Federal Voting Assistance Program (FVAP) Technology Projects

Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative

---

Prepared For:
Federal Voting Assistance Program

Department of Defense
4800 Mark Center Drive
Mailbox 10
Alexandria, VA 22350-5000

Prepared By:
CALIBRE
6354 Walker Lane, Suite 300
Metro Park
Alexandria, Virginia 22310-3252
www.calibresys.com

Contract No.:
GS-35F-5833H

[redacted]

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

CALIBRE
Our Success Follows Yours

COMPARATIVE RISK ANALYSIS OF THE CURRENT UOCAVA VOTING SYSTEM AND AN ELECTRONIC ALTERNATIVE

CONTRACT # GS-35F-5833H

Task # 2.4.4

Final Report

Version # 7
28 February 2013

[redacted]

Executive Summary

The Federal Voting Assistance Program (FVAP) is investigating the risks associated with different voting systems in advance of a Congressionally-mandated requirement for an online voting demonstration project, and to ensure that U.S. citizens and uniformed services personnel living overseas are able to cast their votes securely and accurately.

The potential risks associated with electronic (internet) voting have been intensely debated. However, the risks associated with the current postal-based absentee voting system have never been comprehensively examined nor have the risks associated with these two systems been systematically and quantitatively compared.

This report presents the first systematic risk analysis of the current UOCAVA by-mail voting system with an electronic alternative. It offers a baseline and a reference for future comparative analysis and an original analysis framework allowing quantitative comparison with other voting systems to be evaluated during the research and development phase of the mandated demonstration project.

Aside from the quantitative results discussed in this report and summarized below, the risk analysis framework provides FVAP with:

- A dynamic tool for the evaluation of any voting system of interest.
- A threat tree architecture amenable to high level comparison of risks between voting systems.
- A means to perform individual in-depth analysis of components within voting systems, e.g. the comparison of risks between the "absentee ballot delivery" and "marked ballot return" steps within the current UOCAVA voting system.

This report presents a framework for the quantitative comparison of risks across different voting scenarios. By using a risk analysis centered on a threat tree approach, and dividing the voting process into elemental voting steps, it allows for the side-by-side comparison of voting systems, whether physical (paper ballot transmitted through postal mail) or digital (Web interface with transmission of election materials via the Internet). This comparative risk analysis framework aims to provide FVAP, from a proof-of-concept perspective, with a tool for quantitative and comparative risk analysis across voting scenarios as a foundation for conducting the mandated demonstration project.

Due to the originality of the risk analysis framework and the preliminary nature of this initial risk analysis, the results derived from the work presented in this report should not be construed as conclusive statements, but rather observations drawing the potential towards such conclusions. These observations are detailed below:

Risk Analysis of Voting Systems

- Voting systems can be defined through a specific system architecture and a common voting process adapted to that architecture.
- A threat tree approach can be used to assess voting system risks once both system and process have been defined.
- Systematic and side-by-side comparison of risks across voting systems requires a common analysis framework.
- The risk analysis framework is validated by the concurrence of the risk outputs with empirical observations from the information security and election communities.

Risk Analysis of the Current UOCAVA Voting System

- Unintentional errors constitute the greatest source of risk, as compared to intentional malicious attacks or accidental disruptions.
- Errors at the voter's location appear most preeminent, especially during the physical marking of the absentee ballot by the voter.

Risk Analysis of the Remote Electronic Absentee Voting System

- Unintentional human errors and architecture-specific threats by malicious outsiders (e.g. denial of service) constitute the greatest source of risk.
- Conversely, insider attacks for this architecture yield a risk estimate fifty percent lower than the risk estimate for outsider attacks.

Quantitative Comparison of Risks across Voting Systems

- The current UOCAVA voting system appears to exhibit a greater risk from unintentional errors, while its electronic counterpart is equally subjected to attacks and errors.
- Security objectives are more affected by attacks in the context of the remote absentee voting system, and by errors in the context of the current UOCAVA voting system.
- Overall, the remote electronic absentee voting system and the current UOCAVA voting system exhibit similar risks, from a statistical standpoint.

With regards to the risk analysis framework, the following recommendations are made:

- This tool should be further validated and optimized by a wider panel of election and security experts to ensure that its outputs reflect the diverse opinions of the election community at large.
- This tool can and should be continuously updated with any new relevant threat-vulnerability pairings upon discovery.

Due to the diverse landscape of risk modeling, the following precautions should be used when using the risk analysis framework:

- Risk estimates must be used in the context of a defined risk management strategy.
- Risk estimates should not be compared to other estimates from different models.
- Risk estimates are dependent on the panel's expertise.

In light of the pending pilot demonstration project mandated by Congress, the following recommendations are made regarding the use of this tool as a first step in a risk management strategy crucial to a successful pilot deployment:

1. The current threat tree architecture presented in this report should be used for high level comparison of risks between pilot and demonstration project proposed systems and the current UOCAVA by-mail voting system. This comparison will provide a first level of selection across voting system native architectures.
2. Upon refinement of the voting system architectures, individual in-depth analyses of these systems should be performed using this tool by refining the threat tree and procuring specialized expert inputs relevant to the system's component under scrutiny. Such individual analyses will assist FVAP in assessing the risks associated with vulnerability-threat pairings specific to a particular component or subsystem and guiding the design of a voting system's architecture with the least residual risk.
3. Once a voting system architecture has been finalized, the risks associated with the selected pilot system should be compared to the baseline risks of the current by-mail voting system to assist FVAP in the design of a coherent and tailored mitigation strategy for any future pilots of the electronic voting demonstration project.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

Under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA[1]) of 1986, the Federal Voting Assistance Program (FVAP) assists active duty uniformed service members, their families, and United States citizens residing outside the United States in exercising their right to vote by absentee ballot when they are away from their permanent address. FVAP administers this law on behalf of the Secretary of Defense and works cooperatively with other federal agencies and state and local election officials to carry out its provisions to assist UOCAVA voters.

UOCAVA legislation was enacted before the advent of today's global electronic communications technology. At that time, the absentee voting system relied exclusively on U.S. domestic and military mail systems, as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s, it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA citizens, thus preventing them from successfully exercising their right to vote. This disenfranchisement has the potential to alter the outcomes of elections, especially in close races, as observed during the 2000 Presidential election in Florida.

Understanding inherent barriers in the current UOCAVA voting system and developing remediating solutions are key elements in the assistance FVAP provides to the UOCAVA population. As businesses, governments and the general public widely adopted the Internet for a variety of communication and data transfer services. FVAP and the states began to consider the potential of electronic communication as an alternative to the "by-mail" UOCAVA voting system.

The National Defense Authorization Act (NDAA) of 2002[2] required FVAP to carry out an electronic voting demonstration project in the 2002 or 2004 general elections, using a statistically significant number of absent uniformed services voters. The 2005 NDAA[3] amended this mandate, allowing FVAP to delay the implementation of the demonstration project until the U.S. Election Assistance Commission (EAC) had established electronic absentee voting guidelines and certified that it would assist FVAP in carrying out the project. In 2009, Congress passed the Uniformed and Overseas Voters Empowerment (MOVE[4]) Act, authorizing FVAP to run pilot programs testing the ability of new or emerging technologies to better serve uniformed and overseas citizens during the voting process. The MOVE Act also mandated EAC and the

National Institute of Standards and Technology (NIST) provide FVAP with best practices or standards in accordance with electronic absentee voting guidelines to support the pilot programs.

As a result of this mandate, EAC and NIST have investigated the risks associated with electronic absentee voting, and especially the study of threats to the privacy, integrity, and auditability of the voting system. The EAC published a report on the electronic transmission of voting materials[5] in 2007, funded a research project – the Election Operations Assessment[6] – at the University of South Alabama in 2010, and published a *Survey of Internet Voting*[7] report in 2011. Since 1995, NIST has assisted federal agencies in implementing best practices in cybersecurity related to their information technology systems, and published many reports[8,9,10,11,12,13,14,15,16] to that effect. With regards to absentee voting, NIST has leveraged its information technology expertise to assist FVAP in evaluating security risks associated with electronic absentee voting, resulting in several UOCAVA-centric reports.[17,18,19,20,21] However, while many academic studies, federally-funded projects, and other efforts have been made to identify risks related to both the by-mail absentee voting system and electronic absentee voting propositions, no rigorous framework for the quantitative comparison of these risks has been introduced. As a result, the risks associated with the current UOCAVA voting system have not yet been quantitatively compared side-by-side to the risks associated with an electronic alternative.

1.2 Scope

This report aims at conducting a quantitative comparison of risks between the current UOCAVA voting system, as a baseline and reference system, and an electronic alternative system for the implementation of a remote electronic voting demonstration project, as mandated by Congress.

The full scope of this effort is intended to achieve five objectives, reflected in the following report outline, and illustrated in the workflow in Figure 1.1:

Chapter 2 Provide definitions related to voting and risk analysis.

Chapter 3 Provide a detailed methodology for the comparative and quantitative risk analysis of voting systems.

Chapter 4 Conduct individual quantitative risk analyses of the current UOCAVA by-mail voting system and an electronic absentee voting system.

Chapter 5 Conduct a quantitative comparison of the risks associated with the by-mail voting system and the electronic absentee voting system, using the comparative risk analysis framework.

Chapter 6 Provide conclusions and recommendations for comparative risk analysis and individual in-depth analysis of voting systems.

