REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/28/2021	Master's Degree Thesis	September 2020-May 2021

4. TITLE AND SUBTITLE

STUCK IN A RUT
AN ANALYSIS OF SUITABLE MISSIONS TO HELP GET
TSA's VISIBLE INTERMODAL PREVENTION AND RESPONSE PROGRAM
BACK ON THE ROAD

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Nelson Minerly
Transportation Security Administration
Department of Homeland Security

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Advanced Warfighting School
7800 Hampton Blvd.
Norfolk, VA 23511

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joint Forces Staff College - NDU
Joint Advanced Warfighting School
7800 Hampton Blvd.
Norfolk, VA 23511

10. SPONSOR/MONITOR'S ACRONYM(S)
NDU-JAWS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES
Open source information as of 01 May 2021.

14. ABSTRACT

The Transportation Security Administration's (TSA) Visible Intermodal Prevention and Response (VIPR) program deploys screening and law enforcement resources to augment and enhance transportation security. This thesis evaluates potential missions selected from TSA's 2020 Biennial National Strategy for Transportation Security Report to Congress that lend themselves to the VIPR program's unique legal authority, ability to provide federal resources, and its embedded capability to deploy personnel and resources to assist stakeholders in all modes of transportation. Recommendations presented in this thesis will enhance VIPR's utility in identifying, detecting, and preventing violent extremist attacks.

15. SUBJECT TERMS
Department of Homeland Security, Transportation Security Administration, Visible Intermodal Prevention and Response, Unmanned Aircraft Systems, Improvised Explosive Devices, Lone-Offender

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Nelson Minerly
U	U	U	UU	57	19b. TELEPHONE NUMBER *(Include area code)* 757-443-6252

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

STUCK IN A RUT
AN ANALYSIS OF SUITABLE MISSIONS TO HELP GET TSA's VISIBLE INTERMODAL PREVENTION AND RESPONSE PROGRAM BACK ON THE ROAD

By:

Nelson Minerly

Department of Homeland Security
Transportation Security Administration

Page Intentionally Left Blank

STUCK IN A RUT
AN ANALYSIS OF SUITABLE MISSIONS TO HELP GET TSA's VISIBLE INTERMODAL PREVENTION AND RESPONSE PROGRAM BACK ON THE ROAD

by Nelson Minerly

Department of Homeland Security
Transportation Security Administration

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Student: Nelson Minerly
Signature: 
28 May, 2021

Thesis Advisor:
Signature: 
Mary S. Bell, Ph.D.
Associate Professor

Approved by:
Signature: 
Glenn H. Jones, Ph.D.
Committee Member

Signature: 
Miguel L. Peko, USN, CAPT
Director, Joint Advanced Warfighting School

Abstract

The mission of the Transportation Security Administration's (TSA) Visible Intermodal Prevention and Response (VIPR) program is to "promote confidence in and protect our nation's transportation systems through targeted deployment of integrated assets utilizing screening and law enforcement in coordinated activities to augment and enhance security."[1] Since the VIPR program's stand-up in 2005, the transportation domain's threat profile has evolved significantly. State, Local, Tribal, and Territorial (SLTT) authorities have partnered with TSA to enhance their security and law enforcement posture throughout the transportation domain. Due to the open nature of the transportation domain, US transportation systems continue to be an attractive target for violent extremists.[2] This thesis evaluates potential missions selected from TSA's *2020 Biennial National Strategy for Transportation Security Report to Congress* that lend themselves to the VIPR program's unique legal authority, ability to provide federal resources, and its embedded capability to deploy personnel and resources to augment SLTT transportation security, with distinctly federal capabilities, in all modes of transportation. Recommendations presented in this thesis will enhance VIPR's utility in identifying, detecting, and preventing violent extremist attacks in the transportation domain.

[1] U.S. Transportation Security Administration. "TSA Management Directive No. 2800.13: Visible Intermodal Prevention and Response Program (VIPR)," 10 March 2017

[2] U.S. Transportation Security Administration, "2020 Biennial National Strategy for Transportation Security Report to Congress," 29 May 2020, https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf (Accessed 25 October 2020) Pg. 5

Page Intentionally Left Blank

Dedication

To my wife and children, thank you for your support during this challenging year.

To all the Federal Air Marshals who have tirelessly protected the traveling public in the post 9/11 era, it is an honor serving alongside you.

Page Intentionally Left Blank

Acknowledgments

Thank you to the Transportation Security Administration/Law Enforcement for providing me with the opportunity to attend the Joint Advanced Warfighting School. Many thanks to the Transportation Security Operations Center management team for supporting my studies and carrying my workload during my absence from the office.

To Seminar 2, I was humbled to be part of such an amazing group. Your professionalism and insight allowed me to gain a broader perspective of the world beyond the borders of the United States. As we pass this *decisive point* in our careers, I look forward to seeing each of you rise in the ranks and become the *centers of gravity* in your respective organizations.

Captain James Jacobs, Colonel Kristian Smith, and Dr. David Rodearmel, thank you for the academic challenge and guidance throughout the year. Dr. Mary Bell and Dr. Glenn Jones, my thesis advisors, thank you for mentoring me throughout the year of study and specifically with the development of this thesis.

Page Intentionally Left Blank

Table of Contents

Page Intentionally Left Blank

Chapter 1: Introduction

9/11, TSA, and the Transportation Domain

On the morning of 11 September 2001 (9/11), the United States was attacked by members of the violent extremist organization al-Qaida. Using commercial aircraft as weapons of mass destruction, the 9/11 hijackers focused the Nation's attention on the transportation domain's security vulnerabilities. In November 2001, the newly created Transportation Security Administration (TSA) received the herculean task of securing the US transportation domain. The *Aviation and Transportation Security Act* (ATSA) of 2001 consolidated federal transportation security responsibilities into a single agency, the TSA.[1] Since 2001 TSA has been famous, and more often infamous, for its aviation security programs; airport checkpoint security, Federal Air Marshal (FAM) deployments, and air cargo screening. Under ATSA, TSA is also granted statutory security responsibilities throughout the domestic surface transportation domain; mass transit, freight rail, highway motor carrier, and pipeline.[2] Within the transportation domain, TSA works to protect:[3]

- 440 federalized airports serving approximately 23,000 domestic and 2,600 international flights per day
- Four million miles of roadways
- 140,000 miles of railroad track
- 612,000 bridges and more than 470 tunnels

---

[1] U.S. Transportation Security Administration. "Aviation and Transportation Security Act of 2001" https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf (Accessed on 24 October 2020)

[2] U.S. Transportation Security Administration. "Aviation and Transportation Security Act of 2001" https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf (Accessed on 24 October 2020)

[3] U.S. Transportation Security Administration. "Factsheet: TSA by the Numbers," 4 February 2020, https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet.pdf (Accessed on 20 December 2020)

- 360 maritime ports, over 3,700 marine terminals
- 12,000 miles of coastline
- 2.75 million miles of pipeline
- 30 million daily trips taken on public transportation

Today, TSA is the Department of Homeland Security's (DHS) component agency responsible for security across the transportation domain. The *DHS Strategic Plan for Fiscal Years 2020-2024* identifies six overarching strategic goals to secure the homeland.[4] The first of the six DHS strategic goals is to "Counter terrorism and homeland security threats." This goal includes protecting special events of national significance and enhancing the overall security of soft targets and crowded places nationwide.[5] The 2019 *DHS Strategic Framework for Countering Terrorism and Targeted Violence* provides further guidance to component agencies to coordinate efforts across the department. The four goals in DHS' strategic framework for countering terrorism and targeted violence are:

Goal 1: Understand the evolving terrorism and targeted violence threat environment and support partners in the homeland security enterprise through this specialized knowledge.

Goal 2: Prevent terrorists and other hostile actors from entering the United States, and deny them the opportunity to exploit the Nation's trade, immigration, and domestic and international travel systems.

Goal 3: Prevent terrorism and targeted violence.

Goal 4: Enhance US infrastructure protections and community preparedness.

---

[4] U.S. Department of Homeland Security, "The DHS Strategic Plan Fiscal Years 2020-2024," https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf, (Accessed 25 July 2020)

[5] U.S. Department of Homeland Security, "The DHS Strategic Plan Fiscal Years 2020-2024," https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf, (Accessed 25 July 2020), Pg. 13-14

Special events of national significance under the purview of DHS include Special Event Rating Assessment (SEAR) events and National Special Security Events (NSSEs).

To support DHS's strategic goals and secure the vast transportation domain, TSA manages several security programs to assist State, Local, Tribal, and Territorial (SLTT) transportation stakeholders. However, only TSA's Visible Intermodal Prevention and Response (VIPR) program has the broad legislative mandate to leverage DHS law enforcement and security resources to augment security throughout the transportation domain.[6] *DHS Strategic Framework for Countering Terrorism and Targeted Violence* goal 2.2 specifically leverages the VIPR program as a resource to "promote confidence in and protect our Nation's transportation systems through targeted deployments of integrated TSA assets utilizing law enforcement and screening capabilities to augment [the] security of any mode of transportation."[7]

TSA's VIPR Program

TSA developed the VIPR program in 2005 to counter security vulnerabilities in the US surface transportation domain in the wake of the March 2004 Madrid train bombings.[8] *The Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act) subsequently codified the VIPR program. The 9/11 Act authorized TSA to use DHS law enforcement and security assets to augment SLTT efforts and enhance security throughout the transportation domain.[9] Today the VIPR program remains the only federal

---

[6] Find Law. "6 USC 1112 – Authorization of Visible Intermodal Prevention and Response teams" https://codes.findlaw.com/us/title-6-domestic-security/6-usc-sect-1112.html (Accessed 29 September 2020)

[7] U.S. Department of Homeland Security, "Strategic Framework for Countering Terrorism and Targeted Violence," September 2019, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf (Accessed 25 July 2020) Pg. 19-20

[8] U.S. Government Accountability Office, "Federal Air Marshal Service: Actions Taken to Fulfill Core Mission and Address Workforce Issues," 23 July 2009, https://www.gao.gov/assets/gao-09-903t.pdf, (Accessed 25 October 2020)

[9] U.S. Government Publishing Office, "Implementing Recommendations of the 9/11 Commission Act of 2007," Public Law 110–53 Sect. 1303, 3 August 2007, https://www.govinfo.gov/content/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf, (Accessed 25 October 2020)

effort dedicated explicitly to augmenting SLTT security and law enforcement efforts to promote confidence in and protect the US transportation domain.

SLTT transportation stakeholders can access a wide array of TSA and DHS law enforcement and security assets through the VIPR program. A TSA VIPR team is modular by design. It can be composed of Federal Air Marshals (FAMs), Transportation Security Officers (TSOs), Transportation Security Inspectors (TSIs), Explosive Detection Canine (EDC) Teams, and various threat detection technologies depending on the SLTT stakeholder's security needs. [10] In addition to TSA assets, VIPR teams can request support from other DHS components such as the; US Coast Guard, US Secret Service, US Customs and Border Protection, or others to support SLTT at a particular transportation venue, during a special event, or in response to specific threat information.

The TSA protects specific information regarding its security programs, including the VIPR program, as Sensitive Security Information (SSI).[11] The SSI designation precludes obtaining detailed or current VIPR program information. Publicly available information indicates that: TSA has conducted tens of thousands of VIPR operations since 2005, VIPR operations directly support National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events nationwide, VIPR teams deployed to assist in hurricane recovery in 2017, and there are numerous media stories of VIPR

[10] U.S. Transportation Security Administration. "TSA Management Directive No. 2800.13: Visible Intermodal Prevention and Response Program (VIPR)," 10 March 2017

[11] U.S. Transportation Security Administration, "Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors," *tsa.gov*, https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf (Accessed 15 February 2021)

teams conducting routine law enforcement operations in various transportation systems nationwide.[12]

An Uncertain Future for the VIPR Program

Since the VIPR program's stand-up in 2005, US Government auditors have been critical of the VIPR program's ability to develop effective metrics to measure the program's contribution to US transportation security.[13] As recently as 2018, a DHS Office of the Inspector General (DHS IG) review of the VIPR program found that "FAMS [Federal Air Marshal Service] maintains performance measures for its VIPR operations; however, these performance measures fail to determine the effectiveness of the operations."[14] Specifically, DHS IG found that VIPR program metrics were "output-based, not outcome-oriented."[15] A review of TSA Congressional Budget Justifications

---

[12] Information obtained from internet searches using the search terms "VIPR", "TSA VIPR" and "Visible Intermodal Prevention and Response"
https://www.govinfo.gov/content/pkg/CHRG-114hhrg97917/pdf/CHRG-114hhrg97917.pdf
https://www.tsa.gov/about/employee-stories/tsa-teams-secret-service-un-general-assembly
https://www.hstoday.us/subject-matter-areas/airport-aviation-security/tsa-officers-step-up-to-secure-inauguration/
https://www.securitymagazine.com/articles/94545-dhs-and-partners-coordinated-to-secure-super-bowl-lv
https://crsreports.congress.gov/product/pdf/R/R43560
https://www.tsa.gov/news/press/releases/2017/09/07/tsa-preparing-hurricane-irma

[13] U.S. Department of Homeland Security, Office of the Inspector General, "TSA's Administration and Coordination of Mass Transit Security Programs," June 2008, https://www.oig.dhs.gov/assets/Mgmt/OIG_08-66_Jun08.pdf (Accessed 3 October 2020)
U.S. Government Accountability Office, "Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities," 27 May 2010, https://www.gao.gov/assets/gao-10-435r.pdf, (Accessed 3 October 2020)
U.S. Department of Homeland Security, Office of the Inspector General, "Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)," August 2012, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf, (Accessed 25 September 2020) Pg. 58

[14] The Federal Air Marshal Service (FAMS) is the office of record within TSA that is responsible for management of the VIPR program.
U.S. Department of Homeland Security, Office of the Inspector General, "FAMS Needs to Demonstrate How Ground-based Assignments Contribute to TSA's Mission (REDACTED)," July 2018, https://www.oig.dhs.gov/sites/default/files/assets/2018-08/OIG-18-70-Jul18.pdf (Accessed 3 October 2020) Pg. 4

[15] U.S. Department of Homeland Security, Office of the Inspector General, "FAMS Needs to Demonstrate How Ground-based Assignments Contribute to TSA's Mission (REDACTED)," July 2018,

from FY 2019 to FY 2021 suggests that TSA has failed to develop outcome-oriented performance metrics that measure the VIPR program's contribution to SLTT transportation stakeholders recommend by DHS IG.[16] TSA's FY 2020 budget justification for defunding the VIPR program also confirms that it is considered redundant to current SLTT law enforcement and security efforts.[17] In the author's experience, working with and alongside the VIPR program for over 12 years, the focus on quantity over quality led TSA to focus almost exclusively on VIPR operations as a force multiplier and random deterrent to mitigate risk in the transportation domain. TSA's strategy of deploying VIPR assets to augment routine law enforcement patrols fails to leverage the VIPR program's unique legal authority, access to federal resources, and its embedded capability to deploy personnel and resources in support of SLTT security efforts.

