2023-03

ALONG FOR THE RIDE: THE UNITED STATES NEEDS TO PREPARE SECURITY STANDARDS NOW FOR COMMERCIAL SPACE TRAVEL

Babin, Jared M.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71976

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ALONG FOR THE RIDE: THE UNITED STATES NEEDS TO PREPARE SECURITY STANDARDS NOW FOR COMMERCIAL SPACE TRAVEL

by

Jared M. Babin

March 2023

Co-Advisors: Nadav Morag (contractor)
Mollie R. McGuire

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE ALONG FOR THE RIDE: THE UNITED STATES NEEDS TO PREPARE SECURITY STANDARDS NOW FOR COMMERCIAL SPACE TRAVEL	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jared M. Babin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

The concept of regulating the physical security of commercial spaceports has received little attention. Currently, no federal agency is responsible for developing physical security standards or enforcing regulatory compliance within the industry. This thesis examines the need to create and apply ground-based physical security standards to commercial space facilities within the United States. This thesis explores three policy options as potential paths forward if commercial space travel is designated as critical infrastructure and assesses their effectiveness, cost, political challenges, and viability. The analysis determines that taking proactive measures now will mitigate the potential costs and impacts of an attack and would save substantial amounts of money, keep a burgeoning market on track, and could save lives. Ultimately, this thesis concludes that implementing a regulatory approach like the one employed by the Transportation Security Administration's surface transportation program would be effective if it prevents the explosion of one Falcon 9 rocket, or similar, every approximately 188 years.

14. SUBJECT TERMS space, security, ground-based, vetting, regulations	**15. NUMBER OF PAGES** 93
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

ALONG FOR THE RIDE: THE UNITED STATES NEEDS TO PREPARE SECURITY STANDARDS NOW FOR COMMERCIAL SPACE TRAVEL

Jared M. Babin
Federal Security Director, TSA, Department of Homeland Security
BA, High Point University, 2007
MPA, College of Charleston, 2009

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
March 2023**

Approved by: Nadav Morag
Co-Advisor

Mollie R. McGuire
Co-Advisor

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The concept of regulating the physical security of commercial spaceports has received little attention. Currently, no federal agency is responsible for developing physical security standards or enforcing regulatory compliance within the industry. This thesis examines the need to create and apply ground-based physical security standards to commercial space facilities within the United States. This thesis explores three policy options as potential paths forward if commercial space travel is designated as critical infrastructure and assesses their effectiveness, cost, political challenges, and viability. The analysis determines that taking proactive measures now will mitigate the potential costs and impacts of an attack and would save substantial amounts of money, keep a burgeoning market on track, and could save lives. Ultimately, this thesis concludes that implementing a regulatory approach like the one employed by the Transportation Security Administration's surface transportation program would be effective if it prevents the explosion of one Falcon 9 rocket, or similar, every approximately 188 years.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AOSC	Aircraft Operator Security Coordinator
AOSSP	Aircraft Operator Standard Security Program
ASP	Airport Security Program
ATLAS	Advanced Threat Local Allocation Strategy
ATSA	Aviation and Transportation Security Act
BASE	Baseline Assessment for Security Enhancement
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
CPI	Consumer Price Index
CSLA	Commercial Space Launch Act
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOS	Department of State
DOT	Department of Transportation
E.O.	Executive Order
EXIS	Exercise Information System
FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
FOP	First Observer Plus
FTE	Full-Time Equivalent
GAO	Government Accountability Office
GSC	Ground Security Coordinators
H.R.	House of Representatives
I.D.	Identification
ISS	International Space Station

NASA	National Aeronautics and Space Administration
MTSA	Maritime Transportation Security Act
OIG	Office of Inspector General
PCSSP	Private Charter Standard Security Screening Program
PIC	Pilot in Command
PPD	Presidential Policy Directive
Rap Back	Record of Arrest and Prosecution Background
SAI	Security Action Items
SD	Security Directive
SETA	Security Enhancement Through Assessment
SPP	Screening Partnership Program
SSI	Sensitive Security Information
STA	Security Threat Assessment
TFSSP	Twelve-Five Standard Security Program
TSA	Transportation Security Administration
TSI	Transportation Security Inspectors
TWIC	Transportation Worker Identification Credential

EXECUTIVE SUMMARY

The concept of regulating the physical security of commercial spaceports has received little attention, and as such, there is no robust literature or government analysis to draw from. However, there is an assumption that commercial spaceport operators have an inherent incentive to provide security for their assets. The security level for each site remains in question and can vary based on the private sector's desire to protect its resources. This lack of uniformity in baseline standards across the industry poses a security threat, giving an opportunity for intelligent actors to inflict damage on these targets. Currently, no federal agency is responsible for developing physical security standards and enforcing regulatory compliance with the industry. This thesis examines the need to create and apply ground-based physical security standards to commercial space facilities within the United States.

This thesis contains a policy options analysis that compares existing regulations surrounding the protection of transportation infrastructure and literature on the successes and failures in physical security applied to the different modes of transport, then assesses methodologies and technologies employed to safeguard critical infrastructure. It next compares the effectiveness, cost, political challenges, and viability (i.e., personnel, administrative burden) of potential paths forward if commercial space travel is designated as critical infrastructure. The policy options analysis conducted explores the pros and cons of applying the various levels of transportation security regulations (e.g., surface, cargo, and aviation). Qualitative and quantitative assessments are applied and ranked for each policy option.[1]

This policy options analysis uses qualitative data to derive scoring relating to effectiveness, political challenges, and viability while using quantitative scoring to assess potential costs. Based on the numerical values assigned for each category, composite scores are derived and compared to the proposed alternatives. Based on the composite scores for

[1] California State University, Long Beach, "670 Steps in Policy Analysis," The Policy Analysis Process, April 16, 2021, https://home.csulb.edu/~msaintg/ppa670/670steps.htm.

each option analyzed, recommendations are made and articulated in this thesis's conclusion.

The analysis uses a uniform assessment rubric to quantify composite scores of the three proposed methods to secure the physical security of spaceport ground-based operations. The assessment criteria provide a composite score by adding the qualitative and quantitative sums of the assessment scores assigned for each measure. Scores ranging from one to five, with one being the least favorable and five being the most favorable, are assigned for each grading criterion—effectiveness, cost, political challenges, and viability—after discussion and analysis of each criterion based on the limited data for each category. Once an assessment of each proposed strategy concludes, a recommendation is made based on each proposed securitization strategy's comparative scores and merits.

The policy options analysis examines three potential schemes that resemble the current ways the Transportation Security Administration (TSA) applies security across the different modes of transportation it regulates and oversees. The first is a regulatory scheme employed for surface transportation that uses a series of security development programs. The second is baseline physical security mechanisms with federal oversight that closely matches current aviation and cargo standards. The third is full federalization of operations, including compliance and physical screening of persons and property. These three potential paths are assessed based on the grading criteria.

The analysis determines that leveraging a regulatory scheme like those used for surface transportation is the most advantageous and cost-effective way to improve the physical security of the 17 spaceports currently in operation. However, the federal government will still have other considerations, such as personnel vetting, cyber security, and other emerging threats. Based on the current threat picture, by utilizing the recommendations outline in this thesis, the federal government would better align itself with the emerging commercial space industry, enabling it to build upon these relationships as the sector grows. Implementing this recommendation will establish a baseline for appropriate measures to safeguard commercial spaceports and accompanying infrastructure, allowing the industry to flourish.

ACKNOWLEDGMENTS

Many people had a direct impact on my success through this program. First and foremost, I want to thank my employees at the Transportation Security Administration El Paso International Airport for their unwavering support and for holding everything down while I pushed through the program and writing this thesis. You have all been the most amazing team and I would put your dedication, commitment, and hard work against anyone. The country is safer because of you.

I am also extremely appreciative for the guidance my advisors, Dr. Mollie McGuire and Dr. Nadav Morag, provided me through this process. Their thoughtful suggestions on how to approach a novel problem provided me with the vision I needed to see this major milestone to fruition. If it wasn’t for their recommendations and insight, I would not have completed this thesis in a timely manner and with a product that makes me proud.

I would also be remiss not to acknowledge the leaders who supported me getting into this program and after. I owe a huge debt of gratitude to Executive Director Carolyn Dorgham, Region Security Director Melvin Carraway, and Federal Security Director Tim Berroyer. You have and continue to provide advice, guidance, and perspective as we navigate the world of transportation security together.

Moreover, I would like to give thanks to all the amazing faculty and staff at the Center for Homeland Defense and Security (CHDS) and all who continually do the great work of providing educational foundations to those who are protecting our great nation. The Naval Postgraduate School (NPS) community is in a league of its own.

Lastly, I will forever be part of Cohort 2105/2106. The lifelong bonds I have made with this group are indelible. You will forever have a piece of my heart and I know this country will be safe with all of you at the helm. You are my brothers and sisters, and our combined strength could overcome any obstacle. You are all amazing.

THIS PAGE INTENTIONALLY LEFT BLANK

I. COMMERCIAL SPACEPORT EXPANSION: GENERATING A NEW WOULD-BE TARGET

A. PROBLEM STATEMENT

What once seemed like science fiction is now becoming a reality. Although the National Aeronautics and Space Administration (NASA) just launched the first human-crewed mission to the International Space Station (ISS) on a commercially developed rocket in May of 2020, multiple billionaires such as Jeff Bezos, Richard Branson, and Jared Isaacman have already launched into space on privately funded commercial spacecraft in 2021.[1] Commercial space travel is cost-prohibitive for most people. Still, it can become a reality for those with at least half a million dollars to burn and represents the first bold step toward making space travel a mode of transportation for the masses.[2] Despite commercial space travel's rapid expansion, there is no standardization of physical security requirements for private-sector ground-based operations and no agency tasked within the federal government to establish security standards and enforce compliance. The Federal Aviation Administration (FAA) is the lead agency for domestic space travel in the United States and almost exclusively focuses on commercial spacecraft safety, not spaceport physical security. The physical security of these installations falls to the private sector entity that owns and operates the spaceport.

The U.S. government has aimed to expand space travel through the private sector since the 1980s when NASA's shuttle could not keep pace with the demand for launching satellites. Since then, interest in speed and innovation has removed many barriers to commercial entry into this industry.[3] The Commercial Space Launch Act (CSLA) of 1984, which named the FAA the regulatory body for commercial space travel, began loosening

[1] "Space: Investing in the Final Frontier," Morgan Stanley, accessed February 3, 2022, https://www.morganstanley.com/ideas/investing-in-space.

[2] Jon Kelvey, "Inspiration4: How Much Does a Ticket to Space Cost?," Inverse, September 15, 2021, https://www.inverse.com/science/inspiration-4-how-much-is-a-ticket-to-space.

[3] Daniel Morgan, *Commercial Space: Federal Regulation, Oversight, and Utilization*, CRS Report No. R45416 (Washington, DC: Congressional Research Service, 2018), https://crsreports.congress.gov/product/details?prodcode=R45416.

regulations. The CSLA has been revised and codified multiple times, the most recent being in 2015. The law extended the "learning period"—during which FAA cannot establish new regulations—to 2023, and authorized third-party indemnification until 2025.[4] However, with the expansion of domestic private-sector space activities and launches, a lack of foresight concerning physical security standards could cripple this burgeoning market, making regulations necessary. There needs to be a balance between allowing the private sector carte blanche and instituting regulation—too much government regulation could hinder advancements, but not enough could create vulnerabilities, resulting in serious consequences for the space program and government interests if exploited.

Until recently, the Department of Homeland Security (DHS) had meaningful contact with commercial space travel only through the National Space Council, created in 1989 and convened for the first time in almost 25 years in 2017.[5] In December 2021, President Biden affirmed President Trump's 2017 Executive Order (E.O.) through an E.O. mandating that the council meet annually.[6] Presently, four cabinet-level departments oversee space activities in the United States: the Department of Commerce (DOC), the Department of Defense (DOD), the Department of State (DOS), and the Department of Transportation (DOT). Each of these departments has subcomponents responsible for different aspects of space-related activities. However, no federal agency is responsible for developing physical security standards and enforcing regulatory compliance within the industry. This thesis examines the need to create and apply ground-based physical security standards to commercial space facilities within the United States.

[4] Space Policy Online, "Space Law," accessed February 7, 2022, https://spacepolicyonline.com/topics/space-law/.

[5] Morgan, *Commercial Space: Federal Regulation, Oversight, and Utilization*, 14.

[6] Exec. Order No. 13655, "Executive Order 13803- Reviving the National Space Council," 82 F.R. 31429 § (2017), https://www.govinfo.gov/content/pkg/FR-2017-07-07/pdf/2017-14378.pdf; White House, "Executive Order on the National Space Council," The White House, December 1, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/01/executive-order-on-the-national-space-council/.

B. RESEARCH QUESTION

How should commercial ground-based space facilities be regulated in terms of physical security?

C. LITERATURE REVIEW

1. Mitigations against Potential Terrorist Attacks

This literature review addresses the primary schools of thought on target hardening, then delves into the scholarly debate on the effectiveness of some of the most employed hardening methods. Finally, it discusses the various countermeasures employed and their effectiveness.

Much debate concerns the hardening, or in other words fortification by applying security measures, of potential targets and the forms they should take. Many argue that the hardening of targets pushes would-be attackers to other target areas and softer targets. Others note that target hardening can intensify the desire of threat actors to attack because hardening increases the symbolic value of the target.[7] Success results even if the attack is unsuccessful. An attack on these targets can be viewed as a symbolic victory and force expenditures to prevent future attacks. Despite the debate on hardening's effectiveness, a sub-debate focuses on which hardening methodologies prove most effective. The discussion revolves around the limited data or highly controlled information on efficacy, leaving many practitioners to compare incomplete data sets or examine fields, such as criminology, for comparative study.

2. Generalized Target Hardening

Despite a successful narrative in terrorism prevention and mitigation, the United States has struggled to keep up with the evolution of terroristic threats.[8] Attack modes of terrorism have changed since 9/11, but groups like al-Qaeda measure success in carnage

[7] Justin V. Hastings and Ryan J. Chan, "Target Hardening and Terrorist Signaling: The Case of Aviation Security," *Terrorism and Political Violence* 25, no. 5 (November 25, 2013): 777–97, https://doi.org/10.1080/09546553.2012.699906.

[8] Lauren O'Brien, "The Evolution of Terrorism Since 9/11," *FBI: Law Enforcement Bulletin 09/01/2011*, September 1, 2011, https://leb.fbi.gov/articles/featured-articles/the-evolution-of-terrorism-since-911.

inflicted on their enemy. However, these groups quickly realized through unsuccessful attacks, as in the case of Richard Reed and the failed shoe bombing, the failed 2006 liquids plot, and the botched Christmas Day 2009 airline bombing, that costly signaling is also an effective strategy. Hastings and Chan argue that target hardening—which applies resources and physical constraints to counteract or dissuade potential attacks—corresponds to an increase in signaling attacks, that is, attacks that demonstrate terrorists' strengths and determinations.[9] Such acts result in large resource expenditures by implementing mitigation methods, personnel, techniques, and technology.[10] Although in partial agreement, Lum et al. attribute this displacement of attacks to hardening but point to the success of target hardening at airports and the creation of the Transportation Security Administration (TSA).[11]

Some contend that the nation still overlooks many areas of transportation security despite the touted successes. Lum, Kennedy, and Sherley and Stein and Levi note a lack of evaluation data on the various countermeasures employed.[12] However, the work done in the aviation security sector receives the most significant attention, and people credit the lack of follow-up attacks after 9/11 as a success. Conversely, Jashari sees the dichotomy between TSA's two leading roles in aviation security—providing security screening and overseeing regulatory compliance—as creating complications and confusion.[13] For example, the entity responsible for protecting the airport public areas lacks clarity in TSA's governing regulations. The TSA aviation security regulations do not refer to public area protections nor mitigations for soft targets: persons or property that lack physical security

[9] Hastings and Chan, "Target Hardening and Terrorist Signaling," 777.

[10] Hastings and Chan, 793.

[11] Cynthia Lum, Leslie W. Kennedy, and Alison Sherley, "Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research," *Journal of Experimental Criminology*, no. 2 (2006): 509, https://doi.org/10.1007/s11292-006-9020-y.

[12] Lum, Kennedy, and Sherley, "Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research"; Janice Gross Stein and Ron Levi, "Testing Deterrence by Denial: Experimental Results from Criminology," *Studies in Conflict & Terrorism*, June 19, 2020, 511, 15, https://www.tandfonline.com/action/showCitFormats?doi=10.1080/1057610X.2020.1777710.

[13] Linda Jashari, "Soft Target Security: Environmental Design and the Deterrence of Terrorist Attacks on Soft Targets in Aviation Transportation" (master's thesis, Naval Postgraduate School, 2018), https://calhoun.nps.edu/handle/10945/58317.

barriers or mechanisms within the airport environment.[14] The lack of responsibility in these public spaces leads to contention and confusion when incidents arise.

