington, DC: Department of Justice Office of the Inspector General, 2006), 35–107, https://oig.justice.gov/reports/plus/e0608/final.pdf.35–107.

[73] Department of Justice Office of the Inspector General, 35–107.

performance of their official duties."[74] In contrast, CBP reported 2,170 misconduct cases from 2005 to 2012.[75] If CBP administered specific-issue polygraphs for only 10 percent of its reported misconduct cases during the aforementioned period, the 217 hypothetical polygraphs would be greater than the 149 polygraphs conducted by the four DOJ components combined. It must be considered that CBP is a larger organization than the four DOJ agencies individually, but combined, the four components have a larger workforce than CBP. The aforementioned polygraph data demonstrates that not all federal law enforcement organizations that also work along the U.S.-Mexico border have the same documented levels of misconduct and corruption as CBP. Further research into the correlation between post-employment polygraphs and misconduct investigations is necessary to determine if the mere possibility of a post-employment polygraph reduces misconduct.

Even if incumbent periodic or random polygraph testing were instituted in CBP, it would not guarantee that employees engaging in misconduct or corruption would show deception during testing that would have resulted in a positive polygraph exam. Several documented cases show federal employees or law enforcement officers or agents having taken polygraph exams and passed even while engaging in nefarious activities. One of the most famous cases was Aldrich Ames, a CIA employee who was arrested for selling classified information to the Russians. During his time as a spy, Ames successfully passed two polygraph exams that specifically targeted the activities he engaged in as a spy.[76]

4. Issues and Problems—Pros and Cons to Polygraph Examinations

As a deception detection tool, much debate surrounds the accuracy of polygraphs. A polygraph device is a diagnostic tool able to measure physiological responses indicative

[74] Department of Justice Office of the Inspector General, 29.

[75] Government Accountability Office, *Border Security*, 2.

[76] Karen E. Sims, "Unauthorized Disclosure: Can Behavioral Indicators Help Predict Who Will Commit Unauthorized Disclosure of Classified National Security Information?" (master's thesis, Naval Postgraduate School, 2015), 87.

of deception.[77] The physiological responses are a result of psychological arousals during a state of lying or untruthfulness (deception).[78] Deception is defined as a deliberate attempt to create a false belief in others.[79] Proponents of the polygraph exam argue that polygraphs are approximately 80 to 98 percent accurate.[80] Opponents argue that polygraphs are approximately 60 percent accurate, or only slightly better than flipping a coin.[81] Judging which side is "correct" is not so easy.

Research confirms that a polygraph device measures physiological reactions that may be associated with stress, fear, guilt, anger, excitement, or anxiety about detection, regardless of an examinee's guilt or innocence.[82] Regardless of beliefs, the polygraph's utility remains. Some of the polygraph's effectiveness may be linked to examinees' expectations where the examinees confess to misconduct or corruption because of their belief in the power of the exam.

CBP pre-employment examinees admitted to a wide range of illicit activity during their polygraph examinations. Examinees admitted to seeking a job with CBP simply to commit crimes. Other examinees admitted to being involved in drug smuggling or excessive use of illegal drugs. One applicant admitted that a drug smuggler, who was also his brother-in-law, asked him to gain employment with CBP and assist him with cocaine smuggling.[83] A different applicant admitted he used marijuana 9,000 times, to include the night before his polygraph.[84] The same applicant admitted to using cocaine 30 to 40 times,

[77] Jerry D. Yocom, "An Assessment of the Validity of Polygraph Examinations for the Psychophysiological Detection of Deception: A Judicial Opinion and Research Study Review," *Journal of Police and Criminal Psychology* 22, no. 2 (November 27, 2007): 113–119.

[78] "Lie Detection: The Science and Development of the Polygraph," Illumin, accessed August 7, 2017, http://illumin.usc.edu/43/lie-detection-the-science-and-development-of-the-polygraph/.

[79] David C. Raskin, Charles R. Honts, and John C. Kircher, eds., *Credibility Assessment: Scientific Research and Applications* (Cambridge, MA: Academic Press, 2013), 4.

[80] Yocom, "An Assessment of the Validity of Polygraph Examinations," 115.

[81] Illumin, "Lie Detection: The Science and Development of the Polygraph."

[82] Yocom, "An Assessment of the Validity of Polygraph Examinations," 116.

[83] Government Accountability Office, *Border Security*, 17.

[84] Government Accountability Office, 17.

using hallucinogenic mushrooms on 15 occasions, and using ecstasy approximately 50 times.[85] In this sense, polygraphs have a positive role in the screening process.

Admission during pre-employment polygraph testing underscores the importance of polygraph examinations to ensure persons with a history of illicit activity looking to gain employment simply to commit crimes are removed from the CBP applicant pool. The polygraph is an important investigative tool used to verify whether applicants were untruthful, omitted information, or blatantly lied to background investigators regarding their criminal history, involvement in illicit activity, or disciplinary issues with previous employers.[86] However, polygraph examinations for incumbent employees are reactive and not proactive. Even as proposed by the Anti-Border Corruption Act of 2010, it only requires polygraph examinations during the employee's five-year periodic reinvestigation. Therefore, if an employee engages in corruption immediately after a periodic reinvestigation, the employee arguably has five years to engage in illicit activities and act unhindered until the next polygraph examination.

Conversely, challenges exist with expanding CBP's polygraph program. The first challenge with implementing such a program is CBP's bargaining units. CBP's bargaining units are comprised of the National Border Patrol Council (NBPC) and the National Treasury Employee Union (NTEU). Even though the unions cannot affect the agency's security operations, negotiating is required when an employee's established working conditions are changed. Since most uniformed CBP employees do not hold a secret or top-secret security clearance, they are eligible to become union members. Therefore, a new procedure, such as adding a polygraph exam to a periodic re-investigation, generally requires negotiation with the bargaining units either unless or until the Anti-Border Corruption Act of 2010 is enacted into law. Contract negotiations with the NBPC and NTEU will more than likely be tedious, lengthy, and expensive, which makes incumbent polygraph examinations an undesirable option.

[85] Government Accountability Office, 17.

[86] Government Accountability Office, 17.

The second challenge is the size of the CBP polygraph unit. CBP does not have the number of polygraph examiners necessary to continue 100 percent pre-employment testing and begin testing incumbent employees. CBP would have to hire enough polygraph examiners to conduct both pre-employment and incumbent testing, but that is prohibitively expensive because of additional salary requirements, polygraph equipment for new examiners, either negotiation or modification to existing union contracts, and either added office workspace or testing locations.[87] Therefore, depending solely on periodic polygraph examinations as the only proactive anticorruption mitigation strategy is unsound.

B. PATH FORWARD

Evidence has demonstrated that criminal corruption and misconduct within the CBP ranks pose a threat to the homeland security enterprise. The American public deserves a border agency free of corrupt officers and agents because the country relies on the legitimate trade and travel facilitated by CBP. CBP steps to mitigate criminal corruption and misconduct within its ranks include implementing pre-employment polygraph examinations, ensuring five-year incumbent employee reinvestigations are completed in a timely manner, and hiring more professional responsibility (IA) criminal investigators. These implementations highlight the threats posed by compromised CBP officers and agents in both front line and management positions. In the past, Americans envisioned border security personnel as hard working, understaffed, and under-resourced federal agents working diligently to combat drug trafficking and alien smuggling organizations.

Despite improvements in the hiring process, CBP still faces challenges with incumbent employee corruption and misconduct. Currently, the only proactive tools available to CBP to screen incumbent employees are periodic five-year reinvestigations and random drug testing. However, CBP randomly drug tests only 10 percent of employees in designated law enforcement positions.[88] Even though a positive drug test does not indicate corruption, it does indicate potential egregious misconduct. A continuous proactive approach combatting corruption and misconduct that does not require a five-year

[87] Government Accountability Office, 22.

[88] Government Accountability Office, 19.

hiatus between screenings is necessary. Implementing an ongoing proactive all-encompassing approach provides a better opportunity to mitigate corruption and misconduct within the CBP ranks.

Tools are available to monitor employee behavior and conduct continually. Two exceptional programs studied in this thesis are the Crime Stoppers model and the NYPD VAP. The Crime Stoppers program monetarily rewards persons who provide information to law enforcement that leads to the arrest and prosecution of criminals. The VAP is comprised of front line employees who observe and report corruption and misconduct to IA investigators. VAP participants leverage their unfettered access to the frontline workforce to provide information to IA. The combination of these two exceptional programs follows a motivation theory known as the carrot and stick approach. The carrot and stick approach is a motivational theory that elicits desired behaviors or induces cooperation by providing either incentives (rewards) or punishment.[89] The following chapters discuss each program in depth.

[89] *Merriam-Webster*, s.v. "definition of carrot-and-stick," accessed December 11, 2020, https://www.merriam-webster.com/dictionary/carrot-and-stick.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDY A: CRIME STOPPERS

This chapter examines the aspects of the Crime Stoppers program including its benefits and possible drawbacks to derive lessons learned for CBP. Crime Stoppers was examined because it is an incentive program that encourages persons to report crime while allowing them to maintain anonymity. The chapter also argues that offering incentives to report crimes is an effective tool that has been used for centuries all around the world and still used to this day in the United States, such as the False Claims Act and programs instituted by the Internal Revenue Service and the Securities Exchange Commission.[90] Offering rewards or some type of compensation for information on crimes committed against a person or a business is as old as written history.

Money has a value beyond being an exchange of value, but for symbolic reasons. Tool theory argues that humans see money as a "tool" in a metaphorical sense and will use time and effort to collect such a "tool."[91] Explained differently, humans are the only species that incentivizes obtaining modern objects, such as televisions, newspapers, books, etc. Humans obtain those items not because they are necessary to survival, but also for their informational value. Therefore, money when thought of as a tool is a means to increase knowledge by gathering information about the environment, which humans use to their benefit. Information allows people to exchange resources efficiently and is a means to an end. Tool theory also argues that money can be used as a social display, for social communication, and social protection extending the range of this "tool."[92] In addition to using money as a tool, research finds that having money makes humans feel strong and

[90] Marsha J. Ferziger and Daniel G. Currell, "Snitching for Dollars: The Economics and Public Policy of Federal Civil Bounty Programs," *University of Illinois Law Review* 1999, no. 4 (September 22, 1999): 1–4.

[91] Lea and Webley, "Money as Tool, Money as Drug," 163.

[92] Lea and Webley, 163.

self-sufficient.[93] A stronger and more self-sufficient person will arguably allow for more personal growth and better decision making.

A. INTRODUCTION

The Crime Stoppers organization did not begin as an organization that offered money for information, but because of public reluctance to provide information about crimes for a variety of reasons, the organization quickly came to offer money in exchange for information. Police Officer Greg MacAleese of Albuquerque, New Mexico founded Crime Stoppers in 1976.[94] Officer MacAleese's program was not the first program to offer monetary incentives and anonymity for information regarding crimes, but it was the first to feature the media in a central role.[95]

Crime Stoppers came into existence when officer MacAleese was investigating the homicide of Michael Carmen, a gas station attendant. Six weeks after the crime, he was frustrated and had few leads. Officer McAleese contacted a local television manager and proposed that the station air a reenactment of the crime during a newscast; the television manager agreed and broadcasted the first Crime Stoppers spotlight.[96] After this reenactment on the nightly news, a witness called the police department and provided information that led to the apprehension of the two subjects responsible for Carmen's murder.[97] McAleese determined that people were reluctant to provide information regarding criminal events due to fear or apathy. Due to McAleese's concerns, he determined one of Crime Stoppers' tenets would be the reporting party's secrecy and

[93] Kathleen D. Vohs, "The Mere Thought of Money Makes You Feel Less Pain," *Harvard Business Review* 88, no. 3 (March 2010): 28, http://libproxy.nps.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=48219376&site=ehost-live&scope=site.

[94] Walsh, "Crime Stoppers," 122–123.

[95] Rosenbaum, Lurigio, and Lavrakas, "Enhancing Citizen Participation and Solving Serious Crime," 403.

