Mitigating the Threat: A Strategic Checklist for Securing Federal Courthouses

by David Charles Hyatt

B.A. Criminal Justice, May 2014, American Public University System
M.A. Political Science, May 2017, American Public University System
M. S. Data Analytics, December 2020, The George Washington University

A Praxis submitted to

The Faculty of
The School of Engineering and Applied Science
of The George Washington University
in partial fulfillment of the requirements
for the degree of Doctor of Engineering

August 15, 2025

Praxis directed by

Curtis Larsen
Professorial Lecturer in Engineering and Applied Science

The School of Engineering and Applied Science of The George Washington University certifies that David Charles Hyatt has passed the Final Examination for the degree of Doctor of Engineering as of July 24, 2025. This is the final and approved form of the Praxis.

Mitigating the Threat: A Strategic Checklist for Securing Federal Courthouses

David Charles Hyatt

Praxis Research Committee:

Curtis Larsen, Professorial Lecturer in Engineering and Applied Science, Praxis Director

Daniel Veit, Professorial Lecturer in Engineering and Applied Science, Committee Chair

Cory Fagan, Professorial Lecturer in Engineering and Applied Science, Committee Member

© Copyright 2025 by David Charles Hyatt
All rights reserved

Dedication

This work is dedicated to all who protect, serve, and stand watch. To the first responders and public servants who show up daily, often without recognition, to keep our communities safe.

To my close friends and colleagues, thank you for challenging and keeping me grounded. I am especially thankful for those who have kept me focused and never let me give up when things got tough.

And to my family, especially my children, everything I do is for you. You are my reason. You push me to keep going, to be better, and to set an example I hope you'll be proud of.

Acknowledgement

Thank you, Dr. Curt Larsen, for all the conversations that sparked ideas and for letting me chase every rabbit hole without hesitation. To Dr. Shahram Sarkani, thank you for giving me this opportunity. You took a chance, and without your support, I would not have gotten this far. Finally, Dr. Thomas Mazzuchi, thank you for your mentorship, patience, and guidance over the past four years. You've been my greatest advocate and support system throughout this process. I would not have considered this an option had you not encouraged me to do so. I wouldn't be here without any of you. Thank you all for everything.

Abstract of the Praxis

Mitigating the Threat: A Strategic Checklist for Securing Federal Courthouses

Federal courthouses are a critical infrastructure for the United States justice system, a cornerstone for our democracy. As one of the pillars of our democratic society, these facilities are vulnerable to various and evolving threats; however, the current security posture remains fragmented and reactive. This praxis develops a systems engineering-based prototype checklist that leverages incident data with cross-sector best practices that align with stakeholder responsibilities. The praxis drew from 1,273 incident reports generated from the Southern District of New York between 2013 and 2024, identifying vulnerabilities rooted in systemic gaps, particularly in communication, role clarity, and procedural consistency. Using root cause analysis methods, the highlights the compounding nature of the underlying weakness in these reports. Through this process, a prototype checklist was developed to enhance the resilience of these facilities through integrated insights from sectors such as aviation and healthcare. This checklist is a proactive tool that institutionalizes accountability, standardizes operational procedures, and supports decision-making. The ultimate objective of the praxis was to demonstrate how a data-driven checklist can significantly reduce the impact and likelihood of disruptive incidents while strengthening the public's trust in the federal judiciary.

Table of Contents

Dedication iv

Acknowledgement v

List of Figures xi

List of Tables xii

List of Acronyms xiii

Chapter 1: Introduction 1

1.1 Problem Statement 1

1.2 Thesis Statement 2

1.3 Research Objectives 4

1.4 Research Questions and Hypotheses 6

1.5 Research Limitations 7

1.6 Praxis Organization 9

Chapter 2: Literature Review 11

2.1 Protecting the Courts 11

2.1.1 Interagency Security Committee 11

2.1.2 United States Marshals Service 15

2.1.3 Administrative Office of the United States Courts 16

2.1.4 General Services Administration 18

2.1.5 Department of Homeland Security 20

2.1.6 Conclusion 21

2.2 Significant Incidents against the Judiciary 21

2.2.1 Timothy McVeigh and the Oklahoma City Bombing 22

2.2.2 Violence Inside Courthouses 22

2.2.3 Deficiencies Exposed Outside Courthouses 23

2.2.4 Targeted Attacks on Judicial Personnel 23
2.2.5 Violence upon Entry 23
2.2.6 Historical Attacks on Judges 24
2.2.7 Other Notable Incidents 24
2.2.8 Conclusion 25
2.3 Best Practices for Protecting Large Facilities 25
2.3.1 Risk Assessments 26
2.3.2 Defense-in-Depth 27
2.3.3 Personnel and Training 29
2.3.4 Interagency Collaboration 30
2.3.5 Emerging Technologies 32
2.3.6 Continuous Improvements 34
2.3.7 Conclusion of Best Practices 36
2.4 Risk Assessment Methodologies 36
2.4.1 Incident Reporting 37
2.4.2 Root Cause Analysis 39
2.4.3 Checklists 41
2.4.4 Data Collection 48
2.4.5 Data analysis 49
2.4.6 Conclusion of Risk Assessment Methodologies 50
2.5 Literature Review Conclusion 51
Chapter 3: Methodology 54
3.1 Statement of Purpose and Problem Boundary: What's In and What's Out 55
3.1.1 In-Scope Elements 55
3.1.2 Out-of-Scope Elements 56
3.1.3 Justification for Boundary Definition 56
3.2 Understanding the scope of the problem – Event Trees and Ishikawa diagram with Reason's Swiss Cheese 57
3.3 Current Best Practice Vulnerabilities 60
3.4 Data to Drive Home Gaps 64

3.4.1 Incident Report Collection 64
3.4.2 The Data Cleaning and Preparation Process 66
3.4.3 Categorization of Incidents 67
3.4.4 Conclusion of Data to Drive Home Gaps 68
3.5. Checklist Elements to Alleviate the Gaps 68
3.6 Conclusion to Methodology 71
Chapter 4: Results and Findings 73
4.1 RQ 1: What are the current courthouse security procedures in place, and how effective are they in mitigating operational and threat-based risks in high-consequence judicial environments? 73
4.2 RQ2: What are the most frequent and preventable security failures occurring in federal courthouses, and what systemic factors contribute to them? 83
4.2.1 Broader Implications Across Judicial Districts 86
4.2.2 The Role of a Standardized Checklist in Risk Mitigation 87
4.3 RQ3: How can incident reporting data be structured and analyzed to inform proactive, checklist-based security interventions? 88
4.4 RQ4: What design features are essential to ensure the adoption, usability, and effectiveness of a security checklist in a multi-agency courthouse environment? 91
4.5 RQ5: In what ways does an interdisciplinary checklist framework improve risk visibility, role clarity, and operational consistency across courthouse security stakeholders? 93
4.6 The Prototype 95
4.6.1 Framework and Function 101
4.6.2 Checklist User Guide and Implementation Protocol 104
4.7 Conclusion 105
Chapter 5: Discussion and Conclusions 107
5.1 Conclusion 107
5.2 Contributions to Body of Knowledge 109

5.3 Limitations and Delimitations 110

5.3.1 Limitations 110

5.3.2 Delimitations 111

5.4 Policy and Future Research Recommendations 112

5.4.1 Policy Recommendations 112

5.4.2 Future Research Directions 113

References 115

List of Figures

Figure 1: Integrating Courthouse Security 21
Figure 2: Defense-in-Depth Model for Courthouse Security 28
Figure 3: Event Tree Diagram 58
Figure 4: Fishbone Diagram with Swiss Cheese Model.....59
Figure 5: Map of Methodology 71
Figure 6: Potential Undesired Scenarios 79
Figure 7: Operational Risk Factors Leading to Security Vulnerabilities at SDNY.....86

List of Tables

Table 1: In-Scope vs. Out-of-Scope Elements 57
Table 2: Current Best Practices in Facility Security.....63
Table 3: Sample of Incident Data 66
Table 4: Incident data with classification and general description.....67
Table 5: Problem Categories and Examples.....68
Table 6: Checklist Elements to Mitigate Security Gaps.....70
Table 7: Operational Risk Factors Leading to Security Vulnerabilities at SDNY 83
Table 8: Mapping of Incident Categories to Checklist-Based Security Interventions 90
Table 9: Prototype Interagency Courthouse Security Checklist.....97
Table 10: Checklist User Guide and Implementation Protocol.....104

List of Acronyms

ACSO	Armed Contract Security Officer
AG	Attorney General
AOUSC	Administrative Office of the United States Courts
BJS	Bureau of Justice Statistics
CBP	Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
CPS	Cyber-Physical Systems
CSO	Court Security Officer
CCTV	Closed-Circuit Television
DCJS	Division of Criminal Justice Services
DHS	Department of Homeland Security
DOJ	Department of Justice
DUSM	Deputy United States Marshal
eTVRA	Enhanced Threat and Vulnerability Risk Assessment
FAS	Federal Acquisition Service
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Services
FSC	Federal Security Committee
FSL	Facility Security Level
GSA	General Services Administration
GIS	Geographic Information Systems

ICE	Immigration and Customs Enforcement
ICS	Incident Command System
ISC	Interagency Security Committee
IT	Information Technology
JSD	Judicial Security Division
JSU	Judicial Security Unit
LOP	Level of Protection
LDA	Latent Dirichlet Allocation
MOU	Memorandum of Understanding
NIBRS	National Incident-Based Reporting System
NIMS	National Incident Management System
OCS	Office of Court Security
OEP	Occupant Emergency Plan
OSHA	Occupational Safety and Health Administration
OT	Operational Technology
PBS	Public Building Service
PII	Personally Identifiable Information
PIDS	Perimeter Intrusion Detection System
SDNY	Southern District of New York
SEIPS	Systems Engineering Initiative for Patient Safety
SOP	Standard Operating Procedures
SSO	Special Security Officer
TSA	Transportation Security Administration

USAO United States Attorney's Office

USDJ United States District Judge

USMS United States Marshals Service

VMP Vulnerability Management Program

Chapter 1: Introduction

On September 24, 1789, President George Washington approved the Judiciary Act of 1789 into law (United States Courts, 2019). It was one of the first acts of the First United States Congress, and it established the federal judiciary. This legislation formed the United States' judicial system and established an effective federal court system to interpret and apply federal law.

Federal courthouses are vital to the nation's judicial system. Their continued viability is essential in facilitating the resolution of legal disputes and the fair dispensing of justice. Federal courthouses serve as theaters of the judicial process that manifest fairness, neutrality, and the truth-finding function of the judicial system, inspiring public confidence in the courts and promoting the effective administration of justice in a democratic society. These courthouses are essential to the efficient operation of the U.S. judicial system. Yet their symbolism as agents of the rule of law exposes them to vulnerabilities.

1.1 Problem Statement

Federal courthouses have been the victim of many malevolent acts (Campbell & Reinkensmeyer, 2007) throughout history that include bombings, arson, and organized armed raids. These attacks are frequently intended to inflict widespread damage, obstruct the administration of justice, intimidate court personnel and undermine public confidence in the administration of justice. Past occurrences have inflicted damage to physical assets as well as human beings, undermining the level of public trust. Maintaining the integrity of the courts requires secure facilities and corrective action to counteract deficient security procedures (Zaruba, 2007). Protecting these facilities demands an integrated

approach involving advanced threat detection, risk management, and effective coordination among federal, state and local agencies. These measures are necessary to prevent threats and deterring attacks, to maintain business continuity, and to safeguard personnel, judges, court employees, and visitors. This background motivates the formulation of the following problem statement in this study:

Currently, there is no systematic method for evaluating and monitoring the variety of the dynamic threats to the successful operation of the federal courthouse facilities that exist across jurisdictions, and without an agnostic and scalable, all-hazards approach, these facilities remain vulnerable to operational disruption, reputation harm and physical harm.

1.2 Thesis Statement

Efforts are undertaken to enhance security within these courthouses; however, the current practices do not offer a framework that is adaptable or efficient enough to address the variety and dynamic nature of potential threats. This creates the following potential issues which may increase the risk to the facilities:

- Defective Physical Security: Poor maintenance and training procedures can lead to gaps in physical security
- Poor communication amongst stakeholders: Securing the judiciary requires strong communication and collaboration.
- Insider threats: The lack of effective surveillance and control over personnel can lead to insider abuse of critical areas.

This study is motivated by the necessity to close the gaps that are creating current or prospective vulnerability to the judiciary. The research is intended to protect federal courthouses by enabling the practical and scalable construction of safe, secure, and continuously operable courthouses based on interdisciplinary knowledge and innovative approaches. The research verified the following statement:

Physical security measures, personnel procedures, procedural protections and technology solutions can be organized into a thorough and operationally effective security checklist that can be used to focus and augment security at Federal courthouses and protect the justice system.

The rationale is to establish a structured, evidence-based instrument for the security of courthouses that fosters:

- Proactive Risk Management: Understand exposure to risk and match defenses to industry best practices.
- Standardized Security Procedures: Discuss and resolve jurisdictional and local issues, and localized deficiencies.
- Building and Improving Preparedness: Develop clear procedures that can be followed to prevent, detect and respond appropriately to physical and cyber incidents.
- Building Public Trust: Increase the public's trust in the ability of the judiciary to do its business in a safe, undisturbed manner.

A systematic document outlining measures necessary for courthouse security provides an approach that is pragmatic and adjustable to current gaps. By

assessing historical data, risk assessment models, and best practices for securing facilities, this approach can facilitate hardening this critical infrastructure against new and evolving threats, resulting in a more resilient and sustainable future. Federal courthouses can accomplish the following by instituting a checklist:

- Reduce Risk: Secure against potential vulnerabilities that could lead to unauthorized personnel and unauthorized physical and cyber access leading to improved continuity of operations and safeguarding core judicial functions and delivering uninterrupted access to justice, despite threats.
- Public Trust: Provide the assurance of a safe facility which enhances public trust.
- Agility: Be able to respond to emerging threats by updating protocols on a timely basis and incorporating best practices.

The establishment and implementation of a checklist thus also reflects higher national objectives in safeguarding key institutions even as it protects judges, court support staff and the public.

1.3 Research Objectives

The focus of this research is to produce a prototype evidence-based security checklist, suitable for the operational and risk landscape of federal courthouses. To do this, the research is directed toward the following research objectives:

- **Systematic review and collation of available information from published literature, policy sources and procedural documents on courthouse security**.

Review information on federal agency guidance on judicial security, academic research regarding facility security, and industry reports to develop a baseline knowledge of how wider courthouse security is currently being practiced and what challenges currently exist.

- **Assimilation, organization and analysis of factual threat and incident information regarding the federal judiciary.**

  A comprehensive analysis of facility incident reports, identify repeated points of vulnerability, operational failure, and systemic risk that an intervention like the checklist might address.

- **Evaluation and adaptation of checklist methodologies and best practices from highly reliable sectors**.

  Validated checklist-based systems are used in areas such as healthcare, aviation or critical infrastructure protection to address complex risks. This goal analyzes their development, implementation, and effectiveness to translate cross-sector learning into courthouse-specific applications.

- **Development of a Courthouse Security Checklist based on data analysis, literature review, and validated models from other sectors.**

  The resulting product will be a tool for enhancing institutional preparedness, reducing human error, and solidifying security operations by implementing procedures that are consistent and ensure accountability.

1.4 Research Questions and Hypotheses

This research addresses the issues as they relate to the use of extensive checklists, personnel training, and high technology to bolster courthouse security. The research questions for the study are as follows:

Research Question 1 (RQ1): What are the current courthouse security procedures in place, and how effective are they in mitigating operational and threat-based risks in high-consequence judicial environments?

RQ 2: What are the most frequent and preventable security failures occurring in federal courthouses, and what systemic factors contribute to them?

RQ3: How can incident reporting data be structured and analyzed to inform proactive, checklist-based security interventions?

RQ4: What design features are essential to ensure the adoption, usability, and effectiveness of a security checklist in a multi-agency courthouse environment?

RQ5: In what ways does an interdisciplinary checklist framework improve risk visibility, role clarity, and operational consistency across courthouse security stakeholders?

By answering the above research questions, this study's aim is to provide insights which can inform the development of a robust, adaptive security strategies for federal courthouses.

In addressing these research questions, the following hypotheses are considered for evaluation:

Hypothesis 1 (H1): Current security procedures within the courthouse are inconsistently implemented and only partially effective due to procedural gaps, poor communication, and inadequate incident reporting standards.

H2: The most frequent and preventable security failures occur due to insufficient training,

communication breakdowns, and poor maintenance practices.

H3: Structuring and analyzing incident data can identify patterns that will directly influence the creation of a checklist by identifying operational risks and vulnerabilities.

H4: Security checklists that are adaptive, incorporate role-specific tasking, and encourage collaboration are more likely to be consistently used and enhance the effectiveness of the security posture in and around the courthouse.

H5: An interdisciplinary checklist will clarify roles and responsibilities and improve operational efficiency by aligning stakeholder expectations and procedures and reducing ambiguity in security operations.

1.5 Research Limitations

When designing a prototype checklist for security in the federal courthouse several limitations must be kept in mind:

- Data Sensitivity: A key challenge that must be overcome is the accessibility of sensitive data. The physical protection of federal courthouses almost always involves classified or sensitive information that may be off limits because of security clearance and privacy rules. This restriction might slow down attempts to gather fine-grained data about current security imperfections and practices. To remedy this situation, the researcher has reviewed each incident report and compiled a summary of each incident, removing all personally identifiable information (PII) and pedigree information pertaining to individuals or units involved.
- Legal and Regulatory Barriers: There are also legal and regulatory barriers. Federal Courthouses are subjected to many laws and regulations including

the Federal Protective Service (FPS) and the United States Marshals Service (USMS). These laws can limit what forms of security can be recommended or taken. This study must ensure the proposed checklist is legally valid, and to what extent changes can be implemented to stay within the framework of existing legal norms.

- Geography and Architecture: Courthouse facilities are often located in various geographical locations. This makes the checklist difficult to produce due to varying architecture, site characteristics, and duty station requirements. Older courthouses, which are frequently historic, can contain structural impediments that newer buildings might not. To overcome this, the prototype checklist is flexible and able to be modified to suit the needs of individual facilities.
- Rapid Development of Technology: Given the speed with which security technologies, like surveillance and threat detection, get outdated, some checklist items may be irrelevant after some time. The checklist addressed this by focusing on security basics and looking to incorporate new technology when possible. Also, leaving the suggestion for regular updates to ensure that the latest technology developments and the most up-to-date security measures are in place.
- Human factors: Security systems are still very much dependent on human behavior and compliance and challenges such as insider threats and human mistakes cannot be resolved with physical security. Staff education,

awareness programs and periodic security audits to minimize behavioral risk in concert with physical security upgrades are guided by the checklist.

- Budgetary Limitations: Adding modern security measures can be expensive, and courthouses may have constrained funding or other needs. To address this, the prototype does not include recommending facility hardening or security system upgrades.
- Interagency Collaborations: Implementation of an enhanced security posture requires cooperation amongst stakeholders. The checklist serves to facilitate interagency partnerships and coordination by providing a framework for conflict resolution among stakeholders and decision makers.
- Evaluation: Measuring a protective posture is difficult. There is no way to accurately gauge the effectiveness of a system until it has been tested in an unsimulated environment. To address this, the research shows how best practices could have prevented the occurrence of various incidents discussed in the study.

1.6 Praxis Organization

The structure of the praxis provides a clear presentation of the research development. Chapter 1 provides background information, a problem statement, aims of the research, and introduces limitations. Chapter 2 conducts a comprehensive review of existing literature on courthouse security, discusses previous incidents against the judiciary, explores interagency coordination and its challenges, and explores evidence-based effectiveness of checklists seen throughout various industries. Chapter 3 outlines the methodology employed to design and justify the security checklist.

It incorporates a mixed-methods approach using Event Tree Analysis, the Swiss Cheese Model, and the Ishikawa Diagram. This integrated framework addresses courthouse-specific vulnerabilities through procedural standardization, system-level diagnostics, and simulation-driven validation. Chapter 4 presents the findings from the analysis of incident reports from the Southern District of New York (SDNY), highlighting vulnerabilities and demonstrating how a security checklist can address operational gaps and improve courthouse security outcomes. Chapter 5 provides the summary, policy implications and recommendations for future research.

Chapter 2: Literature Review

This literature review provides a background for examining the risks confronting the federal judiciary and the potential methods that can be used to mitigate those risks. The review begins with an overview of the various stakeholders responsible for protecting the judiciary. It clarifies roles, responsibilities, and areas of overlap. Next, it transitions into discussing realized attacks. Following this, it examines best practices in physical security for large facilities to identify principles that apply to those required in federal courthouses. Finally, it reviews established risk assessment methodologies, focusing on incident reporting, root cause analysis, checklists, and data collection and analysis.

2.1 Protecting the Courts

Security around a federal courthouse is a shared responsibility among several stakeholders. Built from the standards established by the Interagency Security Committee, each stakeholder brings a unique mandate, authority, and operational nexus. Understanding who is involved and the collaborative architecture of this system is essential for the development of an operational checklist that integrates roles, eliminates redundancy, and opens communication to enhance collaboration across judicial facilities with diverse requirements.

2.1.1 Interagency Security Committee

The Interagency Security Committee (ISC) was established to enhance the quality and effectiveness of security in non-military government buildings. The standards set forth apply to any facility occupied by nonmilitary federal employees. These buildings include:

- Existing buildings, new construction, or major reconstructions
- Owned, to be purchased, or leased facilities
- Stand-alone facilities, federal campuses, and where appropriate, individual facilities on federal campuses
- Special-use facilities

The ISC was founded on October 19, 1995, by President Bill Clinton under Executive Order (EO) 12977, in response to the Oklahoma bombing. This was the deadliest act of domestic terrorism to ever occur in the United States. It exposed physical security vulnerabilities, leading to the reassessment of how the federal government secures its personnel and property.

It was created to serve the following purpose:

- Develop and implement security standards for non-military federal facilities in the U.S. Coordinate security policies across agencies.
- Provide a permanent interagency body to address government-wide physical security challenges.

Prior to establishment, there were no existing standards for securing these facilities. This committee filled the gap by centralizing the development of risk-based standards and best practices.

