



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**THE MANCHURIAN RESPONDER? HOW MILITARY
AND FEDERAL GOVERNMENT PRACTICES CAN
HELP STATE AND LOCAL PUBLIC SAFETY
AGENCIES PREVENT MALICIOUS INSIDER ATTACKS**

by

Ryan J. McGovern

March 2018

Thesis Co-Advisors:

Erik Dahl
Paul Smith

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2018	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE THE MANCHURIAN RESPONDER? HOW MILITARY AND FEDERAL GOVERNMENT PRACTICES CAN HELP STATE AND LOCAL PUBLIC SAFETY AGENCIES PREVENT MALICIOUS INSIDER ATTACKS			5. FUNDING NUMBERS	
6. AUTHOR(S) Ryan J. McGovern				
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. IRB number 2017.0165-DD-N.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) A treacherous police officer or firefighter has the training, access, and expertise to cause numerous casualties among his or her colleagues and the public at large. In response to this threat, state and local public safety agencies may be greatly overestimating the ability of current pre-employment screening procedures to prevent radicalized individuals from infiltrating their ranks. Principally, psychological exams are insufficient to screen out terrorists because terrorists are ideologically, rather than psychopathically, motivated. Simply put, terrorists are sane, rational actors seeking to correct a grievance. However, this thesis reveals that the greater risk lies not with infiltrators, but with existing members of the agency who become radicalized. Consequently, this thesis focuses on how an agency should protect itself against this form of insider threat. Organizations should implement stricter and more in-depth screening of individuals seeking positions in police or fire departments, educate existing members on the signs of radicalization, and provide a clear reporting mechanism that culminates in appropriate investigative procedures and mitigation strategies to prevent a terrorist plot. To protect American lives, police and fire departments must consider the legitimate risk of a radicalized first responder developing within their ranks before a malicious plot materializes.				
14. SUBJECT TERMS insider threat, radicalization, terrorism, public safety, pre-employment screening, malicious insider			15. NUMBER OF PAGES 141	
			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

Approved for public release. Distribution is unlimited.

**THE MANCHURIAN RESPONDER? HOW MILITARY AND FEDERAL
GOVERNMENT PRACTICES CAN HELP STATE AND LOCAL PUBLIC
SAFETY AGENCIES PREVENT MALICIOUS INSIDER ATTACKS**

Ryan J. McGovern
Captain, Boston Fire Department
B.S., University of Maryland University College, 2014

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
March 2018**

Approved by: Erik Dahl
Co-Advisor

Paul Smith
Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A treacherous police officer or firefighter has the training, access, and expertise to cause numerous casualties among his or her colleagues and the public at large. In response to this threat, state and local public safety agencies may be greatly overestimating the ability of current pre-employment screening procedures to prevent radicalized individuals from infiltrating their ranks. Principally, psychological exams are insufficient to screen out terrorists because terrorists are ideologically, rather than psychopathically, motivated. Simply put, terrorists are sane, rational actors seeking to correct a grievance. However, this thesis reveals that the greater risk lies not with infiltrators, but with existing members of the agency who become radicalized. Consequently, this thesis focuses on how an agency should protect itself against this form of insider threat. Organizations should implement stricter and more in-depth screening of individuals seeking positions in police or fire departments, educate existing members on the signs of radicalization, and provide a clear reporting mechanism that culminates in appropriate investigative procedures and mitigation strategies to prevent a terrorist plot. To protect American lives, police and fire departments must consider the legitimate risk of a radicalized first responder developing within their ranks before a malicious plot materializes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH DESIGN	3
C.	THESIS OVERVIEW AND CHAPTER OUTLINE.....	6
II.	LITERATURE REVIEW	7
A.	DEFINITIONS	8
B.	INSIDERS AND INFILTRATORS.....	11
C.	PSYCHOLOGICAL MODELS.....	14
D.	CURRENT INSIDER THREAT DETECTION PROGRAMS.....	16
E.	CONCLUSION	19
III.	RADICALIZATION OF AN ALREADY SWORN FIRST RESPONDER.....	21
A.	CASE STUDIES.....	22
1.	Nidal Hasan	22
2.	Syed Rizwan Farook.....	25
3.	Mevlut Mert Altintas	29
4.	Nicholas Young.....	31
5.	Summary of Findings	33
B.	FOCUSING ON BEHAVIORS	35
C.	CONCLUSION	38
IV.	CLEAN-SKIN INFILTRATORS AND POTENTIAL METHODS TO THWART THEM.....	39
A.	TYPES OF CLEAN-SKIN INFILTRATORS.....	40
B.	INFILTRATORS VERSUS DISGRUNTLED INSIDERS AS POTENTIAL THREATS.....	41
C.	THREAT ASSESSMENTS	43
1.	FBI Profiling Method	44
2.	Secret Service Targeted Violence Method.....	45
3.	Department of Defense Model	47
D.	ANALYSIS	49
E.	CONCLUSION	51

V.	PROCEDURES FOR SCREENING IN PUBLIC SAFETY OFFICERS AND THEIR INEFFECTIVENESS AT SCREENING OUT RADICALS.....	53
A.	PRE-EMPLOYMENT PSYCHOLOGICAL SCREENING	53
B.	CRIMINAL BACKGROUND CHECKS	56
1.	Criminal History Check	58
2.	Polygraph Exams	59
3.	Verification of a Candidate’s Background.....	61
4.	Financial Records Check.....	61
5.	Documentation Verification.....	62
C.	ANALYSIS	63
D.	CONCLUSION	64
VI.	HOW THE U.S. MILITARY AND FEDERAL GOVERNMENT SCREEN FOR AND PREVENT TARGETED VIOLENCE	67
A.	FEDERAL LAW ENFORCEMENT POSITION PRE-SCREENING.....	68
1.	Polygraph Exams	69
2.	Social Media	70
B.	MILITARY PRE-SCREENING.....	72
1.	Fingerprints.....	73
2.	Tattoos.....	73
3.	Questionnaires.....	75
C.	METHODS FOR PREVENTING CURRENT EMPLOYEES FROM RADICALIZING.....	76
1.	Range of Threats.....	76
2.	Prevention and Deterrence Models for Avoiding Employee Radicalization	77
3.	Information Sharing	86
D.	CONCLUSION	87
VII.	CONCLUSION AND RECOMMENDATIONS.....	91
A.	FINDINGS.....	92
B.	RECOMMENDATIONS.....	93
1.	Pre-recruitment Selection and Screening Procedures.....	94
2.	Awareness, Education, and Target Hardening	94
3.	Reporting Mechanism	96
4.	Investigations and Threat Management Units.....	99
C.	IN CLOSING.....	100

APPENDIX A. INSIDER THREAT BEHAVIORAL INDICATORS.....	103
APPENDIX B. PROPOSED REPORTING STRUCTURE.....	105
LIST OF REFERENCES	107
INITIAL DISTRIBUTION LIST	113

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Suicide Warning Signs.....	36
-----------	----------------------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Summary of Pre-attack Indicators from Case Studies	34
Table 2.	Observable Behavioral Indicators.....	83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AWG	U.S. Army Asymmetric Warfare Group
DoD	Department of Defense
DSB	Defense Science Board
FTO	foreign terrorist organization
IPI	Inwald Personality Inventory
MMPI	Minnesota Multiphasic Personality Inventory
PTSD	post-traumatic stress disorder
Rap Back	Retained Applicant Fingerprint Background Check
TMU	threat management unit
TSA	Transportation Security Administration

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The issue of a malicious insider is one of the greatest concerns to the security of an organization, including public safety agencies; as one expert put it, it is “irrefutably one of the greatest threats to United States national security.”¹ This thesis asks: What lessons can local and state public safety agencies learn from their federal counterparts and the U.S. military about screening and preventing the malicious insider from carrying out an attack? The term “malicious insider” for this study focuses on the person who has privileged access to non-public or proprietary domains and who seeks to do harm to the organization or public in furtherance of a terrorist objective.²

Additionally, this thesis argues that the insider threat will evolve and include public safety agencies at both the local and state levels. It is hoped that the lessons presented and learned from federal agencies and the military can be applied at the local and state levels to prevent and deter this type of action.

If a person were to infiltrate an organization or radicalize to an extremist ideology within a local or state public safety agency, that person’s ability to operationalize and carry out an attack, whether against the agency or against the public writ large, would be exacerbated. The public sees police officers and firefighters as people upon whom they can depend for their protection. But the ability to betray that public trust exists, and it is incumbent upon leadership within the public safety disciplines to recognize and mitigate the threat before it becomes a problem.

The primary concern is: How can an organization stop this type of threat? Can the organization catch a potential malicious insider before that person is hired into the department through current pre-employment screening procedures? Currently, this author

¹ Caitlin Squire Hall, “The Trusted Shadow and Trojan Horse of the United States Government: Human Behavior and the Insider Threat,” *Small Wars Journal*, March 20, 2014, www.smallwarsjournal.com/printpdf/15439.

² Jeffrey Hunker and Christian W. Probst, “Insiders and Insider Threats,” *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications* 2. no. 1 (2011): 5, <http://isyou.info/jowua/papers/jowua-v2n1-1.pdf>.

believes that a determined individual can elude detection, be hired, and carry out an attack. Most agencies depend on standardized psychological evaluations and testing to vet candidates for positions within police or fire departments.³ These tests focus more on whether or not an applicant is mentally capable of doing the job of a police officer or firefighter, not on whether the applicant may be prone to violence or extremist activity.⁴ This oversight opens the door for a person to radicalize while employed by a public safety agency, and later decide to carry out an attack by leveraging his or her status as a trusted public safety official. Background criminal history checks also have their limitations. For example, some background checks do not capture an applicant's criminal history if the crime occurred over ten years prior, or in another state. This deficiency and others may open the door for extremists and terrorists to infiltrate a public safety department.

Much of the current research into insider threats agrees that individuals are more apt to become lone-wolf actors, who deal with their perceived grievances by themselves, rather than to engage in a larger plot or on behalf of an extremist or terrorist ideology. As a result, there are fewer opportunities within current protocols to detect these insiders before they act. Furthermore, Marleah Blades believes that each new study released on the malicious insider confirms that these individuals pose a major threat to organizations in both the private and public sectors.⁵

There are conflicting views on which type of malicious insider will pose the greatest risk. Nicholas Catrantzos argues that an outside infiltrator poses a greater risk than a disgruntled insider.⁶ He believes that the disgruntled insider is potentially unstable and difficult to control, making him or her unreliable; because this type of individual cannot be

³ Peter A. Weiss and William U. Weiss, "Criterion-Related Validity in Police Psychological Evaluations," in *Handbook of Police Psychology*, ed. Jack Kitaeff (New York: Routledge, 2011), 126; Louis Laguna, Joseph Agliotta, and Stephanie Mannon, "Pre-employment Screening of Police Officers: Limitations of the Mmpi-2 K-Scale as a Useful Predictor of Performance," *Journal of Police and Criminal Psychology* 30, no. 1 (2015): 1, <https://doi.org/10.1007/s11896-013-9135-9>.

⁴ "The Minnesota Multiphasic Personality Inventory-2 (MMPI-2) in Career Development," *Career Research*, March 12, 2015, 4, <http://career.iresearchnet.com/career-development/minnesota-multiphasic-personality-inventory-2-mmpi-2/>.

⁵ Marleah Blades, "The Insider Threat," *Security Technology Executive* (November/December 2010): 32.

⁶ Blades, 43.

trusted with a devious plan, he or she is more likely to commit an act of workplace violence than terrorism.⁷ In comparison, James Kenny shifts blame from the employee to the organization; he believes that “organizations can produce or facilitate aggressive work climates that may instigate violence by employees, clients or external intruders.”⁸ This thesis recognizes the threat from an infiltrator, but contends that the greatest threat comes from the employee already within the ranks.

Currently, public safety agencies conduct psychological evaluations to assess potential new hires’ prospective success in the career field. Therefore, it is important to understand how psychological testing is used to eliminate candidates from employment, and the deficiencies of these exams in identifying potential insider threats. Timothy Roufa suggests that the focus of these exams is to prevent the organization from hiring an individual who does not possess the desired traits for public safety officers.⁹ These tests were not initially designed for pre-employment screening, but rather for diagnostic purposes related to psychopathology.¹⁰ Where it relates to preventing the hiring of a terrorist or other extremist, these procedures appear to miss the mark; most terrorists are not linked to mental health problems, according to Clark McCauley.¹¹ Jeff Victoroff agrees, saying psychopathology is not found in the majority of terrorist actors.¹²

With the current screening models employed in local and state public safety hiring practices, terrorists can gain employment into a department or agency if they are not disqualified for other reasons, granting them access within the agency and a status of trust

⁷ Blades, 42.

⁸ James F. Kenny, “Threats in the Workplace: The Thunder before the Storm?,” *Security Journal* 18, no. 3 (May 2005): 45–56, <http://doi.org/10.1057/palgrave.sj.8340203>.

⁹ Timothy Roufa, “Should Police Have Psychological Tests?,” *The Balance*, accessed October 23, 2016, <https://www.thebalance.com/psychological-exams-and-screening-for-police-officers-974785>.

¹⁰ Weiss and Weiss, “Criterion-Related Validity,” 125.

¹¹ Clark McCauley, “Psychological Issues in Understanding Terrorism and the Response to Terrorism,” in *Psychology of Terrorism*, ed. Chris E. Strout (New York: Oxford University Press), 5, <http://www.start.umd.edu/publication/psychological-issues-understanding-terrorism-and-response-terrorism>.

¹² Jeff Victoroff, “The Mind of the Terrorist: A Review and Critique of Psychological Approaches,” *Journal of Conflict Resolution* 49, no. 1 (2005): 3–42, <http://doi.org/10.1177/0022002704272040>.

throughout the community. While much available literature explains the process of radicalization, there is less literature about the process of how an insider threat is created.

For the purpose of this study, two models are used to outline the basics of how persons are radicalized: Mohammed Hafez and Creighton Mullins’s “radicalization puzzle,” and Fathali Moghaddam’s “staircase to terrorism.” Hafez and Mullins postulate that those who radicalize to an ideology are influenced by four factors that lead to extremism: grievances, networks, ideologies, and enabling structures.¹³ This framework was chosen for this thesis because it is flexible enough to be applied to the wide swaths of extremist and terrorist ideologies, and for its simplicity. This is compared to Moghaddam’s staircase to terrorism model, which has its merits, but focuses more on the psychological aspects of radicalization.¹⁴ Both theories agree that individuals who turn to terrorism are seeking to correct a grievance or feeling of deprivation.¹⁵ Additionally, they both agree that group and network building is a major part of radicalization; groups help the individual feel like a part of something greater, and fill an empty space in his or her life.¹⁶

As there have been no cases to date of local or state public safety officials conducting a domestic terrorist attack, it is necessary to look to examples of radicalization among government employees in the United States as well as overseas. Of the four cases explored in this thesis, two involved persons in the United States—one a soldier and the other a public employee. The third case comes from overseas, while the fourth case examines a local police officer who did not carry out a violent attack, but was in a position to do so after radicalizing.¹⁷ These cases help us understand the risk that a violent insider

¹³ Mohammed Hafez and Creighton Mullins, “The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism,” *Studies in Conflict & Terrorism* 38, no. 11 (November 2, 2015): 961, <http://doi.org/10.1080/1057610X.2015.1051375>.

¹⁴ Fathali M. Moghaddam, “The Staircase to Terrorism: A Psychological Exploration,” *American Psychologist* 60, no. 2 (February 2005): 161–69, <http://dx.doi.org/10.1037/0003-066X.60.2.161>.

¹⁵ Hafez and Mullins, “Radicalization Puzzle,” 963; Moghaddam, “Staircase to Terrorism,” 162.

¹⁶ Hafez and Mullins, “Radicalization Puzzle,” 965; Moghaddam, “Staircase to Terrorism,” 165.

¹⁷ Another example is the 1984 assassination of Indira Gandhi by two of her Sikh bodyguards, Satwant Singh and Beant Singh. The Gandhi case highlights the ability of an individual trusted and trained with weapons to get close to an important person and carry out an attack such as an assassination. However, because that case is based on revenge and not attributed to radicalization, it is not discussed further.

represents, and also indicate the types of behaviors and precursors to an attack that such individuals may demonstrate. The cases discussed are as follows:

Major Nidal Hasan perpetrated attacks in Fort Hood, Texas, in November 2009, killing thirteen people and injuring thirty-one. Hasan entered a soldier readiness center where he worked, and began shooting soldiers who were deploying to or returning from conflicts overseas.

Syed Farook, a public health inspector for the San Bernardino County Department of Public Health—with his wife, Tashfeen Malik—shot and killed fourteen people and severely wounded twenty-two at a holiday party at the Inland Regional Center on December 2, 2015.

On October 23, 2016, Mevlut Mert Altintas, an Ankara police officer, assassinated Andrey Karlov, the Russian Ambassador to Turkey, at an art exposition. Altintas, who was off duty that day, used his police credentials to obtain access to the event and to side-step metal detectors and other security measures, which allowed him close access to the ambassador.¹⁸

Finally, Nicholas Young, a Washington, DC, transit officer was arrested and convicted of providing support to a foreign terrorist group. Though Young never carried out an attack within the United States, he represents the potential threat that exists if a public safety officer radicalizes to a terrorist ideology.

The commonality that ties these individuals together, making the insider threat such an issue, is that they all had access. These men were already a part of the organization they attacked, and had become part of the group. Once inside, they were free to carry out any mission they chose, including murder.

In all of these cases, the individuals had communicated with a foreign terrorist organization; in the cases involving an actual attack, the perpetrators conducted pre-attack reconnaissance of the target area. This is important because it illustrates the effectiveness

¹⁸ Laura Pitel and Roland Oliphant, “Mevlut Mert Altintas: Boy from a Small Town on Aegean Coast Who Became a Murderer,” *Telegraph*, December 21, 2016, <http://www.telegraph.co.uk/news/2016/12/20/mevlut-mert-altintasboy-small-town-aegean-coast-became-murderer/>.

of an individual exploiting his or her position as a first responder to carry out an attack, and how devastating this tactic can be.

Public safety agencies should understand that anyone can commit an act of violence, and that radicalized individuals generally do not advertise their plots. In the case of terrorism, it may be a specific ideology rather than a specific event that is driving the individual. The most important finding of this thesis is that public safety agencies that screen applicants will most likely not detect a determined infiltrator. Public safety organizations must understand this finding; recognizing an infiltrator once he or she is within the agency should become the priority. This is not very different from recognizing the employee who is in the process of radicalizing. However, because the organization is now dealing with a person who has already ascended the “staircase to terrorism,” that person is a greater acute threat than the radicalizing responder.

Current pre-employment screening procedures were never intended to evaluate applicants for the threat of terrorism, which is ideologically driven; they screen for potential criminality, which is psychologically driven. Further, because having a terrorist ideology is not a mental health disorder, tests designed to screen for mental health problems are unlikely to identify radicalizing individuals. It is important for local and state public safety agencies to recognize this deficiency, and perhaps establish procedures to eliminate potential malicious radicals from infiltrating their departments via the pre-employment hiring processes.

Having dealt with violent attacks by service members who have radicalized, the U.S. military and federal law enforcement agencies have had to respond and develop strategies to prevent future attacks. The two main methods discussed are prevention and deterrence, and information sharing. The three primary models used for prevention and deterrence are the Record of Arrest and Prosecution Background (or Rap Back, used by federal law enforcement), threat management units, and a model developed by the Asymmetric Warfare Group to recognize radicalization and prevent an individual’s movement to violence. Information sharing among agencies is also discussed, along with how looping all parties together to share information can be critical to avoiding violence in the future.

Between the author's experience within public safety and the research conducted, this thesis proposes the following four general recommendations to prevent a malicious insider within a public safety organization. First, organizations should make themselves difficult to infiltrate. Next, first responders need to be aware that the threat exists and be familiar with signs of radicalization; this is the awareness and education piece to the solution. Third, procedures should be established that give responders a clean, "fast track" reporting mechanism for suspicions about fellow responders. As part of this third recommendation, internal procedures should be developed so any report from a concerned member of staff is dealt with appropriately before a fellow responder fully radicalizes and carries out a violent attack. This aligns with the final recommendation: there should be a strong investigation and mitigation strategy to handle reports of potential first responder radicalization.

This thesis shows that by properly acknowledging the threat and instituting training for employees and leadership that mirrors U.S. military and federal law enforcement agencies, state and local first responder agencies can be safer and can prevent the deaths of Americans. The threat of terrorism continues to evolve and tactics continue to change; state and local first responders must evolve with that threat, and must safeguard their agencies against a malicious insider's act of terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Throughout my life I have been blessed to be surrounded by loving and supportive people who have always sought to provide me with every opportunity to improve myself. Throughout my time at NPS, this has been no different. Foremost in this is my beloved family, who put up with the long nights and missed events so that I could focus on this program and complete this thesis. I recognize that it was never an easy journey for them, and they still always showed unwavering strength and resilience throughout this process. Without their love, I could not have finished this project. Extensions of this are my brothers and sisters in cohort 1601/1602, who all endured more than eighteen months together, for better or for worse. Our diverse and combined strengths are what made us succeed, whether we saw it or not.

I would also like to thank my advisors, Paul Smith and Erik Dahl, for having the patience to work through some difficult times, and opening their minds to my opinions on this subject matter. Thank you for always asking more questions to pull out more answers from me. Your knowledge and insight have been invaluable in crafting this product, and I am confident it will capture the interests of those within the public safety realm.

Finally, during those dark moments when I felt lost in what I was trying to accomplish and where I was trying to go, I remembered my navigation training, which taught me that the stars will always guide you. Without their peace, consistency, and luster, I may not have found the path to where I was going.

Thank you, everyone, and goodnight stars.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The issue of a malicious insider is one of the greatest concerns to the security of an organization, including public safety agencies. As one expert put it, malicious insiders are “irrefutably one of the greatest threats to United States national security.”¹ This thesis asks: What lessons can local and state public safety agencies learn from their federal counterparts and the U.S. military about screening and preventing the malicious insider from carrying out an attack? The term “malicious insider” for this study focuses on the person who has privileged access to non-public or proprietary domains and who seeks to do harm to the organization or public in furtherance of a terrorist objective.²

A. PROBLEM STATEMENT

If a person were to infiltrate an organization or radicalize to an extremist ideology within a local or state public safety agency, that person’s ability to operationalize and carry out an attack, whether against the agency or against the public writ large, would be exacerbated. The public sees police officers and firefighters as people upon whom they can depend for their protection. But the ability to betray that public trust exists, and it is incumbent upon leadership within the public safety disciplines to recognize and mitigate the threat before it becomes a problem. Some strategies for doing so are addressed in this thesis.

Sworn public safety officers, with a badge and a uniform, are given free access to non-public spaces, including vulnerable and critical facilities. This level of access could be extremely alluring to an individual who is seeking to commit an organized attack. If successful, the impact of a first responder’s malicious action against the community would have consequences on the home agency, the community, and the nation. Part of the

¹ Caitlin Squire Hall, “The Trusted Shadow and Trojan Horse of the United States Government: Human Behavior and the Insider Threat,” *Small Wars Journal*, March 20, 2014, www.smallwarsjournal.com/printpdf/15439.

² Jeffrey Hunker and Christian W. Probst, “Insiders and Insider Threats,” *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications* 2. no. 1 (2011): 5, <http://isyou.info/jowua/papers/jowua-v2n1-1.pdf>.

question becomes: How does an agency know that the personnel entrusted with such access are always committed to acting for the safety of the public?

Imagine, for example, two scenarios. In the first, a police officer reports to work to escort the annual Veteran's Day parade through town. The officer harbors a disdain for the wars in Iraq and Afghanistan, and for anyone who has served the country by fighting in these conflicts. The officer has silently radicalized and pledged allegiance to a foreign terrorist organization (FTO). The officer signs out a cruiser and arrives at the parade's starting point. A little over halfway through the parade route, the officer sees a troop of twenty Girl Scouts on the side of the road, waving to the procession as it approaches. Seeing this as a target that will result in the most public impact and will spread the strongest message in support of the FTO, the officer begins to accelerate and sharply turns left into the crowd, first striking the Girl Scout troop and then continuing to drive over spectators until the cruiser crashes into a mailbox and comes to a stop. The final count: the officer has run over fifty people, with twenty-six fatally wounded.

In the second scenario, a firefighter has similarly radicalized to an extremist ideology—in this case, a white supremacist organization. As part of an operation to emulate the 2008 attacks on the Taj hotel in Mumbai, India, the white supremacists are planning to attack a hotel downtown where a speaker from the National Association for the Advancement of Colored People (NAACP) is holding a dinner for Black History Month. The firefighter's initial mission is to disable the fire suppression system on the 14th floor of the hotel, where the group will mount its assault, eventually moving to the ballroom on the 16th floor. The firefighter also disables the automatic fire doors—which will allow fire to spread, unimpeded, through the fire floor and up the stairwells—and sabotages the smoke detectors and standpipe systems. The firefighter tells the group to set the fire on an upper-level floor of the building, above the reach of the aerial ladders that the fire department uses to rescue victims and suppress blazes. This will slow response efforts to the main area of attack, and enable the group to carry out the rest of its complex coordinated attack: they plan to shoot their victims, using fire as a weapon to trap and kill them.

In these two scenarios, the radicalized first responders' subject-matter expertise is a force multiplier to any group that seeks to carry out an attack. Badged and credentialed

first responders have virtually unlimited access in their communities. This access, coupled with an expert knowledge of systems, tactics, and vulnerabilities throughout the community, is unrivaled and highly valuable to a nefarious organization.

How can an organization stop this type of threat? Through current procedures, can the organization catch potentially radicalized individuals before they are hired into the department? Most agencies depend on standardized psychological evaluations and testing to vet candidates for positions within police or fire departments.³ However, these tests focus on the applicant's mental capacity to do the job, not on the applicant's susceptibility to violence or extremist activity.⁴ This oversight opens the door for a person to radicalize while employed by a public safety agency, and later decide to carry out an attack by leveraging his or her status as a trusted public safety official. Additionally, the limitations of background criminal history checks may allow extremists and terrorists to infiltrate a public safety department.

B. RESEARCH DESIGN

This thesis uses a case study approach to examine insider targeted violence in order to frame the threat that is being discussed within the public safety realm. The intent is to identify behaviors and actions that an individual displays before he or she carries out an attack, and determine if local and state public safety agencies are using measures that can identify at-risk individuals and prevent an attack from within. The following are some of the cases that will be discussed in greater detail in later chapters.

In November 2009, Major Nidal Hasan entered a soldier readiness center where he worked in Fort Hood, Texas, and began shooting at soldiers who were deploying or

³ Peter A. Weiss and William U. Weiss, "Criterion-Related Validity in Police Psychological Evaluations," in *Handbook of Police Psychology*, ed. Jack Kitaeff (New York: Routledge, 2011), 126; Louis Laguna, Joseph Agliotta, and Stephanie Mannon, "Pre-employment Screening of Police Officers: Limitations of the Mmpi-2 K-Scale as a Useful Predictor of Performance," *Journal of Police and Criminal Psychology* 30, no. 1 (2015): 1, <https://doi.org/10.1007/s11896-013-9135-9>.