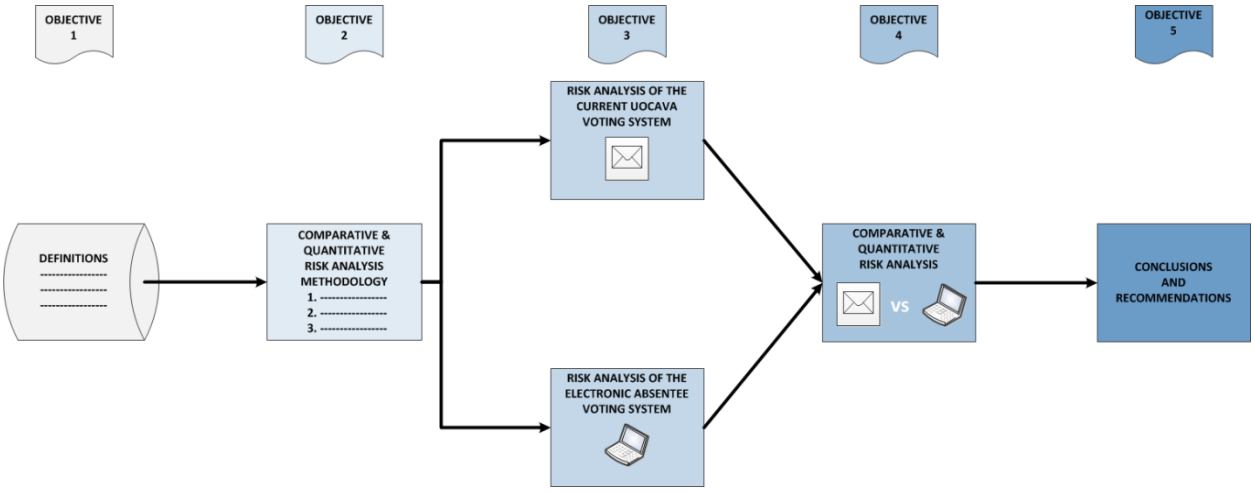


Figure 1.1: Comparative and Quantitative Risk Analysis Workflow

The analysis presented in this report is not intended to represent or resolve all potential risks associated with UOCAVA voting. Likewise, this report is not an endorsement of any one particular vendor's product or any specific technological solution, nor does it provide acquisition-level cost information. However, the comparative risk analysis framework presented in this report aims to provide FVAP, from a proof-of-concept perspective, with a tool for quantitative and comparative risk analysis across voting scenarios as a foundation for conducting the mandated demonstration project.

2 Definitions

For the purpose of this report, all voting definitions solely refer to absentee voting. Likewise, the only targeted voters in this analysis are absentee voters defined under the UOCAVA (Section 1.1).

2.1 Voting System

A voting system is defined as the combination of the following three voting-related elements organized in a specific voting architecture:

- A local election office element
- A transmission element
- A voter element

The architecture of a generic absentee voting system is illustrated in Figure 2.1 and organized as follows:

- The local election office (LEO) submits ballots and forms to the voter, and the voter communicates and submits ballots and forms to the LEO.
- A Voter Registration Database (VRDB) is used for voter registration and ballot request.
- The ballots and forms are transmitted between the LEO and the voter. Transmission may involve transport by road and air, and/or transport by electronic communication channels.

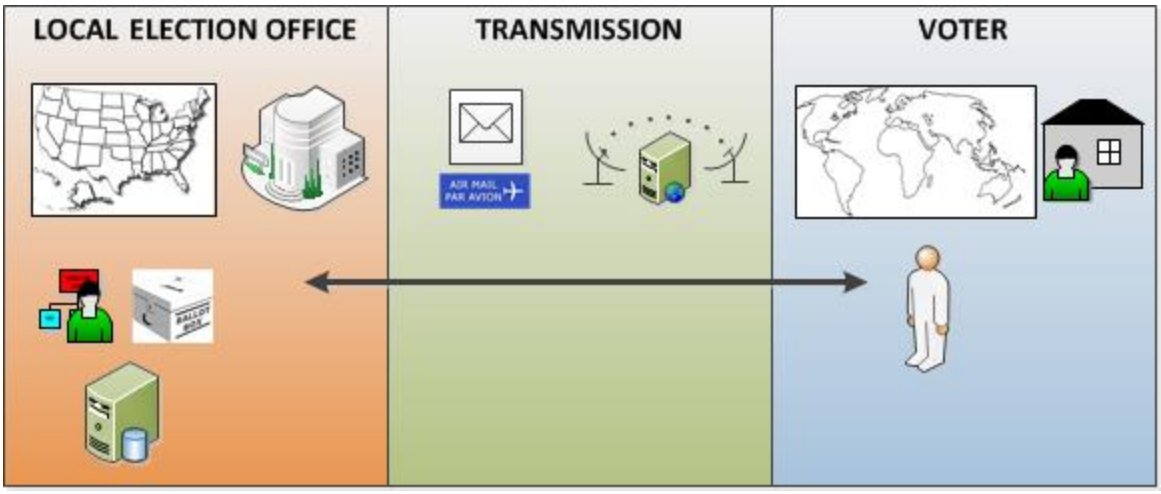


Figure 2.1: Generic Absentee Voting System

2.2 Voting Process

A voting process is defined as a series of actions carried out toward the specific aim of successfully casting a ballot. It is implemented within a voting system as described in Section 2.1.

While Article 1 Section 4 of the Constitution[22] states that the "*Times, Places and Manner of holding Elections for Senators and Representatives"* are prescribed by each individual state and not the federal legislature, most states' voting processes adhere to the following seven consecutive steps regardless of the voting system being used. These steps are hyperlinked to their detailed definition in Appendix A.

- Registration
- Absentee ballot request
- Absentee ballot delivery
- Ballot marking
- Marked ballot return
- Returned ballot processing, and tabulation which consists of the following:
  - receipt at the LEO
  - sorting
  - validation by precinct
  - formal acceptance
  - privacy separation
  - tabulation
  - adjudication
- Post-election audit

The voting process within a generic absentee voting system is illustrated in Figure 2.2.

All specific regulations and requirements related to the voting process in individual states can be found in the FVAP Voting Assistance Guide.[23]

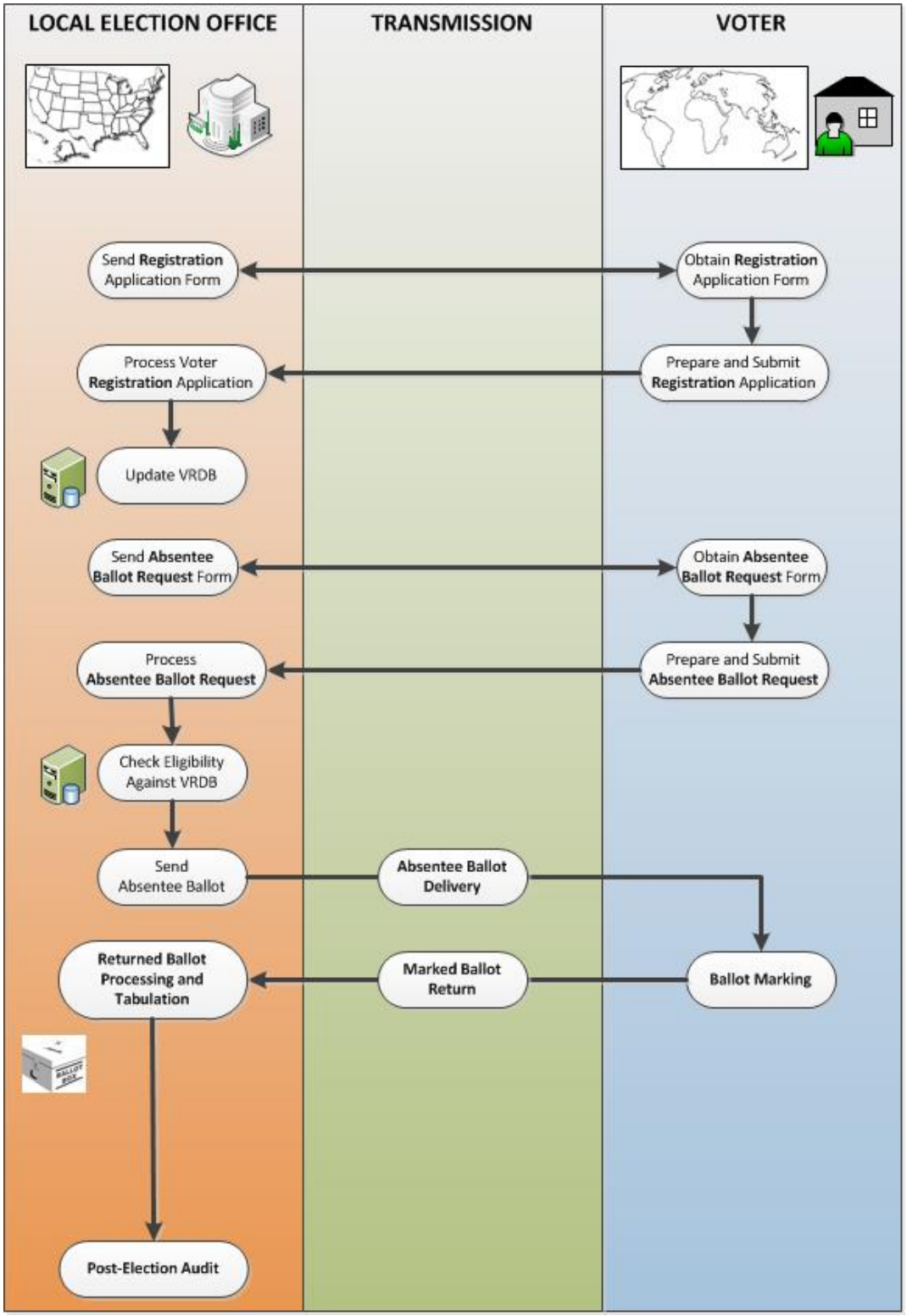


Figure 2.2: Voting Process Within a Generic Absentee Voting System

2.3 Voting Security Objectives

Throughout the voting process, the following six security objectives must be achieved to safeguard the voting system, and ensure fair, accurate and transparent elections, as illustrated in Figure 2.3:

- Authentication
- Vote secrecy
- Vote integrity
- Vote privacy
- Auditability
- Service availability

Detailed definitions of these terms are provided in Appendix A.