The ISC is Chaired by the Cybersecurity and Infrastructure Security Agency (CISA) and has 66 member agencies. These agencies include the Department of Homeland Security (DHS), the General Services Administration (GSA), the USMS, and the Administrative Office of the United States Courts (AOUSC), which are tasked with securing federal courthouses.

The ISC issues policies and best practice guides across several operational domains:

- Risk Management Framework
- Facility Access Control
- Security Convergence
- Occupant Emergency Programs (OEP)
- Armend Contract Security Officers (ACSO)
- Compliance Benchmarking

Below is a list of guidelines and policies released by the ISC:

- Risk Management Framework: *The Risk Management Process* (2024) provides a five-step approach for identifying Facility Security Levels (FSL), assessing risk, defining Levels of Protection (LOP), implementing mitigation strategies, and measuring performance. It also describes the responsibilities for agencies, security personnel, and Facility Security Committees (FSCs)
- Facility Access Control: In *Facility Access Control* (2020), the ISC describes best practices for identification credentialing (e.g., PIV cards), foreign visitor management, and security screening procedures. These standards are designed to foster consistency in access control mechanisms government-wide
- Security Convergence: The 2022 guide, *Security Convergence: Achieving Integrated Security*, promotes an integrated model for physical, cybersecurity, and information assurance. It advocates a mission-focused planning approach that includes defense-in-depth, supply chain risk management, and

performance measures. This document highlights the urgency for bridging traditional and digital security domains considering evolving threats.

- Occupant Emergency Programs (OEPs): The ISC's 2024 update to *Occupant Emergency Program,* mandates comprehensive emergency preparedness procedures, including threat assessments, special population planning, emergency communications, and drills. It emphasizes the roles of Designated Officials, Occupant Emergency Coordinators, and the Occupant Emergency Organization in maintaining life-safety continuity during crises.
- Armed Contract Security Officers (ACSOs): Acknowledging the importance of frontline security personnel, the 2019-Armed *Contract Security Officers in Federal Facilities,* best practice guide, sets the minimum hiring, training, equipment, and conduct standards for ACSOs. This ensures consistent standards and professional conduct of these guards at federal facilities.
- Compliance and Benchmarking: The 2024 *ISC Compliance Policy and Benchmarks* provide a set of tools to compare the level of implementation of ISC standards used by agencies. They describe the reporting responsibilities, the verification process, and the responsibility of Senior Officials in the department or agency. This framework enables the ISC to monitor performance and assist in continuous improvement related to security at federal facilities.

These documents created by the ISC take a systems approach to federal facility protection. They outline and define technical countermeasures, training standards, institutional responsibilities, and verification mechanisms, shifting the federal security

posture from reactive to proactive, risk-informed, and integrated operational model. The comprehensive guidance provided by the ISC is foundational for any federal agency with a mission of protecting personnel and infrastructure. Its relevance provides oversight, collaboration, and resilience planning among stakeholders. The evolving threat climate requires standards that unify in securing the physical and operational integrity of all federal facilities.

2.1.2 United States Marshals Service

The USMS is the nation's first and oldest federal law enforcement agency. Its origins date back to 1789, following the passing of the Federal Judiciary Act, creating the Office of the United States Marshals (United States Marshals Service, 2024). In 1969, the agency formally unified to support the work of the various districts nationwide. This unification provided structured guidance and oversight for operational functionality within the district (United States Marshals Service, 2024). As an agency within the Department of Justice (DOJ), the agency operates under the direction of the Attorney General (AG) and is led by a presidentially appointed director (United States Marshals Service, 2024).

The mission of the USMS is broad and integral to the operation of the federal justice system. Its core responsibilities include securing federal court facilities and ensuring the safety of judges, jurors, and court staff; apprehending fugitives; managing and transporting federal prisoners; executing federal court orders; overseeing the seizure and disposition of illegally obtained assets; protecting government witnesses and their families; and facilitating the collection and disbursement of court-ordered funds. Each of the 94 federal judicial districts is led by a U.S. Marshal, supported by a national force of

over 3,800 deputy marshals and criminal investigators, and more than 1,500 administrative staff and detention enforcement officers (United States Marshals Service, 2024).

The USMS is the lead agency for protecting the federal judiciary. Approximately 5,600 Court Security Officers (CSOs) are deployed across all federal judicial districts and appellate courts to provide screening, patrol, and courtroom security (United States Marshals Service, n.d.). These officers play a vital role in maintaining order and safety within courthouse environments, particularly during high-profile or high-risk proceedings. The agency's Threat Management Center operates around the clock, processing over 1,000 threats against judicial officials annually (United States Marshals Service, n.d.). This number continues to rise due to increasing societal tensions and digital harassment.

2.1.3 Administrative Office of the United States Courts

The Administrative Office of the U.S. Courts (AOUSC) was established by an act of Congress on November 6, 1939, marking the first time the federal judiciary was granted independent authority over its own budgetary and personnel matters, separate from the executive branch (United States Courts, 2024). Prior to this, administrative responsibilities for the courts had shifted over time from the Treasury Department to the Interior Department in 1849, and finally to the Department of Justice in 1870 (United States Courts, 2024). Although the Conference of Senior Circuit Judges served as an advisory body, it lacked administrative authority (United States Courts, 2024). By the early 20th century, growing concerns emerged among judges and legal scholars regarding the inefficiency and potential overreach of executive control through the Justice

Department. Reform advocates, including judges, academics, and Justice Department officials, argued that the effective administration of justice and the preservation of judicial independence required a separate agency overseen by the judiciary itself (United States Courts, 2024). While some proposals called for incremental reforms, such as separate court appropriations or administrative roles for senior judges, broader consensus eventually coalesced around the need for a centralized, judiciary-run administrative body.

The AO was ultimately created in response to these concerns and continues to serve as the central support agency for the federal judiciary (United States Courts, 2024). It manages a wide range of functions, including budget preparation and submission, legislative analysis, personnel administration, and coordination of court services such as clerks, court reporters, probation officers, and public defenders (United States Courts, 2024). Partnering with GSA and the USMS, the AO plays a critical role to ensure each courthouse is secure, functioning efficient and effectively, and meets the operational needs of the judiciary.

Beyond the administrative it provides, the AO has a vital role in emergency preparedness, judicial security by overseeing programs such as Vulnerability Management Program (VMP), redaction of Personally Identifiable Information (PII), and DeleteMe which seeks to reduce or eliminate the electronic footprint of the judiciary and their family members. In 2023 alone, the AO responded to over 500 credible threats, underscoring the growing need for robust protective measures (United States Courts, 2024).

To support this mission at the district level, federal courthouses across the country utilize an Occupant Emergency Plan (OEP), which outlines procedures for responding to

a range of emergencies, including fire, explosions, medical incidents, hazardous materials, civil unrest, and active shooter events (OEP, 2024). The OEP provides an overview but not an organized list that one might want to reference during a crisis.

2.1.4 General Services Administration

The General Services Administration (GSA) was established on July 1, 1949, at the direction of President Harry Truman, to consolidate the administrative work of the federal government (GSA, n.d.). The formation of this agency brought together several existing agencies and offices, including the National Archives Establishment, Federal Works Agency, Public Buildings Administration, Federal Supply Administration, Office of Contract Settlement, and War Assets Administration. The idea behind the consolidation was to expedite decision making for federal supplies and workspaces (GSA, n.d.).

GSA's first duties were comprehensive and served the post-war requirements of the federal government. Those responsibilities involved dealing with war surplus property, keeping government records, being prepared for emergencies, stockpiling strategic materials to be used in wartime. It also oversaw the procurement and distribution of office supplies and supervised special projects like hemp plantations in South America (GSA, n.d.). The authorizing legislation has through the years been expanded to cover three major fields of service to the federal government: real estate management, acquisition services, and technology solutions. Through its Public Buildings Service (PBS) and Federal Acquisition Service (FAS), GSA currently delivers workspaces for over 1 million federal civilian employees, preserves more than 480

historic federal buildings, as well as providing the procurement of cost-effective, high-quality goods and services to government organizations (GSA, n.d.).

GSA is an integral piece of the infrastructure to ensure the security of federal courthouses. As the owner and operator of courthouse and courtroom facilities, GSA is responsible for installing physical security enhancements that provide maximum protection to target infrastructure, including blast resistant windows, security vestibules bollards, and standoff perimeters. These features are developed to enhance the safety of judicial personnel and visitors working with the USMS and FPS (GSA, 2021). This role for GSA is particularly vital in capital projects and long-term planning, where early integration of security into architectural design can minimize long-term risk (Federal Emergency Management Agency, 2013).

Like the local court administration OEP, the *Facilities Standards for the Public Buildings Service (P100)* is an extensive document that outlines public building and site requirements for all the federal buildings produced by GSA. The P100 combines performance-based design with requirements that must be met for the facility to function safely, be accessible, and operate efficiently. Included in this document are considerations such as architectural design, structure, various systems, and fire protection. The P100 is a guiding instrument to maintain uniformity, code compliance, and best practices throughout all federal facilities (General Services Administration, 2024). However, it is not an operational handbook. This document establishes the facility requirements necessary to support safety. Not included are instructions specific to local court administration or the USMS necessary to ensure courthouse security.

2.1.5 Department of Homeland Security

The United States Department of Homeland Security plays an important role in protecting the U.S. from various of threats such as terrorist attacks and natural disasters (United States Department of Homeland Security, 2023). It was established in 2002 following the September 11th attacks in New York City. DHS brought together 22 federal agencies to streamline national security and emergency response capabilities (United States Department of Homeland Security, 2023).

With over 240,000 employees, DHS oversees major operational components such as the Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), Customs and Boarder Protection (CBP), Immigration and Customs Enforcement (ICE), the Coast Guard, and the United States Secret Service (USSS), all of which contribute to a comprehensive homeland security strategy.

Federal Protective Service (FPS) serves as the first line of defense for federal buildings (Reese, 2008), including federal courthouses. Operating under DHS, FPS is responsible for ensuring the physical security of federal facilities, with a focus on preventing unauthorized access and responding to emerging threats (Reese, 2008). Specifically, FPS supports courthouse security by installing and maintaining exterior surveillance systems, responding to incidents, and deploying temporary or permanent physical barriers around courthouse perimeters (Reese, 2008). FPS personnel also conduct vulnerability assessments to identify potential weaknesses and advise on mitigation strategies.

FPS deploys officers to support high profile trials, sensitive hearings, or escalated threat around the courthouse at the request of the USMS. During these events their officers work alongside the USMS and other local agency actively supporting the security

mission (United States Department of Homeland Security, 2020). With live threat monitoring, along with quick emergency response, the judiciary can be confident that they can continue to do business in a safe and secure environment without disruption to operations.

2.1.6 Conclusion

Courthouse security is the responsibility of many stakeholders, making it a complex system. Each has an important role. If one component of the system fails, it creates a risk. The USMS acts as a nexus for coordinating courthouse security (see Figure 1) and this can be a daunting task.

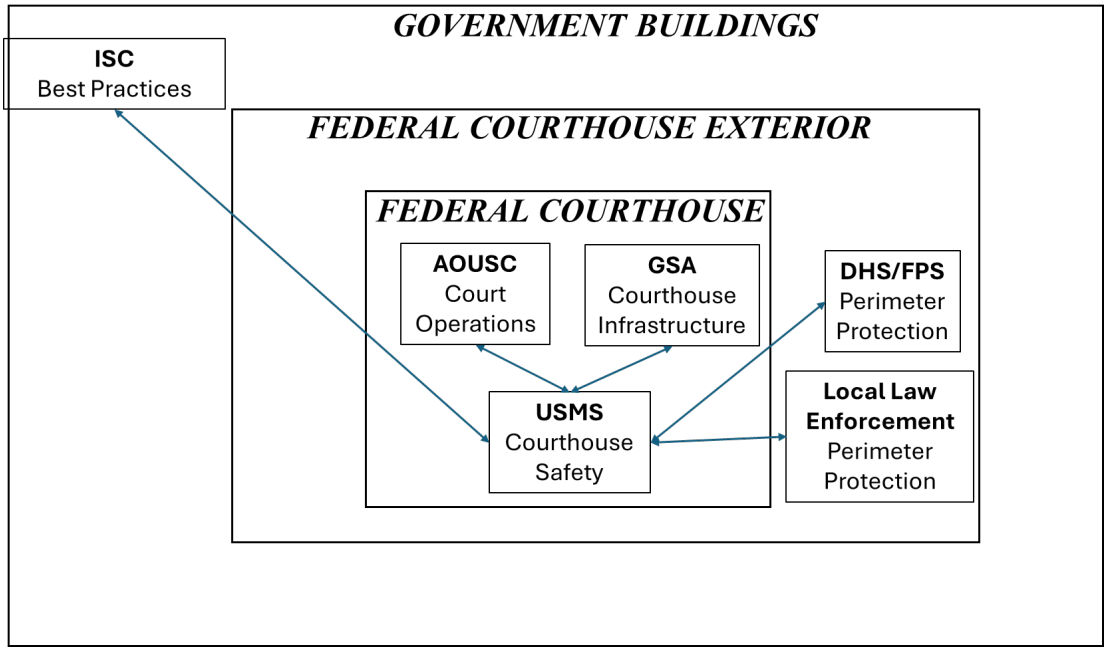

Figure 1: Integrating Courthouse Security

2.2 Significant Incidents against the Judiciary

Federal courthouses and judges have for decades been targeted for violent attacks, from sniper fire and bombings to armed incursions. These events exposed structural weaknesses in the definition of physical and procedural safeguards and reinforced the risk

in ignoring the need for a complete and nimble ordinance safeguarding courthouses (Dow, 2007). The following represent the range and variations of attacks on the judiciary.

2.2.1 Timothy McVeigh and the Oklahoma City Bombing

In April of 1995, Timothy McVeigh ignited a vehicle bomb adjacent to the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, killing 168 and injuring hundreds (Corley, Sr., Sozen, & Thornton, 1998). Driven by anti-government radicalism, the blast produced massive structural damage and became a national wake-up call to the threat of domestic terrorism (Corley, Sr., Sozen, & Thornton, 1998). This event led to drastic changes in building security policy, which included enhanced standoff, blast-resistant construction, and increased attention to perimeter surveillance (Bailey, 2023).

2.2.2 Violence Inside Courthouses

Violent incidents occurring within courthouses have highlighted procedural weaknesses in screening and detainee management. In 1995, during a court proceeding in King County, Washington, a man brought a firearm into the courthouse, fatally shooting his ex-wife and two others (Kelly, 1998). Similarly in 2005, Brian Nichols overtook a deputy in the Fulton County Court House in Atlanta, Georgia, garnered control of her weapon, and went on a deadly rampage that resulted in four deaths with Judge Rowland Barnes being one of the victims (Clark, 2014). Both incidents underscore the importance of strong internal protocols, such as secure conveyance of detainees and improved entry screening.

2.2.3 Deficiencies Exposed Outside Courthouses

A series of incidents outside of courthouse buildings have revealed deficiencies in perimeter and situational awareness. A nonfunctional grenade-wielding protestor entered a Seattle courthouse in 2005 leading to a standoff with law enforcement (Woodward, 2005). In 2006, a disgruntled father opened fire through the window of the Washoe County Courthouse in Nevada, injuring the presiding judge (Hidalgo, 2020). These incidents demonstrate the need for integrated perimeter surveillance, environmental design principles, and staff training to identify and respond to suspicious behavior.

2.2.4 Targeted Attacks on Judicial Personnel

Judges and their family members have also been subjects of attacks outside the courthouse. In 2011, United States District Judge (USDJ) John Roll was killed at a public event in Tucson, Arizona. In 2020, a man dressed like a delivery driver tried to kill USDJ Esther Salas at her home. The subject shot and killed her son, in addition to injuring her husband. The assailant was able to locate her home address (Bailey, 2023), provoking widespread debate over judicial privacy and digital vulnerability (United States Courts, 2023).

2.2.5 Violence upon Entry

Deficiencies in entry point screening have increased the risk of malicious activity upon entry into the facilities. In 2012, a man slipped by security at the Grays Harbor County Courthouse in Washington and assaulted a judge and deputy with a knife (KOMO, 2014). A gunman opened fire outside Forsyth County Courthouse in Georgia in 2014, injuring a police officer. He was shot later by officers ((Botelho, McLaughlin, & Hanna, 2014). The deficiencies of uneven screening protocols were exposed here and the

importance of multiple layers of defense, active monitoring and staff preparedness was emphasized.

2.2.6 Historical Attacks on Judges

Historically, judges have been attacked over their rulings. In 1979, Judge John H. Wood Jr. of the U.S. District Court for the Western District of Texas was murdered outside his home in San Antonio, Texas, by a hit man hired by a drug dealer (Mendoza, 2021). In 1989, Judge Robert Vance of the United States Court of Appeals (USCA) for the Eleventh Circuit was murdered by way of a mail bomb that was mailed by an angry litigant (Corley, Sr., Sozen, & Thornton, 1998). These assaults underscore the long overdue requirement for protective services, mail screening and threat assessment procedures.

2.2.7 Other Notable Incidents

In 2011, in Crawford County, Arkansas, a man entered the courthouse with an automatic weapon and wounded a case coordinator (Palazzolo, 2011). In 2012, a courthouse shooting in Tulsa, Oklahoma, left a police officer and a bystander injured (NBC, 2015). In Grand Marais, Minnesota, a convicted offender shot a county attorney and a victim's father inside a courthouse (CBS, 2011). Attacks in New Castle County, Delaware, and Chesterfield County, South Carolina, have also resulted in fatalities or serious injuries, reflecting the continued threat environment confronting judicial institutions.

The summer of 2020 witnessed an unprecedented wave of unrest near federal courthouses, particularly in Portland, Oregon. Protestors clashed with federal law enforcement officers at the Mark O. Hatfield U.S. Courthouse. Demonstrators vandalized

the building, set fires, and threw projectiles, prompting the deployment of additional federal agents and the erection of security barriers (Wilson & Levinson, 2021). In Oakland, California, a federal security officer was fatally shot outside the Ronald V. Dellums Federal Building during protests (Blankstein, Collins, & Zadrozny, 2020). These events illustrate risk faced by security personnel tasked with protecting judicial infrastructure amid periods of political and social instability This places emphasis on the need for an adaptable real-time threat response system.

2.2.8 Conclusion

The current threat environment across judicial facilities makes it clear that a multi-layered, proactive approach to security that covers various threats is necessary. The response to this challenge requires courthouses to have up-to-date security monitoring, effective screening procedures, strong perimeter security, and secure digital risk mitigation. This approach can standardize protection to ensure knowledge gained from prior events is absorbed.

2.3 Best Practices for Protecting Large Facilities

Security challenges exist in various government facilities such as federal courthouses and utility housing facilities. Having large and complex operations while being open to the public exposes them to a multitude of threats such as security equipment malfunctions and insider attacks. Additionally, these threats may occur simultaneously to compound impacts and challenge responses (Smith et al., 2016).

To be truly secure, a holistic approach to security is needed; one combining people, processes, and advanced technologies with security infrastructure and policy enforcement. Fischer and Halibozek (2015) affirm that integration should be

accompanied by explicit governance, structured protocols, and flexible feedback to respond to emerging threats. In this section, best practices for protecting large facilities are considered, including: risk assessments, layered defense measures, interagency coordination and strategic technological deployment for operational resilience.

2.3.1 Risk Assessments

Risk assessments can serve as a foundation and framework for a security plan to manage risk. According to Purpura (2013), risk assessments help identify risks, calculate the probability of a threat and its impact, and prioritize risk-mitigation techniques. For example, insider threat is becoming more prominent in security literature as it is not easily detectable and may potentially be catastrophic (Greitzer & Frincke, 2010).

Risk assessments may be quantitative and qualitative, involving expert analysis, stakeholder information, and empirical evidence. Good assessments weigh external threats and internal vulnerabilities. Kaplan and Garrick (1981) developed an organized model for risk assessment that combines the approach of probabilistic reasoning with result-oriented decision-making. Their method has been utilized in critical infrastructure protection, where trade-offs between cost, risk reduction, and resilience must be evaluated.

Best practice guidelines from organizations such as the U.S. Department of Homeland Security (United States Department of Homeland Security, 2020) and the Federal Emergency Management Agency (Federal Emergency Management Agency, 2013) emphasize the importance of all-hazards risk modeling. These frameworks encourage facilities to plan not just for likely threats but for low probability, high impact events. Scenario planning should include both historical incidents and emerging risks,

such as drone intrusions, cyber-physical attacks, and coordinated insider threats (Lewis, 2021).

To further strengthen risk assessment, the use of Geographic Information Systems (GIS) and predictive analytics is becoming common in facility security planning. Tools like risk heat maps and simulation software allow for visualization of threat vectors and resource allocation under different scenarios (Biringer, Vugrin, & Warren, 2013).

2.3.2 Defense-in-Depth

A key concept for defending large sites is defense-in-depth, essentially a series of layers of security as one gets closer to the core assets. Garcia (2008) defines three principal zones of physical security: perimeter security, intermediary zone, and core zone. Each principal outlines robust set up practices and procedures to follow:

- Perimeter Zone: Fences, bollards, barriers, motion-sensors, and video surveillance. Smith and Brooks (2012) describe how smart perimeter intrusion detection systems (PIDS) in conjunction with AI analytics with sensor inputs can detect false alarms from malicious activity. Additionally, lighting and landscaping are passive barriers which increase the likelihood of detection (Cozens et al., 2005).
- Intermediate Zone: Access control points, ID verification systems, metal detector equipment, and turnstiles. It is not sufficient to monitor the flow of information through technological controls. An environment must be present to routinely monitor behavior. Schneier (2003) argues that technological controls must be paired with human oversight, such as behavioral monitoring, to detect deception and social engineering tactics. Bi-directional authentication and anti-passback should be leveraged to minimize tailgating and misuse of credentials.

- Core Area: Data centers, USMS control rooms, or judicial chambers. This zone includes areas required methods for secured access and 24/7 surveillance. The National Research Council (2007) recommends integrating physical and cybersecurity controls in core zones to address converging threat domains.

Figure 2: Defense-in-Depth Model for Courthouse Security

The effectiveness of a layered security model, as seen in Figure 2, depends on seamless coordination between security zones and the routine evaluation of their interdependence. Dunlap et al. (2017) reveals that in organizations with locally operating security teams, each team responsible for handling a distinct layer, significantly reduces failures during emergency events.