Re-Investing in the VIPR Program

The VIPR program's mission is to "promote confidence in and protect our nation's transportation systems through targeted deployment of integrated assets utilizing screening and law enforcement in coordinated activities to augment and enhance security."[18] The VIPR program's broad legislative mandate to augment SLTT security

---

https://www.oig.dhs.gov/sites/default/files/assets/2018-08/OIG-18-70-Jul18.pdf, (Accessed 3 October 2020) Pg. 3

[16] U.S. Department of Homeland Security, DHS.gov, Search of DHS component budget justifications, https://search.usa.gov/search?utf8=%E2%9C%93&affiliate=dhs&dc=&channel=&query=Congressional+Budget+Justification&search-type=dhs&commit=Search (Accessed 15 February 2021)

[17] U.S. Department of Homeland Security, "Transportation Security Administration Budget Overview: Fiscal Year 2021 Congressional Justification," https://www.dhs.gov/sites/default/files/publications/transportation_security_administration.pdf (Accessed 15 February 2021) Pg. 38

[18] U.S. Transportation Security Administration. TSA Management Directive No. 2800.13: Visible Intermodal Prevention and Response Program (VIPR), 10 March 2017

throughout the transportation domain is the only fully-funded program of its kind in the Federal government.[19] Congress has remained committed to the VIPR program and has ensured that it remains fully funded despite attempts to scale back and defund the program in recent years.[20] Assuming the VIPR program will remain fully funded, the program must provide services to SLTT transportation security stakeholders that augment transportation security and do not duplicate SLTT security efforts.

This thesis will not attempt to re-invent the VIPR program, develop metrics to measure its performance, or propose incompatible missions with the program's transportation security mission. This thesis evaluates potential mission sets selected from TSA's *2020 Biennial National Strategy for Transportation Security Report to Congress* that lend themselves to the VIPR program's unique legal authorities, ability to enable SLTT, and capabilities to augment SLTT transportation security efforts. Subsequent discussions will explore violent extremist use of Unmanned Aircraft Systems (UAS), Improvised Explosive Devices (IEDs), and Lone-Offender tactics to conduct attacks in the transportation domain where the author believes the VIPR program can supplement SLTT security efforts in all modes of transportation.

---

[19] Find Law. "6 USC 1112 – Authorization of Visible Intermodal Prevention and Response teams" https://codes.findlaw.com/us/title-6-domestic-security/6-usc-sect-1112.html (Accessed 29 September 2020)

[20] Information obtained from internet searches using the search terms "VIPR defunding", "VIPR funding" and "Visible Intermodal Prevention and Response team funding"
https://appropriations.house.gov/news/press-releases/appropriations-committee-releases-fiscal-year-2021-homeland-security-funding
https://appropriations.house.gov/news/statements/chairwoman-roybal-allard-statement-at-hearing-on-fy-2020-tsa-budget-request
https://fas.org/sgp/crs/homesec/R45500.pdf Pg. 16
https://www.hsgac.senate.gov/imo/media/doc/REPORT-Overruled-White-House-Overrules-DHS-Budget-Request-for-Counterrorism-Programs.pdf

Chapter two introduces a relatively new and evolving threat vector, UAS technology. Since the beginning of the Global War on Terror, the US military has used advanced UAS technology to collect intelligence and strike extremist targets.[21] In the past decade, UAS technology has become widely available to the civilian market.[22] In chapter two, UAS incident summaries highlight the evolving UAS threat and the potential nefarious use of UAS technology in the transportation domain. The discussion will include a review of UAS and Counter UAS (C-UAS) technology and the applicable laws governing UAS technology in the US.

Chapter three reviews the continued IED threat to the transportation domain. IEDs used by violent extremists come in many forms, from small pipe bombs and suicide belts to sophisticated devices capable of massive damage to infrastructure and loss of life.[23] The case studies in chapter three underscore the continued threat of IEDs in the transportation domain. They demonstrate the effectiveness of IED attacks in the transportation domain, violent extremists' ability to construct devices undetected, and how violent extremists adapt to overcome mitigation efforts in the transportation domain. The discussion will focus on using TSA EDC teams in the transportation domain to detect, deter, and defeat IED threats in real-time.

---

[21] Fred Kaplan. The Slate Group. "The First Drone Strike" https://slate.com/news-and-politics/2016/09/a-history-of-the-armed-drone.html (Accessed 9 December 2020)

[22] Divya Joshi. Business Insider. "Here are the world's largest drone companies and manufacturers to watch and stocks to invest in 2020" https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks (Accessed 28 November 2020); SuccessStory.com "DJI – Revolutionizing Technology" https://successstory.com/companies/dji (Accessed 28 November 2020)

[23] U.S. Department of Homeland Security. "IED Attack – Improvised Explosive Devices" https://www.dhs.gov/sites/default/files/publications/prep_ied_fact_sheet.pdf (Accessed 14 November 2020)

Chapter four explores the rise of the lone-offender violent extremist threat in the transportation domain.[24] The FBI's *Lone-Offender Terrorism Report* broadly included lone-offender violent extremists who "may have affiliated or associated with a terrorist organization/ideological movement or may have received assistance from others at some stage during the planning or implementation of their attacks, [however] they must have been both the primary architect and the primary actor in the attack action."[25] The case studies in chapter four highlight the unpredictable nature of lone-offenders, the legal challenges to mitigating lone-offender attacks, and the role law enforcement plays in defeating lone-offenders activities. The discussion will focus on using the VIPR program to augment SLTT security during nationally recognized special events and periods of heightened alert within the transportation domain.

Chapter five's policy recommendations will leverage the VIPR program's unique legal authorities, ability to enable SLTT, and capability to augment SLTT transportation security efforts to respond to the three threat vectors proposed in this thesis. The recommendations will limit program redundancies and support, not duplicate SLTT law enforcement and security efforts in the transportation domain. Finally, the recommendations will align with the 2019 *DHS Strategic Framework for Countering Terrorism and Targeted Violence* to ensure a consistent federal effort throughout the US transportation domain.

---

[24] James Blalock. Patrick Henry College. The Intelligencer. Lone Wolf Terrorism: Leaderless Resistance" https://www.phc.edu/intelligencer/lone-wolf (Accessed 8 December 2020)

[25] Lauren Richards et al., "Lone Offender – A Study of Lone Offender Terrorism in the United States (1972-2015)" *National Center for the Analysis of Violent Crime* (November 2019): 10

Chapter 2: Unmanned Aircraft Systems

Unmanned Aircraft Systems meet the Transportation Domain

Since the beginning of the Global War on Terror, the US military has used Unmanned Aircraft Systems (UAS) technology to collect intelligence and strike extremist targets.[1] In 2006, the largest distributor of civilian UAS technology began retail sales of an easy-to-pilot UAS directly to the general public.[2] Since its commercial introduction, UAS technology has proliferated worldwide and fallen into the hands of violent extremists. In 2016 the Combating Terrorism Center at West Point developed a typology depicting extremist UAS technology use. The typology suggests that violent extremists are increasingly interested in developing UAS technology to conduct surveillance, communicate, transport illicit material, disrupt government activities, and deliver improvised explosive devices or other military payloads.[3] TSA's *2020 Biennial National Strategy for Transportation Security Report to Congress* highlights UAS technology as an emerging and unpredictable threat vector impacting the US transportation domain.[4]

As UAS technology continues to evolve, yielding systems capable of carrying larger payloads and accomplishing more complex missions, the potential threat to US

---

[1] Fred Kaplan. The Slate Group. "The First Drone Strike" https://slate.com/news-and-politics/2016/09/a-history-of-the-armed-drone.html (Accessed 9 December 2020)

[2] Business Insider. "Here are the world's largest drone companies and manufacturers to watch and stocks to invest in 2020" https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks (Accessed November 28, 2020); SuccessStory.com "DJI – Revolutionizing Technology" https://successstory.com/companies/dji (Accessed 28 November 2020)

[3] Don Rassler, "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology," *Combatting Terrorism Center at West Point*, October 2016: 12, https://ctc.usma.edu/wp-content/uploads/2016/10/Drones-Report.pdf

[4] U.S. Transportation Security Administration, "2020 Biennial National Strategy for Transportation Security Report to Congress," 29 May 2020, https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf (Accessed 25 October 2020) Pg. 6

critical infrastructure increases.[5] This chapter's research included a review of applicable laws governing UAS technology, UAS technology from both an UAS operator and Counter UAS (C-UAS) perspective, and the potential threat to transportation posed by UAS technology. C-UAS is an emerging field in domestic transportation security. As such, the literature reviewed for this chapter relied on primary sources and media reporting of UAS incidents within the past five years. The summaries of select UAS incidents will highlight the advantages of leveraging the VIPR program's unique legal authorities, ability to enable SLTT, and capability to augment SLTT transportation security efforts in C-UAS operations across the transportation domain. Combining TSA's VIPR program with a sound C-UAS strategy to protect the transportation domain is vital to National security.[6]

VIPR Legal Authorities – McCarran International Airport Incident – 2018

In June 2018, a UAS operator lost control of a UAS while shooting a video over the Las Vegas Strip. The UAS, a DJI Phantom 3, drifted for more than 2 miles at an altitude of 450 feet before landing between runways at McCarran International Airport (LAS).[7] The DJI Phantom 3 UAS has a maximum service ceiling of 6000 meters, a speed of 16 meters/second, a flight time of 25 minutes, and is available to the public for $500 - $800.[8] Authorities tracked down the operator by tracing the FAA registration number of

[5] Angela H. Stubblefield, "Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks," U.S. Department of Transportation, 18 June 2019, https://www.transportation.gov/testimony/drone-security-enhancing-innovation-and-mitigating-supply-chain-risks, (Accessed 28 November 2020)

[6] U.S. President. National Security Strategy of the United States of America, by the White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf Washington, DC: Government Publishing Office, December 2017. Pg. 10

[7] Isabella Lee, "Drone Pilot Fined $20,000 For Landing Drone at McCarran Airport, Las Vegas," *UAVCoach.com*, 3 December 2019, https://uavcoach.com/drone-pilot-fines/

[8] "Phantom 3 Standard Specs" DJI Phantom 3, (Accessed 28 November 2020) https://www.dji.com/phantom-3-standard/info?redirect_info=true#camera

the UAS.[9] The operator reported that he lost control of the UAV, and it accidentally drifted over the airport and landed in the secure runway area at LAS. This incident highlights the legal challenges inherent in preventing a UAS from operating in the controlled airspace of a major US airport when only passive UAS measures are available to prevent an intrusion.

United States Code defines Unmanned Aircraft Systems as: "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system."[10] Because the law classifies UAS technology as an aircraft, it receives the same legal protections as crewed civil aircraft. Shooting down or otherwise interfering with a civil aircraft's safe operation is punishable under 18 USC 32, *Destruction of aircraft or aircraft facilities*.[11] With this legal restriction in place, law enforcement efforts to mitigate UAS activities are focused on locating the operator of the UAS to direct the individual to land or remove the UAS from protected air space.[12]

The Federal Aviation Administration (FAA) regulates all airspace in the United States. The FAA typically issues Notices to Airmen (NOTAMs) to inform pilots of changes to the National Air Space (NAS). NOTAMs are issued to establish restricted

---

[9] Isabella Lee, "Drone Pilot Fined $20,000 For Landing Drone at McCarran Airport, Las Vegas," *UAVCoach.com*, December 3 2019, https://uavcoach.com/drone-pilot-fines/

[10] Cornell Law School, "Unmanned Aircraft Systems, Definitions, 49 USC 44801," https://www.law.cornell.edu/uscode/text/49/44801, (Accessed 28 November 2020)

[11] Cornell Law School, "Destruction of aircraft or aircraft facilities. 18 USC 32," https://www.law.cornell.edu/uscode/text/18/32, (Accessed 28 November 2020)

[12] Federal Aviation Administration, "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," August 2020, https://www.faa.gov/uas/resources/c_uas/media/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf, (Accessed 28 November 2020)

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Protecting Against the Threat of Unmanned Aircraft Systems (UAS)," November 2020, https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf, (Accessed 28 November 2020)

airspace around critical infrastructure or for special events.[13] Unfortunately, amateur UAS operators do not routinely check NOTAMs and are unaware when a flight restriction is in effect. As part of the FAA Modernization and Reform Act of 2012, Congress directed the FAA to develop a plan to integrate UAS technology into the regulated national airspace system safely.[14] Since 2012 the FAA has introduced several regulations governing the safe operation of UAS technology in US airspace. Registration of UAVs became mandatory in 2016 to encourage greater responsibility and awareness of UAS operators.[15] The UAS incident at LAS demonstrates how registration can identify a UAS operator. However, registration alone did not prevent the UAV from entering a major airport's restricted airspace or alert officials to the UAV's presence.[16] During the LAS UAS incident, these passive mitigation efforts could not have prevented the UAS intrusion. Fortunately, this was a benign incident, and investigators were able to identify the UAS operator.