The perceived symbolic nature of an attack method can lead to highly diverse responses and countermeasures, but these responses may merely drive different targeting. The literature on the subject demonstrates that attack diversity from domestic terrorist groups and individuals is greater than that of transnational terrorism. Santifort, Sandler, and Brandt show that "the larger attack diversity for domestic terrorism means that effective counter-terrorism policy must thwart more forms of attack than in the case of transnational terrorism."[15] The lack of attack diversity from transnational terrorists may explain the high frequency of failed attempts since 9/11.[16] However, in the post-9/11 timeframe, attacks increasingly focus on softer targets such as large gatherings and private establishments.[17] Lum et al. reiterate this, suggesting that while target hardening at airports statistically reduced the frequency of hijackings, different types of terroristic acts, such as bombings and armed attacks, may have increased in both incidence and lethality.[18] This redirection suggests that as target hardening may work to deter terroristic incursion against an expected or highly symbolic target, attackers commonly seek softer targets.

Although target hardening is a widely accepted form of terrorist mitigation, much debate concerns its effectiveness, especially within the aviation sector. Hastings and Chan lament the TSA's rigid and restrictive countermeasures after each attack and their failure to achieve the intended effect. In contrast, the counter-response aids adversaries in pushing

[14] Jashari.

[15] Charlinda Santifort, Todd Sandler, and Patrick T. Brandt, "Terrorist Attack and Target Diversity: Changepoints and Their Drivers," *Journal of Peace Research* 50, no. 1 (2012): 88, https://doi.org/10.1177/0022343312445651.

[16] Erik J. Dahl, "The Plots That Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States," *Studies in Conflict & Terrorism* 34, no. 8 (July 21, 2011): 621–48; Santifort, Sandler, and Brandt, "Terrorist Attack and Target Diversity," 89.

[17] Patrick T. Brandt and Todd Sandler, "A Bayesian Poisson Vector Autoregression Model," *Cambridge University Press* 20, no. 3 (2012): 312, https://doi.org/:10.1093/pan/mps001.

[18] Lum, Kennedy, and Sherley, "Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research," 504.

their narrative.[19] Moreover, Hsu and McDowall conclude that attacks on hardened targets pertain to symbolism more than casualties. Their research indicates that hardening targets do not correlate to increased occurrences or the deadliness of attacks.

Additionally, Stewart and Mueller deduce that the post-9/11 measures to harden cockpit doors would be cost-effective if they prevented one hijacking every two hundred years. In contrast, two otherwise successful hijacking attempts per year would have to take place to justify the Federal Air Marshal Service (FAMS) cost.[20] Consequently, the effectiveness and unintended consequences of target hardening should be evaluated and debated rather than applying quick and highly reactive mitigation efforts.

Even though specific targets such as aviation undergo massive hardening measures, scholars debate whether other modes of transportation should take a different approach. Haphuriwat and Bier's research offers some insight into the reasons for the variability of security and target hardening between different transportation modes.[21] They find that budgeting for target hardening versus overarching protection could be expected with a small number of high-value targets. Contrastingly, they suggest that when all things are equal regarding target value, providing broad and shared levels of defense is more effective than hardening efforts.[22] Therefore, consideration for target hardening should be dependent, in part, on the volume of targets for a potential attack.

The effectiveness of target hardening, in general, is contested. Examples, such as in the aviation sector, win accolades as successes. However, target hardening consumes extensive resources and lacks sufficient public data about its efficacy. Many scholars conclude that target hardening may result in increased protection. However, as indicated in the literature, the hardening efforts can expand the symbolic value of terrorist targeting.

[19] Hastings and Chan, "Target Hardening and Terrorist Signaling," 793.

[20] Stewart Mg and Mueller J, "Terrorism Risks and Cost-Benefit Analysis of Aviation Security," *Risk Analysis: An Official Publication of the Society for Risk Analysis* 33, no. 5 (May 2013): 893, https://doi.org/10.1111/j.1539-6924.2012.01905.x.

[21] N. Haphuriwat and V.M. Bier, "Trade-Offs between Target Hardening and Overarching Protection," *European Journal of Operational Research* 213, no. 1 (August 16, 2011): 320–28, https://doi.org/10.1016/j.ejor.2011.03.035.

[22] Haphuriwat and Bier, "Trade-Offs between Target Hardening and Overarching Protection."

This effort results in making an unsuccessful attack into a symbolic victory. Scholars also argue that target hardening can have an undesired consequence of supplanting terrorist targeting with softer targets. With a limited number of targets, hardening may provide the best means to secure them. Still, with many targets under threat, a broad approach with shared responsibility may more effectively ensure the security of physical assets.

a. Countermeasures

Threats can come in many forms but are always a result of intelligent actors who are looking to cause damage to a specific target. As Brown et al. point out, practitioners must plan for possible things, not just what subjective assessments suggest are likely to occur. Moreover, unless potential targets are secure through countermeasures or defended, every component should be assumed susceptible to attack.[23] In contrast, Lapham argues that it cannot be assumed that every facility risks attacks from terrorist elements.[24] He also states that the analysis of threats needs to be predictive.[25] Meanwhile, Jaspersen and Montibeller note that some of the best predictors of future attacks can be acquired by studying more recent attacks.[26] They say that terrorist organizations are generally more creative shortly after their founding and move to predictable threat patterns the longer the organization exists.[27]

The countermeasures employed to mitigate or dissuade potential terrorists are vast, but their efficacy varies based on the situation and structure. In a survey of executive-level aviation security personnel conducted by Wallace and Loffi on the use of countermeasures in aviation security to combat insider threats, they note the varying levels of success of background investigations, employee screening, random security checks, and behavior

[23] G. Brown et al., "Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses," *Calhoun: The NPS Institutional Archive*, 2005, 104, https://doi.org/doi 10.1287/educ.1053.0018.

[24] Robert Lapham, *Risk Analysis and Security Countermeasure Selection* (CRC Press, 2015), 125, https://doi.org/10.1201/b18632.

[25] Lapham, 148.

[26] Johannes G. Jaspersen and Gilberto Montibeller, "On the Learning Patterns and Adaptive Behavior of Terrorist Organizations," *European Journal of Operational Research* 282, no. 1 (April 1, 2020): 233, https://doi.org/10.1016/j.ejor.2019.09.011.

[27] Jaspersen and Montibeller, 232.

detection.[28] However, Brown et al. posit that the attacker always has the advantage and that some countermeasures systems are naturally robust while others are not. They state that countermeasure answers are not always obvious and that worst-case scenario analysis should be conducted to mitigate the vulnerability.[29] Aziz et al. add through a game-theoretical resource allocation model that the effectiveness of multiple-compounded security investments directly influences the defensive allocation of budget across many potential targets.[30] Meanwhile, Keohane and Zeckhauser note that "averting actions and amelioration" should be included in the government's ideal policy portfolio and that decreasing the terrorist threat is a public good.[31]

Many argue that there needs to be a concerted effort to provide countermeasures to protect critical infrastructure. Endress states that there needs to be coordination and cooperation between government and non-governmental entities to create and deploy effective and adequate tools and countermeasures to combat threats.[32] He says this will likely include a combination of technological detection, surveillance, tracking, and imaging capabilities and conventional means such as roving patrols and air monitoring systems.[33] Wiater adds to this when discussing public-private partnerships in critical infrastructure protection, noting that the state cannot divest itself of its obligation to provide security within the homeland, but that the government must also realize that private sector expertise should not be overlooked.[34] She states that introducing legal requirements on

[28] Ryan Wallace and Jon M. Loffi, "The Unmitigated Insider Threat to Aviation (Part 2): An Analysis of Countermeasures," *Springer Science + Business Media* 7 (September 2014): 307–31, https://doi.org/10.1007/s12198-014-0150-6.

[29] Brown et al., "Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses," 120.

[30] Ridwan Al Aziz, Meilin He, and Jun Zhuang, "An Attacker–Defender Resource Allocation Game with Substitution and Complementary Effects," *Risk Analysis* 40, no. 7 (July 1, 2020): 1481–1506, https://doi.org/10.1111/risa.13483.

[31] Nathaniel O. Keohane and Richard J. Zeckhauser, "The Ecology of Terror Defense," *The Journal of Risk and Uncertainty* 26, no. 2/3 (2003): 224.

[32] Christian Endress, "Critical Infrastructure Protection – Strategies and Technologies," *Military Technology* 31, no. 7 (2007): 79–80.

[33] Endress.

[34] Patricia Wiater, "On the Notion of 'Partnership' in Critical Infrastructure Protection on JSTOR," *Cambridge University Press* 6, no. 2 (n.d.): 259.

private sector critical infrastructure protection is the government's only real recourse. She notes that instituting binding contracts of regulation between the government and industry regarding critical infrastructure protection "may serve as a promising compromise between a laissez-faire approach and regulation."[35] However, she points out that if these types of contracts fail, the government has no choice but to implement more rigid regulations and monitor compliance.[36] However, Jaksec argues that the best way to protect critical infrastructure is for the government to develop and implement security standards and create more incentives. Such incentives include indemnification and tax breaks to drive motivation to increase security countermeasures.[37]

b. Summary

There are varying opinions regarding the hardening of potential targets and the means of doing so. Some suggest that target hardening leads to the unforeseen consequence of pushing terrorists' attention elsewhere to less fortified and susceptible locations. Even unsuccessful attack attempts can, and are, seen as a symbolic victory. Therefore, many recommend a shared and overarching responsibility and approach between the government and private sector to thwart potential incidents. Moreover, even after a consensus that something is a potential target, there remains the matter of providing protection effectively and efficiently. There are examples, such as the successes in fortifying the commercial aviation sector. However, the lack of publicly available data for other areas of transportation makes it difficult to gauge the effectiveness of established programs.

D. RESEARCH DESIGN

This thesis provides a policy options analysis based on three case studies examining how TSA regulates surface, cargo, and aviation security as possible means to safeguard commercial space travel ground-based operations. Acknowledging the vast complexity of

[35] Wiater, 262.

[36] Wiater, 262.

[37] Gregory M. Jaksec, "Public-Private-Defense Partnering in Critical Infrastructure Protection" (master's thesis, Monterey, California. Naval Postgraduate School, 2006), 33, https://calhoun.nps.edu/handle/10945/2878.

systems within these operations, this thesis does not examine all security aspects or address safety. It focuses on the physical security of these locations within the United States. Moreover, this thesis does not address the myriad of legal issues involving international space law nor the current jurisdictional challenges between the various agencies under the components of DOD engaged in space, NASA, or the FAA. Additionally, cyber security, logistical security of components transiting to and from facilities, and other matters outside U.S. territory are not discussed. Instead, this policy options analysis involves a combination of qualitative and quantitative analysis of existing transportation security programs to provide baseline physical security standards for ground-based commercial space operations.

Since commercial space operations are still relatively novel, three existing transportation security programs were examined to look for best practices for protecting the physical security of ground-based commercial space infrastructure. The overarching surface, cargo, and aviation transportation security programs are the basis for this examination. Based on the best practices of these current modes of transportation, three policy options for safeguarding the physical security of ground-based commercial space operations were assessed through a policy options analysis for ground-based commercial space operations. The three options assessed consist of a regulatory scheme that mirrors TSA's approach regarding surface transportation, a method resembling regulatory compliance for commercial aviation and cargo operations, and complete federalization of commercial spaceport security.

Comparisons are made using the existing regulations surrounding the protection of transportation infrastructure, literature on the successes and failures in physical security applied to the different modes of transport, and an assessment of methodologies and technologies employed to safeguard critical infrastructure. This thesis compares the effectiveness, cost, political challenges, and viability (i.e., personnel, administrative burden) of potential paths forward if commercial space travel is designated as critical infrastructure. This policy options analysis explores the pros and cons of applying the various levels of transportation security regulations (e.g., surface, cargo, and aviation). Qualitative and quantitative assessments are applied and ranked for each policy option.[38]

For this policy options analysis, qualitative data derive scoring relating to effectiveness, political challenges, and viability, while quantitative scoring assesses potential costs. Based on the numerical values assigned for each category, composite scores were derived, and the proposed alternatives are compared. Based on the composite scores for each option analyzed, recommendations are made in this thesis's conclusion.

For the analysis, a uniform assessment rubric quantifies composite scores of the three proposed methods to secure the physical security of spaceport ground-based operations. The assessment criteria provide a composite score by adding the qualitative and quantitative sums of the assessment scores assigned for each measure. Scores ranging from one to five, with one being the least favorable and five being the most favorable, were assigned for each grading criteria (e.g., effectiveness, cost, political challenges, and viability) after discussion and analysis of each criterion based on the limited data for each category. Once the assessment was completed for each proposed strategy, a recommendation is made based on each proposed securitization strategy's comparative scores and merits. The assessment rubric used is shown in Table 1.

[38] California State University, Long Beach, "670 Steps in Policy Analysis."

Table 1. Assessment Rubric

Criterion	1	2	3	4	5	Composite Score
Effectiveness	Provides the least amount of securitization	Provides some securitization but is less than moderate	Provides a moderate level of securitization	Provides an improved level of securitization	Considered completely hardened	
Cost	Extreme cost	High level of cost	Moderate cost	Above minimal cost	Least cost	
Political Challenges	Almost no political support	Tough opposition- a great deal of scrutiny	Split decision but still able to implement	Some opposition but relatively easy support	Easily implemented with little to no opposition	
Viability	Extremely difficult to implement and sustain	High level of difficulty in implementing and sustaining	Moderately difficult to implement and sustain	Low difficulty in implementing and sustaining	Little to no difficulty in implementing and sustaining	

a. Assumptions

For this analysis, assumptions regarding the threat scenario and associated costs are necessary. Other assumptions regarding effectiveness, cost, political challenges, and viability were established. This analysis used the direct cost of infrastructure replacement and associated economic losses resulting from the attack scenario. However, the analysis did not consider the costs associated with the loss of human life. Additionally, other figures and estimates were approximated based on established transportation security modes, as direct impacts prove challenging to obtain at this time.

Additionally, the calculation of the actual cost of vetting is not accounted for separately, as there is an assumption that there is some level of government vetting in all the policies analyzed. The form of this vetting may differ dependent on the approach taken by federal regulation. However, this paper assumes that some level of vetting is necessary to ensure the reduced potential impact of insider threat vulnerabilities. Vetting could be a Transportation Worker Identification Credential (TWIC), Record of Arrest and Prosecution Background (Rap Back), or any other periodic background investigation and will likely vary based on the expansion of the space programs.

Moreover, the analysis factored in the reported number of employees working in the commercial space field as of 2020. There is an assumption that the industry will continue to grow as it did even amid a global pandemic by roughly 3.2%.[39] As of 2020, the private sector employed 147,953 employees in various capacities.[40] For this analysis, 150,000 employees serve as the benchmark, assuming that the industry has and will continue to grow based on the past trajectory of employment and the expansion of commercial space endeavors.

b. Threat Scenario and Cost Estimate

Although some contend that a worst-case analysis is the preferred metric to assess potential countermeasures,[41] this analysis used a reduced worst-case scenario for comparative purposes—the estimated cost of losing a commercial rocket and the delays in future launches. To this end, the analysis used the cost associated with the Falcon 9 rocket explosion in 2016 and its impact on subsequent launches as our impact figure. As SpaceX is not a public institution, exact cost figures are not obtainable. However, some estimates cite that the company may have lost upwards of $740 million due to the incident.[42] When adjusted for inflation, this equates to approximately $910 million in 2022 dollars based on the Consumer Price Index (CPI) inflation calculator of the U.S. Bureau of Labor Statistics. The target is $910 million USD for forthcoming analysis.[43]

[39] Ramona Schindelheim, "Private Companies Propelling Job Growth in the Space Industry," *WorkingNation* (blog), June 2, 2021, https://workingnation.com/private-companies-propelling-job-growth-in-the-space-industry/.

[40] Schindelheim; OECD, "Remedying the Gender Gap in a Dynamic Space Sector," OECD iLibrary, 2022, https://www.oecd-ilibrary.org/sites/c5996201-en/1/2/3/index.html?itemId=/content/publication/c5996201-en&mimeType=text/html&_csp_=ffe5a6bbc1382ae4f0ead9dd2da73ff4&itemIGO=oecd&itemContentType=book.

[41] Brown et al., "Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses," 120.

[42] Dave Mosher, "SpaceX Lost a Quarter of a Billion Dollars after One of Its Rockets Blew Up," *Business Insider*, January 13, 2017, https://www.businessinsider.com/spacex-financials-rocket-accident-costs-revenue-2017-1.