⁴ "The Minnesota Multiphasic Personality Inventory-2 (MMPI-2) in Career Development," Career Research, March 12, 2015, 4, <http://career.iresearchnet.com/career-development/minnesota-multiphasic-personality-inventory-2-mmpi-2/>.

returning home from conflicts overseas. Hasan killed thirteen people and injured thirty-one.

Syed Farook, a public health inspector for the San Bernardino County Department of Public Health—along with his wife, Tashfeen Malik—shot and killed fourteen people and severely wounded twenty-two at a holiday party at the Inland Regional Center on December 2, 2015.

On October 23, 2016, Ankara police officer Mevlut Mert Altintas assassinated Andrey Karlov, the Russian Ambassador to Turkey, at an art exposition. Altintas, who was off duty that day, used his police credentials to obtain access to the event and side-step metal detectors and other security measures, allowing him close access to the ambassador.⁵

Finally, Nicholas Young, a Washington, DC, transit officer, was arrested and convicted of providing support to a foreign terrorist group. Though Young never carried out an attack within the United States, he represents the potential threat that exists if a public safety officer radicalizes to a terrorist ideology.

The commonality that ties these individuals together, making the insider threat such an issue, is that they all had access. These men were already a part of the organization they attacked, and had become part of the group. Once inside, they were free to carry out any mission they chose, including murder.

This is a threat that will not go away. In fact, according U.S. Air Force Intelligence Officer Caitlin Hall, “Each new study that is released further confirms that the malicious insider continues to pose a major threat to organizations in both public and private sector.”⁶ The insider is more likely to know which information to target and how to obtain it, according to Hall.⁷ This thesis argues that this threat will evolve and include public safety agencies at both the local and state levels. It is hoped that lessons learned from federal

⁵ Laura Pitel and Roland Oliphant, “Mevlut Mert Altintas: Boy from a Small Town on Aegean Coast Who Became a Murderer,” *Telegraph*, December 21, 2016, <http://www.telegraph.co.uk/news/2016/12/20/mevlut-mert-altintasboy-small-town-aegean-coast-became-murderer/>.

⁶ Hall, “Trusted Shadow.”

⁷ Hall.

agencies and the military can be applied at the local and state levels to prevent and deter this type of threat.

Two hypotheses are tested in this thesis to determine if this threat requires more attention and if the lessons learned from federal partners and the Department of Defense (DoD) are enough to prevent related actions from occurring:

- H1: If local and state public safety agencies do not take appropriate measures to recognize the insider threat and to prevent and deter insider attacks, then a motivated first responder is more likely to leverage his or her status as a trusted first responder to carry out an attack.
- H2: If state and local public safety agencies implement insider threat detection programs modeled after U.S. federal agency programs, they will be more likely to detect potential threats and deter or prevent terrorist attacks within their agencies.

It is difficult—but not impossible—to determine which individuals within an organization or agency are most likely to be malicious insiders. There is no cookie-cutter model for potential insiders; like violent extremists, they are extremely challenging to profile.⁸ Cole et al. explain that insiders “come from diverse ethnic and social backgrounds, ranging from school dropouts and reformed criminals to university graduates with bright prospects. Some are from poor backgrounds, while others are wealthy. Some are very religious, others are not. Many are young, single men, but a significant number are married with children.”⁹ Each of these examples could be someone we know: a neighbor, a family member, or a coworker.

This thesis leverages prior lessons learned from case study analyses and applies them to the public safety realm; the goal is to prevent this evolving threat from manifesting itself in officer malfeasance in the United States. Various programs and strategies

⁸ Jon Cole et al., “Free Radicals— Stopping Extremists before They Start,” *Jane’s* by HIS Markit, September 16, 2010, <https://janes.ihs.com.libproxy.nps.edu/IntelligenceReview/Display/1196061>.

⁹ Cole et al.

implemented within the DoD and other federal agencies are evaluated for their transferability to local and state public safety personnel, and are offered as measures to protect these agencies and their employees.

To date, there have been no malicious insider attacks within local or state public safety agencies in the United States on behalf of a terrorist agenda. Attacks have occurred overseas and within other branches of U.S. government, and it is the author's belief that this insider threat will eventually manifest within U.S. local and state agencies. Because the scenario is therefore hypothetical, this thesis leverages other organizations' experiences with malicious insider attacks to bridge the gaps in each chapter.

C. THESIS OVERVIEW AND CHAPTER OUTLINE

Chapter II provides an overview of the literature used to examine and evaluate how a malicious insider within a public safety agency could be a viable threat, and how a related attack may be prevented. Chapter III connects behaviors and precursors that indicate an already sworn individual may radicalize to an extremist ideology and carry out an attack. Chapter IV evaluates the ability of a "clean-skin" individual to infiltrate a public safety agency and then utilize his or her status to carry out an attack. Chapter V evaluates the current use of psychological testing and other procedures for pre-employment screening for state and local public safety positions, and their effectiveness for screening out a potential terrorist. Chapter VI compares and contrasts procedures for pre-employment screening used by the federal government and U.S. military to assess and screen for potential terrorists and extremists. Chapter VII closes with conclusions and recommendations based on the previous chapters, and offers suggestions to help public safety leadership prevent an attack by a sworn public safety officer.

II. LITERATURE REVIEW

This literature review describes existing and ongoing research that addresses the current threat of a malicious insider, and how it relates to public safety. The first two sections show how experts have defined the malicious insider threat, and the two different models for this threat profile. The following section evaluates the psychological models used to describe malicious insiders, as well as terrorism. The final section reviews some of the current programs and recommendations for how organizations can prevent and deter a malicious insider from operationalizing an attack.

Much of the current research into insider threats agrees that individuals are more apt to become lone-wolf actors, who deal with their perceived grievances by themselves, rather than to engage in a larger plot or on behalf of an extremist or terrorist ideology. As a result, there are fewer opportunities within current protocols to detect these insiders before they act. As stated by Caitlin Hall—and as mentioned in Chapter I, but it is worth noting again—the malicious insider is “irrefutably one of the greatest threats to U.S. national security.”¹⁰ Hall also believes that each new study released on malicious insiders confirms that these individuals pose a major threat to organizations in both the private and public sectors.¹¹

This threat is especially concerning considering the ease with which insiders can carry out an action against the agency or organization targeted. According to Blades, insiders have five distinct advantages that make them particularly dangerous to an organization:

1. Insiders do not have to infiltrate perimeter defenses on the network or in the facility.
2. They tend to plan their actions in advance and carefully cover their tracks.

¹⁰ Caitlin Hall, “Trusted Shadow.”

¹¹ Marleah Blades, “The Insider Threat,” *Security Technology Executive* (November/December 2010): 32.

3. They often use appropriate and approved access to systems and areas to commit their crimes.
4. They often have no criminal background.
5. They may have a variety of targets within the organization and they may act based on a wide range of motivations.¹²

Essentially, a person who comes into an organization or agency and who has no criminal past is given full access to that agency and its systems, which puts that person in a perfect position to carry out an attack. In particular, when attackers are properly motivated—regardless of their ideology—they plan out their violent incidents more carefully than someone with a simple workplace grudge.

When put into context, this describes first responders across the country. First responders must have a clean criminal history and, once they are hired into the department, they become part of the greater organization; and because insider attacks are not motivationally specific, anyone can carry them out.

A. DEFINITIONS

In viewing the insider threat issue from the ground level up, it is important to be able to define the problem, and to know what exactly constitutes a “malicious insider” and what the “insider threat” looks like. The federal government and military agencies are no closer to having a succinct and universal definition for these terms than state and local public safety agencies are. Definitions from the Department of Homeland Security and Transportation Security Administration (TSA) hint at the base problem: someone within the organization using his or her position to attack the organization, either internally or externally. The U.S. military has a similar definition, but the military definition is still not completely in line with other federal agencies. The DoD Insider Threat Working Group defines the insider threat as:

A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic

¹² Blades, 33.

actions resulting in personal injury or loss or degradation of resources or capabilities.¹³

The Department of Homeland Security defines the insider threat as:

The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.¹⁴

Most of the agencies and departments that have developed policies to address the insider threat have agreed that access is the key component. Other agencies agree, including the U.S. Army, the Defense Security Service, the DoD, and the TSA (which operates under the Department of Homeland Security).¹⁵ These definitions highlight the importance of agencies screening individuals before granting them employment, but also the need to continuously monitor employees for changes that indicate predilection toward radicalization.

The second piece to this definition, highlighted among the different agencies' definitions, is the intention to do harm to the organization from within. The U.S. Army and Defense Security Service definitions focus on an insider intentionally or unintentionally causing loss or degradation of resources or capabilities that impact the organization's ability to accomplish its mission.¹⁶ The DoD and TSA are more focused on their agencies'

¹³ *Compilation of Hearings on Islamist Radicalization, Vol. II: Joint Hearing before the Committee on Homeland Security, House of Representatives and the Committee on Homeland Security and Governmental Affairs, United States Senate*, 112 Cong. 1 (2011) (statement of Paul N. Stockton) (Washington, DC: U.S. Government Printing Office, 2012), 17, <https://catalog.hathitrust.org/Record/100668900>.

¹⁴ "DHS-ALL-PIA-052 DHS Insider Threat Program," Department of Homeland Security, July 13, 2015. <https://www.dhs.gov/publication/dhs-all-pia-052-dhs-insider-threat-program>.

¹⁵ Department of the Army, *Threat Awareness and Reporting Program*, AR 381-12 (Washington, DC: U.S. Government Printing Office, 2010), 4; Department of Defense (DoD), "DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team," Defense Technical Information Center, accessed March 4, 2017, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380; Department of Homeland Security Office of Inspector General, *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain*, OIG-12-120 (Washington, DC: Department of Homeland Security, 2012), <http://thehill.com/images/stories/blogs/flooraction/jan2012/oigtsa.pdf>; Department of Homeland Security, "Insider Threat Program"; "Insider Threats: Combating the Enemy within Your Organization," Defense Security Service, accessed February 17, 2018, <https://www.hsd1.org/?abstract&did=752042>.

¹⁶ Department of the Army, *Threat Awareness and Reporting Program*, 4.

mission and systems.¹⁷ Each agency focuses its definition on its own particular concerns, which is a key deficiency found in the numerous other definitions on this topic. There is no flexibility to allow for wider interpretation across all the fields that could be impacted by a malicious insider. Specificity is appropriate when viewed through the lens of precise agency needs, but when trying to view the issue of the malicious insider in a context that is underexplored, there is little room for interpretation, which potentially dilutes the intended meaning and purpose of the definition.

Christine Baker writes that there is no broadly agreed-upon definition of the insider threat among local, state, and federal agencies.¹⁸ In turn, there is no comprehensive strategy to address this threat, particularly at the local and state levels within public safety. Various agencies and private corporations have established insider threat prevention programs that benefit their agencies specifically; at a national or industry level, however, there is no universal program or guidance for preventing and handling the insider threat, specifically within public safety. This is perhaps because there have been no major insider threats within public safety, and so the issue has not been elevated to a priority.

To summarize these definitions into a single main point, Greitzer et al. define the malicious insider as a trusted individual who carries out a harmful act that causes damage to an organization or that benefits the individual.¹⁹ This is what makes an insider a true threat. Predd et al. further characterize the malicious insider as “an individual with privileges who misuses them or whose access results in misuse.”²⁰ Ultimately, the combination of these two definitions sums up why insider threats are so dangerous, and the importance of recognizing individuals who may be threats before they carry out an attack.

¹⁷ DoD, “Insider Threat Mitigation”; Department of Homeland Security Office of Inspector General, *Transportation Security Administration*.

¹⁸ Christine Baker, “Change of Detection: To Find the Terrorist Within the Identification of the U.S. Army’s Insider Threat” (master’s thesis, U.S. Army Command and General Staff College, 2012), 4, <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA565992>.

¹⁹ Frank L. Greitzer et al., “Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis,” *E-Service Journal* 9, no. 1 (July 3, 2014): 107, <https://muse.jhu.edu/article/548560>.

²⁰ Joel Predd et al., “Insiders Behaving Badly,” *IEEE Security & Privacy* 6, no. 4 (July 2008): 67, <http://doi.org/10.1109/MSP.2008.87>.

If someone has already breached a secure perimeter, the threat is now inside, making it far more difficult to detect and isolate—a modern-day Trojan horse attack.

B. INSIDERS AND INFILTRATORS

Malicious insiders, or those who seek to do harm to an agency from within, generally fall into two categories: disgruntled or radicalized employees and infiltrators.²¹ Nicholas Catrantzos, in his Naval Postgraduate School master’s thesis, defines disgruntled insiders as “those who work for an organization, and have developed a grievance against that organization, and seek to harm that organization in some way.”²² He describes an infiltrator, by contrast, as a “person who has been injected in to the organization with the expressed purpose of harming it from within, based on increased access to facilities or systems.”²³ Catrantzos makes the point that, once in the door, regardless of how he or she got there, the employee now has the ability to carry out any plot to further a personal agenda; in the case of first responders, the plot may be against either the organization or the public.

There are conflicting views on which type of malicious insider poses the greater threat. Catrantzos argues that the infiltrator poses a greater threat than the disgruntled insider.²⁴ He believes that the disgruntled insider is potentially unstable and difficult to control, making him or her unreliable; because this type of individual cannot be trusted with a devious plan, he or she is more likely to commit an act of workplace violence than terrorism.²⁵ In comparison, James Kenny shifts blame from the employee to the organization; he believes that “organizations can produce or facilitate aggressive work climates that may instigate violence by employees, clients or external intruders.”²⁶ This

²¹ Nicholas Catrantzos, “No Dark Corners: Defending against Insider Threats to Critical Infrastructure” (master’s thesis, Naval Postgraduate School, 2009), 42–43, <http://calhoun.nps.edu/handle/10945/4656>.

²² Catrantzos, 42–43.

²³ Catrantzos, 42–43.

²⁴ Catrantzos, 43.

²⁵ Blades, “Insider Threat,” 42.

²⁶ James F. Kenny, “Threats in the Workplace: The Thunder before the Storm?,” *Security Journal* 18, no. 3 (May 2005): 45–56, <http://doi.org/10.1057/palgrave.sj.8340203>.

thesis recognizes the threat from an infiltrator, but contends that the greatest threat comes from the employee already within the ranks.

Regardless, Blades argues that insider attacks are more costly and dangerous because they are more likely than hackers or even organized groups to know which information to target and how it can be obtained.²⁷ These individuals know what vulnerabilities exist within the organization, or what types of liabilities are exploitable around the community.

The infiltrator, however, is viewed throughout the literature as a more focused and calculated individual who does not have to spend a protracted amount of time within the organization to be effective, according to Marleah Blades.²⁸ Catrantzos believes that if an infiltrator gains access into an organization, he or she will be able to quickly accumulate sufficient knowledge upon which to base an insider attack to the organization without having to pretend to be fully invested in the organization.²⁹ Catrantzos goes on to say that the infiltrator need only gain the necessary level of unimpeded access within that organization to operationalize his or her plan.³⁰ This is valuable to understand because the threat does not require a prolonged incubation period to develop, especially with the infiltrator. Once the individual has infiltrated the organization, he or she only requires enough time to learn the systems and procedures, and how to exploit their vulnerabilities. Despite the opinions among experts on this topic, there is no evidence that infiltrators are a greater threat to public safety agencies than disgruntled employees.

Common among the research is a recognition that employee reporting is one of the most effective tools for detecting an insider threat. Many public safety agencies have programs for suspicious activity reporting, which are focused on what responders may encounter in the course of their duties. In her thesis, Baker mentions that it is essential for personnel to be aware of high-risk behaviors, and to report behaviors that may have a nexus

²⁷ Blades, "Insider Threat," 32.

²⁸ Blades, 43.

²⁹ Blades, 43.

³⁰ Catrantzos, "No Dark Corners," 44.

to homegrown terrorist activity.³¹ Employees must be educated about behaviors that indicate potential radicalization and movement to action for a terrorist ideology. This is mentioned in most of the current literature on this topic, but Baker emphasizes this approach, thinking of every fellow employee as, in essence, a sensor.³² This approach needs to be translated into the public safety realm to prevent attacks from first responders.

Catrantzos considers a similar strategy in his “no dark corners” approach. He advocates for a workspace that maximizes opportunities for employees (teammates) to take ownership of the workplace and to promote transparency. This approach relies on “employees—legitimate insiders—defending an institution and its infrastructure by taking ownership” and watching out for one another.³³ He believes that a malicious insider will be hindered from enacting a plot or exploiting information in a place of work where all the employees support each other.³⁴ This theory is a valid argument for increasing surveillance and cultivating a supporting environment for employees—one in which they can be more aware of signs of extremism or radicalization in fellow employees.

Much of the data on insider threat attacks have been generated from the information technology field, which has been dealing with this threat extensively over the past few decades. As a result, the field has developed policies to address the concern, as well as indicators to help identify radicalizing individuals and prevent an attack. One finding from an information technology study confirms that coworkers have the ability to spot a malicious insider in the making. Moore, Cappelli, and Trzeciak believe that “ninety-seven percent of the insiders in the [study] cases who committed [information technology] sabotage came to the attention of supervisors or coworkers from concerning behavior prior to an attack.”³⁵ Again, an individual’s behaviors indicate a malicious insider’s potential

³¹ Baker, “Change of Detection,” 18.

³² Baker, 38.

³³ Catrantzos, “No Dark Corners,” 61.

³⁴ Catrantzos, 61.

³⁵ Andrew Moore, Dawn Cappelli, and Randall Trzeciak, *The “Big Picture” of Insider IT Sabotage across U.S. Critical Infrastructures* (Pittsburgh, PA: Carnegie Mellon University, 2008), <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8703>.

actions. Dr. Eric Cole mirrors this opinion, stating, “Over eighty percent of personnel who were insider threats exhibited some form of indicators and behavior modifications before they conducted their attack.”³⁶ This demonstrates that if organizations institute programs that help employees look after one and other, they have a higher likelihood of preventing someone within the organization from successfully carrying out an attack.

C. PSYCHOLOGICAL MODELS

Currently, public safety agencies conduct psychological evaluations to assess potential new hires’ prospective success in the career field. Therefore, it is important to understand how psychological testing is used to eliminate candidates from employment, and the deficiencies of these exams in identifying potential insider threats. Timothy Roufa suggests that the focus of these exams is to prevent the organization from hiring an individual who does not possess the desired traits for public safety officers.³⁷ These tests were not initially designed for pre-employment screening, but rather for diagnostic purposes related to psychopathology.³⁸ Where it relates to preventing the hiring of a terrorist or other extremist, these procedures appear to miss the mark; most terrorists are not linked to mental health problems, according to Clark McCauley.³⁹ Jeff Victoroff and Joshua Sinai agree, saying psychopathology is not found in the majority of terrorist

³⁶ Eric A. Cole, “SANS Analyst Program: Correlating SIM Information to Detect Insider Threats” (white paper, SANS Institute, 2007), 5, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.592.8151&rep=rep1&type=pdf>.

³⁷ Timothy Roufa, “Should Police Have Psychological Tests?,” The Balance, accessed October 23, 2016, <https://www.thebalance.com/psychological-exams-and-screening-for-police-officers-974785>.

³⁸ Weiss and Weiss, “Criterion-Related Validity,” 125.

³⁹ Clark McCauley, “Psychological Issues in Understanding Terrorism and the Response to Terrorism,” in *Psychology of Terrorism*, ed. Chris E. Strout (New York: Oxford University Press), 5, <http://www.start.umd.edu/publication/psychological-issues-understanding-terrorism-and-response-terrorism>.

actors.⁴⁰ They do not discount that psychopaths may be employed by terrorists, but most terrorist leaders are mentally sane.

With the current screening models employed in local and state public safety hiring practices, terrorists can gain employment into a department or agency if they are not disqualified for other reasons, granting them access within the agency and a status of trust throughout the community. While much available literature explains the process of radicalization, there is less literature about the process of how an insider threat is created. A key point found in this thesis is that the biggest threat will come from the employee who radicalizes, not the employee that infiltrates an organization.

For the purpose of this study, two models are used to outline the basics of how individuals are radicalized: Mohammed Hafez and Creighton Mullins's "radicalization puzzle," and Fathali Moghaddam's "staircase to terrorism." Hafez and Mullins postulate that those who radicalize to an ideology are influenced by four factors that lead to extremism: grievances, networks, ideologies, and enabling structures.⁴¹ This framework was chosen for this thesis because it is flexible enough to be applied to wide swaths of extremist and terrorist ideologies, and for its simplicity. This is compared to Moghaddam's staircase to terrorism model, which has its merits, but focuses more on the psychological aspects of radicalization.⁴² Both theories agree that individuals who turn to terrorism are seeking to correct a grievance or feeling of deprivation.⁴³ Additionally, they both agree that group and network building is a major part of radicalization; groups help the individual

⁴⁰ Jeff Victoroff, "The Mind of the Terrorist: A Review and Critique of Psychological Approaches," *Journal of Conflict Resolution* 49, no. 1 (2005): 3–42, <http://doi.org/10.1177/0022002704272040>; Joshua Sinai, "Can Terrorists Be Psychologically Profiled?," *Journal of Counterterrorism and Homeland Security International* 17, no. 2 (Summer 2011), <http://www.lexisnexis.com.libproxy.nps.edu/lnacui2api/api/version1/getDocCui?lni=54K8-YNS1-DYRW-V4BK&csi=244681&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true>.

⁴¹ Mohammed Hafez and Creighton Mullins, "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism," *Studies in Conflict & Terrorism* 38, no. 11 (November 2, 2015): 961, <http://doi.org/10.1080/1057610X.2015.1051375>.

⁴² Fathali M. Moghaddam, "The Staircase to Terrorism: A Psychological Exploration," *American Psychologist* 60, no. 2 (February 2005): 161–69, <http://dx.doi.org/10.1037/0003-066X.60.2.161>.

⁴³ Hafez and Mullins, "Radicalization Puzzle," 963; Moghaddam, "Staircase to Terrorism," 162.

feel like a part of something greater, and fill an empty space in his or her life.⁴⁴ The models divert from one another in other parts of the theories, though not in ways that affect this study.

The U.S. Army Asymmetric Warfare Group (AWG) discusses many of the popular sociological and psychological theories used to explain why persons radicalize to extremist ideologies. In a report for the AWG, Crosset and Spitaletta focus on counter-radicalization and outline sixteen behaviors or features of a person who is susceptible to radicalization; if these risk factors are recognized early, an insider attack could be mitigated before harm comes to the person or organization.⁴⁵ Many of these factors revolve around how individuals interact with their environment, and where they feel they fit into that environment. If an individual disagrees with the political status quo or with a political activist group, or sees a benefit to political violence based on a grievance or in-group/out-group dynamic, he or she possesses some key factors that indicate possible radicalization to an extremist or terrorist ideology.⁴⁶ Other factors highlighted in the report focus on an individual's age, and whether or not the individual has or can receive outside support or resources.⁴⁷ The report simplifies and explains many of the popular theories on radicalization, but also presents the risk factors—as presented in this paragraph—that can help identify an individual who may pose a threat to an organization.

D. CURRENT INSIDER THREAT DETECTION PROGRAMS

Currently, the FBI is spearheading a program designed to monitor people who are in trusted positions for real-time reporting of criminal activities and interactions with law enforcement. Most existing literature on the FBI program discusses how the system works to increase information sharing at a quicker speed, but does not study the system from an analytical standpoint. The program was intended to increase criminal activity reporting for

⁴⁴ Hafez and Mullins, "Radicalization Puzzle," 965; Moghaddam, "Staircase to Terrorism," 165.

⁴⁵ Chuck Crossett and Jason Spitaletta, "Asymmetric Warfare Group Report: Psychological and Sociological Concepts of Radicalization," Public Intelligence, September 2010, 5, <https://publicintelligence.net/us-army-radicalization-concepts>.

⁴⁶ Crossett and Spitaletta.

⁴⁷ Crossett and Spitaletta.

those under law enforcement supervision, and reduce the burden on employers to conduct follow-up criminal background checks, which often are skipped after the initial screening for employment.⁴⁸ This program is known as Rap Back (short for Record of Arrest and Prosecution Background), and it is being recommended that more public safety agencies subscribe to this service. According to the FBI, “prior to the deployment of Rap Back, the national criminal history background check system provided a one-time snapshot view of an individual’s criminal history status.”⁴⁹ If an individual commits a crime after his or her initial hire, law enforcement may never inform the organization.

Rap Back is run using the Next Generation Identification (NGI) system within the Criminal Justice Information System, and will flag an individual within the system if his or her fingerprints are taken and then added to the system.⁵⁰ It is designed to share real-time information that will alert participating agencies to potential criminal activity within their ranks.⁵¹ Currently, TSA has partnered with the FBI to have this feedback mechanism used for their personnel.⁵² Had this system been in place within the U.S. Navy, for instance, Aaron Alexis, the Washington Naval Yard shooter, would have been flagged when he was found with an illegal handgun in Texas during his enlistment.⁵³ The need for increased information sharing regarding criminal interactions with law enforcement is also why fusion centers were established.

The military has experienced attacks from within, and has been forced to adapt and adopt new measures to reduce potential service member-on-service member attacks. The

⁴⁸ “Next Generation Identification (NGI),” FBI, accessed September 6, 2017, <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

⁴⁹ FBI.

⁵⁰ Ernest Babcock, “PIA: NGI Rap Back Service” (assessment, FBI, 2016), <https://www.fbi.gov/file-repository/pia-ngi-rap-back-service.pdf/view>.

⁵¹ Babcock.

⁵² Homeland Security Committee, *America’s Airports: The Threat from within* (Washington, DC: U.S. House of Representatives, 2017), 14, <https://homeland.house.gov/press/committee-releases-report-america-airports-threat-within/>.

⁵³ *The Insider Threat to Homeland Security: Examining Our Nation’s Security Clearance Processes, Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security, House of Representatives*, 113 Cong. 1 (2013) (Washington, DC : U.S. Government Printing Office, 2014), 41, <https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87372/html/CHRG-113hhrg87372.htm>.

first check occurs when an individual seeks to join the military. Applicants are screened for affiliation with any groups that are contrary to the mission of the U.S. military.⁵⁴ According to DoD Directive 5205.16, once employed, service members are regularly educated on behaviors and actions that may indicate an insider threat of targeted violence.⁵⁵ This essentially employs a “no soldier left behind” approach in which soldiers all support each other and stay on the lookout for changes in fellow service members that could indicate a problem or potential violent action. The description of the DoD plan is clear and simple, leaving little room for misinterpretation; this makes it a strong model to follow and employ in other fields.