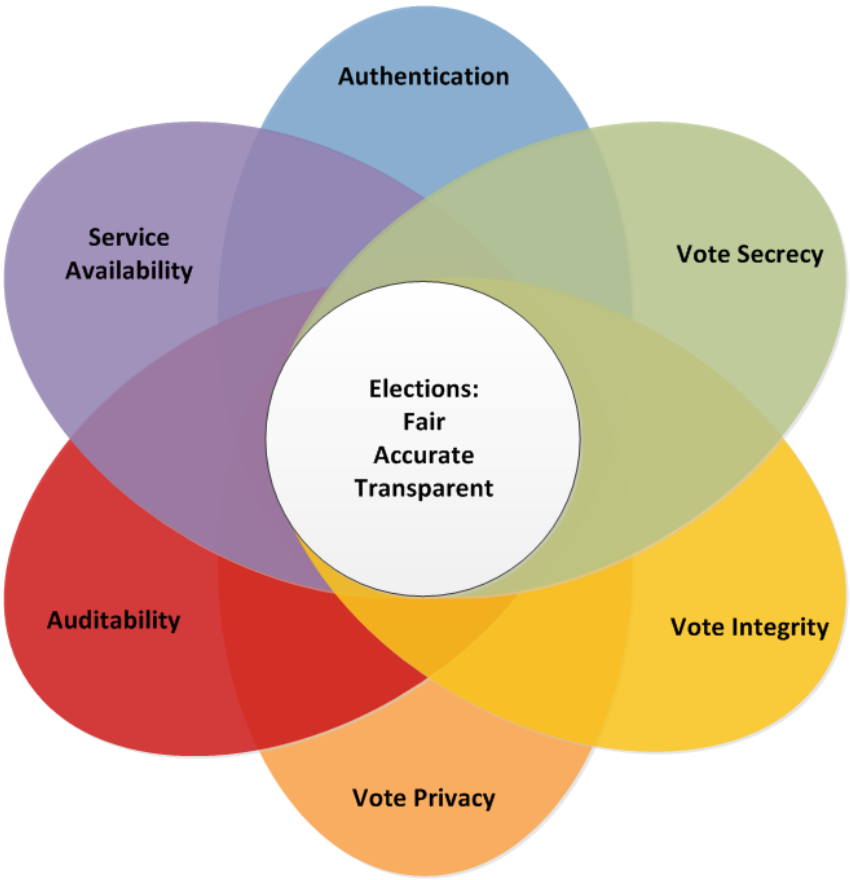


Figure 2.3: Voting Security Objectives

2.4 Voting-Related Risk

The terms "vulnerability," "threat," "attack," and "risk" tend to be used interchangeably in the literature and the voting community. In order to conduct an accurate risk analysis of a voting system, it is important to understand their specific meaning in the voting context.

Voting-related risk is defined as a function of the likelihood of a given threat vector acting upon an existing vulnerability by a threat agent, and the resulting impact on any or all parts of the voting system.[24]

For the purpose of clarity throughout the reports produced under this contract, and for consistency across voting scenarios, as described in Section 1.2, the definitions detailed in the National Information Assurance Glossary[25] of the Council on National Security Systems (CNSS) will be used, and adapted to the voting context. These definitions are detailed in Appendix A.

Figure 2.4 illustrates all the factors involved in quantifying voting-related risks and shows the interdependency of threat agents, threat vectors, and vulnerabilities resulting in potential impact to the voting system, as well as the existence of likelihood for a threat vector to be exercised by a threat agent on an existing voting system vulnerability. It also provides the following example:

In the context of the current UOCAVA voting system, a malicious Mobility Airman in the Air Mobility Command (threat agent, in red) destroys a bag of election mail containing marked ballots from overseas Armed Forces service members (the attack) by taking advantage of the lack of supervision and security around the election mail (the existing vulnerability of the voting system), thus affecting the marked ballot return step of the voting process, yielding a high impact level of compromise to the voting system.

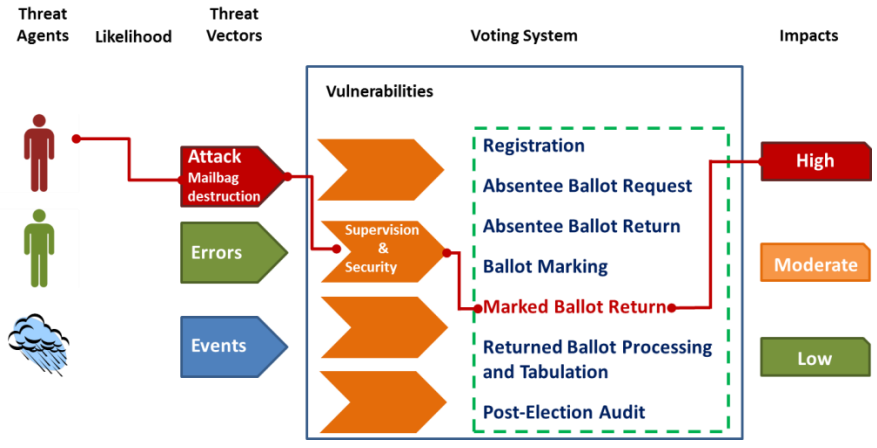


Figure 2.4: Illustration of the Factors Involved in Quantifying Voting Risk

3 Methodology

While many attempts have been made to evaluate the risks associated with electronic voting systems, little effort has been dedicated to quantitatively assess the risks of the by-mail voting system, and to systematically compare them with risks of other voting scenarios. The scope of this work requires a side-by-side comparison of risks across voting systems in a quantitative fashion. To that effect, an original framework was built for the comparative and quantitative risk analysis, hereafter referred as the framework. It was crafted to encompass the full scope of threats and vulnerabilities in voting systems for a systematic analysis of risks applicable to any voting scenario. Its foundation is a thorough literature review, and its main features are a model for comparative risk analysis, as well as a computational model for the quantification of risks. The former is used to shape the methodology used for individual risk analysis and standardize its outputs to allow for their side-by-side comparison across different voting systems. The latter is used to assign quantitative risk values to these comparable outputs. This framework aims at providing a greater understanding of the current risks being accepted with respect to the by-mail voting system, and allows for the comparison of these risks in a quantifiable fashion with the risks associated with other voting systems.

The methodology for the comparative and quantitative risk analysis of voting systems consists of the following six-step process, as illustrated in Figure 3.1 and detailed in the following sections:

1. Definition of the methodology for individual risk analysis;
2. Creation of the framework for comparative and quantitative risk analysis;
3. Translation of the methodology for individual risk analysis into a methodology for comparative risk analysis via a comparative risk analysis model included in the framework;
4. Application of the methodology for comparative risk analysis to different voting systems,
5. Quantification of risk via computation of risk analysis outputs, i.e. likelihood and impact, via the computational model included in the framework; and
6. Side-by-side comparison of quantitated risks from different voting systems.

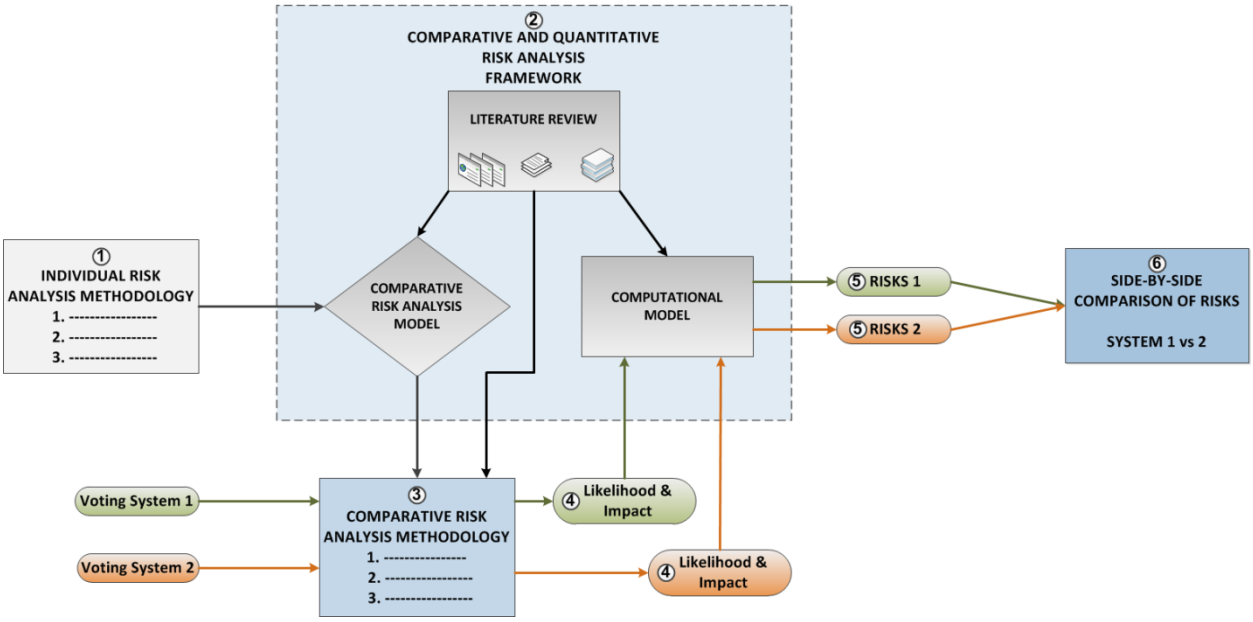


Figure 3.1: Methodology for Comparative and Quantitative Risk Analysis

3.1 Individual Risk Analysis Methodology

The methodology for individual risk analysis is modeled on the methodology proposed in NIST Special Publication 800-30[26] for risk management in information technology systems, and adapted to a voting environment as follows, with all terms defined in Section 2 and Appendix A:

1. Voting system characterization;
    a. Definition of the voting system's architecture
    b. Definition of the voting process
    c. Identification of the voting system's security objectives
2. Vulnerability identification;
3. Threat identification;
    a. Identification of threat agents
    b. Identification of threat vectors
4. Likelihood determination; and
5. Impact evaluation.

These steps are described in Appendix B, and discussed in further details during the methodology implementation to individual systems in Section 4.

3.2 Framework for Comparative and Quantitative Risk Analysis

The framework consists of a thorough literature review, a comparative risk analysis model, and a computational model described hereafter.

3.2.1 Literature Review

An extensive literature of academic peer-reviewed articles and technical reports from several federal, commercial, and grassroots organizations were examined to achieve the following goals:

1. Identify vulnerabilities and threats to voting systems;
2. Define a comparative risk analysis model for the side-by-side comparison of voting-related risks associated with different voting systems; and
3. Define a computational model for the quantification of voting-related risks.

A total of 128 documents were retained spanning research conducted from 1995 to the present. The full reference list of documents is present in Appendix B.