[43] "CPI Inflation Calculator," accessed August 31, 2022, https://www.bls.gov/data/inflation_calculator.htm.

c. Effectiveness

The basis for the effectiveness evaluation of the three proposed measures to securitize ground-based commercial spaceports is an assessment of the current programs employed by the TSA to secure aviation, cargo, and surface transportation systems. These are government security programs. Therefore, direct data on effectiveness is unobtainable for this paper due to the classification and security concerns revolving around it. However, the analysis leverages many open-source reports and Congressional findings to assess the proposed securitization strategies qualitatively.

d. Cost

The measure of cost-effectiveness, although difficult to quantify, is an assessment of the perceived reduction in the likelihood that the threat scenario is deterred or thwarted by the security measure. This cost-effectiveness measures the proposed policy based on existing transportation security programs. The assessment uses the costs associated with the above threat scenario to evaluate the proposed policies. This cost is then compared to the potential cost to the government and U.S. taxpayers to provide varying levels of securitization. Personnel and administrative costs from the TSA's Budget Overview for FY 2023 are the basis for calculating the estimated costs associated with each proposal. The analysis uses figures from the FY 2021 enacted budget. These figures factor in carryover funds and other surplus allocations. For simplification purposes, the analysis uses the TSA's estimate of federalized airports as a denominator for analysis and breakdown of estimates of personnel and administrative costs accordingly. The analysis then applies these estimates vis-à-vis numerical comparison of airports to current spaceports within the United States. Total cost comparison for each proposed policy is rendered through total government expenditure per program size based on the current number of spaceport operations.

e. Political Challenges

Information is used from the implementation of the comparative TSA programs to gauge the political challenges surrounding the implementation of the three proposed policies. A literature review is conducted to extrapolate the level of scrutiny applied to the various program options. Based on this review, assumptions are made that commensurate levels of support or opposition will follow for the proposed securitization strategies. Based on the review, subjective scores are assigned through a logical assessment of support and opposition.

f. Viability

The viability assessment is conducted on each of the proposed policies. Scoring is based on the scalability of existing programs utilized for other critical transportation infrastructure. Values are assigned based on the scalability of existing programs, maturity, and the estimated time to implement each proposal. Higher scores are assigned to securitization efforts that more easily leverage existing programs and require less start-up effort to initiate the program's rollout. Consideration is given to how the proposed policy would integrate into existing government transportation infrastructure protection programs.

g. Overall Assessment

Based on the case studies explored, a policy options analysis was conducted for each of the three cases (e.g., surface, cargo, and aviation). Each of the options are assessed using the grading rubric for each of the criteria (e.g., effectiveness, cost, political challenges, and viability), and composite scores were derived. A comparison of the three options are discussed, and a final recommendation is made using the composite scores and overall assessment of each option.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter discusses the burgeoning transportation sector of commercial space travel. Due to the United States government's desire to allow private sector expansion and efficiency to drive innovation and break down bureaucratic barriers, the expansion of regulations on this promising industry has been lifted. As such, commercial space travel has not yet been given the critical infrastructure designation and is, therefore, currently treated very differently than other modes of transportation that are more established. In the following subsections, attacks on transportation systems and the resulting mitigations, the current regulations of other modes of transportation, and the current mechanisms for employee and passenger vetting are discussed.

A. ATTACKS ON TRANSPORTATION AND THE RESULTING MITIGATIONS

Modes of transportation have been prime targets of terrorism for decades. Aviation has been an ideal and symbolic target since the 1960s even though it did not come into the mainstream as a form of travel until the early 1950s. However, methods of targeting aviation and other modes of transportation have changed drastically. In the United States, pre-9/11, hijacked planes were expected to go to Cuba or seek a ransom, not for terrorism purposes. Despite the rise in aviation hijackings from the 1950s through the 1970s, it was not until 1973 that the U.S. mandated screening passengers and their accessible property for commercial flights. However, the airline industry in the United States was not inclined to implement intrusive screening practices like in other countries, such as Israel, due to several customer service concerns and public resistance.[44]

Additionally, it took the 1988 bombing of Pan Am flight 103 over Lockerbie, Scotland, to require that all checked baggage be inspected before being loaded onto passenger airplanes.[45] Despite that the "number of transnational terrorist incidents have

[44] Alex P. Schmid, *Handbook of Terrorism Prevention and Preparedness*, 1st ed. (The Hague: ICCT Press, 2020), 817, 10.19165/2020.6.0126.

[45] R. William Johnstone, *Protecting Transportation: Implementing Security Policies and Programs* (Oxford, UNITED STATES: Elsevier Science & Technology, 2015), 21, PoQuest.

fallen by about 40 percent since the start of the 1990s…each incident was much more likely to involve casualties since then."[46] This trend has forced the world to increase mitigation efforts and drastically enhance security at airports and other transportation facilities.

Some argue that many areas of transportation security are still being overlooked despite the touted successes. The notion that passenger aircraft could be weaponized was not at the forefront of most people's minds. Therefore, the events of 9/11 sparked the creation of the Transportation Security Administration to ensure more robust protections. The TSA now provides federalized security screening of passengers and property on commercial aircraft. Additionally, the agency regulates aviation, cargo, and surface transportation modes in accordance with the Aviation and Transportation Security Act (ATSA) [47] Each of these transportation sectors represents extensive and diverse components comprised of various domestic and international nodes. However, the work done in the aviation security sector receives the most significant attention, and people credit the lack of follow-up attacks after 9/11 as a success.

Conversely, some see the dichotomy between TSA's two prominent roles in aviation security, providing security screening and overseeing regulatory compliance, as creating complications and confusion.[48] For example, the entity responsible for protecting the airport public areas lacks clarity in TSA's governing regulations. The governing regulations of TSA aviation security do not refer to public area protections nor mitigations for soft targets, described as persons or property that lack physical security barriers or

[46] Khusrav Gaibulloev and Todd Sandler, "What We Have Learned about Terrorism since 9/11," *Journal of Economic Literature* 57, no. 2 (June 2019): 320, https://doi.org/10.1257/jel.20181444.

[47] "Civil Aviation Security: General Rules," 49 C.F.R. 1540 (2002), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1540; "Airport Security," 49 C.F.R. 1542 (2002), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542; "Aircraft Operator Security: Air Carriers and Commercial Operators," 49 C.F.R. 1544 (2002), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1544; "Foreign Air Carrier Security," 49 C.F.R. 1546 (2002), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1546; "Aviation Security – Indirect Air Carrier Security," 49 C.F.R. 1548 (2002), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1548; "General Rules," 49 C.F.R. 1570 (2020), https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1570.

[48] Linda Jashari, "Soft Target Security: Environmental Design and the Deterrence of Terrorist Attacks on Soft Targets in Aviation Transportation" (Monterey, CA, Naval Postgraduate School, 2018), https://calhoun.nps.edu/handle/10945/58317.

mechanisms within the airport environment.[49] The lack of responsibility in these public spaces leads to contention and confusion when incidents arise.

Despite a successful narrative in terrorism prevention and mitigation, some believe the United States has struggled to keep up with the evolution of terroristic threats. Attack modes of terrorism have changed since 9/11, but groups like al-Qaeda measure success in terms of carnage inflicted on their enemy. However, these groups quickly realized through unsuccessful attacks, as in the case of Richard Reed and the failed shoe bombing, the failed 2006 liquids plot, and the botched Christmas Day 2009 airline bombing, that costly signaling is also an effective strategy. Target hardening can equate to increasing signaling attacks—that is, attacks that demonstrate terrorists' strengths and determination. The effects of such acts result in large resource expenditures through implementing mitigation methods, personnel, techniques, and technology.[50] Therefore, some caution should be applied to hardening for would-be targets, as too much may result in terrorists supplanting one target for another, less hardened one.

The perceived symbolic nature of an attack method can lead to highly diverse variations of response and countermeasures, but these responses may merely drive different targeting. A review of attacks demonstrates that attack diversity from domestic terrorist groups and individuals is greater than that of transnational terrorism. Santifort, Sandler, and Brandt show that "the larger attack diversity for domestic terrorism means that effective counter-terrorism policy must thwart more forms of attack than in the case of transnational terrorism."[51] The lack of attack diversity from transnational terrorists may explain the high frequency of failed attempts since 9/11.[52] However, in the post-9/11 timeframe, attacks increasingly focus on softer targets such as large gatherings and private establishments.[53] Lum, Kennedy, and Sherley reiterate this, suggesting that while target

[49] Jashari, 37.

[50] Hastings and Chan, "Target Hardening and Terrorist Signaling," 793.

[51] Santifort, Sandler, and Brandt, "Terrorist Attack and Target Diversity," 88.

[52] Dahl, "The Plots That Failed"; Santifort, Sandler, and Brandt, "Terrorist Attack and Target Diversity," 89.

[53] Brandt and Sandler, "A Bayesian Poisson Vector Autoregression Model," 312.

hardening at airports statistically reduced the frequency of hijackings, different types of terroristic acts, such as bombings and armed attacks, may have increased in both incidence and lethality.[54] This redirection suggests that as target hardening may work to deter terroristic incursion against an expected or highly symbolic target, attacks are commonly pushed to other, softer targets.

Even though specific targets such as aviation undergo massive hardening measures, scholars debate whether other modes of transportation should take a different approach. As noted earlier, Haphuriwat and Bier's research and analysis give some insight into the reasons for the variability of security and target hardening between different transportation modes. They find that budgeting for target hardening versus overarching protection could be expected to be seen where there is a small number of high-value targets. Contrastingly, they note that when all things are equal regarding target value, providing broad and shared levels of defense is more effective than hardening efforts. This is especially true when the total number of potential targets is expansive, broad, and geographically diverse.[55] The types of attacks terrorists can perpetrate are boundless.[56] Therefore, commensurate measures must be put in place to impede attacks. Not everything can be nor should be hardened just because it has been or may be a desirable target.

Surface transportation is vastly complex and expansive, making it challenging to harden or secure. Think of the numerous railroads, light rail, bus terminals, highway systems, pipelines, and other means of transportation that fall under the surface label. This complexity does not reduce the attractiveness of surface transportation. The imagery of a train plummeting into a ravine provided such a stunning picture that it became al-Qaeda's obsession after 9/11. Files recovered from Osama bin Laden's hideout after his death in 2011 showed plans for derailment attacks to commemorate the tenth anniversary of the 9/

[54] Lum, Kennedy, and Sherley, "Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research," 504.

[55] Haphuriwat and Bier, "Trade-Offs between Target Hardening and Overarching Protection," 326.

[56] Radoslav Ivančík and Pavel Nečas, "Air Transport Terrorism: One of the Most Feared Types of Asymmetric Security Threat" 2020, 233, ProQuest

11 attacks.[57] Attacks against passenger rail have resulted in extensive death tolls, such as the 2005 London bombing, where fifty-two people were killed, and the 2006 Mumbai attack claiming 209 lives.

Nevertheless, implementing aviation-style screening and oversight has not happened because the costs would be astronomical, and the measures would render the systems almost inoperable. Therefore, unlike aviation, surface transportation security is the responsibility of the owners and operators because it is too large for one entity to handle. These transit modes are exceedingly difficult to secure because they are specifically designed to move people and commerce quickly with minimal obstruction.[58] However, the TSA collaborates with its industry partners to bolster its programs and provides critical training and outreach activities.[59] Regardless, security professionals need to take steps to secure all modes of transportation from attack. They will remain high-value targets for terrorist actors in the United States and abroad.

B. RELEVANT REGULATIONS COVERING TRANSPORTATION CRITICAL INFRASTRUCTURE

Numerous parts under 49 Code of Federal Regulations (CFR) govern transportation security. Title 49 of the CFR Part 1540 outlines the general rules for civil aviation security. Part 1542 handles an airport's responsibilities, and Part 1544 pertains to domestic air carrier requirements, establishing the bulk of the aviation-related provisions in the U.S. These parts require airport-specific security plans regulated by the TSA.[60] These security programs are scaled based on the size of the operations, risks associated with the aircraft flying out of the port, and the maximum passenger capacity of the planes being utilized.

[57] Schmid, *Handbook of Terrorism Prevention and Preparedness*, 834.

[58] Annelie Holgersson and Ulf Bjornstig, "Mass-Casualty Attacks on Public Transportation" *Journal of Transportation Security,* 7, no. 1 (2013): 2, http://dx.doi.org/10.1007/s12198-013-0125-z.

[59] Transportation Security Administration, "TSA Surface Transportation Security" (Washington, DC, February 2020), 3, https://www.tsa.gov/sites/default/files/guidance-docs/surface_101_to_stakeholders_0.pdf.

[60] Civil Aviation Security: General Rules; Airport Security; Aircraft Operator Security: Air Carriers and Commercial Operators.

Moreover, 49 CFR Part 1546 adds additional requirements for foreign air carriers.[61] Although these regulations are not all-encompassing, they set a baseline for security standards for the industry most closely related to ground-based commercial space activities.

In addition to the regulations that govern commercial aviation, other transportation sector requirements are also pertinent. Title 49 Part 1548 deals with Indirect Air Carrier (IAC) security requirements. Part 1548 is the governing regulation for cargo screening and facility requirements failing outside of a complete program under Parts 1544 and 1546. Like all the previously mentioned aviation program-related requirements, there is mandatory training on security for those working within this sphere and a need to establish designated security coordinators to oversee specific security programs.[62] Moreover, Part 1570 of 49 CFR deals with surface transportation, which encompasses rail, mass transit, pipeline, cyber and other concerns.[63] This program focuses more broadly on developing these entities to increase security standards. Transportation Security Inspectors' (TSI) work in the surface mode of transportation varies from the rest of the agency's TSIs. There is a focus on non-regulatory functions that require voluntary participation by regulated entities. These programs generally serve the various surface entities that aim to increase their security posture through outreach events, security upgrade recommendations, and training exercises. Many of the programs have follow-on components that allow regulated entities to evaluate their mode-specific security plans so that they may focus on areas of deficiency. The regulatory requirements are minimal, and public and private entities are encouraged to self-report incidents for further investigation.[64] A risk-based approach is taken, and tasks are prioritized based on perceived need.[65]

[61] Foreign Air Carrier Security.

[62] Department of Transportation and Homeland Security, Aviation Security – Indirect Air Carrier Security.

[63] General Rules.

[64] Government Accountability Office, "Surface Transportation Security: TSA Has Taken Steps to Improve Its Surface Inspector Program, but Lacks Performance Targets," Congressional (Washington, DC, July 2020), ProQuest.

[65] Transportation Security Administration, "TSA Surface Transportation Security," 3.

C. VETTING

Employee and passenger vetting is prominent among transportation sector security requirements. Under the security programs discussed previously, there are many employee vetting mechanisms and barriers to entry for those with criminal or terroristic backgrounds to combat potential insider threat situations. This section will first discuss the tools for vetting employees working in the transportation sector. Per TSA Security Directives (SD) and individual Airport Security Programs (ASP), airport employees must undergo fingerprinting and a Criminal History Records Check (CHRC) before being issued airport-specific Identification (ID) media.[66] Additionally, many airports and other public and private entities have enrolled in the Federal Bureau of Investigation's (FBI) Rap Back, which provides for continuous vetting of employees using collected biometric trackers.[67]

There is also a unique form of vetting and badging specific to the transportation sector, Transportation Worker Identification Credential (TWIC). The TWIC program was established under the Maritime Transportation Security Act (MTSA) and required certain transportation workers to undergo TSA's Security Threat Assessment (STA). The credential serves three purposes: First, it establishes a person's identity. Second, it indicates that the individual in possession of the credential is a licensed TWIC holder. Third, it alerts if the individual has legitimate business at a transportation facility.[68] The TWIC requirements come under Title 33 Part 101.[69]

Regarding vetting passengers frequenting commercial aircraft, TSA's Secure Flight Program is tasked with gathering information travelers provide at the time of booking and then vetting it against watchlists to assign a risk score for each passenger. The Secure Flight

[66] Wallace and Loffi, "The Unmitigated Insider Threat to Aviation (Part 2)," 310.

[67] Ava Kofman, "The FBI Is Building a National Watchlist That Gives Companies Real-Time Updates on Employees," *The Intercept*, February 4, 2017, https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/.

[68] Heather J. Williams, and Kristin Van Abel et al., *The Risk-Mitigation Value of the Transportation Worker Identification Credential: A Comprehensive Security Assessment of the TWIC Program* (RAND Corporation, 2020), xi, https://www.rand.org/pubs/research_reports/RR3096.html.

[69] "TWIC Requirement," 33 C.F.R. 101.514 (2016), https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-E/section-101.514.

Program allowed TSA to launch the TSA Pre√ program in October 2011 after Kenneth Fletcher proposed the risk-based model.[70] Although the model has been refined over the years, it is essentially the same as when it was rolled out. TSA Pre√ allows for greater efficiencies in security screening by focusing on unknown or high-risk individuals and applying commensurate screening to these passengers while relaxing security screening for the pre-vetted population.

[70] Laura A Albert et al., "A Review of Risk-Based Security and Its Impact on TSA PreCheck," *Operations Engineering & Analytics* 53, no. 6 (2021): 657, https://doi-org.libproxy.nps.edu/10.1080/24725854.2020.1825881; Kenneth C Fletcher, "Aviation Security: A Case for Risk-Based Passenger Screening" (master's thesis, Naval Postgraduate School, 2011), 174, Calhoun, http://hdl.handle.net/10945/10601.