The AWG also weighs in on the topic of insider threats, and recommends methods for preventing attacks from within. The primary audience for the AWG document is soldiers who are stationed overseas, working with partnering groups.⁵⁶ The document identifies three areas of focus: first, to inform military leaders and personnel about “indicators associated with insider threat activity while serving in partnering environments”; second, to present options for dealing with a potential insider threat; and third, to generate open dialogue among deployed personnel, and to improve partnerships.⁵⁷ Overall, despite its focus on deployed military personnel dealing with the questionable allegiances of foreign nationals, this guide can be aptly adapted for use in the domestic theater. Many of its tenets can be applied to public safety agencies because behaviors transcend geographic boundaries; however, proper interpretation is necessary to make the AWG recommendations fit domestic public safety agencies.

The Defense Science Board (DSB) recommends a threat management style for addressing the risks of targeted violence within the U.S. armed forces. According to the

⁵⁴ Mark Flacks and Martin Wiskoff, *Gangs, Extremists Groups, and the Military: Screening for Service*, SRC-TR-98-003 (Monterey, CA: Security Research Center, 1998), <http://www.dtic.mil/dtic/tr/fulltext/u2/a359551.pdf>.

⁵⁵ DoD, *Insider Threat Program*, DoDD 5205.16 (Washington, DC: DoD, 2017), www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516_dodd_2014.pdf?ver=2017-08-28-090609-503.

⁵⁶ “Insider Threats in Partnering Environments,” U.S. Army Asymmetric Warfare Group (AWG), June 2011, <https://info.publicintelligence.net/AWG-InsiderThreats.pdf>.

⁵⁷ AWG.

DSB, the mission of their threat management units (TMUs) “is to prevent targeted violence by developing calculated responses to troubling behavior.”⁵⁸ This is accomplished by using “a cross-functional, multi-disciplinary team approach to assist in assessing threatening situations and developing threat abatement plans that minimize the potential risk of violence,” says the DSB.⁵⁹ This is an effective strategy because it focuses on preventing—rather than predicting—violence. The Naval Criminal Investigative Service (NCIS) says that TMUs help “to identify risk factors, patterns of escalation, and to construct an environment that inhibits or prevents violence.”⁶⁰

In comparison, the Rap Back program captures activity by potential attackers in an effort to prevent the attack from occurring, possibly before the attacker radicalizes.⁶¹ The DSB TMU approach harkens back to the model mentioned by Baker, using all soldiers as sensors while empowering commanders to take action to prevent a violent attack. With the right direction and drive to empower supervisors, this approach can be adapted for public safety use as well.

E. CONCLUSION

This thesis seeks to address an under-studied gap in insider threat research. There are many journal articles and media reports on previous malicious insider attacks, but none of this work focuses on how to prevent a public safety official from using his or her access to carry out an insider terrorist attack.

This literature review described existing and ongoing research that addresses the current threat of a malicious insider, and how it relates to public safety. The first two sections showed how experts have defined what a malicious insider threat is, and two models for this threat profile: the infiltrator and the radicalized employee. Psychological models used to describe malicious insiders, as well as terrorism, were also discussed, along

⁵⁸ Defense Science Board, *Task Force Report: Predicting Violent Behavior* (Washington, DC: Department of Defense, 2012), 5, <http://www.acq.osd.mil/dsb/reports/predictingviolentbehavior.pdf>.

⁵⁹ Defense Science Board, 5.

⁶⁰ “Threat Management Unit,” Naval Criminal Investigative Service, accessed September 7, 2017, <http://www.ncis.navy.mil/CoreMissions/CI/Pages/ThreatManagementUnit.aspx>.

⁶¹ Babcock, “PIA: NGI Rap Back Service.”

with their effect on studying this threat to attempt to prevent it through psychological measures. Finally, the last section reviewed some of the current programs in use by federal agencies and the U.S. military to prevent this threat, and provided recommendations for how organizations can prevent and deter a malicious insider from operationalizing an attack.

III. RADICALIZATION OF AN ALREADY SWORN FIRST RESPONDER

The term “insider threat” frequently elicits thoughts of a disgruntled employee who decides to avenge some perceived grievance against an employer either by violence or through the theft or sabotage of company information or equipment. Cases such as former Los Angeles Police Department Officer Christopher Dorner, who killed four people and wounded three in response to frustrations with his employer, demonstrate that despite the unique work environment and bond shared between first responders, public safety agencies face the same risk of violence as private-sector employers.⁶²

This chapter, however, focuses on a potentially more significant threat: that of a first responder who is not aggrieved specifically by his or her organization, but who radicalizes after becoming an employee and decides to use his or her position within that organization to further a terrorist objective.

An attack by a radicalized first responder has not occurred domestically, but like other terrorist tactics, this threat is likely to migrate to the United States in the future; foreign terrorist organizations (FTOs) such as al Qaeda and the Islamic State (ISIS) have already voiced desires to inspire first responders to carry out attacks.⁶³ This chapter first examines four cases of insiders who were radicalized, including the history of the case itself and the damage caused; the chapter then examines how the individual radicalized, and reviews indicators that were either noticed or not noticed. Following the case studies, the next sections review why these insiders were motivated to radicalize, and what these cases tell us about the types of indicators that are usually present, but missed, when an insider radicalizes. Finally, this chapter concludes with recommendations to help public safety agencies better address the problem of insider radicalization.

⁶² Mallory Simon, “Alleged Cop-Killer Details Threats to LAPD and Why He Was Driven to Violence,” CNN, February 9, 2013, <http://www.cnn.com/2013/02/07/us/dorner-manifesto/index.html>.

⁶³ *Inspiration, Not Infiltration: Jihadist Conspirators in the United States: U.S. House Committee on Oversight, Subcommittee on National Security, Subcommittee on Health Care, Benefits, and Administrative Rules*, 114 Cong. 1 (2015) (testimony of Brian Michael Jenkins), <https://www.rand.org/pubs/testimonies/CT447.readonline.html>.

A. CASE STUDIES

As no public safety official has yet to conduct a domestic terrorist attack, it is necessary to look to examples of radicalization among government employees in the United States as well as overseas. Of the four cases presented in this section, two involved persons in the United States: one a soldier and the other a public employee. The third case comes from overseas, while the fourth case involves a local police officer who, although he did not carry out a violent attack, was in a position to do so after radicalizing.⁶⁴ These cases help describe the risk that a violent insider represents, and also indicate the types of behaviors and precursors to an attack that such individuals may demonstrate.

1. Nidal Hasan

One of the deadliest malicious insider attacks in the United States occurred on November 5, 2009, at Fort Hood, when Nidal Hasan killed thirteen and wounded over thirty soldiers and civilians at the soldier readiness center. Hasan, a psychiatrist assigned to Fort Hood, began showing signs of disgruntlement and radicalization early in his career, indicating that there were opportunities for intervention that could have prevented this attack. These signs were noted by members of Hasan's chain of command, as well as by fellow soldiers, but actions were not taken to investigate his movement to violence.

Hasan was born in the United States to two Palestinian parents, and was raised as a devout Muslim. He graduated from Virginia Tech in 1992 with an engineering degree and began his service with the U.S. Army in 1995. In 1997, he attended the military's medical school at the Uniformed Services University of the Health Sciences; he graduated in 2003, continuing his psychiatry residency at Walter Reed Army Medical Center.⁶⁵

⁶⁴ Another example is the 1984 assassination of Indira Gandhi by two of her Sikh bodyguards, Satwant Singh and Beant Singh. The Gandhi case highlights the ability of an individual who is trusted and trained with weapons to get close to an important person and carry out an attack such as an assassination. Because that case is based on revenge and not attributed to radicalization, it is not discussed further in this chapter.

⁶⁵ *A Ticking Time Bomb Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack: Hearing before the Committee on Homeland Security and Governmental Affairs, United States Senate*, 112 Cong. 1 (2011), 27.

During this time, many of Hasan’s fellow soldiers and physicians noted disturbing conduct linked to Major Hasan’s views about radical Islamic extremism. According to the congressional inquiry into the Fort Hood attack, “classmates—who were military officers, some outranking Hasan—described him as having ‘fixed radical beliefs about fundamentalist Islam’ that he shared ‘at every possible opportunity’ or as having irrational beliefs.”⁶⁶ Justifying fratricide by Muslim soldiers against non-Muslims and defending the attacks on September 11, 2001, by Osama bin Laden were a few of the topics that raised the suspicions of Hasan’s instructors and peers, and prompted reports of these concerns to be sent through Hasan’s chain of command for inquiry.⁶⁷ Hasan also stated that “Sharia law trumped the Constitution,” and equated bombers to U.S. service members.⁶⁸ Hasan’s outward espousing and preaching of an opposing ideology should have prompted further scrutiny and investigation.

Later in his career, Hasan was assigned to Fort Hood, Texas. While there, he counseled U.S. service members returning from the battlefields of Afghanistan and Iraq; he was one of the initial mental health professionals to see and advise service members in their fight against battle fatigue and post-traumatic stress disorder (PTSD). During this assignment, fellow soldiers reported that Hasan was extremely vocal to these returning troops about his convictions.⁶⁹

Prior to his arrival at Fort Hood in December 2008, members of the FBI San Diego Joint Terrorism Task Force intercepted email communications from Hasan to Anwar al-Awlaki, an influential Salafist imam who would later become the leader of al Qaeda Arabian Peninsula (AQAP), and identified the email as a “product of interest.”⁷⁰ These

⁶⁶ S., *A Ticking Time Bomb*, 29.

⁶⁷ S., 31.

⁶⁸ *Findings of the Department of Defense Independent Review Relating to Fort Hood: Hearing before the Full Committee of the Committee on Armed Services, House of Representatives*, 111 Cong. 2 (2010), 9, <https://www.gpo.gov/fdsys/pkg/CHRG-111hrg57664/pdf/CHRG-111hrg57664.pdf>.

⁶⁹ *Lessons from Fort Hood Improving Our Ability to Connect the Dots: Hearing before the Subcommittee on Oversight, Investigations, and Management of the Committee on Homeland Security, House of Representatives*, 112 Cong. 2 (2012), 2.

⁷⁰ H.R., 5.

emails, which are mostly classified, show Hasan pledging his assistance to al-Awlaki and discussing the use of suicide bombs to kill soldiers in order to save fellow Muslims.⁷¹ The FBI Washington Field Office later identified Hasan as a military officer, but decided not to contact his chain of command for fear of besmirching his reputation.⁷²

Hasan made no attempt to disguise his identity, or to communicate covertly abroad. This included using an email address that used his proper name in his communications with al-Awlaki.⁷³ Looking back, “an analysis of the full extent of Hasan’s communications would have shown that Hasan’s interest in the Suspected Terrorist [al-Awlaki] belied any conceivable research purposes.”⁷⁴ Hasan further offered his assistance, telling al-Awlaki to “keep me on your rolodex.”⁷⁵ Hasan was not only considering action, but was moving toward committing a violent act. However, because others had recognized his radicalization, with proper intervention, it still would not have been too late to prevent Hasan from carrying out his attack.

Hasan displayed multiple indicators leading up to his attack on the soldier readiness center; although the indicators were recognized, they were not properly acted upon. It is apparent that Hasan was in the process of radicalizing, even if the Army did not consider him a real threat. He was espousing a form of radical Islam, was communicating with a FTO, and had openly spoken out against U.S. military actions when he advocated for killing U.S. service members in the name of jihad. The U.S. Army was aware of his actions and beliefs, but chose not to act upon complaints and suspicions.

A key finding of this case study is that Hasan used his status as an Army officer to both access the base and to explain away his communications with Anwar al-Awlaki and

⁷¹ H.R., 2.

⁷² H.R., 14.

⁷³ William H. Webster Commission, “Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009,” Internet Archive, accessed September 1, 2016, 41, <https://ia600501.us.archive.org/32/items/final-report-of-the-william-h.-webster-commission/final-report-of-the-william-h.-webster-commission.pdf>.

⁷⁴ H.R., *Lessons from Fort Hood*, 64.

⁷⁵ H.R., 31.

his strange internet research. Today, this type of behavior would be seen as a person moves up Moghaddam's "staircase to terrorism"; at this step on the staircase, the person would be considered a legitimate threat to the organization. Hasan was not an anomaly that came out of the shadows, unknown to anyone; he was a fellow soldier who was openly displaying signs of radicalization that were seen but not acted upon.

As a result of this attack, the DoD has instituted policies to protect against and prevent the threat of a malicious insider. The DoD has adopted a more cohesive model of "my brother's keeper," in which everyone watches out for each other, and has established threat management units (TMUs) to educate soldiers and keep them aware of signs of potential radicalization.⁷⁶ This education of U.S. military staff and leadership, coupled with strong command intent, is a model that public safety agencies could reproduce to prevent a violent malicious insider from radicalizing and carrying out an attack.

2. Syed Rizwan Farook

On December 2, 2015, Syed Rizwan Farook, along with his wife, Tashfeen Malik, executed one of the few direct insider terrorist attacks in the United States in support of a FTO. Using his access as a food inspector for the San Bernardino County Department of Public Health, Farook attended, and later returned with Malik, to a holiday party at the Inland Regional Center, where he shot and killed fourteen and injured twenty-two people. After a four-hour manhunt, Farook and Malik were killed in a gunfight with police officers.⁷⁷

Farook graduated from California State University San Bernardino with a degree in environmental health, and was hired by San Bernardino County in 2010 as a seasonal employee; he gained a permanent position on February 8, 2014.⁷⁸ Family members

⁷⁶ Baker, "Change of Detection."

⁷⁷ Rory Carroll, Yvette Cabrera, and Paul Lewis, "How San Bernardino Shooters Killed 14 People after Christmas Party 'Dispute,'" *Guardian*, December 3, 2015, <https://www.theguardian.com/us-news/2015/dec/03/how-san-bernardino-shooters-killed-14-people-after-christmas-party-row>.

⁷⁸ Saeed Ahmed and Ralph Ellis, "Mass Shooting at Inland Regional Center: What We Know," CNN, December 5, 2015, <http://www.cnn.com/2015/12/03/us/what-we-know-san-bernardino-mass-shooting/index.html>.

described Farook as an “observant Sunni Muslim” who had made multiple trips to Saudi Arabia, including a trip in 2013 to Mecca for his hajj.⁷⁹ He also attended morning and evening prayers at the Islamic Center of Riverside each day, but “kept a bit of a distance between him and other people,” according to the Center’s director, Mustafa Kuko.⁸⁰

On the morning of the attack, Farook attended a combination staff meeting and holiday party with his coworkers. After approximately one hour, he exited the meeting, leaving a black duffle bag containing an improvised explosive device under the table where he was sitting.⁸¹ Farook returned approximately one hour later with Malik, both of whom were dressed in black tactical clothing and armed with two rifles and two handguns.⁸² During the attack, according to the FBI, Malik posted on Facebook, “We pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi,” which is believed to be directed to the leader of ISIS, Abu Bakr al-Baghdadi.⁸³ After the assault, while circling around the city of Redlands, a patrol officer recognized the description of the couples’ rental vehicle, and pursued them.⁸⁴ Farook and Malik fired their weapons at responding officers, and were eventually killed in the gunfight that ensued.

According to the FBI, Farook had begun self-radicalizing in 2011, while employed in the county, by watching videos of Anwar al-Awlaki and sharing these views with his

⁷⁹ Jennifer Medina et al., “San Bernardino Suspects Left Trail of Clues, but No Clear Motive,” *New York Times*, December 3, 2015, <https://www.nytimes.com/2015/12/04/us/san-bernardino-shooting.html>.

⁸⁰ Adam Nagourney et al., “Couple Kept Tight Lid on Plans for San Bernardino Shooting,” *New York Times*, December 3, 2015, <https://www.nytimes.com/2015/12/04/us/san-bernardino-shooting-syed-rizwan-farook.html>.

⁸¹ United States of America. v. Enrique Marquez, Jr, 5:15MJ498, United States District Court for the Central District of California December 17, 2015, 25–26, 3, <https://www.justice.gov/opa/file/800606/download>.

⁸² Eli Saslow and Stephanie McCrummen, “‘Where’s Syed?’: How the San Bernardino Shooting Unfolded,” *Washington Post*, December 3, 2015, https://www.washingtonpost.com/national/wheres-syed-how-the-san-bernardino-shooting-unfolded/2015/12/03/2ee90128-9a15-11e5-8917-653b65c809eb_story.html.

⁸³ Pamela Engel, “Here’s the ISIS Message the Female San Bernardino Shooter Posted on Facebook during the Attack,” *Business Insider*, December 17, 2015, <http://www.businessinsider.com/isis-message-tashfeen-malik-posted-on-facebook-during-attack-2015-12>; United States of America. v. Enrique Marquez, Jr, 25–26.

⁸⁴ Joel Rubin et al., “‘All Hell Broke Loose’ as Police Chased the San Bernardino Shooters,” *Los Angeles Times*, December 13, 2015, <http://graphics.latimes.com/san-bernardino-chase/>.

neighbor and friend, Enrique Marquez.⁸⁵ Marquez helped Farook purchase the firearms used in the Inland Regional Center attack, and had previously plotted with Farook to shoot at cars on State Route 91.⁸⁶ According to senior FBI sources, Farook also is believed to have reached out to members of al Qaeda's Syrian affiliate Jabhat al Nusra, as well as al Shabaab in Somalia.⁸⁷ Farook also may have communicated with, or was inspired by, Mohamed Abdullahi Hassan, the man reportedly responsible for encouraging the attacks on the Garland, Texas, "draw Mohammed" cartoon contest.⁸⁸ This appears to prove that Farook was not affiliated directly with one group, as al Qaeda and ISIS were opposed to one another ideologically. Farook was seeking self-approval of his radicalization, even if that approval or guidance came from dueling ideologies. This path parallels Nidal Hasan's prior to the 2009 shooting at Fort Hood in: reaching out to foreign terrorists and watching radical imams such as al-Awlaki.

Both Nidal Hasan and Farook had acted strangely in the eyes of their friends and coworkers, but there was a difference. Hasan was more open; he raised the attention of his coworkers more than Farook did, and may have benefitted from better cover with a position in the military. Farook, however, became more insular and quiet, but never openly espoused radical views. In fact, months earlier, Farook's coworkers threw a baby shower for Farook and Malik, demonstrating his involvement with his peers and attempts to not appear self-isolating.

The only person who was in a position to alert authorities of Farook's radicalization was Enrique Marquez, the provider of the firearms used in the attack and fellow radicalizee. After their initial plot was aborted, the two began to distance themselves from one another. It is unknown if Marquez knew Farook was still seeking to carry out an attack, but he did

⁸⁵ Joel Rubin et al., "'All Hell Broke Loose' as Police Chased the San Bernardino Shooters," *Los Angeles Times*, December 13, 2015, <http://graphics.latimes.com/san-bernardino-chase/>.

⁸⁶ United States of America. v. Enrique Marquez, Jr, 3.

⁸⁷ "Everything We Know about the San Bernardino Terror Attack Investigation so Far," *Los Angeles Times*, December 14, 2015, <http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htlstory.html>; "San Bernardino Shooting a Terrorist Attack with Al Qaeda and ISIS Footprints," *AEI*, December 4, 2015, <http://www.aei.org/multimedia/san-bernardino-shooting-a-terrorist-attack-with-al-qaeda-and-isis-footprints/>.

⁸⁸ "Everything We Know"; "San Bernardino Shooting."

have knowledge of the prior plot. Again, it is important to note that Farook was not an infiltrator into the San Bernardino County employment system; he was a clean employee who had radicalized to a terrorist ideology during his time in his position.

The Farook case also illustrates how access enabled an employee to plan an attack and conduct reconnaissance at the attack site beforehand, without anyone questioning his activities. This venue was a familiar building to Farook, so he was aware of all the entrances and exits, and the estimated number of people who would be present during the holiday party and staff meeting.

Additionally, Farook was in contact with various FTOs, a pattern seen in all of the cases illustrated in this thesis. However, unless his employer, San Bernardino County, was monitoring Farook's internet usage in his off-time, it is unlikely that this would have been picked up. Still, since a counterterrorism investigation against Farook was never initiated, this was never a consideration. Farook did begin to change his behavior and outward appearance when he began further radicalizing, according to his neighbors and coworkers, who also mentioned he had become more reserved and less social.⁸⁹ These factors alone do not suggest Farook was radicalizing; when considered in the totality of the circumstances, however, these were key indicators that should have prompted further investigation. If Farook had been placed under surveillance, or a search warrant executed on his home, law enforcement would have found weapons and bomb-making materials which were later found at his residence after the attack on the Inland Regional Center.

Lastly, another indicator, though it may have been hard to find without access to Farook's personal computer, was that Farook watched radicalization videos featuring Anwar al-Awlaki. This, too, is a common indicator among these cases, as well as in external cases not presented in this thesis.⁹⁰ However, Enrique Marquez was privy to watching these videos with Farook while radicalizing and preparing for their initial plot.

⁸⁹ Emily Shapiro, "Shooting Suspect's Neighbor Says He Became 'More Withdrawn,'" ABC News, December 6, 2015, <http://abcnews.go.com/US/syed-farooks-neighbor-describes-withdrawn/story?id=35610054>.

⁹⁰ Some notable cases include Ahmad Khan Rahami, Umar Farouk Abdulmutallab, Tamerlan, and Dzhokhar Tsarnaev.

This is where Enrique Marquez had a missed opportunity for intervention. For public safety officers, this demonstrates the need to stress reporting of suspicious activities up and through the chain of command for review by law enforcement anti-terrorism personnel.

3. Mevlut Mert Altintas

On October 23, 2016, Mevlut Mert Altintas, an Ankara police officer, assassinated Andrey Karlov, the Russian Ambassador to Turkey, at an art exposition. Altintas, who called in sick to work that day, used his police credentials to obtain access to the event and side-step metal detectors and other security measures, allowing him close access to the ambassador.⁹¹

Altintas grew up in a small town called Söke along Turkey's Aegean coast, where his family still lives.⁹² This area of the country is generally known for its exporting of culinary snails, and not for terrorism.⁹³ Aside from being a hub for cotton production—a trade in which Altintas's parents, Hamidiye and Israfil, used to work—Söke appears to be a hub for right-wing ultra-nationalism.⁹⁴ There is no link between any nationalist groups in the assassination of Ambassador Karlov, which is worth noting when considering the motive for the killing.⁹⁵ The focus of this case study is directed more to Altintas's radicalization to a terrorist ideology while being employed by the Ankara Police Department.

Altintas was appointed to the Ankara Police Department in 2014.⁹⁶ Once appointed, he was assigned to the anti-riot police unit, where he worked for two and a half

⁹¹ Laura Pitel and Roland Oliphant, "Mevlut Mert Altintas: Boy from a Small Town on Aegean Coast Who Became a Murderer," *Telegraph*, December 21, 2016, <http://www.telegraph.co.uk/news/2016/12/20/mevlut-mert-altintas-boy-small-town-aegean-coast-became-murderer/>.

⁹² Pitel and Oliphant.

⁹³ Wikipedia, s.v. "Söke," July 1, 2017, <https://en.wikipedia.org/w/index.php?title=S%C3%B6ke&oldid=788380715>.

⁹⁴ Pitel and Oliphant, "Boy from a Small Town."

⁹⁵ Pitel and Oliphant.

⁹⁶ "Killer of Russian Envoy Had Provided Security for Erdogan: Report," *The National*, December 22, 2016, <https://www.thenational.ae/world/killer-of-russian-envoy-had-provided-security-for-erdogan-report-1.94049?videoId=5656421988001>.

years.⁹⁷ During this time, in 2015, Altintas allegedly traveled to Syria to fight with Jabhat al-Nusra against the Bashar al-Assad regime.⁹⁸ This raises an interesting point: How was a sworn law enforcement officer able to travel to a war zone on his own and not raise the suspicions of coworkers or superiors?

According to the Turkish newspaper *Zaman*, “Altintas’ psychological background indicates that he murdered a number of Syrian soldiers and that some of his colleagues were also killed.”⁹⁹ Turkish media states that Altintas “desired the act of killing” since his involvement in the Syrian conflict. This sheds light on who Altintas was, along with his motivations and ability to assassinate Karlov, and shows that psychological screenings were either ineffective or Ankara police disregarded the findings.

There is evidence to show that Altintas had been planning his attack on the envoy for some time. The week prior to the assassination, he had requested his commander to assign him to the Russian embassy security detail.¹⁰⁰ This can be seen as an attempt to perform pre-operational reconnaissance and intelligence gathering to help carry out his plan. Altintas also checked into a hotel near the art gallery where the assassination occurred a few days prior, and was seen in the gallery in the same suit, and with his badge on, that he would wear to carry out the attack, according to the exhibition coordinator, Timur Özkan.¹⁰¹

On the day of the exhibition, once within the venue, Altintas drew his service pistol and, without warning, shot Karlov in the back nine times.¹⁰² In the aftermath of the shooting, Altintas was heard saying, “Don’t forget about Syria, don’t forget about Aleppo.

⁹⁷ “Killer of Russian Envoy.”

⁹⁸ “The Killer of the Ambassador of Russia in Turkey Visited Qatar Several Times,” Alalam News, December 26, 2016, <http://en.alalam.ir/news/1902831>.

⁹⁹ “The Killer of the Ambassador.”

¹⁰⁰ “The Killer of the Ambassador.”

¹⁰¹ Pitel and Oliphant, “Boy from a Small Town.”

¹⁰² James Rothwell, “Mevlut Mert Altintas: The Policeman Accused of Killing Russian Ambassador Andrey Karlov?,” *Telegraph*, December 20, 2016, <http://www.telegraph.co.uk/news/2016/12/19/turkish-police-officer-shot-dead-russian-ambassador-andrey-karlov/>.

All those who participate in tyranny will be held accountable.”¹⁰³ He was killed soon afterwards by Ankara police officers responding to the incident. Because of his status as a police officer in that city, Altintas was able to gain access that only a small, trusted group would be given, facilitating the ambassador’s murder.

Based on his level of access—and because his credentials, where authentic, were not questioned—Altintas was able to get within ten feet of another country’s ambassador and murder him on national television in support of a FTO. Could this happen within the United States? Based on the Altintas case, it appears to be very possible. This case confirms the need to vet personnel appropriately, but also the need for coworkers to keep an eye on one another for behavioral signs of radicalization and potential violence.

Altintas was able to exploit his access to conduct reconnaissance of the ambassador in both the Embassy and around the art gallery prior to the exhibition, a common finding in pre-attack indicators. He then used his access as a police officer to get into the art exhibition and kill Karlov. Access is again seen as a major advantage that public safety employees have over regular civilians—an advantage that could be easily exploited by a radicalized first responder. An additional common indicator seen in this case was the communications with a FTO; Altintas even (allegedly) traveled to Syria to fight on the group’s behalf. If fellow members of Altintas’s unit were aware of this trip, this information should have been forwarded up the chain of command for further action, and may have put Altintas under enough scrutiny to have prevented the attack, or to have removed him from public service.

4. Nicholas Young

The final case considered in this thesis involves a police officer who radicalized, but who did not carry out an attack. Nicholas Young, a DC Metro Transit police officer, was arrested and charged with “attempt[ing] to provide material support to a designated foreign terrorist organization.”¹⁰⁴ He was found guilty on December 18, 2017. Young is

¹⁰³ Pitel and Oliphant, “Boy from a Small Town.”