Furthermore, regular intrusion testing, threat assessments, and continuity-of-operations exercises are needed to maintain resilience. These tests expose potential deficiencies to ensure integration and permit any adaptive enhancement deemed necessary. Pei et al. (2018) states dynamic defenses in high-risk environments require iteration and feedback loops. This means that defense measures must not remain static. An adequate security posture requires the system to be dynamic and adaptable to the threat environment.

2.3.3 Personnel and Training

Although technology plays a major role in protecting facilities, well-trained personnel are irreplaceable. No matter how high-tech or advanced the systems or the specific technology being used, it is up to humans to use, interpret, and act on the information. There are several examples in the literature where the most advanced built-in technology fails due to human error, miscommunication, and inconsistent policy enforcement.

Cole and Ring (2006) emphasize that "insider" vulnerabilities present the most difficult problems to identify and control. These threats often come from authorized individuals with a degree of access, so conventional security is rendered inadequate. These threats can come in the form of an intentional or unintentional act. Depending on the degree of expertise and familiarity of the security system.

Comprehensive self-defense measures should include:

- Mandatory Training Requirements: Security professionals must be appropriately trained on their specific role and the function of that position. This training includes emergency response protocols, threat recognition, de-escalation, and use of technology. Studies like Kraemer and Carayon (2007) show how ongoing, and refresher training helps enhance situational awareness, and reduces operational errors.
- Threat Detection Programs: Incorporating behavior analytics, anonymous reporting channels, digital tracking and deep background checking are crucial. Greitzer and Frincke (2010); Greitzer and Carley (2013) reason the emergent influence of technical filtering with psychosocial profiling justifies greater confidence in sensitive threat detection frameworks.

- Red Team Exercises: Simulated intrusion testing, phishing, or physical-breach attempts put staff can simulate a threat environment accessing individual or team response. Through this, both strengths and weaknesses in capabilities and knowledge of protocols can be exposed. Keller et al. (2019) found that red teaming encourages adaptive and process-driven thinking and increases staff confidence.

Apart from these, having a security culture is the most critical part. Security staff must feel comfortable reporting security-related concerns without fear of reprimand. Reinforcing that personnel are essential to the system is a must. As noted by Puhakainen and Siponen (2010), motivational and cultural factors are key determinants that can influence whether or not employees comply with security policies. Additionally, communication protocols for emergencies need to be normalized and practiced often. Communication hierarchies, decision support tools, and predefined roles should be established to reduce confusion and delay (National Institute of Standards and Technology, 2022). In high-stress environments, clear communication is the difference between containing and escalating a situation.

Ultimately, human resources constitute the cornerstone of any sound security strategy. Investing in training, empowerment, and communication are as important as technology investments. A courthouse that provides its staff with information, tools, and faith creates a more resilient and responsive organizational culture.

2.3.4 Interagency Collaboration

Large facilities often rely on a combination of public and private entities to keep people safe when danger arises. These partnerships are necessary when responding to

various incidents too robust for a single stakeholder to handle alone. The ability of local, state, and federal agencies to plan, communicate, and share resources is essential for incident response and returning operations back to normal.

For example, a disaster such as a pandemic or terrorist attack requires effective coordination among first responders. These include local police and fire departments, emergency medical responders, and federal agencies, such as the DHS and the Federal Bureau of Investigation (FBI). Each agency brings unique capabilities and jurisdictional authority. Their cooperation ensures a comprehensive security and response framework, establishing a more robust system for security and response.

During multi-jurisdictional events or incidents, a command and control should be established. FEMA's National Incident Management System (NIMS) provides a standardized, scalable approach to command, control, and coordination across various jurisdictions and disciplines (Federal Emergency Management Agency, 2017). NIMS promotes common terminology, integrated communication systems, and unified command structures. Comfort et al. (2010) show that facilities integrating NIMS into their internal emergency response plans demonstrate faster mobilization, improved situational awareness, and clearer communication during multi-agency drills and real-world emergencies. The incident command system (ICS), which is a part of NIMS, has been proven to increase coordination during emergencies, thanks to clearly defined roles and responsibilities. Kapucu and Garayev (2011) noted that facilities who employed ICS procedures with local responders during a disaster were able to manage resources more effectively during time-sensitive situations.

Additionally, a memorandum of understanding (MOU) between facility managers and public safety officials governs authority for joint operations and helps to eliminate confusion regarding jurisdiction. These prearranged agreements set information flow rules, joint exercise scenarios, and authority sharing statements which enable a smooth collaborative response during times of emergency (Waugh & Streib, 2006). Tabletop exercises also improve readiness. According to Auf der Heide (2006), exercises that include all the participants are important to identify operational and communication breakdowns that are not noticed unless under stress. Through these exercises, interagency relationships are strengthened, and trust and familiarity are established among individuals from the various entities that they will work with under the stress of real-world scenarios.

Finally, strong interagency collaboration and coordination turns disaster response from a reactive function to an aggressive proactive policy for risk reduction. These relationships ensure that when things go wrong, everyone is on the same page with a well-rehearsed script. As a matter of principle, federal courthouses, by virtue of their symbolism and distinct risk profile, should prioritize these partnerships among the foundational elements of their security doctrine.

2.3.5 Emerging Technologies

New and emerging technologies have the potential for covert surveillance, intrusion detection, and threat analysis. These advancements are changing the way security is done in facilities. Field professionals can utilize both proactive and reactive techniques faster and more accurately.

Examples of these technologies are:

- Video analytics and AI-embedded surveillance: These tools record, watch, and identify when things are not right. They can observe loitering, perimeter crossing, tailgating or depositing unattended packages in real-time (Aghajan & Cavallaro, 2009). These systems are backed by machine learning aiding in fewer instances of falls alarms and increased situational awareness for security personnel.
- Biometric-based access control systems: Access control systems use biometric for identification, verifying users, and controlling the accessibility of a secure area (Jain et al., 2011). These mechanisms decrease the likelihood of lost or stolen credentials being misused and can provide audit trails that can aid in post-incident analysis.
- Cyber-physical systems (CPS): Connect utilities equipment with automation systems to provide centralized and intelligent control. This facilitates greater operational efficiency and responsiveness, but it also presents potential cyber vulnerabilities. Boyes et al. (2018) note that under-segmentation of informational technology (IT) and operational technology (OT) networks has been responsible for breaches that exposed critical infrastructure.
- Emergency alert software: Prompt, multi-channel communication is critical in secure environments. Multimodal systems that include SMS, email, announcement systems, and mobile applications have the potential to warn all tenants and stakeholders even if they are located offsite disabilities (Fautsko et al., 2013). This software is useful during situations such as

active shooter, fire, and other catastrophic events that require a life-saving response to prevent a tragic outcome.

Emerging technologies offer unprecedented monitoring, intrusion detection, and threat analysis capabilities. These innovations are transforming how facilities approach security, enabling both preventative and responsive measures with greater speed, accuracy, and efficiency.

Beyond these tools, security professionals are exploring technologies that include drone detection, AI-driven behavior analytics, and digital twin modeling showing threat scenarios and response strategies to be tested virtually. But security can't be assured by technology alone. Wyss et al. (2023) states that overdependence on automation with inadequate human monitoring may result in a state of complacency, blind spots and slow response.

Technology is only one piece of the puzzle. It must be coupled with policies and practices, maintenance, and trained personnel capable of responding to the data these systems generate. Technology should be used as a supplemental force multiplier. The cornerstones of courthouse security are the stakeholders responsible and their coordination amongst each other.

2.3.6 Continuous Improvements

Securing a facility requires continuous review, and possible adjustment, of security layers. Risk landscapes are constantly evolving, with new risks originating from technological developments and socio-political conflict. A major challenge is creating an adaptive and flexible system to the evolving threat climate.

Internal and third-party security audits are important for this process. They can detect obsolete installations, policy violations, or overlooked vulnerabilities (Aldridge, 2023). These assessments lay the groundwork for strategic implementation and accountability at all system levels.

Best practices for continuous improvement include:

- Regular security assessments address emerging threats and changes to policy or regulations. These reviews ensure security measures are up-to-date and appropriate for the operational environment.
- After-action reports are used to document lessons learned and develop better responses. These reports turn events into learning exercises. Lessons learned should be adopted to avoid repeating the same mistakes.
- Checklist-based inspections standardize facility review and prevent nothing from falling through the cracks. The Checklist Manifesto by Gawande (2010) state that these lists are a way to convert professional knowledge into a repeatable game plan. They assist staff by moving through complex procedures efficiently with precision increasing reliability.

In addition to physical security and procedures, security managers must be committed and strive for organizational cooperation. Actively listen to personnel to assess issues they are experiencing. Feedback-rich environments are more likely to identify deficiencies and make implementing proactive changes easier.

Continued training and simulation drills combined with data analytics can further strengthen this model. Strive to transform courthouse security from a static to a dynamic environment. Finally, ongoing development makes courthouse

security not just something that "is" but something that "learns" and that finally has the potential to deal with a wide range of known and unknown dangers.

2.3.7 Conclusion of Best Practices

The security of critical infrastructure requires a multi-layered, multi-disciplinary strategy which combines physical assets, personnel preparedness, interagency working, and advanced technologies. Best practices begin with assessing risk levels which include challenging in postures in place such as perimeter defense and intrusion detection. Techniques must be fluid, frequently tested, and adaptable.

As threat climates evolve, so must the architecture for facility security. Practical approaches should emphasize scalable and flexible systems that offer adaptable capabilities to provide security without sacrificing accessibility or the continuity of the mission.

2.4 Risk Assessment Methodologies

Discussed in this section are interdisciplinary approaches that can be utilized for enhancing the security posture in and around federal courthouses. The section begins with a discussion on the significance of incident reporting and thorough documentation. The next focus is root cause analysis, which can align current practices with historical incident data. This aids in identifying vulnerabilities and operational gaps. This is followed by exploring the use of checklists as a structured tool in various industries. Lastly, the section covers the importance of data collection and analysis in evaluating a system’s performance and uncovering areas which need improvement.

2.4.1 Incident Reporting

The reporting of incidents is a fundamental to risk management and operational safety in critical industries. Through systematic monitoring and analysis of incident data patterns can be observed, resources allocated, and proactive measures put in place (Phimister, Oktem, Kleindorfer, & Kunreuther, 2003). Campbell et al. (2020) report that timely documentation and reporting played a role in discovery of important risk factors that were not identified in retrospective or delayed accounts. Its findings are easily disaggregated to courthouse events involving disruptive behaviors, verbal threats, or procedural infractions that commonly precede more egregious behaviors.

In the field of public safety, incident reports are used for planning and operations. The National Incident-Based Reporting System (NIBRS), operated jointly by the Bureau of Justice Statistics (BJS) and the FBI, contains detailed information on crimes, victims and circumstances for the express purpose of evidence-based policing (Federal Bureau of Investigation, 2024).

Another aspect of policing is the use of force reporting. In New York, the Division of Criminal Justice Services (DCJS) (2021) studied over 6,000 cases to improve training and identify trends in the use of excessive force. The results of the study showed that the implementation of standard reporting protocols improves accountability and detects geographic or temporal patterns that can help drive resource allocation and procedural revision. When adapted to court settings, recording incidents enables predictive models and responsive checklists to be developed according to local threat environments.

Incident reporting is a tool government agencies rely upon to enhance their oversight, and shape enforcement and regulatory reform. The Occupational Safety and

Health Administration (OSHA) mandates that workplace incidents be reported to identify hazards and inform compliance interventions (Suh, 2021). Suh applied Latent Dirichlet Allocation (LDA) to OSHA narrative reports and uncovered thematic signals, such as fall risk or equipment failure, that could remain hidden in the structured fields. Such findings reinforce the value of narrative data, which may highlight system failures that so-called structured checklists subsequently can target.

Cybersecurity is fragmented when it comes to incident reporting. Santos and Ferreira (2023) reporting on provisions across sectors found varied thresholds, reporting timelines, and definitions of what constitutes a reportable incident. Inconsistencies are a barrier for early detection and a coordinated response. As the world's courthouses move towards a digitized operation and sensitive legal information is increasingly being stored online, consistent reporting policies are critical to successfully address cyber threats.

The health sector is a good example of how incident reporting systems have evolved into a more developed and established component of organizational learning. The Systems Engineering Initiative for Patient Safety (SEIPS) framework referenced in Weaver, Stewart, and Kay (2021) aims to support moving from a focus on blame to a learning system. Weaver, Stewart, and Kay (2021) contend that safety problems often arise from latent organizational characteristics than from individual culpability. Kodate et al. (2022) examined reporting cultures in Japanese hospitals, and reported that the existence of a hierarchy, fears of retaliation and lack of feedback undermined the effectiveness of reporting systems. These are akin to those in court settings, where legal confidentiality and institutional stiffness may reduce open reporting unless joined by a change in culture and policy.

According to Vincent et al. (2014) patient safety reports also stress the need for closing the loop on feedback. They state an organization that collects, but also acts on, incident data will see significant improvements in safety outcomes. Applied to courthouse security, the previous can correlate only with incident data that continually inputs the revision of checklists so that it continually adapts to emerging threats and organizational learning.

In law enforcement, government regulatory agencies, and healthcare, incident reporting is highlighted as a key component to operational resilience. Effectiveness will depend on what it collected and the potential to synthesize and respond to that information. In the domain of the courthouse, where confidentiality and procedural formalism inherent to courtrooms are potentially compromising to crime victims, an effective incident reporting system could serve as a catalyst for organizational learning.

When integrated into a courthouse-specific, dynamic checklist, this intel becomes a preventative tool that shifts the focus from observation to actionable response. This assimilation turns bureaucracy reporting into proactive safety that contribute to continuous development and hazard reduction. The following flowchart demonstrates how incident report data can become transformed in a structured format to a feasible listing of preventive measures, from raw observation data to itemized intervention recommendations.

2.4.2 Root Cause Analysis

Some of the most popular methods for root cause analysis are the event tree (Hoyland and Rausand, 1994) and Ishikawa, or fishbone, diagram (Ishikawa, 1985). The event tree traces possible system failure scenarios through failures of subsystems

designed to protect the overall system, while Ishikawa Diagrams provides a visualization of potential root causes by placing contributing factors into multiple categories (e.g., people, processes, technology, and environment). Thus, it creates a structured framework for analyzing failure events and for finding common causes, ultimately processing interacting effects that yield ultimate failure.

Botezatu et al. (2019) demonstrate the versatility of the Ishikawa model in applications such as chemical processing, systems outages, and production defects. Their research has shown the benefit of causal-inference style explanations in revealing the underlying dependencies that would inhibit future repeat failures. The same application can be applied to courthouse security measures during incidents such as failed coordination or unauthorized access. For example, a security breach is likely not the consequence of individual error but the intersection of unclear procedures, poor training, and failed communication. These can be traced through a fishbone diagram as pressures to prompt meaningful change.

The use of visual analysis tools is only as good as their reach and transparency. Gartlehner et al. (2017) found that when Ishikawa diagrams were used in clinical quality improvement settings, stakeholders unfamiliar with the format often misinterpreted their structure, leading to communication breakdowns. These findings highlight the necessity of accompanying diagram use with correct orientation, training, and simplification. This is particularly true in the realm of courthouse security, where multiple agencies and different levels of technical literacy exist.

In addition to the Ishikawa diagram, Reason's Swiss Cheese Model (1990) theorizes that system failure results from multiple defensive layers where each has its own holes or potential weak points. When aligned across layers, these holes become a pathway which errors or threats can penetrate. Each slice of cheese represents a defensive barrier, such as physical infrastructure, policies, human oversight, or technology. In courthouse settings, for example, physical access controls (one slice) may be compromised if combined with poor badge protocols (another slice) and undertrained personnel (a third slice). The model reinforces the idea that failures are rarely the result of a single cause, but rather a convergence of latent and active failures across multiple domains (Reason, 2000).

Applied together, the Ishikawa diagram and the Swiss Cheese Model offer two complementary views of risk, one aimed at categorizing and visualizing contributing causes, and another that visualizes how multiple levels of defense can fail together. By combining both, agencies tasked with defending federal courthouses could create an assessment that would encourage a proactive and systems-based approach for an enhanced security posture.

2.4.3 Checklists

Checklists are tools used in arenas that manage risk to protect operations from being exploited by vulnerabilities. A checklist could be a promising tool for courthouse security. This tool can take the knowledge about risks faced by an institution and the procedures established to protect it and turn it into methods capable of reducing human error. This section presents an overview of relevant literature on using checklists by sectors facing similar risks to those found in courthouse environments.

Biases in the human brain disrupt decision-making in high-risk industries such as aviation, healthcare, and judicial security. These flaws cause people to overlook or underestimate the risks and failures of our decision-making process. Emmons et al. (2018) addressed this problem for the aerospace community and developed a checklist to reduce bias in risk management. Their research has shown that checklists help prevent failure by incorporating adequate procedures and reducing decision-making errors, allowing experts to follow a process with a proven track record.

This realization directly relates to courthouse security, where the day-to-day activities of perimeter checks, access control screening, and surveillance can cause complacency. To the extent that we can institutionalize critical decision points and cognitive guardrails, security checklists can help to counteract our natural inclination to concentrate on anomalous events or prematurely dismiss incidents as benign, particularly in environments we know well or during long shifts.

The Checklist Manifesto, Gawande (2010) suggests that checklists have functions beyond reproducing work as done. By operationalizing collective expectations and decision-making criteria, checklists promote uniformity and decrease dependence on memory or individual judgment. This model particularly applies to the court-based setting, which requires multi-agency coordination (mixing trained and non-trained practitioners, varying protocols), which may contribute to inconsistent implementation of crucial duties.

Green (2012) has extended this argument by showing us how protocols applied in aerospace checklists developed by NASA have successfully translated into hospitals. This adaptation, featuring transparent task allocation, structured communication, inventorying exercises, and case-based training, was associated with quantifiable decreases in error rates and patient deaths. Additionally, this process indicates that applying a checklist to judicial security can enhance the protective posture, if known site-specific, human, and organizational risk can be incorporated.

The healthcare industry shows how checklists generate measurable improvements in high-risk environments. Hales et al. (2008) emphasized that the success of checklists in clinical settings hinges not only on the checklist's content but also on its design rigor, user integration, and institutional commitment. To avoid becoming a superficial or neglected tool, a checklist must be seamlessly embedded into existing workflows and endorsed at multiple levels of the organization.

Building upon this, Wyss, Kolbe, and Grande (2023) conducted a World Health Organization Surgical Safety Checklist meta-analysis and found that while checklists offer a strong framework for reducing errors, their actual value is seen when paired with comprehensive team training, leadership support, and stakeholder communication. These factors created an environment where procedural compliance is reinforced through shared accountability and procedural norms.

These findings translate directly to the federal courthouse security environment, where checklist implementation must extend beyond an operational culture. Effectively adopting a courthouse security checklist requires a coordinated effort among all

stakeholders. Much like healthcare, these agencies must invest in cross-training, joint rehearsals, and communication protocols that promote cohesion. Without this alignment, even the most technically sound checklist may fail to deliver its intended security outcomes.

In high-stakes environments, a checklist's power extends beyond the climate present at that time. Since these documents are available, they make a difference in team management as they help coordinate team action and maintain accountability. A good checklist is both practical and fluid in language. This device acts as a conduit through uncertainty and helps stabilize the understanding of performance across team members.

Consistency is critical to ensure standards are followed to minimize human error. Inada et al. (2011) found that multisensory involvement could help decrease the chance of skipping steps and increase focus, especially when tasks were repetitive. The focus of their study investigated "pointing and calling," a method used in Japanese railways and other industrial settings. The technique combines verbal confirmation and physical gestures in verifying task completion.

This approach is applicable in a courthouse setting. For example, verbal confirmations and purposeful action improve accountability and situation awareness during security checkpoint operations or conducting a controlled movement. These practices reduce risks tied to general complacency or miscommunications, both of which can occur in teams with shifting crews or ones where team members might have different levels of experience.

Moreover, when checklists are employed as part of a multilayered system of reference, they help create a shared vigilance. This establishes an environment for

security professionals to become less individuals and a more tight-knit unit. Alignment is essential in times of elevated stress. It eliminates uncertainty by providing clarity, trust, and intent, all of which have a degree of bearing on these instances.

The value of checklists does not stop in aviation and healthcare. Other areas, such as engineering, disaster recovery, and information systems testing, support their value and applicability to developing security programs for complex facilities such as federal courthouses.

In disaster risk management, Mora and Keipi (2006) discuss the applicability of checklists for planning the multisectoral response to natural hazards across Latin America. The study stressed incorporating checklists into pre-disaster planning, community participation, and infrastructure assessment. Checklists help identify and mitigate dangers while strengthening accountability and coordination among various agencies. An example can be seen in courthouse security, where the roles of FPS, GSA, and the USMS should complement each other in routine and emergency operations.

In a related field of occupational engineering and ergonomics, Kuo et al. (2015) conducted various experiments to examine the balance ability of the human body. The research validated the capability of checklists in detecting the risk factors of musculoskeletal disorders (MSDs) in hotel housekeeping workers. They found that checklist items could systematize identifying injury risks associated with tasks and the environment's layout. These findings are relevant to proceedings in courtrooms, where court staff, CSOs, or other administrative

personnel may be subject to repetitive tasks. Incorrect use of equipment or unsafe physical conditions could increase the risk of injury, resulting in a medical emergency. A security checklist can help prevent injury, lower the risk of litigation, and contribute to staff well-being.

In software and systems validation, Johanning et al. (2014) considered using checklists to verify compliance in pharmaceutical IT systems governed by FDA regulations. Their research demonstrated how defined verification processes established a shared language and quality denominator between IT teams, quality assurance, and production departments. Their results have favorable implications for courthouse security, where multiple stakeholders must cooperate and work through agency-specific policies and regulations. In the study, checklist protocols helped software developers adhere to rules and integrate their coding into a workflow, maximizing transparency, accountability, and repeatable processes. This same approach can be applied to courthouses to detect, respond to, and track threats.

These cases demonstrate that checklists are not simply prompts. They are efficient coordinating systems within and between institutions capable of enforcing compliance with established standards and aiming to prevent errors. Checklists provide a scalable framework that can be modified to strengthen courthouse security systems' procedural structure and operational robustness.