III. A CASE FOR DESIGNATING COMMERCIAL SPACE TRAVEL AS CRITICAL INFRASTRUCTURE

Space exploration is considered the final frontier. The United States populace now lives in an age where space travel is more of a reality than at any time in human history. Still, as has been seen through previous disasters, many punctuating events can set an industry back. To this end, many players are involved with space activities in the United States. The space exploration industry is no longer an inherently governmental function as the demand has grown significantly. In contrast, NASA and the American taxpayer grew unable to keep up with the imagination and ingenuity of the private sector and its envisioned applications. With increased demand and expansion of space activities by the private sector come concerns over infrastructure protection.

Many agencies are engaged in a multitude of ways to secure space assets. However, most focus on risks posed by state-based actors, threats after launch, or cyber-based threats. There is currently no agency focused exclusively on the physical security of ground-based commercial space operations, and the literature on the topic is minimal. As pointed out by Abeyratne, "on the subject of sub-orbital flights [,] space security has generally escaped the scrutiny of both academics and professionals."[71] Therefore, the discussion will begin with the security requirements of similar modes of transportation, threats to other comparable infrastructure, and various mitigation techniques that could be used to secure ground-based commercial spaceports.

The U.S. government dictates the sectors that receive the designation "critical infrastructure," and there are currently sixteen distinct sectors laid out under Presidential Policy Directive (PPD) 21, of which the transportation sector is part.[72] Each critical infrastructure sector is vast, and how critical infrastructure is defined has been continually

[71] Ruwantissa Abeyratne, "Commercial Space Travel: Security and Other Implications," *Journal of Transportation Security*, no. 6 (2013): 257, https://doi.org/10.1007/s12198-013-0115-1.

[72] CISA, "Critical Infrastructure Sectors," Critical Infrastructure Sectors, accessed March 22, 2022, https://www.cisa.gov/critical-infrastructure-sectors.

refined as advancements are made, and potential threats evolve.[73] The transportation sector comprises aviation, highway, maritime, mass transit and passenger rail, pipeline, freight rail, and postal and shipping.[74] Additionally, many government agencies and actors safeguard critical infrastructure within the U.S. and interests abroad. Currently, "space systems, services, and technology" are not considered critical infrastructure.[75] However, a bill, House of Representatives (H.R.) 3713, has been introduced in the House of Representatives to provide these space activities with critical infrastructure status.[76]

Commercial ground-based spaceports are expanding across the United States. There are currently fourteen FAA-licensed launch sites spanning ten states. However, three exclusive-use sites are not FAA licensed, all in Texas. Additionally, there are only two FAA-licensed reentry sites, located in Huntsville, Alabama, and Cape Canaveral, Florida. Figure 1 shows the current locations of these facilities.

[73] Colleen M. Newbill, "Defining Critical Infrastructure for a Global Application," *Indiana Journal of Global Legal Studies* 26, no. 2 (2019): 778.

[74] "Transportation Systems Sector | CISA," accessed March 22, 2022, https://www.cisa.gov/transportation-systems-sector.

[75] Lieu, "Space Infrastructure Act," Pub. L. No. H.R.3713 (2021), https://www.congress.gov/117/bills/hr3713/BILLS-117hr3713ih.pdf.

[76] Lieu.

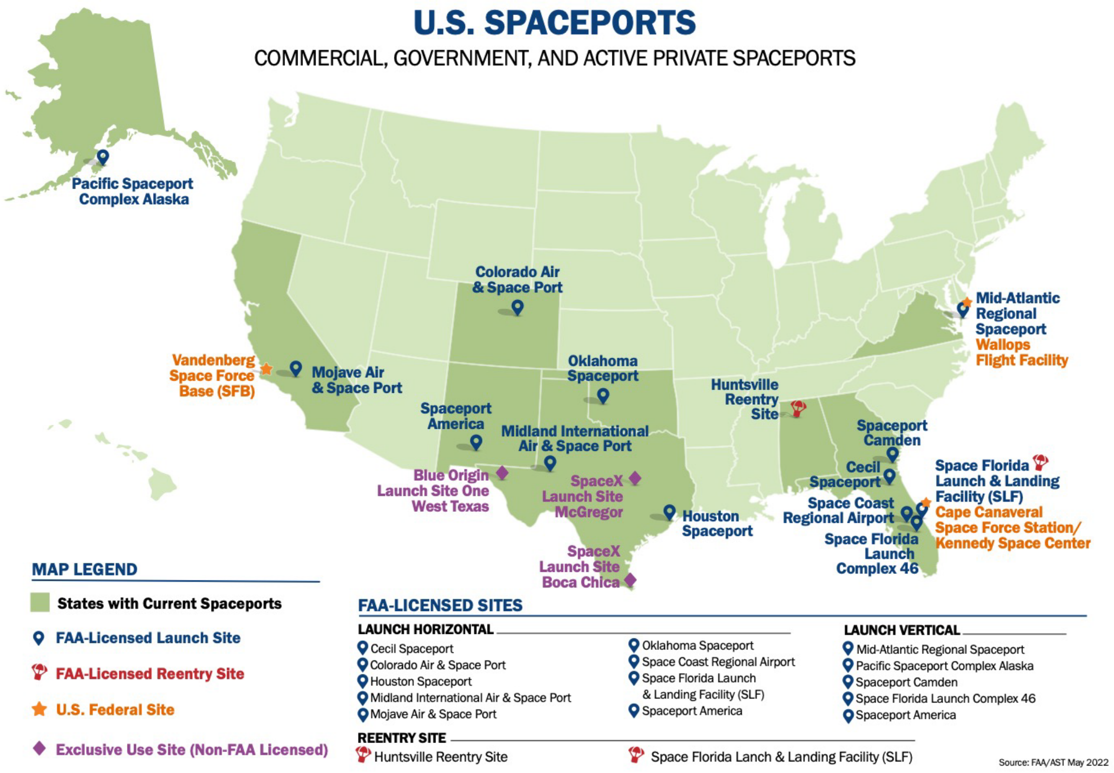
U.S. SPACEPORTS
COMMERCIAL, GOVERNMENT, AND ACTIVE PRIVATE SPACEPORTS
Pacific Spaceport Complex Alaska
Colorado Air & Space Port
Mid-Atlantic Regional Spaceport
Wallops Flight Facility
Vandenberg Space Force Base (SFB)
Mojave Air & Space Port
Oklahoma Spaceport
Huntsville Reentry Site
Spaceport America
Midland International Air & Space Port
Spaceport Camden
Blue Origin Launch Site One West Texas
SpaceX Launch Site McGregor
Cecil Spaceport
Space Florida Launch & Landing Facility (SLF)
Space Coast Regional Airport
Cape Canaveral Space Force Station/ Kennedy Space Center
Houston Spaceport
Space Florida Launch Complex 46
SpaceX Launch Site Boca Chica
MAP LEGEND
States with Current Spaceports
FAA-Licensed Launch Site
FAA-Licensed Reentry Site
U.S. Federal Site
Exclusive Use Site (Non-FAA Licensed)
FAA-LICENSED SITES
LAUNCH HORIZONTAL
Cecil Spaceport
Colorado Air & Space Port
Houston Spaceport
Midland International Air & Space Port
Mojave Air & Space Port
Oklahoma Spaceport
Space Coast Regional Airport
Space Florida Launch & Landing Facility (SLF)
Spaceport America
LAUNCH VERTICAL
Mid-Atlantic Regional Spaceport
Pacific Spaceport Complex Alaska
Spaceport Camden
Space Florida Launch Complex 46
Spaceport America
REENTRY SITE
Huntsville Reentry Site
Space Florida Lanch & Landing Facility (SLF)
Source: FAA/AST May 2022

Figure 1. U.S. Spaceports Map[77]

Since domestic space operations have not been established as critical infrastructure and do not have the accompanying requirements set, this thesis examines the security regulations of the most closely related sector with the critical infrastructure designation, transportation. Within this sector, there are various modes, such as the SpaceX Launch Facility shown in Figure 2. Each of these areas has specific regulations that govern the security requirements. The Code of Federal Regulations codifies the security requirements associated with each transportation segment and accompanying protocols to combat threats and mitigate the introduction of threat items into the system. As Shmuel Bar has noted, "many of the most spectacular terrorist acts in the last decades were perpetrated against- or

[77] Source: Federal Aviation Administration, *Spaceport Map,* May 13, 2022), https://www.faa.gov/space/spaceport-map.

using- mass public transportation such as aircrafts, trains, buses, and even cruise ships."[78] Therefore, transportation remains a prominent target for those looking to engage in nefarious activities. Murray-Tuite and Fei amplify this by stating, "terrorist attack scenarios have extremely small probabilities of occurrence, but should not be treated as zero, even if a specific attack has never previously occurred, as long as the possibility exists that the scenario could be executed."[79]

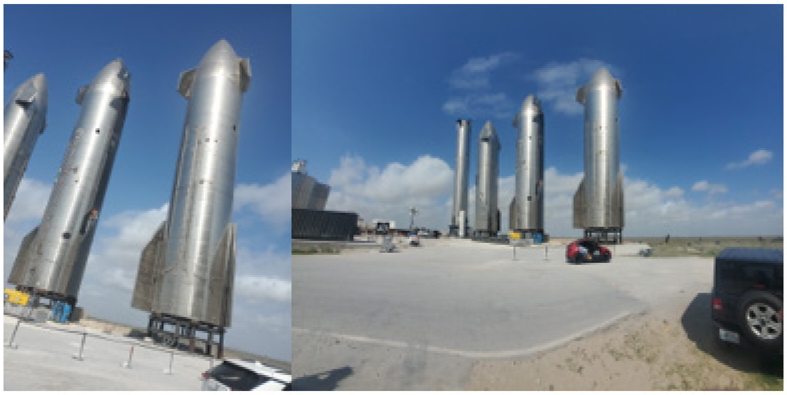

Figure 2. SpaceX Launch Facility Brownsville, TX [80]

Although commercial space launch sites have not been a primary target of terrorism, the lack of baseline security standards leaves commercial space infrastructure vulnerable to would-be attackers. Spaceport physical security has not garnered much attention. The possibility remains that terrorists may target space launch facilities and infrastructure for many reasons and beliefs ranging from national ideology to neo-anarchism or for antitechnology purposes.[81] It has been said that the attacks of 9/11 are

[78] Shmuel Bar, *Securing Transportation Systems*, ed. Simon Hakim, Gila Albert, and Yoram Shiftan (New York: John Wiley & Sons, Inc., 2015), ProQuest.

[79] Pamela M. Murray-Tuite and Xiang Fei, "A Methodology for Assessing Transportation Network Terrorism Risk with Attacker and Defender Interactions," *Computer-Aided Civil and Infrastructure Engineering* 25 (2010): 398, https://doi.org/10.1111/j.1467-8667.2010.00655.x.

[80] Source: Corina Armendariz, "SpaceX Launch Facility- Brownsville, TX," April 10, 2022.

[81] Gregory D. Miller, "Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists: Nonstate Threats in Space," *Air & Space Power Journal* 33, no. 3 (2019): 39.

attributable to a failure of imagination.[82] The United States should not have another failure of imagination regarding commercial space travel. Therefore, action should be taken to designate this sector as critical infrastructure to open the door to providing safeguards to fortify this industry from attack. The rest of this thesis examines possible options for doing so. Regardless, Congress will need to take action to incorporate commercial space infrastructure as critical before any securitizing policy can be instituted.

[82] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report" (New York, NY, 2004), https://9-11commission.gov/report/.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDY ON EXISTING TSA PROGRAMS THAT SECURITIZE VARIOUS TRANSPORTATION SECTORS

A. SURFACE TRANSPORTATION SECURITY COMPLIANCE PROGRAM

The TSA's Surface Transportation Security Program is expanding as new outreaches and modes are incorporated. Currently, four distinct programs target a myriad of modes of transportation. The four programs are TSA's Baseline Assessment for Security Enhancement (BASE), Exercise Information System (EXIS), First Observer Plus (FOP), and Security Enhancement Through Assessment (SETA). These programs are mode specific and focus on providing essential oversight and aid to various modes of transportation within the United States.[83]

The BASE program specifically targets mass transit and highway motor carriers to provide a no-cost evaluation of the entities' security posture. The program is focused on security fundamentals employed by the service provider. BASE looks at the organization's Security Action Items (SAI) regarding security training and awareness and the entities' cyber security and physical protections specific to their mode and location. Based on the assessments of the employed countermeasures and security posture, TSIs provide written feedback and analysis confirming worthiness and recommendations on improving the program's overall effectiveness.

Under the BASE model, there are five assessment levels based on the specific mode of transportation. They are mass transit, large and small, and highway motor carrier, broken down into motor coach, trucking, and school bus. The TSIs work with these partners to schedule BASE assessments, provide best practices, and provide resources to buttress the existing security programs at each entity. Additionally, they interview the personnel at each location to get a proper gauge of the security program and a feel for how the individual security programs are being implemented. They then provide debriefs to the stakeholder

[83] Keelan Sweeny and Eric Begin, "BASE Fact Sheet" (TSA, June 2019); Joseph Martynski, "EXIS Fact Sheet" (TSA, May 2021); Transportation Security Administration, "First Observer Brochure Final," n.d., accessed October 6, 2022; Transportation Security Administration, "First Observer Plus Program Overview" (TSA, n.d.), accessed October 6, 2022; Jimmy Beasley, "Security Enhanced Through Assessment Fact Sheet," September 2022.

personnel and their respective executive leadership. The assessments are specifically tailored to the operation and focus on specific areas of improvement. TSA personnel provide guidance and advice on acquiring grants and funding to bolster the security posture and provide an outstanding service to strengthen security measures and employee security awareness.[84]

The EXIS program overlaps with BASE. This is also a no-cost service provided by TSA to strengthen security posture. However, the EXIS program more narrowly focuses on the development of participating stakeholders to respond more effectively to security incidents that arise. These security strengthening measures are specifically tailored to the operations and home in the mission areas of "Prevention, Protection, Mitigation, Response, and Recovery." The security strengthening exercises are entirely collaborative, and specific feedback is provided to stakeholders based on their exercise or workshop. This program is executed on all modes of surface transportation, which includes freight (trucking, freight rail, and shipper and receiver), passenger (pupil transportation, mass transit, motor coach, and passenger rail), maritime (faculties that fall under the MTSA), and infrastructure (tunnel, pipeline, and bridges). The workshops, exercises, and tabletops are scaled to meet the level of involvement based on the number of personnel at each location.[85]

In the same vein, the SETA program is a free of charge service provided to industry and involves freight, maritime, passenger, and infrastructure protection, just like EXIS. However, the effort between the two is differentiated particularly by the level of focus. The SETA program is a lengthy process conducted in three distinct phases: The first phase encompasses the TSIs working with stakeholder leadership to identify areas of vulnerability in their current security structure. Secondly, TSIs provide training and briefings on the shortcomings and potential mitigation strategies to combat them. In the third phase, inspectors reassess the security posture after implementing the additional security measures and provide extensive feedback to the stakeholder management and the frontline employees on implementing the additional training. As a best practice, the third

[84] Sweeny and Begin, "BASE Fact Sheet."

[85] Martynski, "EXIS Fact Sheet."

phase is conducted within one to two months after the training and briefings have concluded.[86]

The fourth platform that the TSA surface compliance program implements are First Observer Plus (FOP). Like the others, this is a development program focused on educating transportation professionals to detect suspicious and potentially dangerous activities and report them to the appropriate parties. The program's simple yet meaningful message is observe, assess, and report. The FOP is the older and more established of the surface transportation compliance programs, getting its founding in 2008 to increase security awareness for highway transportation. It was modeled after a program called Highway Watch but quickly expanded and was updated to include other modes of transportation.

The FOP program works with transportation partners and their employees to expand the knowledge of what may constitute a terroristic threat, giving them the tools to act and report threats to the appropriate parties for actionable measures. The required training can be conducted virtually or live. This program expands the capacity of force multipliers to transportation security by enlisting those most likely to exhibit illicit behaviors or actions indicative of threats against critical transportation infrastructure. The primary objective is to promulgate vigilance and to empower those on the frontline to report suspicious activity or persons.[87]

All surface compliance programs are free to industry and aim to develop transportation carriers, service providers, and personnel with the tools to identify potential problems effectively. There is very little onerous regulation on these industries regarding security, and the paradigm is to develop capacity within transportation organizations. These are entirely partnership-oriented relationships and are generally well-received by the industry.[88]

[86] Beasley, "Security Enhanced Through Assessment Fact Sheet."

[87] Transportation Security Administration, "First Observer Brochure Final"; Transportation Security Administration, "First Observer Plus Program Overview."

[88] Transportation Security Administration, "Surface Transportation | Transportation Security Administration," Resources, accessed November 16, 2022, https://www.tsa.gov/for-industry/resources.