¹⁰⁴ United States of America v. Nicholas Young., 1:16mj355 (Eastern District of Virginia) (2016).

believed to have radicalized to an extreme version of Islam while being employed with the Metro Transit Police Department. This case has not been extensively covered in literature, apart from the news reports of Young's arrest and criminal complaints against him, limiting available analysis of his motives.¹⁰⁵

Initially, Young was connected to a person of interest under FBI surveillance, Zachary Chesser, who was arrested in 2010 for "attempting to provide material support to al-Shabaab, another designated FTO."¹⁰⁶ Young was questioned about his association with Chesser, and he stated it would be his duty to report any suspicious activities. The following year, an undercover law enforcement officer reported on conversations he had with Young, stating that Young believed the FBI was surveilling him, and was acting cautiously to avoid being tracked; he boasted about the countermeasures he employed to avoid being surveilled and tracked. Young also began an association with Amine El Khalifi, who would later be arrested and charged with "attempting to use a weapon of mass destruction (an improvised explosive device), and detonate himself within the U.S. Capitol building."¹⁰⁷ In 2014, while still under the interest of the FBI, Young was approached by a confidential human source who asked Young for advice and assistance in joining ISIS, and how to best travel overseas without being caught.¹⁰⁸ Young had traveled twice to the region in 2011, while employed by the Metro Transit, to fight in Libya against the Qaddafi regime, giving him first-hand experience in traveling outside of the United States without attracting unnecessary attention.¹⁰⁹

Eventually, that confidential human source would feign a trip to Syria, and would communicate with Young as if overseas. During this time, the source would ask for support and advice on how to best navigate the area, and for financial support, which Young

¹⁰⁵ Rachel Weiner, "Police Officer for D.C. Subway System Accused of Trying to Help ISIS," *Washington Post*, August 3, 2016, https://www.washingtonpost.com/local/public-safety/metro-police-officer-arrested-on-terrorism-charges/2016/08/03/6b7541de-5981-11e6-9aee-8075993d73a2_story.html; *United States of America v. Nicholas Young*.

¹⁰⁶ *United States of America v. Nicholas Young*, 3.

¹⁰⁷ *United States of America v. Nicholas Young*, 6.

¹⁰⁸ *United States of America v. Nicholas Young*, 6.

¹⁰⁹ *United States of America v. Nicholas Young*, 6.

obliged by sending gift cards.¹¹⁰ Young was arrested soon after for his connection with and support for ISIS.

This case is important because it links a sworn public safety officer with supporting the goals of a FTO. This case is different, however, because Young did not use his position and access to accomplish that goal; but it does raise the question: Would Young have eventually exploited his position as a police officer to carry out a violent plot, and if so, would he have been successful? The available literature and court documents do not note that coworkers had suspicions about Young, which indicate he probably would have been successful in his attack if he were not being observed by the FBI. But, like Altintas, how does a sworn law enforcement officer travel to a war zone without attracting the attention of coworkers or any acquaintances during the hiring process or while employed? If Young's coworkers were taught to be vigilant and on the lookout for strange activities, this may have triggered further scrutiny.

5. Summary of Findings

Table 1 presents a short synopsis of each case along with relevant pre-attack indicators. These indicators highlight some of the behaviors exhibited by past perpetrators of insider violence in furtherance of a terrorist ideology. These are signs that were missed, that today are recognized as markers of someone about to carry out a violent attack. By recognizing these markers, public safety leaders can institute policies that help members identify these signs and make actionable decisions to prevent a violent attack.

¹¹⁰ United States of America v. Nicholas Young, 6.

Table 1. Summary of Pre-attack Indicators from Case Studies

Case Summary	Missed Pre-attack Indicators				
	<i>Watched Radicalization Videos</i>	<i>Traveled Abroad to Train or Fight</i>	<i>Spoke with a FTO</i>	<i>Organization Noted Behavior Change or Issue</i>	<i>Conducted Pre-attack Recon</i>
Nidal Hasan On November 5, 2009, opened fired on soldiers and civilians at Fort Hood, TX, killing 13, wounding 33.	XX		XX	XX	XX
Syed Farook On December 2, 2015, attacked a holiday party at the Inland Regional Center in San Bernardino, CA killing 14 and wounding 22.	XX	XX	XX		XX
Mevlut Mert Altintas On October 23, 2016, assassinated Andrey Karlov, the Russian Ambassador to Turkey, at an art exposition.		XX	XX	XX	XX
Nicholas Young DC Transit Police Officer who Radicalized- No Attack, but provided financial support to a FTO.		XX	XX		N/A

In all of these cases, the individuals had communicated with a FTO; in the cases involving an actual attack, the perpetrators conducted pre-attack reconnaissance of the target area. This is important because it illustrates the effectiveness of exploiting a position as a first responder to carry out an attack, and how devastating this tactic can be.

B. FOCUSING ON BEHAVIORS

According to Dr. Eric Cole, “over eighty percent of personnel who were insider threats exhibited some form of indicators and behavior modifications before they conducted their attack.”¹¹¹ The case studies examined tend to support what is seen in the literature, which is that individuals who pose a threat almost always demonstrate some sort of odd or dangerous behavior, and such behaviors can be seen as indicators that, when recognized, can help prevent future attacks.

Employees and supervisors should be aware of what Liang and Biros specifically mention as indicators of potential insider threat activity: “suspicious verbal behavior, confrontation with peers or supervisors ... problems of accepting feedbacks and criticisms, and anger management issues.”¹¹² Nidal Hasan demonstrated anger against what he felt were unjust military actions by the United States, and was unreceptive to constructive criticism while in his residency.¹¹³

It is fair to assume that someone might notice a behavioral change in a coworker, and could be empowered to prevent that coworker from carrying out a nefarious action. Although these behaviors changes alone do not indicate that an employee will carry out some form of attack, they are common characteristics of those who have carried out attacks in the past. If public safety agencies educate their members and keep them on the lookout for these characteristics as potential indicators of either radicalization or disgruntlement, an attack may be thwarted in the planning stages. Currently, police and fire departments are putting a lot of effort and emphasis into preventing PTSD and depression-related suicide by their members. Initiatives like the Code Green Campaign are educating first responders about the signs and symptoms of someone who may be contemplating suicide and empowering those same responders to report coworkers who may need help.¹¹⁴

¹¹¹ Cole, “SANS Analyst Program,” 5.

¹¹² Nan Liang and David Biros, “Validating Common Characteristics of Malicious Insiders: Proof of Concept Study,” *IEEE International Conference on System Sciences* (January 2016): 3718, <http://doi.org/10.1109/HICSS.2016.463>.

¹¹³ H.R., *Relating to Fort Hood*, 9.

¹¹⁴ The Code Green Campaign, accessed September 23, 2017, <http://webcache.googleusercontent.com/search?q=cache:http://codegreencampaign.org/>.

Some of the signs of a person radicalizing (listed further in Appendix A), including “withdrawal, mood changes, reckless or risky activities and, rage and anger,” also correspond to potential suicidal ideations. Reporting of this activity would be beneficial to the first responder in both cases.

Figure 1 illustrates the current recommendations for preventing suicide within the law enforcement community, which are equally applicable to all public safety fields. Noticing behavioral changes requires a unique perspective; only people who spend large, intimate amounts of time together—like first responders—may be able to pick up on the changes. By recognizing the parallel behaviors and actions between a potential suicide victim and a person radicalizing, public safety agencies can leverage existing programs to aid in preventing a first responder from carrying out a terrorist act.

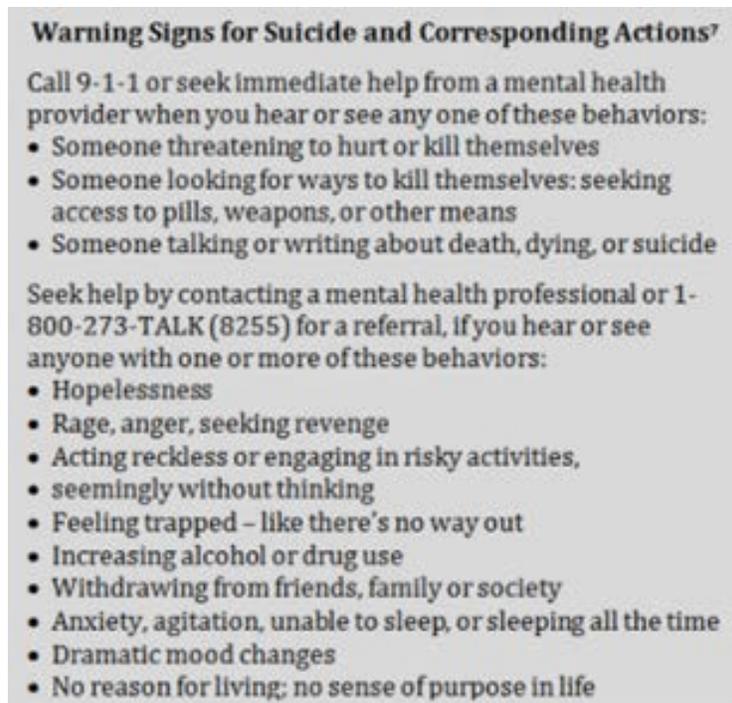


Figure 1. Suicide Warning Signs¹¹⁵

¹¹⁵ Source: “Preventing Law Enforcement Suicide,” COPS, accessed September 28, 2017, https://cops.usdoj.gov/html/dispatch/06-2014/preventing_officer_suicide.asp.

This type of education and empowerment campaign can be applied to suspicious activity reporting of fellow first responders to get the appropriate resources involved to help the individual in need, and potentially prevent a terrorist act.

Referring back to the Farook case, Farook's neighbors noticed a change in his appearance and behavior; he became more withdrawn and changed his physical appearance to favor a long beard and long robes. This is a delicate situation; people are afraid of stereotyping others, especially Muslims, out of what Ali Rizvi calls "phobia of being called an Islamophobe."¹¹⁶ Organizations should recommend that their employees report on behaviors that are out of the ordinary, regardless of political correctness, which was cited as a major reason why Nidal Hasan was not stopped.¹¹⁷ This is not to suggest that personnel should profile other people, but it is worth noting when other people change their behaviors; these changes can be indicators of potential radicalization. As mentioned previously, people can be different, but when those differences are indicators of suspicious activity, it is crucial that their behaviors are reported. Early recognition of these changes, and more importantly early reporting of these changes, could have prompted further inquiry into Farook, and possibly uncovered his plot.

A final common factor seen in these cases is the fact that all perpetrators conducted pre-attack surveillance on the locations where they carried out their attacks. But because these locations are where the perpetrator worked, with the exception of Altintas, no one would have thought it was suspicious for a fellow employee to be looking around the building. This reinforces how difficult it is to capture an individual who is conducting such surveillance, unless the individual does not belong in a specific location. In the case of Altintas, he asked to be assigned to the embassy security detail, which may or may not have raised the attention of his coworkers; when he stayed at the hotel across the street from the art gallery, this in itself would not have aroused suspicion unless it was realized and scrutinized by a coworker who knew Altintas's job duties.

¹¹⁶ Ali A. Rizvi, "The Phobia of Being Called Islamophobic," *Huffington Post*, June 28, 2014, http://www.huffingtonpost.com/ali-a-rizvi/the-phobia-of-being-called-islamophobic_b_5215218.html.

¹¹⁷ H.R., *Relating to Fort Hood*, 13.

C. CONCLUSION

The threat of a first responder who is already employed within an agency one day radicalizing to an extremist or terrorist ideology is real, especially because of the access the position affords the responder. The threat from a radicalized insider is significant, but the good news is that these case studies of radicalized insiders confirm the findings of the broader research. Such individuals almost always demonstrate odd or threatening behavior, which can be used to help identify them before they carry out acts of violence. Recognizing the behavioral changes that accompany movement to carrying out a violent act will be vital to public safety agencies working to avert this type of incident within their jurisdictions.

Given the exceptionality of this threat, public safety agencies have a duty to take additional precautions not just before employees are hired, but throughout their employment. To do this, they need to increase awareness of this issue, educate their leadership and employees, and instill a culture of vigilance while providing a reporting mechanism for suspicious employee behavior.

Increased awareness of the problem and increased vigilance is a strong method of preventing a violent attack from within, and should be adopted within public safety agencies. If agencies institute a program for educating mid-level management and briefing members of police and fire departments—with the program focusing on some of the behaviors described in this chapter, combined with awareness of precipitating events in the employee's life these—they may have a better chance of detecting a malicious insider who is moving toward a violent action.

This chapter has examined one kind of insider threat: an individual who becomes radicalized while employed as a first responder. The next chapter examines a second type of insider threat: that of a Manchurian insider—someone who is radicalized before becoming a public service employee, and who seeks to infiltrate a police or fire department to specifically carry out an attack.

IV. CLEAN-SKIN INFILTRATORS AND POTENTIAL METHODS TO THWART THEM

This chapter focuses on how someone who does not have a criminal record and adheres to an extremist or terrorist ideology can use that “clean skin” to gain employment as a police officer or firefighter. This can occur because these agencies are not screening for behaviors associated with radicalization.¹¹⁸ As explained in Chapter I, a terrorist or other extremist group would do well to consider implanting one of their trusted individuals within a target public safety organization, because it gives them unrestricted access to a trusting public.¹¹⁹

Various extremist groups, such as the Ku Klux Klan (KKK), al Qaeda, and ISIS, have already made calls for bad actors to infiltrate into an organization.¹²⁰ In fact, there are reports of members of the KKK infiltrating multiple law enforcement agencies throughout the United States.¹²¹ In 2006, the FBI noted in an intelligence assessment that “white supremacist leaders and groups have historically shown an interest in infiltrating law enforcement communities and recruiting law enforcement personnel,” acknowledging that the biggest threat comes from the access gained to restricted areas, as well as from the ability to gather intelligence.¹²²

This chapter explains that, due to the relative ease with which clean-skin infiltrators can gain employment, they are a legitimate threat to public safety agencies and the public. It presents the two different manifestations of this type of insider and explains that the

¹¹⁸ Emergency medical services (EMT) are not considered in this study because many fire departments in the United States handle this discipline, or there is a reliance on private companies to provide this service. EMS would require a separate study in itself.

¹¹⁹ David BaMaung et al., “The Enemy Within? The Connection between Insider Threat and Terrorism,” *Studies in Conflict & Terrorism* 41, no. 2 (October 2016): 9, <http://doi.org/10.1080/1057610X.2016.1249776>.

¹²⁰ Jenkins, *Inspiration, Not Infiltration*, 1–2; Alice Speri, “The FBI Has Quietly Investigated White Supremacist Infiltration of Law Enforcement,” *The Intercept*, January 31, 2017, <https://theintercept.com/2017/01/31/the-fbi-has-quietly-investigated-white-supremacist-infiltration-of-law-enforcement/>.

¹²¹ Speri, “White Supremacist Infiltration.”

¹²² Speri.

simple fact that they *can* infiltrate—regardless of their motivations—is the actual threat. The chapter then compares the differences between an infiltrator and a disgruntled insider, and explains why a disgruntled employee is a poor recruit to carry out a terrorist act. Finally, three threat assessment methods are discussed for their use in screening applicants for potential malicious infiltrators during state and local public safety agencies’ employment processes.

A. TYPES OF CLEAN-SKIN INFILTRATORS

There are two main types of clean-skin malicious infiltrators that can gain access into a public safety agency. The first is the clean-skin radical. At some point in his or her life, this individual comes to believe in and adopt a radical ideology, later prompting a desire to infiltrate the public safety field as a means to carry out an attack in the name of that ideology.

The second type of clean-skin infiltrator is the individual who is raised from a young age within a community that espouses radical or extremist views, and who is groomed to maintain a clean record with the intent of infiltrating a public safety agency on behalf of the group. This speaks to the truest sense of the “The Manchurian Responder” idea in that this individual may only know that his or her purpose is to join a local or state public safety department, learn the structure of the organization, gain the trust of its employees, and then carry out an attack controlled by someone within the extremist group. This type of infiltrator is less likely to exist because of the required constraints: the need to maintain cover for the duration of his or her life, keep a clean criminal record, and then successfully get hired; a long-term plot like this one allows ample opportunities for disruption. Due to the complexity and length of time needed to maintain this clean appearance, it seems this tactic of infiltration would be less likely in the United States. But if it were carried out, it would be incredibly damaging to the credibility of all public safety agencies, making this a low-probability, high-impact event.

For example, the use of infiltrators was seen in Afghanistan in June 2017, when two police officers reportedly opened fire and killed six fellow police officers in Kandahar

province.¹²³ A spokesperson for the Taliban, Qari Yusouf Ahmadi, claimed responsibility for the attack, stating that “both attackers were their men who joined the police rank just to carry out such attack and both devoted their lives for their aim.”¹²⁴ Ahmadi’s statement may be embellished and intended to further undermine the morale of the Afghan National Police, but the attack was at least in part successful because of the lack of sufficient vetting for military and public safety positions.

B. INFILTRATORS VERSUS DISGRUNTLED INSIDERS AS POTENTIAL THREATS

When imagining the ideal candidate to carry out an attack from within, it was initially believed that a disgruntled employee would be the best person for the job. But, according to the Delphi panel of experts selected by Nicholas Catrantzos, research into private-sector insider threats suggests “it preferable by a 2:1 ratio to infiltrate an agent rather than recruit one already in place.”¹²⁵ This may be because a terrorist organization would not attempt to implant an operative whom they did not already trust. Trying to get a current employee to shift alliances, however, may be seen as more challenging, and may risk compromising the larger plot. If an organization infiltrates an operative who is loyal to its ideology, the organization does not have to indoctrinate a new follower to conduct violence on its behalf. This may be true in the private sector, but there have been no cases to support that assertion in the public safety realm.

As the infiltrator’s purpose is to seek and exploit vulnerabilities, they do not need to become experts on how the organization functions. There is therefore a greater risk of new employment being exploited, further emphasizing the necessity of stringent vetting. Catrantzos’s Delphi experts believe that a malicious insider would only need enough time to enable an attack, and would not need to “masquerade” as an employee for a prolonged period of time.¹²⁶ It is easy to imagine how an insider could plan calculated stress tests of

¹²³ Mirwais Khan, “Afghan Officials: 6 Police Killed in Insider Attack,” AP News, June 4, 2017, <https://apnews.com/d551cacf986746d286793ce4062aee89%20%0D> .

¹²⁴ Khan.

¹²⁵ Catrantzos, “No Dark Corners,” 37.

¹²⁶ Catrantzos, 43.

an organization's policies and procedures to find weak points and then simply feign ignorance if caught, as supervisors or coworkers might easily brush off the mistake as a "typical rookie move."

Catrantzos believes that, "unless the new hire does something egregious to excite remark, he or she is unlikely to face a random audit, active monitoring of computer key strokes or time and duration of access into a given work space."¹²⁷ The rookie officer is usually given a grace period to learn the baseline skills to be successful within the department, and is not punished for minor mistakes or infractions if they are seen as part of the learning process.

Why would a terrorist or extremist group go through the trouble of inserting a group member when there is already a fair supply of current employees, some of whom may be harboring a grievance against the organization and may be willing to assist in a plot against that organization? Catrantzos states simply that "infiltrators are the better choice for a terrorist seeking an insider for a devastating attack," suggesting that terrorists would prefer to infiltrate their own members, because established employees have their own sets of inherent problems.¹²⁸ He also asserts that, while career employees may best know how to disable or cripple an organization, they are often too ego-driven and focused on their own grievances.¹²⁹ This lends to the belief that the disgruntled employee would be difficult to direct, potentially compromising details of an operation because they were not consulted, or disagree with the plan.¹³⁰ An individual who is radicalized to an ideology is a different kind of threat than someone aggrieved over a missed promotion or a simple workplace gripe.

According to Catrantzos, if the infiltrator eludes detection or interference, he or she is free to operate in the dark corners of insufficient oversight and supervision, as long as his or her behavior and work performance do not deviate too much from the norm as to

¹²⁷ Nicholas Catrantzos, *Tackling the Insider Threat* (Alexandria, VA: ASIS International, 2010), 21, <http://www.popcenter.org/library/crisp/insider-threat.pdf>.

¹²⁸ Catrantzos, 17.

¹²⁹ Catrantzos, "No Dark Corners," 42.

¹³⁰ Catrantzos, 42.

invite attention.¹³¹ Maintaining an appropriate level of stealth is imperative to the success of an insider operation. If the infiltrator is compromised, the entire operation could be jeopardized.

What differentiates these two sub-groups is their motivations. The disgruntled employee is driven more by a desire to fix a personal wrong, whereas the infiltrating terrorist is not motivated by a petty workplace issue; this type of infiltrator generally would not be with the company long enough to gain that negative experience. His or her grievance is derived from a greater problem, one borne of a cultural or group identity. They want to join a public safety department not because they are angry at the police or fire service as a whole, but to gain the access needed to carry out their attack in support of the greater grievance, not the local one seen in the disgruntled employee.

C. THREAT ASSESSMENTS

Threat assessments offer a framework for the evaluation of potential applicants based on lessons learned through previous cases. They are designed to identify, manage, and assess an individual's likelihood to commit violence. The assessments can be used to establish baseline criteria regarding whether or not an individual is harboring threatening behaviors or could present a threat to the organization. But are they effective at capturing a focused individual who is trying to infiltrate a public safety department to commit violence? This section presents three leading models for assessing individuals for potential violence, though none are designed for initial screening at the beginning of an individual's career. These models are evaluated for their efficacy and translatability into a pre-employment screening method to potentially identify a radicalized infiltrator.

The first model, used by the FBI's Behavioral Sciences Unit (now known as the Behavioral Analysis Unit), is focused on developing a personality profile of a likely attacker based on witnessed characteristics of prior violent perpetrators. The second, introduced by the U.S. Secret Service to combat targeted violence in schools, is based on the belief that anyone is capable of carrying out an attack, and the person will not advertise

¹³¹ Catrantzos, *Tackling the Insider Threat*, 18.

that an attack is being planned. This model also believes that there is generally a precipitating event that sends the perpetrator down the road to committing violence. The third method, which is presented by the Defense Science Board (DSB), advocates for cataloguing behavioral indicators and precursor indications of violence, and educating soldiers to recognize these signs to prevent targeted violence.

Proper assessment of a potential asset versus a potential threat in employees is something all employers should take seriously both during hiring and throughout employment. A continued emphasis on developing psychological profiles of potential offenders has done little to stop mass violence, and therefore does not appear to be an effective tool for preventing an act of targeted violence. Each of these models has something it can contribute to preventing targeted violence, but their use is questionable for screening candidates out during the hiring process.

1. FBI Profiling Method

The FBI's Behavioral Analysis Unit has a specific method for profiling offenders in an attempt to identify a possible perpetrator. The model focuses on gathering information from a crime and generating a set of hypotheses to predict targeted violence, and to develop a personality profile.¹³² These hypotheses are generated from the "characteristics—physical, demographic, personality, and others—of the person most likely to have committed the crime."¹³³ This approach, however, is not used in screening of potential employees; it is focused on developing profiles of criminal offenders, based on analysis of their behaviors before and after a crime.¹³⁴ This is an important distinction to mention when the assessment is being discussed in a realm of pre-employment screening.

¹³² Marisa Reddy, et al., "Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches," *Psychology in the Schools* 38, no. 2 (March 2001): 161, <http://doi.org/10.1002/pits.1007>.

¹³³ John E. Douglas et al., "Criminal Profiling from Crime Scene Analysis," *Behavioral Sciences & the Law* 4, no. 4 (1986): 414–415.

¹³⁴ Katherine Ramsland, "Criminal Profiling: How It All Began," *Psychology Today*, March 23, 2014, <https://www.psychologytoday.com/blog/shadow-boxing/201403/criminal-profiling-how-it-all-began>.

This method is retrospective in the sense that it begins at the time of the crime and works backward to try to identify the perpetrator. When public safety departments are hiring candidates, they are not looking through a crime-prevention lens; they are focused on hiring the best people for vacant positions. Personality profiling falls short of its goal to identify a potential threat because it is strictly based on personality characteristics of prior perpetrators of violence and not on behaviors and actions. Also, a person who willfully attempts to infiltrate a police or fire department is unlikely to display outward signs that may lead an investigator to think that the applicant is hiding something. A deeper evaluation of the applicant's personal history would be needed to put the pieces together, which the Behavioral Analysis Unit is recommending in its assessments.

2. Secret Service Targeted Violence Method

An alternative method is “prospective profiling,” which is “used both to *identify* individuals likely to become perpetrators (absent a behavior or communication that brings someone to official attention) and to *assess* a given individual who has come to someone's attention for some troubling communications or behavior.”¹³⁵ Expanding from the FBI model, the Secret Service method attempts to develop a profile of what a potential perpetrator looks like in an effort to prevent an attack from occurring. This approach is also not used in the screening of prospective employees, but was developed in an effort to prevent school shootings. Again, the focus is on prevention of a crime through prediction, not on recognition of behaviors that hint at potential violence.

Reddy et al. give three key guiding principles to their threat assessment approach. The first is that there is no single, simple profile of a subject who threatens targeted violence. Instead, they believe that attacks result from how the perpetrator relates with the situation, target, and setting.¹³⁶ Each individual interprets their environment differently, which means different motives may trigger a violent response in different people.

¹³⁵ Reddy et al., “Evaluating Risk for Targeted Violence in Schools,” 161–162.

¹³⁶ Reddy et al., 167.

The next key guiding principle is that there is a difference between making a threat and actually posing a true threat.¹³⁷ Reddy et al. elaborate on this difference, stating that no public figure assassin ever warned the target before committing murder if the perpetrator was fixated on completing his or her objective.¹³⁸ Simple rhetoric may not be the only sign a fellow first responder would recognize, but if combined with other signs such as social isolation and change in behavior, these indications may point to someone who has radicalized and is moving toward action.¹³⁹

The third guiding assumption is the keystone to Reddy et al.'s argument: that "targeted violence is not random or spontaneous; it does not occur because someone 'just snapped,'" but rather it is ascribed to a behavior directly attributed to a defined pattern of thinking and behavior.¹⁴⁰ Most incidents trace back to a triggering point that led the perpetrator down the road to violence, such as pre-employment radicalization.

This model does work for a person who is already within the agency, like those referenced in Chapter III. However, it would be difficult to use for someone who is veiling his or her true intentions to infiltrate a public safety agency. The infiltrator who does make it in may begin to show signs of having previously radicalized and may offer an opportunity for intervention. If coworkers can identify behaviors that link a person to radicalizing, and are empowered to notify their supervisors of their concerns, this would be a key step in preventing a violent attack from a malicious insider. Also, knowing that anyone is capable of conducting this type of violence, and that something has motivated and driven the individual to violence, provides an opportunity for intervention.

¹³⁷ Reddy et al, 167.

¹³⁸ Reddy et al., 168.

¹³⁹ Reddy et al., 168.

¹⁴⁰ Reddy et al.,168.