In October 2018, Congress passed the *Preventing Emerging Threats Act of 2018*, granting DHS the authority to develop and employ active mitigation technology to counter UAS threats. The Act exempts DHS from several laws to enable C-UAS activities that are otherwise prohibited in the US. In specific circumstances, DHS law

---

[13] Federal Aviation Administration, "Notices to Airmen (NOTAMs) Back to Basics," https://www.faa.gov/about/initiatives/notam/what_is_a_notam/ (Accessed 27 March 2021)

[14] Cornell Law School, "FAA Modernization and Reform Act of 2012. 49 U.S.C. 44802," https://www.law.cornell.edu/uscode/text/49/44802 (Accessed 28 November 2020)

[15] Federal Aviation Administration, "The FAA's New Drone Rules Are Effective Today," 29 August 2016, https://www.faa.gov/news/updates/?newsId=86305, (Accessed 28 November 2020)

[16] TSA classifies the Nation's airports into one of five security categories (X, I, II, III, and IV) based on factors such as the number of takeoffs and landings annually, annual passenger volume, security program requirements, and other security considerations. Category X airports have the largest number of passenger boarding's and Category IV airports have the smallest.

Charlotte Gill, "TSA's Security Playbook," *George Mason University*, http://cebcp.org/wp-content/publications/PhaseII-Final-Report-Redacted.pdf, (Accessed 28 November 2020) Pg. 52

enforcement officers may conduct C-UAS activities to detect, monitor and, track UAS technology, disrupt control of the UAS, seize control of the UAS, and if necessary, use reasonable force to disable, damage, or destroy the UAS.[17] It is important to note that the authorities granted under the *Preventing Emerging Threats Act of 2018* to intercept UAS technology are limited to the DHS, the Departments of Justice, Energy, and Defense and do not extend to SLTT security or law enforcement officers. DHS proposes to use C-UAS technology in a specific timeframe at select locations within designated public spaces or other covered assets to mitigate UAS threats.[18] With this new authority, the VIPR program is the only DHS effort with the broad legal authority to deploy FAMs and utilize cutting-edge technology throughout the transportation domain to electronically or kinetically intercept UAS technology.

Enabling SLTT – Gatwick Airport UAS Incident – 2018

London Gatwick Airport (LGW) in West Sussex, UK, was the first major airport to shut down for an extended period due to UAS technology. The shutdown disrupted hundreds of flights, thousands of passengers and cost the airlines approximately 50 million GBP.[19] For three days in December 2018, officials received 115 credible reports of UAS in controlled airspace around LGW.[20] UAS sightings near Gatwick airport

---

[17] U.S. Government Publishing Office, "FAA Reauthorization Act of 2018," Public Law 115–254, 5 October 2018, https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf, (Accessed 25 October 2020)

[18] U.S. Department of Homeland Security, "Privacy Impact Assessment for the Counter-Unmanned Aircraft Systems (C-UAS)," 15 July 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall085-c-uas-august2020_updated.pdf, (Accessed 15 February 2021) Pg. 4

[19] Samira Shackle, "The mystery of the Gatwick drone," *The Guardian*, 1 December 2020, https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

[20] SkyNews Editors, "Gatwick drone inquiry: 93 'credible sightings'," *SkyNews.com*, 29 December 2018, https://news.sky.com/story/some-gatwick-drone-sightings-may-have-been-police-drones-chief-constable-says-11593854

reinforced fears of extremist attacks via this new threat vector. LGW had conducted a site survey and identified potential UAS launch sites before the 2018 incident.[21] Although airport operators erred on the side of caution, shutting down flight operations ten times for 33 cumulative hours, the airport's C-UAS plan allowed police to respond to the most likely UAS launch sites quickly, possibly disrupting the UAS operator. The 18 month-long police investigation ultimately yielded no credible suspects.[22] Following the three-day UAS incident, LGW invested "millions of pounds" in undisclosed counter UAS technology.[23] This UAS incident highlights the importance of conducting C-UAS assessments of transportation venues and developing robust C-UAS action plans to counter UAS threats.

In 2020 the US Cybersecurity and Infrastructure Security Agency published a C-UAS best practices guide titled *Protecting Against the Threat of Unmanned Aircraft Systems (UAS)*. The guide shares C-UAS best practices across the government and encourages vulnerable facilities to consider the UAS threat as part of overall security planning. The UAS specific vulnerability assessment outlined in the guide assists SLTT transportation stakeholders in determining how a venue may be vulnerable to UAS threats and help develop a comprehensive C-UAS action plan.[24] The guide recognizes

---

[21] Michael Huerta, "Blue Ribbon Task Force on UAS Mitigation at Airports: Final Report," *The Moak Group*, October 2019, https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf, Pg. 39 (Accessed 10 December 2020)

[22] Samira Shackle, "The mystery of the Gatwick drone," *The Guardian*, 1 December 2020, https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

[23] Kanishka Singh, "Gatwick, Heathrow airports order military-grade anti-drone equipment," *Reuters*, 3 January 2019, https://www.reuters.com/article/us-britain-drones-gatwick-idUSKCN1OX1KX

[24] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Protecting Against the Threat of Unmanned Aircraft Systems (UAS)," November 2020, https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf, (Accessed 28 November 2020) Pg. 9-22

that SLTT, Private, and most Federal entities do not have the legal authority to electronically or kinetically intercept UAS technology. However, the guide reiterates that a comprehensive C-UAS action plan can substantially mitigate risk to protected facilities.

The 2018 UAS incident at LGW prompted the National Security Council to develop the *Unified National-Level Response to Persistent UAS Disruption of Operations at Core 30 Airports,* a federal concept of operations (CONOPS) to coordinate US C-UAS activities.[25] The CONOPS named TSA as the Lead Federal Agency (LFA) for incident response in the event of a persistent UAS disruption of the national airspace.[26] As demonstrated by the LGW incident, a comprehensive C-UAS action plan can reduce the threat and impact of a UAS incident. The responsibility of assisting airports with security assessments would generally fall on TSA's Joint Vulnerability Assessment (JVA) program.[27] Adding C-UAS assessments to the JVA program's duties, however, may not be feasible. A 2016 GAO audit found that the JVA program conducted only 11 assessments per year.[28] This rate would be too slow to assess the nearly 440 federalized airports and thousands of surface transportation facilities nationwide. However, the VIPR program is currently fully funded and regarded as redundant in its current role. Realigning the VIPR program to enable SLTT C-UAS efforts through coordination,

---

[25] Cal Biesecker, "Plan for TSA to Lead Federal Counter Drone Operations at Airports 'Unlawful,' Hill Aide Says" *Defense Daily*, 17 December 2019, https://www.defensedaily.com/plan-tsa-lead-federal-counter-drone-operations-airports-unlawful-hill-aide-says-2/unmanned-systems/ (Accessed on 28 November 2020)

[26] U.S. Department of Homeland Security, "Privacy Impact Assessment for the Counter-Unmanned Aircraft Systems (C-UAS)," 15 July 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall085-c-uas-august2020_updated.pdf, (Accessed 15 February 2021) Pg. 19

[27] Cornell Law School, "Domestic air transportation system security 49 U.S. Code § 44904," https://www.law.cornell.edu/uscode/text/49/44904, (Accessed 28 November 2020)

[28] U.S. Government Accountability Office, "Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates," May 2016, https://www.gao.gov/assets/gao-16-632.pdf, (Accessed 28 November 2020) Pg. 24

training, and assessment helps leverage an underutilized program to enhance the security of the transportation domain and fulfill one of TSA's strategic goals.[29]

Augmenting SLTT Capabilities – Abha International Airport – 2021

In February 2021, Yemeni rebels launched a UAS strike against Abha International Airport (AHB) in Saudi Arabia.[30] Officials reported that a civilian aircraft caught fire during the attack. Photos obtained by the Associated Press show a hole in the side of a civilian aircraft resulting from a UAS vehicle penetrating the airframe. The UAS vehicles used in the attack are reported to be Iranian inspired Samad-3 and Qasef-2K military drones.[31] The Qasef-2K UAS is manufactured by Yemini rebels using a design similar to the Iranian Ababil-T combat drone. The Ababil-T combat drone is reported to carry a 40Kg warhead a distance of 120km using a semi-autonomous GPS guidance system.[32] Additional media reporting indicates that ABH has been attacked several times by rebel drone strikes in recent years. Although there were no injuries reported during this attack, two drone attacks in June and July 2019 injured 26 and 9 people respectively at the airport.[33] In recent months the Saudi military has utilized its air force to intercept

---

[29] U.S. Transportation Security Administration, "TSA Strategy 2018-2026," https://www.tsa.gov/sites/default/files/tsa_strategy.pdf, (Accessed 1 October 2020) Pg. 8 Goals 1.2, 1.4, and 1.5

[30] Reuters Staff, "Yemen's Houthis say they carried out drone attack on Saudi airport," *Reuters,* 10 February 2021, https://www.reuters.com/article/us-yemen-security-saudi-airport/yemens-houthis-say-they-carried-out-drone-attack-on-saudi-airport-idUSKBN2AA1IG

Isable Debre, "Saudi TV: Yemen rebel attack on airport sets plane on fire," *AP News*, 10 February 2021, https://apnews.com/article/middle-east-yemen-dubai-saudi-arabia-united-arab-emirates-a351ca2f95c68ebf08c385742deef2ac

[31] Thomas Newdick, "Yemen's Houthi Rebels Strike Airliner In New Drone Attack On Saudi Airport," *The Drive.com,* 10 February 2021, https://www.thedrive.com/the-war-zone/39186/yemens-houthi-rebels-strike-airliner-in-new-drone-attack-on-saudi-airport

[32] Martin Streetly, ed., *Jane's All the World's Aircraft: Unmanned 2014–2015* (London: IHS Jane's, 2014), 79-80.

[33] Chandler Thornton, "Rebels launch drone attack on Saudi airport, injuring 9," *CNN.com,* 2 July 2019, https://www.cnn.com/2019/07/02/middleeast/saudi-abha-airport-drone-attack-intl

drone attacks and trained with the US military as part of its ongoing C-UAS efforts.[34] This recent UAS incident highlights the shortcoming of legal and administrative means to prevent a determined attacker from successfully carrying out a UAS attack. Stopping a persistent UAS attack requires the development and deployment of specialized C-UAS technology.

Current C-UAS technology focuses on electronic manipulation of the UAS control datalink and kinetic action to damage or destroy the Unmanned Aircraft Vehicle (UAV).[35] Electronic methods of manipulating the UAS control datalink are currently the most reliable way to actively protect controlled airspace from UAS intrusion.[36] Electronic manipulation interrupts the UAS operator's control of the UAV and can provide an opportunity for law enforcement officials to seize control of the UAV in flight. The development of kinetic C-UAS technology for use in US airspace is in its infancy. Kinetic C-UAS technology uses a projectile or high-energy beam to damage or destroy the UAV. Currently, neither system is 100% effective for use in the US airspace. Electronic systems may be ineffective against some UAS technology or may inadvertently damage other systems. While kinetic solutions may create unacceptable

---

[34] Joseph Trevithick, "Watch A Saudi F-15 Fighter Swoop In Low To Blast A Houthi Rebel Drone Out Of The Sky," *The Drive.com*, 30 March 2021, https://www.thedrive.com/the-war-zone/39992/watch-a-saudi-f-15-fighter-swoop-in-low-to-blast-a-houthi-rebel-drone-out-of-the-sky

Arab News Staff, "Saudi, US air forces train to down enemy drones," *Arab News*, 10 February 2021, https://www.arabnews.com/node/1806671/saudi-arabia

[35] U.S. Department of Homeland Security, "Counter-Unmanned Aircraft Systems Technology Guide," September 2019, https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf, (Accessed 1 October 2020) Pg. 22

[36] Georgia Lykou, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors*, June 22, 2020: 14-15, https://www.semanticscholar.org/paper/Defending-Airports-from-UAS%3A-A-Survey-on-and-Lykou-Moustakas/cdccb4ad90f9155c3d62d00d071f5331d4ac29ea

collateral damage when a kinetic projectile strikes an unintended target, or a damaged UAV falls to the ground.

The US military has developed reliable capabilities to conduct C-UAS operations in combat conditions.[37] Although many C-UAS solutions are available most are designed for battlefield conditions and are not viable options for US airspace above urban areas.[38] Since 2016, the DHS Science and Technology Directorate (DHS S&T) has worked with Federal and SLTT stakeholders to develop and test C-UAS technology that is compatible with the legal and technical constraints inherent in US airspace.[39] DHS S&T routinely partners with SLTT stakeholders to test and evaluate new technologies. However, as noted in the LAS incident, SLTT stakeholders do not have the legal authority to operate C-UAS systems independently. Complicating matters is that DHS's authority to use C-UAS technology in the US is limited to specific locations to defend against a persistent UAS threat for a finite amount of time.[40] To overcome these challenges, DHS must invest in resources to provide the full range of C-UAS activities throughout the transportation domain. The VIPR program has both the legal authority to augment law enforcement resources throughout the transportation domain and conduct C-UAS operations to support SLTT transportation stakeholders as directed by the DHS Secretary.

---

[37] Courtney Kube, "New law would give federal government the right to shoot down private drones inside U.S.," *NBCNews.com*, 24 September 2019, https://www.nbcnews.com/politics/national-security/new-law-would-give-federal-government-right-shoot-down-private-n912381

[38] Seibler Snead, "Establishing a Legal Framework for Counter-Drone Technologies," *The Heritage Foundation,* 16 April 2018, 5. https://www.heritage.org/sites/default/files/2018-04/BG3305_1.pdf

[39] Department of Homeland Security, "Snapshot: Countering Unmanned Aerial Systems in Urban Environments," Science and Technology, May 11, 2018, https://www.dhs.gov/science-and-technology/news/2018/05/11/snapshot-c-uas-urban-environments.

[40] U.S. Government Publishing Office, "FAA Reauthorization Act of 2018," Public Law 115–254, 5 October 2018, https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf, (Accessed 25 October 2020)

Summary – VIPR Capability Enhances DHS C-UAS Efforts

UAS technology is an emerging threat vector in the US transportation domain. Securing the transportation domain against this threat is a daunting challenge. The UAS incidents summarized in this chapter highlight how easily UAS technology can exploit security vulnerabilities in the Nation's transportation domain. Since 2018 DHS, in coordination with its' Federal and SLTT partners, has made strides to mitigate malign use of UAS technology in the United States. However, a 2020 DHS OIG report found that DHS did not expand the C-UAS mission across all affected components to sufficiently mitigate UAS risk.[41] With nearly 440 federalized airports, 4 million miles of roadways, 140,000 miles of railroad track, and 360 maritime ports to protect, DHS must leverage its full capabilities in new and innovative ways to defend the homeland.