3.2.2 Comparative Risk Analysis Model

The main objective of this work is to perform a comparative and quantitative risk analysis of two different voting systems. To achieve this goal, the following sources from NIST were used to guide in the selection of a risk analysis model that allows the systematic comparison of risks across voting scenarios:

- NIST Special Publication 800-30: *Risk Management Guide for Information Technology Systems* (2002)[27]
- NIST: *A Threat Analysis on UOCAVA Voting Systems* (2008)[28]
- NIST: *Risk Methodology for UOCAVA Voting Systems* (2010)[29]

Several risk analysis models were assessed, with the main ones highlighted below:

- *Managing Information Security Risks – The OCTAVE Approach* (2002)[30]
- NIAC: *Common Vulnerability Scoring System* (CVSS, 2004)[31]
- *Voting System Risk Assessment via Computational Complexity Analysis* (2008)[32]
- EAC: *Election Operations Assessment – Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA)* EAC Advisory Board and Standards Board Draft Report (2009)[33]
- *Quantitative Security Analysis of Internet Voting vs. Two Other Voting Systems* (2010)[34]
- *Towards Internet Voting Security: A Threat Tree for Risk Assessment* (2010)[35]

- *Applying a Reusable Election Threat Model at the County Level* (2011)[36]

The OCTAVE approach,[37] using a hierarchical method of organizing threats, was not selected as it related more to information security than to voting risks. Similarly, the CVSS[38] was rejected, in part due to its cybersecurity-centric approach, but also due to the significant amount of resources required to adapt it to voting systems. Wallach's complexity analysis method (2008)[39]and the attack team approach of Lazarus et al. (2010)[40] were not selected as they focused on the attacker and not on the voting system and process themselves. Instead, the threat tree approach of Dr. Alec Yasinsac et al. on the Election Operations Assessment (EOA) project [41] was selected, as it was considered most promising for comparative and quantitative risk analysis of voting systems.

A threat tree is a hierarchical method of categorizing threat vectors in increasing levels of specificity by levels or branches. Threat trees are effective for determining relative risks because their structure allows for the standardization of risk analysis outputs across voting systems, thus allowing their side-by-side comparison. The threat tree approach also provides the level of abstraction necessary to encompass all voting scenarios. In addition, its relevance and applicability to the risk analysis of voting systems has been validated by a panel consisting of election officials, a representative from NIST, security experts, voting equipment vendors, voting equipment testing labs, election law attorneys, and academics.[42]

However, the threat tree model developed by Dr. Yasinsac et al. was aimed at analyzing voting-related risks for individual voting systems, independently (to that effect, the research team had built a different threat tree for each of the seven voting systems under consideration), and from an attacker's perspective. Each threat tree derived from this project organized threats but was structured around the steps required to carry out specific attacks. Thus, a threat tree designed for "Vote by Mail" could not be used for assessing "Vote by Internet", since the steps required to carry out system-specific attacks are different from one voting system to the other. As a result, departing from the single system attacker-centric approach of the EOA threat trees, it was deemed that one unique threat tree architecture based on the steps in the voting process and threat vectors rather than threat agents (or attackers) would be more appropriate to encompass all voting scenarios and allow the systematic comparison of risks across different voting systems.

To build such a universal threat tree, threat vectors are categorized in increasing levels of specificity to encompass all the vulnerabilities associated with each element in the voting system and each step in the voting process, as follows, and illustrated in the workflow in Figure 3.2:

System/Step Level	This level encompasses all threat vectors either at the level of the voting system, or at the level of a voting step of interest.
Level 1.	Threat vectors are first categorized as intentional or unintentional disruptions, i.e. attacks or unintentional disrupting events.
Level 2.	Intentional disruptions, implicitly carried out by malicious individual(s), are subdivided based on access to any step in the voting process (i.e. insider and outsider attacks), while unintentional disruptions are divided between voting-related errors linked to voting system elements, and accidental disruptions not directly related to the voting process.
Level 3.	Threat vectors are further categorized by action in the voting process, e.g. transmission of absentee ballots, and chronologically organized by voting step.

The universal threat tree resulting from this segregation of threat vectors is shown in indented format in Figure 3.3 (intentional disruptions) and Figure 3.4 (unintentional disruptions). Shaded threat vectors are only applicable to an online absentee voting scenario.

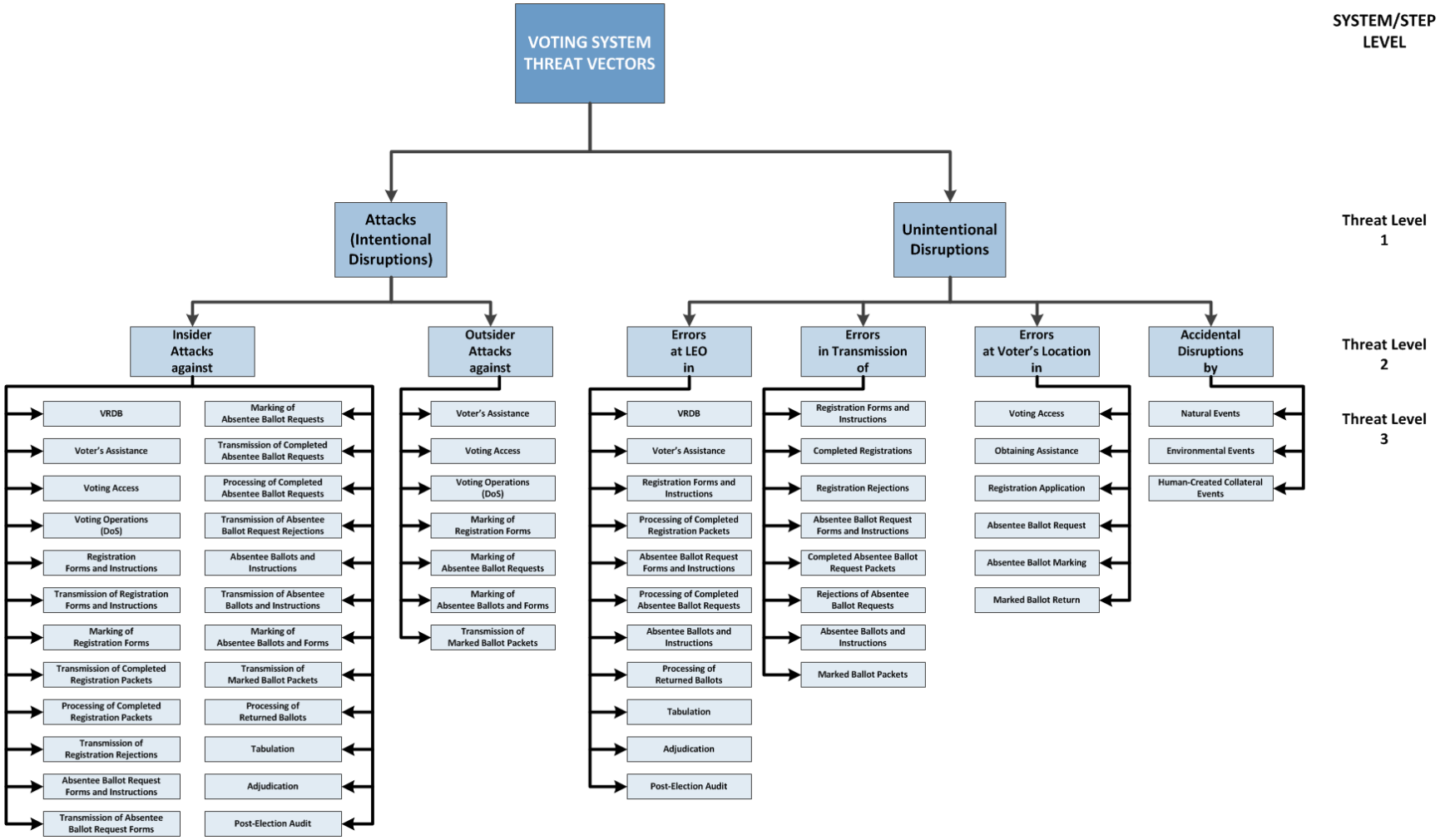


Figure 3.2: Workflow for the Design of a Universal Voting System Threat Tree

- **1 ATTACKS**
  - **1.1 INSIDER ATTACKS**
    - **1.1.1 Attacks Against VRDB**
    - **1.1.2 Attacks Against Voter's Assistance**
    - **1.1.3 Attacks Against Voting Access**
    - **1.1.4 Attacks by Denial of Service**
    - **1.1.5 Attacks Against Registration Forms and Instructions**
    - **1.1.6 Attacks During Transmission of Registration Forms and Instructions**
    - **1.1.7 Attacks Against Marking of Registration Forms**
    - **1.1.8 Attacks During Transmission of Completed Registration Packets**
    - **1.1.9 Attacks Against Processing of Completed Registration Packets**
    - **1.1.10 Attacks During Transmission of Registration Rejections**
    - **1.1.11 Attacks Against Absentee Ballot Request Forms and Instructions**
    - **1.1.12 Attacks During Transmission of Absentee Ballot Request Forms and Instructions**
    - **1.1.13 Attacks Against Marking of Absentee Ballot Requests**
    - **1.1.14 Attacks During Transmission of Completed Absentee Ballot Request Packets**
    - **1.1.15 Attacks Against Processing of Completed Absentee Ballot Request Packets**
    - **1.1.16 Attacks During Transmission of Rejections of Absentee Ballot Requests**
    - **1.1.17 Attacks Against Absentee Ballots and Instructions**
    - **1.1.18 Attacks During Transmission of Absentee Ballot and Instructions**
    - **1.1.19 Attacks Against Marking Absentee Ballots and Forms**
    - **1.1.20 Attacks During Transmission of Marked Ballot Packets**
    - **1.1.21 Attacks Against Processing of Returned Ballots**
    - **1.1.22 Attacks Against Tabulation**
    - **1.1.23 Attacks Against Adjudication**
    - **1.1.24 Attacks Against Post-Election Audit**
  - **1.2 OUTSIDER ATTACKS**
    - **1.2.1 Attacks Against Voter's Assistance**
    - **1.2.2 Attacks Against Voting Access**
    - **1.2.3 Attacks by Denial of Service**
    - **1.2.4 Attacks Against Marking of Registration Forms**
    - **1.2.5 Attacks Against Marking of Absentee Ballot Requests**
    - **1.2.6 Attacks Against Marking Absentee Ballots and Forms**
    - **1.2.7 Attacks During Transmission of Marked Ballot Packets**

Figure 3.3: Universal Voting System Threat Tree – Intentional Disruptions
(Shaded threat vectors are only applicable to an online absentee voting scenario)