3. Department of Defense Model

The DoD defines targeted violence as

Acts of pre-meditated attacks against specific individuals, populations or facilities with behaviors that precede and are related to their attacks. Perpetrators consider, plan and prepare before engaging in acts of violence. These behaviors are often detectable; providing an opportunity for disruption of the intended violence by utilizing a comprehensive, multi-disciplinary approach to assessment and intervention.¹⁴¹

Most perpetrators display signs of intent to act without necessarily voicing those intentions. These acts are not random, and therefore are disruptable if the signs are recognized and appropriately reported. While acts of terrorism are acts of targeted violence, it is important to understand that targeted violence is not always terrorism.

Since 2012, in an effort to prevent workplace violence, the DoD has focused on identifying those persons who may be planning targeted violence. The DoD visualizes targeted violence as an understanding of thoughts and behavioral processes that lead soldiers to attack fellow soldiers.¹⁴² The DSB reports that “the purpose of threat assessment is to identify potential perpetrators of targeted violence and to assess and manage the risks of such violence.”¹⁴³ The DSB believes that “the demographic and psychological characteristics central in profiling-based approaches to the identification of potential perpetrators of targeted violence are de-emphasized in favor of identifying ... behaviors consistent with future violence toward an identifiable target or targets.”¹⁴⁴ Psychoanalyzing and developing profiles of individuals does not prevent an attack because the profiles are not highly accurate in predicting targeted violence. However, cataloging behavioral characteristics that have been previously seen in perpetrators of targeted violence affords a better preventive strategy, based on actual incidents.

¹⁴¹ Defense Science Board, *Predicting Violent Behavior*, 14.

¹⁴² Defense Science Board, 20.

¹⁴³ Defense Science Board, 20.

¹⁴⁴ Defense Science Board, 20.

The DoD model also recognizes that violence stems from three causative factors. The model believes that the perpetrator is influenced by a triggering event, the current environment, and a belief that violence is the answer to his or her problems.¹⁴⁵ However, the triggering event may not be the tipping point to commit the act, as much as it may be the motivation to accept a differing ideology. The DoD theory is supported by consensus in literature, including an article by expert Dr. Mohammed Hafez and Creighton Mullins, whose radicalization model identifies grievances as a key trigger in initiating and seeking support for radicalization.¹⁴⁶ If a person has radicalized before he or she becomes a police officer or firefighter, that person may harbor these feelings, but would intentionally hide them as to not attract unneeded attention while in the employment process.

Infiltrators feel that justifiable violence is the only option to right a perceived grievance against themselves, or their group identity. In the case studies explained in Chapter III, all three attackers believed that violence was the only solution to their problems, which drove them to commit their attacks. This model appears to have the most translatability to local and state public safety agencies, but it still focuses on catching the employee who radicalizes, rather than preventing a radical from gaining employment. These three models offer effective methods for preventing targeted violence, but seem to offer little value in identifying a malicious infiltrator at the point of entry.

The individual committed to infiltrating a public safety department, in an attempt to blend in, will most likely not be displaying signs of radicalization. These individuals would not be espousing radical beliefs and making threats to an organization or individual while going through the employment process. The agency screening the individual would also not be privy to the applicant's past, so there would be no knowledge of a precipitating event or trigger that would either eliminate the applicant from the hiring process or increase scrutiny of the applicant. These models cannot predict behavior; rather, they attempt to assess dangerousness. However, this approach will not work if a committed infiltrator is masking his or her true intentions in order to gain access to a public safety department.

¹⁴⁵ Defense Science Board, 20.

¹⁴⁶ Hafez and Mullins, "The Radicalization Puzzle."

D. ANALYSIS

It may be believed that a group would do best to infiltrate as many operatives as possible to maximize the chances of success or magnitude of a plot. However, Corri Zoli believes that an attack of this nature would most likely be carried out by a lone-wolf operator, as opposed to a group of infiltrators. She says that many infiltrators “are often ‘clean-men’... committed, linked, or instructed by organizational [group] operatives—because they are less likely to be tracked, especially in the West,” because of sophisticated intelligence and law enforcement sharing services.¹⁴⁷ Additionally, the fewer individuals involved in a plot, the fewer opportunities for interdiction. The group or individual would now have a direct path through the front door to operationalize or facilitate a plot.

Public safety agencies should understand that anyone can commit an act of violence, and that more than likely an individual will not advertise his or her plot. But, in the case of terrorism, it may be not a specific event but a specific ideology that is driving the individual. Probably the most important finding of this chapter is that, when public safety agencies screen applicants, they will not detect a determined infiltrator. Understanding this finding, and shifting focus to recognizing an infiltrator once he or she is within the agency should become the priority. This is not very different from recognizing the employee who is in the process of radicalizing, but now the organization is dealing with a person who has already ascended the “staircase to terrorism,” making him or her a greater threat than the radicalizing responder.

Public safety agencies should put greater emphasis on developing and applying stronger methods to block infiltrators from gaining employment. The first step should be increased awareness throughout police and fire departments that radicalized infiltrators may be attempting to gain access to their departments. Following this understanding, agencies should carry out a strong information campaign to dissuade malicious actors from desiring to infiltrate a public safety agency, in an attempt to dissuade those would-be infiltrators from attempting to gain access. If infiltrators think they will be scrutinized more

¹⁴⁷ Corri Zoli, “Lone-Wolf or Low-Tech Terrorism? Emergent Patterns of Global Terrorism in Recent French and European Attacks,” *Lawfare*, August 17, 2016, <https://www.lawfareblog.com/lone-wolf-or-low-tech-terrorism-emergent-patterns-global-terrorism-recent-french-and-european>.

than they would be today, they may second guess their intentions to infiltrate a public safety department, or would at least have to work harder to elude detection.

Police and fire departments should also begin teaching their employees what a potential infiltrator may look like. From outward appearance, the infiltrator is most likely to attempt to blend in as best as possible, to avoid unnecessary scrutiny or questioning. This blending in may belie them, as they may appear to be the “perfect employee.” This is not to suggest that anyone who excels in his or her career field should be labeled as a malicious infiltrator. However, if the model employee were scrutinized, he or she would not feel threatened; on the other hand, the infiltrator may feel the pressure of his or her cover unraveling. But, unlike the outward behavioral signs discussed in Chapter III with the radicalizing employee, this employee may hide his or her true motives more effectively. This is not a fledgling terrorist, but an individual who should be seen as a calculated professional and who has eluded detection up until this point.

If an infiltrator has successfully gained employment and access within a public safety agency, how should fellow responders and the department respond? If an infiltrator is suspected, fellow responders should feel empowered and mandated to report their suspicions up the chain of command and to intelligence personnel for evaluation. Similar to the “my brother’s keeper” approach discussed in Chapter III, by reporting the suspicious behavior for evaluation, the infiltrator would be investigated for his or her potential level of threat, and resolved appropriately. If it turns out the person was just acting strangely, this could be ascertained and the investigation would not have to go any further.

As mentioned, however, up to this point there are no cases of terrorist or extremist groups infiltrating a member into a public safety agency and successfully carrying out an attack. Currently, the more significant threat, based on history, is from those individuals already within the organization who radicalize and conduct an attack, such as Nidal Hasan and Syed Farook.

E. CONCLUSION

A nefarious individual or organization may attempt to infiltrate a public safety agency to increase access to facilitate a plot either against the public safety agency itself, or the public. Under current first responder pre-employment screenings, if the applicant does not have a criminal history upon application, it is unlikely that he or she will be caught and excluded from the potential applicant pool.

It should be a high-priority goal to intercept and prevent an infiltrator from gaining access and employment into a police or fire department. Because a potential infiltrator is unlikely to voice affiliation with an extremist or terrorist group, and also unlikely to display overt signs of such affiliation, it may be difficult to capture these individuals during the initial employment screening process.

This chapter discussed how a motivated individual may attempt to infiltrate a local or state public safety agency to gain trusted access and carry out an attack. It does not matter if the individual is acting on behalf of a terrorist organization or as a lone wolf, as the individual must have a “clean-skin” background, and must gain employment to carry out his or her plot. Threat assessments were discussed as a method to prevent a terrorist infiltrator from gaining access into a public safety agency, but were seen as a more effective method for preventing an attack by someone radicalizing, and not a professional infiltrator.

The pre-employment focus should be on presenting an environment that is serious about preventing a malicious infiltrator or anyone seeking to use his or her position to carry out a bad act. Educating the employees who screen applicants for these positions, as well as current employees, on the signs of radicalization also creates the type of defensible environment necessary to deter bad actors from trying to get in. Understanding that this is a very real threat, and one that can be combatted, should be a priority for public safety leadership in the recruitment of new employees and in the education of current employees. In the following chapter, the current methods of pre-employment screening are discussed, including recognizing where they may miss an infiltrator attempting to gain access. The chapter also presents a method that may increase the chances of identifying a malicious infiltrator.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PROCEDURES FOR SCREENING IN PUBLIC SAFETY OFFICERS AND THEIR INEFFECTIVENESS AT SCREENING OUT RADICALS

Personnel who are charged with screening and adjudicating prospective employees need to be aware that there may be people seeking to gain a position in public safety simply to exploit it. It is often assumed that pre-employment psychological tests will identify all nefarious traits, but this is not the case.

Current pre-employment screening procedures were never intended to evaluate applicants for the threat of terrorism, which is ideologically driven; they screen for potential criminality, which is psychologically driven. Further, because having a terrorist ideology is not a mental health disorder, tests designed to screen for mental health problems are unlikely to catch terrorist ideologies. Therefore, it is important for local and state public safety agencies to recognize this deficiency and establish plans to eliminate potential malicious radicals from infiltrating their departments.

This chapter discusses the different pre-employment screening tests, including psychological, used for evaluating potential applicants for local and state public safety agencies, and why they fail to identify a radicalized individual. The chapter concludes by suggesting several screening procedures that offer greater promise in identifying and screening out potential infiltrators.

A. PRE-EMPLOYMENT PSYCHOLOGICAL SCREENING

One of the hiring requirements for 90 percent of public safety agencies is the ability to pass a psychological exam.¹⁴⁸ Police officers and firefighters are exposed to high levels of psychological stress and operate in high-threat environments that require split-second, level-headed decision making. These psychological exams primarily look for traits that indicate a higher likelihood that the individual will have a successful public safety career—

¹⁴⁸ Robert E. Cochrane, Robert P. Tett, and Leon Vandecreek, "Psychological Testing and the Selection of Police Officers: A National Survey," *Criminal Justice and Behavior* 30, no. 5 (October 1, 2003): 511, <http://doi.org/10.1177/0093854803257241>.

such as impulse control, honesty, courage, integrity, and ability to tolerate stress—while also screening for anti-social traits like psychopathology.¹⁴⁹ According to Weiss and Weiss, psychopathology and other personality problems are usually detected early in the hiring process through interviews and interactions with the applicant; if initially detected, psychological tests would eliminate candidates possessing those traits.¹⁵⁰

However, as Clark McCauley believes, “terrorism is not to be understood as pathology”; he argues that, “terrorists emerge out of a normal psychology of emotional commitment to cause and comrades.”¹⁵¹ Rarely are diagnosable psychological disorders found when interviewing terrorists.¹⁵² This means that even if a terrorist were psychologically screened, his or her ideology would likely go undetected, and the individual would be free to gain employment.

One problem with relying on psychological pre-screening to screen out radicals is that the tests were not developed for this specific task. According to Weiss and Weiss, most tests were developed for assessing a patient’s psychological status as a tool for diagnosing mental illness, and not as an assessment tool for predicting ability and success in a career.¹⁵³ Such tests should not be used or attempted to be adapted for screening of potential first responders in eliminating potential radicals or terrorists.

Some exams have been purposefully revamped to account for the unique needs of emergency responders. One example is the Minnesota Multiphasic Personality Inventory-2 (MMPI-2), which was designed primarily for law enforcement but is also used for prospective firefighters.¹⁵⁴ The MMPI-2 is a 567-item true-or-false test that measures an

¹⁴⁹ Timothy Roufa, “Should Police Have Psychological Tests?,” *The Balance*, accessed October 23, 2016, <https://www.thebalance.com/psychological-exams-and-screening-for-police-officers-974785>.

¹⁵⁰ Weiss and Weiss, “Police Psychological Evaluations,” 128; Peter A. Weiss et al., “Exploring the MMPI-2 L Scale Cutoff in Police Selection,” Matrix Incorporated, accessed September 17, 2016, <http://www.matrixinc.cc/publications/Exploring%20the%20MMPI-2%20L%20Scale%20Cutoff%20In%20Police%20Selection.pdf>.

¹⁵¹ McCauley, “Psychological Issues in Understanding Terrorism,” 5.

¹⁵² McCauley, 5; Sinai, “Can Terrorists Be Psychologically Profiled.”

¹⁵³ Weiss and Weiss, “Police Psychological Evaluations,” 125.

¹⁵⁴ According to Weiss and Weiss, these exams require more validity testing to conclusively assess their applicability to test this cohort. This is an area that is being actively studied today.

individual's personality and psychological characteristics to detect psychopathology. This exam was reformatted in 2008 as the MMPI-2-RF, and now asks 338 questions.¹⁵⁵ Both of these versions of the exam are currently in use, but the MMPI-2 is still the most widely used.¹⁵⁶ Specifically, these exams evaluate a candidate's emotional adjustment, impulse control, responsibility, and level of defensiveness, and look for potential substance abuse problems.¹⁵⁷ The goal of the tests is to determine an applicant's potential for success in the law enforcement and firefighting fields, and the probability of problem behaviors within that career; however, it does not address potential indicators of radicalization or terrorist ideology.¹⁵⁸

Another exam that has been used to evaluate the psychological stability of applicants into police and fire departments is the Inwald Personality Inventory (IPI). This 310-question exam was designed in 1979 as "the first comprehensive behaviorally-based personality measure designed and validated specifically for use in high risk occupations, such as law enforcement."¹⁵⁹ Since 1979, the IPI has been updated to the IPI-2, which consists of fewer questions (202), and measures both personality characteristics and behavior patterns. The IPI-2 can differentiate between individuals who "express socially deviant attitudes and those who act on them," based on the characteristics and patterns for which it tests.¹⁶⁰ This test also focuses on predicting the success of public safety officers, while eliminating those who have a higher possibility of psychosis or other mental

¹⁵⁵ "MMPI-2-RF® Overview," University of Minnesota Press, accessed November 28, 2017, <https://www.upress.umn.edu/test-division/MMPI-2-RF>.

¹⁵⁶ Jane Framingham, "Minnesota Multiphasic Personality Inventory (MMPI)," Psych Central, May 17, 2016, <https://psychcentral.com/lib/minnesota-multiphasic-personality-inventory-mmipi/>.

¹⁵⁷ "The Minnesota Multiphasic Personality Inventory-2 (MMPI-2) in Career Development—IResearchNet," Career Research, March 12, 2015, <http://career.iresearchnet.com/career-development/minnesota-multiphasic-personality-inventory-2-mmipi-2/>.

¹⁵⁸ Weiss and Weiss, "Police Psychological Evaluations," 128.

¹⁵⁹ Robin Inwald, "The Inwald Personality Inventory (IPI) and Hilson Research Inventories: Development and Rationale," *Aggression and Violent Behavior* 13, no. 4 (August 2008): 298, <http://doi.org/10.1016/j.avb.2008.04.006>.

¹⁶⁰ "Inwald Personality Inventory-2 (IPI-2) Report," 16pf.com, accessed September 25, 2017, <https://www.16pf.com/product/inwald-personality-inventory-2-ipi-2-report/>.

instability. Like the MMPI, this test also does not address indicators of radicalization or terrorist ideology.

Accurate interpretation of the results is also crucial to properly screening applicants. It is important to note that results need to be assessed by skilled practitioners in “test theory, personality, psychopathology and psychodiagnosis,” and not by laypeople.¹⁶¹ Non-psychotic terrorists may still circumvent these screenings, but these screenings do provide a strong baseline for eliminating threats that this thesis does not study.

It is difficult to positively predict terrorist behavior in applicants for police and fire departments based on psychological screenings. This is why, as stated in Chapter IV, profiling individuals will not predict if they are likely to commit an act of targeted violence. This is especially true if an organization hopes to screen out potential terrorists using these exams.

B. CRIMINAL BACKGROUND CHECKS

Gaining a position within public safety requires a check of an applicant’s criminal background. It does not make sense to hire a convicted felon into a position that must enforce the law in an objective and unbiased fashion. Unfortunately, there have been cases in which agencies do not conduct thorough background checks, and unintentionally hire someone with a criminal history. Kyle Bacon was hired into the Blackhawk, Colorado, Police Department in 2012, despite a conviction for felony trespassing and theft.¹⁶² His hiring was an accident that resulted from inadequate screening of his criminal record.

Colorado now intentionally grants waivers to convicted felons that allow them to apply for positions as law enforcement officers, in an effort to increase career opportunities.¹⁶³ Many of these exemptions are being given to applicants with felony

¹⁶¹ Career Research, “MMPI-2.”

¹⁶² Christopher Osher, “Colorado Grants Waivers to Police Applicants with Criminal Backgrounds,” *Denver Post*, January 22, 2016, <http://www.denverpost.com/2016/01/22/colorado-grants-waivers-to-police-applicants-with-criminal-backgrounds/>.

¹⁶³ Osher.

convictions for assault, drug crimes, domestic violence, and larceny.¹⁶⁴ If agencies are lowering hiring standards in an effort to fill a quota, the potential for a bad actor to slip through the front door is increased. Hiring standards exist to keep both the membership of police and fire departments safe, but also for the safety of the public they serve.

Generally, the background checks involved with the hiring process for police and fire department jobs do not vary much. Some agencies have candidates submit to a polygraph exam, while others do not. Also, the size of the department typically dictates the level of depth that the background investigation entails, based on resources and funding to carry out these checks. Most police and fire departments do their own background investigations, but there are some agencies that contract this to an outside service due to the extensive time required to complete the investigation effectively.¹⁶⁵ Contracting this service out also opens another opportunity to subvert the background screening process; for instance, the contractor may seek to infiltrate an operative into an organization.

Most departments, regardless of their size and location, require applicants to submit a set of fingerprints, a driving record, address history list, and a list of references including neighbors, former neighbors, and former coworkers.¹⁶⁶ This is an effort to begin developing a background on who the candidate is, and to discover any inconsistencies in his or her application.

There are four main checks that an applicant is subjected to during their evaluation and verification process. Most agencies conduct a check of an applicant's criminal history, subject applicants to a polygraph exam, and verify their references and financial records. A fifth check, now being pressed, is the verification of an applicant's documentation against forgery, which potentially offers the greatest chance of identifying a malicious

¹⁶⁴ Osher.

¹⁶⁵ Thomas Noonan and Edmund Archuleta, "The Insider Threat to Critical Infrastructures" (Report, National Infrastructure Advisory Council, 2008), 26, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

¹⁶⁶ "Demystifying the Background Investigation Process: What You Can Expect When Applying for a Law Enforcement Job," *In Public Safety*, February 4, 2014, <http://inpublicsafety.com/2014/02/demystifying-the-background-investigation-process-what-you-can-expect-when-applying-for-a-law-enforcement-job/>.

infiltrator. If those screening applicants recognize that a person is attempting to gain employment to a public safety agency using fake documents, it should be seen as a sign of bad intent.

1. Criminal History Check

The criminal history check is used to paint a picture of the applicant's past and find out if there are any bad associates, determine residency, and to conduct a criminal background check through the Interstate Identification Index (III). This system aims to "assure positive identification of offenders and helps to avoid false-positive record association and false negative 'no record' responses, which is possible with name-only checks of less comprehensive criminal history databases."¹⁶⁷ The fingerprints verify the specific identity of the applicant, who may have the same name as someone else with a criminal history.

One problem with background checks, as cited by the TSA, is that they can miss some candidates who have served time in prison prior to applying. According to a report from the House Homeland Security Committee, "one airport security official noted that an individual's mandatory ten-year criminal background check could conceivably come back clean, if the person had been serving a prison sentence during that entire ten-year period."¹⁶⁸

This shows that there is a gap in criminal background checks that can be exploited in keeping criminals and terrorists out of public safety agencies. Because of established information-sharing avenues between agencies, this should not be an issue if the person was incarcerated in the same state in which he or she is currently seeking a job. However, it may be a concern when an individual serves a prison sentence in another state and then applies for a position in a jurisdiction where those information-sharing networks have not caught up.

¹⁶⁷ Noonan and E. Archuleta, "The Insider Threat," 26.

¹⁶⁸ Homeland Security Committee, *America's Airports*, 5.

An additional problem is that most local and state public safety agencies only go back seven years in a person's background, in accordance with the Fair Credit Reporting Act.¹⁶⁹ If an applicant had a criminal background more than seven years prior, aside from a major felony conviction, this information would not be used in the screening process. This gap is also concerning because it provides a criminal or terrorist an additional deficiency to exploit when attempting to gain employment into a police or fire department.

2. Polygraph Exams

Polygraph exams, or "lie detectors tests," are also used as a screening tool for many law enforcement and government positions. While it is estimated that approximately 62 percent of law enforcement agencies use polygraph exams in the hiring process, it is less common for firefighters, potentially making fire departments a softer target.¹⁷⁰ Polygraph exams are used to identify deception through the use of carefully chosen questions that assess physiologic changes such as increased respiratory rate, blood pressure increase, or galvanic sweat responses.¹⁷¹ Candidates are asked a set of questions, usually related to involvement in criminal activities such as drugs or violence; if they are lying, the candidate's body will react physiologically.¹⁷² If the individual being tested elicits responses to critical questions, he or she is generally given a follow-up interview to discuss the reason for displaying signs of deceit and, at the agency's discretion, that person may be tested again with more focused questions.

Although questions have been raised about their effectiveness and accuracy, many law enforcement agencies in the United States still rely heavily on polygraph exams.¹⁷³ In

¹⁶⁹ "Background Screening Made Simple," Verified Person, accessed December 17, 2017, <http://www.verifiedperson.com/FCRAbystate.html>.

¹⁷⁰ "Polygraph Frequently Asked Questions," American Polygraph Association, accessed October 13, 2017, <http://www.polygraph.org/polygraph-frequently-asked-questions>; Mark Handler et al., "Integration of Pre-employment Polygraph Screening into the Police Selection Process," *Journal of Police and Criminal Psychology* 24, no. 2 (October 1, 2009): 70, <https://doi.org/10.1007/s11896-009-9050-2>.

¹⁷¹ Handler et al., "Pre-employment Polygraph Screening," 73–74.

¹⁷² Handler et al., 73–74.

¹⁷³ National Research Council, "The Polygraph and Lie Detection. Committee to Review the Scientific Evidence on the Polygraph. Division of Behavioral and Social Sciences and Education," *The National Academic Press*, no. 7 (2003): 9.

fact, Gaschler et al. believe that these exams have higher rates of accuracy in determining a person's likelihood to be dishonest and lacking characteristics needed to be successful in public safety positions when compared to personality inventories like the MMPI-2.¹⁷⁴ This is attributed to the body being physiologically less able to hide deceit, whereas a person can simply provide dishonest answers in a personality inventory.

A similar finding was discovered with the use of the IPI-2. A study conducted in 1986 of thirty-nine criminal justice and security management students at a large Midwestern University discovered that people are more likely to be dishonest in a written personality exam than they are in a polygraph exam.¹⁷⁵ The students were administered the IPI-2, and were later given a two-hour polygraph exam focusing on the same questions as the written exam. This study showed more admissions of criminal activity in the polygraph than in the pencil-and-paper exam.¹⁷⁶ According to Timm and Hedges, "it does not appear paper and pencil integrity tests such as the IPI can effectively take the place of background investigations, polygraph testing, and other integrity screening procedures."¹⁷⁷ Instead, these tests should all be utilized to effectively screen in candidates for public safety positions in police and fire departments.

Presently, according to Handler et al., "the polygraph remains the most mature and developed form of scientific credibility or honesty testing available for use in field settings."¹⁷⁸ The consensus in the field is that polygraphy should be used to augment personality inventories, and not as a substitute to the inventories. Handler et al. suggest that "using polygraph results alone to disqualify a candidate from employment is a misguided field practice."¹⁷⁹ Timm and Hedges further suggest using these tests as adjuncts also.¹⁸⁰

¹⁷⁴ William J. Gaschler et al., "Review of Polygraph Screening Assessment Method," *Polygraph* 30, no. 4 (2001): 257.

¹⁷⁵ H. W. Timm and W. K. Hedges, "Factors Theoretically Affecting the Incidence of Deceptive Responses During Preemployment Screening Procedures," *Polygraph* 22, no. 3 (1993): 229–244.

¹⁷⁶ Timm and Hedges, 239–40.

¹⁷⁷ Timm and Hedges, 242.

¹⁷⁸ Handler et al., "Pre-employment Polygraph Screening," 84.

¹⁷⁹ Handler et al., 69.

¹⁸⁰ Timm and Hedges, "Deceptive Responses," 242.

3. Verification of a Candidate's Background

Another part of this process is the verification of references, former employment, and residences. Investigators usually call those listed on the candidate's application and verify that they are who the candidate says they are, and verify that the reference knows the candidate and the information given is accurate.¹⁸¹ If the investigator does not physically meet with these references and investigate the applicant thoroughly, it can leave room for unchecked dishonesty.

Records requests verify information the candidate provides, but these are subject to what the candidate chooses to provide, and therefore may not give a complete picture of the candidate. It is possible for someone who does have a criminal past to put down persons and contact information to verify a false identity. Catrantzos notes this gap within background checks for critical infrastructure agencies, saying, "Accommodation addresses and [a] false front 'former employer' may be accepted as references over the phone, when a field visit would reveal the 'business' is a residential mail drop."¹⁸² Physically investigating and visiting a candidate's references is necessary to eliminate the gap in telephone-only investigations.

4. Financial Records Check

Many agencies also look into financial records to see if an applicant has financial problems that may make the individual vulnerable to bribery or blackmail.¹⁸³ These searches, governed by the Fair Credit Reporting Act, evaluate employment history and confirm where sources of income originate.¹⁸⁴ Hershkowitz also recommends checking for "loans from an unofficial or illegal money source," further looking for illicit transactions and bad associations.¹⁸⁵ Though it is unlikely that a local loan shark would be

¹⁸¹ *In Public Safety*, "Demystifying the Background Investigation Process."

¹⁸² Catrantzos, "No Dark Corners."

¹⁸³ Pattie Hunt Sinacole, "Financial Background Checks on Candidates," *Boston Globe*, January 16, 2012, https://www.boston.com/jobs/job-doc/2012/01/16/financial_background_checks_on.

¹⁸⁴ Noonan and Archuleta, "The Insider Threat," 27.

¹⁸⁵ Martin Hershkowitz, "The 'Insider' Threat: How to Minimize it," *Journal of Police Crisis Negotiations* 7, no. 1 (January 2007): 110.

openly reporting loans, a recipient of these funds would have disparities in his or her financial records that would be otherwise inexplicable. This check is another layer in verifying a person's identity, which also reduces the potential for false addresses and contacts.

5. Documentation Verification

Application documents themselves may also present an opportunity to catch potential infiltrators. Some cases of attempted infiltration to the U.S. military have included falsified documents such as identification cards and birth certificates.¹⁸⁶ In 2007, Daniel Torres illegally enlisted into the U.S. Marine Corps after providing his recruiter with a fake birth certificate, allowing him to remain a Marine for three years.¹⁸⁷ In this case, Torres just wanted to serve in the U.S. military out of a love for his adopted country. However, had he had more nefarious intentions, he had been granted the access to carry out a malicious plan.