TSA's VIPR program will enhance DHS C-UAS posture throughout the transportation domain. VIPR's inherent legal authorities allow it to operate in all modes of transportation throughout the United States. The *Preventing Emerging Threats Act of 2018* granted C-UAS authorities to DHS. If designated, FAMs, the VIPR programs federal law enforcement officers, can leverage the law's full authority to conduct C-UAS missions to support national security goals. As legitimate UAS use increases, benign UAS intrusion into controlled airspace is anticipated to grow as well.[42] While the FAA will regulate the national airspace and educate UAS operators, DHS will remain

---

[41] Courtney Kube, "New law would give federal government the right to shoot down private drones inside U.S.," *NBCNews.com*, 24 September 2019, https://www.nbcnews.com/politics/national-security/new-law-would-give-federal-government-right-shoot-down-private-n912381

[42] Federal Aviation Administration, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap," Second Edition, July 2018, https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf Pg. 28-29

responsible for hardening vital infrastructure against UAS threats. The Transportation Security Inspectors (TSI) assigned to the VIPR program have regulatory authority to enforce security regulations and to enable SLTT stakeholders to improve security in the transportation domain. TSI's can assist SLTT transportation stakeholders in assessing site vulnerabilities and developing comprehensive C-UAS action plans. The VIPR program's greatest strength is its ability to form coalitions and coordinate joint Federal-SLTT efforts throughout the transportation domain. In partnership with DHS S&T, the VIPR program can deploy proven C-UAS technology anywhere in the transportation domain to augment SLTT response capability. During persistent UAS incidents, VIPR personnel can leverage relationships across SLTT jurisdictional boundaries to coordinate effective responses.

As DHS works to safeguard the homeland from UAS threats, the department must utilize all available resources to counter emerging threats. It is recommended that DHS delegate C-UAS responsibilities to the VIPR program to enhance the traveling public's safety and security in all modes of transportation.

Chapter 3: Improvised Explosive Devices

Explosive Detection Canines, Protectors of the Transportation Domain

To ensure the free and rapid flow of commuters' transportation hubs have multiple access points, serve various modes of transportation, and concentrate travelers in relatively confined areas.[1] While these features help make the transportation domain convenient for travelers and commuters, they also make transportation a desirable target for violent extremist attacks. TSA's *2020 Biennial National Strategy for Transportation Security* highlights Improvised Explosive Devices (IEDs) as a persistent threat across all modes of transportation.[2] An IED is a "homemade" bomb composed of commonly available materials to create an explosive effect. The United Nations defines an IED as, "a device placed or fabricated in an improvised manner incorporating explosive material, destructive, lethal, noxious, incendiary, pyrotechnic materials or chemicals designed to destroy, disfigure, distract or harass" which "may incorporate military stores, but are normally devised from non-military components."[3] Constructed from commonly available materials, IEDs can come in many forms, ranging from small pipe bombs to sophisticated vehicle-borne devices capable of causing massive damage and loss of life.[4]

The use of Explosive Detection Canine (EDC) teams to reliably detect explosives in a wide range of environments is well established in the law enforcement and security

---

[1] U.S. Government Accountability Office, "Surface Transportation: DHS Is Developing and Testing Security Technologies, but Could Better Share Test Results," September 2019, https://www.gao.gov/assets/gao-19-636.pdf (Accessed 25 October 2020) Pg. 1

[2] U.S. Transportation Security Administration, "2020 Biennial National Strategy for Transportation Security Report to Congress," 29 May 2020, https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf (Accessed 25 October 2020)

[3] United Nations, "Office of Disarmament Affairs, Production and delivery [of IEDs]," https://www.un.org/disarmament/convarms/production/, (Accessed 14 November 2020)

[4] U.S. Department of Homeland Security. "IED Attack – Improvised Explosive Devices" https://www.dhs.gov/sites/default/files/publications/prep_ied_fact_sheet.pdf (Accessed 14 November 2020)

communities.[5] Canines are known for their keen sense of smell and can quickly alert to explosive odors. As violent extremists continue to improve and adapt their IEDs to defeat mitigation efforts and detection technologies, it is imperative that TSA fully leverage its resources to protect the traveling public across all modes of transportation.[6] This chapter's research is limited to the effective deployment of EDC teams in the transportation domain. While other explosive detection technologies exist, to date, none are proven to be more versatile or effective than a trained EDC team.[7] The research for this chapter includes a review of applicable laws governing EDC teams' deployment and the potential threat to transportation posed by IEDs. Information regarding EDC training and capability is generally restricted in domestic transportation security. Law enforcement and security organizations are hesitant to publish information that may demonstrate weaknesses in their EDC programs. At the same time, researchers view their work as proprietary and for sale to the law enforcement and security community. As such, literature reviewed for this chapter relies on primary sources and media reporting of IED incidents within the transportation domain. The summaries of select IED incidents will highlight the advantages of leveraging the VIPR program's unique legal authorities, ability to enable SLTT, and capability to augment SLTT transportation security efforts in EDC missions across the transportation domain. Combining the broad authority and

[5] Jehuda Yinon, ed., *Counterterrorist Detection Techniques of Explosives* (Oxford: Elsevier Science & Technology, 2007), 397-398

[6] U.S. Department of Homeland Security. Science and Technology. "Snapshot: Testing Locations for Homemade Explosives Keep the Traveling Public Safe" https://www.dhs.gov/science-and-technology/news/2018/10/02/snapshot-testing-homemade-explosives-keep-travelers-safe (Accessed 14 November 2020)

[7] Haley Cohen Gilliland, "Why explosives detectors still can't beat a dogs nose," *MIT Technology Review*, 24 October 2019, https://www.technologyreview.com/2019/10/24/132201/explosives-detectors-dogs-nose-sensors/ (Accessed 15 February 2021)

capabilities of TSA's VIPR program with a sound EDC deployment strategy is vital to protecting the transportation domain.

VIPR Legal Authorities – Madrid Train Attacks - 2004

In March 2004, a violent extremist group detonated ten IEDs concealed in backpacks aboard four commuter trains during the morning rush hour in Madrid, Spain. The attack killed 193 people and injured nearly 2,000 commuters, making this incident Spain's deadliest terror attack.[8] The extremists made the IEDs with commercial explosives and packed metal fragments around the explosive to increase the devices' lethality. To synchronize the attack, the extremists used cell phones wired to detonate the IEDs at a preset time.[9] The Madrid attack shifted US attention toward surface transportation security and prompted TSA to develop the VIPR program. In an open and free society, this incident prompts discussion of the legal implications of balancing security with individual freedom in a large and open public transportation system.

The Fourth Amendment of the United States Bill of Rights protects US residents from unreasonable searches and seizures by the government without a judicially issued warrant supported by probable cause. However, the Supreme Court has ruled that legitimate government interests, such as public safety, may create exemptions to the Fourth Amendment protections.[10] Note, the following is a general summary of case law as it applies to EDC teams in the transportation domain and is not legal guidance or

---

[8] History.com Editors, "Terrorists bomb trains in Madrid," 10 March 2020, https://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid, (Accessed 25 October 2020)

[9] U.S. Department of Homeland Security, "Factsheet: News &Terrorism, Communicating in a crisis, IED Attack Improvised Explosive Devices," https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, (Accessed 14 November 2020)

[10] U.S. Courts.gov, "What Does the Fourth Amendment Mean?" https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (Accessed 15 February 2021)

advice. The use of canines has been challenged in several court cases as a violation of the Fourth Amendment.[11] The majority of the case law involves the use of narcotics detection canines in a variety of differing law enforcement situations. However, the Supreme court has generally upheld that judicious use of canines to detect scents of prohibited materials is not a violation of the Fourth Amendment. This decision is based primarily on three principles; 1) There is no expectation of privacy in the public domain, 2) Odors emitted by a prohibited material freely enter the public domain, and 3) scent detection only enables probable cause a prohibited substance is present, it does not otherwise invade the privacy of the individual. When deployed in accordance with applicable laws and policies, TSA EDC teams provide a reasonable balance between privacy and security while conducting explosive detection missions throughout the transportation domain.

The *Aviation and Transportation Security Act* (ATSA) of 2001 consolidated a broad range of federal transportation security responsibilities into the TSA.[12] Following the Madrid attack, TSA developed the VIPR to enhance security throughout the transportation domain. In 2007 the VIPR program was codified in *The Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act). The 9/11 Act specifically authorized the VIPR program to utilize TSA and DHS law enforcement and security assets to augment SLTT stakeholder security efforts throughout the transportation domain.[13] To detect and deter an IED attack in the surface transportation

---

[11] Sherry F. Colb, "Who's a Good Boy? US Supreme Court Considers Again Whether Dog Sniffs Are Searches," *Verdict.Justia.com*, 16 January 2019, https://verdict.justia.com/2019/01/16/whos-a-good-boy-us-supreme-court-considers-again-whether-dog-sniffs-are-searches, (Accessed 15 February 2021)

[12] U.S. Transportation Security Administration. "Aviation and Transportation Security Act of 2001" https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf (Accessed on 24 October 2020)

[13] U.S. Government Publishing Office, "Implementing Recommendations of the 9/11 Commission Act of 2007," Public Law 110–53 Sect. 1303, 3 August 2007,

domain, EDC teams were specifically included in the 9/11 Act as assets available to the VIPR program to counter IED threats.

Enabling SLTT – Boston Marathon Bombing – 2013

In April 2013, two improvised explosive devices detonated near the Boston Marathon's finish line, killing three bystanders and wounding over 260 others. The attackers detonated two pressure-cooker bombs loaded with shrapnel and concealed in backpacks near the marathon's finish line.[14] Instructions to build a pressure cooker bomb are readily available online in *Inspire* magazine, a violent extremist publication that promotes attacks against western nations.[15] Personnel from across the government, including VIPR teams, assisted the FBI with their investigation. Within days the suspects in the incident were identified, apprehended and charged with the use of a weapon of mass destruction and malicious destruction of property resulting in death.[16] This incident highlights the importance of building enabling relationships and partnerships across all levels of government prior to an IED incident to ensure a coordinated response and rapid recovery.

The DHS after-action summary of the Boston Marathon bombings highlighted the importance of the Federal-SLTT partnerships prior to and following the attack.[17] Leading

---

https://www.govinfo.gov/content/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf, (Accessed 25 October 2020)

[14] History.com Editors, "Boston Marathon Bombing," 7 June 2019, https://www.history.com/topics/21st-century/boston-marathon-bombings#section_2, (Accessed 25 October 2020)

[15] U.S. District Court, District of Massachusetts, "Charging Affidavit: U.S. vs Dzhokhar A. Tsarnaev", 27 June 2013, https://www.justice.gov/iso/opa/resources/6320136271620385133 70.pdf (Accessed 13 March 2021)

[16] U.S. District Court, District of Massachusetts, "Charging Affidavit: U.S. vs Dzhokhar A. Tsarnaev", 27 June 2013, https://www.justice.gov/iso/opa/resources/6320136271620385133 70.pdf (Accessed 13 March 2021)

[17] Mike Levine, "Boston One Year Later: DHS's Lessons Learned," *ABC News Online*, 10 April 2014, https://abcnews.go.com/images/Blotter/DHS%20After%20Action%20Review%20-%20FINAL.PDF, (Accessed 13 March 2021) Pg. 6

up to the marathon, DHS representatives from the Federal Emergency Management Agency (FEMA) and Federal Protective Service (FPS), and the FBI's Joint Terrorism Task Force (JTTF) participated in Boston Marathon Security Coordination meetings with their SLTT counterparts. The coordination meetings allowed all parties to have a common operating picture and an understanding of response duties and capabilities in an incident. Leveraging pre-existing relationships with SLTT stakeholders across the Northeast, VIPR teams quickly increased deployments by approximately 90% to maintain the security of the transportation domain.[18] VIPR's quick response enabled SLTT law enforcement stakeholders to focus on post-incident response and recovery.

To counter IED threats to the transportation domain, TSA manages the National Explosive Detection Canine Team Program (NEDCTP). NEDCTP is the largest EDC program in DHS, and the second largest in the federal government.[19] The NEDCTP oversees two parallel EDC training pipelines to support IED detection in the transportation domain. The first pipeline trains TSA Transportation Security Inspectors (TSI) handlers to work with EDCs at the nation's busiest airports and support the VIPR program. The second pipeline trains SLTT law enforcement (LE) stakeholders to work with EDCs with the understanding that the SLTT LE teams will spend approximately

---

[18] Mike Levine, "Boston One Year Later: DHS's Lessons Learned," *ABC News Online*, 10 April 2014, https://abcnews.go.com/images/Blotter/DHS%20After%20Action%20Review%20-%20FINAL.PDF, (Accessed 13 March 2021) Pg. 6

[19] Kimberly Hutchinson, "Dogs of DHS: How Canine Programs Contribute to Homeland Security," *TSA.gov*, https://www.tsa.gov/news/press/testimony/2016/03/03/dogs-dhs-how-canine-programs-contribute-homeland-security#:~:text=TSA%E2%80%99s%20National%20Explosives%20Detection%20Canine%20Team%20Program%20%28NEDCTP%29,TSA%E2%80%99s%20NEDCTP%20through%20its%20continued%20support%20and%20funding, (Accessed 13 March 2021)

80% of their time working in the transportation domain.[20] In 2018 NEDCTP reported 372 TSI EDC teams and 675 SLTT LE EDC teams deployed throughout the transportation domain.[21] The VIPR program, in coordination with SLTT transportation security stakeholders, can request additional TSI EDC teams from the local airport to enable enhanced security during special events. During special events of national significance, such as the Boston Marathon or other DHS SEAR events, the VIPR can coordinate with NEDTCP to provide additional SLTT LE EDC teams from outside the local area.[22]

Augmenting SLTT Capability – Brussels Airport Bombing - 2016

In March 2016, violent extremists conducted a coordinated IED attack in Brussels, Belgium. The bombers detonated two IEDs in the departures hall's public area at Brussels Airport (BRU) and the third device at a metro station in central Brussels.[23] The attacks killed 32 people and wounded 340, and all three bombers died in the blasts.[24] In response to the attacks, the Belgian government temporarily shut down the metro system and evacuated the airport.[25] Experts believe that the explosive material used in the IEDs was Triacetone Triperoxide (TATP).[26] A skilled bombmaker can assemble a TATP

---

[20] U.S. Transportation Security Administration. "Factsheet: TSA Canine Training Center," https://www.tsa.gov/sites/default/files/resources/caninetrainingcenter_factsheet_0.pdf, (Accessed 20 December 2020)

[21] U.S. Department of Homeland Security, Office of the Inspector General, "TSA's Challenges with Passenger Screening Canine Teams (REDACTED), 28 April 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-04/OIG-20-28-Apr20.pdf (Accessed 20 December 2020)

[22] TSA Blog, "Furry friends flock to Tampa for Super Bowl LV," 9 February 2021, https://www.tsa.gov/about/employee-stories/furry-friends-flock-tampa-super-bowl-lv, (Accessed 14 February 2021)

[23] Hannah Bloch, "Brussels Attacks: What Happened, In Photos and Maps," *NPR*, 22 March 2016, https://www.npr.org/2016/03/22/471423692/brussels-attacks-what-happened-in-photos-and-maps

[24] BBC Editors, "Brussels explosions: What we know about airport and metro attacks," *BBC.com*, 9 April 2016, https://www.bbc.com/news/world-europe-35869985, (Accessed 27 March 2021)

[25] Counter Extremism Project, "Belgium: Extremism and Terrorism," https://www.counterextremism.com/node/13508/printable/pdf, (Accessed 27 March 2021)

[26] Thomas Gibbons-Neff, "Brussels terrorists probably used explosive nicknamed 'the Mother of Satan'," The Washington Post, 23 March 2016,

device with commonly available materials in a kitchen.[27] The homicide bombing outside the secure perimeter of an airport is a concerning development in violent extremist tactics. This tactic forces transportation stakeholders to push the security perimeter out further, effectively increasing the effort and cost of providing a consistent security level.