B. AVIATION TRANSPORTATION SECURITY COMPLIANCE PROGRAM

There are many aviation security program types, and the breadth of scope and rigor is associated with the size of the operation and its varying components. Commercial airport operator security programs are broken down into full or partial programs that are differentiated by the size of the commercial aircraft being flown out of a particular airport. Additionally, there are Twelve-Five Standard Security Program (TFSSP) and charter operations which are considered special security programs and operate under a completely different set of rules.[89]

Regardless of the type of program being implemented, there is a shared security responsibility between aircraft operators and the airport hosting the operations, and the TSA provides guidance and oversight to bolster security while ensuring that both airlines and airports comply with security plans and governing regulations. However, airlines and airports fall under different requirements. There are three essential aviation air-carrier programs with varying requirements based on risk and complexity. They are the TFSSP, the Private Charter Standard Security Screening Program (PCSSP), and the Aircraft Operator Standard Security Program (AOSSP). The TFSSP regulates carriers operating commercial aircraft based on weight at takeoff between 12,500 and 100,309.3 pounds and is required under FAA Part 135. The PCSSP governs charter airline activities with the same maximum takeoff weight as the TFSSP, but for airline operators providing service with aircraft designed to hold more than 61 passenger seats. This program operates under FAA Parts 121, 125, and 135; passenger screening is required. However, the screening level is less invasive than what is imposed for standard commercial airlines operating out of federalized airports.[90]

Most airports and operators, including public charters, operating at major airports are under a complete program and fall under the AOSSP. Under this program, airlines create specific programs that govern their internal security based on the overarching

[89] Jeffrey Price and Jeffrey S. Forrest, *Practical Aviation Security: Predicting and Preventing Future Threats*, 2nd ed. (Waltham, MA: Elsevier Science & Technology, 2013), 287, ProQuest.

[90] Transportation Security Administration, "Aviation Programs | Transportation Security Administration," Accessed November 7, 2022, https://www.tsa.gov/for-industry/aviation-programs.

standards dictated under the AOSSP. Once vetted by TSA for sufficiency, these programs are deemed Sensitive Security Information (SSI) and must be controlled as such.[91] This system is implemented by the major commercial airlines within the U.S. that most people and their property transit. Additionally, for aircraft operators under the AOSSP, the TSA generally provides all security screening of passengers, their accessible property, and checked baggage. The exception is when the airport is a Screening Partnership Program (SPP) airport that uses contracted private security personnel trained and regulated under the TSA.[92]

In addition to the governing programs that oversee security operations for airlines, carriers have specific requirements to appoint certain personnel to security roles within the organization. Every airline must designate an Aircraft Operator Security Coordinator (AOSC) through formal appointment. This individual has a broad role and oversees the complete security program for a particular airline. The expansiveness of this role will be governed by the size of the airline and the number of locations it operates. This role requires massive coordination efforts across multiple locations and with federal, state, and local partners.[93]

At specific airport locations, Ground Security Coordinators (GSC) are assigned direct security responsibility for each aircraft. The GSC position requires training and expertise in security operations, and constant contact is needed with airport and TSA personnel. GSCs determine whether unruly passengers will be allowed to fly in conjunction with the Pilot in Command (PIC) for an airplane and use their security training and experience to prevent incidents before a plane leaves the ground.[94] Security takes teams of people from various organizations working in concert with specific plans tailored to the operational mission.

[91] Price and Forrest, *Practical Aviation Security: Predicting and Preventing Future Threats*, 289.

[92] Transportation Security Administration, “Screening Partnership Program,” accessed November 7, 2022, https://www.tsa.gov/for-industry/screening-partnerships.

[93] Price and Forrest, *Practical Aviation Security: Predicting and Preventing Future Threats*, 299.

[94] Price and Forrest, 299–300.

In the same vein as requirements for airline operators, the airports have independent security programs to implement and follow. Much like the security programs discussed above, airports providing service to airlines that operate aircraft with 61 or more seats must engage in a complete security program based on TSA regulations. They must put together an Airport Security Program (ASP) that is specific to the airport and is vetted through TSA. Just like the air carrier's security programs, these ASPs are considered SSI and are protected from public disclosure. They are updated frequently based on revised SDs instituted by the TSA.[95] ASP amendments are submitted by the airport, reviewed by TSIs, and approved by the Federal Security Director for TSA. Moreover, 49 CFR Section 1542.3 requires airports to designate a trained Airport Security Coordinator and alternate(s) to be the airport's point person for all security-related matters.[96]

The TSA plays a crucial role in the airplane and airport security. Aviation TSIs conduct periodic inspections and security plan reviews to look for vulnerabilities or non-compliance in plan execution. The agency can institute civil penalties under 49 CFR Section 1503.401 to individuals, airlines, airports, and others.[97] However, in 2017, TSA moved to an action plan program called outcome-focused compliance, which allows regulated entities to enter into a collaborative agreement to fix a security violation instead of initiating a civil enforcement action.[98] Approximately 80% of all violations were closed out with counseling between 2017 and 2021.[99] The counseling is documented and can be used for progressive enforcement action if a continued violation of the exact nature

[95] Aircraft Owners and Pilots Association, "TSA Airport Access Security Requirements," October 10, 2018, https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements.

[96] "Airport Security Coordinator," 49 C.F.R. 1542.3 (2002), https://www.law.cornell.edu/cfr/text/49/1542.3.

[97] Transportation Security Administration, "Enforcement Sanction Guidance Policy," February 8, 2021, 1, https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf.

[98] Government Accountability Office, *Aviation Security Programs: TSA Should Clarify Compliance Program Guidance and Address User Concerns with Its Data Systems* (Washington, DC: Government Accountability Office, 2022), 5, https://www.gao.gov/assets/gao-22-105063.pdf.

[99] Government Accountability Office, 17.

occurs.[100] By most accounts, this program has been positively received by regulated entities, leading to greater collaboration between security partners.[101]

C. PHYSICAL SCREENING OF PASSENGERS, PROPERTY, AND EMPLOYEES

The September 11, 2001 attacks sparked many massive undertakings, but one of the most major was the creation of TSA and the implementation of physical screening at all federalized airports. The screening had existed before the attacks, but the level and depth quickly increased. All persons and their property getting on commercial airlines were required to be screened to the same standards implemented by the agency.[102] Now in the year 2021 alone, TSA screened 585.3 million passengers and their accompanying properties.[103]

In recent years, the focus has remained on passengers and their property. However, there has been increasing interest in expanding screening and random checks to airport and airline employees to combat potential insider threat issues. The insider threat program was established by TSA in 2013 and included various program offices within the agency. These threats can come from various sources, including things that seem benign, like unknowingly causing a vulnerability, to insiders purposely smuggling prohibited items onboard aircraft and sabotage.[104] As a result, TSA and its partners have instituted a series of additional layers to identify and combat these instances. Many partners have implemented more robust vetting programs. Some airports have enrolled in mandatory Rap Back participation for all airport employees. TSA has leveraged the Advanced Threat Local

[100] Government Accountability Office, 17.

[101] Government Accountability Office, 25.

[102] Katherine A. Lowe, "Safety in the Sky: Will Reforming and Restructuring the TSA Improve Our Security or Merely Infringe on Our Rights?" *Journal of Air Law and Commerce* 81, no. 2 (2016): 291–92, https://scholar.smu.edu/jalc/vol81/iss2/5/.

[103] Transportation Security Administration, "TSA Highlights the Top 21 Accomplishments in Transportation Security to Close Out 2021," Press Release, January 18, 2022, https://www.tsa.gov/news/press/releases/2022/01/18/tsa-highlights-top-21-accomplishments-transportation-security-close.

[104] Government Accountability Office, *Aviation Security TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*, GAO-20-275 (Washington, DC, 2020), 10, https://www.gao.gov/assets/gao-20-275.pdf.

Allocation Strategy (ATLAS) program to provide random checks of employees at direct access points within the airport.

Moreover, some airports have even gone as far as building employee-only screening checkpoints to ensure one hundred percent compliance of all airport personnel entering secured areas. Additionally, airports have locked down all other direct access points into these areas.[105] In 2019, The Government Accountability Office (GAO) found that seven of the largest airports in the country and 13 of the next largest category performed one hundred percent screening of all airport employees accessing secured areas of the airport. Only 34 of 400+ airports nationwide perform one hundred percent screenings across all airport sizes.[106] These programs continue to garner interest as incidences of insider threat activity continue.

The programs referenced above continue to grow in response to insider threat activity. However, standardization across all airports continues to be a struggle due to funding, staffing, and infrastructure constraints. As seen with many pushes to drive drastic and sweeping changes to security posture, it takes a catastrophic incident, such as 9/11, or near-misses like the Richard Reed, 2006 liquids plot, and the underwear bomber, to make a compelling argument for increased securitization and fortification of potential targets. Insider threats remain a vulnerability and are a very complex and expansive problem that will take a conglomeration of various vetting, training, and screening efforts to combat.

[105] Ronnie Garrett, "Miami International Adds New Layers to Employee Screening Checkpoint," *Airport Improvement*, August 2017, https://airportimprovement.com/article/miami-intl-adds-new-layers-employee-screening-checkpoint.

[106] Government Accountability Office, *Aviation Security TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*, 21–22.

V. ANALYSIS OF ALTERNATIVES TO HARDEN COMMERCIAL SPACE LAUNCH SITES

The concept of regulating the physical security of commercial spaceports has received little to no attention, and as such, there is no robust literature or government analysis to pull. However, there is a safe assumption that commercial spaceport operators have an implied incentive to provide security for their assets. The level for each site remains a question and can be assumed to vary based on the private sector's desire to protect its various resources. This lack of uniformity in baseline standards across the industry poses a potential weakness regarding intelligent actors who wish to do damage or inflict economic pain on these targets. Therefore, for this policy analysis of alternatives, qualitative and quantitative data is used to derive scoring relating to each policy option's effectiveness, cost, political challenges, and viability. Based on the numerical values assigned for each category, composite scores are derived, and a comparison of the proposed alternative is assessed. Based on the assessment and analysis, recommendations are made and articulated in this thesis's conclusion.

For the analysis, a uniform assessment rubric was used to quantify composite scores of the three proposed methods to secure the physical security of spaceport ground-based operations. The assessment criteria provide a composite score by adding the quantitative sum of the assessment scores assigned for each measure of feasibility. Scores ranging from one to five, with one being the least favorable and five being the most favorable, were assigned for each grading criteria (e.g., effectiveness, cost, political challenges, and viability) after discussion and analysis of each criterion based on the limited data for each category. Once each proposed strategy was assessed, a recommendation is made based on each proposed securitization strategy's comparative scores and merits. The assessment rubric used is as follows:

A. APPROACH

The analysis of the three proposed alternatives relies mainly on qualitative data based on the rubric outlined in Table 2. Using the TSA's 2021 enacted budget, cost estimates are determined based on extracting relevant data as it could pertain to an expansion of regulatory activity. The figures are then divided based on the proportionality of the number of commercial spaceports vis-a-vis the number of federalized airports.

TSA reports it is responsible for the security of nearly 440 federalized airports. For this analysis, that number was used. The exact number of federalized airports varies since federalization can frequently change with seasonal service and de-federalization, where lines of business are added or lost. Additionally, TSA reports having more than 600 Full-Time Equivalents (FTE) aviation Transportation Security Inspectors. Six hundred TSIs/ 440 federalized airports= 1.363636363636364 TSIs per airport. The actual number varies substantially based on the size of the airport and the requirements of different levels of security programs based on the specific airport operations.[107] For this analysis, the number is rounded to 2 TSI FTE to allow for continuity.

Table 2. Assessment Rubric Template (repeated from Table 1)

Criterion	1	2	3	4	5	Composite Score
Effectiveness	Provides the least amount of securitization	Provides some securitization but is less than moderate	Provides a moderate level of securitization	Provides an improved level of securitization	Considered completely hardened	
Cost	Extreme cost	High level of cost	Moderate cost	Above minimal cost	Least cost	
Political Challenges	Almost no political support	Tough opposition- a great deal of scrutiny	Split decision but still able to implement	Some opposition but relatively easy support	Easily implemented with little to no opposition	
Viability	Extremely difficult to implement and sustain	High level of difficulty in implementing and sustaining	Moderately difficult to implement and sustain	Low difficulty in implementing and sustaining	Little to no difficulty in implementing and sustaining	

[107] Transportation Security Administration, "TSA by the Numbers," May 19, 2021, https://www.tsa.gov/news/press/factsheets/tsa-numbers.

B. ASSUMPTIONS

For this analysis, assumptions must be made regarding the threat scenario and associated cost. Other assumptions must also be established regarding effectiveness, cost, political challenges, and viability measures. The direct cost of infrastructure replacement and associated economic losses resulting from the attack scenario are used for this analysis. However, the cost associated with human life is not considered. Additionally, other figures and estimates are approximated based on established transportation security modes, as direct impacts prove challenging to obtain.

Furthermore, the cost of vetting is not calculated as some level of government vetting is assumed in all the policies analyzed. The form of this vetting may differ dependent on the approach taken by federal regulation. However, this thesis assumes that some level of vetting is implemented to ensure the reduced potential impact of insider threat vulnerabilities. This could be in the form of TWIC, Rap Back, or any other periodic background investigation and will vary based on the expansion of the space programs.

Moreover, the analysis factors in the reported number of employees working in the commercial space field as of 2020. It is assumed that the industry will continue to grow as it did even amid a global pandemic by roughly 3.2%.[108] As of 2020, the private sector employed 147,953 employees in various capacities.[109] For this analysis, 150,000 employees is used as it can be assumed that the industry has and will continue to grow based on the past trajectory of employment and the expansion of commercial space endeavors.

C. THREAT SCENARIO AND COST ESTIMATE

Although some contend that a worst-case analysis should be conducted to assess potential countermeasures, this analysis uses a reduced worst-case scenario for comparative purposes—the estimated cost of losing a commercial rocket and the delays in

[108] Schindelheim, “Private Companies Propelling Job Growth in the Space Industry.”

[109] Schindelheim; OECD, “Remedying the Gender Gap in a Dynamic Space Sector.”

future launches.[110] To this end, the analysis used the cost associated with the Falcon 9 rocket explosion in 2016 and its impact on subsequent launches as our impact figure. As SpaceX is not a public institution, exact cost figures are not obtainable. However, some estimates cite that the company may have lost upwards of $740 million due to the incident.[111] When fixed for inflation, this equates to approximately $910 million in 2022 dollars based on the CPI inflation calculator of the U.S. Bureau of Labor Statistics. Nine hundred and ten million U.S. dollars is the figure used for the forthcoming analysis.[112]

D. EFFECTIVENESS

The effectiveness of the three proposed measures to securitize ground-based commercial spaceports is based on current programs employed by the TSA to secure aviation, cargo, and surface transportation systems. These are government security programs. Therefore, direct data on effectiveness is unobtainable for this paper due to the classification and security concerns revolving around it. However, many open-source reports and Congressional findings are used to judge the proposed securitization strategies through logical analysis.

E. COST

The measure of cost-effectiveness, although difficult to quantify, is an assessment of the perceived reduction in the likelihood that the threat scenario is deterred or thwarted by the security measure. This cost-effectiveness measure approximates the proposed policy based on existing transportation security programs. The cost associated with the above threat scenario is used to compare the potential cost to the government and U.S. taxpayers to provide the varying levels of securitization of the proposed policies. Personnel and administrative costs from the Transportation Security Administration’s Budget Overview for FY 2023 are used to calculate the estimated cost associated with each proposal. The analysis uses figures from the FY 2021 enacted budget since these have been reconciled to

[110] Brown et al., “Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses,” 120.

[111] Mosher, “SpaceX Lost a Quarter of a Billion Dollars after One of Its Rockets Blew Up.”

[112] “CPI Inflation Calculator.”

factor in carryover funds and other surplus allocations. For simplification purposes, the analysis uses the TSA's estimate of federalized airports as a denominator for analysis and breakdown of estimates of personnel and administrative costs accordingly. The analysis then applies these estimates vis-à-vis numerical comparison of airports to current spaceports within the United States. A total cost comparison for each proposed policy is rendered through total government expenditure per program size based on the current number of spaceport operations. Table 3 shows the itemized budget summary for the FY2021 budget that was used to compare airport security expenditures to the proportion of commercial spaceports within the United States.