A well-coordinated plot could encompass the resources to falsify major documents in an effort to provide proper cover for an operative who is trying to infiltrate an organization. As a result, the DoD has increased investigations into document fraud and has recommended adopting e-signatures for documents, consistent with many other federal agencies.¹⁸⁸ BaMaung et al. believe that civilian public safety agencies are likely to experience similar problems and should also be on the lookout for falsified documents.¹⁸⁹ They recommend adopting stronger identification verification methods to prevent false applications resulting in illicit employment.¹⁹⁰ Training should be adopted and

¹⁸⁶ Kelly R. Buck et al., *Screening for Potential Terrorists in the Enlisted Military Accessions Process* (Monterey, CA: Defense Personnel Security Research Center, 2005), xviii.

¹⁸⁷ Griselda Navarez, "Immigrant Who Lied to Join Marines Is Naturalized: 'Now the Law's on My Side,'" *Guardian*, April 23, 2016, <https://www.theguardian.com/us-news/2016/apr/23/daniel-torres-marine-fake-birth-certificate-citizen>.

¹⁸⁸ Navarez.

¹⁸⁹ David BaMaung et al., "The Enemy Within? The Connection between Insider Threat and Terrorism," *Studies in Conflict & Terrorism*, October 25, 2016, 9, doi:10.1080/1057610X.2016.1249776

¹⁹⁰ BaMaung et al., "The Enemy Within," 9.

incorporated for those involved in document handling and reading to prevent infiltration caused by document falsification.

C. ANALYSIS

Currently, the methods most state and local public safety agencies use to screen candidates for employment do not necessarily identify a malicious infiltrator motivated by a terrorist ideology. This threat is not discussed enough in current literature and within professional circles in public safety, which means it is not a priority for prevention. Many public safety leaders believe that psychological exams will capture these individuals, but they do not realize that terrorist ideologies and motivations are not psychologically driven. Psychological screening should not be eliminated, as these tests are still needed to do what they successfully accomplish—to eliminate psychologically unstable individuals from the hiring pool. However, additional reliance on other screening procedures should be embraced to screen out potential terrorists.

Polygraph exams, which are not always used, are very difficult to defeat, making them an accurate and useful screening tool. If more agencies included this test in their pre-employment screening process, and asked specific, pointed questions, the “clean-skin” infiltrator may not be able to lie his or her way into a police or fire department. Those departments seeking to hire candidates should take their assessments seriously, and ensure the appropriate level of scrutiny and verification is administered in vetting candidates.

When properly administered, with specific questions relating to whether or not a person is a member of a terrorist group or identifies with a dangerous and offensive ideology, a polygraph exam is more likely to identify that individual compared to the personality inventory assessments commonly used today. A candidate should not simply be asked, “Do you belong to a terrorist group, or espouse a radical belief system?,” as the candidate may honestly not believe he or she does. Instead, a more focused question should be asked; for instance, if trying to weed out a white supremacist, the examiner can ask: “Do

you feel that you are superior to another race?” The questions should be focused enough to reduce ambiguity, and leave little room for misinterpretation.¹⁹¹

Nefarious actors and intelligent adversaries, with proper planning, do have the ability to exploit vulnerabilities within the hiring process to present an identity that would prevent them from being hired into a police or fire department. False contacts and false addresses can be used to create a clean-skin individual and build up a personal history to bolster the candidate’s appearance. If the candidate does not have a criminal past, his or her fingerprints will not reveal a criminal background, masking any intention to carry out a violent act. If he or she does not have a blemished financial history, his or her record will not be flagged. These vulnerabilities are simple enough to prevent an infiltrator from gaining access to a public safety department, but only if departments recognize these gaps and take measures to close them.

However, one area presents the greatest opportunity for interdiction of an infiltrator: document verification. If an infiltrator attempts to use fraudulent paperwork to build a clean skin, organizations can recognize this method and prevent the infiltrator from making it through the hiring process. By recognizing an applicant who is attempting to use falsified documents, the screening agency can alert appropriate law enforcement or intelligence personnel to further investigate the individual, potentially unveiling a larger plot. The simplicity of confirming documentation authenticity can yield great results, such as preventing the major impact of allowing a malicious infiltrator into a public safety department.

D. CONCLUSION

Many psychological exams were not designed for public safety officer screenings; but the few that were designed for this purpose were not designed to evaluate for radicalized individuals. Psychological screenings can filter out candidates who suffer from some form of psychopathology, but may miss the ideologically driven rational actor. However, properly administered polygraph exams, asking the correct questions, could

¹⁹¹ Handler et al., “Pre-employment Polygraph Screening,” 80–81.

better indicate that an individual with cruel intentions is attempting to infiltrate a police or fire department.

The focus should come back to investigating the individual more thoroughly through the use of polygraphy and physical, in-person verification of references. As noted, a deficiency in performing many of these verification checks is their reliance on virtual and telephonic validation. If an intelligent adversary gives false addresses or false contacts to verify his or her identity, an infiltrator may be able to gain entry into an agency with little resistance or scrutiny from the hiring department. Investigators should physically inspect addresses given by applicants, and include questions that may not be expected or rehearsed with a person providing a character background reference.

No single testing procedure can provide all the answers. But when procedures are used concurrently, agencies screening individuals for employment in public safety agencies will get a more complete and honest picture of applicants. Education of staff is the greatest overall method to protect a public safety agency against an infiltrator.

This chapter covered the current pre-employment screening procedures employed by local and state public safety agencies for new applicants. The next chapter discusses the procedures being used by federal agencies and the U.S. military to screen their applicants, and how these procedures may be adapted for use by local and state public safety agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. HOW THE U.S. MILITARY AND FEDERAL GOVERNMENT SCREEN FOR AND PREVENT TARGETED VIOLENCE

As stated in previous chapters, both the U.S. military and federal agencies have dealt with malicious insiders committing targeted violence and murder on behalf of a terrorist ideology. Because of these experiences, there are lessons that state and local public safety agencies can learn from the U.S. military and federal government to deter and prevent an attack from a malicious insider and, specifically, to prevent someone who identifies with a terrorist ideology from being hired.

Currently, what separates the federal government and U.S. military from local and state agencies is the depth of analysis of background checks and screenings for federal positions. This is in part because, unlike local and state agencies, federal agencies and the military have direct access to systems and analysts to adjudicate employment applications, along with stricter policies to govern those systems and analysts. This difference is specifically seen in how security clearances are investigated and granted, with fewer local and state responders requiring this level of scrutiny. However, would this level of scrutiny be appropriate to help local and state responders prevent an attack from within, or is it too great an investment in time and resources to prevent a threat that has not yet materialized in the United States? This thesis believes that attributes of the DoD and federal government show promise for preventing an attack if implemented appropriately, which can save valuable time and resources; implementing existing methods would prevent state and local public safety agencies from having to develop a new strategy to protect against this threat.

This chapter covers current processes used by the federal government and U.S. military to screen candidates for employment and briefly discusses their effectiveness and limitations at thwarting a potential infiltrator. Then these methods are compared to the current state and local public safety procedures to discern which tenets the state and local agencies can adopt for a more stringent employee vetting process. This chapter also discusses methods developed by the U.S. military for preventing radicalization in current employees, and how to prevent violent plots from being conducted. Finally, the chapter examines how these methods can be tailored to police and fire departments to prevent

radicalization, and finds that incorporating some of these programs would decrease the ability of a radicalized employee to carry out an attack.

A. FEDERAL LAW ENFORCEMENT POSITION PRE-SCREENING

In comparison to other industries or agencies, the federal government conducts more extensive and focused vetting of potential employees for federal law enforcement and security positions. The federal process is similar to the procedures of local and state agencies, incorporating criminal background checks through fingerprint analysis, financial records checks, and drug testing, but the federal model also more comprehensively assesses an applicant's personal history.¹⁹² For example, the FBI requires all applicants to be able to hold an FBI Top Secret security clearance, for which the background check "reviews an applicant's actions, relationships, and experiences beginning with the present and working back 10 years or to their 18th birthday."¹⁹³ If an applicant were associated with a criminal or terrorist group, it would likely be found at this point, provided there is a criminal record of the affiliation. By contrast, local background checks may not go back as far as ten years into the applicant's history. Also, as discussed in previous chapters, it is unlikely that an infiltrator would attempt to infiltrate an agency if he or she had a criminal record. These checks are therefore good for screening criminality, but not for detecting criminal or terroristic intent.

This section reviews several screening methods used by the federal government, beginning with polygraph exams. Regardless of an applicant's history, one main component that differentiates federal screenings from state and local agency screenings is the use of polygraph exams for all candidates, along with an evaluation of the candidate's social media usage. Both methods help to establish a more complete profile of the candidate when assessing fitness for a career position.

¹⁹² "Special Agents," FBI Jobs, accessed September 26, 2017, <https://www.fbijobs.gov/career-paths/special-agents>.

¹⁹³ FBI Jobs.

1. Polygraph Exams

In addition to verifying an applicant's history and vetting for security clearance positions, polygraph exams can be given for a variety of reasons. Polygraph exams are broken into two categories: counterintelligence exams and lifestyle exams.¹⁹⁴ The counterintelligence exams focus on uncovering espionage and terrorism, whereas the lifestyle exam is concerned with criminal activities and falsification of forms.¹⁹⁵ The issue is, as stated in Chapter V, that local and state public safety agencies do not always polygraph applicants; if they do, the counterintelligence exam is not given, which affords a terrorist the opportunity to slip through the ranks while being completely candid and honest.

That said, the practice of initially screening individuals through polygraphy does not capture or predict those applicants who decide later to deceive their organization. The FBI learned this lesson firsthand from senior counterintelligence investigator Robert Hanssen, who was never subjected to a polygraph exam beyond his initial employment screening.¹⁹⁶ In February 2001, Hanssen was arrested and charged with committing espionage by providing highly classified national security information to Russia and the former Soviet Union.¹⁹⁷ Ultimately, Hanssen had compromised over 6,000 pages of sensitive material during his period of espionage.¹⁹⁸ As a result of the Hanssen case, the FBI has instituted regular follow-up polygraph exams of employees every five years.

¹⁹⁴ William Henderson, "How to Prepare for a Security Clearance Polygraph Examination," Clearance Jobs, June 6, 2011, <https://news.clearancejobs.com/2011/06/06/how-to-prepare-for-a-security-clearance-polygraph-examination/>.

¹⁹⁵ Henderson.

¹⁹⁶ Gaschler et al., "Polygraph Screening Assessment Method," 256.

¹⁹⁷ "Robert Hanssen," FBI, accessed January 1, 2017, <https://www.fbi.gov/history/famous-cases/robert-hanssen>.

¹⁹⁸ FBI.

2. Social Media

Federal agencies also review an applicant's social media accounts and postings. Today, it is uncommon for a person in North America to not have a social media account. In fact, as of January 2017, it is estimated that 81 percent of Americans have at least one social media account.¹⁹⁹ What people post on their profiles helps investigators develop a clearer picture of the applicant and any affiliations the applicant did not disclose when interviewed. For example, if a person posts violent rhetoric in support of a group or ideology that is contrary to the organization's mission, the hiring agency could find this and disqualify the applicant from service.

Cole et al. remark that "extensive engagement with media that promotes and justifies the use of violence will often influence an individual's decision to engage in violent extremism as the solution to real and perceived grievances."²⁰⁰ If a person has posted content that supports violent action, this may be an indicator of a plot that is moving toward violence.

Cole et al. further state that "active association with individuals and groups who are known to have links to violent extremists indicates that an individual is at risk of being targeted for recruitment When coupled with other types of behaviour, it could indicate that an individual is becoming potentially vulnerable to recruitment."²⁰¹ This was evidenced in Chapter III by Nicholas Young's affiliation with Zachary Chesser and Amine El Khalifi. If a person associates with others who are thought to be "bad actors," there is a higher possibility that the individual may also be a bad actor, which should demand further scrutiny. Though it is labor-intensive to do so, organizations may also consider looking into the backgrounds of the candidate's friends and associates. Recognizing these bad associations may be another method of preventing a bad actor from entering an agency.

¹⁹⁹ "U.S. Population with a Social Media Profile 2017," Statista, accessed September 26, 2017, <https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/>; Shannon Greenwood, Andrew Perrin, and Maeve Duggan, "Social Media Update 2016," Pew Research Center, November 11, 2016, <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>.

²⁰⁰ Cole et al., "Free Radicals," 4.

²⁰¹ Cole et al., 4.

On the other hand, a person who is seen as a loner and has no visible associations may also elicit the attention of a background screener. Social isolation has been cited as a precursor to a person radicalizing, or as a sign that someone is on the verge of committing a terrorist act.²⁰² Isolation was seen in all four cases discussed in this thesis: Hasan, Farook, Altintas, and arguably Young. Kamaldeep Bhui supports this correlation, indicating that social isolationism does increase the likelihood that an individual in the wrong circumstances will radicalize.²⁰³

However, a negative finding (no network affiliation) is not a guarantee that the individual has radicalized, or will radicalize. In fact, the applicant may see the public safety agency as his or her desired network. Nevertheless, isolation is something worth noting during the screening process. Isolation, however, does not just mean the person does not have a social media account; some people choose to not have these types of accounts for various reasons, and a lack of social media does not mean the individual is radicalizing. Additionally, it may be difficult to tell if a person is actually isolating him or herself from others or is simply not overt when demonstrating sociality.

The procedures used by the federal government to verify potential employees for positions within federal law enforcement agencies generally mirror those used by state and local public safety agencies, with a few exceptions. The criminal background checks are more invasive and go back further in an applicant's history to gain a better understanding of who the applicant is, and any potential criminal or terrorist group associations. Additionally, polygraph exams are seen as effective measures of an applicant's honesty and history. One final screening that is different from the state and local model is the incorporation of analysis and evaluation of an applicant's social media. The U.S. military uses many similar methods to screen applicants for service, as well as different methods resulting from prior incidents within the armed forces.

²⁰² Joe Navarro, "Unmasking Terrorists—Two Critical Characteristics!," *Psychology Today*, December 31, 2009, <http://www.psychologytoday.com/blog/spycatcher/200912/unmasking-terrorists-two-critical-characteristics>.

²⁰³ Kamaldeep Bhui, "Radicalisation: A Mental Health Issue, Not a Religious One," *New Scientist*, April 8, 2015, <https://www.newscientist.com/article/mg22630160-200-radicalisation-a-mental-health-issue-not-a-religious-one/>.

B. MILITARY PRE-SCREENING

The screening process for those joining the military mirrors many of the same processes used for local, state, and federal positions. An applicant still needs to submit to a criminal background check; the applicant's fingerprints are run through the FBI's Integrated Automated Fingerprint Identification System and National Crime Information Center. Applicants also have to give a list of references, previous addresses, and names of past employers; depending on the job applied for, applicants may additionally need to submit to further background screening for security clearances. This section also discusses tattoo screenings and questionnaires used by the U.S. military to vet applicants for service.

The U.S. military has also experienced attacks from malicious insiders. Buck et al. clarify that the presence of extremists and terrorists in the military "is significant in its own right; the actual numbers are extremely small relative to the denominator representing the millions of personnel who have been enlisted in the Armed Forces."²⁰⁴

Nevertheless, as a result of past attacks, the military has instituted more thorough screening procedures for applicants and has bolstered its programs that watch for radicalization of current service members. The U.S. military has adopted a model of "prevention over prediction" to protect its forces.²⁰⁵ According to the DSB, "the simplest bottom line is that the predictive approach to human behavior is not useful for low probability/high consequence events, but the preventive approach is likely to be promising."²⁰⁶

In the 1980s, the U.S. military faced a surge in extremist and gang activities within its ranks, prompting more stringent screening procedures.²⁰⁷ Flacks and Wiskoff say this problem was seen in "the formation of extremist subcultures or 'cells' within military installations; and activities of lone, unaffiliated extremists living or working in military

²⁰⁴Buck et al., *Screening for Potential Terrorists*.

²⁰⁵ Defense Science Board, *Predicting Violent Behavior*.

²⁰⁶ Defense Science Board, 47.

²⁰⁷ Flacks and Wiskoff, *Gangs, Extremist Groups, and the Military*.

installations and communities.”²⁰⁸ As a result, the military needed to establish a program to prevent these individuals from joining its ranks. Many of the procedures adopted are still in use today as primary screening tools to keep extremists and terrorists out of the military; however, these procedures are also not foolproof. Fingerprint screenings, tattoo evaluation, and questionnaires are all unique procedures used by the military, but none are immune to subversion.

1. Fingerprints

One example of a screening process that can be subverted is fingerprint screenings; when a fingerprint screening shows that the applicant has a criminal background, this finding does not always make it back to the military. Buck et al. state that “when the DoD submits fingerprints for checks of the FBI’s criminal record files, a check of the FBI’s Violent Gangs and Terrorist Organization File (VGTOF) is also conducted . . . Hits on this file are not returned to the recruiting commands, however, but rather go to the submitting agency of the record found, such as a local police department.”²⁰⁹ It then becomes the responsibility of the initial reporting agency to notify the DoD if a person in its system is attempting to enlist in the U.S. military.²¹⁰ Although this does not appear to be a widespread issue, it is one the DoD is looking to resolve.

2. Tattoos

Another example of a unique screening process used by the military is the identification and evaluation of applicant tattoos. If an entrant into military service does not have a criminal record but held membership in a gang or extremist movement, that individual would pass the screening process. However, the military accession process uncovered that tattoos are a marker of affiliation with extremist groups such as gangs and white supremacist groups, both internationally and domestically. The Centre for European and North Atlantic Affairs states, “There are several cases when supporters of extremist

²⁰⁸ Flacks and Wiskoff, vi.

²⁰⁹ Buck et al., *Screening for Potential Terrorists*, xvii.

²¹⁰ Buck et al., xvii.

groups were detected in the army based on the neo-Nazi symbols (e.g., the case of the soldier with Blood & Honor tattoo, receiving a decoration from President of Slovak Republic in 2009; or members of Armed Forces of the Czech Republic with symbols of Nazi Germany on their uniforms).”²¹¹ An example from the U.S. military is Wade Michael Page, who was responsible for the August 5, 2012, Sikh temple shooting in Oak Creek, Wisconsin. Page had been indoctrinated into the white supremacist movement during his military service at Fort Bragg, North Carolina.²¹² Screening for these types of markers has been seen as one of the most effective methods for identifying individuals who fit in with these groups, prompting Buck et al. to recommend the development of a tattoo database within the military.²¹³

At this time, the screening procedure simply involves medical personnel noting the presence of a tattoo and describing it on a medical form (DD-2808).²¹⁴ The personnel can search through databases and files to determine if the tattoo signifies affiliation with an offensive group and requires further investigation. One problem, however, is that not all of the services are connected, and there is not a clear connection between law enforcement and recruiting commands.²¹⁵ This is why it has been recommended that the U.S. military develop a centralized database that all branches of service—as well as law enforcement agencies—can contribute to and use to conduct research.

The development of this database could also benefit state and local public safety agencies when they are vetting candidates. If an applicant had previously served in the military, he or she may have joined a group counter to the U.S. government since separating, gotten a tattoo, and now applied for service as a police officer or firefighter.

²¹¹ “Extremism vs. Armed Forces: Implications for Internal Security and Recommendations for the Future,” Centre for European and North Atlantic Affairs, September 2013, http://cenaa.org/en/wp-content/uploads/2013/09/RT3_final_ENG.pdf.

²¹² Daniel Trotta, “U.S. Army Battling Racists within Its Own Ranks,” Reuters, August 21, 2012, <https://www.reuters.com/article/us-usa-wisconsin-shooting-army/u-s-army-battling-racists-within-its-own-ranks-idUSBRE87K04Y20120821>.

²¹³ Buck et al., *Screening for Potential Terrorists*, xx.

²¹⁴ Buck et al., 35.

²¹⁵ Buck et al., 35.

Prior military service and screening for the military cannot be counted on to have vetted an applicant. Therefore, if such a database is developed, it is imperative for state and local public safety agencies to be given access if they begin screening applicants for problematic tattoos. This database offers comparative samples of offensive tattoos, which public safety can use to further evaluate candidates. For example, Nichols Young had a tattoo of a Nazi SS unit crest on his shoulder, which coworkers noticed during his career; this shows that agencies may need to regularly re-evaluate employees for new or existing tattoos.

However, it is also important to note that not all terrorists or extremists will adorn their bodies with tattoos, so this is not a foolproof method. This is simply one of many different levels on which an individual should be screened; it should not be the primary measure of whether an individual represents an offensive ideology or group.

3. Questionnaires

Another method the military uses to determine eligibility for employment or potential affiliation with extremism or terrorism is the use of a simple questionnaire, something that state and local public safety agencies do not employ in screening. All branches of the military, in the early stages of processing an enlistment, ask applicants questions regarding foreign influence, where the applicant has lived, and if he or she is/was a member of a gang or terrorist group.²¹⁶ These questions seek to determine if an applicant will be honest and knowingly admit an affiliation that may disqualify him or her from enlistment.

Flacks and Wiskoff counter that “[screeners] obviously presume a great deal of honesty on the part of applicants but more importantly, the questions might be interpreted by even the most honest extremist as not being applicable to him or her.”²¹⁷ In relation to white supremacists or militia members, Flacks and Wiskoff say that “many of today’s right-wing extremists see themselves as true patriots whose actions are intended to *restore* the ‘legitimate’ U.S. government, rather than overthrow it, and many others see their

²¹⁶ Buck et al., 40–44.

²¹⁷ Flacks and Wiskoff, *Gangs, Extremist Groups, and the Military*, 39.

actions as simply self-defense against an out-of-control federal government.”²¹⁸ These questions are good because they do elicit a fair amount of willing information from an applicant; but the disadvantage is in the deception that can be intentionally employed, which has to be cleared out later.

As stated in Chapter III, the greater threat lies in the current employee radicalizing, so preventing an infiltrator should not be the only method of defense against terrorists. The following section discusses the methods used by the U.S. military to address this threat.

C. METHODS FOR PREVENTING CURRENT EMPLOYEES FROM RADICALIZING

Having dealt with violent attacks by service members who have radicalized, the U.S. military and federal law enforcement agencies have had to respond to and develop strategies to prevent such attacks. This section highlights some of the main threats that the military and public safety agencies are facing, and later discusses methods to prevent an individual from radicalizing and then moving to violence. The two main methods discussed are prevention and deterrence, and information sharing. The three main models used for prevention and deterrence are Rap Back, used by federal law enforcement; threat management units (TMUs); and a model developed by the Asymmetric Warfare Group to recognize radicalization and prevent an individual’s movement to violence. Information sharing among agencies is later discussed, along with how looping all stakeholders together to share information can be critical to avoiding violence in the future.

1. Range of Threats

The threat from radical Islamic extremists to the United States receives a high level of attention today, but it is important to recognize that the threat from right-wing extremists and other groups within the United States far surpasses the threat from radical Islam. In March 2016, the National Consortium for the Study of Terrorism and Responses to Terrorism discovered that between 1990 and 2014, domestic extremists affiliated with the far-right movement were responsible for four times as many ideology-based killings as

²¹⁸ Flacks and Wiskoff, 39.

al Qaeda and similar movements.²¹⁹ Additionally, David Sterman says that “right-wing extremists are more likely than violent Islamist extremists—or, as they are sometimes called, jihadists—to have military experience. They are also better armed, and are responsible for more incidents.”²²⁰ Kris Axtman echoes this belief, saying that “these groups are likely to pose a greater threat through infiltration of the U.S. military than are Militant Jihadists.”²²¹ Agencies need to be aware of the threat, and must know how to prevent it through appropriate screening and subsequent training.

The U.S. Army also recognizes this threat in potential new recruits. It acknowledges that “the most dangerous potential extremists may not be those who engage in unruly youthful behavior (and thus have arrest records), but those who are well-educated and socially conforming, yet capable of becoming committed to violent extremist ideological goals.”²²² The ability to recognize how people radicalize is a skill that must be further evaluated if public safety agencies wish to exclude potential extremists or terrorists from their ranks. By training employees to recognize common behavioral characteristics related to radicalization, and empowering them to report suspicions appropriately up the chain of command, agencies can prevent an attack before it is operationalized.

2. Prevention and Deterrence Models for Avoiding Employee Radicalization

a. Rap Back

The FBI has developed a program for reporting when people in trusted positions are involved in criminal activities and have interactions with law enforcement. As

²¹⁹ William S. Parkin et al. “Twenty-Five Years of Ideological Homicide Victimization in the United States of America” (report, National Consortium for the Study of Terrorism and Response to Terrorism, 2016), http://start.umd.edu/pubs/START_CSTAB_ECDB_25YearsofIdeologicalHomicideVictimization_US_March2016.pdf.

²²⁰ David Sterman, “The Greater Danger: Military-Trained Right-Wing Extremists,” *The Atlantic*, April 24, 2013, <http://www.theatlantic.com/national/archive/2013/04/the-greater-danger-military-trained-right-wing-extremists/275277/>.

²²¹ Kris Axtman, “The Terror Threat at Home, Often Overlooked; As the Media Focus on International Terror, a Texan Pleads Guilty to Possessing a Weapon of Mass Destruction,” *Christian Science Monitor*, December 29, 2003, sec. USA.

²²² Flacks and Wiskoff, *Gangs, Extremist Groups, and the Military*.

discussed in Chapter II, this program was initially intended to increase reporting of criminal activity for those under law enforcement supervision and reduce the burden on agencies to provide continuous criminal background checks, which are often skipped after the initial screening for employment.²²³ Although initially developed for tracking prior criminals, the program has been adapted to also include public safety officers, if desired by the agency. The program is called Rap Back, and this thesis recommends that more public safety agencies subscribe to it. According to the FBI, “prior to the deployment of Rap Back, the national criminal history background check system provided a one-time snapshot view of an individual’s criminal history status.”²²⁴ Now, Rap Back provides those using the service a rapid and up-to-date picture of the individual being investigated.

The Rap Back system flags an individual within the system if his or her fingerprints are run through the system because of a criminal action.²²⁵ TSA and the Department of Homeland Security have already partnered with the FBI to have this feedback mechanism used for their personnel. According to a report from the House Homeland Security Committee, TSA says that Rap Back “provides 24/7 vetting of credentialed populations, and would give TSA, airport operators, and air carriers significantly better insight into instances of arrest, arraignment, prosecution, and other circumstances which could potentially disqualify an employee from maintaining their secure area access.”²²⁶ It is a form of continuous monitoring, under which an agency that employs an individual will be notified if that individual is later arrested.

Prior to this program, TSA employees were expected to self-report any interactions with law enforcement, a system that relied heavily on the honesty of employees, many of whom were concerned with potentially losing their jobs. Legally, the TSA has to re-assess an employee’s background every two years, allowing for an offense to go unreported and

²²³ “Next Generation Identification (NGI),” FBI, accessed September 6, 2017, <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi> .