In high-risk and high-performing environments, checklists are risk management tools that support operational risk control, maintain consistency, and prevent costly omissions. The two main philosophies of checklist design, formal and pragmatic, can be

distinguished. These two methods provide complementary but opposite strengths. Their differences are significant to consider when designing a checklist in its operational environment to ensure it is as effective as possible.

A formal checklist is based on systems engineering, regulatory requirements, and predefined protocols. These checklists prioritize fullness, standardization, and trackability. Their development is based on institutional policy, risk analysis models, and validation through formal testing. Checklists are particularly useful in complex, regulated environments where accountability and procedural correctness are key (Degani & Wiener, 1993), such as equipment inspections, threat assessments, and judicial compliance procedures.

A pragmatic checklist is developed with the end user's usability in mind. The focus is efficiency and adaptability, making it useful in dynamic environments where time is of the essence. Pragmatic checklists are created from the user input and operational experience. This approach is suitable when critical response time and situational awareness are required (Hales et al, 2008). Morali (2011) compared security assessment methodologies and showed that although formalized techniques such as enhanced Threat and Vulnerability Risk Assessment (eTVRA) could provide deeper analysis, checklist-based approaches were quicker, more intuitive, and accessible to non-specialist users.

The formal versus pragmatic checklist dichotomy is vital in contexts involving the security of federal courthouses, as there is increased operational complexity, varying levels of personnel proficiency, and high-speed changes in the threat environment. Checklists serve the frontlines with clarity, speed, and

flexibility. Even under stress, security measures are carried out reliably. On the other hand, formal checklists serve institutional requirements by enforcing regulatory compliance.

The trade-off between consistency and responsiveness is not acceptable in a courthouse environment. In this environment, a hybrid model combining the strengths of the two models is better suited. This type of framework makes it possible to systematically follow established protocols while retaining the operational flexibility required for real-time decision-making. This hybrid framework not only underscores the value of criminal justice security but also helps properly align with larger policy goals and interagency cooperation while fortifying the security framework within diverse courthouse environments.

2.4.4 Data Collection

The successful construction of a checklist relies on the collection of sufficient and accurate data. Structured and narrative incident reports are a cornerstone of operational learning in acute risk sectors. In the healthcare sector specifically, Mahajan (2010) advocates for using non-punitive reporting systems to promote a whistleblowing culture that serves as a vehicle for improvement. Institutions must not promote a culture where individuals fear reporting honestly due to fear of consequences. An alternative approach is anonymous reporting to collect more accurate and transparent information due to complete data based on unfiltered content.

Obstacles such as underreporting, insufficient follow-up and deficient feedback loops exist impacting the accuracy of data collection. Psarros, Skjong and Eide (2010) studied maritime accident reporting and found that only 41% of accidents were registered

in national databases. Additionally, they found 30% of accidents were listed for global databases. This massive underreporting not only distorts risk evaluation but also results in missed opportunities for threat mitigation reform. The parallel to courthouses, meanwhile, is clear. Vulnerabilities can go unchecked without a public ledger for security breaches. An established checklist created without a foundation of incident reports may not be built to mitigate real threats.

Cybersecurity reporting also highlights the difficulty in defining an "incident" and determining the promptness of a report about the incident. Marotta and Madnick (2023) claim that terminology and reporting order make it difficult to justify and prepare for regulations. Some of this uncertainty can be resolved by a clear, quantifiable checklist that standardizes what should be reported, how it should be reported, and when it should be reported.

2.4.5 Data analysis

Raw data is converted into insight through the process of data analysis. In Cooper, Newbower, and Kitz (1984), anesthesia mishaps were retrospectively analyzed to identify if they resulted from human error or a malfunctioning machine. Many of these events were found to be due to procedural lapses, poor communication, or training deficiencies, rather than the technology itself. This is strongly correlated in cases of courthouse security, where malicious activity is frequently a result of procedural failures like the failure to properly follow screening protocol or a lack of clarity in identifying roles during emergencies.

Mahajan (2010) suggests incorporating a model such as Reason's Swiss Cheese to follow a chain of events within an organization. This model differentiates between active

failures, such as a court security officer failing to check ID, and latent conditions, such as for inadequate manpower, which may lead to an increased probability for human error. Applying that kind of analysis provides a structured way of thinking about what and how an incident occurred, as well as why it was allowed to happen.

The newer technologies result in timely detection. A study by Chan et al. (2024) proposed a deep learning model with the help of AI-implanted cameras to identify errors in hospitals with 99.6% precision. This technology is applicable in a courthouse setting to minimize the time it takes to detect a threat. This proves that data analysis is not only retrospective, but it can be implemented in day-to-day operations.

2.4.6 Conclusion of Risk Assessment Methodologies

This section explored various interdisciplinary tools which can be used for risk assessment methodology. It demonstrated the importance of why a structured process is necessary for securing facilities, such as federal courthouses. Incident reporting provides a potential foundation for recognizing patterns and guiding responsive measures. Root cause analysis frameworks, like the Ishikawa diagram and Reason's Swiss Cheese Model, demonstrate and clarify the nature of failures and the impact they can have in an operational setting. Checklists have been proven to be an effective tool used in various industries. They offer a scalable mechanism that can translate insights into operational consistency capable of reducing human error and reinforcing accountability. The value of these tools in conjunction with a robust data collection and analysis process ensures feedback loops, transparency, and continuous learning. Jointly, they support the development or enhancement of an effective operational security posture desired in any level of risk environment.

2.5 Literature Review Conclusion

This literature review has presented a growing threat environment directed at federal courthouses and court personnel, an intricate interagency of protection, and its structure. It has also contributed to understanding how structured tools like checklists can manage risk in a high-stakes, multi-stakeholder environment.

Evidence suggests the judiciary became susceptible to ideologically driven violence, personal vendettas, and cyber-facilitated confrontation (Bailey, 2023; Rosenblatt, 2013). Mass causality events, such as the 1995 Oklahoma City Bombing (Corley et al., 1998), and the personal vulnerability of the judiciary, as occurred in the assassination attempt on Judge Esther Salas in 2020, exemplify how both infrastructure and personal vulnerability combine in this domain. Violence in courthouses, such as the 2005 Fulton County shootings, courtroom stabbings, and other various threats, has highlighted decades of lapses in procedures and inadequate awareness of threats (Dow, 2007; Baehler & Somerlot, 2005).

Federal agencies, such as the USMS, have deployed security assets considering the increasing threat landscape. Over 1,000 threat investigations occur annually, and over 800 facilities are protected using approximately 5,600 Court Security Officers (United States Marshals Service, 2023). FPS and GSA aid in establishing perimeter security and structural hardening. The AOUSC has expanded threat management programs, which enhance digital privacy applications and emergency preparedness programs (United States Courts, 2024).

Examining incident reporting practices in law enforcement (Federal Bureau of Investigation, 2024), government regulation (Santos & Ferreira, 2023), and healthcare (Weaver, Stewart & Kay, 2021) provides additional evidence of this finding. A

disciplined collection process must be applied to utilize this information effectively for a structured checklist. Those reviewing must be able to make sense of the data. After it has been analyzed, the information must be used and put into practice. Inadequate reporting is a recurring limitation in all sectors (Psarros et al., 2010; Kodate et al., 2022), highlighting the importance of reporting protocols. Organizations can learn by identifying patterns and implementing best practices into a checklist to mitigate those patterns.

Analytical tools such as Reason's model (Mahajan, 2010), the Ishikawa diagram (Ishikawa, 1985; Botezatu et al., 2019), and emerging AI applications (Chan et al., 2024) provide further insight into how latent failures can be visualized and addressed. These tools emphasize that security failures are seldom random; they result from compounding systemic weaknesses. A checklist that reflects these layered vulnerabilities can serve as a preventive mechanism.

The development and application of checklists in high-risk industries like aerospace and medicine (Emmons et al., 2018; Green, 2012; Wyss et al., 2023) offer direct lessons for judicial facility security. These fields have shown that checklist success depends on design, culture, training, and institutional support. As Gawande (2010) argues in *The Checklist Manifesto*, checklists do not replace expertise; they amplify it. They are simple but profound tools to ensure critical steps are not overlooked, particularly under stress, time pressure, or cognitive fatigue.

In federal courthouse security, the checklist becomes more than a procedural aid; it becomes an operational philosophy grounded in data, driven by prevention, and sustained through collaboration. From documenting elevator malfunctions that endanger

jurors to standardizing responses to PII leaks or unauthorized access, the checklist translates vulnerability into vigilance.

This literature review argues that protecting the federal judiciary requires more than funding, manpower, and reactive measures. It requires a deliberate approach that anticipates threats, collaborates with stakeholders, and implements best practices. A checklist for judicial security can safeguard the integrity, continuity, and credibility of the judicial process.

Chapter 3: Methodology

A federal courthouse security checklist requires the use of physical security theory with practical application. This chapter outlines an approach that identifies vulnerabilities and designs an operational security checklist that mitigates any risk that may exploit those vulnerabilities. The framework of the applied methods supports this study as it efficiently explores vulnerabilities and implements security measures that effectively secure the judicial process.

The first method is a root cause analysis employed through a combination of the event tree method and the Ishikawa (fishbone) diagram with the Reason's Swiss Cheese Model. This approach maps how conditions, operational weaknesses, and failures align to create vulnerabilities within the physical security of federal courthouses. Second, an empirical analysis of incident report data from the Southern District of New York (SDNY) is conducted. The study drew upon these reports to explore real-world operational data. Third, a review of best practices from high-risk sectors was performed to identify practices applicable to courthouse environments. Finally, a validation exercise, circling back, was implemented to map the developed checklist elements to historical incident patterns, explaining how the implemented measures would mitigate the risk of vulnerability from being exploited. Together, this approach forms a methodology that integrates systems theory, data analysis, cross-sector best practices, and validation to produce a checklist advanced enough for the high-stakes environment of judicial security.

3.1 Statement of Purpose and Problem Boundary: What's In and What's Out

This research serves as a call to action. A comprehensive, data-driven security checklist should be developed and implemented as a tool used to expand courthouse protective postures against both current and future risks. This blueprint would also enable institutions to identify current and potential vulnerabilities within and outside courthouse perimeters.

This checklist is designed to be a living model incorporating historical data, operational best practices, and systems thinking. Created is a tool which aids in identifying gaps, guides mitigation strategies, and promotes a proactive security culture.

3.1.1 In-Scope Elements

The checklist addresses areas that courthouse personnel and facility managers can directly influence through daily, weekly, or monthly actions. Specifically, it includes:

- Physical Security Controls: Access management, perimeter protection, surveillance monitoring, visitor screening, and intrusion detection.
- Operational Readiness Procedures: Routine inspections, incident reporting, emergency response drills, and communication system verification.
- Personnel Training and Accountability: Recurring training and threat observation protocols.
- Technology and Equipment Maintenance: Preventive testing and operational checks for security-related infrastructure.
- Emergency Response Coordination: Pre-incident planning, communication with external agencies, and onsite emergency activation protocols.

These areas were prioritized because they are actionable at the facility level, support immediate improvements in security posture, and align with established best practices for protecting critical infrastructure.

3.1.2 Out-of-Scope Elements

Conversely, the checklist excludes areas considered beyond the operational control of courthouse facility teams, including:

- Judicial and Legislative Policy Reforms: Broad changes to judicial security statutes or federal protective mandates.
- Major Facility Hardening Projects: renovations, structural upgrades, or physical redesigns that require significant funding and long-term planning.
- External Law Enforcement Investigations: Intelligence gathering, criminal investigations, and other operations outside the courthouse's internal scope.
- Medical and Public Health Emergency Management: Responses to pandemics, biological threats, or mass casualty medical events, which are governed by distinct emergency management protocols.
- Comprehensive Cybersecurity Measures: While cybersecurity protections for physical security systems (e.g., surveillance access controls) are included, broader judicial cybersecurity defenses (e.g., case management databases) are excluded.

3.1.3 Justification for Boundary Definition

Out-of-scope areas were removed because they require a level of authority that goes beyond that of locally based personnel. This ensures that the checklist

remains a manageable, implementable management tool for staff in local contexts. For example, projects for structural hardening require long-term planning and coordination in addition to dedicated funding, which falls out of the control of onsite staff.

Table 1: In-Scope vs. Out-of-Scope Elements

Included (In-Scope)	Excluded (Out-of-Scope)
Physical security measures (access, perimeter, surveillance)	Policy Reforms
Daily inspections, emergency drills, communication testing	Major Facility Hardening Projects
Security personnel training and insider threat monitoring	External law enforcement investigative operations
Maintenance and testing of security equipment	Medical and public health emergency management frameworks
Cybersecurity protections for access/surveillance systems	Broader judicial cybersecurity (e.g., database protection)

The objective for developing a security checklist is to put another tool into the hands of those responsible for managing the day-to-day security operations. As shown in Table 1, the problem boundary provides a practical and manageable approach to maximize the effectiveness and efficiency of this tool.

3.2 Understanding the scope of the problem – Event Trees and Ishikawa diagram with Reason's Swiss Cheese

The level of vulnerabilities within federal courthouse facilities needs to be understood through systematic analysis, beyond the level at which an incident occurs. Three complementary standard risk assessment frameworks, the event tree, the Ishikawa diagram and the Reason's Swiss Cheese Model, provide ways to diagnose the root causes of the layered, intertwined onset of security failures.

Event tree analysis is a formal method for illuminating the potential path through protective barrier failures that can lead to undesirable events (see figure 3 below). In risk assessment these are usually determined through thought exercises but documented past events of courthouse breaches have provided a clear picture of past scenarios that have had deadly consequences.

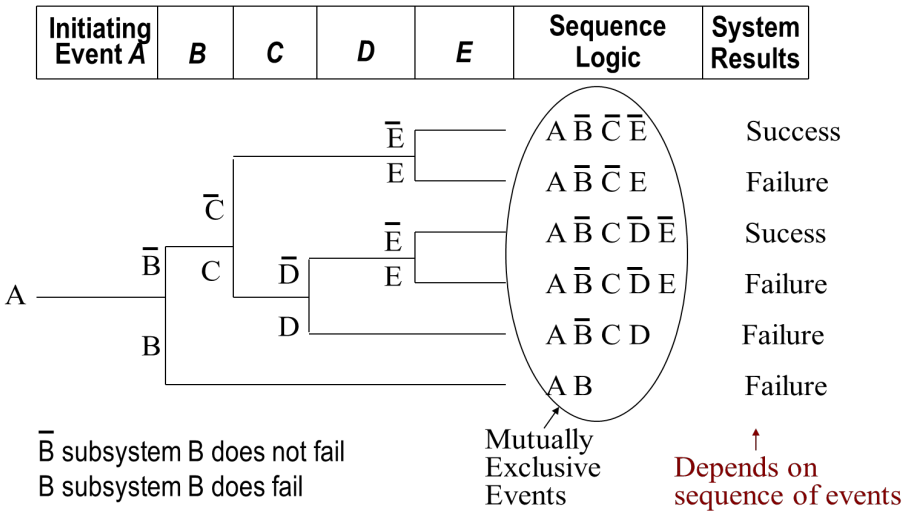

Figure 3: Event Tree Diagram

Once the above scenarios have been constructed, the Ishikawa diagram classifies causes in broad domains that may include people, processes, technology, and environments. By representing these causes, security stakeholders can develop an understanding of the broader system problems that create security incidents rather than giving each an individual label and treating them as a byproduct of human error.

Reason's Swiss Cheese Model offers a systemic view of gaps. Each slice of the cheese represents a layer of protection, such as doors and locks or policies and procedures. The holes inside each slice symbolize a condition or active failure.

Individually, these vulnerabilities seem harmless. However, when these vulnerabilities temporarily align throughout various layers and components of the system, they form a threat that can invade the systems, resulting in catastrophic failures (Reason, 1997). Figure 4 presents a visualization that integrates a Fishbone Diagram with Reason's Swiss Cheese Model, illustrating how underlying root causes and layered vulnerabilities contribute to security failures within the courthouse environment:

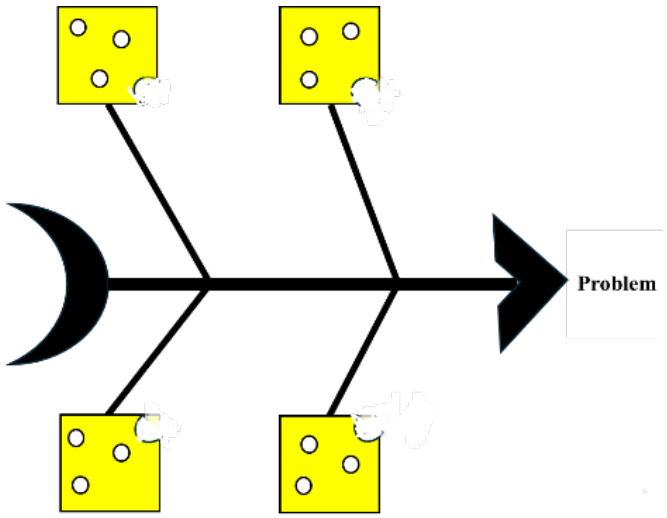

Figure 4: Fishbone Diagram with Swiss Cheese Model

Regarding courthouse security, the holes include structural, procedural, and behavioral components. Structure vulnerabilities encompass failed infrastructure like non-functional alarm systems, surveillance blind spots, or mechanical breakdowns of equipment that render environmental control ineffective (Wyss, Kolbe, & Grande, 2023). Procedural failures reflect inconsistent access policies, for example, inconsistent screening practices (Valeo et al., 2012). Regarding behavior, relying too much on verbal coordination, failing to consistently

document and report incidents, and delayed reporting contribute to less effective threat response (Emmons et al., 2018).

Disintegrating responsibilities is an especially pervasive problem within courthouse security. Although the USMS, GSA, and AOUSC manage different elements, lacking a centralized communication system and interagency oversight contributes to siloed working conditions (United States Courts, 2024). For example, a contraband item may elude security screening (procedural gap), overlooked with a surveillance failure (technological gap), and unreported through shift changeover lapse (communication gap). If these failures happen to sync up, they undermine the entire protective posture of the facility.

Integrating the event tree with the structured root cause analysis of the Ishikawa diagram with the systemic perspective of the Swiss Cheese Model provides a comprehensive understanding of courthouse vulnerabilities. This approach identifies security lapses and uncovers hidden organizational deficiencies underlying the need for a checklist-based methodology that facilitates interagency coordination, tracks incident trends, and validates procedural compliance. This addresses Research Question 1, establishing a proactive framework for closing security gaps and strengthening institutional resilience against emerging and recurring threats.

3.3 Current Best Practice Vulnerabilities

Physical security is a critical component in numerous industries, each having designed security plans to protect people, assets, and organizations. Government facilities, hospitals, and other robust facilities with layered security postures such as perimeter security, access controls, and threat-specific response

procedures (United States Department of Homeland Security, 2019). These are designed to counteract threats that may range from a terrorist attack to denial of service and ensure operations continue with minimal disruption.

In healthcare, hospitals, research facilities, and clinics are all challenged by theft of narcotics, workplace violence, and unauthorized entry. To avoid these threats, best practices recommend complete visitor management programs, secure storage of confidential material, use of duress alarms, and close collaboration with local law enforcement (The Joint Commission, 2022). Similarly, commercial and corporate organizations, especially company headquarters, data centers, and R&D labs, are interested in intellectual property protection and minimizing insider threats. Their security strategies incorporate risk-based evaluations, processes to manage employee access, surveillance solutions with analytics, and proactive insider threat programs (ASIS International, 2019).

Energy and utilities are among the critical infrastructure sectors that devote significant attention to protecting power plants, oil refineries, and water facilities. Best practices in these environments prioritize hardened perimeters, cybersecurity integrated with physical security systems, intrusion suppression technologies, and layered response plans that help these systems recover and remain resilient in the face of attacks (North American Electric Reliability Corporation, 2021). Transportation facilities such as airports and railway terminals are particularly focused on their security needs since they accommodate high volumes of cargo and passengers. Their best practices focus on a multi-layered screening process for passengers and cargo, effective restricted area access control, continuous

perimeter surveillance, and incident response plans that closely integrate with national security agencies (Transportation Security Administration, 2022).

From grade schools to universities, educational organizations acknowledge the need for better physical security to safeguard students and faculty. Best practices include threat assessment teams, access procedures, emergency communication strategies, and regularly scheduled lockdown drills (Department of Justice, 2019). Meanwhile, retailers encounter numerous threats, including theft, violence, and crowd control issues. Effective methods include using closed-circuit television (CCTV) systems with behavioral analytics, inventory controls, training staff with a focus on situational awareness, and having visible security personnel (NRF, 2023).

Across all sectors, universal physical security practices are implemented as best practices. These defensive-in-depth strategies are layers of security measures tasked with securing the perimeter (Smith & Brooks, 2012), regularly conducting risk and vulnerability assessments (ISO, 2018), establishing strict access control policies, and committing to continuously looking to improve security posture by reviewing historical incident data and evaluating available after-action analysis. These best practices are a foundational framework for designing, implementing, and maintaining effective physical security programs across diverse operational environments. Table 2 outlines current best practices in facility security.