Table 3. TSA Appropriations and Program, Project, or Activity (PPA) Summary[113]

	FY2021 Enacted	**FY 2022 Annualized CR**	**FY 2022 President's Budget**	**FY 2023 President's Budget**
Operations and Support	**$8,135,506**	**$8,135,506**	**$8,451,537**	**$9,860,475**
Mission Support	$901,672	$901,672	$980,037	$1,042,958
Aviation Screening Operations	$5,497,847	$5,497,847	$5,709,431	$6,949,548
Screening Workforce	$4,082,668	$4,082,668	$4,158,822	$5,234,716
Screening Partnership Program	$226,406	$226,406	$231,068	$238,784
Screener Personnel, Compensation, and Benefits	$3,620,403	$3,620,403	$3,680,701	$4,732,094
Screener Training and Other	$235,859	$235,859	$247,053	$263,838
Airport Management	$651,622	$651,622	$721,038	$834,435
Canines	$169,513	$169,513	$170,186	$180,046
Screening Technology Maintenance	$477,711	$477,711	$532,300	$565,309
Secure Flight	$116,333	$116,333	$127,085	$135,042
Other Operations and Enforcement	$1,394,196	$1,394,196	$1,405,319	$1,550,219
Inflight Security	$784,655	$784,655	$774,332	$864,432
Federal Air Marshals	$764,643	$764,643	$754,069	$843,334
Federal Flight Deck Officer and Crew Training	$20,012	$20,012	$20,263	$21,098
Aviation Regulation	$238,468	$238,468	$246,416	$268,009
Air Cargo	$107,456	$107,456	$114,242	$127,746
Intelligence and TSOC	$76,497	$76,497	$83,554	$89,677
Surface Programs	$142,203	$142,203	$146,723	$156,639

[113] Adapted from Transportation Security Administration, *Transportation Security Administration Budget Overview*, 5–6, https://www.dhs.gov/sites/default/files/2022-03/Transportation%20Security%20Administration_Remediated.pdf.

	FY2021 Enacted	FY 2022 Annualized CR	FY 2022 President's Budget	FY 2023 President's Budget
Vetting Programs	$44,917	$44,917	$40,052	$43,716
Vetting Operations	$44,917	$44,917	$40,052	$43,716
Vetting Fees	$341,791	$341,791	$356,750	$317,750
TWIC Fee	$64,567	$64,567	$66,200	$63,100
Hazardous Materials Endorsement Fee	$18,126	$18,126	$19,200	$19,200
General Aviation at DCA Fee	$45	$45	$600	$600
Commercial Aviation and Airports Fee	$5,956	$5,956	$10,200	$10,000
Other Security Threat Assessments Fee	-	-	$50	$50
Air Cargo/Certified Cargo Screening Program Fee	$4,624	$4,624	$5,000	$5,000
TSA Precheck Fee	$245,020	$245,020	$249,500	$213,800
Alien Flight School Fee	$3,453	$3,453	$6,000	$6,000
Procurement, Construction, and Improvements	**$134,492**	**$134,492**	**$134,492**	**$119,345**
Aviation Screening Infrastructure	$134,492	$134,492	$134,492	$119,345
Checkpoint Support	$100,000	$100,000	$104,492	$105,405
Checkpoint Property Screening System	$39,133	$39,133	$104,492	$105,405
Checkpoint Property Screening System	$39,133	$39,133	$104,492	$105,405
Credential Authentication Technology (CAT)	$60,867	$60,867	-	-
Checked Baggage	$34,492	$34,492	$30,000	$13,940
Electronic Baggage Screening Program	$34,492	$34,492	$30,000	$13,940
Research and Development	**$29,524**	**$29,524**	**$35,532**	**$33,532**
Research and Development	$29,524	$29,524	$35,532	$33,532
Emerging Alarm Resolution Technologies	$3,000	$3,000	$3,000	$3,000
On-Person Detection/Next Gen Advanced Imaging Technology (AIT)	$5,000	$5,000	$5,000	$5,000
Innovation Task Force	$16,534	$16,534	$18,292	$16,292
Checkpoint Automation (CPAM)	$4,990	$4,990	$4,990	$4,990
Mobile Driver's License	-	-	$4,250	$4,250
Aviation Passenger Security Fee	**$250,000**	**$250,000**	**$250,000**	**$250,000**
Aviation Security Capital Fund	$250,000	$250,000	$250,000	$250,000
Operations and Support (O&S) Offset	$820,652	$820,652	$2,368,503	$4,012,443
Total	**$8,549,522**	**$8,549,522**	**$8,871,561**	**$10,263,352**

(Dollars in Thousands)

F. POLITICAL CHALLENGES

Information is used from the implementation of the comparative TSA programs already discussed to gauge the political challenges surrounding the implementation of the three proposed policies. A review of literature on the subject is assessed to extrapolate the level of scrutiny applied to the various programs that have been implemented. Based on this review, assumptions were made that commensurate levels of support or opposition will follow for the proposed securitization strategies. Based on the review, subjective scores are assigned through a logical assessment of support and opposition.

G. VIABILITY

A viability assessment is conducted on each of the proposed policies. Scoring is based on the scalability of existing programs utilized for other critical transportation infrastructure. Values are then assigned based on the scalability of existing programs, maturity, and the estimated time it will take to implement each proposal. Higher scores are assigned to securitization efforts that more easily leverage existing programs and require less start-up effort to initiate the program's rollout. Consideration is given to how the proposed policy would integrate into existing transportation infrastructure protection programs.

1. Government Security Development Programs

The implementation of this proposed policy option revolves around the federal government implementing a structure very similar to the one employed by the TSA to improve the security posture of surface transportation security. Under this system, transportation security inspectors work with the industry to provide training and conduct outreach activities to strengthen the security posture of commercial spaceports. Some basic levels of regulation are established. However, regulations are minimal. The inspectors essentially provide a service to the industry by conducting vulnerability assessments and implementing development programs to bolster industry awareness of possible threats and provide recommendations to mitigate vulnerabilities.

The level of effort and cost is the least of the three policy options analyzed in this paper. For this analysis, some basic figures are used. Since the data on aviation is more readily accessible and reliable, the personnel numbers and cost are used and applied instead of the estimations for surface or cargo transportation security compliance. Therefore, the analysis assumes a relative level of effort as an extrapolated personnel assumption based on the 1.2 million workers reported to be working in the aviation sector in the United States.[114] The 440 federalized airport number is used, and the proportionality of commercial spaceports to the number of airports are compared. Currently, there are seventeen commercial spaceports within the United States. The commercial space industry employs 147,953 personnel as of 2020. This number is rounded to 150,000 as growth is assumed based on historical data indicating industry growth of 3% yearly.[115]

a. Effectiveness

Admittingly, evaluating the effectiveness of all the potential paths being assessed is extremely difficult due to the lack of available public data. Security agencies and programs must keep all performance metrics close hold so as not to signal any potential vulnerabilities in the system and programs. However, Congress has expanded the TSA's footprint by increasing the number of programs and modes of transportation, such as the issuance of new and increased Security Directives for pipeline cyber security in the wake of the ransomware attack on the Colonial Pipeline in 2021.[116] Therefore, there can be some inference that there is a level of effectiveness the agency's surface transportation programs provide, or they would be diminishing, not expanding.

Despite not having concrete effectiveness numbers, some level of program effectiveness must be assumed. However, the real influence of the program can only be assumed by the relative number of inspectors/ personnel in the vast locations that operate

[114] Harriet Baskas, "How Many People Does It Take to Run an Airport?," USA TODAY, April 2, 2016, https://www.usatoday.com/story/travel/flights/2016/03/30/airport-workers-employees/82385558/.

[115] Schindelheim, "Private Companies Propelling Job Growth in the Space Industry."

[116] Shannon E. O'Neal and Michael T. Borgia, "TSA Revises Cybersecurity Requirements for 'Critical' Pipelines and LNG Facilities | Davis Wright Tremaine," Technology+ Privacy & Security, *Davis Wright Tremaine LLP* (blog), August 22, 2022, https://www.dwt.com/blogs/privacy--security-law-blog/2022/08/cybersecurity-tsa-pipelines-liquified-natural-gas.

under the surface umbrella. The authorities and responsibility of TSA's surface compliance program span many industries, including highway, bus, rail, pipeline, maritime, and now cyberinfrastructure. It is difficult to imagine that with only around 250 surface TSIs, the agency can have constant and meaningful contact and development with all these partners.

Based on these circumstances, there must be a level of value associated with the programs implemented, but resources and expanding requirements most certainly constrain it. Therefore, for this assessment, this option is given a rating of three as it fares moderately effectively to secure commercial spaceports.

b. Cost

Using the TSA Appropriations and Program, Project, or Activity (PPA) Summary listed above, personnel costs are established for a program proportionate to the number of commercial spaceports to airports within the United States. The TSA reports having roughly 600 aviation inspectors that provide security compliance oversight at approximately 440 airports and 250 surface TSIs to secure thousands of locations, including approximately 612,000 bridges, 470 tunnels, 360 maritime ports, 3,700 maritime terminals, 12,000 miles of coastline, and 2.75 million miles of pipeline.[117] Since the ratio of TSIs to airports is more manageable to calculate and sits at approximately 1.3 FTE per airport, the analysis uses the figure of two TSIs per spaceport to allow for coverage and continuity. Given that there are currently only 17 commercial spaceports in the U.S., it would only require 34 TSIs nationwide to provide this level of oversight and security development. The figures listed above are used, and it is assumed that there are additional costs beyond the baseline personnel expenditure for 34 TSIs to approximate the total government cost to implement such a program. Expansion of mission support and management functions are calculated based on the proportionality of this proposed expansion based on 2021 costs. However, since this analysis assumes some level of vetting is required for any policy options, this was not calculated separately.

[117] Transportation Security Administration, "TSA by the Numbers."

The TSA reports having approximately 60,000 employees in various capacities. For this analysis, this number is used to estimate the total cost per employee outside of the cost to employ 34 spaceport TSIs, accounting for program-associated costs such as mission support, management, technology, and administration. The total TSA enacted budget figures are used and divided by the total number of TSA employees to capture the cost of adding 34 TSI FTE. Therefore, the calculation is as follows:

$8,549,522,000/ 60,000= $142,492.033 per FTE

$142,492.033x 34 TSIs = $4,844,729.13 total cost to implement per year in 2022 dollars.

Using the $910 million that SpaceX was estimated to lose because of the Falcon 9 explosion in 2016 and fixed for inflation, it can be estimated that implementing this policy option would have to thwart an attack roughly every 188 years.

$910,000,000 loss/ $4,844,729.13 yearly expenditure= 187.832999 years of implementing the program to reach the cost of one explosion because of attack in 2022 U.S. dollars.

Based on these figures, a score of five is assigned in the grading rubric as this policy option has the "least cost" when factored against the potential risk posed by losing a single rocket.

c. Political Challenges

Arguably, it is time to start thinking about potential security issues before they become a reality. With the CSLA of 1984's termination of the "learning period" in which the FAA could not establish new regulations coming to an end in 2023, it is an opportune time to begin crafting preventative measures to ensure security at these sites.[118] However, given Congress' reluctance to place overarching regulations on this industry to allow the private sector's ingenuity to take shape and drive innovation, there will likely be some

[118] Space Policy Online, "Space Law."

hesitancy on the part of lawmakers and policymakers. Therefore, whatever measure to be taken, shy of no action, will meet some resistance.

However, implementing the lowest cost and most minorly intrusive security measures should prove significantly easier politically than widely promulgating restrictive regulations. Instituting a program like the ones used for the various modes that fall under surface transportation does seem politically viable. Given that these types of programs are built on fostering partnerships and expanding the security knowledge of the private sector, they are generally well-received. It is assumed that it would meet minimal political resistance compared to the much more restrictive and costly government oversight and regulation implementation.

Based on the political underpinnings of previous Congresses' intent, and the minimalist nature of instituting a program of this type, this option is assessed with a score of 4 under political challenges.

d. Viability

The measure of viability needs to consider the measures of effectiveness, cost, and political challenges. Nevertheless, the critical consideration for assessing viability must rest on the ease with which existing programs can be leveraged and expanded to commercial spaceport security. Therefore, with some level of effectiveness assumed, a minimal cost of a mere 34 FTE, and a political environment that might have more of an appetite for proving some level of regulation than any other time in the past, it comes down to scalability and level of effort to assess the viability of an option.

Provided that there are already programs to work with surface transportation partners to bolster physical security at various modes of transportation, the addition of spaceports appears to be a relatively light lift. It requires the internal training of TSI personnel to familiarize them with the workings of these facilities, a significant level of outreach to the industry, and the development of programs to provide value-added training and robust vulnerability assessments to the industry. However, it takes some time to get any meaningful programs instituted, but this allows time for rulemaking proceedings, industry outreach, and training of agency personnel. Additionally, this option is scalable because TSA could leverage existing programs such as BASE, NEXIS, SETA, and FOP as a foundation.

Given that TSA already has time-tested training and assessments for other modes of transportation and could leverage existing expertise and that this option only calls for a relatively small expansion of the agency's footprint to implement, a score of 5 is assessed due to its minimum difficulty to implement and sustain.

e. Overall Assessment

Overall, this option has a composite score of 17 out of 20 (see Table 4). The effectiveness measure is the hardest to gauge due to the lack of publicly available performance metrics. However, it was assumed that there is some positivity associated with these programs based on continued expansion into other facets of surface transportation security. Adding a relative cost of only 34 FTE and an expenditure assumption that a return on investment would result if this option prevented one rocket from exploding every approximately 188 years, with the minimal political challenges and robust viability obtained by leveraging existing surface programs, makes this a feasible option for safeguarding spaceports.

Table 4. Assessment Rubric: Government Security Development Programs

Criterion	1	2	3	4	5	Composite Score
Effectiveness	Provides the least amount of securitization	Provides some securitization but is less than moderate	Provides a moderate level of securitization	Provides an improved level of securitization	Considered completely hardened	3
Cost	Extreme cost	High level of cost	Moderate cost	Above minimal cost	Least cost	5
Political Challenges	Almost no political support	Tough opposition- a great deal of scrutiny	Split decision but still able to implement	Some opposition but relatively easy support	Easily implemented with little to no opposition	4
Viability	Extremely difficult to implement and sustain	High level of difficulty in implementing and sustaining	Moderately difficult to implement and sustain	Low difficulty in implementing and sustaining	Little to no difficulty in implementing and sustaining	5

2. Baseline Physical Security Mechanisms and Federal Oversight

The implementation of this proposed policy would revolve around the federal government implementing a structure very similar to the one employed by the TSA to improve the security posture of aviation and cargo transportation security. Under this system, transportation security inspectors work with the industry to provide training and conduct outreach activities to strengthen the security posture of commercial spaceports. Additionally, codified regulations about the security mechanisms at each location are inspected for compliance and regulated contingent on each spaceport’s size and risk designation. Some basic levels of regulation are established and enforced through current civil enforcement mechanisms. Under this policy option, regulations are increased and enforceable. The inspectors provide a service to the industry by conducting vulnerability assessments and implementing development programs to bolster industry awareness of possible threats and provide recommendations to mitigate vulnerabilities. However, this policy option also includes civil enforcement for non-compliance through warning notices and civil penalties for non-compliance with TSA-vetted security plans for each spaceport.

The level of effort is moderate and leverages existing transportation security compliance programs. For this analysis, the exact basic figures will be used. Since the data on aviation is more readily accessible and reliable, the personnel numbers and cost are used and applied instead of the estimations for surface or cargo transportation security compliance. Therefore, the analysis assumes a relative level of effort as an extrapolated personnel assumption based on the 1.2 million workers reported to be working in the aviation sector in the United States.[119] The figure of 440 federalized airports is used, and the proportionality of commercial spaceports to the number of airports are compared. Currently, there are seventeen commercial spaceports within the U.S. The commercial space industry employs 147,953 personnel as of 2020. This number is rounded to 150,000 as growth should be assumed based on historical data that indicates industry growth of over 3% year over year.[120]

a. Effectiveness

The level of effectiveness, like all the options assessed, is difficult to measure based on the lack of publicly available performance metrics due to its security sensitivity. However, there are some public data available through the GAO. In a 2018 report, the GAO's analysis of TSA data found that 16% of the approximately 5000 domestic cargo air carrier inspections conducted from FY 2012–2017 resulted in a finding of non-compliance with TSA regulations. Additionally, GAO found that 25% of foreign airport assessments of international cargo were discovered to be in non-compliance.[121] In another report from the GAO on aviation-related security programs, they found that roughly 9% of air carrier and airport inspections found one or more security violations between FY 2017–2021. Eighty percent of these instances of non-compliance were resolved with counseling.[122]

[119] Baskas, "How Many People Does It Take to Run an Airport?"

[120] Schindelheim, "Private Companies Propelling Job Growth in the Space Industry."

[121] Government Accountability Office, "TSA Uses a Variety of Methods to Secure U.S.-Bound Air Cargo, but Could Do More to Assess Their Effectiveness" (Washington, DC, November 2018), https://www.gao.gov/assets/gao-19-162.pdf.

[122] *Aviation Security Programs: TSA Should Clarify Compliance Program Guidance and Address User Concerns with Its Data Systems*, 16.

Therefore, it is assumed that TSA is operating an effective program in identifying areas of ineffectiveness by regulated aviation and cargo entities.

However, the effectiveness of TSA's action plans has been called into question. This is mainly due to the TSA's lack of guidance on when these plans should be instituted for systemic failures versus one-off occurrences of non-compliance.[123] Nevertheless, TSA regulations and inspections can identify weaknesses in security posture and instances of non-compliance with screening regulations. The program is broad and has oversight of both foreign and domestic.