[96] Walsh, "Crime Stoppers," 122–123.

[97] Walsh, 122–123.

anonymity.[98] Another key portion of program was to offer monetary rewards if the information provided led to an arrest.[99]

Crime Stoppers as structured now, is a private, non-profit organization. Citizens are responsible for creating a local Crime Stoppers chapter in accordance with Crime Stoppers International policies and directives.[100] Each local Crime Stoppers organization votes on a board of directors responsible for fundraising, volunteer services, media relations, and law enforcement collaboration.[101] The local board of directors selects volunteers to roles required for the organization to function, such as media relations, community relations, call takers, and a law enforcement coordinator.[102] No publicly available data on required training for volunteer roles was located other than information regarding call takers' requirement to ensure confidentiality and caller anonymity.

Community members anonymously report information regarding crimes through a website on the local Crime Stoppers site or through local or toll-free phone numbers.[103] No personal information is collected from the tipster. The operator gives the tipster a code number to ensure anonymity and to differentiate different tipsters should several leads come in.[104] The code number is auto-generated if the tipster uses a local website to provide information or a locally generated mobile phone application.[105] The secure code number is used for the tipster to receive payment should an arrest occur based on the tipster's information.

Reward sizes are based on a point system. Points vary by the type of crime solved, the number of times the reporting party has provided valid information, the number of

[98] Walsh, 122–123.

[99] Walsh, 122–123.

[100] "Profile," Crime Stoppers USA, accessed August 31, 2020, https://www.crimestoppersusa.org/profile/.

[101] Crime Stoppers USA.

[102] "Media Relations," Crime Stoppers USA, accessed August 31, 2020, https://www.crimestoppersusa.org/profile/media-relations/.

[103] Crime Stoppers USA, "Profile."

[104] Crime Stoppers USA.

[105] Crime Stoppers USA.

persons arrested for that crime, and the value of any recovered or seized items.[106] Additional funds may be available for particular crimes based on donations or rewards offered by other parties for that specific crime.[107] Crime Stoppers focuses on felony crimes and fugitive felons; however, the local board of directors may authorize payment for non-felony crimes.[108]

According to Crime Stoppers International, the Crime Stoppers program is active in 26 countries in North and South America, the Caribbean, Europe, Africa, and the Southern and West Pacific region.[109] Crime Stoppers accepts information regarding fugitive criminals, human trafficking, cybercrime, illicit trade, and environmental crime.[110] As per Crime Stoppers International, cumulative statistics are as follows: 965,163 arrests made, 1,501,776 cases cleared, $2,122,776,681 in property recovered, and $8,976,384,548 in drugs seized.[111] The information provided by Crime Stoppers International is staggering; however, no metric determines how many tipsters contact Crime Stoppers per successful outcome to provide a more nuanced indicator of efficacy. Since Crime Stoppers only shares cumulative statistics, it is not possible to compare their efficacy or clearance rate to law enforcement databases that keep statistical information on crimes committed versus crimes solved.

B. TENETS

The Crime Stoppers model was innovative at the time because it was the first program of its kind to use the media to air reenactments of specific cases, allow the reporting party to remain anonymous, and offer cash rewards for information leading to an arrest. Crime Stoppers has several tenets that make the program successful. The first tenet

[106] "How It Works," Crime Stoppers of Houston, accessed August 31, 2020, https://crime-stoppers.org/our-programs/how-it-works.

[107] Crime Stoppers of Houston.

[108] Crime Stoppers of Houston.

[109] "Regions," Crime Stoppers International, accessed October 8, 2018, https://csiworld.org/regions.

[110] "Crime Areas," Crime Stoppers International, accessed October 8, 2018, https://csiworld.org/crime-areas.

[111] Crime Stoppers International.

is anonymity.[112] Why do people fail to report crime? Witnesses and victims themselves fail to report crime because of fear, feelings of powerlessness, and concern of further victimization.[113] The most common reason victims do not report crime because they believe the crime did not warrant police intervention, but others do not report crimes because they fear the police themselves.[114] Crime Stoppers anonymity was a novel approach because it severs the link between the caller and the police and thereby eliminates any fears of retribution should the criminal face arrest and incarceration. By allowing all reporting parties to remain anonymous, Crime Stoppers also removes the stigma of "snitching" and the fear associated with providing information directly to law enforcement. Crime Stoppers does not make caller data available. It is unknown whether some callers are anonymous callers who provide no information to this confidential program; all callers are given an identification number that does not contain any personal information should they wish to claim a reward.

The second tenet is protection against reprisals associated with whistleblowing.[115] A whistleblower does not have the protection of anonymity. Whistleblowers must follow strict procedures and channel complaints through certain oversight mechanisms merely to remain "confidential" without any guarantee that they will remain completely anonymous.[116] Research demonstrates that employees in the private sector believe that reporting misconduct or corruption to superiors will cause harm to their professional lives.[117] When reporting parties provide information to Crime Stoppers, that party does not need to provide the personal information required of a whistleblower. Therefore, the reporting party does not fear reprisals from employers or the criminal element.

[112] Erdwin H. Pfuhl, "Crimestoppers: The Legitimation of Snitching," *Justice Quarterly* 9, no. 3 (September 1992): 506, http://www.tandfonline.com/doi/abs/10.1080/07418829200091501.

[113] Robert F. Kidd and Ellen F. Chayet, "Why Do Victims Fail to Report? The Psychology of Criminal Victimization," *Journal of Social Issues* 40, no. 1 (1984): 39–50.

[114] Carl Levin, "Text—S.20—101st Congress (1989–1990): Whistleblower Protection Act of 1989," 1, last modified April 10, 1989, https://www.congress.gov/bill/101st-congress/senate-bill/20/text.

[115] Pfuhl, "Crimestoppers," 507.

[116] Levin, "Text—S.20," 1.

[117] Lisa Zipparo, "Factors Which Deter Public Officials from Reporting Corruption," *Crime, Law and Social Change* 30, no. 3 (1998): 273–287.

The third tenet is promoting anonymous reporting through incentives, such as monetary rewards.[118] Ordinarily, reporting a crime to law enforcement was seen as an ethical and moral responsibility. Specifically, a person's conscience was considered the driving force to reporting criminal activity or wrongdoing in the workplace. However, as previously discussed, the fear of retribution, further victimization, or reprisal from an employer constrains people from reporting after witnessing crimes or misconduct in the workplace.[119] Balliet et al. indicated that incentives for cooperation encourage people to sacrifice their self-interest, such as fear of reprisal for the collective benefit.[120] Therefore, by offering monetary rewards for information leading to either the apprehension, arrest, or conviction of persons accused of committing a crime, Crime Stoppers mitigates a reporting party's fear of reprisal.

C. PROGRAM SCOPE

Crime Stoppers is a non-profit organization overseen by a supervisory board nominated from each of its seven regions.[121] The seven regions include the United States, Canada, the Caribbean, Bermuda, Latin America, Europe, Australia and New Zealand, the Pacific, and Africa.[122] Three sub-committees are governance, finance and risk, and communications and marketing to support the supervisory board.[123] An advisory council comprised of subject matter experts and leaders from the law enforcement community, legal experts, corporate experts, and academia support the supervisory board and support collaborative efforts.[124] Crime Stoppers collaborates with stakeholders, such as governments, international agencies, global corporations, law enforcement entities, and the

[118] Pfuhl, "Crimestoppers," 507.

[119] John Bone and Dominic Spengler, "Does Reporting Decrease Corruption?" *Journal of Interdisciplinary Economics* 26, no. 1–2 (2014): 162.

[120] Daniel Balliet, Laetitia B. Mulder, and Paul A. M. Van Lange, "Reward, Punishment, and Cooperation: A Meta-Analysis," *Psychological Bulletin* 137, no. 4 (2011): 594.

[121] Crime Stoppers International, "About Us."

[122] Crime Stoppers International, "Regions."

[123] Crime Stoppers International, "About Us."

[124] Crime Stoppers International.

media to bring awareness of either crimes or criminal activity and to garner financial support for rewarding tipsters.[125] This complex organizational structure demonstrates that a crime reporting mechanism works despite governmental, geographic, and cultural differences.

As a worldwide brand, Crime Stoppers is arguably recognized globally in the seven regions in which it operates. The media provide Crime Stoppers information on crime and criminal events to the public free of charge.[126] Due to Crime Stoppers' relationship with the media through local news broadcasts, print, and web-based, the program reaches many viewers of locally syndicated news programs. Finally, due to collaboration with law enforcement entities, the general public has a trusted anonymous gateway to report crimes. It is common to watch a local news program with a Crime Stoppers segment regarding a recent crime offering a reward for information leading to a suspect's arrest and conviction with the ever-important tenet of anonymity. Before Crime Stoppers, no record of a concerted effort existed to provide information on crimes to the general public using news broadcasts with a guarantee that the caller's identity would remain anonymous and the possibility of a reward.

D. PROGRAM EFFICACY

Crime Stopper tenets hold that anonymity and incentives in the form of money encourage citizen participation in fighting crime. Crime Stoppers proponents tout the expansion of the program into a worldwide operation as proof of the program's success. Nonetheless, opponents of the Crime Stoppers program argue that anonymity and incentives promote false reporting. Research indicates that Crime Stoppers is successful at solving violent crimes and property crimes.[127] However, opponents argue that the measure of Crime Stoppers' success rate is cumulative and not a true indicator of the program's

[125] Crime Stoppers International.

[126] Ronald D. Hunter, "Crime Stoppers," in *Encyclopedia of Victimology and Crime Prevention*, ed. Bonnie Fisher and Steven Lab (Thousand Oaks, CA: SAGE Publications, Inc., 2010), 231, http://sk.sagepub.com/reference/victimologyandcrime/n76.xml.

[127] Randy Lippert, "Policing Property and Moral Risk through Promotions, Anonymization and Rewards: Crime Stoppers Revisited," *Social & Legal Studies* 11, no. 4 (December 2002): 475–502, http://journals.sagepub.com/doi/10.1177/096466390201100401.

effectiveness.[128] Cumulative success rate shows the program's effectiveness over a period of time, but it does not show its effectiveness on the clearance rates of crimes reported versus crimes solved. It is difficult to argue that a crime-fighting program that has been in existence since 1976 has not led to the apprehension of criminals and returned property to its rightful owners. Skeptics question whether rewarding reporting parties is the most effective method to garner public participation.[129] Arguably, providing an incentive to report crime may lead to false reports to receive a reward. Thus, the role of incentives for reporting crime remains contentious.

Debatably, the Crime Stoppers model is successful because of the anonymity and monetary incentives the program offers. Nevertheless, the power of money as an incentive and psychological tool also plays a role in why people choose to report crime. Analysis of rewards and incentives in social dilemmas proves that incentives can and do have positive physical and psychological effects. As discussed earlier, money is a psychological tool that confers feelings of self-worth and self-sufficiency.[130] Lea and Webley argue that sociobiological traits lead people to perform a certain act because it confers a selective advantage; these acts conferred a selective advantage in the developmental stages of early homo sapiens, or because the tendency of such an act is a by-product of another tendency that does or did at some time confer an advantage.[131] Following this train of thought, if reporting crime via Crime Stoppers allows for an incentive, the act confers the advantage of receiving money. Studies performed by Vohs, Mead, and Goode demonstrated that money enables people to achieve goals without help from others.[132] The studies found that persons worked for longer periods before requesting assistance when they were reminded

[128] Lippert, 475–502.

[129] Randy K. Lippert and Kevin Walby, "Funnelling through Foundations and Crime Stoppers: How Public Police Create and Span Inter-Organisational Boundaries," *Policing and Society* 27, no. 6 (August 18, 2017): 602–619, https://www.tandfonline.com/doi/full/10.1080/10439463.2017.1341509.

[130] Vohs, "The Mere Thought of Money Makes You Feel Less Pain," 28–29.

[131] Lea and Webley, "Money as Tool, Money as Drug," 161–162.