²²⁴ FBI.

²²⁵ Babcock, “PIA: NGI Rap Back Service.”

²²⁶ Homeland Security Committee, *America’s Airports*, 14.

potentially undiscovered during that period of time.²²⁷ Rap Back has taken the onus of reporting out of the employee's hands and makes it a continuous feedback loop, thereby drastically decreasing the amount of time needed to notify an agency of employee indiscretions. One deficit of this system, however, is that it is a domestic system only. If a person were to engage in criminal activity overseas, and that incident was not reported back to the United States, it would be like the crime never happened, and no one would be notified.

According to the Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence, if this system had been in place, and if the U.S. Navy were monitoring it, Aaron Alexis, the Washington, DC, Navy Yard shooter, would have been flagged when he was found with an illegal handgun in Texas during his enlistment.²²⁸ This need to share information about criminal interactions with law enforcement is similar to why fusion centers were established; they provide real-time information among stakeholders to prevent potential criminal activity from those employed by participating agencies.²²⁹

b. Threat Management Units

Having dealt with street gangs, white supremacists, and terrorists, the U.S. military has adapted to deal with the threats placed before them. The DSB recommends a style of threat mitigation to address the risks for targeted violence within the U.S. armed forces by developing TMUs. As previously mentioned, the DSB states that "the TMU's mission is to prevent targeted violence by developing calculated responses to troubling behavior."²³⁰ They accomplish this utilizing "a cross-functional, multi-disciplinary team approach to assist in assessing threatening situations and developing threat abatement plans that minimize the potential risk of violence."²³¹

²²⁷ Homeland Security Committee, 14.

²²⁸ H.R., *The Insider Threat to Homeland Security*, 41.

²²⁹ Babcock, "PIA: NCI Rap Back Service."

²³⁰ Defense Science Board, *Predicting Violent Behavior*, 5.

²³¹ Defense Science Board, 5.

This is an effective strategy because it focuses on prevention of violence as opposed to prediction. This model is also a team-based approach that utilizes “professional competence in law enforcement; risk assessment; clinical medical and psychological expertise; and social and behavioral training.”²³² This model does not “guarantee” to eliminate the potential of “targeted violence,” but the DSB found no other method that was as cost effective and that provided a high level of capability.²³³ The TMU concept of having members of different disciplines coordinating responses to potential radicalization or threats of targeted violence allows the team to approach a problem from different angles, leveraging the subject matter expertise of its multi-disciplinary members.

The military has also instilled a culture of watching out for each other. According to DoD Directive 5205.16, once employed, service members are annually briefed on behaviors and actions that may indicate an insider threat of targeted violence and procedures for reporting suspicious behaviors.²³⁴ This training instills a “no one gets left behind” attitude within soldiers, emphasizing that service members should all support each other and be vigilant for changes that could be indicative of potential violent action. It is especially important for organizational leaders to receive this kind of training and be an example for subordinates to set a strong and supportive command tone.²³⁵ The Naval Criminal Investigative Service (NCIS) further describes the mission of a TMU as to “help to identify risk factors, patterns of escalation, and to construct an environment that inhibits or prevents violence.”²³⁶ This is in contrast to the Rap Back program, which captures illegal activity by individuals and alerts the individual’s employer in an effort to prevent a potential criminal act or attack.²³⁷ The intent of the TMU is to prevent an individual from

²³² Defense Science Board, 5.

²³³ Defense Science Board, 5.

²³⁴ DoD, *Insider Threat Program*.

²³⁵ Baker, “Change of Detection,” 70–71.

²³⁶ “Threat Management Unit,” Naval Criminal Investigative Services, accessed September 7, 2017, <http://www.ncis.navy.mil/CoreMissions/CI/Pages/ThreatManagementUnit.aspx>.

²³⁷ Babcock, “PIA: NCI Rap Back Service.”

getting wound into the cycle of radicalizing and preventing him or her from ever seeking to carry out violence against the agency or the public.

The TMU concept is not a new one; it has been revised over time. The DSB “reviewed several programs with generally acknowledged best practices (e.g., U.S. Postal Service, Virginia Tech, Intel Corporation, etc.) that could easily be molded to serve the DoD environment.”²³⁸ This same approach can be molded to fit local and state public safety agencies with little effort and cost. This model has several components that work toward reducing the threat of targeted violence:

- Increase likelihood of early detection and warning of problems to commanders, supervisors, co-workers with improved information sharing and knowledge.
- Enhance awareness of the risk of targeted violence throughout DoD.
- Address information sharing restrictions.
- Employ advancements in behavioral sciences, data mining, and monitor research in the neurosciences and genomics.²³⁹

If public safety agencies adopt this model or its tenets, they will have a higher likelihood of preventing a radicalized individual from carrying out a violent attack. As mentioned in previous chapters, this ability goes beyond the agency: it extends into the public space as well. If police and fire departments are more aware of the threat of a radicalized responder and have an ability to share concerning information with appropriate personnel, a radical employee’s ability to carry out a plot becomes greatly diminished.

This unit should comprise members from different disciplines, such as law enforcement, fire/rescue, public health, and the mental health fields to give a multi-faceted look at potential problem individuals. A TMU could reside within each department and be staffed by interagency liaisons, or a jurisdiction could elect to develop a single TMU for the city or town composed of members from each department (a task force model). Training in investigation techniques and radicalization would need to be conducted for all who

²³⁸ Defense Science Board, *Predicting Violent Behavior*, 5.

²³⁹ Defense Science Board, 4.

volunteer or are assigned to the TMU. This group would be available to respond to department requests for focused and specialized evaluation and intervention of employees identified as potentially radicalizing to a violent or extreme ideology, prior to formal legal action being taken against the employee.

The TMU approach harkens back to the model mentioned by Baker: using all soldiers as sensors while empowering commanders to take action to prevent a violent attack. This approach can be adapted for public safety use as well, empowering and encouraging supervisors to watch out for their employees while instilling a supportive leadership environment and creating an undesirable environment for someone who is seeking to conduct a violent act.

c. Asymmetric Warfare Group Model

The U.S. Army's Asymmetric Warfare Group (AWG) also weighs in on the topic of insider threats and makes recommendations for preventing attacks from within. The mission of the AWG is to operationally support and develop rapid solutions for commanders to increase soldier survivability and combat effectiveness against current and emerging global threats.²⁴⁰ Primarily, the focus of the AWG's guidance is for soldiers who are deployed overseas and are working with partnering groups, but their model appears to be adaptable for use in public safety agencies.²⁴¹ The AWG document identifies three areas of focus: first, to guide military leaders and personnel on "indicators associated with insider threat activity while serving in partnering environments;" second, to give options for how to deal with a potential insider threat; and finally, to generate open dialogue among deployed personnel that will improve partnerships.²⁴²

The AWG has created a matrix that can be used as a guide for identifying troubling behaviors and indicators. The group also provides a recommended process to follow based

²⁴⁰ United States Army Asymmetric Warfare Group, last modified November 2, 2017, www.awg.army.mil/.

²⁴¹ "Insider Threats in Partnering Environments," Asymmetric Warfare Group, June 2011, <https://info.publicintelligence.net/AWG-InsiderThreats.pdf>.

²⁴² Asymmetric Warfare Group.

on the level of threat. The indicators are broken into three categories based on the level of threat, illustrated in Table 2.

Table 2. Observable Behavioral Indicators²⁴³

OBSERVABLE INDICATORS	
Category I Indicators <ul style="list-style-type: none"> > Complains about other nations or religions > Advocates violence beyond what is the accepted norm > Abrupt behavioral shift > Desires control > Socially withdraws in some occasions > Appears frustrated with partnered nations > Experiences personal crisis > Demonizes others > Lacks positive identity with unit or country > Reclusive > Strange Habits > Peculiar Discussions 	Category II Indicators <ul style="list-style-type: none"> > Verbally defends radical groups and/or ideologies > Speaks about seeking revenge > Associates with persons that have extremist beliefs > Exhibits intolerance > Personally connected to a grievance > Cuts ties with unit, family, or friends > Isolates self from unit members > Intense ideological rhetoric > Attempts to recruit others > Choice of questionable reading materials in personal areas
Category III Indicators <ul style="list-style-type: none"> > Advocates violence as a solution to problems > Shows a sudden shift from "upset" to normal > Takes suspicious travel or unauthorized absences > Stores or collects ammunition or other items that could be used to injure or kill multiple personnel > Verbal hatred of partner nation or individual from partner nation > Exhibits sudden interest in partner nation headquarters or individual living quarters > Makes threatening gestures or verbal threats 	

Baker says, “in this process, the model attempts to differentiate between a high risk individual and the terrorist insider threat individual as a category one behavior,” signifying high-risk behavior, compared to category 3 behaviors, which indicate “terroristic planning.”²⁴⁴ The guide describes which indicators deserve immediate attention and which can be addressed with less aggressive techniques. The aim is to identify threats as quickly and effectively as possible, while still protecting the dignity of the soldier in question, who may be innocent.

²⁴³ Source: Asymmetric Warfare Group, “Insider Threats in Partnering Environments.”

²⁴⁴ Baker, “Change of Detection,” 41.

For example, if an employee begins acting strangely for no apparent reason, an “abrupt behavioral shift,” there may be a motive that indicates what is causing this change. The AWG recommendation for category 1 behaviors is to “closely monitor the situation and/or discuss problems with individual.”²⁴⁵ Baker adds, the “individual [coworkers] can take several actions such as seeking legal consultation, reporting the behavior or asking the suspect for clarification rather than observing to see if the behavior worsens.”²⁴⁶ It could be that the suspect employee is having family issues and has become withdrawn because of embarrassment or out of a desire not to burden coworkers with his or her personal problems. This kind of intervention involves fellow employees directly helping their coworker. If coworkers show concern, this may be enough to bring the withdrawn individual back into the group, making the person feel better and potentially ruling out the threat of insider threat activity. This is in line with the “no soldier left behind” mentality of each employee looking after one another.

For category 2 indicators, more involvement from supervisory staff is required, which makes it a more official intervention. If an individual is openly supporting or defending radical groups or ideologies, this should be seen as an overt indicator that the individual is radicalizing.²⁴⁷ This was a major indicator seen in Nidal Hasan, and should have tipped U.S. Army leadership off that he was radicalizing and moving toward mobilizing an attack on behalf of a terroristic agenda. The recommendation for behavior in this category is “administrative action (such as counseling)” and referral to counterintelligence.²⁴⁸ Not all state and local public safety agencies have counterintelligence units that deal specifically with terrorism; however, each state does have a fusion center to which suspicious activity reports can be forwarded for further review.²⁴⁹

²⁴⁵ Army Asymmetric Warfare Group. “Insider Threats in Partnering Environments.”

²⁴⁶ Baker, “Change of Detection,” 41.

²⁴⁷ Baker, 41.

²⁴⁸ Baker, 41.

²⁴⁹ “Fusion Centers,” National Fusion Center Association, accessed September 28, 2017, <https://nfcausa.org/default.aspx/MenuItemID/117/MenuGroup/Public+Home.htm>.

Reporting suspicious behavior to intelligence or fusion center personnel is a non-punitive method for disseminating concerns and having them appropriately adjudicated as either a legitimate concern or something that does not require immediate action.²⁵⁰ Sometimes a person is having a bad day, says something he or she should not have, and has no intention to carry out a threat. In other cases, like Hasan's, the individual moves to violence and carries out an attack.

Category 3 behaviors are seen as the most severe and should be flagged as violent activity. These are "actions conducted by the subject that would indicate violent or terroristic planning, showing a commitment to carrying out a violent attack."²⁵¹ Some signs would be strange travel habits and absences, collection of weapons or large amounts of ammunition, and violent gestures or direct threats.²⁵² Individually, these may not be foolproof indicators of a plot that will be carried out. For example, the collecting of firearms and ammunition alone could be an indicator of an upcoming hunting trip. But if the individual is also expressing hateful messages, suddenly withdrawing from the organization, or advocating violence as a solution to problems, these signs may be indicators of a malicious action about to be carried out.²⁵³

If an individual has crossed into this category, the recommended action is to "refer [the individual] to counterintelligence and chain of command. Immediate actions, such as removing weapon or detention should be seen as a last resort."²⁵⁴ In career fields for which carrying a weapon is part of the job, it is necessary to prevent the individual from using that weapon to conduct a violent act, but is important to not tip the person over the edge by disarming them unnecessarily. If a fellow employee reports up the chain of command through a suspicious activity report, that individual can be investigated and determined to be a threat or not.

²⁵⁰ Nationwide SAR Initiative, accessed December 4, 2016, <https://nsi.ncirc.gov/>.

²⁵¹ Asymmetric Warfare Group, "Insider Threats in Partnering Environments."

²⁵² Asymmetric Warfare Group.

²⁵³ Asymmetric Warfare Group.

²⁵⁴ Asymmetric Warfare Group.

This guide provides the user with a clear list of indicators to be aware of and breaks them down into categories of severity. Overall, this guide can be adapted for use domestically within the field of public safety. However, one limitation is that it is focused on deployed military personnel dealing with foreign nationals who have questionable allegiances and loyalties; because it is not primarily focused within the home agency, some minor adjustments and changes in terminology would be needed. Regardless, the tenets can be applied to public safety agencies because behaviors transcend geographic boundaries.

3. Information Sharing

In response to the threat of violence, information sharing among agencies can also identify dangerous individuals. On September 16, 2013, Aaron Alexis went on a shooting spree at the Washington, DC, Navy Yard, killing twelve and injuring three others.²⁵⁵ Alexis was a former Navy reservist who separated from service and attained a job as a Department of the Navy civilian at the Navy Yard. During Alexis's enlistment, he was charged with a felony weapons violation while in Texas for "discharging a firearm within a municipality of 100,000 or more."²⁵⁶ Because Alexis failed to disclose this charge to his supervisors, it was never picked up in background checks for his civilian position.²⁵⁷ If this information had been shared, or if those adjudicating Alexis's security clearance had known about this incident, Alexis would have been scrutinized further and he may not have been hired as a Department of the Navy civilian or been able to purchase the firearm used in the Navy Yard shooting.

The Nidal Hasan case also illustrates how a failure in interagency communication can lead to a violent outcome. The event's lead investigator from the San Diego Joint

²⁵⁵ Michael S. Schmidt and Michael D. Shear, "Gunman and 12 Victims Killed in Shooting at D.C. Navy Yard," *New York Times*, September 16, 2013, <http://www.nytimes.com/2013/09/17/us/shooting-reported-at-washington-navy-yard.html?pagewanted=all>.

²⁵⁶ Chief of Naval Operations, *Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices* (Washington, DC: Department of the Navy, 2013), 28, http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf.

²⁵⁷ H.R., *Insider Threat to Homeland Security*, 6.

Terrorism Task Force, a Defense Criminal Investigative Services agent, misidentified “Comm Officer” as communications officer rather than a commissioned officer. This failure to properly distinguish Hasan’s identity led to the agency not sending an Intelligence Information Report to other agencies, including the Army, fearing that Hasan may have access to such reports, which could compromise the investigation.²⁵⁸ Evidence reveals that a combination of poor intelligence sharing and personal biases left Hasan’s behaviors ignored, and prevented proper investigation.²⁵⁹ It is surmised that the FBI and DoD both had important pieces to a puzzle that, if put together, could have possibly saved the lives of those killed that day.²⁶⁰

Verification of an employee’s information has also been seen as a failure point in vetting potential employees. During the congressional hearings on the Navy Yard shooting, it was determined that many applications for security clearances and jobs get filed with incomplete information. The Government Accountability Office comments that “87 percent of 3,500 investigative reports that DoD adjudicators used to make a clearance eligibility decisions were missing some required documentation, such as the verification of all of the applicant’s employment.”²⁶¹ About 12 percent of those did not contain the required applicant’s interview.²⁶² Verification of paperwork and applicant information is crucial to avoiding missteps like the ones described in this section. Authenticating an applicant’s paperwork is particularly important for career fields in which public trust is involved. As discussed in Chapter V, it is also important to verify the authenticity of an applicant’s documentation.

D. CONCLUSION

This chapter summarized the current pre-employment screening procedures for persons seeking to gain employment with the federal government or U.S. military. Many

²⁵⁸ S., *Ticking Time Bomb*, 35; H.R., *Lessons from Fort Hood*, 14.

²⁵⁹ S., *Ticking Time Bomb*, 38–39.

²⁶⁰ H.R., *Lessons from Fort Hood*, 3.

²⁶¹ H.R., *Insider Threat to Homeland Security*, 21.

²⁶² H.R., 21.

of the same procedures are used by local and state public safety agencies, but the level of scrutiny is not as in-depth and some tests are not always conducted, like the polygraph examination. Local and state public safety agencies may do well to incorporate this deeper level of screening and mandate polygraphy in their pre-screening hiring practice.

Another lesson that can be gained from the federal sector is having a program that mandates annual follow-on screenings of employees. Had the FBI had this requirement, Robert Hanssen may have been deterred from sharing secrets with Russia or perhaps would have been caught earlier in his plot. These screenings should include repeat polygraph exams, and should evaluate the employee's presence on social media. Today, public safety agencies do a good job of screening candidates for employment, but generally fail to ensure that those individuals are still maintaining a clean history throughout their careers.

The military also assesses candidates' tattoos for affiliations with extremist groups or gangs. Currently, public safety agencies do not evaluate potential meanings and affiliations of tattoos on candidates for employment. This is not a foolproof method of determining if a candidate is affiliated with an extremist group, but is another layer that a potential radical would have to defeat to gain employment. Based on a similar recommendation to the military, public safety agencies should either establish a tattoo database to screen candidates or should partner with the military and federal counterparts to establish a larger database to access and share tattoo data.

The incorporation of the Rap Back system, which ties in real-time reporting of individuals whose fingerprints are taken, is a major step in closing the information-sharing loop. Currently, if a police officer or firefighter is arrested and fingerprinted, it is incumbent on that individual to pass the arrest information onto his or her host agency. If the arrest occurs out of state and the responder never reports it, no one other than the responder and the arresting agency would be aware of the arrest. Rap Back guarantees that subscribing agencies would be notified of a change to an employee's status, and if his or her fingerprints were run for any reason.

Another recommendation is to incorporate TMUs into public safety agencies. Employing a multi-disciplined team approach to identifying actions and behaviors of potential violent insiders keeps in line with the “prevention over prediction” model of stopping targeted violence. This, coupled with the ASW’s insider threat guidelines, develops a strong, supportive command environment that motivates all members to look after one another. Identifying some of the behaviors should come easy for tight-knit groups like police officers, soldiers, or firefighters; however, being empowered to recognize and take action to take care of their “brother” or “sister” is the important task to thwarting a violent act from the inside. Further study of the efficacy of employing these models into state or local public safety agencies will need to be undertaken, but based on the experiences of military and federal partners these programs seem to be an appropriate fit for local and state public safety agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION AND RECOMMENDATIONS

This thesis began by investigating if a malicious insider within a state or local public safety agency would be able to infiltrate, conceal him or herself, and then carry out a violent attack through the use of his or her access. The infiltrator threat is best demonstrated through Hollywood movies and television shows, most notably the movie *The Manchurian Candidate*, which was the inspiration for the title of this thesis. The made assumption by many who study the insider threat is that the primary threat comes from malicious infiltrators who attempt to join an agency in order to carry out an attack.

The initial research for this thesis confirmed that such an insider is a significant threat, but it also presented a question: Why has there not, to date, been an example of such an insider threat within public safety? This is a point initially raised in Chapter I. The hypothesis was that such individuals were most likely screened out through pre-employment evaluations, which would suggest that continued attention to screening would be the most effective way to continue to reduce the threat of a violent insider.

Instead, the research conducted for this thesis demonstrated that the problem of the insider threat, and the potential solutions to that problem, are more complex than initially believed. This thesis examined federal agency and U.S. military programs that are designed to counter violent insider threats; through case studies of insider threats that have been prevented—and some that were not prevented—it developed lessons learned that may be applied to local or state public safety agencies.

The cases referenced in this thesis all point back to radical Islam, but this is not to say that police and fire departments should be hyper-vigilant when hiring Muslims into the ranks, or that the predominant threat is from radical Islam. In actuality, the findings and recommendations are ideologically neutral, and what motivates the aggressor is not as important as recognizing the signs and behavioral cues of someone radicalizing within a public safety agency. For example, if a person traveled to an area of strife without being a member of an organized or authorized group, this travel may gain the attention of vigilant coworkers. Both Altintas and Young traveled to war zones to fight on behalf of terrorist

organizations. If coworkers were briefed to be aware of strange activity like this travel, perhaps they may have picked up on other signs and prevented their coworkers' actions.

A. FINDINGS

Many of the current pre-employment screening procedures focus on psychological factors to determine if a candidate for a law enforcement or fire department job would be able to carry out the duties of the position. As noted in Chapter V, these tests assess for psychopathology, and other factors associated with success or failure within the public safety fields, like impulse control, honesty, and integrity. This thesis found that psychopathy does not appear to be a prevalent characteristic in terrorists or extremists. As a result, this thesis believes less emphasis should be placed on psychological screenings to detect and deter potential terrorists and extremists, and more focus should be placed on monitoring employees' behaviors and actions for signs of radicalization.

This finding contrasts with Martin Hershkowitz's recommendation, which advocates for continuous psychiatric or psychological screenings. He believes that "a psychological examination by a Certified Clinical Psychologist should be performed no less often than every two or three years in order to build on the psychological baseline and to detect early signs of terrorist discipline breakdown or anxiety development among employees under continuing stress from the [homeland security/homeland defense] missions."²⁶³ This recommendation comes from the belief that psychological examinations and re-examinations should be carried out to initially determine a psychological baseline, and then to see if a shift in that baseline occurs, which may be indicative of an insider attack. This thesis, as supported by the research conducted, does not advocate for completely disregarding this recommendation, as psychological changes may occur that may negatively affect an employee; but in screening for potential radicalization, psychological baselines will not be relevant. According to the research on this topic, there would not generally be a shift in psychology as much as an ideological or behavioral change.

²⁶³ Hershkowitz, "The 'Insider' Threat," 108.

The major finding of this thesis, which was contrary to the initial assumption, is that the biggest threat from a malicious insider exists from employees who are already in the organization. This opposes the findings of some researchers like Nicholas Catrantzos, who advocates for more attention to be placed on combatting infiltrators. However, based on the case studies and historical data within the U.S. military, state and local public safety agencies, and overseas, the insider threat consists primarily of individuals who radicalize to an ideology while already employed. Examples from Chapter III such as Nidal Hasan, Syed Farook, and Mevlut Mert Altintas highlight this finding, as all three were already invested in their host agencies before they radicalized.

B. RECOMMENDATIONS

This thesis sought to recognize how a malicious insider would most likely carry out a terrorist attack, reliant upon his or her access within local and state public safety agencies, and what vulnerabilities the malicious insider could exploit in doing so. The research led the author to discover vulnerabilities in the current pre-employment screening process, and in the culture of first responders, that could enable a malicious insider. These discoveries led to the development of recommendations that local and state public safety agencies can implement based on best practices established by federal agencies and the U.S. military.

Between the author's experience within public safety and the research described in the previous chapters, this thesis proposes the following four general recommendations to prevent a malicious insider within public safety. First, organizations should make themselves difficult to infiltrate, a practice that requires stricter pre-recruitment and screening procedures. Next, first responders must be aware that the threat exists, and must be familiar with the signs of radicalization; this is the awareness and education piece to the solution, and is a form of target hardening. Third, public safety agencies should establish procedures that give responders a clean reporting mechanism for any suspicions about fellow responders. Additionally, internal procedures should be developed to ensure any report from a concerned member of staff is dealt with appropriately before a fellow responder fully radicalizes and carries out a violent attack. Finally, there should be a strong

investigative and mitigation strategy to handle reports of potential first responder radicalization.

1. Pre-recruitment Selection and Screening Procedures

A key takeaway from the literature is that organizations should make it difficult for employees to become malicious insiders. This applies to both the infiltrator and the employee who is already employed within an agency when he or she radicalizes. If the candidate for employment or current employee does not fear that the present culture and structure would thwart a nefarious plot, he or she is more likely to attempt to actionize a plan. In the case of a police or fire department, preventative action could simply involve educating the public and likely applicants for employment. If those seeking to gain employment as a firefighter or police officer are aware that they will be subject to extreme scrutiny, they may second guess their plans to infiltrate a public safety department. Additionally, as indicated in Chapters V and VI, agencies should increase the depth of their screening procedures and employ polygraphy. Specifically, if the examiner asks questions that seek to identify potential terrorists or extremists, applicants are put on notice that dishonesty will be identified, along with affiliation with extremist or terrorist groups and potential signs of radicalization.

If malicious applicants feel that they are being watched, the possibility that they will be reported—or their plot thwarted—increases, and therefore their desire to plan a malicious attack decreases. This is strongly tied to the next recommendation; education will strengthen the organization’s ability, as a whole, to prevent a malicious insider from furthering his or her plans. This is a practice known as target hardening.

2. Awareness, Education, and Target Hardening

Teaching current employees about the signs of radicalization and how to report concerns is a key to hardening the “target” of a public safety department. BaMaung describes this as target hardening, a concept employed in many defensive strategies and physical security protection programs. He believes that “if the organization has a weak security culture, poor security practices may be accepted as being normal. This could allow

a hostile individual, be they terrorist, criminal, or disaffected employee, to better avoid detection of potential aberrant behavior.”²⁶⁴

However, the level of training first responders receive on insider threat awareness varies throughout the country. Some agencies mention this threat in the context of a disgruntled employee, but fail to mention it in the context of terrorism. Even still, the majority of local and state public safety agencies do not put much emphasis on this training, defaulting instead (under budget constraints) to higher-priority trainings for job-related requirements. Hershkowitz articulates that “all employees and management should be trained to recognize those characteristics that imply that the individual displaying those characteristics may be a saboteur, terrorist, criminal or simply dangerous person for their mission(s) and how to handle the next steps.”²⁶⁵

Educating employees about the signs of radicalization and potential violence is a major step in prevention. Shaw and Fischer agree that more training for management personnel should also be stressed.²⁶⁶ Many of these signs, such as disregard for authority, confrontational behavior, and disengagement, are highlighted in the table in Appendix A. A job aid, similar to the one developed by the Asymmetric Warfare group referenced in Chapter VI, should be developed and distributed to first responders to help guide decision making and identification of potential radicalization.

An environment of education, coupled with a strong command attitude that all employees should look after one another, presents a major deterrent to an individual who seeks to use his or her trusted access as a first responder to conduct a violent attack. Scrutiny of employees’ performance and behavior at all levels should be instilled from upper management, and seen as an opportunity for improved performance rather than as a punitive measure. This scrutiny may also uncover the nefarious actor within a public safety

²⁶⁴ BaMaung et al., “The Enemy Within,” 142.

²⁶⁵ Hershkowitz, “The ‘Insider’ Threat,” 110.