- **2 UNINTENTIONAL DISRUPTIONS**
  - **2.1 ERRORS AT LOCAL ELECTION OFFICE**
    - **2.1.1 Errors in VRDB**
    - **2.1.2 Errors in Voter's Assistance**
    - **2.1.3 Errors in Registration Forms and Instructions**
    - **2.1.4 Errors in Processing Completed Registration Packets**
    - **2.1.5 Errors in Absentee Ballot Request Forms and Instructions**
    - **2.1.6 Errors in Processing Completed Absentee Ballot Request Packets**
    - **2.1.7 Errors in Absentee Ballots and Instructions**
    - **2.1.8 Errors in Processing of Returned Ballots**
    - **2.1.9 Errors in Tabulation**
    - **2.1.10 Errors in Adjudication**
    - **2.1.11 Errors in Post-Election Audit**
  - **2.2 ERRORS DURING TRANSMISSION OF ELECTION MATERIALS**
    - **2.2.1 Errors in Transmission of Registration Forms and Instructions**
    - **2.2.2 Errors in Transmission of Completed Registration Packets**
    - **2.2.3 Errors in Transmission of Registration Rejections**
    - **2.2.4 Errors in Transmission of Absentee Ballot Request Forms and Instructions**
    - **2.2.5 Errors in Transmission of Completed Absentee Ballot Request Packets**
    - **2.2.6 Errors in Transmission of Rejections of Absentee Ballot Requests**
    - **2.2.7 Errors in Transmission of Absentee Ballot and Instructions**
    - **2.2.8 Errors in Transmission of Marked Ballot Packets**
  - **2.3 ERRORS AT VOTER'S LOCATION**
    - **2.3.1 Errors in Voting Access**
    - **2.3.2 Errors in Obtaining Voter's Assistance**
    - **2.3.3 Errors in Registration Application**
    - **2.3.4 Errors in Absentee Ballot Requests**
    - **2.3.5 Errors in Absentee Ballot Marking**
    - **2.3.6 Errors in Marked Ballot Return**
  - **2.4 ACCIDENTAL DISRUPTIONS**
    - **2.4.1 Disruptions by Natural Events**
    - **2.4.2 Disruptions by Environmental Events**
    - **2.4.3 Disruptions by Human-Created Collateral Events**

Figure 3.4: Universal Voting System Threat Tree – Unintentional Disruptions

To allow the comparison of voting systems from a process standpoint, seven process-based threat trees were derived from the universal threat tree for each of the voting steps in the voting process (Section 2.2). To build these voting step threat trees, the threat vectors relevant to each voting step need to be selected among all the threat vectors on the universal threat tree. All threat vectors from the system/step level through Level 2 are common to all voting steps. This similar structure among voting step threat trees is intended to facilitate comparisons across voting steps and voting scenarios. Threat vectors at the third level are categorized by actions in the voting process. To illustrate this categorization, the threat vectors from the universal threat tree under "Insider attacks" are illustrated below in Figure 3.5, and color coded against the steps in the voting process:

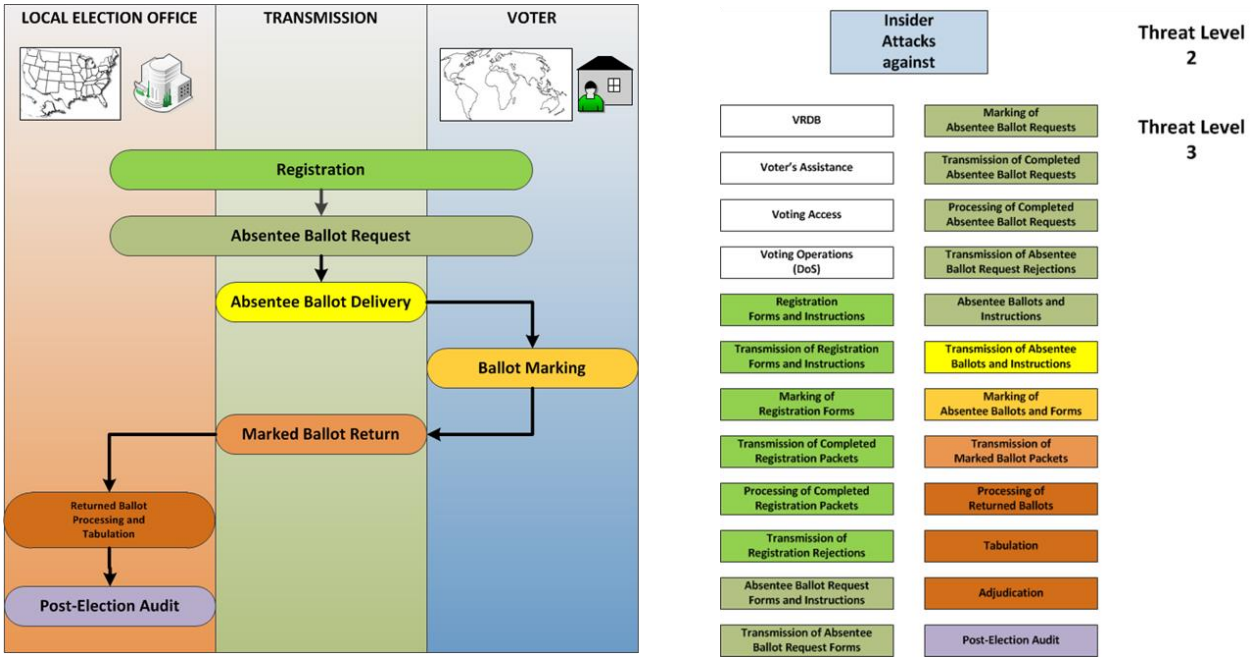


Figure 3.5: Categorization by Voting Step of Level 3 Threat Vectors

As a result of this organization, threat vectors at the third level of indentation of the universal threat tree can be selected for each relevant voting step. As an example, the green shading on

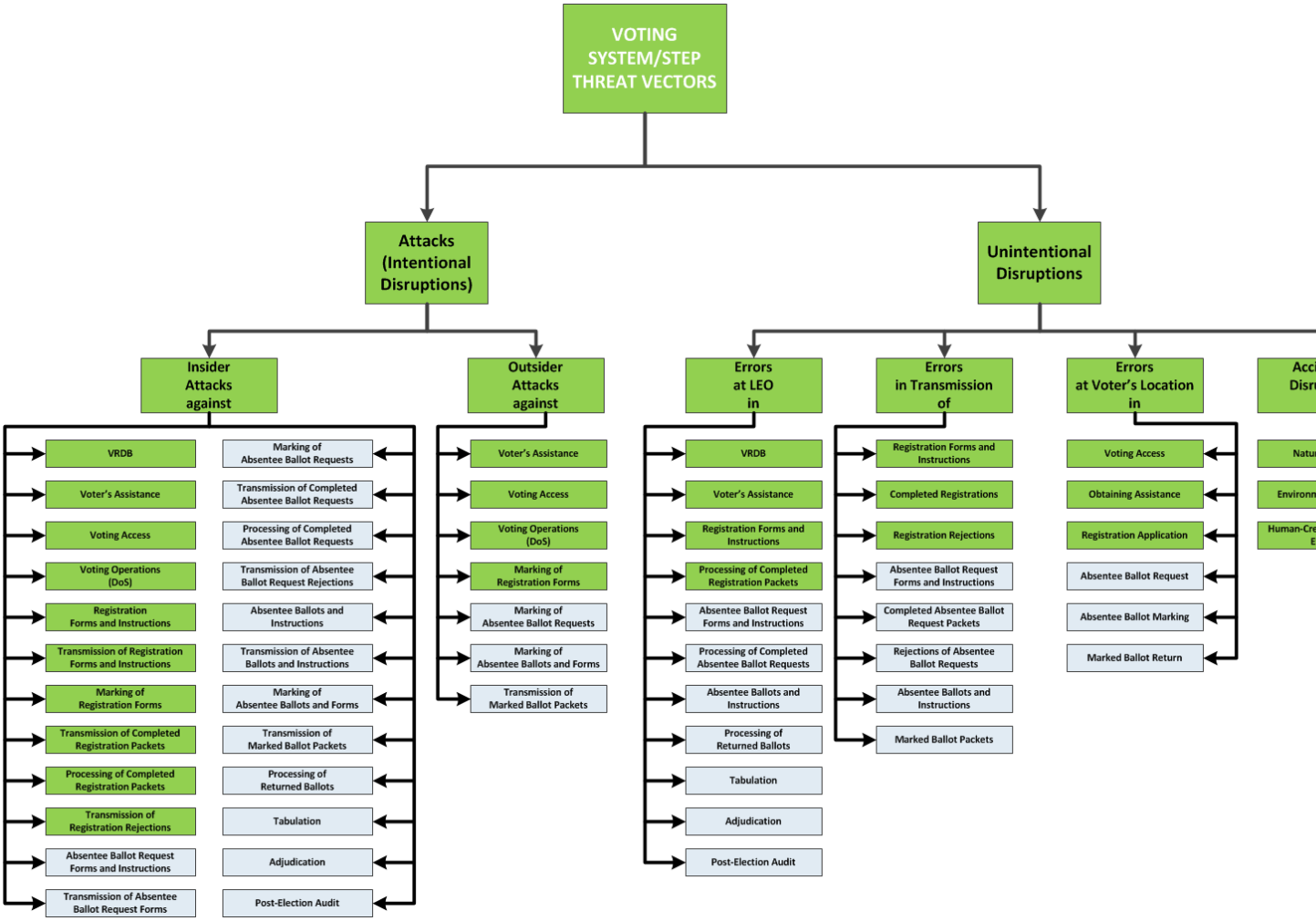


Figure 3.6 illustrates the selection within the universal threat tree of the threat vectors relevant to the registration step. This process yields the registration threat tree for the current UOCAVA voting system shown on Figure 3.7, and provided in indented format in Figure 3.8. All voting step threat trees are provided in indented format in Appendix B.