[132] Kathleen D. Vohs, Nicole L. Mead, and Miranda R. Goode, "The Psychological Consequences of Money," *Science* 314, no. 5802 (November 17, 2006): 1154–1156, http://www.sciencemag.org/cgi/doi/10.1126/science.1132491.

of possible monetary rewards.[133] Research by Zhou, Vohs, and Baumeister found that physical pain can be decreased by merely thinking about money, and that money gives people the ability to deal with setbacks, as well as fulfil their needs because money has the ability to function as a societal resource.[134]

However, monetary rewards do not always yield positive results. For example, monetary rewards could be counterproductive and counterintuitive to human nature and create negative outcomes when rewards are not seen as commensurate to the task.[135] In other words, if a monetary reward is offered for reporting misconduct, but the reward is seen as trivial or inconsequential, the reporting party is less likely to report misconduct in the future. Research regarding the detrimental effects of reward-based systems argues both for and against the system. Eisenberger and Cameron argue the following:

> Our examination of the research literature revealed that (a) detrimental effects of reward occur under highly restricted, easily avoidable conditions; (b) mechanisms of instrumental and classical conditioning are basic for understanding incremental and decremental effects of reward on task motivation; and (c) positive effects of reward on generalized creativity are easily attainable using procedures derived from behavior theory.[136]

In social dilemma studies, incentives undermined autonomy, the motivation to cooperate, and rejection of the incentive.[137] However, the same studies found that manipulation to incentive structures reduced self-interest and can promote higher rates of cooperation.[138] Therefore, changing the incentive structure to suit the reporting party (increase in monetary reward, adherence to local customs, etc.) will promote more cooperation. Likewise, Drug Theory argues that even though money is a metaphorical tool

[133] Vohs, Mead, and Goode, 1154–1156.

[134] Xinyue Zhou, Kathleen D. Vohs, and Roy F. Baumeister, “The Symbolic Power of Money: Reminders of Money Alter Social Distress and Physical Pain,” *Psychological Science* 20, no. 6 (June 2009): 700–706, http://journals.sagepub.com/doi/10.1111/j.1467-9280.2009.02353.x.

[135] Balliet, Mulder, and Van Lange, “Reward, Punishment, and Cooperation,” 594–595.

[136] Robert Eisenberger and Judy Cameron, “Detrimental Effects of Reward: Reality or Myth?” *American Psychologist* 51, no. 11 (1996): 1154–1156.

[137] Paul A. M. Van Lange, Bettina Rockenbach, and Toshio Yamagishi, *Reward and Punishment in Social Dilemmas* (Oxford: Oxford University Press, 2014), 35, ProQuest Ebook Central.

[138] Van Lange, Rockenbach, and Yamagishi, 35.

(Tool Theory), because of the psychological and physical effects money has on a person, it can also be seen as a drug.[139] Debatably, a drug addiction may lead to negative effects, such as lying, stealing, and dishonesty without the proper treatment. Therefore, the synthesis of the research indicates that incentives are positive tools, and that any negative effects the incentives may have can be avoided by using proven psychological theories, such as behavior, tool, and drug theories.

Crime Stoppers appears to be an effective tool in allowing the general public to provide information to law enforcement entities. Can the Crime Stoppers model mitigate corruption or insider threats within the law enforcement environment? Traditional insider threat mitigation strategies employ disincentives to compel employees to act in the best interests of the organization. However, when relied on excessively, disincentives can lower morale and cause unintended consequences because employees only expect negative outcomes for their actions. Positive incentives, such as the Crime Stoppers model encourages employees by extrinsically, through rewards, or intrinsically, by fostering commitment, to act in the best interests of the organization. Although research regarding active incentive programs in law enforcement organizations is not publicly available, research does exist regarding incentive programs targeting the mitigation of corruption.

Empirical studies demonstrate that officials refrain from reporting people attempting to bribe them because of a lack of evidence, a lack of protection, personal disconnection, or a fear of negative repercussions.[140] Bone and Spengler argue that employees will not report attempted bribes without a reward (or an insufficiently large reward) and that employees will report an attempted bribe if the reward for reporting was greater than the simplicity of merely not reporting the attempted bribe.[141] Bone and Spengler's study conducted studies where participants played the role of an inspector where the inspector had the opportunity to report an attempted bribery or merely ignore the attempted bribe. They found that when the reporting mechanism was cumbersome and time

[139] Lea and Webley, "Money as Tool, Money as Drug," 194–195.

[140] Bone and Spengler, "Does Reporting Decrease Corruption?" 166.

[141] Bone and Spengler, 179–180.

consuming, the inspectors were less likely to report the attempted bribe. Conversely, they found that as the reporting becomes more profitable, the inspectors were more likely to report the attempted bribe. Moore et al. argue that employees who feel engaged, have organizational support, and feel connected at work, are more prone to report corruption.[142] Moore's study suggests that negative incentives (punishment) that force employees to act in the interest of the organization do not increase the likelihood that an employee will report corruption. Positive reinforcements, on the other hand, encourage employees to act in the interest of the organization extrinsically (with incentives) or intrinsically (fostering a sense of commitment). That is not to say that officials will not report corruption or misconduct without incentives. A study of the Philadelphia Police Department found that survey respondents stated they were more prone to report misconduct when the corrupt act had a deep negative ethical impact.[143] However, the study also found that officers lacked consensus regarding their personal code of ethics and the ethical violations the officers perceived as trivial.[144] Furthermore, corrupt officers generally blame the system for their cynicism and misconduct.[145] Therefore, employees arguably require a prompt or push to report misconduct especially with a lack of consensus of what is a reportable offense. Incentive programs provide that prompt or push.

Recommendations to reduce employee theft and misconduct generally include the following tenets: screen potential employees, create an ethical organizational culture, remove temptations, and punish theft and reward honesty.[146] Literature on employee theft identifies deviant behavior (clinical psychology), poor employee screening (industrial psychology), vices, such as gambling (criminology), inadequate security controls (security), and work group norms (organizational science), as some of the causes of either

[142] Andrew P. Moore et al., *The Critical Role of Positive Incentives for Reducing Insider Threats*, CMU/SEI-2016-TR-014 (London: Figshare, 2018), 1–2, http://dx.doi.org/10.1184/R1/6585104.

[143] Vedat Kargin, *Peer Reporting of Unethical Police Behavior* (El Paso, TX: Scholarly Publishing LLC, 2010), 104, ProQuest EBook Central.

[144] Kargin, 128.

[145] Edwin J. Delattre and David R. Bores, *Character and Cops: Ethics in Policing* (Washington, DC: AEI Press, 2011), ProQuest EBook Central.

[146] William I. Sauser, "Employee Theft: Who, How, Why, and What Can Be Done," *S.A.M. Advanced Management Journal* 72, no. 3 (Summer 2007): 13–25, ProQuest.

employee corruption or misconduct.[147] However, literature does not provide insight into how misconduct can be entirely prevented.

Social psychology research indicates that those who give rewards are viewed more favorably than those who punish.[148] Arguably, if employees view their employers in a positive light, they are more likely to report either misconduct or corruption, and if employees view their employers in a negative light, they are less likely to report. Employee levels of moral and ethical outrage determine whether an employee will report corruption or misconduct. When employees have a low level of moral and ethical outrage to certain acts, financial incentives might be more likely to motivate the reporting of corruption or misconduct.[149] In other words, when employees perceive the act (criminal or misconduct) as insignificant, monetary incentives play a decisive factor in reporting the alleged act. The challenge managers and leaders have is to determine the price tag necessary to persuade employees to report corruption and misconduct. If an adequate incentive amount satisfies the employee and management, money-priming theory hypothesizes that presenting money will make employees work harder and arguably report more misconduct.[150] Psychological motivation to report corruption increases as the monetary reward does.[151] Conversely, money-priming theory also speculates that money reduces the concern employees have for others.[152] Employers must take into account that some employees may actually report less because of a holier-than-thou effect in which an employee feels that a moral compass must

[147] Sauser, 20–22.

[148] Kyle Irwin, Laetitia Mulder, and Brent Simpson, "The Detrimental Effects of Sanctions on Intragroup Trust: Comparing Punishments and Rewards," *Social Psychology Quarterly* 77, no. 3 (2014): 253–272.

[149] Yuval Feldman, and Orly Lobel, "The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegally," *Texas Law Review* 88, no. 6 (May 2010): 1207.

[150] Jeremy M. Beus and Daniel S. Whitman, "Almighty Dollar or Root of All Evil? Testing the Effects of Money on Workplace Behavior," *Journal of Management* 43, no. 7 (2017): 2147–2167.

[151] Feldman and Lobel, "The Incentives Matrix," 1207.

[152] Beus and Whitman, "Almighty Dollar," 2147.

be ethically and not financially driven.[153] Therefore, employers must understand the importance of monetary incentives and the employees' decision to report.

It must be emphasized that no definitive profile for malicious insiders exists.[154] Since no malicious insider profile exists, positive incentive strategies, such as providing money for information regarding insider threats, must be considered as a viable option for law enforcement entities. As previously discussed, punishment systems undermine employee trust in the organization. Trust is associated with group solidarity, commitment, and social identification.[155] However, not every employee trusts the organization regardless of the organization's design. Some employees who do not trust the organization are not inclined to cooperate and act detrimentally to the organization unless sanctions are actually implemented.[156] A proactive internal method to identify such employees is necessary.

E. A HYPOTHETICAL APPLICATION OF CRIME STOPPERS TO CBP

This hypothetical scenario of how a program, such as Crime Stoppers, would work in CBP is loosely based on the author's experience in investigating a CBP employee for corruption:

A group of CBP employees engages in corrupt activities, such as allowing narcotics to enter illegally between the POEs along the southwest border. The employees also sell intelligence reports and border fence keys that allow access through the border barrier to drug trafficking organizations. Other employees notice the corrupt employees' odd behavior, such as not working in their assigned areas, working alone despite being assigned partners, or disappearing and being unaccounted for during their scheduled work shift. Employees notice unusual increased spending habits for the salary the employees earn, but

[153] Feldman and Lobel, "The Incentives Matrix," 1207.

[154] Erika C. Leach, "A Review of the United States Air Force's Current Posture" (master's thesis, Air Force Institute of Technology, 2009), 162.

[155] Irwin, Mulder, and Simpson, "The Detrimental Effects of Sanctions on Intragroup Trust," 254.

[156] Welmer E. Molenmaker, Erik W. de Kwaadsteniet, and Eric van Dijk, "On the Willingness to Costly Reward Cooperation and Punish Non-Cooperation: The Moderating Role of Type of Social Dilemma," *Organizational Behavior and Human Decision Processes* 125, no. 2 (2014): 175–183.

not exorbitant enough to draw management’s attention. Employees are concerned, but do not want to report the actions of the corrupt employees overtly because they have not witnessed any illicit activity first-hand. Employees also do not want to report the actions of the corrupt employees overtly because if they are mistaken, they will live with the stigma of being an informant for the rest of their careers.

In the aforementioned scenario, a tipster working in the same area arguably would have noticed the corrupt employees’ odd behavior or may have first-hand knowledge regarding criminal activity. The tipster would report this knowledge through either the anonymous telephone number or website available to tipsters without fear of reprisal. The tipster earns an incentive award as dictated by CBP for reporting corruption. Alternatively, as in this hypothetical case, a year-long investigation could have ended much sooner with less illicit activity if a tipster provided information leading to the corrupt employees’ arrest. All this hypothetical intelligence combined with investigative techniques arguably would have directed investigators to the corrupt employees.