Table 2: Current Best Practices in Facility Security

Best Practice	Description	Source
Comprehensive Risk Assessments	Facility security must begin with a thorough and recurring assessment of risks, encompassing both internal and external threats. These evaluations should consider environmental vulnerabilities, operational workflows, and potential insider or outsider threats to prioritize and tailor mitigation strategies.	Securitas, 2024
Layered Physical Security Architecture	A best practice in securing facilities is the application of a multi-layered defense strategy. This includes perimeter barriers, surveillance systems, secure entry controls (e.g., biometrics), and reinforced zones for sensitive operations, establishing redundancy to deter or delay adversarial actions.	Amarok, 2024
Integrated Security Technology Platforms	The convergence of security systems—surveillance, alarms, access controls, and environmental sensors—into a unified platform enhances situational awareness and operational efficiency. Integration allows for centralized monitoring and faster incident response.	Buildings.com, 2024
Formalized Facility Security Plan	A formal Facility Security Plan (FSP) outlines site-specific threats, operational vulnerabilities, mitigation tactics, and agency responsibilities. These documents must be periodically reviewed and updated to reflect evolving risks and organizational changes.	SelectHub, 2024
Routine Security Audits and Emergency Drills	Regular audits verify the functionality of security systems and protocols, while emergency drills serve as practice exercises to prepare staff for diverse scenarios, improving real-time readiness and identifying procedural weaknesses.	Citizens Guard, 2024
Personnel Training and Security Culture	Continuous employee education on access control, emergency procedures, and suspicious activity reporting is fundamental. A strong security culture empowers staff to serve as force multipliers for incident detection and prevention.	Securitas, 2024
Controlled Access Management	Access should be restricted based on roles and responsibilities, using layered authentication (e.g., smart cards, PINs, biometrics) and a monitored visitor entry system. Logs should be maintained and regularly reviewed.	CISA, 2023
Power Continuity and System Redundancy	Critical infrastructure requires uninterruptible power supplies and backup generators to maintain security functionality during power outages. Regular testing and load balancing are necessary to ensure operational continuity.	CISA, 2023
Adherence to Security and Cyber Standards	Compliance with national standards (e.g., UL 2050 for alarm systems, NIST for cybersecurity) ensures consistency and resilience against a wide array of physical and digital threats. These benchmarks support both regulatory alignment and institutional integrity.	UL Standards, 2023; NIST, 2023
Preventive Maintenance and System Updates	Hardware and software components of security systems must be maintained proactively to prevent malfunction and eliminate exploitable vulnerabilities. Patch management and system testing are key components of this cycle.	Kisi, 2024

This directly addresses Research Question 4 by identifying the critical features required to develop and implement a security checklist tailored to the unique operational demands of a large facility such as a federal courthouse.

3.4 Data to Drive Home Gaps

Analyzing incident report data from the SDNY contributed to identifying vulnerabilities within the district's facilities. This confirms the importance of implementing a systematic checklist for courthouse security by examining the frequency of the incidents, categorizing them, and identifying the gaps and their impacts on operations. Each gap is tied to incident trends so that the checklist targets the relevant security feature found to be vulnerable.

The sub-sections below present a data-driven account of the analytical process utilized for this study. The methods include those followed in data pre-processing, data cleaning, normalization, and structuring of the incident reports. Each contributes to ensuring the validity of the findings behind the development of the checklist.

3.4.1 Incident Report Collection

SDNY includes roughly 60 United States District and Magistrate Judges, 10 Bankruptcy Judges, 14 Judges of the Court of International Trade, and 27 Judges for the United States Court of Appeals. Physical security is provided by a security force comprising more than 200 Court Security Officers (CSO), Special Security Officers (SSO), and about 80 operational USMS personnel. Beyond judicial officers, these courthouses include employees from numerous federal agencies, including the United States Attorney’s Office (USAO), United States Probation and Pretrial Services, the General Services Administration (GSA), approximately 1,200 court administrative employees, and media members.

The district includes six federal courthouses from Lower Manhattan to Poughkeepsie, New York. These facilities do more than facilitate the administration of justice. They host various functions, including conferences, ceremonies, mock trials, and public events that inform and educate the public. From 2013 to 2024, 1,273 security incidents were documented and reported in the SDNY. Sensitive data has been redacted to ensure operational security and personal privacy (e.g., facility names and identities). The review of this data provided a key aspect for developing the security checklist.

When properly analyzed and categorized, incident reports expose vulnerabilities in operations. Faults and failures often stem from events that may not appear serious at first, e.g., equipment malfunction or the introduction of contraband. Issues frequently seem routine; however, they may signal deficiencies or weaknesses that malicious actors can exploit. Incident classification turns raw data into reliable information that can facilitate the transition from a reactive approach to proactive risk reduction. This process enables the development of the checklist, which aims to achieve content based on empirical evidence and has operational relevance.

The USMS adopted a reporting system called CAPTURE (Case Analysis and Processing Through Unified Reporting and Entry) several years ago to assist with operational matters. This system permits USMS employees to document incidents and events. As the program is relatively new, its adoption has been mixed across facilities. Most of the incidents being examined were not documented in CAPTURE. This research examined paper-based incident reports

manually documented in an Excel database. Each incident includes metadata such as the date and time of the incident, a description, and additional details necessary for analysis and categorization. Table 3 is a sample of the incident data:

Table 3: Sample of Incident Data

Date of Incident	Time	Description
2/25/21	18:30	Individual stabbed by unknown person
2/16/21	18:00	Chambers door left unsecured
5/4/20	11:30	Hazardous contents found in package
3/12/19	11:00	Individual outside courthouse attempts to set it on fire
4/14/18	5:00	Security monitor malfunction caused by power outage

3.4.2 The Data Cleaning and Preparation Process

Before the incident data could be analyzed, the data set needed to undergo a data cleaning process that was consistent, complete, and analytically sound. The raw SDNY incident reports had challenges like those of other types of operational data:

- Missing Information: Incomplete entries were found, e.g., date of the incident. These were systematically populated from available incident narratives, with context clues in detailed descriptions used to reasonably impute missing classification.
- Generalization of Descriptions: Incident descriptions displayed a variance of terms used to describe similar event types. To minimize noise and facilitate systematic pattern recognition, incident descriptions were generalized to more concise terms, e.g., false fire alarm and elevator failure are both under equipment malfunction.

- Category Consolidation: Types of incidents were collapsed into broader categories. For example, descriptions involving protests, disturbances, and demonstrations were categorized under Disruptive Conduct and Behavioral Security Risks.

Table 4: Incident data with classification and general description

Date of Incident	Time	Description	Classification	Classification Name	General Description
2/25/21	18:30	Individual stabbed by unknown person	1	Critical Health and Safety Emergencies	emergency
2/16/21	18:00	Chambers door left unsecured	2	Physical Access Violations and Security Breaches	breach
5/4/20	11:30	Hazardous contents found in package	3	Threat Intelligence and Hazardous Risk Management	threat
3/12/19	11:00	Individual outside courthouse attempts to set it on fire	4	Disruptive Conduct and Behavioral Security Risks	disorderly conduct
4/14/18	5:00	Security monitor malfunction caused by power outage	5	Infrastructure Integrity and Systemic Failures	equipment malfunction

This process made it possible to represent the frequencies of events and patterns without segmentation reasonably and enabled actionable insights to be obtained at the system level. Table 4 presents a sample of incident records with their corresponding classifications and general descriptions.

3.4.3 Categorization of Incidents

Following the data cleaning process, incidents from the SDNY dataset were categorized into five operational domains. These categories capture the nature of the incident and its impact on operations. This process facilitates the development of a

checklist by identifying vulnerabilities with specific intervention methods. Refer to the table below. Table 5 illustrates the problem categories identified in the research, accompanied by examples they encompass.

Table 5: Problem Categories and Examples

Problem Category	Representative Examples
Infrastructure Integrity and Systemic Failures	False alarms, equipment malfunctions, system control failures
Critical Health and Safety Emergencies	Medical emergencies, staff or visitor injury events, life safety crises
Disruptive Conduct and Behavioral Security Risks	Protests/demonstrations, disorderly behavior/conduct
Threat Intelligence and Hazardous Risk Management	Suspicious activity, threats, hazardous materials outside facility

3.4.4 Conclusion of Data to Drive Home Gaps

Data to drive home gaps provides the framework for identifying courthouse vulnerabilities. This addresses Research Question 2 by getting to know the incident report data and enabling the checklist to identify repeat incidents. It also answers Research Question 3, showing how incident data can be structured and used to enforce proactive and evidence-based security reactions.

3.5. Checklist Elements to Alleviate the Gaps

To address vulnerabilities found in courthouse facilities, checklist elements must be implemented. The elements are lessons learned in related literature and best practices from other high-risk industries. They seek to embed consistency, accountability, and proactive risk reduction.

The checklist items below come from best practices found in the Department of Homeland Security (United States Department of Homeland Security, 2022), Smith and Brooks (2012), Wyss, Kolbe, and Grande (2023), and the National Institute of Standards

and Technology (2018), and Hales et al. (2008), among others. Each item aims at closing gaps and recommends verification phases to ensure they remain effective over time. Table 6 shows categories of identified problems found in similar facilities and the elements were identified with patterns from SDNY incident data that other sectors implemented into practice. The table outlines a practical preventative effect, demonstrating the checklist as a tool for mitigating risks in real-bureaucracy court facilities.

The checklist elements do not replace existing protocols. They are designed to represent daily activities that can make courthouses more resilient to the evolving threat environment. When implemented correctly, they support stakeholder collaboration and preparedness, which is essential. The focus areas are designed to address security deficiencies based on interdisciplinary security measures and response protocols. The elements in Table 6 map common vulnerabilities and align them with the best practices found in existing literature. The various referenced sources recommend assessment frequencies aiming to minimize complacency and incorporate risk mitigation into everyday activities. This includes bridging these components into a proactive, layered defense framework that continues to evolve dynamic resilience, promotes interagency interoperability, and helps protect the federal courthouses from emerging threats.

Table 6: Checklist Elements to Mitigate Security Gaps

Problem Category	Relevant Checklist Elements	Source	Expected Preventative Impact
Infrastructure Integrity and Systemic Failures	- Conduct daily operational checks on critical facility equipment - Schedule preventive maintenance as required for all security-related equipment	Smith & Brooks (2012); Pei et al. (2018)	Early detection and correction of system malfunctions; reduced operational disruptions
Disruptive Conduct and Behavioral Security Risks	- Enforce strict visitor screening and logging protocols - Conduct behavioral threat awareness training for staff - Randomize secondary visitor screenings	USC (2024); DHS (2022)	Enhanced detection of disruptive individuals; improved de-escalation readiness
Physical Access Violations and Security Breaches	- Verify functionality of all access control points (daily) - Review badge audit logs (weekly) - Conduct perimeter barrier inspections (per shift) - Patrol perimeter areas at opening, mid-day, and closing	DHS (2022); Smith & Brooks (2012)	Improved access control discipline; early identification of unauthorized entry attempts
Critical Health and Safety Emergencies	- Test radios, public address systems, and internal communication devices per shift - Maintain updated emergency contact lists at all posts (weekly) - Conduct quarterly interagency tabletop exercises	Wyss, Kolbe, & Grande (2023); NIST (2018)	Faster incident reporting; enhanced coordinated emergency response
Threat Intelligence and Hazardous Risk Management	- Conduct monthly refresher training for all security personnel - Administer random knowledge and compliance checks (monthly) - Enforce dual-authentication protocols for sensitive areas (daily enforcement)	Hales et al. (2008); Insider Threat Task Force (DNI, 2020)	Strengthened internal compliance; mitigation of insider misconduct and procedural lapses

This answers Research Question 5 by identifying features which facilitate a security checklist's adoption, usage, and effectiveness within a multi-agency courthouse.

3.6 Conclusion to Methodology

Figure 5 below maps the methodology applied in this research:

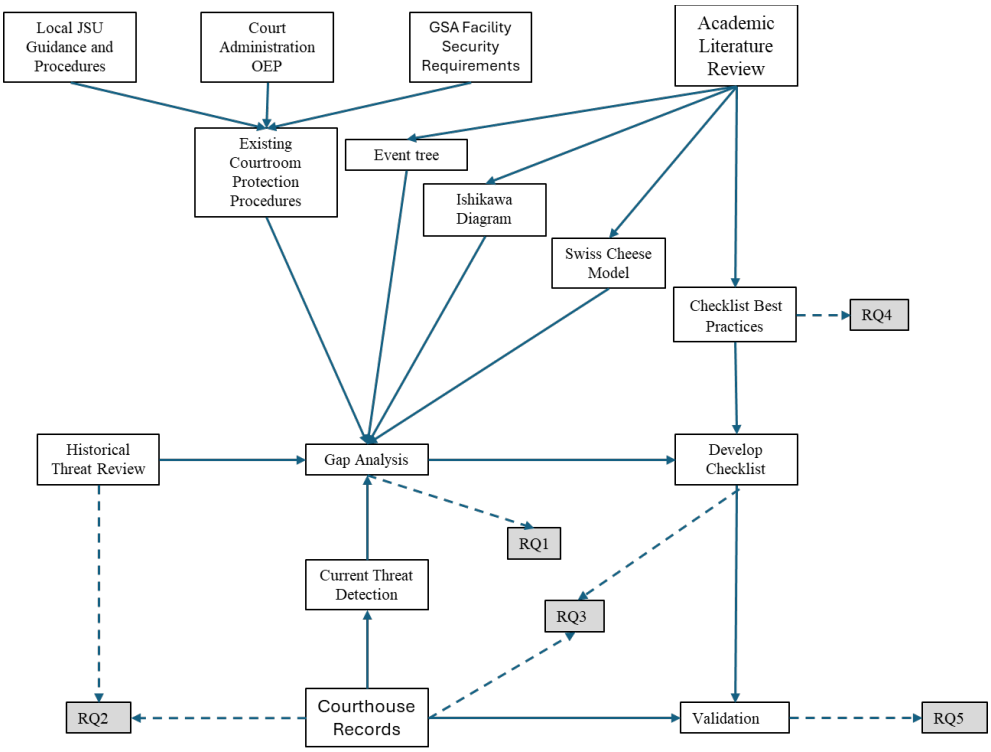

Figure 5: Map of Methodology

This approach translates incident data into a systems-based approach that may enhance courthouse security operations. Applying tools such as the Ishikawa diagram with the Reason's Swiss Cheese model creates a framework to identify root causes and understand vulnerabilities. It is not limited to singular failures. This approach maps shortcomings in security and builds a list of remedies to address vulnerabilities in a courthouse setting.

Additionally, this is designed to remain actionable at the local courthouse level. It accounts for the limitations such as the inconsistencies amongst the 94 districts throughout the country, evolving threat climate, and gaps caused by poor interagency collaboration. The result is a responsive and scalable tool. The following section will discuss the results found based on the applied methodology.

Chapter 4: Results and Findings

This chapter addresses the results of the research questions from Chapter 1 answered by the methodology outlined in Chapter 3. The research reviewed 1,273 incident reports, which exposed operational failures that have gone unaddressed within the SDNY. Due to oversight and inadequate application of best practices, procedural gaps exposed vulnerabilities within the district. These findings are essential for understanding how systemic failure arises in the landscape of courthouse operations.

The following subsections address the research questions in the introduction, drawing on reported incident data and critically considering how the introduced checklist interventions may have alleviated or prevented the incidents. The analysis ends with developing a prototype security checklist applicable to the operational setting of federal courthouses based on reported incidents.

4.1 RQ 1: What are the current courthouse security procedures in place, and how effective are they in mitigating operational and threat-based risks in high-consequence judicial environments?

Securing the federal judiciary out of SDNY is built from a framework established by the USMS, the AOUSC, and GSA. These stakeholders oversee the security operations, including access control, surveillance, emergency preparedness, and facility operations. Entry into SDNY facilities requires screening through metal detectors and x-ray systems operated by over 200 Court Security Officers (CSOs) and Special Security Officers (SSOs) under USMS supervision. Surveillance technologies monitor public and restricted areas, while emergency preparedness is coordinated through Occupant Emergency Plans

(OEPs), developed in collaboration with external agencies such as the NYPD and FDNY. Threat assessments are informed by regular coordination with intelligence partners, including the FBI's Joint Terrorism Task Force.

These procedures have been established to provide several barriers for those who intend to do harm. Such barriers include:

- External Intelligence
- External Monitoring
- Physical Infrastructure
- Internal Screening Procedures
- Personnel Training
- Internal Medical Facilities
- Communication with Outside Emergency Agencies

Though there are established procedures for the construction and maintenance of these barriers, there have been past documented breaches where sequential failures of these barriers have occurred indicating a need for tighter and continuous scrutiny of their design and maintenance.

Even with formal procedures in place, vulnerabilities are still present. An event tree analysis from past events illuminates several scenarios which lead to undesirable consequences. These scenarios are motivated by documented events.

Scenarios 1 - Internal Medical Emergencies:

On April 10, 2014**,** a juror was struck by an elevator inside a federal courthouse after a mechanical malfunction. While not a malicious act, this

personal safety incident demonstrates how non-hostile initiating events can escalate due to systemic breakdowns. Preventive maintenance and early-warning systems were insufficient. No real-time alert or monitoring system identified the elevator malfunction in progress. The infrastructure failure was the elevator itself, a critical facility system with no redundancy or warning safeguard. There were no protective barriers or procedures in place to prevent access to the malfunctioning elevator, representing a screening failure. Most critically, a communication breakdown occurred when malfunctioning radios delayed the medical response, pointing to gaps in personnel readiness, coordination, and emergency communication protocols.

Scenario 2 – Internal Disturbance Resulting in Attack:

On January 6, 2021**,** an individual under the supervision of U.S. Probation became disruptive inside the Clerk's Office of a federal courthouse. This initiating event, a behavioral disturbance, escalated due to multiple systemic failures. There was no indication that the individual had been flagged for behavioral risk, reflecting an intelligence failure. Monitoring capabilities were insufficient, with no real-time observation or behavioral alerts in place. Critically, a malfunctioning duress alarm represented a breakdown in external infrastructure, preventing prompt notification to Court Security Officers. The absence of safeguards to detect behavior in public spaces indicated a screening failure. Ultimately, the delay in response exposed vulnerabilities in communication systems and emergency coordination, highlighting a failure in personnel readiness and procedural execution.

Scenario 3 – Unarmed Attack from Inside Courthouse:

On January 26, 2024, an individual who was actively listed on the district's watchlist gained unauthorized access, the initiating event of entry by a known threat. This breach stemmed from an intelligence failure, as existing procedures designed to flag and intercept barred individuals were either not followed or improperly implemented. A monitoring failure followed, as CSOs were unaware of the subject's status. The fact that the individual was able to bypass security and reach a courtroom highlights an external infrastructure failure**,** specifically in access control enforcement and checkpoint oversight. A clear screening failure also occurred, as the subject was not intercepted at the point of entry despite visible protocols being in place. The situation escalated into physical violence, and the delayed removal of the individual by responding law enforcement exposed further personnel, medical, and communication failures, including inadequate readiness, insufficient escalation procedures, and gaps in interagency coordination. This incident underscores how compounded failures across multiple domains of the fault tree can enable a prohibited individual to penetrate courthouse defenses and threaten the integrity of judicial operations.

Scenario 4 – Armed Attack from Inside Courthouse:

On February 19, 2024, an individual carrying a visible knife walked around the exterior perimeter of a federal courthouse, passing multiple law enforcement patrol vehicles and security posts before entering the building. This incident began with an initiating event**,** a visibly armed individual approaching and accessing federal property without immediate interdiction. The fact that the subject's

weapon was not recognized or intercepted by law enforcement before entry reflects an intelligence failure, as there was no situational awareness or recognition of the threat despite visible patrol presence. A monitoring failure occurred in that surveillance or visual observation systems did not detect or escalate the threat as the individual approached the facility. The ease of movement around the perimeter and into the courthouse, without challenge or deterrent measures, highlights an external infrastructure failure**,** particularly regarding roving coverage, surveillance zone integration, and access control. Upon entry, a screening failure emerged. While the CSO appropriately engaged the subject, the individual was able to bypass all outer layers of security and reach the building entrance while armed. Finally, a delayed response in removing the individual from the premises and involving law enforcement demonstrated a breakdown in personnel readiness and communication protocols, as coordinated intervention did not occur until the subject had caused multiple disturbances outside the entrance. This event illustrates how the absence of proactive detection, interagency coordination, and layered physical security can allow a potentially dangerous individual to reach the entry of a critical facility.

Scenario 5 – Attack from Outside Courthouse:

On June 24, 2021, a disorderly individual began throwing debris at the main entrance of a courthouse. Several projectiles struck the building's facade, shattering a lower glass panel near the entryway and initiating a security event involving external disorderly conduct and property damage. An intelligence failure was evident, as prior reports had documented the individual loitering and

harassing pedestrians near the courthouse in the days leading up to the incident; however, no alert notifications were created. This was followed by a monitoring failure, as perimeter surveillance systems failed to detect or escalate the behavior due to poorly positioned cameras and inadequate monitoring. The resulting damage revealed an external infrastructure failure, as the affected glass was not reinforced, and the entrance lacked features to shield it from direct attacks. Although the individual never breached the interior, the absence of proactive deterrence or engagement from exterior security posts reflected a screening failure. This was a missed opportunity to de-escalate the threat before property damage occurred. Lastly, a delayed response by law enforcement and a lack of internal communication with court occupants highlighted a personnel and communication failure, exposing deficiencies in situational awareness, response coordination, and threat containment protocols. This incident demonstrates how even seemingly minor disturbances can escalate into operational and security risks when multiple layers of defense break down simultaneously.

The above scenarios are depicted via block diagrams of sequential failures rather than standard event tree form in Figure 6 below. The standard representation would be too complicated due to the number of potential barriers and this allows the focus on the observed shortfalls which can be further analyzed using the Ishikawa Diagram and Swiss Cheese Model.

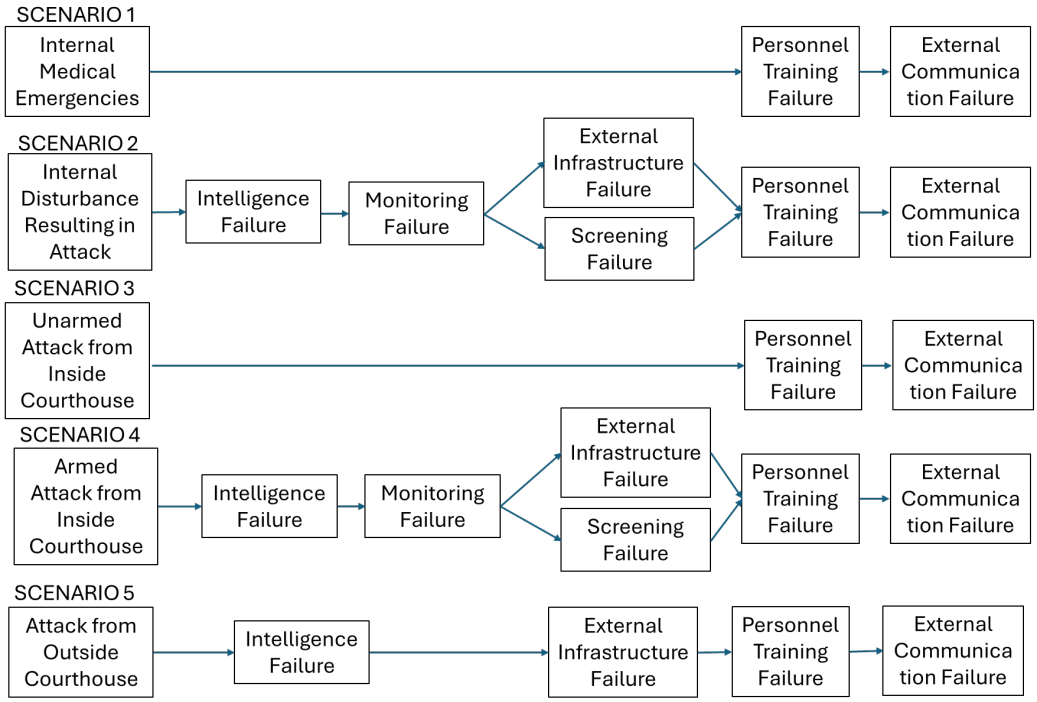

Figure 6: Potential Undesired Scenarios

The incident data from the district identified that stakeholders follow their standard operating procedures (SOPs), but poorly communicate with each other, and seldom share accountability. This approach has resulted in repeated systematic failures. For example, 25% of the reported incidents were caused due to infrastructure issues, such as equipment failures. Another example is the inconsistent practices in access control and threat monitoring have led to poor identification practices and unauthorized access attempts.