If these regulations and inspections are applied to commercial spaceports, they would be more in-depth than the previous option analyzed. This type of program requires the establishment of security directives particular to the level of spaceport operation being run. It also requires the development of security personnel for each entity, as was referenced earlier in this paper. However, it is assumed that with strict protocols, the establishment of well-versed security professionals within each private sector entity, and robust inspections, the program has a high level of effectiveness involving the identification of security non-compliance and egregious violations.

Conversely, implementing a purely regulatory scheme does not eliminate threats imposed by those coming into the facilities. Potential risks of adversaries penetrating security and insider threat vulnerabilities still exist due to the lack of sentry checkpoints and routine inspections. However, the level of security needed to harden a target is entirely up for debate. Therefore, this option provides increased security assurance, and most security activities would fall to the regulated entity.

Based on the level of effectiveness afforded by employing this option, an assessment rating of 4 is assigned.

b. Cost

Using the TSA Appropriations and Program, Project, or Activity (PPA) Summary listed previously, personnel costs are established for a program proportionate to the number

[123] *Aviation Security Programs.*

of commercial spaceports to airports within the United States. The TSA reports having roughly 600 aviation inspectors that provide security compliance oversight at approximately 440 airports and 250 surface TSIs to secure thousands of locations, including approximately 612,000 bridges, 470 tunnels, 360 maritime ports, 3,700 maritime terminals, 12,000 miles of coastline, and 2.75 million miles of pipeline.[124] Since the ratio of TSIs to airports is more manageable to calculate and sits at approximately 1.3 FTE per airport, the analysis used a figure of 2 TSIs per spaceport to allow for coverage and continuity for the first policy option. However, it is assumed that increased regulation will require more personnel. Figuring that there are 2.4 times more aviation inspectors than surface TSIs (600/250= 2.4), this analysis rounds up to 3 TSIs per spaceport due to the increased complexity of implementing this option.

Given that there are currently only 17 commercial spaceports in the U.S., it would only require 51 TSIs nationwide to provide this level of oversight and security development. The figures listed above is used, and it is assumed that there will be additional costs beyond the baseline personnel expenditure for 51 TSIs to approximate the total government cost to implement such a program. The expansion of mission support and management functions are calculated based on the proportionality of this proposed expansion based on 2021 costs. However, since this analysis assumes some level of vetting is required for any of the policy options, this was not calculated separately.

The TSA reports having approximately 60,000 employees in various capacities. For this analysis, this number is used to estimate the total cost per employee outside the cost to employ 51 spaceport TSIs, accounting for program-associated costs such as mission support, management, technology, and administration. The total TSA enacted budget figure is used and divided by the total number of TSA employees to capture the full cost of adding 51 TSI FTE. Therefore, the calculation is as follows.

$8,549,522,000/ 60,000= $142,492.033 per FTE.

[124] Transportation Security Administration, “TSA by the Numbers | Transportation Security Administration.”

$142,492.033x 51 TSIs = $7,267,093.68 total cost to implement per year in 2022 dollars.

Using the $910 million that SpaceX was estimated to lose because of the Falcon 9 explosion in 2016 and fixed for inflation, it is estimated that implementing this policy option would have to thwart an attack roughly every 125 years.

$910,000,000 loss/ $7,267,093.68 yearly expenditure= 125.221999 years of implementing the program to reach the cost of one explosion because of attack in 2022 U.S. dollars.

Based on these figures, the grading rubric is assigned a score of four. This policy option has a cost just slightly above the previously assessed policy option when factored against the potential risk of losing a single rocket.

c. Political Challenges

The political challenges associated with this type of regulatory scheme are tough. The restrictions on imposing regulations under the CSLA are ending in 2023; however commercial spaceports have yet to be established as critical infrastructure despite pending legislation in Congress. Therefore, it will be difficult to sell to lawmakers and industry to move to this level of regulation right away after a long period with no federal oversight. Additionally, there have been no recorded attacks against these facilities, so they have not become reverent objects in need of increased security. The resource expenditure to fortify these ports seems substantial when there is no clear and present danger.

Provided that there is no current discussion around the protection and regulation of these facilities, coupled with the winding down of legislation explicitly prohibiting regulation on these entities, the likelihood of instituting this policy option is politically challenging. As such, this policy option has an assessment score of 2.

d. Viability

The measure of viability needs to consider the measures of effectiveness, cost, and political challenges. Nevertheless, just as for all options assessed, the critical consideration for assessing viability must rest on the ease with which existing programs can be leveraged and expanded to the area of commercial spaceport security. Therefore, with a greater level of effectiveness than the last option assessed assumed, a moderate cost of a mere 51 FTE, and a political environment likely to reject such a substantial measure, it comes down to scalability and level of effort to assess the viability of an option.

The aviation and cargo regulatory programs already exist and could be leveraged for applicability to spaceports. Just like the previous option assessed, it requires the internal training of TSI personnel to familiarize them with the workings of these facilities, a significant outreach to industry and politicians, and the development of policy, regulation, and security directives. This level of effort takes substantial time to implement meaningful programs. These programs are entirely contingent on a critical infrastructure designation and accompanying lawmaking to provide federal oversight for spaceport security. This option being instituted is contingent on many components came together, but this option's viability seems extremely unlikely.

Provided that spaceports are not currently designated as critical infrastructure and that the prohibition of the CSLA on new regulation is still in effect, the viability of instituting this type of option appears to have a high level of difficulty to implement and sustain at this time. For the reasons cited, an assessment score of 2 for viability has been assigned.

e. Overall Assessment

Overall, this option has a composite score of 11 out of 20 (see Table 5). The political challenges and viability currently make this option difficult to adopt and implement. The associated cost is moderate, with an estimated addition of 51 FTE despite an expenditure assumption that a return on investment would result if this option prevented one rocket from exploding every approximately 125 years. Regardless of the effectiveness of instituting this policy option, the political appetite, viability, and associated cost likely outweigh the perceived benefit of providing security oversight to an area currently not considered at risk. However, the score for this option could be adjusted substantially if the attack focus changes to commercial spaceports in the future.

Table 5. Assessment Rubric: Baseline Physical Security Mechanisms and Federal Oversight

Criterion	1	2	3	4	5	Composite Score
Effectiveness	Provides the least amount of securitization	Provides some securitization but is less than moderate	Provides a moderate level of securitization	Provides an improved level of securitization	Considered completely hardened	4
Cost	Extreme cost	High level of cost	Moderate cost	Above minimal cost	Least cost	3
Political Challenges	Almost no political support	Tough opposition- a great deal of scrutiny	Split decision but still able to implement	Some opposition but relatively easy support	Easily implemented with little to no opposition	2
Viability	Extremely difficult to implement and sustain	High level of difficulty in implementing and sustaining	Moderately difficult to implement and sustain	Low difficulty in implementing and sustaining	Little to no difficulty in implementing and sustaining	2

3. Full Federalization

The implementation of this proposed policy revolves around the federal government implementing a structure very similar to the one employed by the TSA to securitize passenger aircraft in the wake of 9/11. Under this system, transportation security inspectors work with the industry to provide training and conduct outreach activities to strengthen the security posture of commercial spaceports. Additionally, codified regulations on the security mechanisms at each location are inspected for compliance and regulated contingent on each spaceport's size and risk designation. Some basic levels of regulations need to be established and enforced through current civil enforcement mechanisms. Moreover, TSA supplies security screening personnel to conduct on-person and in-property inspections of passengers and property before being allowed entry onto a spacecraft. This will also be expanded to employee screening efforts, as discussed earlier in this paper.

Under this policy option, regulations are increased and enforceable. The inspectors enforce codified regulations, and TSA personnel are responsible for security screening.

Measures are taken to combat insider threats, such as employee inspections at direct access points to secured areas of spaceports. This policy option includes civil enforcement for non-compliance through warning notices, action plans, and civil penalties.

The level of effort is high, but its implementation leverages existing transportation security compliance programs, technology, and screening practices. For this analysis, the exact basic figures are used. Since the data on aviation is more readily accessible and reliable, the personnel numbers and cost are used and applied instead of the estimations for surface or cargo transportation security compliance. Therefore, the analysis assumes a relative level of effort as an extrapolated personnel assumption based on the 1.2 million workers reported to be working in the aviation sector in the United States.[125] The figure of 440 federalized airports is used, and the proportionality of commercial spaceports to the number of airports are compared. Currently, there are seventeen commercial spaceports within the U.S. The commercial space industry employs 147,953 personnel as of 2020. This number is rounded to 150,000 as growth should be assumed based on historical data that indicates industry growth of over 3% year over year.[126]

a. Effectiveness

The level of effectiveness, like all the options assessed, is challenging to measure accurately, and the previous policy option's assessment needs to be leveraged as it is a significant component of this policy option. Moreover, this policy option considers combating external threats and those associated with insider threats. A component of this scheme will help ensure that prohibited items and people cannot access the secured areas of spaceports by providing physical security barriers and checks at all direct access points within these facilities.

Notwithstanding, it is assumed that providing some form of physical screening to persons and property is more significant than providing no screening. However, the actual effectiveness of this type of screening has come under much scrutiny in the past. In an

[125] Baskas, "How Many People Does It Take to Run an Airport?"

[126] Schindelheim, "Private Companies Propelling Job Growth in the Space Industry."

unclassified report released by the DHS Office of Inspector General (OIG) in 2017, it was disclosed that TSA screening personnel failed approximately 70% of the time at detecting prohibited items when being covertly tested.[127] This came from a report issued two years earlier that TSA personnel failed 67 out of 70 tests conducted by OIG for a 95% failure rate.[128] These failures caused many to call into question the screening work conducted by the TSA.

Provided TSA's less-than-stellar results, it is assumed that effectiveness is substantially greater than zero but less than entirely impermeable. Although considering that no mechanisms are in place for regulatory oversight nor providing physical screening of persons and property, this policy option provides a substantial level of effectiveness and is assigned an assessment score of 4 for providing an improved level of securitization.

b. Cost

Using the TSA Appropriations and Program, PPA Summary listed previously, personnel costs are established for a program proportionate to the number of commercial spaceports to airports within the United States. The TSA reports having roughly 60,000 total employees as of 2022. Federalization of commercial spaceports is the costliest policy option of the ones assessed in this paper. This analysis assumes the median figure as spaceport size and complexity will vary much like airports within the U.S to figure out the number of personnel and the total cost to implement. For example, some airports are small and can have as few as four Transportation Security Officers working at the location. Others, such as category X airports, may have a workforce numbering in the thousands. For this analysis, we will use the following figure.

60,000 current TSA employees/ 440 federalized airports= 136.363636 FTE per location.

[127] Michael Goldstein, "TSA Misses 70% Of Fake Weapons But That's An Improvement," Forbes, November 9, 2017, https://www.forbes.com/sites/michaelgoldstein/2017/11/09/tsa-misses-70-of-fake-weapons-but-thats-an-improvement/.

[128] Justin Fishel et al., "Undercover DHS Tests Find Security Failures at U.S. Airports," ABC News, June 1, 2015, https://abcnews.go.com/US/exclusive-undercover-dhs-tests-find-widespread-security-failures/story?id=31434881.

Based on the median FTE needed per location of 136.363636 x 17 spaceports= 2,318.18182 FTE needed across the sector. This equates to $8,549,522,000/ 60,000= $142,492.033 per FTE x 2,318.18182 = $330,322,440 annually.

Using the $910 million that SpaceX was estimated to lose because of the Falcon 9 explosion in 2016 and fixed for inflation, it is estimated that implementing this policy option would have to thwart an attack roughly every 2.75 years.

$910,000,000 loss/ $330,322,440 yearly expenditure= 2.75488399 years of implementing the program to reach the cost of one explosion because of an attack in 2022 U.S. dollars.

Based on these figures, a score of two is assigned in the grading rubric as this policy option has a high cost above the expenditure of the previously assessed policy options when factored against the potential risk of losing a single rocket.

c. Political Challenges

The political challenges associated with this type of policy option are significant since there are currently no security regulations and no impending fear of danger for commercial spaceports. The restrictions on imposing regulations under the CSLA are ending in 2023; however, commercial spaceports have yet to be established as critical infrastructure despite pending legislation in Congress. Therefore, it is difficult to sell to lawmakers and industry to move to this level of regulation right away after a long period with no federal oversight. Additionally, there have been no recorded attacks against these facilities, so they have not become reverent objects needing increased security. The resource expenditure to fortify these ports seems substantial when there is not a clear and present danger, and it took the events of 9/11 to spark this level of effort to increase security at airports to this level.

Provided that there is no current discussion revolving around the protection and regulation of these facilities, coupled with the winding down of legislation explicitly prohibiting regulation on these entities, and there has been no punctuating event like 9/11 to drive such a change, the likelihood of instituting this policy option is almost politically impossible at this time. As such, this policy option has an assessment score of 1.

d. Viability

The measure of viability needs to consider the measures of effectiveness, cost, and political challenges. Nevertheless, just as for all options assessed, the critical consideration for assessing viability must rest on the ease with which existing programs can be leveraged and expanded to the area of commercial spaceport security. Therefore, with a greater level of effectiveness than the last option assessed, a substantial cost of approximately 2,318 FTE at the cost of $330,322,440 annually, and a political environment that is very likely to reject such a substantial measure, it comes down to scalability and level of effort to assess the viability of an option.

The programs for regulatory oversight and federalized security screening are in place and can be leveraged to roll out this policy option. However, providing federal resources at all spaceports, as well as accompanying security technology, is a daunting task. Currently, airports do not even provide one hundred percent screening of all employees. Trying to implement something similar at spaceports would be more complex because the types of items these personnel bring into work would vary substantially from the standard stream of commerce that goes through an airport by the traveling public or by airport employees.

Provided that spaceports are not currently designated as critical infrastructure and that the prohibition of the CSLA on new regulation is still in effect, the viability of instituting this type of option appears to have a high level of difficulty to implement and sustain at this time. For the reasons cited, an assessment score of 1 for viability has been assigned.

e. Overall Assessment

Overall, this option has a composite score of 8 out of 20 (see Table 6). The political challenges, cost, and viability make this option extremely difficult to adopt and implement. The associated cost is high, with an estimated addition of approximately 2,318 FTE at the cost of $330,322,440 despite an expenditure assumption that a return on investment would result if this option prevented one rocket from exploding every approximately 2.75 years. Regardless of the effectiveness of instituting this policy option, the political appetite, viability, and associated costs outweigh the perceived benefit of providing security oversight and screening to an area currently not considered at risk. However, the score for this option will be adjusted substantially if the attack focus changes to commercial spaceports in the future and complete target hardening like commercial airports becomes a necessity.

Table 6. Assessment Rubric: Full Federalization

Criterion	1	2	3	4	5	Composite Score
Effectiveness	Provides the least amount of securitization	Provides some securitization but is less than moderate	Provides a moderate level of securitization	Provides an improved level of securitization	Considered completely hardened	4
Cost	Extreme cost	High level of cost	Moderate cost	Above minimal cost	Least cost	2
Political Challenges	Almost no political support	Tough opposition- a great deal of scrutiny	Split decision but still able to implement	Some opposition but relatively easy support	Easily implemented with little to no opposition	1
Viability	Extremely difficult to implement and sustain	High level of difficulty in implementing and sustaining	Moderately difficult to implement and sustain	Low difficulty in implementing and sustaining	Little to no difficulty in implementing and sustaining	1

VI. RECOMMENDATIONS AND CONCLUSION

The time has come to begin thinking about a world with expanded space capabilities in the private sector. Although there are currently only 17 commercial spaceports within the U.S., this number is expected to continue expanding as technology increases and the cost to operate decreases. Looking at the aviation sector, it is easy to see how fast transportation industries can expand, and there should be an assumption that as costs per pound of delivery of goods go down, other sectors will begin to leverage this mode of transportation to move products across the world in record time. Additionally, commercial space travel has already become a reality for a few private citizens. This trend is likely to continue as viability is proven and costs decrease. To those ends, as we have seen with past incidents, transportation continues to be a prime target for terrorist attacks. Punctuating events such as 9/11 can have a profound impact on the industry and everyday life. Therefore, the United States should begin to get ahead of potential threats and not suffer from another failure of imagination.

There should be some urgency, but there should also be caution around taking on too much, too fast. One of the ways to get around this is by having a forward-looking mindset as to potential scenarios that may arise and providing commensurate countermeasures to safeguard and harden areas that may become targets, or symbolic targets, in the not-so-distant future. This is financially prudent as it protects critical assets while preventing knee-jerk reactions leading to costly securitization efforts. A little preparation, collaboration, and oversight now will not only mitigate the impact on the private sector in case of an attack—it will also safeguard other infrastructure and lives and mitigate the tax expenditure resulting from a broad expansion of regulation and security mechanisms in the wake of a disaster.