F. CONCLUSION

This chapter discussed incentive techniques that could be applied to encourage employees to report corruption and misconduct while allowing the reporting party to remain anonymous. Tenets of an innovative and successful incentive program, such as anonymity for the informant, protection against reprisals, monetary incentives (rewards), and directly providing information to authority figures, were described and discussed. Analysis of rewards and incentives in social dilemmas and other psychological studies demonstrated that human behavior leads people to perform certain acts because it is beneficial or advantageous. Discussing monetary incentives in particular, research revealed that humans see money as a tool that is a means to increase knowledge while at the same time making people feel strong and self-sufficient. Research also suggested that even when discussing the detrimental effects of a reward-based system, arguments both support and challenge such a system. This same research determined that the detrimental effects of a reward system could be avoided by understanding the effects of rewards on motivation through behavior theory.

Lastly, the chapter discussed malicious insider profiles. Research determined no conclusive profile existed to detect malicious insiders proactively. Research also determined that incentive-based reporting systems increased the reporting of corruption. However, employees willing to report insider threats may not always be in a position where they witness corrupt acts. Therefore, an additional tactic to obtain information is critical to mitigating insider threats. One innovative approach to obtaining information directly from employees is the NYPD's VAP.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDY B: NEW YORK POLICE DEPARTMENT VOLUNTARY ASSISTANCE PROGRAM

This chapter examines the aspects of the NYPD's VAP and its adaptation for CBP. The VAP was examined because it is an innovative proactive intelligence gathering and anti-corruption program. The program allows firsthand employee involvement in the agency's anti-corruption strategy and gives CBP an additional tool to mitigate corruption and misconduct.

A. INTRODUCTION

The NYPD has experienced numerous scandals and corruption allegations. Cycles of scandals, corruption, and reform have rocked the NYPD from as early as 1894. After a major scandal, the NYPD typically sets up a committee to determine the cause and recommend a path forward. The Lexow Committee of 1894, the Curran Committee of 1913, the Seabury Committee of 1930, the Harry Gross investigation of 1950, the Knapp Commission of 1971, and the Mollen Commission of 1992, are all examples of investigative committees and commissions that delved into corruption at the NYPD.[157] Most agree that the two most memorable corruption investigations faced by the NYPD were the Knapp Commission and the Mollen Commission.

Frank Serpico was a NYPD officer in the late 1960s and 1970s. Frustrated that senior NYPD staff did not investigate his allegations of widespread police corruption, Serpico took his story to *The New York Times*.[158] The paper subsequently published a series of articles regarding Serpico's allegations that caused John Lindsay, the then-mayor of New York City, to appoint a committee to investigate the allegations.[159] The committee quickly realized the scope of the investigation was massive and requested that Mayor Lindsay appoint a full-time commission to conduct the investigation. In May 1970, Lindsay

[157] Baer and Armao, "The Mollen Commission Report," 1.

[158] Richard J. Condon, "The Investigation of Police Corruption in New York City," *The Police Journal: Theory, Practice and Principles* 55, no. 3 (July 1982): 208–218, http://journals.sagepub.com/doi/10.1177/0032258X8205500303.

[159] Condon, 208–218.

created the Commission to Investigate Allegations of Police Corruption and the City's Anti-Corruption Procedures, also known as the Knapp Commission, after its chairman, Whitman Knapp.[160]

The Knapp Commission concluded its investigation in December 1972 and found pervasive and well-organized corruption in the NYPD.[161] At the conclusion of the investigation, the *Knapp Commission Report on Police Corruption* indicated that many officers provided the commission information only after they were assured that their identities would not be revealed to the NYPD.[162] *The Knapp Commission Report* recommended restructuring NYPD's IA department in conjunction with anticorruption and management policies and practice to mitigate organized corruption.[163] Other recommendations made by the Knapp Commission included eliminating situations that expose police to corruption and controlling exposure where the hazards are unavoidable. Additional recommendations were to ensure that the public and the police were subject to significant risks of detection, apprehension, conviction, and penalties if engaged in corruption, to increase incentives for meritorious police performance, to change police culture toward corruption, and to generate a climate of reform supported by the public.[164] To address the officers' concerns regarding anonymity and providing information to the commission, the NYPD created an innovative unit to give volunteer officers an opportunity to report corruption while shielding their identities from all but a few trusted managers.[165] The unit, which proactively combatted police corruption through intelligence gathering, was initially called the Field Associates Program and later renamed the VAP.[166] Field Associates were members of the Public Morals or Narcotics Divisions (plainclothes units)

[160] Condon, 208–218.

[161] George Braziller, *The Knapp Commission Report on Police Corruption* (New York: The Knapp Commission, 1972), 1.

[162] Jeffrey Liss, email message to author, November 6, 2018.

[163] Braziller, *The Knapp Commission Report*, 13–16.

[164] Braziller, 18–23.

[165] Jeffrey Liss, email message to author, November 6, 2018.

[166] Braziller, *The Knapp Commission Report*, 214.

who volunteered to report evidence of misconduct to the precursor of the IAB, the Field Control Division.[167]

However, the Knapp Commission's policies and practices did not evolve over time to combat new and innovative corruption trends. In May 1992, approximately 20 years after the Knapp Commission, Suffolk County, NY police arrested Michael Dowd and five other NYPD officers for participating in a conspiracy to sell narcotics.[168] Dowd and his co-conspirators, known as the "Seven Five" (for the 75th precinct where they worked) became arguably the second-most famous corruption investigation in the NYPD's history. Shortly after Dowd's arrest, the press disclosed that Dowd had been the subject of more than 15 corruption allegations over the previous six years.[169] However, the NYPD had substantiated none of the allegations, even though evidence proved Dowd's involvement in criminal activity.[170] Arguably, the allegations against Dowd were not substantiated because of corruption within the NYPD itself and because the NYPD was unable or unwilling to police itself. Therefore, in July 1992, David N. Dinkins, the then-mayor of New York City, established the Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, also known as the Mollen Commission, after chairman Judge Milton Mollen, to again investigate corruption within the NYPD.[171]

The Mollen Commission issued a report of its findings with recommendations in July 1994. This report proposed over 100 recommendations, including changes in police culture and management, recruiting and hiring standards, internal investigations, increased

[167] Braziller, 213–218.

[168] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, *Anatomy of Failure: A Path for Success (The Mollen Commission Report)* (New York City: City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 1994), 23.

[169] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 215.

[170] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 215.

[171] Joe Pascarella, "The Mollen Commission," in *Encyclopedia of Law Enforcement*, ed. Larry E. Sullivan et al. (Thousand Oaks, CA: SAGE, 2004), 291–93, http://sk.sagepub.com/reference/lawenforcement/n116.xml.

deterrence and sanctions, and community outreach.[172] It found a culture within the NYPD that favored ignoring corruption because acknowledging it might reflect poorly on management.[173] It further determined that without a change in culture, no reforms, regardless of how well structured, would mitigate corruption in the NYPD. The Mollen Commission recommended a dual-prong approach to cultivate integrity within the ranks of the NYPD. The focus of the first prong was on the NYPD's internal policies and operations.[174] The second prong focused on creating an independent body that monitored NYPD activity.[175] The recommendations argued the changes would improve the NYPD's culture and improve integrity by mitigating current cultural norms that would otherwise go unchecked.

The Mollen Commission recommended that the IAB proactively begin investigations based on intelligence and analysis instead of relying on a reactive, complaint-driven approach.[176] One of the proactive approaches to mitigating corruption recommended bolstering the VAP and placing it under the direct control of the IAB deputy commissioner. The VAP was directed to recruit a unit of officers in the most corruption-prone precincts who would work as VAP informants.[177] These officers, working undercover for the VAP, would gather information regarding corruption and provide sufficient cause to conduct integrity tests, surveillance, or other proactive investigative activity as necessary to prove or disprove illicit officer activity.[178]

[172] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, *Anatomy of Failure*, 110–111.

[173] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 225.

[174] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 110.

[175] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 110.

[176] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 140.

[177] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 140.

[178] City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 140.

B. TENETS

As in its inception following the Knapp Commission, the VAP remains a support unit within the IAB. Today's VAP continues to function as an intelligence-gathering unit rather than an investigations unit. Although VAP members are encouraged to report misconduct they observe proactively, IAB investigative units rely on the VAP for information or intelligence regarding ongoing IAB investigations. VAP agent coordinators, as the VAP detectives (handlers) are known, solicit information from their field agents during regular meetings and regularly receive information when the field agent observes potential corruption or misconduct. However, an additional and equally important VAP function is to obtain specific information requested from IAB investigators. VAP members provide IAB investigators with information that likely could not be obtained by other investigative means, such as character assessments, secondary or unknown cellular phone numbers, subject associates, financial issues, or specific information regarding an individual or incident. Investigative tools include character assessments, or assessments generated through an analysis of known character traits and actions, secondary or unknown cellular phone numbers, or phone numbers kept by employees without the employer's knowledge, subject associates, or persons of interest or persons with known criminal histories who associate with the employee, financial issues, or known financial issues the employee may have, and lastly, specific information regarding an incident, or specific knowledge or involvement an employee may have regarding a topic of interest to the employer.

C. ANONYMITY

Anonymity is another tenet of the VAP. The only persons with knowledge of VAP participant identities are their respective IAB handlers and the supervisory officers of the IAB agent coordinators or handlers. VAP participants do not know the identity of other VAP participants and thus cannot reveal their participation in the program to anyone. Each VAP participant receives a cellular phone with no paper trail leading back to the NYPD. Only the IAB handlers know the cellular phone number issued to their VAP participants. Secrecy and anonymity are keys to the success of the VAP. Although police databases are arguably secure, an insider threat with hacking abilities, or a non-employee who is an experienced hacker, can breach police databases and discover the identity of VAP participants. Research conducted by the Defense PERSEREC on documented insider threats revealed that hacking into databases was alarmingly common.[179] Authors of intelligence and counter-intelligence works note the increasing challenge to avoid leaving digital traces when purchasing and using electronic devices.[180] Therefore, tight controls, such as cellular phone numbers with no links to the NYPD, no knowledge of participants' identities by other participants, and strict anonymity protocols decrease the likelihood of identification by insider saboteurs. However, all NYPD officers know that the VAP exists as a support unit for the IAB; the threat of exposure if an officer engages in corrupt activity arguably acts as a deterrent.

D. PROGRAM SCOPE

Based on the recommendations from the Mollen Commission, the VAP evolved into the program that it is today, which is to gather and disseminate information regarding NYPD officers who may be engaged in corruption or other serious misconduct as requested by IAB investigators.[181] One particular study of NYPD police misconduct argued that a higher level of deviance among officers existed among a more vulnerable population, such as in a higher crime rate area.[182] In other words, misconduct and corruption more commonly happen among vulnerable populations where officers believe or residents lack the means, or the desire to report misconduct and corruption, given it is the same police that "protect" them. However, effectively predicting which employees will engage in corruption or other types of serious misconduct is challenging. To date, no research demonstrates the effectiveness of predictive modeling in pinpointing which employees will

[179] Eric D. Shaw and Lynn F. Fischer, *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations*, Technical Report 05-13 (Monterey, CA: Defense Personnel Security Research Center, 2005), 39.

[180] Isabelle Duyvesteyn, ed., *The Future of Intelligence*, 1st ed. (London; New York: Routledge, 2015), 152.

[181] Jeffrey Liss, email message to author, November 6, 2018.

[182] Robert J. Kane, "The Social Ecology of Police Misconduct," *Criminology* 40, no. 4 (November 2002): 867–896, http://doi.wiley.com/10.1111/j.1745-9125.2002.tb00976.x.

engage in corruption or misconduct. Psychosocial models incorporating behavioral indicators and word use analysis show some promise.[183] However, word use analysis requires employees' written words (e-mail, reports, texts) or either background or psychological evaluations, which provokes privacy concerns. Even with cause to search employees' e-mails or reports, studies have shown that the majority of insider threats have not been apprehended due to the actions of security personnel or by electronic means, but by their interactions with people.[184] Therefore, person-to-person interaction is key to successfully mitigating insider threats.