Courthouse security relies heavily on fragmented documentation, ad hoc verbal coordination, and reactive crisis management. Without a centralized framework, best practices are inconsistently applied, and routine security oversight is often inadequate. As a result, critical protective functions are undermined not by the absence of protocol but by the failure to integrate existing agency efforts into a cohesive, preventive system.

A review of the ISC Armed Contract Officers' best practices, which are the foundation of post standards for Court Security Officers, shows how federal policy cuts across the landscape of district operations and imposed building standards, which are often unevenly enforced. These practices were compared in relation to both incident data out of SDNY and modern best practices and guidance, such as the infrastructure mandates provided in GSA's P100 (2024). OEPs tend to become less than what is needed in a crisis. These plans often allocate roles to actors, but there is rarely a detailed identification of actual or concrete tasks or cooperation protocols. The vagueness leads to varying behaviors, such as disruptive behavior and medical emergencies that repeatedly occurred in the SDNY dataset.

The USMS and its Judicial Security Division (JSD) represent a more centralized and professionalized security model. The Office of Court Security (OCS), under JSD, serves as a liaison for training, research, facility evaluations, and protective operations. JSD has improved the quality and consistency of the USMS response in these facilities throughout the agency. However, locally it can be less effective as it is impossible to develop application standards based on each district's unique dynamics.

For example, the USMS Judicial Security Unit (JSU) of SDNY has established its SOPs and guidelines for judiciary protection, escorting high-profile individuals, and responding to equipment maintenance. This builds internal inconsistency and points to the larger issue: There are 94 federal districts, and each does security differently. This process dilutes the possible effects of the agency's directives and makes it difficult to gauge, share, and replicate successful

outcomes across the districts. Additionally, GSA's P100 (2024) is the most widely encompassing and enforceable of infrastructure standards documents for federal government facilities, including courthouse security. Within the context of the ISC Risk Management Process, the P100 includes prescriptive physical and operational countermeasures, including level-specific facility measures for each building's Facility Security Level (FSL) and needed Level of Protection (LOP). Key infrastructure requirements and standards are summarized as follows:

- Blast-resistant construction and progressive collapse prevention
- Ballistic glazing and access-controlled circulation zones
- Chemical, biological, and radiological filtration systems
- Protected utility corridors and emergency power redundancy
- Hardened mailrooms and secure detainee movement pathways

These features are required by law for all FSL III and IV courthouses, including facilities like those in SDNY. However, the existence of sophisticated infrastructure is not sufficient to ensure security, as indicated by the data in the field. More incidents stem not from issues with architectural deficiencies but from oversights in implementing the process, lack of personnel oversight, inconsistent access procedures, and inadequate maintenance on equipment.

Poor coordination and communication among stakeholders amplify the lack of process transparency, particularly within OEPs and local SOPs. Even where infrastructure-level defenses are deployed, their effectiveness is undermined by unclear policies and uncoordinated operational implementation. Also, in contrast to restoring identity, despite adequate training and guided strategies, there is no

continuous system for assessing performance, receiving feedback on incidents, and validating procedures across districts.

These results validate the primary argument presented in the introduction: *"Currently, there is no systematic method for evaluating and monitoring the variety of the dynamic threats to the successful operation of the courthouse that exist across jurisdictions, and without an agnostic and scalable, all-hazards approach, courts of law remain vulnerable to operational disruption, reputation harm and physical harm."* The findings also support the hypothesis that current courthouse security procedures are inconsistently implemented and only partially effective due to procedural gaps, fragmented communication, and insufficient incident reporting standards. What is needed is an intervention that is checklist-driven, mapping operational behavior to actual world vulnerability. SDNY incident data shows that the hidden vulnerabilities of the system's protective posture are the root cause of the security issues in the district.

The development and implementation of a site-specific operational security checklist must:

- Translate national standards into daily practices
- Promote interagency collaboration and shared accountability
- Be validated against historical incident data
- Remain adaptable to unique facility risk profiles

The integration of guidelines and processes discussed in this section directly supports the prototype of the checklist model proposed at the end of Chapter 4.

This chapter of findings, therefore, serves as the transition from identified weaknesses to a system-engineered solution to protecting federal courthouses.

4.2 RQ2: What are the most frequent and preventable security failures occurring in federal courthouses, and what systemic factors contribute to them?

An analysis of 1273 reported incidents from 2013 to 2024 in SDNY (see Appendix) revealed that the most common type of security failures consisted of incidents categorized as Infrastructure Integrity and Systemic Failures. This category accounted for 24% of the reported incidents. This is the most structurally avoidable domain of vulnerability in the courthouse as it pertains to equipment upkeep and maintenance. As seen in Table 7, these failures cover a variety of operational problems, including safety, security, and functionality of courthouse environments.

Table 7: Operational Risk Factors Leading to Security Vulnerabilities at SDNY

Gap Area	% of Total Incidents	Operational Impact
Infrastructure Integrity and Systemic Failures	24%	Alarm failures, elevator malfunctions, critical facility disruptions
Critical Health and Safety Emergencies	23.6%	Medical emergencies, life safety risks requiring immediate response
Disruptive Conduct and Behavioral Security Risks	22%	Protests, disorderly conduct, volatile visitor incidents
Threat Intelligence and Hazardous Risk Management	16.8%	Suspicious packages, hazardous material threats
Physical Access Violations and Security Breaches	13.6%	Intrusion tests, unauthorized access attempts

Infrastructure Integrity and Systemic Failures include alarm malfunctions and inoperable equipment, which could lead to an unsafe environment. Additionally, power failures have shut down cameras, access control systems, and communications systems required for monitoring building activity. Faulty HVAC

systems have damaged courthouse property, which can create quality-of-life issues, especially if the utility has a nexus to life and health. In total, these problems lead to poor situational awareness, which may reduce security personnel's ability to operate at an efficient capacity.

Failures are the result of predictable, yet overlooked factors, such as old equipment, sporadic preventative maintenance, and a lack of real-time diagnostics. Elevators might malfunction due to mechanical wear or misalignment of parts. HVAC systems can fail due to dirty filters or compressor issues. Access control systems can fail due to server desync or broken badge readers. The fact that these vulnerabilities remain highlights a broader systemic failure, where facility management does not approach infrastructure resilience in a planned and proactive way. Below is an account from the other four categories:

- Critical Health and Safety Emergencies (23.6%): Include fires, medical emergencies, and other life-threatening incidents. These conditions may require immediate evacuation, emergency services response, or shutdown. When it comes to federal courthouses, such crises shut the system down and require some level of joint interagency response.
- Disruptive Conduct and Behavioral Security Risks (22%): Include disorderly conduct by unruly people, demonstrations and protests, and behavioral health emergencies. The source of the conduct may stem from the public, litigants, or staff. Behavior-based threats need strategic response plans that combine physical security measures and de-escalation tactics with mental wellness considerations.

- Threat Intelligence and Health Risk Emergencies (16.8%): These include threats to the facility or its personnel. They may be communicated by phone, email, or online. They can be received from intelligence provided by other law enforcement agencies, indicating an individual is being targeted, or public health risks such as pandemics. The focus is on proactive measures grounded in external intel or health advisories that impact security posture and continuity of operations.
- Physical Access Violations and Security Breaches (13.6%): Incidents such as unauthorized personnel in secure spaces, tailgating through restricted doors, doors not locking properly, and access card readers not working. These shortfalls are frequently exposed in such breaches and are among the most avoidable through better monitoring, access rules, and periodic checks.

Together, these categories indicate that the most preventable breakdowns in federal courthouse security generally do not result from an isolated mistake but from a combination of outdated technology, disjointed protocols, inadequate coordination, and gaps between training and procedure enforcement. When mapped through Reason's Swiss Cheese Model, these vulnerabilities can be seen to intersect with active threats to result in security holes. Figure 7 below illustrates this interaction by visualizing how multiple layers of defense, each with its own set of weaknesses, can align to allow incidents to penetrate the courthouse's protective posture.

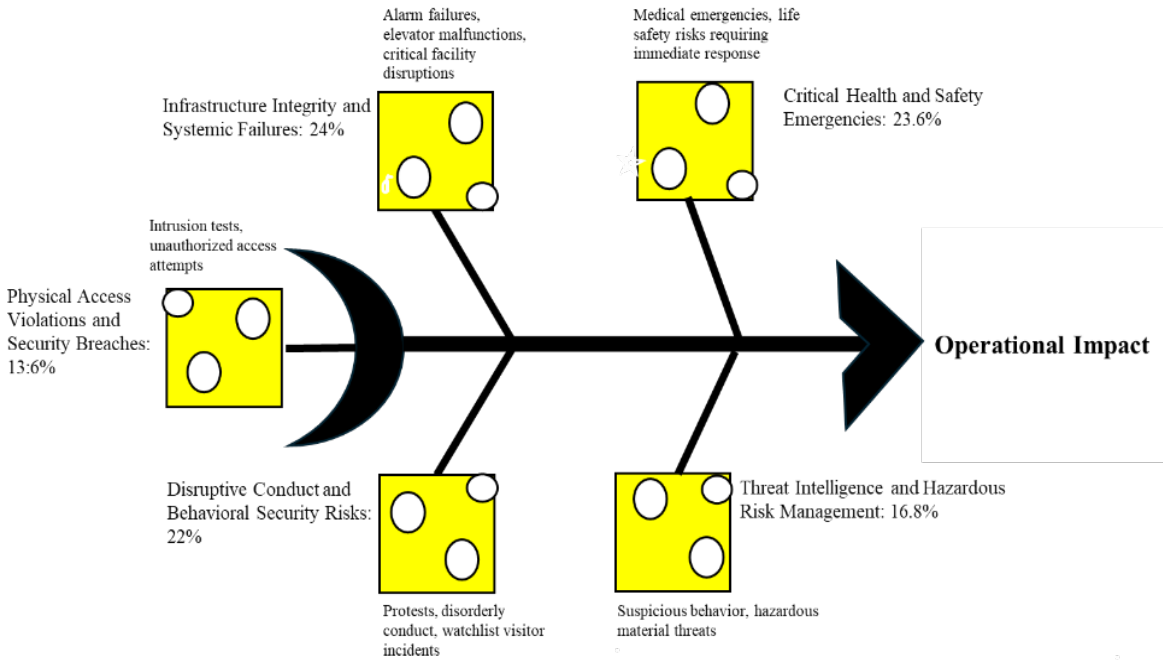

Figure 7: Operational Risk Factors Leading to Security Vulnerabilities at SDNY

4.2.1 Broader Implications Across Judicial Districts

While the SDNY provides a critical case study due to its high-profile judicial docket, specific environmental and architectural accommodations, and threat environment, it is important to note that each of the 94 districts may face different threat patterns, local environmental and jurisdictional factors, and operational considerations:

- Remote and rural districts may not be able to support and maintain the latest technological equipment, which may reduce the level of surveillance or create delays in emergency response.
- Border areas often face smuggling problems, especially contraband, and there is a great need for external law enforcement coordination.

- Organized protests and politically motivated disruptions may be enhanced in urban high-threat districts.

This supports the hypothesis that the most frequent and preventable security failures stem from insufficient training, communication breakdowns, and inadequate maintenance practices. Despite variations in courthouse environments, common systemic issues consistently emerge: the absence of standardized procedures, fragmented interagency responsibilities, poorly maintained equipment, and a general lack of shared accountability among stakeholders. These recurring vulnerabilities stress the need for a coordinated method, such as a checklist, to address the root causes of failure.

4.2.2 The Role of a Standardized Checklist in Risk Mitigation

This analysis supports a standardized checklist for courthouse security measures. The majority of the failures reported were potentially avoidable if the following appropriate measures had been taken:

- Infrastructure failures: Weekly maintenance validation, pre-scheduled HVAC and power backup checks, and audits of system performance would reduce failure rates.
- Behavioral Risks: Pre-entry behavioral threat assessments and mandated de-escalation training would enable early detection and response to volatile individuals
- Access Violations: Regular testing of access card readers, contractor escort tracking, and secondary screening procedures would mitigate unauthorized access and contraband entry

- Threat Mitigation: Uniform protocols for responding to suspicious activity, supplemented by visual guides for reference, and emergency protocols would enhance hazard triage and minimize chaos during active threats.

These interventions could be institutionalized via a centralized checklist, which improves interagency coordination and procedural uniformity. Furthermore, a tool like this would also decrease stress and cognitive overhead in high-pressure environments by delivering explicit to-do lists informed by immediate reporting and action amid ongoing decision-making, incident reporting, and emergency response.

The adoption of a standardized checklist provides a scalable method to address frequently exploited vulnerabilities in courthouses. This proactive risk management approach mixes principles and experiences that can be tailored to a variety of environments.

4.3 RQ3: How can incident reporting data be structured and analyzed to inform proactive, checklist-based security interventions?

Given suitable structuring and analysis, incident report data can be used to develop a proactive checklist for judicial security. SDNY reports were systematically classified into five broad operational categories:

- Infrastructure Integrity and Systemic Failures
- Critical Health and Safety Emergencies
- Disruptive Conduct and Behavioral Security Risks
- Threat Intelligence and Hazardous Risk Management,
- Physical Access Violations and Security Breaches.

These categories incorporate a process which can facilitate the identification of vulnerabilities and failure patterns.

Common issues include malfunctioning alarm systems and elevators. These failures have a negative impact on courthouse operations and can interrupt an emergency response. A checklist that included preventive maintenance procedures, basic inspections, and ensured daily system verification had been performed would have identified these issues earlier and reduced downtime.

Similarly, an incident involving a letter with a powdery substance that made its way to a judge's chambers revealed how gaps in threat intelligence and mail screening remain. The response was slow because there were inconsistencies with hazardous materials screening. A checklist that incorporates mail screening, instant reporting procedures, and timelier response coordination with local hazmat teams would have created a more seamless structure for handling these situations.

Incidents involving access control were also a serious cause for concern. For example, people have successfully entered secure sites with expired or fraudulent access cards in several instances. This compromises facility security, and these issues often stem from poor access verification. A list allowing real-time access card verification, frequent access reviews, and double verification at secure entry points would have immediately addressed the breaches.

This research translated raw data into a framework for a call-to-action planning model by organizing and analyzing historical incident data. Every detected vulnerability is linked to a checklist item. This occurred because these situations were mapped to a checklist item designed to close procedural gaps,

shifting from a collection of reports to intervention operations that permit learning from past mistakes.

Table 8: Mapping of Incident Categories to Checklist-Based Security Interventions

Incident Category	Representative Incident	Checklist-Based Intervention
Infrastructure Integrity and Systemic Failures	Alarm failure, equipment malfunction	Daily system checks; monthly elevator testing; emergency power drills
Critical Health and Safety Emergencies	Inmate collapsed in holding cell; delayed medical response	Medical response drills; emergency call-point testing; staff role assignments
Disruptive Conduct and Behavioral Security Risks	Disruptive visitor caused courtroom disturbance	Behavioral incident response protocols; courtroom officer positioning review
Threat Intelligence and Hazardous Risk Management	Suspicious powder-filled envelope triggered floor evacuation	Mail screening checklist; hazmat coordination procedure; floor-specific evacuation plans
Physical Access Violations and Security Breaches	Contractor accessed restricted area with expired badge	Real-time badge validation; access permission audits; dual-verification checkpoints

In sum, these findings directly support the hypothesis that structuring and analyzing incident data can reveal patterns that inform the development of an effective security checklist by highlighting operational risks and vulnerabilities. As illustrated in Table 8, incident reporting and data analysis facilitate a shift from a reactive approach to a proactive security posture. By identifying recurring issues and aligning them with procedural shortcomings and known vulnerabilities, this model offers a data-driven strategy for enhancing courthouse security and resilience.

4.4 RQ4: What design features are essential to ensure the adoption, usability, and effectiveness of a security checklist in a multi-agency courthouse environment?

The successful implementation of a checklist in a high-threat, multi-agency environment, like a federal courthouse, depends on how well it adheres to proven best practices. These practices emphasize accountability, adaptability, usability, and practicality. When applied to the operations of a federal courthouse, it ensures the checklist evolves beyond compliance into an active platform, ensuring operational discipline and risk reduction.

A practical checklist prioritizes action over documentation. Each line item must be actionable, brief, and concise, and it must be free of unnecessary complications that may cause confusion and delay in emergency situations. To courthouse personnel, this means easy-to-understand instructions, such as ensuring identification cards are visible when accessing the facility through a secured path. Clearly worded instructions improve execution over vague or overly technical verbiage.

The sequence of individual checklist items should reflect the sequence of courthouse operations. Combining operational tasks makes it easier for the user to apply and less likely for steps to be missed. Mirroring daily security practices enables the performance of intervention methods in the correct order.

Visual cues play a role in checklist usability. A well-structured checklist incorporates formatting such as bold headings, checkboxes, and status indicators to facilitate quick interpretation. These reminders benefit chaotic situations such as dealing with behavior disturbances or suspicious packages, where clear guidance is required. This

clarity supports confident decision-making by frontline personnel such as CSOs and SSOs.

Integrating checklists into the everyday courthouse operations is a long-term requirement. They should not be standalone documents but supplemental to established policies and procedures already put into place. These documents should be present during shift change, staff orientation, and post-incident debriefings. For example, a hazardous substance found in an envelope may have been downgraded in significance had mail screening procedures been reviewed and trained on as part of the security checklist protocol. Adding training helps normalize the use in the field, promoting procedural fluency while honing a safety-conscious operational climate.

Checklists also need to be dynamic and responsive to new threats. A periodic review cycle allows for the inclusion of new lessons learned, new identified vulnerabilities, and changes to processes. Iterative updates based on incident data can also result in integrations of newer verification methods and authentication checks. Accountability and ownership are a must. Each item on the checklist must have a stakeholder responsible for its completion, whether the USMS, GSA, or court administration. This approach facilitates compliance, supervision, and post-incident reviews. It outlines who is responsible for what, when, and how often it should be done. Without this information, the most comprehensive document cannot change behavior or minimize liability. The checklist must also be co-created, reviewed, and universally approved to increase clarity and avoid overlap. This ensures all parties agree and the various operational assignments

are achievable. It also fosters a consistent approach across jurisdictions and encourages a collective response to threats.

Lastly, digital integration improved the reliability and traceability of checklists. Moving from paper to secure digital creates the ability to have real-time access, tracking, and auditing of the historical records. For example, suppose an item on an evacuation plan is overlooked during a drill. In that case, the system can record that and bring it to the attention of the appropriate official to have the discrepancy corrected. Over time, these practices create a more robust and long-term safety culture. Incorporating these as best practices transforms the checklists from a static to a living security document. The facility becomes resistant when collaboration occurs due to improved communication, joint operations, and shared responsibility.

These principles reflect the checklist designed in this paper and form the basis of evidence-based practice. Therefore, they have practical applicability in multiple courthouse settings. This directly supports the hypothesis that security checklists which are adaptive, include role-specific tasking, and promote collaboration are more likely to be consistently used and will enhance the overall effectiveness of the security posture in and around the courthouse. These characteristics are essential drivers of long-term checklist adoption and courthouse resilience.

4.5 RQ5: In what ways does an interdisciplinary checklist framework improve risk visibility, role clarity, and operational consistency across courthouse security stakeholders?

The findings provided throughout this chapter are evidence that a checklist approach to enhancing security in the courthouse will improve risk awareness, clearly

identify roles, and establish consistent operations among agencies. The lack of unified operational leadership has created avoidable gaps, and a piecemeal response in these environments hinders the performance of law enforcement, judicial personnel, and facilities management.

Having combined security procedures, the checklist consolidates unrelated operational domains into a cohesive unit. This method works to eliminate risk and initiates progress to be transparent by taking non-specific policy mandates and incident history into specific and observable actions. For example, repeated infrastructure failures are uncovered as risk domains when they are operationalized as checklist items, such as verify backup generator readiness or conduct access card reader function. This translation of latent vulnerability into operational practice enables agencies to be more proactive in identifying and mitigating risk before it is realized as a security incident.

The checklist clarifies the roles of each stakeholder in an environment where overlapping jurisdiction exists. Reviewing incident data revealed that many failures did not occur due to a lack of protocol. The issue is unclear ownership and insufficient enforcement. By assigning specific roles, the checklist minimizes uncertainty and establishes a line of authority amongst the stakeholders for each security activity. This improves oversight and accountability by establishing consistent procedures.

The checklist promotes operational uniformity, which is most important in the context of courthouse security. Today, all 94 US federal districts interpret federal guidance differently, leading to inconsistent application of security guidelines. By creating an instrument that can be contextualized locally while at the same time staying

consistent with national standards, the checklist guarantees a consistent application of best practice. This minimizes reliance on verbal agreements, ad hoc coordination, or informal exchanges of knowledge and replaces such reliance with transparent, repeatable, and auditable processes.

In summary, this approach is dynamic to the rise of new threats. By integrating various viewpoints in the checklists' design stage, it ensures the product developed is usable across varying judicial climates. Additionally, it improves the ability to see risk by converting system vulnerabilities into measurable actions. Presented is a role that delegates operational duties to specific stakeholders. Operational consistency is driven through standardization so that the systems can become more reliable and responsive to security needs in high-risk judicial contexts. Collectively, these findings support the hypothesis that an interdisciplinary checklist strengthens courthouse security by clarifying roles and responsibilities, enhancing operational efficiency, aligning stakeholder expectations, and reducing ambiguity in security operations.