In response to the Brussels attack, TSA hosted a working group of industry, government, academic, international, and SLTT transportation stakeholders to respond to the evolving tactics and techniques that violent extremists use to attack public areas of transportation venues.[28] In October 2019, the working group published its stakeholder guide titled *Protecting Public Areas Best Practices and Recommendations.* To prevent and respond to IED threats, TSA suggests that "A review of stakeholder resources—personnel, process, and technology—offers several opportunities to better align and strengthen resources to respond to various threats and improve day-to-day operations. Aligning resources across agencies and stakeholders provides for stronger attack prevention; more consistent intelligence, information sharing, and communication; fortified infrastructure; and more responsive operations. These are excellent demonstrations of aligning resources across various domains."[29] EDC Teams are currently the most effective IED detection method to protect public areas in the

---

https://www.washingtonpost.com/news/checkpoint/wp/2016/03/23/the-type-of-bombs-used-in-brussels-have-been-seen-before/, (Accessed 27 March 2021)

[27] GlobalSecurity.org, "Triacetone Triperoxide (TATP)," https://www.globalsecurity.org/military/systems/munitions/tatp.htm (Accessed 27 March 2021)

[28] U.S. Transportation Security Administration, "Protecting Public Areas Best Practices and Recommendations," October 2019, https://www.tsa.gov/sites/default/files/documents/hr302.section_1931.best_practices_9-25-19_3_oct17_final.pdf, (Accessed 25 September 2020) Pg. 2

[29] U.S. Transportation Security Administration, "Protecting Public Areas Best Practices and Recommendations," October 2019, https://www.tsa.gov/sites/default/files/documents/hr302.section_1931.best_practices_9-25-19_3_oct17_final.pdf, (Accessed 25 September 2020) Pg. 8

transportation domain.[30] As the guide suggests, the VIPR program's ability to augment SLTT capabilities by deploying EDC teams across the transportation domain provides a more significant and responsive security benefit to stakeholders.

Before 2011, NEDCTP provided the VIPR program with 45 EDC teams.[31] TSA internally divided these teams between two different groups of handlers. Transportation Security Inspectors (TSI) (non-law enforcement) led 23 teams, and Federal Air Marshals (FAMs) (law enforcement) led the remaining 22 teams. A 2012 DHS IG report stated that TSA realigned all 45 teams to non-law enforcement TSI handlers and reassigned the teams to airport screening duties in November 2011.[32] This realignment effectively removed operational control of all EDC teams from the VIPR program. Since the 2011 realignment, individual VIPR teams request TSI EDC team support from TSA managers at the local airport or SLTT LE EDC teams through agreements with local SLTT LE stakeholders.[33] A 2020 DHS Inspector General (DHS IG) audit of TSA's EDC team deployment methodology found that teams were being misused at TSA airport screening checkpoints to reduce passenger wait times rather than for security.[34] This audit did not

---

[30] Melanie Harvey, "From the Border to Disasters and Beyond: Critical Canine Contributions to the DHS Mission," *TSA.gov*, 18 May 2017, https://www.tsa.gov/news/press/testimony/2017/05/18/border-disasters-and-beyond-critical-canine-contributions-dhs

[31] U.S. Department of Homeland Security, Office of the Inspector General, "Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)," August 2012, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf, (Accessed 25 September 2020) Pg. 58

[32] U.S. Department of Homeland Security, Office of the Inspector General, "Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)," August 2012, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf, (Accessed 25 September 2020) Pg. 58

[33] U.S. Department of Homeland Security, Office of the Inspector General, "Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)," August 2012, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf, (Accessed 25 September 2020) Pg. 8; 60-61

[34] U.S. Department of Homeland Security, Office of the Inspector General, "TSA's Challenges with Passenger Screening Canine Teams (REDACTED)," April 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-04/OIG-20-28-Apr20.pdf, (Accessed 20 December 2020) Pg. 9

study the implications of EDC team availability for VIPR deployments. However, the audit's findings may call into question the actual availability of EDC teams to support VIPR operations when TSA airport managers prioritize checkpoint wait times over transportation security.[35] The 2011 realignment of EDC teams has complicated the relationship between the VIPR program and TSI EDC teams, potentially reducing the VIPR program's ability to mitigate IEDs throughout the transportation domain.

Summary – VIPR Capability Enhances SLTT IED Mitigation Efforts

IEDs are a persistent threat vector in the US transportation domain. IEDs deployed in vehicles, hidden in backpacks, or bags challenge detection and mitigation efforts.[36] The IED incidents summarized in this chapter underscore the extreme danger posed by IEDs and highlight the capability of the VIPR to enable and augment the security efforts of SLTT transportation stakeholders. As security perimeters expand to counter evolving violent extremist tactics, SLTT security stakeholders must stretch further to improve their security posture. TSA's *Protecting Public Areas Best Practices and Recommendations* guide encourages transportation stakeholders to share information and resources to prevent and respond to incidents throughout the transportation domain.[37] The VIPR program is the only federal program specifically dedicated to sharing the full

[35] U.S. Department of Homeland Security, Office of the Inspector General, "TSA's Challenges with Passenger Screening Canine Teams (REDACTED)," April 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-04/OIG-20-28-Apr20.pdf, (Accessed 20 December 2020) Pg. 9

[36] U.S. Transportation Security Administration, "2020 Biennial National Strategy for Transportation Security Report to Congress," 29 May 2020, https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf (Accessed 25 October 2020) Pg. vi

[37] U.S. Transportation Security Administration, "Protecting Public Areas Best Practices and Recommendations," October 2019, https://www.tsa.gov/sites/default/files/documents/hr302.section_1931.best_practices_9-25-19_3_oct17_final.pdf, (Accessed 25 September 2020) Pg. 8

range of DHS security and law enforcement assets with SLTT transportation stakeholders to defend against IED attacks in the public space.

EDC teams have proven to be the most versatile tools to counter the IED threats in public spaces.[38] However, TSA's VIPR program is a program divided. Since the reassignment of TSI EDC teams to airport checkpoint duties in 2011, the VIPR program has not had operational control of a vital IED detection tool. Today, the VIPR team relies on local relationships with TSA airport managers for EDC teams. As evidenced in the 2020 DHS IG audit of TSA's EDC deployment methodology, TSA has not identified and documented mission needs, capability gaps, or operational goals to deploy EDC teams to mitigate IED threats. As violent extremists continue to improve and adapt their IEDs to defeat mitigation efforts and detection technologies, it is imperative that TSA fully leverage its resources to protect the traveling public across all modes of transportation.[39] It is recommended that TSA assess VIPR capability gaps and mission goals to re-integrate TSI EDC teams with the VIPR program to enhance the capabilities of VIPR teams to enable and augment the security efforts of SLTT transportation stakeholders nationwide.

[38] U.S. Government Publishing Office, "Innovations in Security: Examining the Use of Canines," 115th Congress First Session, 3 October 2017, https://www.govinfo.gov/content/pkg/CHRG-115hhrg28507/html/CHRG-115hhrg28507.htm

[39] U.S. Department of Homeland Security. Science and Technology. "Snapshot: Testing Locations for Homemade Explosives Keep the Traveling Public Safe" https://www.dhs.gov/science-and-technology/news/2018/10/02/snapshot-testing-homemade-explosives-keep-travelers-safe (Accessed 14 November 2020)

Chapter 4: Lone-Offender Violent Extremists

Lone-Offenders and the Transportation Domain

Since the 9/11 Attacks, the US Government has dramatically increased its counter-terrorism efforts through enhanced border security, increased law enforcement efforts, and public outreach to identify and dismantle organized violent extremist groups.[1] Unable to operate effectively within the US, extremist organizations have encouraged the rise of lone-offender violent extremists.[2] A 2016 PBS Frontline article noted that although lone-offender attacks are relatively rare compared to other forms of violent extremism, lone-offender attacks are becoming more frequent and more lethal in the US[3]

The FBI's 2019 *Lone-Offender Terrorism Report* broadly defines lone-offenders as individuals who "may have affiliated or associated with a terrorist organization an ideological movement or may have received assistance from others at some stage during the planning or implementation of their attacks, [however] they must have been both the primary architect and the primary actor in the attack action."[4] Lone-offender violent extremists are be inspired by varying and sometimes overlapping cultural, political, religious, and moral beliefs. Law enforcement's efforts to detect and deter lone-offenders can be hindered by inherent characteristics present in many lone-offender threats, including:

---

[1] U.S. Government Publishing Office, "Low Cost, High Impact: Combating the Financing of Lone Wolf and Small Scale Terrorist Attacks," 115th Congress First Session, 6 September 2017, https://www.commerce.senate.gov/services/files/488585FA-FF88-4139-9C63-ED713BEB31D3

[2] J.M. Berger, "The Strategy of Violent White Supremacy Evolving," *The Atlantic*, August 7, 2019, https://www.theatlantic.com/ideas/archive/2019/08/the-new-strategy-of-violent-white-supremacy/595648/

[3] Katie Worth, "Lone Wolf Attacks Are Becoming More Common — And More Deadly," *PBS Frontline,* July 14, 2016, https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

[4] Lauren Richards et al., "Lone Offender – A Study of Lone Offender Terrorism in the United States (1972-2015)" National Center for the Analysis of Violent Crime (November 2019): 10

- Lone-offenders are typically legal residents of the country in which they conduct their attack. This allows lone-offenders to hide in plain sight among the population and negates an opportunity to stop threats at the border.[5]
- Lone-offenders are self-funding, negating law enforcement efforts to trace funding streams usually associated with terrorist actors.[6]
- Lone-offenders plan attacks using readily available or easily improvised weapons. Firearms, fireworks, nails, pressure cookers, lead pipes, and other materials are commonly available in the US and arouse little suspicion when purchased.[7]
- Lone-wolf violent extremists are influenced to self-radicalize. Numerous influences lead to self-radicalization, including; workplace, internet activity, military, prison, adopting external ideology, politically motivated, or personal beliefs.[8]

The summaries of select lone-offender incidents will highlight the advantages of leveraging the VIPR program's unique legal authorities, ability to enable SLTT, and capability to augment SLTT transportation security efforts to counter lone-offenders across the transportation domain. Combining the broad authority and capabilities of TSA's VIPR program with a risk based, intelligence driven deployment strategy is vital to protecting the transportation domain.

---

[5] Claire Wiskind, "Lone Wolf Terrorism and Open Source Jihad: An Explanation and Assessment," *International Institute for Counter Terrorism*, Summer 2016, http://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf#:~:text=Lone%20wolf%20terrorists%20pose%20a%20unique%20threat%20compared,analyzing%20the%20planning%20and%20execution%20of%20terror%20attacks. Pg. 3-4.

[6] U.S. Government Publishing Office, "Low Cost, High Impact: Combating the Financing of Lone Wolf and Small Scale Terrorist Attacks," 115th Congress First Session, 6 September 2017, https://www.commerce.senate.gov/services/files/488585FA-FF88-4139-9C63-ED713BEB31D3

[7] Claire Wiskind, "Lone Wolf Terrorism and Open Source Jihad: An Explanation and Assessment," *International Institute for Counter Terrorism*, Summer 2016, http://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf#:~:text=Lone%20wolf%20terrorists%20pose%20a%20unique%20threat%20compared,analyzing%20the%20planning%20and%20execution%20of%20terror%20attacks. Pg 3-4.