Peer-to-peer contact and information gathering will give greater insight to employees who are possible insider threats or engaged in corruption. Insider threats can engage in malicious activity while still appearing to behave legitimately and relevantly.[185] Therefore, contextual information regarding activities performed by insider threats relevant to what they are supposed to be doing will help detect normal versus abnormal behavior. Consequently, having an eyewitness with proper training to identify behavioral indicators that may signal an employee who is at risk for possibly becoming an insider threat is beneficial to any organization.[186] The VAP provides this benefit to the NYPD. Due to the sensitivity of the VAP, a VAP POC provided all information regarding the VAP.[187]

Another benefit to the NYPD is that the VAP is voluntary and not mandatory for any employee. The VAP, as its title implies, is strictly a volunteer program with no extra pay or benefits for the volunteers. VAP participants do earn the ability to apply for sought after assignments after a successful tour of duty. However, by the same token, participating in the VAP does not guarantee any special assignments or duties or rewards. Unfortunately, no information on why volunteers chose to participate in the program was available.

[183] Greitzer et al., "Psychosocial Modeling of Insider Threat Risk," 130.

[184] Puleo, "Mitigating Insider Threat Using Human Behavior Influence Models," 14.

[185] Eugene Santos et al., "Intelligence Analyses and the Insider Threat," *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans* 42, no. 2 (March 2012): 331, http://ieeexplore.ieee.org/document/6006537/.

[186] Sims, "Unauthorized Disclosure," 39–40.

[187] Jeffrey Liss, email message to author, November 6, 2018.

E. PROGRAM EFFICACY

Due to the confidential nature of the VAP, data regarding information provided to the VAP, investigations, and efficacy of the VAP program are strictly confidential. However, the NYPD now generates an annual report titled *Discipline in the NYPD*.[188] Conversely, the overall total number of IAB investigations does not appear in these reports, but the substantiated cases investigated by the IAB do. The years currently available to the public are from 2016 through 2018.

The NYPD defines a substantiated allegation as:

> When an allegation(s) of misconduct against a police officer is investigated and evidence is found to show that the event did occur, that the officer in question engaged in the action, and that the act itself was a violation of department guidelines, the allegation is deemed by the investigator to be 'substantiated.' Substantiated allegations of misconduct against an officer may result in disciplinary action.[189]

Data for 2018 indicated that IAB investigations yielded 303 substantiated allegations against NYPD officers.[190] Of the 303 substantiated allegations, employees with six to 10 years of service accounted for 30% of the employees facing disciplinary charges while employees with 11 to 15 years of service accounted for 27% of employees facing disciplinary charges.[191] The largest percentage of substantiated cases, 47%, was for department rule violations. However, 9% were for firearms violations, 6% were for use of force incidents, 5% were for either unlawful or criminal conduct, 4% were for false statements, 2% were narcotics related, and 1% was for sexual misconduct.[192] Senior or tenured officers were involved in most of the substantiated misconduct or criminal activity.

Data for 2016–2017 yielded similar results for substantiated allegations. The NYPD had 551 substantiated allegations, with employees who were on the job six to 10

[188] "Discipline Reports," NYPD, accessed June 25, 2020, https://www1.nyc.gov/site/nypd/stats/reports-analysis/discipline.page.

[189] NYPD.

[190] NYPD.

[191] NYPD.

[192] NYPD.

years of service accounting for 32% of the employees facing disciplinary charges, and employees with 11 to 15 years of service accounting for 29% of the employees facing disciplinary charges.[193] Similar results were also found regarding the types of substantiated charges. Department rule violations accounted for 35% of the substantiated charges, use of force incidents accounted for 8% of the substantiated charges, false statements accounted for 8%, unlawful or criminal conduct accounted for 7%, firearms charges accounted for 5%, and 1% accounted for narcotics related charges.[194] See Figure 1.

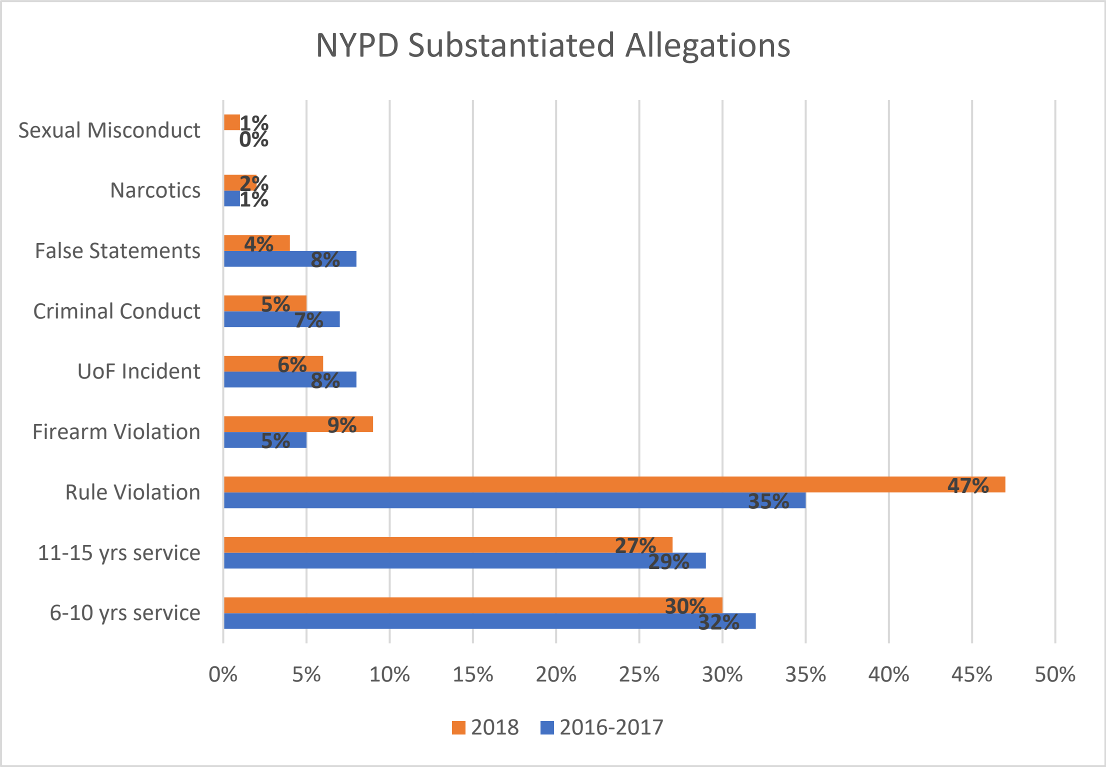

Figure 1. Percentage of Substantiated NYPD Allegations by Type and Years in Service.[195]

[193] NYPD.

[194] NYPD.

[195] Source: NYPD.

Comparatively, CBP had 32,290 total allegations of misconduct between 2006 and 2011 with 3,554 in 2006, 4,343 in 2007, 4,459 in 2008, 5,352 in 2009, 5,746 in 2010, and 5,750 in 2011.[196] Data was not available on how many of the 32,290 misconduct allegations were substantiated. However, if only 25 percent of 32,290 allegations were substantiated, this number would yield a total of 8,072 substantiated allegations, a substantially larger number than the NYPD's totals. Additional research is necessary to determine if CBP's and NYPD's substantiated allegations correlate in any manner, but based on totals alone, CBP appears to have a higher incident of employee misconduct allegations.

The "thin blue line" of police secrecy and reluctance to inform management of misconduct or criminal activity exists in many if not all law enforcement entities. Programs, such as the VAP, provide IA departments, managers, and oversight entities a means to gather information regarding employee corruption and misconduct that may not otherwise be available to them. As outlined in the previous data, a large percentage of senior and or tenured officers engaged in substantiated misconduct or criminal activity. Fellow officers feel reluctant to provide information regarding a senior officer for fear of retribution, without the promise of anonymity.

As demonstrated by the previous data, incumbent employees with six to 15 years accounted for the largest percentage of employees facing either criminal or disciplinary charges in the NYPD from 2016 to 2018. Such employees accused of crimes or misconduct have been on the job for several years and may already have a trusted group of allies or confidants. This factor limits VAP participants' entry into this circle of trust.

VAP participants may have to spend several months or years in a certain station or precinct before they gain the trust of incumbent employees. Arguably, the most obvious challenge is the wariness that incumbent employees have when a newly graduated officer first arrives at a unit or precinct. This wariness is generally overcome in time as the VAP participant works alongside tenured officers on a daily basis. As the VAP participant becomes more familiar with the incumbent officers, the participants can maneuver

[196] Government Accountability Office, *Border Security*, 12.

themselves into a prime intelligence gathering position. Employees monitoring other employees are one of the most effective techniques to identify corruption or other unethical behavior, especially in an organization as large as the NYPD.[197] Therefore, it is extremely important that the newly arrived VAP member be patient and not overly aggressive in joining precinct or unit in-groups without going through the customary "rites of passage." Once the VAP participants are a fixture at the unit or precinct, they generally have unlimited access to intelligence and information that flows freely from employee to employee. The risk of identity spillage is greater if VAP participants force their way into a tight-knit group instead of organically joining. A patient handler and investigative team would more likely discover information regarding the activities of an insider threat. Patience and shrewd tactics must not be overlooked to conduct a hasty investigation without the full integration of the VAP participants into their new roles.

Even though the VAP program provides a valuable additional tool to IAB investigators, the program does have additional challenges. One key challenge faced by the IAB is the misconception held by NYPD staff that VAP members are investigators who conduct self-directed proactive investigations to obtain intelligence or information.[198] Although VAP members are encouraged to report criminality or misconduct to their handlers, such reporting is not their primary role. The VAP participants' primary goal is to be the eyes and ears for the IAB and to provide information they obtain through either their daily activities or work routines. The VAP participants' secondary goal is to obtain information when directed by their IAB handlers on a specific target. VAP members are frontline officers with unprecedented access to in-group activities and conversations that would otherwise be unknown to IAB investigators. Conducting self-directed proactive surveillance or befriending a target they would otherwise not engage with might compromise both the VAP member's identity and safety. However, because of the VAP members' access to other frontline employees, the ability to report changes in employee behavior or discussions regarding planned or previous misconduct cannot be dismissed.

[197] Michael J. Scicchitano et al., "Peer Reporting to Control Employee Theft," *Security Journal* 17, no. 2 (2004): 7–19.

[198] Jeffrey Liss, email message to author, November 6, 2018.

Research into defending against insider threats demonstrated that insider threats generally have observable traits that are reliable markers to future or on-going misconduct.[199] The VAP participants' ability to witness and report these observable traits cannot be underestimated.

Another challenge faced by the VAP is participant retention. A bond built on trust is cultivated between the handler and the participant. When an agent coordinator or handler retires or transfers out of the VAP, participants historically elect to opt-out of the program for fear their identities maybe compromised if they are assigned to either a different coordinator or handler.[200] As per the VAP coordinator, the trust garnered between the participant and the handler through years of working together is difficult to maintain if the handler abruptly leaves the VAP. To combat the exodus of participants when coordinators retire or transfer, the NYPD instituted a policy wherein pending retirement or transfer, the departing coordinators have several face-to-face meetings between the participants and their replacement coordinators.[201] Empirical data demonstrated that the planned transition from one agent coordinator to another aids in participant retention; however, due to the sensitive nature of the program, exact figures were unavailable.[202] However, a policy of this nature may reduce the number of VAP participants who opt out when the agent coordinators retire or transfer.

Research into criminality using intelligence cycles determined that people choose between committing crimes and not committing them if the reward for committing the crime is desirable.[203] In other words, the perceived risk versus reward, or potential consequences, determines the likelihood of engaging in criminality. Hence, if officers believe they can get away with a criminal act or misconduct, the probability of engaging in the activity increases. Additional insider threat research argues that when people realize

[199] Catrantzos, "No Dark Corners," 11–30.

[200] Jeffrey Liss, email message to author, November 6, 2018.

[201] Jeffrey Liss, email message to author, November 6, 2018.

[202] Jeffrey Liss, email message to author, November 6, 2018.