This thesis analyzed three possible policy options for safeguarding commercial spaceports and assigned weighted values for four categories. Based on the assessment, instituting a security scheme like those used for surface transportation appears to be the prudent first step for the federal government. This option would provide outreach to the 17 current spaceports and assessments of the current security posture from trained and experienced personnel. It would also help to work in partnership with industry in order to bolster their security posture, safeguard their assets, and to protect other infrastructure and people from potential harm that could result from attacks on commercial spaceports.

This recommendation is the first step toward improving security at these facilities. It may need to be reevaluated and adjusted based on intelligence, expansion of operations, or other factors that may not yet be apparent. If the industry continues to grow at its current pace, the notoriety and expansion may make spaceports a more desirable target of terrorist actions. If continued proliferation of commercial space travel becomes a reality, the level of effort to secure the facilities would need to be adjusted to meet the scope and threat level at that time. Regardless, the federal government needs to implement something as soon as possible, and then periodically assess whatever programs are instituted for sufficiency.

The U.S. government must also begin to evaluate other potential areas of weakness in commercial space operations. The cyber threat is expanding as we have recently seen impacts on other critical infrastructures. Additionally, threats to property transiting to and from these installations, as well as other imaginable threats, need to be studied. As discussed earlier, there also needs to be more consideration and research revolving around personnel vetting and other insider threat mitigations. The potential threat landscape is significant and will require action planning for future situations that could impact space operations, such as sabotage, hijackings, and other potential threat scenarios. These potential threats should be areas of further research and consideration.

The time to act is now—before an incident occurs. Taking small steps will place the industry in a better position if threats develop. These measures are small on the grand scale but will have a meaningful and substantial impact on the security of commercial spaceports in the United States. The measures will safeguard the industry to allow continuous growth and development in an emerging market. Even a minor attack could have severe consequences for the development and adoption of this novel form of transportation, which could impact the industry for decades.

LIST OF REFERENCES

Abeyratne, Ruwantissa. "Commercial Space Travel: Security and Other Implications." *Journal of Transportation Security*, no. 6 (2013): 257–70. https://doi.org/10.1007/s12198-013-0115-1.

Aircraft Owners and Pilots Association. "TSA Airport Access Security Requirements." Text, October 10, 2018. https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements.

Albert, Laura A, Alexander Nikolaev, Adrian J. Lee, Kenneth Fletcher, and Sheldon H. Jacobson. "A Review of Risk-Based Security and Its Impact on TSA PreCheck." *Operations Engineering & Analytics* 53, no. 6 (2021): 657–70. https://doi-org.libproxy.nps.edu/10.1080/24725854.2020.1825881.

Armendariz, Corina. "SpaceX Launch Facility- Brownsville, TX," April 10, 2022.

Government Accountability Office. *Aviation Security Programs: TSA Should Clarify Compliance Program Guidance and Address User Concerns with Its Data Systems*. Washington, DC: Government Accountability Office, 2022. https://www.gao.gov/assets/gao-22-105063.pdf.

Aviation Security TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals. GAO-20-275. Washington, DC, 2020. https://www.gao.gov/assets/gao-20-275.pdf.

Aziz, Ridwan Al, Meilin He, and Jun Zhuang. "An Attacker–Defender Resource Allocation Game with Substitution and Complementary Effects." *Risk Analysis* 40, no. 7 (July 1, 2020): 1481–1506. https://doi.org/10.1111/risa.13483.

Bar, Shmuel. *Securing Transportation Systems*. Edited by Simon Hakim, Gila Albert, and Yoram Shiftan. New York: John Wiley & Sons, Inc., 2015. ProQuest.

Baskas, Harriet. "How Many People Does It Take to Run an Airport?" USA TODAY, April 2, 2016. https://www.usatoday.com/story/travel/flights/2016/03/30/airport-workers-employees/82385558/.

Beasley, Jimmy. "Security Enhanced Through Assessment Fact Sheet," September 2022.

Brandt, Patrick T., and Todd Sandler. "A Bayesian Poisson Vector Autoregression Model." *Cambridge University Press* 20, no. 3 (2012): 292–315. https://doi.org/:10.1093/pan/mps001.

Brown, G., W. M. Carlyle, J. Salmeron, and K. Wood. "Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses." *Calhoun: The NPS Institutional Archive*, 2005. https://doi.org/doi 10.1287/educ.1053.0018.

California State University, Long Beach. “670 Steps in Policy Analysis.” The Policy Analysis Process, April 16, 2021. https://home.csulb.edu/~msaintg/ppa670/670steps.htm.

CISA. “Critical Infrastructure Sectors.” Critical Infrastructure Sectors. Accessed March 22, 2022. https://www.cisa.gov/critical-infrastructure-sectors.

“CPI Inflation Calculator.” Accessed August 31, 2022. https://www.bls.gov/data/inflation_calculator.htm.

Dahl, Erik J. “The Plots That Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States.” *Studies in Conflict & Terrorism* 34, no. 8 (July 21, 2011): 621–48.

Endress, Christian. “Critical Infrastructure Protection – Strategies and Technologies – ProQuest.” *Military Technology* 31, no. 7 (2007): 79–80.

Federal Aviation Administration. “Spaceport Map.” Washington, DC, May 13, 2022. https://www.faa.gov/space/spaceport-map.

Fishel, Justin, Pierre Thomas, Mike Levine, and Jack Date. “Undercover DHS Tests Find Security Failures at U.S. Airports.” ABC News, June 1, 2015. https://abcnews.go.com/US/exclusive-undercover-dhs-tests-find-widespread-security-failures/story?id=31434881.

Fletcher, Kenneth C. “Aviation Security: A Case for Risk-Based Passenger Screening.” Master’s thesis, Naval Postgraduate School, 2011. Calhoun. http://hdl.handle.net/10945/10601.

Foreign Air Carrier Security, 49 C.F.R. 1546 § (2002). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1546.

Gaibulloev, Khusrav, and Todd Sandler. “What We Have Learned about Terrorism since 9/11.” *Journal of Economic Literature* 57, no. 2 (June 2019): 275–328. https://doi.org/10.1257/jel.20181444.

Garrett, Ronnie. “Miami International Adds New Layers to Employee Screening Checkpoint.” *Airport Improvement*, August 2017. https://airportimprovement.com/article/miami-intl-adds-new-layers-employee-screening-checkpoint.

Goldstein, Michael. “TSA Misses 70% Of Fake Weapons But That’s An Improvement.” Forbes, November 9, 2017. https://www.forbes.com/sites/michaelgoldstein/2017/11/09/tsa-misses-70-of-fake-weapons-but-thats-an-improvement/.

Government Accountability Office. *Aviation Security Programs: TSA Should Clarify Compliance Program Guidance and Address User Concerns with Its Data Systems*. Washington, DC: Government Accountability Office, 2022. https://www.gao.gov/assets/gao-22-105063.pdf.

———. *Aviation Security TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*. GAO-20-275. Washington, DC, 2020. https://www.gao.gov/assets/gao-20-275.pdf.

———. "Surface Transportation Security: TSA Has Taken Steps to Improve Its Surface Inspector Program, but Lacks Performance Targets." Congressional. Washington, DC, July 2020. ProQuest.

———. "TSA Uses a Variety of Methods to Secure U.S.-Bound Air Cargo, but Could Do More to Assess Their Effectiveness." Washington, DC, November 2018. https://www.gao.gov/assets/gao-19-162.pdf.

Haphuriwat, N., and V.M. Bier. "Trade-Offs between Target Hardening and Overarching Protection." *European Journal of Operational Research* 213, no. 1 (August 16, 2011): 320–28. https://doi.org/10.1016/j.ejor.2011.03.035.

Hastings, Justin V., and Ryan J. Chan. "Target Hardening and Terrorist Signaling: The Case of Aviation Security." *Terrorism and Political Violence* 25, no. 5 (November 25, 2013): 777–97. https://doi.org/10.1080/09546553.2012.699906.

Holgersson, Annelie, and Ulf Bjornstig. "Mass-Casualty Attacks on Public Transportation." *Journal of Transportation Security,* 7, no. 1 (2013): 1–16. http://dx.doi.org/10.1007/s12198-013-0125-z.

Ivančík, Radoslav, and Pavel Nečas. "Air Transport Terrorism: One of the Most Feared Types of Asymmetric Security Threat," 2020. ProQuest.

Jaksec, Gregory M. "Public-Private-Defense Partnering in Critical Infrastructure Protection." Thesis, Monterey, California. Naval Postgraduate School, 2006. https://calhoun.nps.edu/handle/10945/2878.

Jashari, Linda. "Soft Target Security: Environmental Design and the Deterrence of Terrorist Attacks on Soft Targets in Aviation Transportation." Master's thesis, Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/58317.

———. "Soft Target Security: Environmental Design and the Deterrence of Terrorist Attacks on Soft Targets in Aviation Transportation." Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/58317.

Jaspersen, Johannes G., and Gilberto Montibeller. "On the Learning Patterns and Adaptive Behavior of Terrorist Organizations." *European Journal of Operational Research* 282, no. 1 (April 1, 2020): 221–34. https://doi.org/10.1016/j.ejor.2019.09.011.

Johnstone, R. William. *Protecting Transportation: Implementing Security Policies and Programs*. Oxford: Elsevier Science & Technology, 2015. ProQuest.

Kelvey, Jon. "Inspiration4: How Much Does a Ticket to Space Cost?" Inverse, September 15, 2021. https://www.inverse.com/science/inspiration-4-how-much-is-a-ticket-to-space.

Keohane, Nathaniel O., and Richard J. Zeckhauser. "The Ecology of Terror Defense." *The Journal of Risk and Uncertainty* 26, no. 2/3 (2003): 201–29.

Kofman, Ava. "The FBI Is Building a National Watchlist That Gives Companies Real-Time Updates on Employees." *The Intercept*, February 4, 2017. https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/.

Lapham, Robert. *Risk Analysis and Security Countermeasure Selection*. CRC Press, 2015. https://doi.org/10.1201/b18632.

Lieu. Space Infrastructure Act, Pub. L. No. H.R.3713 (2021). https://www.congress.gov/117/bills/hr3713/BILLS-117hr3713ih.pdf.

Lowe, Katherine A. "Safety in the Sky: Will Reforming and Restructuring the TSA Improve Our Security or Merely Infringe on Our Rights?" *Journal of Air Law and Commerce* 81, no. 2 (2016): 291–319.

Lum, Cynthia, Leslie W. Kennedy, and Alison Sherley. "Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research." *Journal of Experimental Criminology*, no. 2 (2006): 489–516. https://doi.org/10.1007/s11292-006-9020-y.

Martynski, Joseph. "EXIS Fact Sheet." TSA, May 2021.

Miller PhD, Gregory D. "Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists: Nonstate Threats in Space." *Air & Space Power Journal* 33, no. 3 (2019): 33–51.

Morgan, Daniel. *Commercial Space: Federal Regulation, Oversight, and Utilization*. CRS Report No. R45416. Washington, DC: Congressional Research Service, 2018. https://crsreports.congress.gov/product/details?prodcode=R45416.

Morgan Stanley. "Space: Investing in the Final Frontier." Morgan Stanley. Accessed February 3, 2022. https://www.morganstanley.com/ideas/investing-in-space.

Mosher, Dave. "SpaceX Lost a Quarter of a Billion Dollars after One of Its Rockets Blew Up." *Business Insider*, January 13, 2017. https://www.businessinsider.com/spacex-financials-rocket-accident-costs-revenue-2017-1.

Murray-Tuite, Pamela M., and Xiang Fei. "A Methodology for Assessing Transportation Network Terrorism Risk with Attacker and Defender Interactions." *Computer-Aided Civil and Infrastructure Engineering* 25 (2010): 296–410. https://doi.org/10.1111/j.1467-8667.2010.00655.x.

National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report." New York, NY, 2004. https://9-11commission.gov/report/.

Newbill, Colleen M. "Defining Critical Infrastructure for a Global Application." *Indiana Journal of Global Legal Studies* 26, no. 2 (2019): 761–79.

O'Brien, Lauren. "The Evolution of Terrorism Since 9/11." *FBI: Law Enforcement Bulletin 09/01/2011*, September 1, 2011. https://leb.fbi.gov/articles/featured-articles/the-evolution-of-terrorism-since-911.

OECD. "Remedying the Gender Gap in a Dynamic Space Sector." OECD iLibrary, 2022. https://www.oecd-ilibrary.org/sites/c5996201-en/1/2/3/index.html?itemId=/content/publication/c5996201-en&mimeType=text/html&_csp_=ffe5a6bbc1382ae4f0ead9dd2da73ff4&itemIGO=oecd&itemContentType=book.

O'Neal, Shannon E., and Michael T. Borgia. "TSA Revises Cybersecurity Requirements for 'Critical' Pipelines and LNG Facilities." *Davis Wright Tremaine LLP* (blog), August 22, 2022. https://www.dwt.com/blogs/privacy--security-law-blog/2022/08/cybersecurity-tsa-pipelines-liquified-natural-gas.

Price, Jeffrey, and Jeffrey S. Forrest. *Practical Aviation Security : Predicting and Preventing Future Threats*. 2nd ed. Waltham, MA: Elsevier Science & Technology, 2013. ProQuest.

Santifort, Charlinda, Todd Sandler, and Patrick T. Brandt. "Terrorist Attack and Target Diversity: Changepoints and Their Drivers." *Journal of Peace Research* 50, no. 1 (2012): 75–90. https://doi.org/10.1177/0022343312445651.

Schindelheim, Ramona. "Private Companies Propelling Job Growth in the Space Industry." *WorkingNation* (blog), June 2, 2021. https://workingnation.com/private-companies-propelling-job-growth-in-the-space-industry/.

Schmid, Alex P. *Handbook of Terrorism Prevention and Preparedness*. 1st ed. The Hague: ICCT Press, 2020. 10.19165/2020.6.0126.

Space Policy Online. "Space Law." Accessed February 7, 2022. https://spacepolicyonline.com/topics/space-law/.

Stein, Janice Gross, and Ron Levi. “Testing Deterrence by Denial: Experimental Results from Criminology.” *Studies in Conflict & Terrorism*, June 19, 2020. https://www.tandfonline.com/action/showCitFormats?doi=10.1080/1057610X.2020.1777710.

Stewart, Mark G, and John Mueller. “Terrorism Risks and Cost-Benefit Analysis of Aviation Security.” *Risk Analysis : An Official Publication of the Society for Risk Analysis* 33, no. 5 (May 2013): 893–908. https://doi.org/10.1111/j.1539-6924.2012.01905.x.

Sweeny, Keelan, and Eric Begin. “BASE Fact Sheet.” TSA, June 2019.

Transportation Security Administration. “Aviation Programs | Transportation Security Administration,” https://www.tsa.gov/for-industry/aviation-programs.

———. “Enforcement Sanction Guidance Policy,” February 8, 2021. https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf.

———. “First Observer Brochure Final,” Accessed October 6, 2022.

———. “First Observer Plus Program Overview.” Accessed October 6, 2022.

———. “Screening Partnership Program.” Accessed November 7, 2022. https://www.tsa.gov/for-industry/screening-partnerships.

———. “Surface Transportation.” Resources. Accessed November 16, 2022. https://www.tsa.gov/for-industry/resources.

———. *Transportation Security Administration Budget Overview*. 2023. https://www.dhs.gov/sites/default/files/2022-03/Transportation%20Security%20Administration_Remediated.pdf.

———. “TSA by the Numbers.” May 19, 2021. https://www.tsa.gov/news/press/factsheets/tsa-numbers.

———. “TSA Highlights the Top 21 Accomplishments in Transportation Security to Close Out 2021.” Press Release, January 18, 2022. https://www.tsa.gov/news/press/releases/2022/01/18/tsa-highlights-top-21-accomplishments-transportation-security-close.

———. “TSA Surface Transportation Security.” February 2020. https://www.tsa.gov/sites/default/files/guidance-docs/surface_101_to_stakeholders_0.pdf.

“Transportation Systems Sector | CISA.” Accessed March 22, 2022. https://www.cisa.gov/transportation-systems-sector.ent/title-33/chapter-I/subchapter-H/part-101/subpart-E/section-101.514.

Wallace, Ryan, and Jon M. Loffi. “The Unmitigated Insider Threat to Aviation (Part 2): An Analysis of Countermeasures.” *Springer Science + Business Media* 7 (September 2014): 307–31. https://doi.org/10.1007/s12198-014-0150-6.

White House. “Executive Order on the National Space Council.” The White House, December 1, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/01/executive-order-on-the-national-space-council/.

Wiater, Patricia. “On the Notion of ‘Partnership’ in Critical Infrastructure Protection on JSTOR.” *Cambridge University Press* 6, no. 2 (n.d.): 255–62.

Williams, Heather J. and Kristin Van Abel et al. *The Risk-Mitigation Value of the Transportation Worker Identification Credential: A Comprehensive Security Assessment of the TWIC Program*. RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3096.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California