²⁶⁶ 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, Defense Personnel Security Research Center, 2005), 108–109, <http://docplayer.net/1427558-Ten-tales-of-betrayal-the-threat-to-corporate-infrastructures-by-information-technology-insiders-analysis-and-observations.html>.

agency during the planning stages of a plot; deteriorating performance has been seen as a precursor to targeted violence. Nidal Hasan was seen as a “barely competent psychiatrist” by many of his colleagues and superiors, indicating a lackluster pattern of performance.²⁶⁷

Anti-radicalization training should be extended to employees at all levels within the organization. The legal section of both the police and fire departments and the jurisdictional legal department should be involved, as they will have to deal with any claims erupting as a result of an investigation of a suspicious employee. Hershkowitz believes that “attorneys should undergo annual training on national, state, and local laws governing allowable incursion into an employees perceived rights. Many of these issues have already been decided in favor of the employer; however, the employees’ attorneys continue to raise variables on each situation.”²⁶⁸ Jurisdictions and the public safety departments that protect them need to be prepared for potential litigation, proper or improper, that may be raised against them for investigating their employees.

3. Reporting Mechanism

Once responders are aware of warning signs with regards to radicalization, they should also be taught a proper reporting mechanism to ensure that the right people are made aware of the concern, and that the correct response is initiated against the employee. This could be a simple sit-down with the first line supervisor, and possibly a union representative. If the problem appears beyond the scope of the first line supervisor, or if the initial meeting proves ineffective, the next step should be referral to the threat management unit established within the department or jurisdiction for further evaluation. The point is to evaluate the suspicious responder in as non-invasive and non-threatening a manner as possible.

If further evaluation is required, the case should then be referred for investigation to a regional fusion center or joint terrorism task force, which could adjudicate the individual in question. This investigation may be the piece needed to recognize a larger

²⁶⁷ S., *Ticking Time Bomb*, 33

²⁶⁸ Hershkowitz, “The ‘Insider’ Threat,” 110.

nefarious plot and allow law enforcement to interdict before the insider can operationalize the plot. This cycle is outlined in the flow chart in Appendix B; the chart considers the unique structures of public safety agencies throughout the United States and is adaptable to account for these differences. If both management and labor organizations agree that a TMU should be employed as a last resort prior to legal action, they can intervene with a troubled employee quickly, whether the individual is suspected of plotting an act of targeted violence or is contemplating suicide. Any delay gives the employee time to further his or her plot, and punitive action without proper supervision may prompt the employee to act more quickly.

Before an employee is referred for potential radicalization or movement to violence, a fellow responder is most likely to notice a change in the employee's behavior. People who spend a lot of time together generally understand what is considered "normal" behavior for the other person. Changes in behavior are therefore often apparent between coworkers. Currently, if a first responder is suspected of contemplating suicide, his or her fellow responders are usually quick to respond and try to intervene. The same should be done for those responders suspected of radicalization.

If a responder is referred for evaluation, at a minimum, the responder should receive the care that he or she needs, at least in the case of potential suicide; in the case of radicalization, however, the responder should be evaluated for his or her potential to carry out a violent action against coworkers or society. Recognition and reporting are the two guideposts that should be emphasized in public safety agencies to prevent a person from radicalizing, and to prevent a violent attack.

Fellow employees are in a position to monitor one another, and are in a strong position to notice changes in each others' behavior. As trained observers, police and firefighters are mindful of conditions that are out of the ordinary and have to be able to react to these changes. Noticing strange behavior in fellow responders is no different.

This strategy plays into another recommendation from Chapter III—employing a "my brother's keeper" approach. This approach involves empowering employees to look after one another and to be on the lookout for behavioral changes, and endows them the

power to report that information in a non-punitive and supportive manner. This approach should come from the head of the agency, who must instill a command attitude that encourages support between employees. The U.S. military prides itself in the “leave no soldier behind” mantra. The approach recommended in this thesis branches off from that ethos, encouraging police officers and firefighters to not “leave their coworkers behind”; if a fellow responder is exhibiting behavioral changes, it is going to be the coworkers who will notice these changes first.

Christine Baker advocates that every soldier becomes a sensor, while Catrantzos prefers to think that “every team member becomes not an inquisitor but a co-pilot.”²⁶⁹ Within industries that rely heavily on trust and knowing that the officer to your left or right is entrusted with your well-being, and you are entrusted with theirs, it is important for responders to maintain that level of trust. It is equally important, however, to look after that well-being by reporting suspicious activities or behaviors that could signal a violent action. This should be instilled at the highest command levels and pressed as a safe method to support fellow responders.

Currently, police and fire departments are putting a lot of effort and emphasis into preventing suicide by their members due to PTSD and depression. Initiatives like the Code Green Campaign, mentioned in Chapter III, are educating first responders about the signs and symptoms of someone who may be contemplating suicide and empowering those same responders to report coworkers who may need help.²⁷⁰

The responder who notices these signs in a fellow responder should feel confident in reporting the change in behavior, whether they think the troubled coworker is considering suicide or radicalizing to a terrorist ideology. Reporting the coworker will bring the required help. This thesis advocates the use of the TMU model because it involves mental health professionals early in the process; therefore if the coworker were having

²⁶⁹ Baker, “Change of Detection”; Catrantzos, *Tackling the Insider Threat*.

²⁷⁰ The Code Green Campaign, accessed September 23, 2017, <http://webcache.googleusercontent.com/search?q=cache:http://codegreencampaign.org/>.

psychological problems, help would be readily available. If the coworker were radicalizing, he or she would be identified and handled appropriately by a proper investigation.

Another recommendation that aligns with reporting is for public safety agencies to subscribe to the FBI's Rap Back program. This is not directly tied to recognizing radicalization in employees, but would be a useful tool that increases communication between separate agencies. As referenced in Chapter VI, had this reporting mechanism been in place prior to the Washington, DC, Navy Yard shooting, Aaron Alexis may have been thwarted before he moved to violence, and would not have been able to procure the firearms used in the attack. Nationally, this system also ties public safety agencies together for real-time situational awareness of responders who are being processed for illegal activities.

4. Investigations and Threat Management Units

Had Nidal Hasan's chain of command been more proactive in investigating his rhetoric and lack of support for the U.S. Army, his attack may have been prevented as well. Individuals within agencies need to be able to share their concerns, and need to be aware if another agency has information that indicates the individual may be radicalizing. The failure to share intelligence gathered on Hasan with the U.S. Army and the Army's failure to use what information they had on Hasan to investigate him further have been cited as some of the major failures in this case.

In hindsight, a threat assessment would probably have demonstrated that Hasan was moving toward a violent attack, but this type of assessment was never conducted. As a result of the shooting at Fort Hood, the U.S. military has begun using multi-disciplinary TMUs to assess these threats and intervene if necessary. This is a program that was discussed in Chapter VI for potential use in state and local public safety agencies.

When investigating employees, there are legal concerns, as well as privacy and confidentiality concerns. Police departments are familiar with related procedures through their internal affairs divisions, but this may be an area that the fire service is not as accustomed to dealing with. First responders deserve a degree of privacy in how they live their lives, like anyone subject to a law enforcement investigation.

If an investigation is conducted on an employee, and information that the employee would rather keep private is found, the employer must maintain discretion regarding how that information is used and disseminated. However, provided that any information gained through an investigation is not used against the individual, with the exception of an uncovered criminal or terrorist matter, the concern for privacy should be reduced. This is especially true for possible terrorist activities or actions through which an employee may be threatening to harm him or herself or others; such information would need to be disclosed in the interest of saving lives, despite privacy concerns.

Considering the ramifications of investigating a first responder for potential radicalization to an extremist or terrorist ideology, organizations need to ensure that everyone involved in employing that responder is aware and approves of the process for investigating such concerns. The employee, when hired, should be aware that he or she may be subject to investigation if a concern is raised that he or she may be radicalizing or exhibiting uncharacteristic behavior. Organizational management, human resources, and union and legal representatives all need to approve of and support the procedure for investigating an employee. This reduces any blowback from an employee who feels his or her rights are infringed, but also helps to ensure as smooth and efficient a process to properly adjudicate the employee should a concern be raised. Wasting time with checks and balances while trying to conduct an investigation may provide more opportunities for failure and may allow a violent plot to be successful. The process needs to be clean and systematic.

C. IN CLOSING

This thesis delved into whether or not it would be possible to detect a potential violent insider within a local or state public safety agency before he or she commits an atrocity against fellow first responders or the civilian population. Primarily, it focused on what lessons could be gained from applicable case studies, federal agencies and the U.S. military, and the effectiveness of current programs. A major assumption of this thesis was that most first responders are not aware of what constitutes an insider threat, and what behaviors would be indicative of that threat. Further, it also assumed that this behavior

would not be effectively reported due to a lack of knowledge of the signals associated with radicalization and insider threat activity, coupled with the fact that many organizations do not have established policies for suspicious activity reporting. Generally, leadership in public safety departments has not been trained to handle this potential scenario, and guidelines and procedures are not in place to assist them and their employees in doing so.

This thesis was based on case study analyses; psychological, behavioral, and radicalization theories; and pre-employment psychological testing. This exploration presents opportunities for further study, to include evaluating what the current baseline of knowledge is among local and state first responders. If it can be proven that most local and state first responders know what the signs of radicalization are, and how to report them appropriately, the threat of a malicious insider within this group might be reduced. However, this thesis stands with the belief that less overt signs will be missed and a responder who radicalizes will more than likely be missed, allowing for a violent attack to occur within the agency or the public.

By being mindful of the coworker who radicalizes to an ideology, responders can take action to prevent a fellow first responder from carrying out a violent attack against either the agency or the public. The focus should be shifted from testing individuals who are attempting to gain entry into an organization to training all members of an organization, from leadership down to the recruit officer, to be aware of the signs of radicalization, and to be aware of the steps they should take to react to a radicalizing first responder.

However, one area of concentration that this thesis did not address, as it was out of the scope of the study, was the financial impact of implementing some of these recommendations. Agencies that are not currently using polygraph examinations for new employees may need to consider additional costs to include this as part of initial screening procedures. To establish a TMU in a jurisdiction, there would also need to be buy-in from the different disciplines that would be involved in staffing and maintaining such a unit, should the need arise. Consideration of these factors is both jurisdictionally and individually dependent within a public safety department—it will depend on whether or not the leadership sees terrorist infiltration and radicalization as a large enough problem to

invest money into training and further pre-employment testing. A cost-benefit analysis would need to be undertaken to establish this on a department-to-department basis.

This thesis has identified a serious problem that has been seen in other career fields and in other countries, but that has yet to materialize domestically in the United States. The concept of a first responder using his or her access to further a terrorist goal is a difficult one to imagine, and an equally difficult problem to plan for without considering the threat. This thesis believes that with proper acknowledgement of the threat, and by instituting training for employees and leadership that mirrors U.S. military and federal law enforcement agencies, state and local public safety agencies will be safer and will prevent the deaths of Americans. The threat of terrorism continues to evolve and tactics continue to change; state and local first responders need to be able to evolve with that threat, and must make their agencies difficult to manipulate if malicious insiders wish to conduct an act of terrorism.

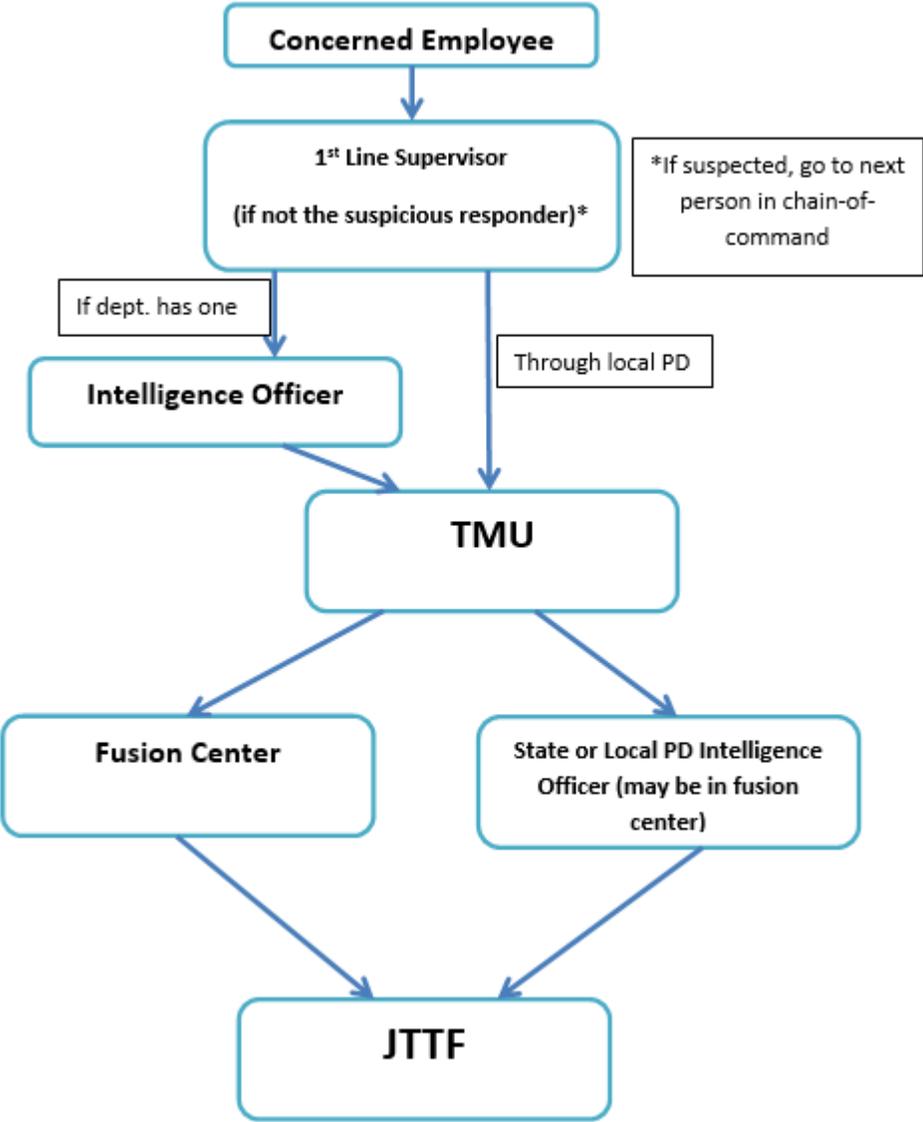
APPENDIX A. INSIDER THREAT BEHAVIORAL INDICATORS

Indicator	Description
Disregard for Authority	The employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.
Disgruntlement	Employee is observed to be dissatisfied in current position; shows chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid or undervalued; may have a poor fit with current job.
Anger Management Issues	The employee often allows anger to get pent up inside; employee observed to have trouble managing lingering emotional feelings of anger or rage; hold strong grudges.
Confrontational Behavior	Employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoids meetings.
Not Accepting Criticism	The employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message is delivered. Employee has been observed being unwilling to acknowledge errors; or admitting to mistakes; may attempt to cover up errors through lying or deceit.
Self-Centeredness	The employee disregards needs or wishes of others, concerned primarily with own interests and welfare.
Stress	The employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.
Performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.
Lack of Dependability	Employee is unable to keep commitments /promises; unworthy of trust.
Personal Issues	Employee has difficulty keeping personal issues separate from work, and these issues interfere with work.
Absenteeism	Employee has exhibited chronic unexplained absenteeism.

Source: Greitzer et al., "Psychosocial Modeling of Insider Threat Risk," 110.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PROPOSED REPORTING STRUCTURE



THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Asymmetric Warfare Group. "Insider Threats in Partnering Environments." June 2011. <https://info.publicintelligence.net/AWG-InsiderThreats.pdf>.
- Babcock, Ernest. "PIA: NGI Rap Back Service." Assessment, FBI, 2016. www.fbi.gov/file-repository/pia-ngi-rap-back-service.pdf/view.
- Baker, Christine. "Change of Detection: To Find the Terrorist Within the Identification of the U.S. Army's Insider Threat." Master's thesis, U.S. Army Command and General Staff College, 2012). <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA565992>.
- BaMaung, David, David McIlhatton, Murdo MacDonald, and Rona Beattie. "The Enemy Within? The Connection between Insider Threat and Terrorism." *Studies in Conflict & Terrorism* 41, no. 2 (October 2016): 1–18, <http://doi.org/10.1080/1057610X.2016.1249776>.
- Bhui, Kamaldeep. "Radicalisation: A Mental Health Issue, Not a Religious One." *New Scientist*, April 8, 2015. <https://www.newscientist.com/article/mg22630160-200-radicalisation-a-mental-health-issue-not-a-religious-one/>.
- Blades, Marleah. "The Insider Threat." *Security Technology Executive* (November/December 2010): 32–37.
- Buck, Kelly R., Andree E. Rose, Martin F. Wiskoff, and Kahlila M. Liverpool. *Screening for Potential Terrorists in the Enlisted Military Accessions Process*. Monterey, CA: Defense Personnel Security Research Center, 2005.
- Catrantzos, Nicholas. "No Dark Corners: Defending against Insider Threats to Critical Infrastructure." Master's thesis, Naval Postgraduate School, 2009. <http://calhoun.nps.edu/handle/10945/4656>.
- . *Tackling the Insider Threat*. Alexandria, VA: ASIS International, 2010. <http://www.popcenter.org/library/crisp/insider-threat.pdf>.
- Centre for European and North Atlantic Affairs. "Extremism vs. Armed Forces: Implications for Internal Security and Recommendations for the Future." September 2013. http://cenaa.org/en/wp-content/uploads/2013/09/RT3_final_ENG.pdf.

- Chief of Naval Operations. *Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices*. Washington, DC: Department of the Navy, 2013. http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf.
- Cochrane, Robert E., Robert P. Tett, and Leon Vandecreek. "Psychological Testing and the Selection of Police Officers: A National Survey." *Criminal Justice and Behavior* 30, no. 5 (October 1, 2003): 511–537. <http://doi.org/10.1177/0093854803257241>.
- Cole, Eric A. "SANS Analyst Program: Correlating SIM Information to Detect Insider Threats." White paper, SANS Institute, 2007. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.592.8151&rep=rep1&type=pdf>.
- Cole, Jon, Ben Cole, Emily Alison, and Laurence Alison. "Free Radicals— Stopping Extremists before They Start." *Jane's* by HIS Markit, September 16, 2010. <https://janes.ihs.com.libproxy.nps.edu/IntelligenceReview/Display/1196061>.
- Crossett, Chuck, and Jason Spitaletta. "Asymmetric Warfare Group Report: Psychological and Sociological Concepts of Radicalization." *Public Intelligence*, September 2010. <https://publicintelligence.net/us-army-radicalization-concepts>.
- Defense Science Board. *Task Force Report: Predicting Violent Behavior*. Washington, DC: Department of Defense, 2012. 14, <http://www.acq.osd.mil/dsb/reports/2010s/PredictingViolentBehavior.pdf>.
- Defense Security Service. "Insider Threats: Combating the Enemy within Your Organization." Accessed February 17, 2018. <https://www.hsdl.org/?abstract&did=752042>.
- Department of the Army. *Threat Awareness and Reporting Program*, AR 381-12. Washington, DC: U.S. Government Printing Office, 2010.
- Department of Defense (DoD). "DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team." Defense Technical Information Center, accessed March 4, 2017. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380.
- . *Insider Threat Program*, DoDD 5205.16. Washington, DC: DoD, 2017. www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516_dodd_2014.pdf?ver=2017-08-28-090609-503.
- Department of Homeland Security Office of Inspector General. *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain*, OIG-12-120. Washington, DC: Department of Homeland Security, 2012. <http://thehill.com/images/stories/blogs/flooraction/jan2012/oigtsa.pdf>.

- Douglas, John E., Robert K. Ressler, Ann W. Burgess, and Carol R. Hartman. "Criminal Profiling from Crime Scene Analysis." *Behavioral Sciences & the Law* 4, no. 4 (1986): 401–421.
- Flacks, Mark, and Martin Wiskoff. *Gangs, Extremists Groups, and the Military: Screening for Service*, SRC-TR-98-003. Monterey, CA: Security Research Center, 1998. <http://www.dtic.mil/dtic/tr/fulltext/u2/a359551.pdf>.
- Gaschler, William J., James P. McGettigan, Paul M. Menges, and James F. Waller. "Review of Polygraph Screening Assessment Method." *Polygraph* 30, no. 4 (2001): 254–259.
- Greenwood, Shannon, Andrew Perrin, and Maeve Duggan. "Social Media Update 2016." Pew Research Center, November 11, 2016. <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>.
- 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 (July 3, 2014): 106–38. <https://muse.jhu.edu/article/548560>.
- Hafez, Mohammed, and Creighton Mullins. "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism." *Studies in Conflict & Terrorism* 38, no. 11 (November 2, 2015): 958–75. <http://doi.org/10.1080/1057610X.2015.1051375>.
- Hall, Caitlin Squire. "The Trusted Shadow and Trojan Horse of the United States Government: Human Behavior and the Insider Threat." *Small Wars Journal*, March 20, 2014. www.smallwarsjournal.com/printpdf/15439.
- Handler, Mark, Charles R. Honts, Donal J. Krapohl, Raymond Nelson, and Stephen Griffin. "Integration of Pre-employment Polygraph Screening into the Police Selection Process." *Journal of Police and Criminal Psychology* 24, no. 2 (October 1, 2009): 69–86. <https://doi.org/10.1007/s11896-009-9050-2>.
- Hershkovitz, Martin. "The 'Insider' Threat: How to Minimize it." *Journal of Police Crisis Negotiations* 7, no. 1 (January 2007): 103–111.
- Homeland Security Committee. *America's Airports: The Threat from within*. Washington, DC: U.S. House of Representatives, 2017. <https://homeland.house.gov/press/committee-releases-report-americas-airports-threat-within/>.
- Hunker, Jeffrey, and Christian W. Probst. "Insiders and Insider Threats." *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications* 2, no. 1 (2011): 4–27. <http://isyu.info/jowua/papers/jowua-v2n1-1.pdf>.

- Inwald, Robin. "The Inwald Personality Inventory (IPI) and Hilson Research Inventories: Development and Rationale." *Aggression and Violent Behavior* 13, no. 4 (August 2008): 298–327. <http://doi.org/10.1016/j.avb.2008.04.006>.
- Kenny, James F. "Threats in the Workplace: The Thunder before the Storm?." *Security Journal* 18, no. 3 (May 2005): 45–56. <http://doi.org/10.1057/palgrave.sj.8340203>.
- Laguna, Louis, Joseph Agliotta, and Stephanie Mannon. "Pre-employment Screening of Police Officers: Limitations of the Mmpi-2 K-Scale as a Useful Predictor of Performance." *Journal of Police and Criminal Psychology* 30, no. 1 (2015): 1–5. <https://doi.org/10.1007/s11896-013-9135-9>.
- Liang, Nan, and David Biros. "Validating Common Characteristics of Malicious Insiders: Proof of Concept Study." *IEEE International Conference on System Sciences* (January 2016). <http://doi.org/10.1109/HICSS.2016.463>.
- McCauley, Clark. "Psychological Issues in Understanding Terrorism and the Response to Terrorism." Om *Psychology of Terrorism*, edited by Chris E. Strout, 3–29. New York: Oxford University Press. <http://www.start.umd.edu/publication/psychological-issues-understanding-terrorism-and-response-terrorism>.
- Moghaddam, Fathali M. "The Staircase to Terrorism: A Psychological Exploration." *American Psychologist* 60, no. 2 (February 2005): 161–69. <http://dx.doi.org/10.1037/0003-066X.60.2.161>.
- Moore, Andrew, Dawn Cappelli, and Randall Trzeciak. *The "Big Picture" of Insider IT Sabotage across U.S. Critical Infrastructures*. Pittsburgh, PA: Carnegie Mellon University, 2008. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8703>.
- National Research Council. "The Polygraph and Lie Detection. Committee to Review the Scientific Evidence on the Polygraph. Division of Behavioral and Social Sciences and Education." *The National Academic Press*, no. 7 (2003): 9.
- Noonan, Thomas, and Edmund Archuleta. "The Insider Threat to Critical Infrastructures." Report, National Infrastructure Advisory Council, 2008 www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
- Navarro, Joe. "Unmasking Terrorists—Two Critical Characteristics!." *Psychology Today*, December 31, 2009. <http://www.psychologytoday.com/blog/spycatcher/200912/unmasking-terrorists-two-critical-characteristics>.

- Parkin, William S., Steven M. Chermak, Joshua D. Freilich, and Jeff Gruenewald. "Twenty-Five Years of Ideological Homicide Victimization in the United States of America." Report, National Consortium for the Study of Terrorism and Response to Terrorism, 2016. http://start.umd.edu/pubs/START_CSTAB_ECDB_25YearsofIdeologicalHomicideVictimizationUS_March2016.pdf.
- Predd, Joel, Shari Lawrence Pfleeger, Jeffrey Hunker and Carla Bulford. "Insiders Behaving Badly." *IEEE Security & Privacy* 6, no. 4 (July 2008): 66–70. <http://doi.org/10.1109/MSP.2008.87>.
- Reddy, Marisa, Randy Borum, John Berglund, Bryan Vossekuil, Robert Fein, and William Modzeleski. "Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches." *Psychology in the Schools* 38, no. 2 (March 2001): 157–172. <http://doi.org/10.1002/pits.1007>.
- 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, Defense Personnel Security Research Center, 2005. <http://docplayer.net/1427558-Ten-tales-of-betrayal-the-threat-to-corporate-infrastructures-by-information-technology-insiders-analysis-and-observations.html>.
- Sinai, Joshua. "Can Terrorists Be Psychologically Profiled?." *Journal of Counterterrorism and Homeland Security International* 17, no. 2 (Summer 2011). <http://www.lexisnexis.com.libproxy.nps.edu/lnacui2api/api/version1/getDocCui?ni=54K8-YNS1-DYRW-V4BK&csi=244681&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true>.
- Timm, H. W., and W. K. Hedges. "Factors Theoretically Affecting the Incidence of Deceptive Responses During Preemployment Screening Procedures." *Polygraph* 22, no. 3 (1993): 229–244.
- Victoroff, Jeff. "The Mind of the Terrorist: A Review and Critique of Psychological Approaches." *Journal of Conflict Resolution* 49, no. 1 (2005): 3–42. <http://doi.org/10.1177/0022002704272040>.
- Weiss, Peter A., and William U. Weiss. "Criterion-Related Validity in Police Psychological Evaluations." In *Handbook of Police Psychology*, edited by Jack Kitaeff, 125–133. New York: Routledge, 2011.
- Weiss, Peter A., William U. Weiss, James E. Vivian, Robert Davis, and Cary Rostow. "Exploring the MMPI-2 L Scale Cutoff in Police Selection." Matrix Incorporated, accessed September 17, 2016. <http://www.matrixinc.cc/publications/Exploring%20the%20MMPI-2%20L%20Scale%20Cutoff%20In%20Police%20Selection.pdf>.

William H. Webster Commission. "Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009." Internet Archive, accessed September 1, 2016. <https://ia600501.us.archive.org/32/items/final-report-of-the-william-h.-webster-commission/final-report-of-the-william-h.-webster-commission.pdf>.

INITIAL DISTRIBUTION LIST

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