[203] Denis F. O'Leary, "Approaching Career Criminals with an Intelligence Cycle" (master's thesis, Naval Postgraduate School, 2015), 13, http://www.dtic.mil/docs/citations/AD1009185.

that in-group members engage in criminality, they themselves are more likely to engage in that behavior as well.[204] Therefore, an organization that discourages in-group members from engaging in illicit activities by varying means is more likely to foster a culture that discourages such behavior. Since NYPD employees know about the VAP and its participants' anonymity, such awareness heightens the risk versus reward, and thus creates the greater likelihood of being discovered if engaging in criminal or unsavory activity. This increased risk in being discovered by an anonymous source thus lowers an employee's willingness to participate in nefarious activity.

Another risk VAP participants face is social norms that stigmatize informants. Informants who report on employees who have earned their trust are not kindly looked upon. The titles of "rat," "stool pigeon," or "stoolie," are not titles of pride. However, when distancing themselves from the social norms of one group and looking at the greater good of their mission through a different lens, the removal of criminals hiding behind a badge is something VAP participants can take pride in doing. In other words, being part of a unit that engages in corruption is shameful to a serious public servant. This realization does not mean that all will accept the methods used by the VAP, and once again, anonymity is paramount to everyone in the program. Social norms also play a role in decision making by potential offenders. Research regarding social norms indicates that when the probability of apprehension increases, improper conduct is considered less justified.[205] If officers believe in a greater probability of being caught when engaging in improper conduct because of the unknown number of VAP participants, improper conduct is less justifiable, and NYPD officers are less likely to engage in the aforementioned conduct.

[204] Akanksha Vashisth and Avinash Kumar, "Corporate Espionage: The Insider Threat," *Business Information Review* 30, no. 2 (June 2013): 87, http://journals.sagepub.com/doi/10.1177/0266382113491816.

[205] Salima Douhou, Jan R. Magnus, and Arthur van Soest, "Peer Reporting and the Perception of Fairness," *De Economist* 160, no. 3 (September 2012): 289–310, http://link.springer.com/10.1007/s10645-012-9192-y.

F. TRAINING

The process of becoming a VAP member generally begins early in an officer's career. The IAB typically recruits volunteers while the officer is a cadet at the academy, though incumbent officers can also volunteer to be part of the VAP. IAB staff conducts cadet integrity training for cadet classes at the NYPD academy and provides information regarding the VAP during that training. Integrity training includes information regarding corruption hazards, consequences of engaging in corruption or other illicit activities, and a general introduction into the VAP mission. If a cadet expresses interest in the VAP, IAB staff speaks to the cadet individually and a rigorous vetting process begins. If the cadet successfully passes the enhanced vetting process, the cadet receives additional training required to become a VAP participant. Once approved, the VAP participant signs a memorandum of understanding confirming and acknowledging the duties and restrictions of the VAP.[206]

In addition to the VAP, the NYPD receives complaints regarding corruption or misconduct through various means. The public provides complaints regarding employee corruption and misconduct. The Conflicts of Interest Board, an independent city agency, also refers complaints to the NYPD. The Commission to Combat Police Corruption and the Inspector General for the NYPD perform audits, studies, and analyses, and make recommendations regarding policies, programs, and practices. Lastly, all NYPD employees must report corruption and misconduct. However, because VAP participants are anonymous and not known to the rank and file, employees can report corruption or misconduct to their supervisors or directly to the IAB.[207]

G. HYPOTHETICAL SCENARIO

This hypothetical scenario presents how a program, such as the VAP, would work in CBP, using the author's experience in investigating a CBP employee for corruption:

[206] Author requested information from the NYPD regarding insider threats within the VAP. The NYPD VAP Point of Contact (POC) advised that the NYPD constantly monitor participants to ensure they do not engage in illicit activities but did not provide information regarding how participants are monitored.

[207] Jeffrey Liss, email message to author, November 6, 2018.

A group of CBP employees engages in corruption-related activities, such as allowing narcotics to enter illegally between the POEs along the southwest border. The employees also sell intelligence reports and border fence keys that allow access through the border barrier to drug trafficking organizations. Other employees notice the corrupt employees' odd behavior, such as not working in their assigned areas, working alone when assigned partners, or disappearing and being unaccounted for during their scheduled work shift. Employees notice unusual increased spending habits for the salary the employees earn, but not exorbitant enough to draw management's attention. Employees are concerned, but do not want to report the actions of the corrupt employees because they have not witnessed any illicit activity first-hand. Employees do not want to report the actions of the corrupt employees because if they are mistaken, they will live with the stigma of being an informant for the rest of their careers.

In the aforementioned scenario, a VAP participant working in the same area would have noticed the corrupt employees' odd behavior and reported it through the chain of command. Alternatively, as in this hypothetical case, a year-long investigation could have ended much sooner with less illicit activity if a VAP participant were directed to gather intelligence by the IA agents investigating the corrupt employees. The VAP participant would be directed to gather intelligence in this case because of access to the corrupt employees, but also the access of other employees who noticed the odd behavior, spending habits, and discussed the situation among themselves. All this hypothetical intelligence gained through a VAP participant combined with investigative techniques would have directed investigators to the corrupt employees.

H. CONCLUSION

In conclusion, at-risk employee research indicated that managers and co-workers witnessed employees who exhibited signs of stress and disgruntlement among other issues, but do not alert anyone.[208] Alerts were not raised because they are not aware of the severity of the behavior, or due to the fear of reprisal should someone become aware of their

[208] Greitzer et al., *Identifying At-Risk Employees*, iii.

notification. Since VAP members are anonymous rank-and-file officers, noticing suspicious behavior or acquiring such information is highly likely due to their daily interaction with subjects of an IAB investigation. Conversely, empirical studies into the development of insider threats indicate that employees displaying the potential for becoming an insider threat are typically known to their agency's human resource and security offices because of their counterproductive interpersonal behaviors.[209] Research does not indicate whether internal investigations follow, but rather only that the employees are known to management. This chapter found that having employees trained to report changes in behavior or other suspicious activity is essential to ensure that appropriate measures are taken to mitigate misconduct or corruption. The implications for a VAP-type program in CBP include better situational awareness of possible employee corruption and misconduct through first-hand information gathering capabilities. Additionally, employee awareness of a VAP-type program will arguably create an atmosphere where corruption and misconduct are not tolerated.

[209] ErShaw, Fischer, and Rose, *Insider Risk Evaluation and Audit*, 39.

V. MASTER MODEL POLICY

The master model policy for a proactive insider threat mitigation strategy for the CBP would combine elements of incentives and punishments previously discussed. The incentive program could be modeled after the Crime Stoppers program. The incentive program would allow employees to provide information anonymously to CBP management regarding corruption or misconduct with the knowledge that if the information led to an arrest or other pre-determined administrative action against the offending employees, some type of incentive award would be offered to the reporting party. The anonymity tenet of the incentive program encourages participation in a way that openness would not. All employees who contact CBP OPR under the incentive program would do so assured of secrecy and protection of their identity. The employee would receive a unique identifier upon contacting CBP OPR. Only CBP OPR and the employees would know the unique identifier attached to the information provided. Should the information provided by the employees lead to the arrest, apprehension, or discovery of serious employee misconduct, incentive rewards would be offered to the employees. This form of compensation mirrors one of the methods used in other incentive programs, which allows participating employees to maintain complete anonymity. Other options CBP can use include time off awards, which are vacation days awarded to employees that do not diminish the employees' earned vacation days, or quality step increases (QSI), which grant an increase in pay before the normal step increase time increments.

The punishment aspect is a program modeled after the VAP. Prior to implementation of the VAP program, the entire CBP workforce would learn about the VAP through agency-wide notifications via electronic mail and video presentations. The notification would serve a dual purpose. First, the notification would make all employees aware that VAP participants work among them with the goal of encouraging employees to adhere to CBP policies and regulations. Second, the notification would draw attention to the program and possibly garner new participants or new investigatory leads. After such public notifications, CBP OPR personnel would conduct awareness training at the CBP academies.

CBP OPR personnel would provide integrity awareness training to new employees at each of the three basic CBP academies and inform the new employees of the VAP. If any employees express interest in the VAP, the employees would speak to CBP OPR staff individually and undergo additional vetting. If the employees successfully complete the additional vetting, the employees would undergo additional VAP training. Training would be developed prior to the implementation of the VAP to address the duties and responsibilities of every VAP participant. VAP participants would undergo training individually at an undisclosed facility to ensure their anonymity. This training could be done prior to the employees reporting to their duty stations or could be conducted remotely to safeguard the participants' identities. During this training, the VAP participants would be assigned CBP OPR handlers. The CBP OPR handlers and the VAP participants would meet and ensure that a good working relationship is established through rapport building and mentoring. If the CBP OPR handlers and the VAP participants could not work well together, different CBP OPR handlers would be assigned to the VAP participants. It is extremely important that the CBP OPR handlers and the VAP participants gel and work as a team to ensure no miscommunication occurs and the goals of each team member are the same.

Only the CBP OPR handlers and CBP OPR management would know the identities of all VAP participants. After successful vetting and training, the VAP participants would be issued a cellular phone without a paper trail leading to CBP OPR to communicate with the participants' handlers. Only the handlers and CBP OPR management would know the cellular phone numbers assigned to the participants. The participants could not disclose their role in the VAP to any person. The participants' anonymity is paramount for individuals, as well as for program success. Therefore, if the VAP participants' identities were ever compromised, the volunteers could no longer participate in the VAP program.

The CBP OPR VAP would be a strictly volunteer program and would confer no additional pay or benefits outside of the psychological gratification for protecting the agency's mission. All employees who wished to become VAP participants must be completely aware of the lack of monetary benefits that accrue from being a VAP participant. However, consideration after a successful VAP tour of duty would be taken into account for promotions or special assignments but would not guarantee selection. VAP tours of duty would vary on each individual agreement between the participants and CBP OPR. Typically, VAP rotations would range from three to five years; however, the time frame would be extended if CBP OPR and the participants agree on the extension. Justification to extend the contract may include an on-going investigation in which the participants play a crucial role or a relationship between participants and possible targets of pending investigations.

Figure 2 shows a hypothetical hierarchy flow chart with the IOD call center, or the Joint Intake Center (JIC) where the VAP Program Manager reports directly to the OID Executive Director and the VAP participants report to their component for their primary duties and to the VAP Program Manager as their secondary duty. See Figure 2.

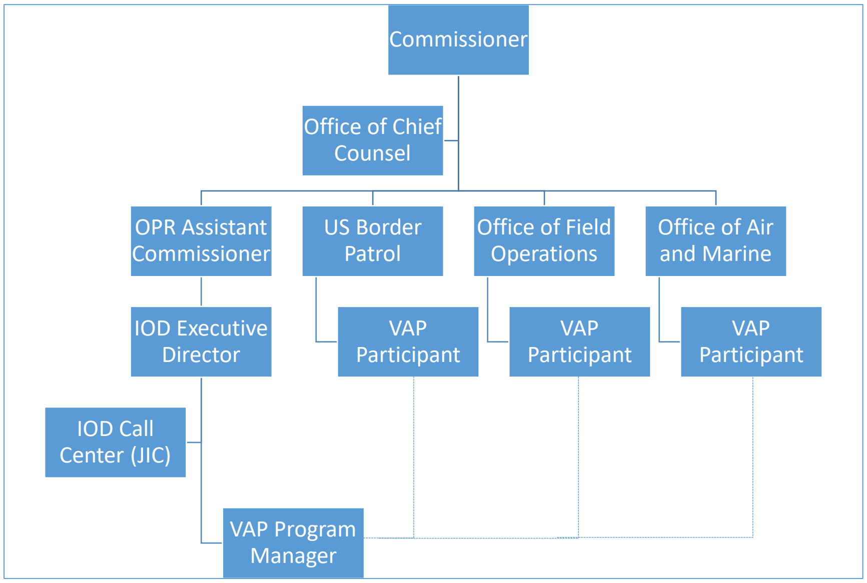

Figure 2. VAP Participant Hierarchy Flow Chart.