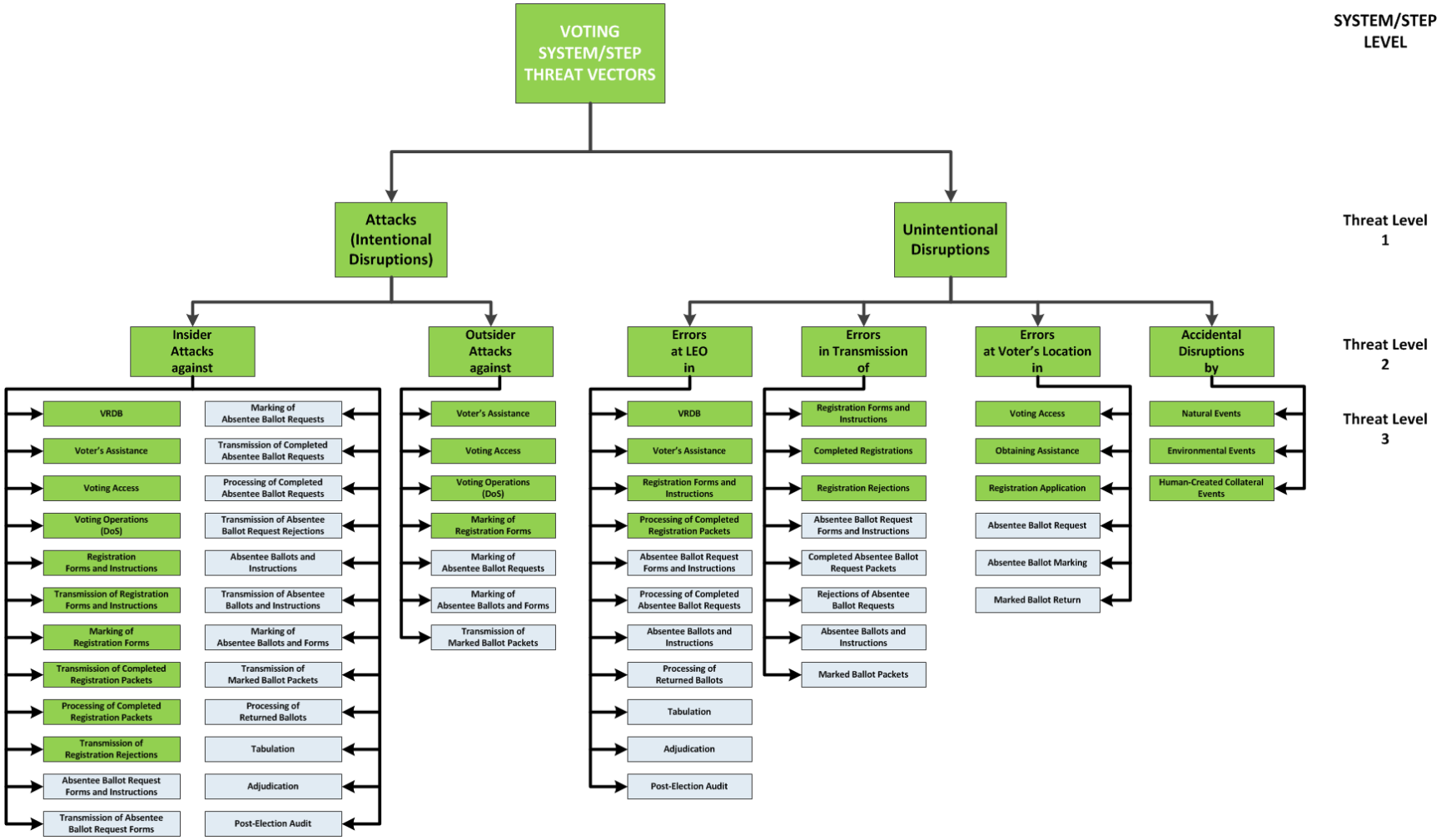


Figure 3.6: Workflow for the Design of the Current UOCAVA Registration Threat Tree

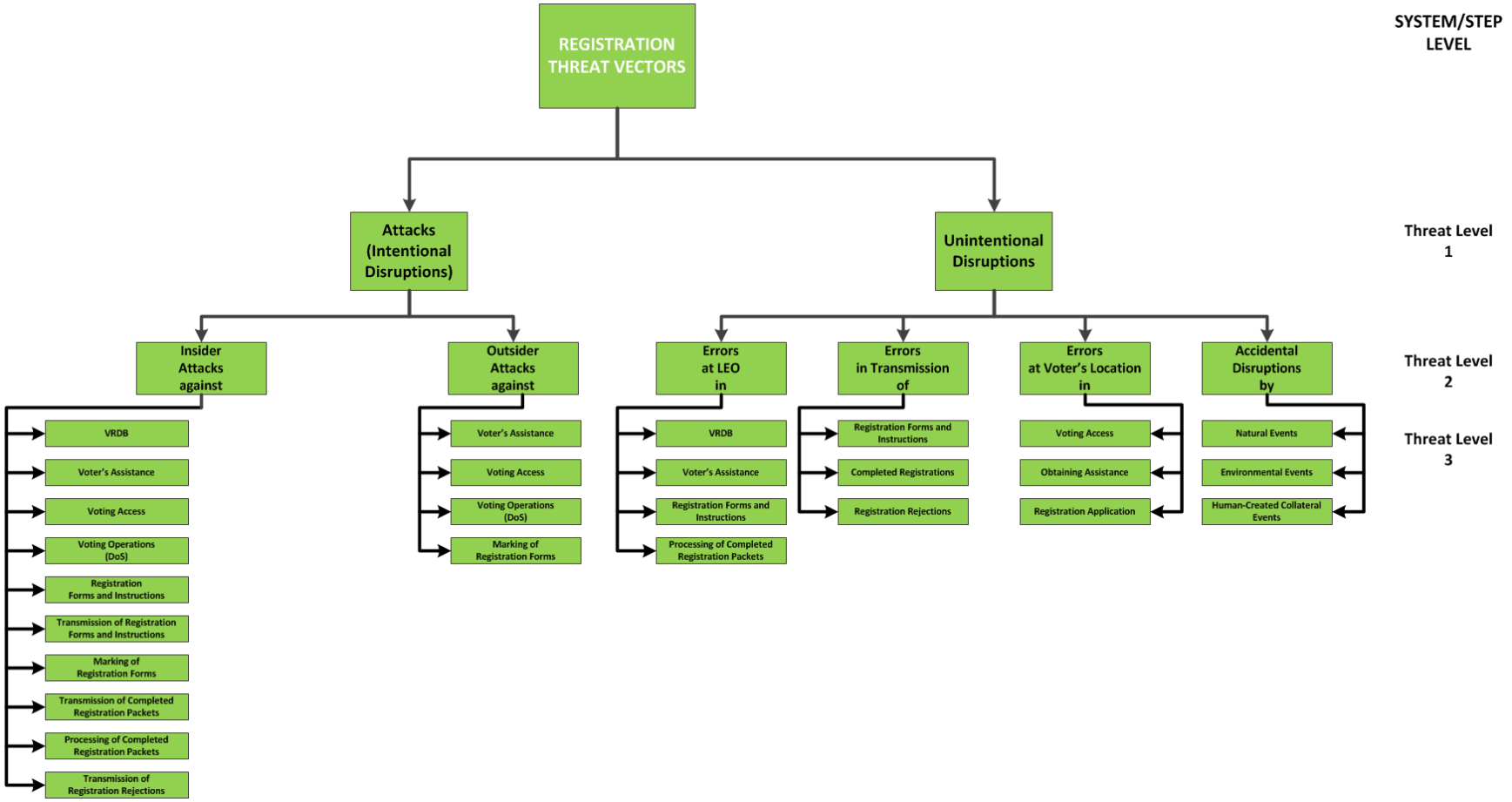


Figure 3.7: Current UOCAVA Registration Threat Tree

- **1 ATTACKS**
  - **1.1 INSIDER ATTACKS**
    - **1.1.1 Attacks Against VRDB**
    - **1.1.2 Attacks Against Voter's Assistance**
    - **1.1.3 Attacks Against Voting Access**
    - **1.1.4 Attacks by Denial of Service**
    - **1.1.5 Attacks Against Registration Forms and Instructions**
    - **1.1.6 Attacks During Transmission of Registration Forms and Instructions**
    - **1.1.8 Attacks During Transmission of Completed Registration Packets**
    - **1.1.9 Attacks Against Processing of Completed Registration Packets**
    - **1.1.10 Attacks During Transmission of Registration Rejections**
  - **1.2 OUTSIDER ATTACKS**
    - **1.2.1 Attacks Against Voter's Assistance**
    - **1.2.2 Attacks Against Voting Access**
    - **1.2.3 Attacks by Denial of Service**
    - **1.2.4 Attacks Against Marking of Registration Forms**
- **2 UNINTENTIONAL DISRUPTIONS**
  - **2.1 ERRORS AT LOCAL ELECTION OFFICE**
    - **2.1.1 Errors in VRDB**
    - **2.1.2 Errors in Voter's Assistance**
    - **2.1.3 Errors in Registration Forms and Instructions**
    - **2.1.4 Errors in Processing Completed Registration Packets**
  - **2.2 ERRORS DURING TRANSMISSION OF ELECTION MATERIALS**
    - **2.2.1 Errors in Transmission of Registration Forms and Instructions**
    - **2.2.2 Errors in Transmission of Completed Registration Packets**
    - **2.2.3 Errors in Transmission of Registration Rejections**
  - **2.3 ERRORS AT VOTER'S LOCATION**
    - **2.3.1 Errors in Voting Access**
    - **2.3.2 Errors in Obtaining Voter's Assistance**
    - **2.3.3 Errors in Registration Applications**
  - **2.4 ACCIDENTAL DISRUPTIONS**
    - **2.4.1 Disruptions by Natural Events**
    - **2.4.2 Disruptions by Environmental Events**
    - **2.4.3 Disruptions by Human-Created Collateral Events**

Figure 3.8: Current UOCAVA Registration Threat Tree in Indented Format

Key identifiers are used to label threat vectors throughout the report and are detailed in Table 3.1:

Table 3.1: Threat Vectors Identifiers

Identifier	Description	Identifier	Description
Voting System		***Level 3 Threat Vectors (cont'd)***	
M	Current UOCAVA Voting System	TREG	Attacks/Errors Involving Transmission of Registration Forms and Instructions
I	REAV	MREG	Attacks/Errors Involving Marking of Registration Forms
Voting Step		TCRP	Attacks/Errors Involving Transmission of Completed Registration Packets
REG	Registration	PCRP	Attacks/Errors Involvingt Processing of Completed Registration Packets
ABR	Absentee Ballot Request	TRRP	Attacks/Errors Involving Transmission of Registration Rejections
ABD	Absentee Ballot Delivery	ABRF	Attacks/Errors Involving Absentee Ballot Request Forms and Instructions
BMK	Ballot Marking	TABR	Attacks/Errors Involving Transmission of Absentee Ballot Request Forms and Instructions
MBR	Marked Ballot Return	MABR	Attacks/Errors Involving Marking of Absentee Ballot Requests
RBP	Returned Ballot Processing and Tabulation	TCAP	Attacks/Errors Involving Transmission of Completed Absentee Ballot Request Packets
ADT	Post-Election Audit	PCAP	Attacks/Errors Involving Processing of Completed Absentee Ballot Request Packets
Level 2 Threat Vectors		TRAP	Attacks/Errors Involving Transmission of Rejections of Absentee Ballot Requests
INS	Insider Attacks	ABSF	Attacks/Errors Involving Absentee Ballots and Instructions
OUT	Outsider Attacks	TABS	Attacks/Errors Involving Transmission of Absentee Ballot and Instructions
ERL	Error at the LEO	MABS	Attacks/Errors Involving Marking Absentee Ballots and Forms
ERT	Error in Transmission	TMBP	Attacks/Errors Involving Transmission of Marked Ballot Packets
ERV	Error at the Voter's Location	PRBT	Attacks/Errors Involving Processing of Returned Ballots
DIS	Accidental Disruptions	TABN	Attacks/Errors Involving Tabulation
Level 3 Threat Vectors		ADJN	Attacks/Errors Involving Adjudication
VRDB	Attacks/Errors Involving VRDB	PADT	Attacks/Errors Involving Post-Election Audit
ASST	Attacks/Errors Involving Voter's Assistance	NATL	Natural Events
ACCS	Attacks/Errors Involving Voting Access	NVRO	Environmental Events
DOSV	Attacks by Denial of Service	HUMN	Human-Created Collateral Events
REGF	Attacks/Errors Involving Registration Forms and Instructions		

3.2.3 Computational Model for Risk Analysis

The computational model used to quantify the risks associated with voting systems is derived from the Draft EOA's Threat Instance Risk Analyzer (TIRA) tool. A copy of this tool (last updated on March 24, 2010) was used for this work. Information related to its functionalities was gathered from the EAC website.[43] This tool is adapted for the purpose of a comparative analysis of two voting systems in line with the modifications made to the original EOA threats trees, as detailed in Section 3.2.2. In the present context of analyzing voting system risks from a process standpoint, the computation of risks is conducted by voting step (as described in Section 3.2.2), and defined as the estimation of risks from threats potentially exercised on vulnerabilities associated with that particular voting step. These threats are identified on voting step threat trees (Figure 3.7 and Figure 3.8) derived from the universal voting system threat tree (Figure 3.3 and Figure 3.4). The estimation of risks with TIRA is derived from the evaluation of likelihood and the determination of impact for threat vectors on a threat tree loaded into the tool. For the purpose of comparing risks across voting systems, voting step threat trees were loaded into TIRA. This tool solicits a "reasonable range of values"[44] from stakeholders for threat likelihood and impact in the form of numerical answers to the following two questions, as shown on the TIRA worksheet in Figure 3.9:

1. Likelihood

   Arbitrarily consider one hundred (100) federal elections. Assume a specific voting system configuration, threat countermeasures, controls, and protocols. First, of these 100 elections, in how many elections do you think this attack will be exercised? Second, express how confident you are in your estimate by indicating the maximum and minimum number of elections in which you think this attack will be exercised. Interpret this range of number as "I think the number will be [most likely], but it could be as high as [maximum] and as low as [minimum]".

2. Impact

   Arbitrarily consider one hundred (100) federal elections. Assume a specific voting system configuration, threat countermeasures, controls, and protocols. If this Threat were exercised, for how many of these elections would the impact be low, medium, and high? See table for definitions.

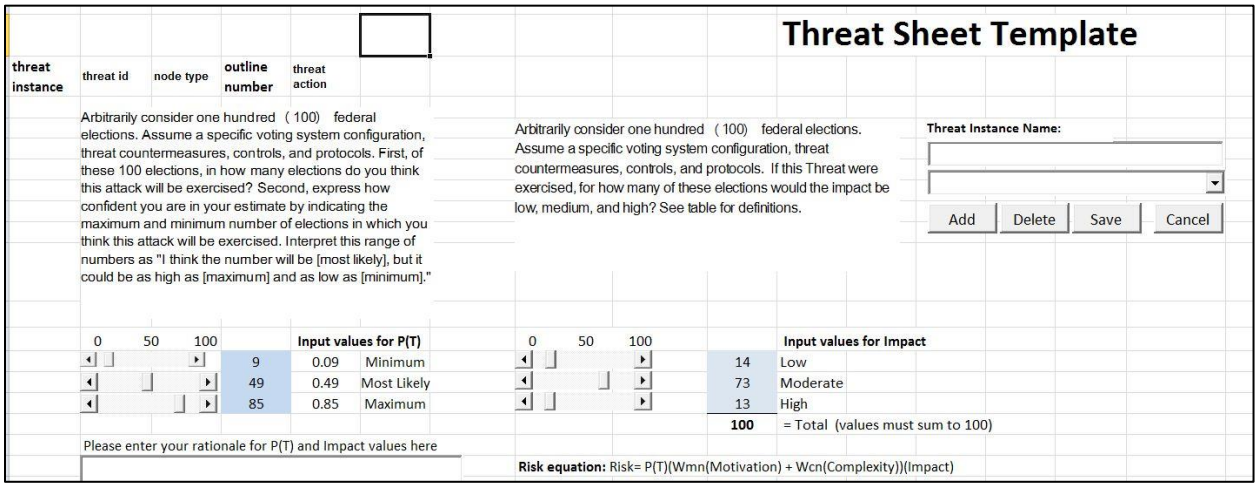


Figure 3.9: EOA's TIRA Worksheet

Based on the focus of this effort, the likelihood and impact questions in the original TIRA model were modified as follows.

1. Likelihood

   In the context of a Federal election, what percentage of the time do you think the threat would be most likely realized and have an observable effect? Provide minimum and maximum values. Interpret this range of values as "I think this threat would be realized and have an observable effect in [most likely] percent (%) of the time but this estimate could be as low as [minimum] % and as high as [maximum] %."

2. Impact

   In the context of a Federal election, assuming the threat is realized, what percentage of the time would it have a low, medium, and high impact? (Numbers should sum to 100)

A Federal election is defined here as a general election for President and Vice-President, election for members of the Senate, and election for members of the House of Representatives. The electoral process associated with the general election for President and Vice-President is restrained to the process of popular vote and does not include the act of voting by the Electoral College.

A panel of subject matter experts including four cyber security experts and three election experts was convened to obtain inputs for the modified TIRA computational model. These subject matter experts (SME) provide their inputs for likelihood and impact for each threat vectors at Level 3 on all voting step threat trees via a questionnaire presented in Appendix B. An extract of the questionnaire associated with the UOCAVA voting system is presented in Figure 3.10.

Specific instructions are provided to each stakeholder to ensure each question is understood as intended, as shown in Figure 3.11. In addition, the use of the CNSS definition of impact for voting risk (Table A.3) provides the user with a means to estimate the scale at which a threat would be exercised, from a retail or wholesale standpoint.

The TIRA model computes these estimates through a Monte Carlo simulation to derive risk values for each threat vector. The statistical method is described in greater detail in Appendix B. This mathematical means of deriving risk estimates for each threat vector was conserved in the modified TIRA model.

Attacker's motivation and attack complexity are also parameters in the original TIRA model. However, based on the goal of estimating voting system risks from a voting process standpoint and across voting scenarios, instead of an attack process standpoint, these parameters were neutralized in the modified TIRA model by providing them with neutral values to avoid their interference with the final output of the model.

The TIRA risk scoring equation is defined as follows for each threat vector and each iteration in the Monte Carlo simulation:

$$Risk\ Score = Threat\ Likelihood\ \times \big(Wmn(Motivation) + Wcn(Complexicity)\big) \times Impact$$

Where: W_{mn} is the weighing factor associated with the input variable "Motivation"

W_{cn} is the weighing factor associated with the input variable "Complexity"

Since motivation and complexity are not considered in the proposed voting system risk model:

$$\big(Wmn(Motivation) + Wcn(Complexicity)\big)\ = 1$$

Hence:

$$Risk\ Score = Threat\ Likelihood\ \times Impact$$

All risk scores derived from each iteration in the Monte Carlo simulation, for a given threat vector, are averaged to obtain one single risk estimate per threat vector.

THREAT VECTORS VOTING SCENARIO: Current UOCAVA absentee voting system, restricted to paper ballots transmitted by postal mail, with no electronic component Voting Step: RETURNED BALLOT PROCESSING & TABULATION	LIKELIHOOD In the context of a Federal election, what percentage of the time do you think the threat would be most likely realized AND have an observable effect? Provide minimum and maximum values. Interpret this range of values as "I think this threat would be realized AND have an observeable effect in [most likely] percent (%) of the time but this estimate could be as low as [minimum] % and as high as [maximum] %." (numbers DO NOT need to sum to 100)			IMPACT In the context of a Federal election, assuming the threat is realized, what percentage of the time would it have a low, medium, and high impact? (numbers should sum to 100)		
	Minimum	Most Likely	Maximum	Low	Medium	High
ATTACKS						
INSIDER ATTACKS						
Attacks Against VRDB						
Types of threat vectors: Intentional modification of registration records; Intentional destruction of registration records; Intentional addition of fake registration records; VRDB intentional crash;						
Attacks by Denial of Service						
Types of threat vectors: Intentional disruption of processing of marked ballots at LEO;						
Attacks Against Processing of Returned Ballots						
Types of threat vectors: Intentional modification of marked ballot packets at the LEO; Intentional destruction of marked ballot packets at the LEO; Intentional addition of fake marked ballot packets at the LEO;						
Attacks Against Tabulation						
Types of threat vectors: Intentional subversion of the counting process; Intentional subversion of the validation process; Intentional destruction of tabulated results; Intentional subversion of the tabulated results;						

Figure 3.10: Extract from the Questionnaire for the Current UOCAVA Voting System

INSTRUCTIONS

PLEASE READ IN FULL, UNTIL THE "END OF PAGE" MARK.