[8] Mark Hamm et al., "Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies" U.S. Department of Justice (February 2015): 3, https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf

VIPR Legal Authorities – LAX Active Shooter - 2013

In November 2013, a lone-offender entered Terminal 3 at Los Angeles International Airport (LAX) in Los Angeles, CA. Armed with a rifle and several hundred rounds of ammunition, the lone-offender opened fire near a TSA security checkpoint. The lone-offender killed a Transportation Security Officer (TSO) and wounded several bystanders. Los Angeles World Airport Police officers apprehended the suspect within eight minutes of the lone-offender's first shot.[9] The lone-offender's roommate later told investigators he had driven the lone-offender to the airport but did not notice any abnormal behaviors prior to the shooting.[10] Before the lone-offender arrived at LAX, he had sent a text message to his family in New Jersey, suggesting something bad was about to happen. Family in New Jersey notified the Los Angeles Police Department (LAPD) of the concerning text message.[11] LAPD officers arrived at the lone-offender's residence 52 minutes after the shooting at LAX had begun. Investigators later found notes in the lone-offender's possession that described his hatred of TSA's "Nazi checkpoints" and its presumption that "every American is a terrorist."[12] Immediately following this incident, TSA mandated an increase in VIPR operations to augment SLTT law enforcement efforts with Federal Air Marshal (FAM) support at airport checkpoints. This event highlights the

[9] Los Angeles World Airport Police, "Active Shooter Incident and Resulting Airport Disruption: A Review of Response Operations," 18 March 2014, https://www.lawa.org/-/media/lawa-web/projects-and-reports/lawa-t3-after-action-report-march-18-2014.ashx (Accessed 6 December 2020)

[10] David Simpson, "LAX shooting: Latest on suspect, victims and warning that may have come too late," *CNN.com*, 5 November 2013, https://www.cnn.com/2013/11/04/justice/lax-shooting/index.html

[11] David Simpson, "LAX shooting: Latest on suspect, victims and warning that may have come too late," *CNN.com*, 5 November 2013, https://www.cnn.com/2013/11/04/justice/lax-shooting/index.html

[12] Joel Rubin, "LAX gunman who targeted TSA officers is sentenced to life in prison," *Los Angeles Times*, November 7, 2016, https://www.latimes.com/local/lanow/la-me-ln-lax-shooting-sentencing-20161107-story.html.

broad legal authorities that allow TSOs and FAMs assigned to the VIPR program to rapidly re-deploy throughout the transportation domain to support SLTT security efforts.

After the 9/11 attacks, airport security underwent a significant overhaul. The most apparent change was shifting the aviation industry's responsibility for screening air passengers to the US Government under the leadership of the TSA.[13] Respecting the Constitutional rights of citizens is of paramount importance to all DHS security and law enforcement officers.[14] 49 US Code § 44901 authorizes TSOs to screen passengers, carry-on and checked baggage, and other articles that pose a threat to transportation security.[15] Additionally, the courts have permitted exemptions to Fourth Amendment protections in the form of administrative searches.[16] In harmony with applicable SLTT laws and regulations, the administrative search exemption allows TSOs to participate in security screening in all modes of transportation. To acquire the knowledge and skills required for threat detection in the transportation domain TSOs receive ten days of in-resident basic training and ongoing professional development throughout their careers.[17] As members of the VIPR program, TSOs have the authority and training to provide

---

[13] Transportation Security Administration, "Transportation Security Timeline: The Aviation and Transportation Security Act," https://www.tsa.gov/timeline (Accessed 15 February 2021)

[14] U.S. Department of Homeland Security, "Implementing 9/11 Commission Recommendations, Report to Congress 2011," 2011, https://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf , (Accessed 15 February 2021) Pg. 63

[15] Cornell Law School, "49 U.S. Code § 44901 - Screening passengers and property," https://www.law.cornell.edu/uscode/text/49/44901, (Accessed 15 February 2021)

[16] U.S. Civil Liberties.org, "Administrative Searches and Seizures," 13 October 2011, https://uscivilliberties.org/themes/3041-administrative-searches-and-seizures.html#:~:text=The%20Supreme%20Court%20has%20interpreted%20reasonableness%20to%20require,advances%20administrative%20interests%2C%20not%20traditional%20law%20enforcement%20objectives., (Accessed on 15 February 2021)

U.S. Civil Liberties.org, "Airport Searches," 13 October 2011, https://uscivilliberties.org/themes/3046-airport-searches.html., (Accessed on 15 February 2021)

[17] U.S. Department of Homeland Security, Federal Law Enforcement Training Accreditation, "Transportation Security Officer Basic Training Program," April 2020, https://www.fleta.gov/programacademy/transportation-security-officer-basic-training-program (Accessed 16 February 2021)

security screening throughout the transportation domain in coordination with SLTT transportation stakeholders.

FAMs are credentialed federal law enforcement officers and are the primary law enforcement element of the VIPR program. FAMs are authorized to; "A) carry a firearm, B) make an arrest without a warrant for any offense against the United States committed in the presence of the officer, or for any felony cognizable under the laws of the United States if the officer has probable cause to believe that the person to be arrested has committed or is committing the felony, and C) seek and execute warrants for arrest or seizure of evidence issued under the authority of the United States upon probable cause that a violation has been committed."[18] In some jurisdictions, FAMs have additional authority under state peace officer statutes. However, these statutes vary by state and locality and are not consistent across the VIPR program. For this reason, peace officer authorities are beyond the scope of this discussion. Operating under their primary authority, FAMs assigned to the VIPR program have the legal authorities to provide a robust law enforcement capability to SLTT transportation stakeholders.

Enabling SLTT – NYC Port Authority Bus Terminal Bombing – 2017

In December 2017, a lone-offender partially detonated a pipe bomb in an underground passageway linking the Port Authority Bus terminal and adjoining subway station in New York City (NYC). The attack injured five commuters and the lone-offender who was taken into custody by Port Authority police.[19] Investigators determined

[18] Cornell Law School, "49 U.S. Code § 114(p)(2) – Law Enforcement Powers," https://www.law.cornell.edu/uscode/text/49/114, (Accessed 15 February 2021)

[19] CBS News, "NYC terror attack suspect claims he did it for ISIS -- live updates," *Channel 7 CBSNews.coms*, 11 December 2017, https://www.cbsnews.com/news/port-authority-bus-terminal-explosion-bomb-2017-12-11-live-stream-updating/

that ISIS online materials viewed by the lone-offender inspired the bus terminal attack. Approximately one year before the attack the lone-offender began researching how to build IEDs on the internet.[20] The lone-offender, convicted on multiple charges relating to the attack in November 2018, faces life in prison at sentencing.[21] In 2018, one year after the lone-offender attack, Gothamist reported that NYC police installed a metal detector as part of a pilot program to enhance security in the NYC subway.[22] This event highlights the difficulty in securing a large and open transportation system with limited resources.

TSOs assigned to the VIPR program have the experience and technology to add a practical and unpredictable layer of screening throughout the transportation domain to detect and deter lone-offender attacks. Research conducted by Andrew R. Morral and Brian A. Jackson for the RAND Corporation finds that, while not well understood or measured, deterrence is a central feature of counterterrorism security and a significant factor in the cost-effectiveness of security programs.[23] Although measuring the deterrent value of any one security measure remains challenging, Jackson states that "deterrence attempts to manipulate terrorist choices to produce net security benefits."[24] Properly deployed deterrence effectively lowers the cost of security measures for SLTT

---

[20] U.S. Department of Justice, "Press Release: Akayed Ullah Charged With Terrorism and Explosives Charges in Connection With the Detonation of a Bomb in New York City," 12 December 2017, https://www.justice.gov/opa/pr/akayed-ullah-charged-terrorism-and-explosives-charges-connection-detonation-bomb-new-york-0

[21] U.S. Department of Justice, "Press Release: Akayed Ullah Convicted In Manhattan Federal Court For Detonation Of A Bomb In New York City," 6 November 2018, https://www.justice.gov/usao-sdny/pr/akayed-ullah-convicted-manhattan-federal-court-detonation-bomb-new-york-city

[22] Ben Yakas, "NYPD Tests Out Metal Detectors In The Subway," 14 December 2018, Gothamist, https://gothamist.com/news/nypd-tests-out-metal-detectors-in-the-subway

[23] Andrew R. Morral, "Understanding the Role of Deterrence in Counterterrorism Security," *Rand Corporation*, 2009, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf: 1

[24] Andrew R. Morral, "Understanding the Role of Deterrence in Counterterrorism Security," *Rand Corporation*, 2009, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf: 17

transportation stakeholders while simultaneously raises the perceived cost to lone-offenders intent on conducting an attack. Leveraging the VIPR program to enable risk-based, random deployments of security screening operations is one element that can complicate the lone-offender calculus and deter potential attacks.

Augmenting SLTT Capabilities – Super Bowl LV - 2021

On 7 February 2021 the Tampa Bay Buccaneers and Kansas City Chiefs in Super Bowl LV in Tampa, FL. Just weeks after unprecedented unrest at the US Capitol, the Super Bowl LV was enjoyed by millions of fans without incident. What football fans did not see was coordinated efforts of 70 local, state, and federal agencies to ensure the safety and security of the event. Each year DHS' Special Event Program partners with the National Football League (NFL) and SLTT stakeholders in Super Bowl cities to coordinate security planning. Approximately 500 DHS personnel supported security efforts during Super Bowl LV, including TSA VIPR Teams, EDC Teams, and TSOs.[25]

Each year the DHS Special Events Program (DHS SEP) receives thousands of requests from SLTT security stakeholders for federal assistance during special events. DHS SEP uses an assessment matrix that measures for threat, vulnerability, and consequences for each event. The matrix rates the events into one of five Special Event Rating Assessment (SEAR) levels. The SEAR levels are:[26]

- SEAR 1: Significant events with national and/or international importance that require extensive federal interagency support.
- SEAR 2: Significant events with national and/or international importance that may require some level of federal interagency support.

[25] U.S. Department of Homeland Security, "Press Release: DHS and Partners Coordinate to Secure Super Bowl LV," 6 February 2021, https://www.dhs.gov/news/2021/02/06/dhs-and-partners-coordinate-secure-super-bowl-lv

[26] U.S. Department of Homeland Security, "Fact Sheet: Special Event Assessment Rating (SEAR) Events," https://www.dhs.gov/sites/default/files/publications/19_0905_ops_sear-fact-sheet.pdf

- SEAR 3: Events of national and/or international importance that require only limited federal support.
- SEAR 4: Events with limited national importance that are managed at the state and local levels.
- SEAR 5: Events that may be nationally recognized but generally have local or state importance.

DHS's SEAR rating methodology prioritizes events that present the most significant risks to national security and public safety. Each year there are several hundred SEAR-rated events that are eligible for federal assistance. Lone-offenders do not provide law enforcement with typical indicators of violent extremist activities. Leveraging the DHS SEAR rating methodology to inform VIPR deployments maximizes opportunities for VIPR teams to provide a deterrent effect or, if necessary, disrupt an active attack.

Summary – VIPR Enhances Transportation Security Against Lone-Offenders

Lone-offender violent extremism is not new to the US In 2015, Indiana State University criminologist Mark S. Hamm partnered with Victoria University sociologist Ramon Spaaij to compile a database of nighty-eight lone-offender incidents between 1940 and 2013.[27] The study found the lone-offender violent extremism an evolving phenomenon in the US, with offenders shifting their focus to anti-government attacks, showing a preference for firearms over explosives in their attacks, and are becoming more independent in their paths to radicalization.[28]

As evidenced by the case studies examined in this chapter, the pre-operational indicators for a lone-offender attack may be subtle or undetectable. The lone-offender's

[27] Mark Hamm et al., "Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies" U.S. Department of Justice (February 2015): 3, https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf

[28] Ramon Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict &Terrorism*, 33(9), (2020): 854-870, https://www.academia.edu/21899455/The_Enigma_of_Lone_Wolf_Terrorism_An_Assessment

secretive and independent nature makes operationalized attacks challenging to deter or disrupt. Deterrence measures have proven effective at limiting the effectiveness of lone-offender attacks.[29] Law enforcement and security presence provide a visible deterrent effect. At the same time, checkpoints or other active screening can physically limit a lone-offender's access to sensitive or more desirable areas of the transportation domain. Providing a high level of law enforcement and security presence at all vital areas of the transportation domain is economically and functionally impractical. However, strategically deploying TSA's thirty Visible Intermodal Prevention and Response (VIPR) teams for special events or in response to intelligence-driven threats can increase law enforcement presence anywhere in the transportation domain. With broad authority to coordinate with SLTT transportation stakeholders, VIPR teams are uniquely positioned to augment transportation security across jurisdictional lines.

[29] Andrew R. Morral, "Understanding the Role of Deterrence in Counterterrorism Security," *Rand Corporation*, 2009, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf: 12

Chapter 5: Recommendations/Conclusion

Recommendations

The Mission of the Transportation Security Administration's (TSA) Visible Intermodal Prevention and Response (VIPR) program is to "promote confidence in and protect our nation's transportation systems through targeted deployment of integrated assets utilizing screening and law enforcement in coordinated activities to augment and enhance security."[1] The VIPR program has not reached its full potential and fails to leverage the full authority granted to TSA law enforcement, security, and regulatory personnel. The below recommendations are offered to enhance VIPR program effectiveness and provide a safe and secure transportation domain for the traveling public.

1. TSA's VIPR Program should re-focus its mission to include coordination of all local transportation domain security issues. Developing a long-term strategy to that includes regional coordination will allow local VIPR teams to build trust and engagement with all SLTT transportation domain stakeholders. With renewed focus, the VIPR program can leverage its unique authority and capabilities to emerge as a leader in transportation security. This recommendation includes relocating a VIPR team nearer to SLTT transportation security stakeholders based on current threat assessments and stakeholder capabilities.

2. TSA's VIPR program should conduct bi-annual surveys of SLTT transportation security stakeholders to ensure VIPR program policies and capabilities

[1] U.S. Transportation Security Administration. TSA Management Directive No. 2800.13: Visible Intermodal Prevention and Response Program (VIPR), 10 March 2017

remain in alignment with SLTT stakeholders' needs. Surveys would provide a forum through which SLTT transportation security stakeholders provide feedback to the VIPR program. Survey feedback will help shape VIPR program policy, ensuring VIPR resources continue to augment and not duplicate SLTT stakeholder capabilities in an evolving threat environment.

3. TSA's VIPR program should develop a Counter Unmanned Aerial System (C-UAS) policy to prioritize training and procurement of technology to augment SLTT C-UAS response. UAS is an evolving threat vector. The vehicles are becoming more advanced, allowing greater control, payload capacity, and range. Extremist groups have already demonstrated the ability to use commercial UAS vehicles to deliver explosive devices on target. Legal restrictions place C-UAS capability beyond SLTT transportation security stakeholders' capabilities. The VIPR program is the only program specifically dedicated and positioned to fill C-UAS capability gaps throughout the transportation domain.