A. IMPLEMENTATION

A workgroup consisting of CBP OPR managers, supervisors, and agents would generate a working draft policy implementing the incentive and voluntary assistance programs. The working draft should include related CBP policies, authorities, and standard operating procedures. Once completed by the workgroup, the working draft would be sent to the CBP OPR Special Agents in Charge (SACs) in all OPR areas of responsibility for their review and input. After review and input by field SACs, the working group would re-review the working draft for any necessary edits, deletions, or additions. The CBP Office of Chief Counsel must review the draft policy and provide legal advice to ensure the policy abides by all federal rules, laws, and regulations.

Concurrent to the working draft policy, revamping or updating the integrity training program must be requested from the CBP Office of Training and Development (OTD). The training must include information regarding the proposed incentive program, as well as the voluntary assistance program. The training must meet all required OTD and OPR prerequisites and fall within CBP's National Training Plan of mandated courses for all CBP employees.

Consideration of a temporary trial period, or a field trial, should be considered to ensure proper implementation. An incremental incorporation of the policy along CBP's busiest corridors would offer CBP executive staff an opportunity to review the program's successes and challenges. A field trial would also afford CBP executive staff the opportunity to poll the CBP workforce on the program's efficacy and acceptance.

Prior to the implementation of such a sweeping proactive policy, the project would require approval from the CBP Commissioner, the OPR Assistant Commissioner, and the OPR Investigative Operations Division (IOD) Executive Director. The CBP Office of Chief Counsel and the Office of Labor and Employee Relations must also review and comment on draft policy documents. CBP's field components, such as the U.S. Border Patrol, the Office of Field Operations, and the Office of Air and Marine, should be given the opportunity to review and comment on the proposed policy and training materials.

B. CHALLENGES

Some organizational challenges to changing a complaint-driven approach to a proactive, intelligence-based format have been raised. Ensuring that smart practices and lessons learned from the NYPD VAP be incorporated into the CBP VAP would mitigate miscalculations during the creation and implementation phases. The NYPD, like CBP, has a workforce under a union bargaining agreement. Although bargaining units cannot dictate policy and operations, input and buy-in from the NTEU and NBPC would reduce resistance to the new programs and ensure the efficient implementation of the policy.

Additional challenges include creating a policy that does not contradict current federal laws and employee protections. Since the research evaluated two unique programs not currently used in CBP, research to ensure program implementation in CBP does not either violate federal laws or employee protections is necessary. Coordination with CBP components is also necessary, as it is the component for employees who will participate in both programs. Careful deliberation with the CBP Office of Chief Counsel and Office of Labor Employee Relations during the creation of the new policy must occur. Incorporating a representative from the CBP Office of Chief Counsel and the Office of Labor Employee Relations into the draft phase would decrease the time each office requires to review the final draft policy.

A cost-benefit analysis for both programs should be considered prior to implementation. Additional positions in the JIC, as well as a VAP program manager, may be required. Locating a funding source for the incentive program with funding requirements for future years are also required. No additional positions are required for VAP participants, as the participants are recruited from employees already in CBP. No additional organizational changes are expected and therefore no additional costs for organizational structure modifications are anticipated.

C. CONCLUSION

This research demonstrated that behavioral models have thus far been unable to predict who will become an insider threat. This research found that psychosocial modeling also failed to predict accurately why employees engage in corruption. However, further research in these fields should help to determine whether one model or a combination or models might yield better results in predicting which employees were likely to become insider threats.

This research found that intelligence and information gathering, as well as incentive-based programs, have been used successfully to identify insider threats in a law enforcement environment and to obtain information regarding criminal activity. However, additional research is required to determine whether CBP employees can participate in an incentive-based information program. Some government agencies bar employees from receiving incentives for information acquired through their work in the federal government. Yet, some programs, such as the False Claims Act, and programs instituted by the Internal Revenue Service and the Securities Exchange Commission, do allow certain federal employees to receive monetary rewards for information provided during an investigation.[210] However, the two aforementioned incentive programs are very specific incentive awards programs regarding either IRS fraud or fraudulent claims for payment that do not translate well to reporting criminal activity or misconduct within CBP. Additional research and legal advice into this topic is necessary.

This research aimed to provide CBP executive leadership with options to mitigate insider threats within the agency. This research highlighted two non-traditional but highly innovative options. Rigorous research was conducted to determine the feasibility of implementing such programs in CBP. The research concluded that implementing an incentive-based program and a program similar to the VAP is feasible if no laws bar bargaining unit employees from participating in such programs. Careful coordination with the CBP Office of Chief Counsel would mitigate any hurdles that might delay the implementation of such programs. Based on research on rewards and incentives in social dilemmas and other psychological studies, as well as inability to predict employee behavior scientifically, the author strongly recommends that Homeland Security leaders and practitioners consider adopting these programs or adaptations of them to current efforts and on-going insider threat mitigation programs.

[210] Ferziger and Currell, “Snitching for Dollars,” 1–4.

Research to determine program efficacy and to determine program modifications must be continuous. Additional and continuous research on behavioral models is required to determine if new data becomes available regarding predicting insider threats. Further research is also required on the efficacy of incentive-based programs when utilized in law enforcement agencies. If implemented, continuous review of both programs will be required to track efficacy and make improvements as necessary. Based on research, CBP should expect additional information regarding employee corruption and misconduct as soon as both programs are fully implemented.

Mitigating insider threats in CBP is of utmost importance in safeguarding the integrity of this nation's frontline homeland security enterprise. CBP employees protect America from persons who wish to cause harm while at the same time promoting legitimate trade and travel. One corrupt employee has the ability to cause irreversible damage.

Front line supervisors first protect against insider threats; however, even good supervisors need help maintaining a functioning workforce while at the same time mitigating employee corruption and misconduct. Expecting frontline supervisors to identify every and all employees who may pose an insider threat in a complex work environment is unreasonable. Implementing insider threat mitigation programs will better prepare CBP to identify these troubled employees.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Archibold, Randal C. “Mexican Cartels Look to Turn Border Agents—With Some Success.” *New York Times*. sec. U.S. December 17, 2009. https://www.nytimes.com/2009/12/18/us/18corrupt.html.

Baer, Harold, Jr., and Joseph P. Armao. “The Mollen Commission Report: An Overview.” *New York Law School Law Review* 40 (1995): 1–13.

Balliet, Daniel, Laetitia B. Mulder, and Paul A. M. Van Lange. “Reward, Punishment, and Cooperation: A Meta-Analysis.” *Psychological Bulletin* 137, no. 4 (2011): 594–615.

Beus, Jeremy M., and Daniel S. Whitman. “Almighty Dollar or Root of All Evil? Testing the Effects of Money on Workplace Behavior.” *Journal of Management* 43, no. 7 (2017): 2147–2167.

Bone, John, and Dominic Spengler. “Does Reporting Decrease Corruption?” *Journal of Interdisciplinary Economics* 26, no. 1–2 (2014): 161–186.

Brackney, Richard C., and Robert H. Anderson. *Understanding the Insider Threat: Proceedings of a March 2004 Workshop*. Santa Monica, CA: RAND, 2004.

Braziller, George. *The Knapp Commission Report on Police Corruption*. New York: The Knapp Commission, 1972.

Catrantzos, Nicholas. “No Dark Corners: Defending against Insider Threats to Critical Infrastructure.” Master’s thesis, Naval Postgraduate School, 2009. http://www.dtic.mil/docs/citations/ADA508935.

Ceresola, Ryan G. “The U.S. Government’s Framing of Corruption: A Content Analysis of Public Integrity Section Reports, 1978–2013.” *Crime, Law and Social Change; Dordrecht* 71, no. 1 (February 2019): 47–65. ProQuest.

City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department. *Anatomy of Failure: A Path for Success (The Mollen Commission Report)*. New York City: City of New York Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, 1994.

Claycomb, William R., Carly L. Huth, Lori Flynn, David M. McIntire, and Todd B. Lewellen. *Chronological Examination of Insider Threat Sabotage: Preliminary Observations*. Pittsburgh, PA: Carnegie Mellon University, 2012.

Cole, Eric, and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. 1st. ed. Rockland, MA: Syngress, 2006.

Condon, Richard J. “The Investigation of Police Corruption in New York City.” *The Police Journal: Theory, Practice and Principles* 55, no. 3 (July 1982): 208–218. http://journals.sagepub.com/doi/10.1177/0032258X8205500303.

Crime Stoppers International. “About Us.” Accessed April 7, 2018. https://csiworld.org/about-us.

———. “Crime Areas.” Accessed October 8, 2018. https://csiworld.org/crime-areas.

———. “Regions.” Accessed October 8, 2018. https://csiworld.org/regions.

Crime Stoppers of Houston. “How It Works.” Accessed August 31, 2020. https://crime-stoppers.org/our-programs/how-it-works.

Crime Stoppers USA. “History.” Accessed March 29, 2021. https://www.crimestoppersusa.org/history/.

———. “Media Relations.” Accessed August 31, 2020. https://www.crimestoppersusa.org/profile/media-relations/.

———. “Profile.” Accessed August 31, 2020. https://www.crimestoppersusa.org/profile/.

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

Delattre, Edwin J., and David R. Bores. *Character and Cops: Ethics in Policing*. Washington, DC: AEI Press, 2011. ProQuest EBook Central.

Department of Homeland Security. *U.S. Customs and Border Protection Has Taken Steps to Address Insider Threat, but Challenges Remain*. OIG-13-118. Washington, DC: Office of the Inspector General, 2013. https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-118_Sep13.pdf.

Department of Justice. “Former Background Investigator for Federal Government Pleads Guilty to Making a False Statement.” Accessed August 11, 2017. https://www.justice.gov/usao-dc/pr/former-background-investigator-federal-government-pleads-guilty-making-false-statement-6.

Department of Justice Office of the Inspector General. *Polygraph Examinations in the Department of Justice*. Washington, DC: Department of Justice Office of the Inspector General, 2006. https://oig.justice.gov/reports/plus/e0608/final.pdf.35–107.

Douhou, Salima, Jan R. Magnus, and Arthur van Soest. “Peer Reporting and the Perception of Fairness.” *De Economist* 160, no. 3 (September 2012): 289–310. http://link.springer.com/10.1007/s10645-012-9192-y.

Durbin, Richard. "S.1560—Integrity in Border and Immigration Enforcement Act." Congress.gov. Last modified July 13, 2017. https://www.congress.gov/bill/115th-congress/senate-bill/1560.

Duyvesteyn, Isabelle, ed. *The Future of Intelligence*. 1st ed. London; New York: Routledge, 2015.

Eisenberger, Robert, and Judy Cameron. "Detrimental Effects of Reward: Reality or Myth?" *American Psychologist* 51, no. 11 (1996): 1154–1156.

Feldman, Yuval, and Orly Lobel. "The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegally." *Texas Law Review* 88, no. 6 (May 2010): 1151–1211.

Ferziger, Marsha J., and Daniel G. Currell. "Snitching for Dollars: The Economics and Public Policy of Federal Civil Bounty Programs." *University of Illinois Law Review* 1999, no. 4 (September 22, 1999): 1–69.

Government Accountability Office. *Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct*. GAO-13-59. Washington, DC: Government Accountability Office, 2012. http://www.gao.gov/assets/660/650505.pdf.

GovTrack. "S. 1560: Integrity in Border and Immigration Enforcement Act." Accessed August 7, 2017. https://www.govtrack.us/congress/bills/115/s1560/text.

Grabo, Cynthia, and Jan Goldman. *Handbook of Warning Intelligence: Assessing the Threat to National Security*. 1st ed. Lanham, MD: Scarecrow Press, 2010.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, and Angela C. Dalton. *Identifying At-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats*. Oak Ridge, TX: Office of Science and Technical Information 2010. http://www.osti.gov/servlets/purl/1000159-1JPnC7/.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Christopher R. Brown, and Thomas Ferryman. "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis." *e-Service Journal* 9, no. 1 (2013): 106–138. https://muse.jhu.edu/article/548560/summary.