4.6 The Prototype

The following prototype security checklist is designed to address the vulnerabilities discovered from incident report analysis and literature review. It comprises five operational areas:

- Physical security
- Access control
- Communication
- Threat detection

- Procedural compliance.

The checklist presented in Table 9 consists of specific action items, divided by how often they should be completed (daily, weekly, and monthly). Developed to improve awareness of risks, define responsibilities between stakeholders, and instill a culture of uniformity in operations, this framework should be practical enough to be applied across all facilities, ensuring security measures are consistent, sustainable, and updated to address a dynamic threat environment.

The tasks defined in the checklist represent the framework to proactively mitigate risks in federal courthouses. Assisting teams by integrating daily, weekly, and monthly routines to ensure each domain is covered, the list turns compartmentalized tasks into a cohesive and repeatable culture of action. Each stakeholder is working in and around the courthouse, whether dealing with normal day-to-day operations or addressing a crisis.

While it is difficult to ascertain the full impact of implementing the above checklist, it is possible to illustrate the effect it would have on the scenarios motivated by actual events

Scenarios 1 - Internal Medical Emergencies:

Regarding the incident involving the injured juror, the checklist would require regular preventive maintenance inspections for all critical building systems, including elevators. Documentation of the completed service and immediate escalation protocols for malfunction indicators to address the initial intelligence failure would be included. It would also include monitoring procedures and alert systems for mechanical failures, ensuring that facility staff are immediately notified of any issues in progress. To prevent unauthorized or

Table 9: Prototype Interagency Courthouse Security Checklist

Domain	Task	Frequency	Responsibility	Done
External & Internal Infrastructure	Ensure external access points (loading docks, utility entrances) are locked and alarmed	Weekly	GSA	☐
	Inspect elevator systems and test emergency stop/alert features	Monthly	GSA	☐
	Inspect and repair courthouse entry points (doors, locks, hinges, etc.)	Monthly	GSA	☐
	Verify perimeter fencing, bollards, and signage are intact and clearly marked	Monthly	GSA	☐
	Ensure windows and perimeter structures are secure and undamaged	Quarterly	GSA	☐
	Conduct building-wide maintenance checks for facility wear or mechanical faults	Quarterly	GSA	☐
Security Monitoring & Screening	Inspect and service CSO/SSO radios and communication devices	Weekly	USMS	☐
	Verify proper function of badge readers and access control panels	Weekly	USMS	☐
	Test and log duress alarm functionality	Weekly	USMS	☐
	Check perimeter surveillance coverage and live-monitoring readiness	Weekly	USMS	☐
	Perform preventive maintenance on X-ray machines and magnetometers	Monthly	USMS	☐
	Test and maintain intrusion detection systems	Monthly	USMS	☐
	Verify integration of fixed cameras and roving patrol zones for perimeter coverage	Monthly	USMS	☐
	Conduct intrusion detection and access system failover tests	Quarterly	USMS	☐
	Inventory all physical security technology and verify calibration	Annually	USMS	☐
Personnel Training & Compliance	Perform randomized secondary screening validations at access points	Weekly	USMS	☐
	Verify access credentials and revoke expired or unauthorized IDs	Weekly	USMS	☐
	Review inmate transport logs and validate restraint compliance	Weekly	USMS	☐
	Verify exterior observation procedures are followed during patrol shifts	Weekly	USMS	☐
	Audit CSO post logs and visitor screening documentation	Monthly	USMS	☐
	Conduct training refresher for CSOs/SSOs on screening procedures	Quarterly	USMS	☐
Administrative Coordination & Intelligence	Facility interagency intelligence briefings	Weekly	Court Administration	☐
	Update and submit list of court-authorized personnel for access	Monthly	Court Administration	☐
	Distribute security protocol updates to court staff and tenants	Quarterly	Court Administration	☐
	Coordinate and facilitate quarterly security committee meetings	Quarterly	Court Administration	☐
	Review and update Occupant Emergency Plan (OEP)	Annually	Court Administration	☐
	Coordinate with USMS for security planning of high-profile court events	As Needed	Court Administration	☐
Emergency Preparedness	Review emergency signage and egress lighting for visibility	Monthly	GSA	☐
	Test facility-wide alert systems (PA, alarms, strobe)	Quarterly	USMS / GSA	☐
	Test medical response protocols and radio communications during drills	Quarterly	USMS / Court Administration	☐
	Review and update procedures for exterior armed threat detection and early intervention	Quarterly	USMS	☐
	Plan and facilitate interagency intelligence-sharing and coordinated response drills with local and federal partners	Biannually	USMS / Local Law Enforcement	☐
	Conduct building-wide active threat and fire evacuation drills	Biannually	USMS / GSA / Court Administration	☐

unsafe access, the checklist would mandate physical safeguards, such as out-of-service signage, restricted access barriers, and staff notification procedures during maintenance events, to address the screening failure. Finally, communication protocols would be tested regularly to ensure that any medical emergency could be swiftly coordinated. By embedding these steps into daily and weekly operations, the checklist would create a layered defense against mechanical hazards and ensure rapid, coordinated responses to protect courthouse personnel and visitors.

Scenario 2 – Internal Disturbance Resulting in Attack:

A security checklist would have introduced multiple safeguards to prevent the escalation of the January 6, 2021 incident. The checklist would include coordination protocols between U.S. Probation and the USMS, ensuring that individuals with recent violations, aggressive behavior, or supervision concerns were flagged and documented prior to their arrival. It would also require daily functionality checks of duress alarms and monitoring systems, with clearly assigned responsibility for verifying operability and initiating immediate corrective action if equipment was found offline. Screening protocols for public-spaces areas like the Clerk's Office would be outlined, including guidance on staff positioning, visual surveillance, and situational awareness. Finally, the checklist would establish communication and response procedures, such as predefined notification chains, CSO dispatch guidelines, and routine drills to reinforce readiness. By implementing these steps into daily courthouse operations, the checklist would close critical gaps and ensure swift, coordinated action in response to emerging threats.

Scenario 3 – Unarmed Attack from Inside the Courthouse

To address the failures observed during the January 26, 2024 incident, several enhancements have been incorporated into the courthouse security checklist. Weekly validation of watchlist integration with screening and access control systems ensures that barred individuals are automatically flagged at entry points. Monthly testing of alert protocols provides an added layer of verification, confirming that system-generated warnings are operational and escalated appropriately. To further strengthen personnel readiness, CSOs will conduct quarterly drills focused on identifying and managing individuals who are on the districts watchlist. Additionally, a weekly task confirms that updated watchlists are distributed in real time to all relevant screening personnel. To reinforce accountability, it is also recommended that a quarterly log of incidents involving prohibited individuals be maintained and reviewed jointly by USMS and court administration to identify procedural gaps. These measures, when implemented consistently, will close critical vulnerabilities and enhance the facility's ability to prevent similar breaches.

Scenario 4 – Armed Attack from within Courthouse:

Regarding addressing the February 2024 weapons incident, the checklist would require routine coordination and situational awareness briefings between CSOs, SSOs, and local law enforcement, ensuring all external posts were actively monitoring pedestrian behavior and identifying potential threats before they reached the building entrance. It would mandate procedures for observing and reporting individuals exhibiting suspicious or erratic behavior, especially when

visibly armed. Additionally, response protocols and escalation steps would be to established to swiftly mitigate the threat without further incident. Exterior surveillance zones and roving coverage would be regularly reviewed and verified to eliminate blind spots around the facility perimeter. Additionally, the checklist would include clear guidance on when to engage individuals outside the secure perimeter and how to coordinate timely intervention with local police. These steps, consistently implemented, would have enabled earlier detection, faster containment, and a more secure layered defense to prevent an armed individual from reaching courthouse doors.

Scenario 5 – Attack from Outside Courthouse:

To address the June 24, 2021 incident involving a disorderly individual throwing debris at the courthouse, the security checklist would have introduced several critical safeguards to prevent or mitigate the event. Routine perimeter surveillance checks and confirmation of live-monitoring readiness would have ensured that suspicious activity outside the facility was identified and escalated in real time. Regular inspections and reinforcement of entry point infrastructure would have reduced the building's vulnerability to impact and damage. In addition, the checklist's weekly verification of exterior patrol procedures and quarterly review of threat response protocols would have prompted earlier detection and intervention, especially if the individual had a prior history of loitering or disruptive behavior near the facility. Finally, clearly defined communication procedures between CSOs, court staff, and local law enforcement would have facilitated a more rapid and coordinated response, limiting the disruption and

physical damage. Together, these safeguards create a proactive, layered security posture that transforms early detection into immediate, effective action.

The scenarios above illustrate how the checklist can help mitigate issues previously reported in courthouse incident data. It was developed specifically to address the common patterns and systemic failures identified across these reports. While the checklist is not intended to solve every security challenge within judicial facilities, its primary purpose is to proactively uncover hidden vulnerabilities and guide actionable steps to reduce risk and enhance overall security posture. After all, you can't fix what you can't see.

4.6.1 Framework and Function

This document permits the adaptation of the courthouse security to evolve with the threat environment by simplifying security operations, increasing accountability, and risk reduction. By leveraging frameworks identified by the ISC, the checklist details how these requirements would break down across the varying areas of operation.

The objective of the checklist:

- Integrate best practices into daily operations
- Promote interagency collaboration through task assignment and scheduling
- Embed a mindset of resiliency into the operational setting to ensure tasks are consistently performed, audited, and improved.

The physical security domain protects the infrastructure both on the exterior and interior. The tasks include visually inspecting perimeter barriers, assessing the

reliability of alarm systems, and inspecting door locks. This is a critical component of courthouse security because, for example, if alarm testing isn't being conducted and cameras aren't being verified, operational threats can go undetected, leading to vulnerabilities in the system. This opens up the potential for a breach or other malicious behavior that may compromise the facility.

The access control domain ensures that screening protocols, access card management, and credentialing integrity measures are in place. Daily tasks include verifying that metal detectors and x-ray scanners are operational, conducting random secondary screenings for compliance, and verifying staff and contractors have credentials visible. Weekly audits of access card issuance and deactivation cycles are designed to reduce the risk of compromise and unauthorized access. For example, ensure that staff or interns who no longer work in the facility have turned in their access cards and their access to the facility has been disabled or restricted. This reduces the risk of an unauthorized access incident.

The communication domain ensures that courthouse personnel can respond quickly and efficiently during a crisis. Conducting daily radio checks and verification of emergency contact information preserves continuity during high-pressure scenarios. Weekly system tests confirm the operational reach of public address systems and incident notification tools. At the strategic level, monthly updates to Occupant Emergency Plan (OEP) and scheduled interagency tabletop exercises promote procedural synchronization among USMS, GSA, and court administration. These measures help correct the communication lapses observed in multiple SDNY incidents, particularly during medical and hazardous materials emergencies.

The threat detection domain is designed to identify and intervene as indicators of disruptive or potentially violent behavior arise. The checklist includes daily behavioral monitoring at entrances and within public spaces and consistent documentation of all disruptive events. Weekly briefings on the present climate and active threats promote situational awareness, while continuous training on threat indicators ensures that operational staff are up to speed in recognizing behavioral red flags. This approach addresses observed failures in managing courtroom disruptions and protest-related escalations, where unstandardized responses delayed appropriate interventions.

Finally, the procedural compliance domain focuses on protecting secured areas and reinforces compliance of procedures. Daily verification of dual-authentication protocols and random-access card compliance audits provide a defense against internal compromise. Weekly reviews of insider threat indicators and policy violations allow for corrections to be made prior to significant breaches occurring. Monthly briefings ensure that all staff receive updated training on SOPs, and evolving threat models. This category is relevant in mitigating risks associated with contractor access, after-hours activity in secured areas, and inconsistencies in access card management.

Each task within the checklist is assigned a frequency (daily, weekly, monthly) and a responsible party (e.g., USMS, GSA, court administration). The checkbox included ensures accountability and promotes usage. By assigning tasks to appropriate stakeholders who are familiar with vulnerabilities makes this document the backbone to ensure routine maintenance is performed, incident responses are timely, and stakeholders are coordinating accordingly.

4.6.2 Checklist User Guide and Implementation Protocol

Table 10 below, Checklist User Guide and Implementation Protocol, establishes the approach for incorporating into daily operations:

Table 10: Checklist User Guide and Implementation Protocol

Implementation Step	Description
Assign Checklist Coordinator	Designate a staff member or supervisor responsible for ensuring checklist completion and quality control.
Customize Role-Specific Tasks	Tailor tasks by agency or role (e.g., CSO, USMS, GSA) to ensure clarity and operational ownership.
Integrate with Daily Briefings	Review checklist items at the start of each shift to reinforce priorities and distribute responsibilities.
Establish Reporting Mechanisms	Ensure completed checklists are logged, submitted, and retained in a centralized repository for oversight.
Schedule Regular Review Cycles	Set intervals (e.g., quarterly) to review task relevance, revise outdated items, and address recurring gaps.
Incorporate Into Training and Drills	Use the checklist in emergency simulations, SOP reviews, and onboarding of new personnel.
Digitize for Auditability	Implement a digital version of the checklist for real-time use, timestamping, and accountability tracking.
Conduct Post-Incident Checklist Review	After major incidents, review checklist performance to assess compliance and identify required updates.

This user guide designates a coordinator for accountability and quality control. It customizes roles for stakeholders, clearly outlining their responsibilities. The checklist encourages daily briefings that cover priorities at the start of each shift to be conducted to reinforce the use of checklists. It creates a standard for logging those completed and maintaining them for oversight. The checklist should regularly be reviewed (i.e., quarterly, semiannually, or annually) to remain current and revise outdated items. Additionally, it should be implemented into training to promote collaboration.

Digitization also allows for real-time monitoring, time stamping, and performance monitoring. Lastly, post-incident reviews should be conducted to assess compliance and identify areas needing improvement.

These implementation steps encourage a promotion feedback system that institutionalizes accountability, promotes coordination, and perpetuates the durability of operations far into the future for court safety and security.

4.7 Conclusion

The results and findings presented in this chapter illustrate the complexity of SDNY facilities and its vulnerabilities with security that urgently need to be addressed. To solve this problem a systematic approach is needed which is driven by data. The 1,273 security incidents that were reviewed displayed a recurring pattern that failure occurs not from a single act of neglect. The system failures exist due to poor communication and adherence to procedures. If communication improved and procedures were appropriately followed the damage caused by incidents would be significantly reduced.

This analysis defined five operational categories, fit each incident into an appropriate category, and identified gaps in the district’s security posture. These gaps were most prominent in areas involving infrastructure, such as emergency and facility equipment. The Ishikawa diagram, in collaboration with Reason’s Swiss Cheese model, traced these failures back to systemic functions that exist within the stakeholders' functionality, mainly that of poor coordination and planning.

In response to the results and findings, a prototype security checklist was developed to be used as a proactive measure to fight vulnerabilities from being exploited in federal courthouse settings. Additionally, a user guide is provided to aid in the implementation process to promote its daily use. This checklist could significantly minimize the threat landscape to judges, courthouse staff, and other tenants who occupy these facilities by addressing areas of weakness. Additionally, it supports public trust as visitors who frequent these buildings can be assured that they are safe while physically present in these facilities.

This research has addressed the thesis statement outlined in the introduction: "A comprehensive and operationally effective security checklist encompassing physical security measures, personnel protocols, procedural safeguards, and advanced technological solutions can be developed to address to enhance the security of federal courthouses and safeguard the judicial process". Further discussions are provided in Chapter 5 regarding the findings of this research. Additionally, research limitations and delimitations are addressed, along with opportunities for future research in judicial security and other fields associated with physical security.

Chapter 5: Discussion and Conclusions

This chapter summarizes the results from Chapter 4 of the relationship between courthouse security and systems engineering in the approach to enhancing security posture through a reduction in vulnerability exploitation. This research investigated the value of incident data and its impact on developing and constructing an organized stakeholder checklist for judicial security. It integrated theory and practical application in a tool driven by data results in an improved security posture.

The purpose of developing a checklist is to address vulnerabilities proactively. This specific version targets five specific areas of concern: infrastructure failures, behavioral and conduct-related risks, health and life safety emergencies, hazardous threats, and breaches in physical access control. These gap areas were identified by analyzing data of incident reports provided by CSOs and SSOs.

5.1 Conclusion

The results in Chapter 4 highlight that courthouse security is a system-level issue. We must look beyond access controls, physical barriers, and security personnel to protect these facilities. Each Stakeholders must collaborate and work together. Procedures must align to ensure roles and responsibilities are known and understood. Analysis of SDNY incident data show that security failures did not occur due to a single point breakdown. The root causes were poor communication, unclear roles, and inconsistent following of procedures. Using gap analysis tools such as the Ishikawa diagram and Reason's Swiss Cheese model, this research mapped incidents across five core categories: infrastructure and systemic failures, critical health emergencies, behavioral disruptions, threat intelligence gaps, and physical security breaches. Each category exhibits patterns of

recurrence. Infrastructure and health-related incidents account for approximately 50% of the total reports identify the fragility of operational integrity and emergency readiness.

The categorization helped shape the courthouse security checklist's content, design, and structure. For example, creating consistent procedures can address recurring problems such as unauthorized access, a problem caused by poor practices and unclear policies. Similarly, consistent maintenance and upkeep of equipment are necessary to address malfunctions. Equipment malfunctions are being caused by poor maintenance practices and a mindset that it's better to wait for it to fail than to preemptively address foreshadowing issues. This approach permits the checklist to be a dynamic tool and a corrective framework, mapping the most vulnerable areas into operational checkpoints corresponding with all stakeholder responsibilities.

Another identified discrepancy is the under-reporting and inconsistent reporting practices of incidents. In doing so, this exposes a greater threat because inconsistent reporting practices ensure that threats and vulnerabilities remain hidden. Using the SDNY dataset built, the checklist development process demonstrates how empirical incident tracking can generate structured safeguards, institutional memory, and a foundation for continuous improvement.

In summary, incident information is important, not only to identify what has failed but to identify misalignments. An unfixed misalignment can turn a small incident into a large, or even catastrophic, event. Using data to identify vulnerabilities mitigates risk by closing gaps in security postures through the correction of misalignments. The prototype checklist designed through this research integrates coordination, communication, and accountability amongst stakeholders with vested interest in judicial

security. In doing so, an anticipatory and responsive environment ins established which helps promote a culture of readiness.

5.2 Contributions to Body of Knowledge

Below are the contributions of this praxis to the body of knowledge of facility security:

- Systems engineering lens: This provides an empirical and engineering focus on federal courthouse security based on incident data. Previous research has addressed courthouse security from legal, policy, or architectural perspectives. This research has introduced a systems engineering framework that operationalizes security as a function of people, processes, technologies, and environments.
- Checklist methodology advancement: The research applies a checklist to the domain of judicial security. Through the exploration of the complexity and constraints found in a courthouse environment, this study demonstrated how a checklist can align each interdependent stakeholder and improve the reliability of security operations. With this, the gap has been bridged through existing literature on organizational practices in securing facilities responsible for the judicial process.
- Mixed Methods Risk Modeling: The study contributes a methodology that integrated structured data into a risk model pipeline. It shows how incident reports, when cleaned, coded, and analyzed using root cause methods, can provide insight into vulnerabilities than structured data alone. This reinforces the value of qualitative data and mixed methods approaches in safety-critical environments, particularly where underreporting and siloed information flow are prevalent.

- Interdisciplinary Design for Risk Governance: This research highlights interdisciplinary design thinking in institutional risk governance. The checklist developed is a byproduct of stakeholder technical information. The success (or failure) of the checklist will reflect the stakeholders participation.

These contributions make the research a unique and practical addition to academic and operational literature on physical security and public sector resilience.

5.3 Limitations and Delimitations

Despite the methodological approach, several limitations were found that must be acknowledged.

5.3.1 Limitations

The following were identified during the research:

- Geographic and Institutional Scope: The data used to conduct root cause analysis and guide checklist development were drawn exclusively from the Southern District of New York (SDNY). SDNY represents one of the highest profile federal judicial districts in the United States; however, it does not capture the diverse operational conditions found in the other 93 districts. Each district operates with its own administrative customs, personnel allocations, facility infrastructure, and interagency relationships, resulting in 94 distinct operational models. Consequently, certain checklist components derived from the SDNY context may require an adjustment based on the needs of other districts.
- Data Completeness and Underreporting: It is suggested that incident reporting is inconsistent and incomplete. Analyzing the dataset suggests that minor incidents

or those perceived as routine may go undocumented. This will create a potential issue during the root cause analysis phase. Underreporting reduces the accuracy of risk profiles and may result in omission of key details needed for checklist development. Although efforts were made to clean, standardize, and categorize the available records, the accuracy of findings remains contingent on the quality and comprehensiveness of the original reporting. Additionally, the amount of available data appeared to be small compared to what was expect based on the districts profile.

- Institutional Dynamics: The dynamics of the institution were acknowledged but fell outside the analytic scope of this research. These dynamics include localized judicial orders, legal liability concerns, and courthouse specific procedural requirements. These factors may influence the practicality, adoption, and the interpretation of necessary checklist protocols. Similarly, the study did not formally assess institutional culture or interagency political dynamics. Other environments that implement this approach could vary due to leadership, institutional history, and trust among stakeholders.

5.3.2 Delimitations

The following delimitations address the limitations found in the research:

- Site specific: This research intentionally concentrated on federal courthouses and the interagency ecosystem (i.e., local representatives of the USMS, GSA, and court administrative personnel) found in the SDNY. The framework of other municipalities (i.e., international, local, and state courts) was purposefully

excluded to maintain operational focus on the distinct mandates and responsibilities that define federal courthouses.

- Human-based checklist intervention model: This model does not include alternative frameworks (i.e., AI-driven surveillance systems or fully automated incident response platforms) to establish a premise for a human-centered checklist. This enhances transparency, adaptability, and practical use in high-profile settings where coordination and decision-making are critical.
- Prioritization of incident analysis: The research focused on analyzing incident data created from observed behaviors. This permits a periodic review (e.g. quarterly, bi-annually, or annually) of procedures and the identification of vulnerabilities. However, it may have limited the ability to capture the cultural, interpersonal, or informal practices that influence security behavior.