4. TSA's VIPR program should develop a Counter Improvised Explosive Device (C-IED) deployment policy that allows for the full employment of all TSA explosive detection resources to enhance SLTT explosive detection capabilities. Improvised Explosive Devices (IEDs) remain an attractive weapon of choice for violent extremists seeking to create many casualties in their attack. VIPR teams can best utilize these existing EDC team capabilities during special events, periods of heightened threat, or as a deterrent presence in coordination with SLTT transportation security stakeholders.

5. TSA's VIPR program should develop a lone-offender violent extremist deterrence and response policy that leverages the DHS SEAR methodology to ensure

VIPR deployments are conducted to protect events of national significance from lone-offender attacks. By their nature, lone-offenders are difficult to deter or disrupt. However, once a lone-offender initiates an attack, law enforcement and security resources must respond rapidly to preserve life and neutralize the attacker. Lone-offenders typically are only stopped when law enforcement personnel confront them. Given the random nature of lone-offenders timing and location, VIPR resources would be best utilized, in response to specific threat information, to support DHS designated special events or as a force multiplier and deterrent in coordination with SLTT transportation security stakeholders.

Conclusion

TSA's VIPR program is uniquely capable of providing a broad range of law enforcement and security capability to augment existing SLTT capacity to support the DHS's countering terrorism and target violence goals to protect against violent extremist threats throughout the transportation domain. Since the creation of the VIPR program in 2005, the transportation security landscape has evolved significantly. Transportation stakeholders nationwide have invested in hardening their facilities against violent extremist attacks. Simultaneously, violent extremists have devised new tactics and leveraged new technologies to continue their transportation domain attacks. In a defender vs. attacker contest where the traveling public's safety and security and the Nation's transportation domain are at stake, the VIPR program must focus its resources where it will provide the most significant benefit. Leveraging the VIPR program's ability to deploy across jurisdictional boundaries and access the full spectrum of DHS law enforcement and security resources will ensure maximum support to SLTT transportation stakeholders during special events, in response to threat information, or as a visible

deterrent. The three proposed mission sets, countering Unmanned Aerial Systems, deterring and detecting Improvised Explosive Devices, and rapidly defeating lone-offender attacks, offer the VIPR program new opportunities to enhance the Nation's transportation security posture. The recommendations provided in this thesis can enhance the VIPR program's ability to leverage its broad authority and unique capabilities to remain a valued partner to SLTT transportation stakeholders. A successful VIPR program fills a capability gap in federal transportation security efforts, and aligns with DHS strategic goals. The VIPR program is the only DHS effort dedicated to "promote[ing] confidence in and protect[ing] our Nation's transportation systems through targeted deployments of integrated TSA assets utilizing law enforcement and screening capabilities to augment [the] security of any mode of transportation."[2]

[2] U.S. Department of Homeland Security, "Strategic Framework for Countering Terrorism and Targeted Violence," September 2019, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf (Accessed 25 July 2020) Pg. 19-20

Bibliography

Arab News Staff, "Saudi, US air forces train to down enemy drones," Arab News, 10 February 2021, https://www.arabnews.com/node/1806671/saudi-arabia.

BBC Editors, "Brussels explosions: What we know about airport and metro attacks," BBC.com, 9 April 2016, https://www.bbc.com/news/world-europe-35869985, (Accessed 27 March 2021)

Biesecker, Cal. "Plan for TSA to Lead Federal Counter Drone Operations at Airports 'Unlawful,' Hill Aide Says" Defense Daily, 17 December 2019, Accessed on 28 November 2020, https://www.defensedaily.com/plan-tsa-lead-federal-counter-drone-operations-airports-unlawful-hill-aide-says-2/unmanned-systems/

Berger, J.M., "The Strategy of Violent White Supremacy Evolving," The Atlantic, August 7, 2019, https://www.theatlantic.com/ideas/archive/2019/08/the-new-strategy-of-violent-white-supremacy/595648/

Blalock, James. Patrick Henry College. The Intelligencer. Lone Wolf Terrorism: Leaderless Resistance"" https://www.phc.edu/intelligencer/lone-wolf (Accessed 8 December 2020)

Bloch, Hannah. "Brussels Attacks: What Happened, In Photos and Maps," NPR, 22 March 2016, https://www.npr.org/2016/03/22/471423692/brussels-attacks-what-happened-in-photos-and-maps (Accessed 15 February 2021)

Brown, Michael E., Owen R. Cote Jr., Sean M. Lynn-Jones, and Steven E. Miller, ed. *Contending with Terrorism: Roots, Strategies, and Responses*. Cambridge: The MIT Press, 2010.

CBS News, "NYC terror attack suspect claims he did it for ISIS -- live updates," Channel 7 CBSNews.coms, 11 December 2017, https://www.cbsnews.com/news/port-authority-bus-terminal-explosion-bomb-2017-12-11-live-stream-updating/.

Cohen Gilliland, Haley. "Why explosives detectors still can't beat a dogs nose," MIT Technology Review, 24 October 2019, Accessed 15 February 2021, https://www.technologyreview.com/2019/10/24/132201/explosives-detectors-dogs-nose-sensors/.

Colb, Sherry F. "Who's a Good Boy? US Supreme Court Considers Again Whether Dog Sniffs Are Searches," Verdict.Justia.com, 16 January 2019, Accessed 15 February 2021, https://verdict.justia.com/2019/01/16/whos-a-good-boy-us-supreme-court-considers-again-whether-dog-sniffs-are-searches.

Cornell Law School, "Destruction of aircraft or aircraft facilities, 18 USC 32," Accessed 28 November 2020, https://www.law.cornell.edu/uscode/text/18/32.

Cornell Law School, "Law Enforcement Powers, 49 U.S. Code 114(p)(2)," Accessed 15 February 2021, https://www.law.cornell.edu/uscode/text/49/114.

Cornell Law School, "Unmanned Aircraft Systems, Definitions, 49 USC 44801," Accessed 28 November 2020, https://www.law.cornell.edu/uscode/text/49/44801.

Cornell Law School, "FAA Modernization and Reform Act of 2012, 49 U.S.C. 44802," Accessed 28 November 2020, https://www.law.cornell.edu/uscode/text/49/44802.

Cornell Law School, "Screening passengers and property, 49 U.S. Code 44901," Accessed 28 January 2021, https://www.law.cornell.edu/uscode/text/49/44901.

Cornell Law School, "Domestic air transportation system security 49 U.S. Code 44904," Accessed 28 November 2020, https://www.law.cornell.edu/uscode/text/49/44904.

Counter Extremism Project, "Belgium: Extremism and Terrorism," https://www.counterextremism.com/node/13508/printable/pdf, (Accessed 27 March 2021)

Creitz, Charles, "Wolf says 'lone, homegrown' terror threat is top DHS focus 19 years after 9/11," *Fox News.com,* September 11, 2020, https://www.foxnews.com/politics/chad-wolf-dhs-lone-homegrown-terror-threat.

Crenshaw, Martha, ed. *The Consequences of Counterterrorism*. New York: Russell Sage Foundation, 2010.

Davis, Paul K. and Brian Michael Jenkins. *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda*. Santa Monica: RAND, 2002. Accessed September 26, 2020. https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1619.pdf#:~:text=xviii%20Deterrence%20and%20Influence%20in%20Counterterrorism%20open%20discussion%2C,nongovernment%20organizations%20%28NGOs%29%20attempting%20to%20build%20civil%20societies.

Debre, Isable. "Saudi TV: Yemen rebel attack on airport sets plane on fire," AP News, 10 February 2021, https://apnews.com/article/middle-east-yemen-dubai-saudi-arabia-united-arab-emirates-a351ca2f95c68ebf08c385742deef2ac.

Federal Aviation Administration, "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," August 2020, Accessed 28 November 2020, https://www.faa.gov/uas/resources/c_uas/media/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf.

Federal Aviation Administration, "Notices to Airmen (NOTAMs) Back to Basics," Accessed 27 March 2021, https://www.faa.gov/about/initiatives/notam/what_is_a_notam/

Federal Aviation Administration, "The FAA's New Drone Rules Are Effective Today," 29 August 2016, Accessed 28 November 2020, https://www.faa.gov/news/updates/?newsId=86305

Federal Aviation Administration, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap," Second Edition, July 2018, https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf.

Find Law, "6 USC 1112 – Authorization of Visible Intermodal Prevention and Response teams" Accessed 29 September 2020, https://codes.findlaw.com/us/title-6-domestic-security/6-usc-sect-1112.html.

Gill, Charlotte. "TSA's Security Playbook," George Mason University, Accessed 28 November 2020, http://cebcp.org/wp-content/publications/PhaseII-Final-Report-Redacted.pdf

Gibbons-Neff, Thomas. "Brussels terrorists probably used explosive nicknamed 'the Mother of Satan'," The Washington Post, 23 March 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/03/23/the-type-of-bombs-used-in-brussels-have-been-seen-before/, (Accessed 27 March 2021)

GlobalSecurity.org, "Triacetone Triperoxide (TATP)," https://www.globalsecurity.org/military/systems/munitions/tatp.htm (Accessed 27 March 2021)

Goodrich, Daniel, Frances Edwards. "Transportation, Terrorism and Crime: Deterrence, Disruption and Resilience" *Mineta Transportation Institute Publications* (2020): https://doi.org/10.31979/mti.2019.1896

Hamm, Mark, Spaaj, Ramon, "Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies" U.S. Department of Justice (February 2015), https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf

Harvey, Melanie. "From the Border to Disasters and Beyond: Critical Canine Contributions to the DHS Mission," *TSA.gov*, 18 May 2017, https://www.tsa.gov/news/press/testimony/2017/05/18/border-disasters-and-beyond-critical-canine-contributions-dhs.

History.com Editors, "Terrorists bomb trains in Madrid," 10 March 2020, Accessed 25 October 2020, https://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid.

History.com Editors, "Boston Marathon Bombing," 7 June 2019, Accessed 25 October 2020, https://www.history.com/topics/21st-century/boston-marathon-bombings#section_2.

Huerta, Michael. "Blue Ribbon Task Force on UAS Mitigation at Airports: Final Report," The Moak Group, October 2019, Accessed 10 December 2020, https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf.

Hutchinson, Kimberly. "Dogs of DHS: How Canine Programs Contribute to Homeland Security," TSA.gov, https://www.tsa.gov/news/press/testimony/2016/03/03/dogs-dhs-how-canine-programs-contribute-homeland-security#:~:text=TSA%E2%80%99s%20National%20Explosives%20Detection%20Canine%20Team%20Program%20%28NEDCTP%29,TSA%E2%80%99s%20NEDCTP%20through%20its%20continued%20support%20and%20funding, (Accessed 13 March 2021)

Jackson, Brian A., Ashley L. Rhoades, Jordan R. Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. *Practical Terrorism Prevention: Reexamining U.S.*

National Approaches to Addressing the Threat of Ideologically Motivated Violence. Homeland Security Operational Analysis Center operated by the RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2647.html.

Joshi, Divya. Business Insider. "Here are the world's largest drone companies and manufacturers to watch and stocks to invest in 2020" https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks (Accessed November 28, 2020)

Kaplan, Fred. The Slate Group. "The First Drone Strike" https://slate.com/news-and-politics/2016/09/a-history-of-the-armed-drone.html (Accessed December 9, 2020)

Kube, Courtney. "New law would give federal government the right to shoot down private drones inside U.S.," NBCNews.com, 24 September 2019, https://www.nbcnews.com/politics/national-security/new-law-would-give-federal-government-right-shoot-down-private-n912381.

Miller, Gregory D. "Terrorist Decision Making and the Deterrence Problem." *Studies in Conflict & Terrorism* Volume 36 - Issue 2 (January 2013): 132-151 https://doi.org/10.1080/1057610X.2013.747075.

Morral, Andrew R. "Understanding the Role of Deterrence in Counterterrorism Security," *Rand Corporation*, 2009, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf.

Lebovic, James H. *Deterring International Terrorism and Rogue States*. London: Routledge, 2007.

Lee, Isabella. "Drone Pilot Fined $20,000 For Landing Drone at McCarran Airport, Las Vegas," UAVCoach.com, 3 December 2019, https://uavcoach.com/drone-pilot-fines/

Levine, Mike. "Boston One Year Later: DHS's Lessons Learned," ABC News Online, 10 April 2014, Accessed 13 March 2021, https://abcnews.go.com/images/Blotter/DHS%20After%20Action%20Review%20-%20FINAL.PDF.

Los Angeles World Airport Police, "Active Shooter Incident and Resulting Airport Disruption: A Review of Response Operations," 18 March 2014, https://www.lawa.org/-/media/lawa-web/projects-and-reports/lawa-t3-after-action-report-march-18-2014.ashx. (Accessed 6 December 2020)

Lykou, Georgia. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," Sensors, June 22, 2020: 14-15, https://www.semanticscholar.org/paper/Defending-Airports-from-UAS%3A-A-Survey-on-and-Lykou-Moustakas/cdccb4ad90f9155c3d62d00d071f5331d4ac29ea

Martin, Gus. *Understand Homeland Security 2nd Edition*. Los Angeles: SAGE, 2017.

Morag, Nadav. *Comparative Homeland Security: Global Lessons 2nd Edition*. Hoboken: 2018.

Mueller, John and Stewart, Mark G. *Terror, Security, and Money Balancing the Risks, Benefits, and Costs of Homeland Security*. New York: Oxford University Press, 2011.

Newdick, Thomas. "Yemen's Houthi Rebels Strike Airliner In New Drone Attack On Saudi Airport," The Drive.com, 10 February 2021, https://www.thedrive.com/the-war-zone/39186/yemens-houthi-rebels-strike-airliner-in-new-drone-attack-on-saudi-airport.

Rassler, Don. "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology," Combatting Terrorism Center at West Point, October 2016, https://ctc.usma.edu/wp-content/uploads/2016/10/Drones-Report.pdf

Richards, Lauren, Molinaro, Peter, Wyman, John, Craun, Sarah. "Lone Offender – A Study of Lone Offender Terrorism in the United States (1972-2015)" National Center for the Analysis of Violent Crime (November 2019). https://www.fbi.gov/file-repository/lone-offender-terrorism-report-111319.pdf/view

Reuters Staff, "Yemen's Houthis say they carried out drone attack on Saudi airport," Reuters, 10 February 2021, https://www.reuters.com/article/us-yemen-security-saudi-airport/yemens-houthis-say-they-carried-out-drone-attack-on-saudi-airport-idUSKBN2AA1IG.