Homeland Security Advisory Council. *Final Report of the CBP Integrity Advisory Panel*. Washington, DC: Department of Homeland Security, 2016. https://www.dhs.gov/sites/default/files/publications/HSAC%20CBP%20IAP_Final%20Report_FINAL%20(accessible)_0.pdf.

Hunter, Ronald D. "Crime Stoppers." In *Encyclopedia of Victimology and Crime Prevention*, edited by Bonnie Fisher and Steven Lab, 230–233. Thousand Oaks, CA: SAGE Publications, Inc., 2010. http://sk.sagepub.com/reference/victimologyandcrime/n76.xml.

Illumin. "Lie Detection: The Science and Development of the Polygraph." Accessed August 7, 2017. http://illumin.usc.edu/43/lie-detection-the-science-and-development-of-the-polygraph/.

Information Institute. "Public Corruption." Accessed April 12, 2018. https://www.law.cornell.edu/wex/public_corruption.

Irwin, Kyle, Laetitia Mulder, and Brent Simpson. "The Detrimental Effects of Sanctions on Intragroup Trust: Comparing Punishments and Rewards." *Social Psychology Quarterly* 77, no. 3 (2014): 253–272.

Kane, Robert J. "The Social Ecology of Police Misconduct." *Criminology* 40, no. 4 (November 2002): 867–896. http://doi.wiley.com/10.1111/j.1745-9125.2002.tb00976.x.

Kargin, Vedat. *Peer Reporting of Unethical Police Behavior*. El Paso, TX: Scholarly Publishing LLC, 2010. ProQuest EBook Central.

Kidd, Robert F., and Ellen F. Chayet. "Why Do Victims Fail to Report? The Psychology of Criminal Victimization." *Journal of Social Issues* 40, no. 1 (1984): 39–50.

Lea, Stephen E. G., and Paul Webley. "Money as Tool, Money as Drug: The Biological Psychology of a Strong Incentive." *Behavioral and Brain Sciences; New York* 29, no. 2 (April 2006): 161–209. ProQuest.

Leach, Erika C. "A Review of the United States Air Force's Current Posture." Master's thesis, Air Force Institute of Technology, 2009.

Levin, Carl. "Text—S.20—101st Congress (1989–1990): Whistleblower Protection Act of 1989." Last modified April 10, 1989. https://www.congress.gov/bill/101st-congress/senate-bill/20/text.

Lippert, Randy. "Policing Property and Moral Risk through Promotions, Anonymization and Rewards: Crime Stoppers Revisited." *Social & Legal Studies* 11, no. 4 (December 2002): 475–502. http://journals.sagepub.com/doi/10.1177/096466390201100401.

Lippert, Randy K., and Kevin Walby. "Funnelling through Foundations and Crime Stoppers: How Public Police Create and Span Inter-Organisational Boundaries." *Policing and Society* 27, no. 6 (August 18, 2017): 602–619. https://www.tandfonline.com/doi/full/10.1080/10439463.2017.1341509.

Lowenthal, Mark M. *Intelligence; From Secrets to Policy*. 7th ed. Washington, DC: CQ Press, 2016.

Marx, Gary T. "When the Guards Guard Themselves: Undercover Tactics Turned Inward." *Policing and Society* 2, no. 3 (April 1992): 151–172. http://www.tandfonline.com/doi/abs/10.1080/10439463.1992.9964639.

Molenmaker, Welmer E., Erik W. de Kwaadsteniet, and Eric van Dijk. "On the Willingness to Costly Reward Cooperation and Punish Non-Cooperation: The Moderating Role of Type of Social Dilemma." *Organizational Behavior and Human Decision Processes* 125, no. 2 (2014): 175–183.

Moore, Andrew P., Sam Perl, Jennifer Cowley, Matthew L. Collins, Tracy M. Cassidy, Nathan VanHoudnos, and Palma Buttles et al. *The Critical Role of Positive Incentives for Reducing Insider Threats*. CMU/SEI-2016-TR-014. London: Figshare, 2018. http://dx.doi.org/10.1184/R1/6585104.

Nixon, Ron. "The Enemy within: Bribes Bore a Hole in the U.S. Border." *New York Times*. sec. U.S. December 28, 2016. https://www.nytimes.com/2016/12/28/us/homeland-security-border-bribes.html.

NYPD. "Discipline Reports." Accessed June 25, 2020. https://www1.nyc.gov/site/nypd/stats/reports-analysis/discipline.page.

O'Leary, Denis F. "Approaching Career Criminals with an Intelligence Cycle." Master's thesis, Naval Postgraduate School, 2015. http://www.dtic.mil/docs/citations/AD1009185.

Office of National Drug Control Policy (ONDCP). *National Southwest Border Counternarcotics Strategy*. Washington, DC: Office of the President of the United States, 2016. https://obamawhitehouse.archives.gov/sites/default/files/ondcp/policy-and-research/southwest_strategy-3.pdf.

Pascarella, Joe. "The Mollen Commission." In *Encyclopedia of Law Enforcement*, edited by Larry E. Sullivan, Marie Simonetti Rosen, Dorthy Moses Schulz, and M. R. Haberfeld, 291–93. Thousand Oaks, CA: SAGE, 2004. http://sk.sagepub.com/reference/lawenforcement/n116.xml.

Pfuhl, Erdwin H. "Crimestoppers: The Legitimation of Snitching." *Justice Quarterly* 9, no. 3 (September 1992): 505–528. http://www.tandfonline.com/doi/abs/10.1080/07418829200091501.

Potter, Gary. "The History of Policing in the United States." EKU Online. Accessed August 8, 2017. http://plsonline.eku.edu/sites/plsonline.eku.edu/files/the-history-of-policing-in-us.pdf.

Puleo, Anthony J. "Mitigating Insider Threat Using Human Behavior Influence Models." Master's thesis, Air Force Institute of Technology, 2006.

Raff, Jeremy. "The Border Patrol's Corruption Problem." *The Atlantic*, May 5, 2017. https://www.theatlantic.com/politics/archive/2017/05/not-one-bad-apple/525327/.

Raskin, David C., Charles R. Honts, and John C. Kircher, eds. *Credibility Assessment: Scientific Research and Applications*. Cambridge, MA: Academic Press, 2013.

Rosenbaum, Dennis P., Arthur J. Lurigio, and Paul J. Lavrakas. "Enhancing Citizen Participation and Solving Serious Crime: A National Evaluation of Crime Stoppers Programs." *Crime & Delinquency* 35, no. 3 (July 1, 1989): 401–420. https://doi.org/10.1177/0011128789035003006.

Santos, Eugene, Hien Nguyen, Fei Yu, Keum Joo Kim, Deqing Li, John T. Wilkinson, Adam Olson, Jacob Russell, and Brittany Clark. "Intelligence Analyses and the Insider Threat." *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans* 42, no. 2 (March 2012): 331–347. http://ieeexplore.ieee.org/document/6006537/.

Sauser, William I. "Employee Theft: Who, How, Why, and What Can Be Done." *S.A.M. Advanced Management Journal* 72, no. 3 (Summer 2007): 13–25. ProQuest.

Scicchitano, Michael J., Tracy Jones, Read Hayes, and Robert Blackwood. "Peer Reporting to Control Employee Theft." *Security Journal* 17, no. 2 (2004): 7–19.

Shaw, Eric D., and Lynn F. Fischer. *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations*. Technical Report 05–13. Monterey, CA: Defense Personnel Security Research Center, 2005.

Shaw, Eric D., Lynn F. Fischer, and Andrée E. Rose. *Insider Risk Evaluation and Audit*. Technical Report 09–02. Monterey, CA: Defense Personnel Security Research Center, 2009. http://www.dtic.mil/docs/citations/ADA563910.

Sims, Jennifer E., and Burton Gerber, eds. *Transforming U.S. Intelligence*. Washington, DC: Georgetown University Press, 2005.

Sims, Karen E. "Unauthorized Disclosure: Can Behavioral Indicators Help Predict Who Will Commit Unauthorized Disclosure of Classified National Security Information?" Master's thesis, Naval Postgraduate School, 2015.

Stinson, Philip M., John Liederbach, Steven P. Lab, and Steven L. Brewer Jr. *Police Integrity Lost: A Study of Law Enforcement Officers Arrested: Final Technical Report*. Bowling Green, OH: Criminal Justice Program, Department of Human Services, College of Health & Human Services, Bowling Green State University, 2016.

Sulick, Michael J. *American Spies: Espionage against the United States from the Cold War to the Present*. Washington, DC: Georgetown University Press, 2013.

Texas Tribune, The. “Cracks in the Wall: When Border Watchdogs Turn Criminal.” July 7, 2016. https://apps.texastribune.org/bordering-on-insecurity/when-border-watchdogs-turn-criminal/.

Turbiville, Graham H. “Silver over the Border: U.S. Law Enforcement Corruption on the Southwest Border.” *Small Wars & Insurgencies* 22, no. 5 (December 2011): 835–859. http://www.tandfonline.com/doi/abs/10.1080/09592318.2011.620811.

U.S. Congress. House of Representatives. *Keeping Pace with Trade, Travel, and Security: How Does CBP Prioritize and Improve Staffing And Infrastructure?: Hearing before the Subcommittee on Border and Maritime Security*. 114th Cong., 2nd sess., April 19, 2016. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg22756/pdf/CHRG-114hhrg22756.pdf.

U.S. Customs and Border Protection. “Border Patrol Agent Duties.” Accessed November 27, 2017. https://www.cbp.gov/careers/frontline-careers/bpa/duties.

———. *Vision and Strategy 2020*. CBP Publication Number 0215–0315. Washington, DC: Department of Homeland Security, 2015. https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf.

U.S. Customs Museum Foundation. “History.” Accessed August 8, 2017. http://customsmuseum.org/history/.

Van Lange, Paul A. M., Bettina Rockenbach, and Toshio Yamagishi. *Reward and Punishment in Social Dilemmas*. Oxford: Oxford University Press, 2014. ProQuest Ebook Central.

Vashisth, Akanksha, and Avinash Kumar. “Corporate Espionage: The Insider Threat.” *Business Information Review* 30, no. 2 (June 2013): 83–90. http://journals.sagepub.com/doi/10.1177/0266382113491816.

Vohs, Kathleen D. “The Mere Thought of Money Makes You Feel Less Pain.” *Harvard Business Review* 88, no. 3 (March 2010): 28–29. http://libproxy.nps.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=48219376&site=ehost-live&scope=site.

Vohs, Kathleen D., Nicole L. Mead, and Miranda R. Goode. “The Psychological Consequences of Money.” *Science* 314, no. 5802 (November 17, 2006): 1154–1156. http://www.sciencemag.org/cgi/doi/10.1126/science.1132491.

Walsh, Jeff. “Crime Stoppers.” In *Encyclopedia of Law Enforcement*, edited by Larry E. Sullivan, Marie Simonetti Rosen, Dorthy Moses Schulz, and M. R. Haberfeld, 122–123. Thousand Oaks, CA: SAGE, 2018. http://sk.sagepub.com/reference/lawenforcement.

Yin, Robert K. *Case Study Research: Design and Methods*. 5th ed. Thousand Oaks, CA: SAGE, 2013.

Yocom, Jerry D. “An Assessment of the Validity of Polygraph Examinations for the Psychophysiological Detection of Deception: A Judicial Opinion and Research Study Review.” *Journal of Police and Criminal Psychology* 22, no. 2 (November 27, 2007): 113–119.

Zhou, Xinyue, Kathleen D. Vohs, and Roy F. Baumeister. “The Symbolic Power of Money: Reminders of Money Alter Social Distress and Physical Pain.” *Psychological Science* 20, no. 6 (June 2009): 700–706. http://journals.sagepub.com/doi/10.1111/j.1467-9280.2009.02353.x.

Zipparo, Lisa. “Factors Which Deter Public Officials from Reporting Corruption.” *Crime, Law and Social Change* 30, no. 3 (1998): 273–287.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California