5.4 Policy and Future Research Recommendations

Below are recommendations to develop policies and encourage future research based on the findings and observed limitations.

5.4.1 Policy Recommendations

The policy recommendations are as follows:

- Incorporate interagency checklist-based protocols: Federal courthouse security protocols should incorporate checklist methodologies into agency SOPs. This integration should include USMS, GSA, and AOUSC. Each entity should be mandated to use checklists for improved accountability and operational continuity.

- Develop stakeholder MOUs: All agencies serving federal courthouses should be required to develop or update MOUs that clearly define jurisdictional responsibilities, communication protocols, and checklist compliance expectations.
- Mandate incident reporting and root cause analysis standards: Congress or the AOUSC should support legislation or administrative guidance requiring all federal courthouse incidents to be reported using standardized formats. The courts should be encouraged or required to apply structured root cause analysis tools to all reportable events, feeding back into checklist updates.
- Establishment of a National Judicial Security Data Repository: A centralized repository for courthouse security data should be established to identify trend analysis, benchmark development, and proactive risk modeling. The AOUSC could administer the repository in collaboration with DHS and DOJ to promote data-driven policymaking and oversight.

5.4.2 Future Research Directions

Below are suggestions for research that can expand on this topic:

- Evaluation of checklist effectiveness: Future research should assess the long-term effectiveness of the checklist, using measurable outcomes such as identifying trends of occurrences (i.e., an increase in emergency response times and an audit of checklist compliance). These measures will build a claim for overall effectiveness.
- Expansion to other judicial and civic facilities: Future research should test the applicability of this checklist framework in other critical infrastructure environments (i.e., state courthouses, municipal buildings, and correctional

facilities). These studies could help identify sector-specific modifications while reinforcing shared best practices.

- Integration with emerging technologies: Future research should explore how checklist protocols can integrate the evolution of technology (e.g., AI-assisted detection systems and digital platforms). These studies should examine how to balance automation with human oversight and how to avoid checklist fatigue in tech-saturated environments.
- Cultural and behavioral dynamics in checklist adoption: Further research is needed on the organizational psychology of checklist adoption (i.e., law enforcement, national security, or regulatory oversight). These studies could investigate factors, training models, and leadership practices that influence uptake and sustainability.
- Cross-sector learning models: Future research should continue to draw from lessons learned in sectors that focus on safety (i.e., healthcare, aviation, and military operations) to refine checklist design principles and implementation strategies. These studies should compare checklist adoption across like industries that could illuminate success factors.

References

Aghajan, H., & Cavallaro, A. (2009). *Multi-camera networks: Principles and applications*. Academic Press.

Aldridge. (2023, October 13). *Safeguarding your business: The power of third-party security audits*. Aldridge. Retrieved from https://aldridge.com/the-power-of-third-party-security-audits/

Baehler, K., & Somerlot, B. (2005). Weapons, threats, and aggression in our courthouses: Courthouse violence in the 21st century. *Journal of Court Security, 1*(1), 15–24.

Bailey, J. F. (2023). Action to ensure that all judges act without fear of personal attack. *Judges' Journal, 62*(3), 21.

Barrett, J. H. (2009). *Protecting court: A practitioner's guide to court security*. Mill City Press.

Biringer, B. E., Vugrin, E. D., & Warren, D. E. (2013). *Critical infrastructure system security and resilience*. CRC Press.

Blankstein, A., Collins, B., & Zadrozny, B. (2020). Airman charged with killing federal officer during George Floyd protests in California. *NBC News*. Retrieved from: https://www.nbcnews.com/news/us-news/airman-charged-killing-federal-officer-during-george-floyd-protests-california-n1231187

Botelho, G., McLaughlin, E. C., & Hanna, J. (2014, June 6). Forsyth County, Georgia, courthouse shooting leaves deputy injured as gunman is killed. *CNN*. Retrieved July 12, 2025, from https://www.cnn.com/2014/06/06/justice/georgia-courthouse-shooting

Botezatu, C., Petrișor, A., & Iacob, A. (2019). Applying Ishikawa diagram in quality improvement. *Journal of Engineering Studies and Research, 25*(1), 7–11.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1–12.

Campbell, A. M., Hicks, R. A., Thompson, S. L., & Wiehe, S. E. (2020). Characteristics of intimate partner violence incidents and the environments in which they occur: Victim reports to responding law enforcement officers. *Journal of Interpersonal Violence, 35*(13–14), 2583–2606.

Campbell, C. F., & Reinkensmeyer, M. W. (2007). The court security challenge: A judicial leadership perspective. *Justice System Journal, 28*(1), 49–54.

CBS News. (2011, December 16). *Court shooter's attorney came to victims' aid*. CBS News. Retrieved July 12, 2025, from https://www.cbsnews.com/news/court-shooters-attorney-came-to-victims-aid/

Chan, Y., Lee, M., & Wong, K. (2024). Real-time AI detection of medication errors using wearable cameras. *Journal of Medical Systems, 48*(1), 12–25.

Clark, D. S. (2014). *The implications of ineffective courthouse security procedures in American courthouses: Revising courtroom security* [Master's thesis, University of Wisconsin]. MINDS@UW. https://minds.wisconsin.edu/bitstream/handle/1793/73573/Clark,%20David.pdf?sequence=1

Cole, E., & Ring, S. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Elsevier.

Comfort, L. K., Boin, A., & Demchak, C. C. (2010). *Designing resilience: Preparing for extreme events*. University of Pittsburgh Press.

Coole, M., Brooks, D. J., & Treagust, D. (2015). The physical security professional: Formulating a novel body of knowledge. *Journal of Applied Security Research, 10*(3), 385–410.

Cooper, J. B., Newbower, R. S., & Kitz, R. J. (1984). An analysis of major errors and equipment failures in anesthesia management: Considerations for prevention and detection. *Anesthesiology, 60*(1), 34–42.

Corley, W. G., Sr., M. A., Sozen, M. A., & Thornton, C. H. (1998). The Oklahoma City bombing: Summary and recommendations for multihazard mitigation. *Journal of Performance of Constructed Facilities, 12*(3), 100–112.

Cybersecurity and Infrastructure Security Agency. (2025). *Interagency Security Committee (ISC)*. U.S. Department of Homeland Security. Retrieved from: https://www.cisa.gov/resources-tools/groups/interagency-security-committee-isc

Dow, C. (2007). Citizens have a right to safety in the courthouse. *Justice System Journal, 28*(1), 36–V.

Dunlap, D., Smith, J., & Taylor, L. (2017). Integrated security systems: A holistic approach to facility protection. *Security Management Journal, 33*(4), 45–52.

Emmons, S., Hamilton, L., & Zhang, T. (2018). Bias-resilient risk assessment in aerospace decision-making. *Aerospace Safety Review, 32*(2), 45–58.

Fautsko, T. F., Hamrick, J. L., & Courtright, R. (2013). *Courthouse security incidents trending upward: The challenges and responsibilities*. National Center for State Courts.

Fautsko, T. F., & Berson, S. V. (2013b). *Courthouse violence in 2010–2012*. Retrieved from: https://www.txcourts.gov/media/1441934/courthouseviolence-in-2010-2012.pdf

Federal Bureau of Investigation. (2024). *National Incident-Based Reporting System (NIBRS)*. Retrieved from: https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/ucr/nibrs

Federal Bureau of Investigation. (n.d.). *Judge Vance murder*. Retrieved from: https://www.fbi.gov/history/famous-cases/judge-vance-murder

Federal Emergency Management Agency. (2013). *Threat and hazard identification and risk assessment (THIRA) guide: Comprehensive Preparedness Guide (CPG) 201* (2nd ed.).

Federal Emergency Management Agency. (2017). *National Incident Management System* (3rd ed.). U.S. Department of Homeland Security. Retrieved from: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

Garcia, M. L. (2007). *Design and evaluation of physical protection systems* (2nd ed.). Butterworth-Heinemann.

Gartlehner, G., Patel, S., & King, V. (2017). Clarity in visualization: Evaluating fishbone diagrams in healthcare. *Health Information Management Journal, 46*(1), 16–23.

Gartlehner, G., Schultes, M. T., Titscher, V., Morgan, L. C., Bobashev, G. V., Williams, P., & West, S. L. (2017). User testing of an adaptation of fishbone diagrams to depict results of systematic reviews. *BMC Medical Research Methodology, 17*, 1–9.

Gawande, A. (2010). *The checklist manifesto: How to get things right*. Metropolitan Books.

Gordon, L. M., & Garrie, D. B. (2020). *Cybersecurity & the courthouse: Safeguarding the judicial process*. Wolters Kluwer.

Gould, J. B. (2007). Security at what cost? A comparative evaluation of increased court security. *Justice System Journal, 28*(1), 62–78.

Government of Oklahoma. (n.d.). *Oklahoma City Bombing After Action Report*. Oklahoma Department of Emergency Management. Retrieved from: https://oklahoma.gov/content/dam/ok/en/oem/documents/bombing-after-action-report.pdf

Green, J. (2012). From NASA to the ICU: How aerospace checklists saved lives in medicine. *Journal of Patient Safety, 8*(4), 159–164.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider threats in cyber security* (pp. 85–113). Springer.

Hales, B., Terblanche, M., Fowler, R., & Sibbald, W. (2008). Development of medical checklists for improved quality of patient care. *International Journal for Quality in Health Care, 20*(1), 22–30.

Harris, W., & Sadok, M. (2024). How do professionals assess security risks in practice? An exploratory study. *Security Journal, 37*(3), 671–685.

Hidalgo, J. (2020, January 7). Judge Chuck Weller, shot by angry pawn shop owner in 2006, decides to retire. *Reno Gazette-*

Journal. https://www.rgj.com/story/news/politics/2020/01/07/reno-judge-shot-angry-defendant-2006-retire/2834206001/

Hogan, C., & Madeira Jr., E. W. (2015). The bar joins the battle for secure courts: The SecureCourts Initiative. *Judges' Journal, 54*, 29.

Inada, N., Koyama, T., Inokuchi, E., Kuroda, M., & Kamio, Y. (2011). Reliability and validity of the Japanese version of the Modified Checklist for Autism in Toddlers (M-CHAT). *Research in Autism Spectrum Disorders, 5*(1), 330–336.

Inada, T., Fujita, Y., & Takahashi, M. (2011). Pointing and calling: Enhancing reliability in industrial operations. *Safety Science, 49*(5), 731–736.

Interagency Security Committee. (2019). *Armed contract security officers in federal facilities: An Interagency Security Committee best practice* (Rev. 2). U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Interagency Security Committee. (2020). *Facility access control: An Interagency Security Committee best practice*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Interagency Security Committee. (2022). *Security convergence: Achieving integrated security*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Interagency Security Committee. (2024). *ISC compliance policy and compliance benchmarks*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Interagency Security Committee. (2024). *Occupant emergency programs: An Interagency Security Committee guide*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Interagency Security Committee. (2024). *The risk management process: An Interagency Security Committee standard*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Ishikawa, K. (1985). *What is total quality control? The Japanese way*. Prentice Hall.

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Iris recognition. In *Introduction to biometrics* (pp. 141–174). Springer.

Jefferson, K. K., & Crane, V. S. (1986). Effectiveness checklist: How to achieve results. *Journal of Pharmacy Technology, 2*(3), 136–139.

Jesmore, K. L. (1973). The courthouse search. *UCLA Law Review, 21*, 797.

Johanning, K., Krogh, B., & Sujan, M. A. (2014). Validation of checklist-based compliance for pharmaceutical IT. *Pharmaceutical Engineering, 34*(6), 23–31.

Johnston, B. (2023). *Cyber-securing US critical infrastructure: The Colonial Pipeline attack and what can be done to protect our pipeline system*.

Jones, T. L. (2003). *Court security: A guide for post 9–11 environments*. Charles C Thomas Publisher.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11–27.

Kapucu, N., & Garayev, V. (2011). Collaborative decision-making in emergency and disaster management. *International Journal of Public Administration, 34*(6), 366–375.

Keller, J., Thompson, R., & Davis, M. (2019). Red teaming: Enhancing organizational security through adversarial testing. *Cybersecurity Review, 7*(1), 23–35.

Kelly, M. (1998). Domestic violence and guns: Seizing weapons before the court has made a finding of abuse. *Vermont Law Review, 23*, 349.

Kimble, J. (2020). Safeguarding courts. *Judicature, 104*(3), 38–39.

Kodate, N., Taneda, K. I., Yumoto, A., & Kawakami, N. (2022). How do healthcare practitioners use incident data to improve patient safety in Japan? A qualitative study. *BMC Health Services Research, 22*(1), 241.

KOMO News Staff. (2014, November 7). Grays Harbor man found guilty of assault in 2012 courthouse attack. *KOMO News*. https://komonews.com/news/local/grays-harbor-man-found-guilty-of-assault-in-2012-courthouse-attack

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143–154.

Kruczkiewicz, A., Klopp, J., Fisher, J., Mason, S., McClain, S., Sheekh, N. M., Moss, R., Parks, R. M., & Braneon, C. (2021). Opinion: Compound risks and complex emergencies require new approaches to preparedness. *Proceedings of the National Academy of Sciences, 118*(19), e2106795118.

Kuo, Y. H., Lai, H. J., & Lin, Y. C. (2015). Development of an MSD risk checklist in hotel housekeeping. *Applied Ergonomics, 47*, 138–145.

Loader, I., Goold, B., & Thumala, A. (2015). Grudge spending: The interplay between markets and culture in the purchase of security. *The Sociological Review, 63*, 858–875.

Lovallo, D., & Kahneman, D. (2003, July). Delusions of success: How optimism undermines executives' decisions. *Harvard Business Review, 81*(7), 56–63.

Macrae, C. (2016). The problem with incident reporting. *BMJ Quality & Safety, 25*(2), 71–75.

Mahajan, R. P. (2010). Critical incident reporting and learning. *British Journal of Anaesthesia, 105*(1), 69–75.

Mallery, J. (2013). Building a secure organization. In J. Vacca (Ed.), *Computer and information security handbook* (pp. 3–24). Morgan Kaufmann.

Marotta, L., & Madnick, S. (2023). Reporting inconsistency in cybersecurity: Terminology and timeliness. *Journal of Cybersecurity, 9*(1), 1–14.

Masys, A. J. (2012). Black swans to grey swans: Revealing the uncertainty. *Disaster Prevention and Management: An International Journal, 21*(3), 320–335.

McMillion, B. J. (2023). *Potential implications of changes in federal courthouse security* (CRS Report No. IN12143). Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN12143

Mendoza, M. (2024, May 9). Woody Harrelson's father took on hitman work to kill San Antonio judge John H. Wood Jr. *San Antonio Express News*. https://www.mysanantonio.com/entertainment/article/charles-harrelson-san-antonio-judge-murder-woody-16217573.php

Moghaddam, F. M. (2010). *The new global insecurity: How terrorism, environmental collapse, economic inequalities, and resource shortages are changing our world*. Bloomsbury Publishing USA.

Mora, M., & Keipi, K. (2006). *Disaster risk management in Latin America: The role of checklists in development policy*(IDB Working Paper). Inter-American Development Bank.

Morali, A., Wieringa, R., & Etalle, S. (2009). A pragmatic and formal approach to checklists in telecom security. *Computers & Security, 28*(3–4), 136–150.

National Institute of Standards and Technology. (2022). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). U.S. Department of Commerce.

National Research Council. (2007). *Protecting people and buildings from terrorism: Technology transfer for blast-effects mitigation*. The National Academies Press.

NBC News. (March 9, 2015). Dramatic shootout outside Tulsa courthouse. *NBC News*.

New York State Division of Criminal Justice Services, Office of Justice Statistics and Analysis. (2021). *Use of force incidents final report*. Retrieved from: https://www.criminaljustice.ny.gov/crimnet/ojsa/use-of-force-report-2021.pdf

Novak, L. (2003). Federal courts adapt for maximum security. *Judges' Journal, 42*, 22.

Palazzolo, J. (September 14, 2011). Gunman who fired assault rifle in Ark. courthouse may have targeted judge in his divorce case. *ABA Journal*. Retrieved from: https://www.abajournal.com/news/article/gunman_who_fired_assault_rifle_in_ark_courthouse_may_have_targeted_judge

Parada-Valdes, L. (2011). The effects of intrusiveness on protective details. *Journal of Applied Security Research, 6*(2), 209–246.

Pei, X., Zhang, Y., & Liu, H. (2018). Iterative testing and feedback loops in dynamic defense systems. *Journal of Security Engineering, 12*(2), 89–102.

Phimister, J. R., Oktem, U., Kleindorfer, P. R., & Kunreuther, H. (2003). Near-miss incident management in the chemical process industry. *Risk Analysis: An International Journal, 23*(3), 445–459.

Psarros, G., Skjong, R., & Eide, M. S. (2010). Underreporting of maritime accidents. *Safety Science, 48*(6), 739–751.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

Purpura, P. (2007). *Security and loss prevention: An introduction*. Elsevier.

Reese, S. (2008, May). *The Federal Protective Service and contract security guards: A statutory history and current status*. Congressional Research Service, Library of Congress.

Reese, S. (2014). *Federal building and facility security: Frequently asked questions*. Congressional Research Service. Retrieved from: https://www.congress.gov/crs-product/R43570

Resnik, J. (2012). Building the federal judiciary (literally and legally): The monuments of Chief Justices Taft, Warren, and Rehnquist. *Indiana Law Journal, 87*, 823.

Rosenblatt, P. G. (2013). Judge John M. Roll: An oral history. *Western Legal History, 26*, 161–174.

Hoyland, A. and Rausand, M. (1994). *System Reliability Theory: Models and Statistical Methods*, Wiley, New York, NY.

Santos, P., & Ferreira, C. (2023). Cyber incident reporting regulations: A literature review. *SN Computer Science, 4*(6), 468.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer.

Scott, B., & Krempley, M. (2012). SAFE and SECURE: A case study explores one federal agency's method to manage security and risk. *Quality Progress, 45*(1), 16.

Smith, C., & Brooks, D. J. (2012). *Security science: The theory and practice of security*. Butterworth-Heinemann.

Suh, Y. (2021). Sectoral patterns of accident process for occupational safety using narrative texts of OSHA database. *Safety Science, 142*, 105363.

Tong, L. H. (2008). *Judicial security: Responsibilities and current issues*. Congressional Research Service, Library of Congress. Retrieved from: https://www.everycrsreport.com/reports/RL33464.html

Tucker, L. A. (2011). Cameras at the Supreme Court: A rhetorical analysis. *Drexel University Earle Mack School of Law Research Paper* (2011-W), 02.

United States Courts. (n.d.). *Court role and structure*. U.S. Courts. Retrieved from: https://www.uscourts.gov/about-federal-courts/court-role-and-structure

United States Courts. (2024). *Anniversary of the federal court system*. U.S. Courts. Retrieved from: https://www.uscourts.gov/anniversary-federal-court-system

United States Department of Homeland Security. (2020). *Homeland Security Risk Assessment Lexicon*. Retrieved from: https://www.dhs.gov/publication/homeland-security-risk-assessment-lexicon

United States Department of Homeland Security. (2023). *Mission*. Retrieved from: https://www.dhs.gov/mission

United States Department of Homeland Security. (2024). *Building and infrastructure protection series: Designing buildings to withstand almost anything*. Retrieved from: https://www.dhs.gov/archive/building-and-infrastructure-protection-series-designing-buildings-withstand-almost-anything

United States Department of Homeland Security. (n.d.). *Creation of the Department of Homeland Security*. Retrieved from: https://www.dhs.gov/creation-department-homeland-security

United States General Services Administration. (2023). *Our mission's evolution*. Retrieved from: https://www.gsa.gov/about-us/mission-and-background/our-missions-evolution

United States General Services Administration. (2024). *Facilities standards for the public buildings service (P100)*. Retrieved from: https://www.gsa.gov/real-estate/design-and-construction/facilities-standards-for-the-public-buildings-service

United States Marshals Service. (2023). *Judicial security: FY 2024 congressional budget justification*. U.S. Department of Justice.

United States Marshals Service. (2024). *Judicial security fact sheet*. U.S. Department of Justice. Retrieved from: https://www.usmarshals.gov/sites/default/files/media/document/2024-Judicial-Security.pdf

United States Marshals Service. (2024). *Judicial security: Fiscal year 2024 congressional budget justification*. Retrieved from: https://www.usmarshals.gov/sites/default/files/media/document/Pub-2-2024-Annual-Report.pdf

United States Marshals Service. (n.d.). *About the U.S. Marshals*. Retrieved from: https://www.usmarshals.gov/who-we-are/about-us

Vincent, C., Burnett, S., & Carthey, J. (2014). Safety measurement and monitoring in healthcare: A framework to guide clinical teams and healthcare organisations in maintaining safety. *BMJ Quality & Safety, 23*(8), 670–677.

Wasby, S. L. (2007). National Association for Court Management. *Justice System Journal, 28*(1), 119.

Waugh, W. L., & Streib, G. (2006). Collaboration and leadership for effective emergency management. *Public Administration Review, 66*(s1), 131–140.

Weaver, S., Stewart, K., & Kay, L. (2021). Systems-based investigation of patient safety incidents. *Future Healthcare Journal, 8*(3), e593–e597.

Wilson, C., & Levinson, J. (2021, March 12). Protesters, federal officers clash outside Portland's courthouse Thursday. *OPB*. Retrieved from: https://www.opb.org/article/2021/03/12/protesters-vandalize-portlands-federal-courthouse-again/

Woodward, C. (2005, June 21). Man shot to death inside Seattle courthouse. *The Spokesman-Review*. Retrieved from: https://www.spokesman.com/stories/2005/jun/21/man-shot-to-death-inside-seattle-courthouse/

Wyss, G. D., Schrader, B. J., & Buehring, W. A. (2023). *Risk analysis and security countermeasure selection*. CRC Press.

Wyss, K., Kolbe, M., & Grande, B. (2023). Implementation of the WHO Surgical Safety Checklist: A multi-country evaluation. *Global Health Action, 16*(1), 1–12.

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy, 39*(10), 6100–6119.

Zaruba, J. E. (2007). Courthouse security: A direction or a destination? *Justice System Journal, 28*(1), 46–49.