Rubin, Joel. "LAX gunman who targeted TSA officers is sentenced to life in prison," Los Angeles Times, November 7, 2016, https://www.latimes.com/local/lanow/la-me-ln-lax-shooting-sentencing-20161107-story.html.

Shackle, Samira. "The mystery of the Gatwick drone," The Guardian, 1 December 2020, https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

Simpson, David. "LAX shooting: Latest on suspect, victims and warning that may have come too late," CNN.com, 5 November 2013, https://www.cnn.com/2013/11/04/justice/lax-shooting/index.html.

Singh, Kanishka. "Gatwick, Heathrow airports order military-grade anti-drone equipment," Reuters, 3 January 2019, https://www.reuters.com/article/us-britain-drones-gatwick-idUSKCN1OX1KX

SkyNews Editors, "Gatwick drone inquiry: 93 'credible sightings'," SkyNews.com, 29 December 2018, https://news.sky.com/story/some-gatwick-drone-sightings-may-have-been-police-drones-chief-constable-says-11593854

Snead, Seibler. "Establishing a Legal Framework for Counter-Drone Technologies," The Heritage Foundation, 16 April 2018, https://www.heritage.org/sites/default/files/2018-04/BG3305_1.pdf.

Streetly, Martin ed., Jane's All the World's Aircraft: Unmanned 2014–2015 (London: IHS Jane's, 2014), 79-80.

Stubblefield, Angela H., "Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks," U.S. Department of Transportation, 18 June 2019, Accessed 28

November 2020, https://www.transportation.gov/testimony/drone-security-enhancing-innovation-and-mitigating-supply-chain-risks.

SuccessStory.com "DJI – Revolutionizing Technology," Accessed 28 November 2020, https://successstory.com/companies/dji

Taquechel, Eric F., and Marina Saitgalina. "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis." Homeland Security Affairs 14, Article 8 (December 2018). https://www.hsaj.org/articles/14699

Trevithick, Joseph. "Watch A Saudi F-15 Fighter Swoop In Low To Blast A Houthi Rebel Drone Out Of The Sky," The Drive.com, 30 March 2021, https://www.thedrive.com/the-war-zone/39992/watch-a-saudi-f-15-fighter-swoop-in-low-to-blast-a-houthi-rebel-drone-out-of-the-sky.

The White House. "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience." Accessed 25 September 2020. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Thornton, Chandler. "Rebels launch drone attack on Saudi airport, injuring 9," CNN.com, 2 July 2019, https://www.cnn.com/2019/07/02/middleeast/saudi-abha-airport-drone-attack-intl.

TSA Blog, "Furry friends flock to Tampa for Super Bowl LV," 9 February 2021, https://www.tsa.gov/about/employee-stories/furry-friends-flock-tampa-super-bowl-lv, (Accessed 14 February 2021)

United Nations, "Office of Disarmament Affairs, Production and delivery [of IEDs]," Accessed 14 November 2020, https://www.un.org/disarmament/convarms/production/.

U.S. Civil Liberties.org, "Administrative Searches and Seizures," 13 October 2011, https://uscivilliberties.org/themes/3041-administrative-searches-and-seizures.html#:~:text=The%20Supreme%20Court%20has%20interpreted%20reasonableness%20to%20require,advances%20administrative%20interests%2C%20not%20traditional%20law%20enforcement%20objectives., (Accessed on 15 February 2021)

U.S. Civil Liberties.org, "Airport Searches," 13 October 2011, https://uscivilliberties.org/themes/3046-airport-searches.html., (Accessed on 15 February 2021)

U.S. Courts.gov, "What Does the Fourth Amendment Mean?," Accessed 15 February 2021, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0.

U.S. Department of Defense. Deterrence Operations Joint Operating Concept. Version 2.0. December 2006. Washington DC: Department of Defense, December 2006

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Protecting Against the Threat of Unmanned Aircraft Systems (UAS),"

November 2020, Accessed 28 November 2020, https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf.

U.S. Department of Homeland Security. "IED Attack – Improvised Explosive Devices," Accessed 14 November 2020, https://www.dhs.gov/sites/default/files/publications/prep_ied_fact_sheet.pdf.

U.S. Department of Homeland Security. Science and Technology. "Snapshot: Testing Locations for Homemade Explosives Keep the Traveling Public Safe," Accessed 14 November 2020, https://www.dhs.gov/science-and-technology/news/2018/10/02/snapshot-testing-homemade-explosives-keep-travelers-safe.

U.S. Department of Homeland Security, "Counter-Unmanned Aircraft Systems Technology Guide," September 2019, Accessed 1 October 2020, https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

U.S. Department of Homeland Security. Office of the Inspector General. "FAMS Needs to Demonstrate How Ground-based Assignments Contribute to TSA's Mission (Redacted)." Accessed 25 September 2020. https://www.oig.dhs.gov/sites/default/files/assets/2018-08/OIG-18-70-Jul18.pdf#:~:text=FAMS%20Needs%20to%20Demonstrate%20How%20Ground-%20based%20Assignments,the%20Office%20of%20Law%20Enforcement%2FFederal%20Air%20Marshal%20Service.

U.S. Department of Homeland Security. Office of Inspector General. "Efficiency and Effectiveness of TSA's Visible Intermodal Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)." Accessed 25 September 2020. https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf.

U.S. Department of Homeland Security, Office of the Inspector General, "TSA's Challenges with Passenger Screening Canine Teams (REDACTED), 28 April 2020, Accessed 20 December 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-04/OIG-20-28-Apr20.pdf.

U.S. Department of Homeland Security, "The DHS Strategic Plan Fiscal Years 2020-2024," Accessed 25 July 2020. https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf.

U.S. Department of Homeland Security. Office of Inspector General. "TSA's Administration and Coordination of Mass Transit Security Programs." Accessed September 25, 2020. http://www.oig.dhs/gov/assets/Mgmt/OIG-08-66_jun08.pdf.

U.S. Department of Homeland Security. "Implementing 9/11 Commission Recommendations: Progress Report 2011." Accessed September 25, 2020. https://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf.

U.S. Department of Homeland Security. "2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience." Accessed September 25, 2020. https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

U.S. Department of Homeland Security, "Privacy Impact Assessment for the Counter-Unmanned Aircraft Systems (C-UAS)," 15 July 2020, Accessed 15 February 2021, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall085-c-uas-august2020_updated.pdf.

U.S. Department of Homeland Security, "Snapshot: Countering Unmanned Aerial Systems in Urban Environments," Science and Technology, May 11, 2018, https://www.dhs.gov/science-and-technology/news/2018/05/11/snapshot-c-uas-urban-environments.

U.S. Department of Homeland Security, "Fact Sheet: IED Attack – Improvised Explosive Devices," Accessed 14 November 2020, https://www.dhs.gov/sites/default/files/publications/prep_ied_fact_sheet.pdf.

U.S. Department of Homeland Security, "Factsheet: News &Terrorism, Communicating in a crisis, IED Attack Improvised Explosive Devices," Accessed 14 November 2020, https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf.

U.S. Department of Homeland Security. "2015 Transportation Systems Sector-Specific Plan." Accessed September 25, 2020. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf.

U.S. Department of Homeland Security. Science and Technology. "Snapshot: Testing Locations for Homemade Explosives Keep the Traveling Public Safe," Accessed 14 November 2020, https://www.dhs.gov/science-and-technology/news/2018/10/02/snapshot-testing-homemade-explosives-keep-travelers-safe.

U.S. Department of Homeland Security. "Strategic National Risk Assessment, December 2011." Accessed September 25, 2020. https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

U.S. Department of Homeland Security, "Strategic Framework for Countering Terrorism and Targeted Violence," September 2019, Accessed 25 July 2020, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.

U.S. Department of Homeland Security, "Transportation Security Administration Budget Overview: Fiscal Year 2021 Congressional Justification," Accessed 15 February 2021, https://www.dhs.gov/sites/default/files/publications/transportation_security_administration.pdf.

U.S. Department of Homeland Security, Federal Law Enforcement Training Accreditation, "Transportation Security Officer Basic Training Program," April

2020, Accessed 16 February 2021, https://www.fleta.gov/programacademy/transportation-security-officer-basic-training-program.

U.S. Department of Justice, "Press Release: Akayed Ullah Charged With Terrorism and Explosives Charges in Connection With the Detonation of a Bomb in New York City," 12 December 2017, https://www.justice.gov/opa/pr/akayed-ullah-charged-terrorism-and-explosives-charges-connection-detonation-bomb-new-york-0.

U.S. Department of Justice, "Press Release: Akayed Ullah Convicted In Manhattan Federal Court For Detonation Of A Bomb In New York City," 6 November 2018, https://www.justice.gov/usao-sdny/pr/akayed-ullah-convicted-manhattan-federal-court-detonation-bomb-new-york-city.

U.S. District Court, District of Massachusetts, "Charging Affidavit: U.S. vs Dzhokhar A. Tsarnaev", 27 June 2013, Accessed 13 March 2021, https://www.justice.gov/iso/opa/resources/632013627162038513370.pdf.

U.S. Government Accountability Office. *National Security Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies*. GAO-19-204SP. Washington, DC, 2019. December 2018. https://www.hsdl.org/?view&did=819570.

U.S. Government Accountability Office, *Federal Air Marshal Service: Actions Taken to Fulfill Core Mission and Address Workforce Issues*. GAO-09-903T. Washington, DC, 2009. 23 July 2009. https://www.gao.gov/assets/gao-09-903t.pdf.

U.S. Government Accountability Office, *Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities*. GAO-10-435R. Washington, DC, 2010. 27 May 2010. https://www.gao.gov/assets/gao-10-435r.pdf.

U.S. Government Accountability Office, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*. GAO-16-632. Washington, DC, 2016. May 2016. https://www.gao.gov/assets/gao-16-632.pdf.

U.S. Government Accountability Office, *Surface Transportation: DHS Is Developing and Testing Security Technologies, but Could Better Share Test Results*, GAO-19-636. Washington, DC, 2019. September 2019. https://www.gao.gov/assets/gao-19-636.pdf

U.S. Government Publishing Office, "FAA Reauthorization Act of 2018," Public Law 115–254, 5 October 2018, Accessed 25 October 2020, https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf

U.S. Government Publishing Office, "Innovations in Security: Examining the Use of Canines," 115th Congress First Session, 3 October 2017, https://www.govinfo.gov/content/pkg/CHRG-115hhrg28507/html/CHRG-115hhrg28507.htm.

U.S. Government Publishing Office, "Low Cost, High Impact: Combating the Financing of Lone Wolf and Small Scale Terrorist Attacks," 115th Congress First Session, 6

September 2017, https://www.commerce.senate.gov/services/files/488585FA-FF88-4139-9C63-ED713BEB31D3.

U.S. President. National Security Strategy of the United States of America, by the White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf. Washington, DC: Government Publishing Office, December 2017.

U.S. Transportation Security Administration, "TSA Strategy 2018-2026," Accessed 1 October 2020, https://www.tsa.gov/sites/default/files/tsa_strategy.pdf.

U.S. Transportation Security Administration. "TSA Management Directive No. 2800.13: Visible Intermodal Prevention and Response Program (VIPR)," 10 March 2017

U.S. Transportation Security Administration, "2020 Biennial National Strategy for Transportation Security Report to Congress," Accessed 29 May 2020, https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf.

U.S. Transportation Security Administration. "Aviation and Transportation Security Act of 2001," Accessed on 24 October 2020, https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf.

U.S. Transportation Security Administration. "Factsheet: TSA by the Numbers," 4 February 2020, Accessed on 20 December 2020, https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet.pdf.

U.S. Transportation Security Administration, "Factsheet: TSA Canine Training Center," Accessed 20 December 2020, https://www.tsa.gov/sites/default/files/resources/caninetrainingcenter_factsheet_0.pdf.

U.S. Transportation Security Administration, "Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors," Accessed 15 February 2021, https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf.

U.S. Transportation Security Administration, "Protecting Public Areas Best Practices and Recommendations," October 2019, Accessed 25 September 2020, https://www.tsa.gov/sites/default/files/documents/hr302.section_1931.best_practices_9-25-19_3_oct17_final.pdf.

U.S. Transportation Security Administration, "Transportation Security Timeline: The Aviation and Transportation Security Act," Accessed 15 February 2021, https://www.tsa.gov/timeline.

Wiskind, Claire. "Lone Wolf Terrorism and Open Source Jihad: An Explanation and Assessment," International Institute for Counter Terrorism, Summer 2016, http://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf#:~:text=Lone%20wolf%20terrorists%20pose%20a%20unique%20thr

eat%20compared,analyzing%20the%20planning%20and%20execution%20of%20terror%20attacks.

Worth, Katie. "Lone Wolf Attacks Are Becoming More Common — And More Deadly," PBS Frontline, July 14, 2016, https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

Yinon, Jehuda, ed., Counterterrorist Detection Techniques of Explosives (Oxford: Elsevier Science & Technology, 2007), 397-398

Yakas, Ben. "NYPD Tests Out Metal Detectors In The Subway," 14 December 2018, *Gothamist*, https://gothamist.com/news/nypd-tests-out-metal-detectors-in-the-subway.

Vita

Mr. Nelson Minerly, Transportation Security Administration/Law Enforcement (TSA/LE), is a career public servant and Department of Homeland Security law enforcement officer. Mr. Minerly currently serves as the TSA Special Event Coordinator. In this position, he is responsible for facilitating TSA support of DHS-rated special events and national special security events. Before this assignment, Mr. Minerly served as a program manager for TSA's Special Mission Coverage program. He oversaw the strategic deployment of Federal Air Marshals aboard high-risk flights across the country and around the world. While assigned to the TSA/LE Washington Field Office, Mr. Minerly served as a Federal Air Marshal Squad and Visible Intermodal Prevention and Response supervisor. During his first TSA/LE headquarters assignment, Mr. Minerly served as the lead public affairs spokesperson for all TSA law enforcement inquires.

Mr. Minerly began his federal service in the US Navy as a nuclear power plant electrician aboard a 688 Los Angeles class fast attack submarine. He earned his Bachelor of Arts degree in Historical Studies from the State University of New York, Empire State College.