Begin by scoring the Registration Step on the first tab "REG L3 Mail Scoring" at the bottom of the worksheet

1. For each threat vector **highlighted in red**, please answer the likelihood and impact questions, **in the context of the voting scenario highlighed in the top banner**, i.e paper ballots transmitted by postal mail, AND restricted to the **REGISTRATION** voting step.

2. For the **likelihood** question, please answer the following:

   In the context of a Federal election, what percentage of the time do you think the threat would be most likely realized AND have an observable effect? Provide minimum and maximum values. Interpret this range of values as "I think this threat would be realized AND have an observeable effect in [most likely] percent (%) of the time but this estimate could be as low as [minimum] % and as high as [maximum] %."

3. For the **impact** question, please answer the following:

   In the context of a Federal election, assuming the threat is realized, what percentage of the time would it have a low, medium, and high impact? (numbers should sum to 100)

   The definition of the different impact levels is provided below (NIST SP 800-30):

Impact Level	Impact Definition
High	Severe or catastrophic adverse effect on the voting process potentially resulting in contest failure, with the effectiveness of the process severely reduced, and major damage to privacy, integrity, and/or auditability.
Medium	Serious adverse effect on the voting process not resulting in contest failure, with the effectiveness of the process significantly reduced, and significant damage to privacy, integrity, and/or auditability.
Low	Limited adverse effect on the voting process not resulting in contest failure, with the effectiveness of the process noticeably reduced, and minor damage to privacy, integrity, and/or auditability.

Continue to score the 6 remaining voting steps by repeating Steps 1 through 3 for each tab. Be sure to restrict your estimates to the voting step at hand. The tab legend is provided below:

REG = Registration
ABR = Absentee Ballot Request
ABD Absentee Ballot Delivery
BM = Ballot Marking
MBR = Marked Ballot Return
RBPT = Returned Ballot Processing and Tabulation
ADT = Audit

Abbreviations

LEO = Local Election Office
VRDB = Voter Registration Database

----------END OF PAGE----------

Figure 3.11: Questionnaire Instructions for the Current UOCAVA Voting System

3.3 Methodology for Comparative Risk Analysis

This methodology is built upon the individual risk analysis methodology (Section 3.1) and modified according to the framework, as follows (modifications and additions to the individual risk analysis methodology are bolded):

1. **Voting system characterization:**
    a. Definition of the voting system's architecture
    b. Definition of the voting process
    c. Identification of the voting system's security objectives
2. **Creation of a Vulnerability-Threat Database - VTDb**
    a. Vulnerability identification
    b. Threat identification
        - Identification of threat agents
        - Identification of threat vectors
3. **Creation of a universal voting system threat tree, and system-specific voting step threat trees with threat vectors and associated vulnerabilities linked to the VTDb**
4. **Creation of a questionnaire to obtain inputs from stakeholders:**
    a. Likelihood determination
    b. Impact evaluation.

3.4 Application of the Comparative Risk Analysis Methodology

The comparative risk analysis methodology described above is applied to voting systems to obtain estimates of likelihood and determination of impact. The architecture of each voting system is defined and taken into account in the questionnaire used to gather this information. The outputs of the comparative risk analysis are sets of "reasonable range of values"[45] for likelihood and impact from each stakeholder and for each threat vector on all system-specific voting step threat trees. These sets of numerical values are the inputs used in the computational model to derive risk estimates.

3.5 Quantification of Voting System Risks

A TIRA computational model is created for each voting system and for each voting step, based on the system-specific voting step threat trees, resulting in seven models per voting system, as illustrated on Figure 3.12. The questionnaire's inputs are divided into subsets of likelihood and impact values for each voting step, which are imported into the corresponding step-specific

TIRA model, one SME at a time, resulting in seven sets of risk values for each SME, as described on Figure 3.13.

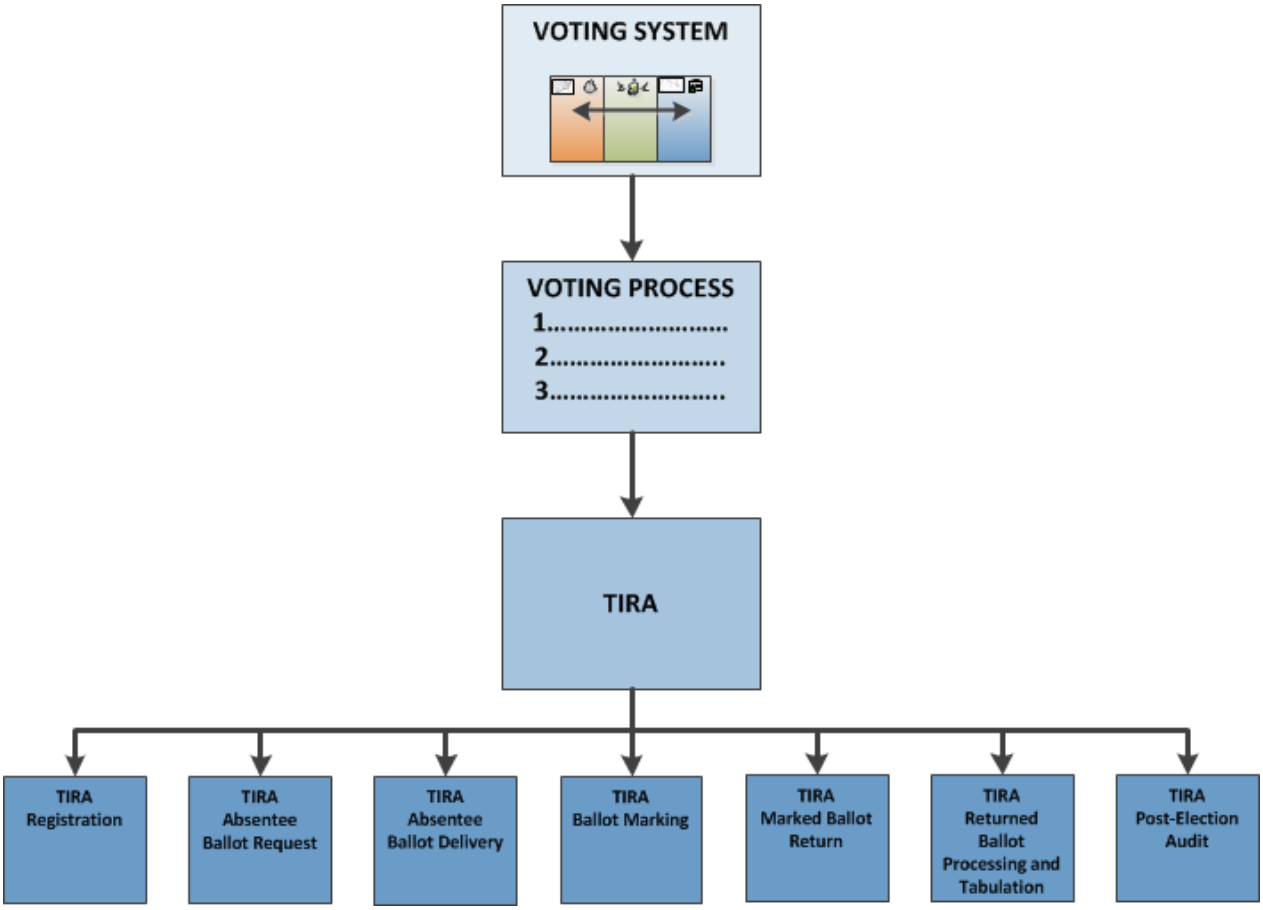


Figure 3.12: Step-Specific TIRA Models

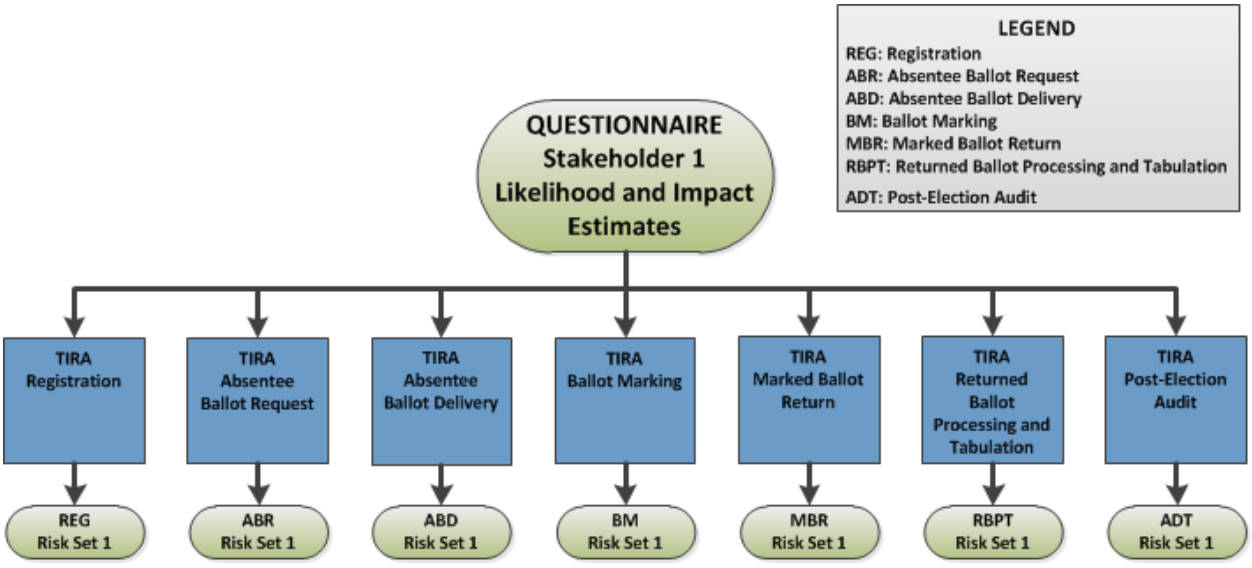


Figure 3.13: Step-Specific Risk Sets

The risk values for each threat vector are summed[i] across all stakeholders to obtain a single risk estimate per threat vector, and a single set of risk estimates per voting step, as described on Figure 3.14.

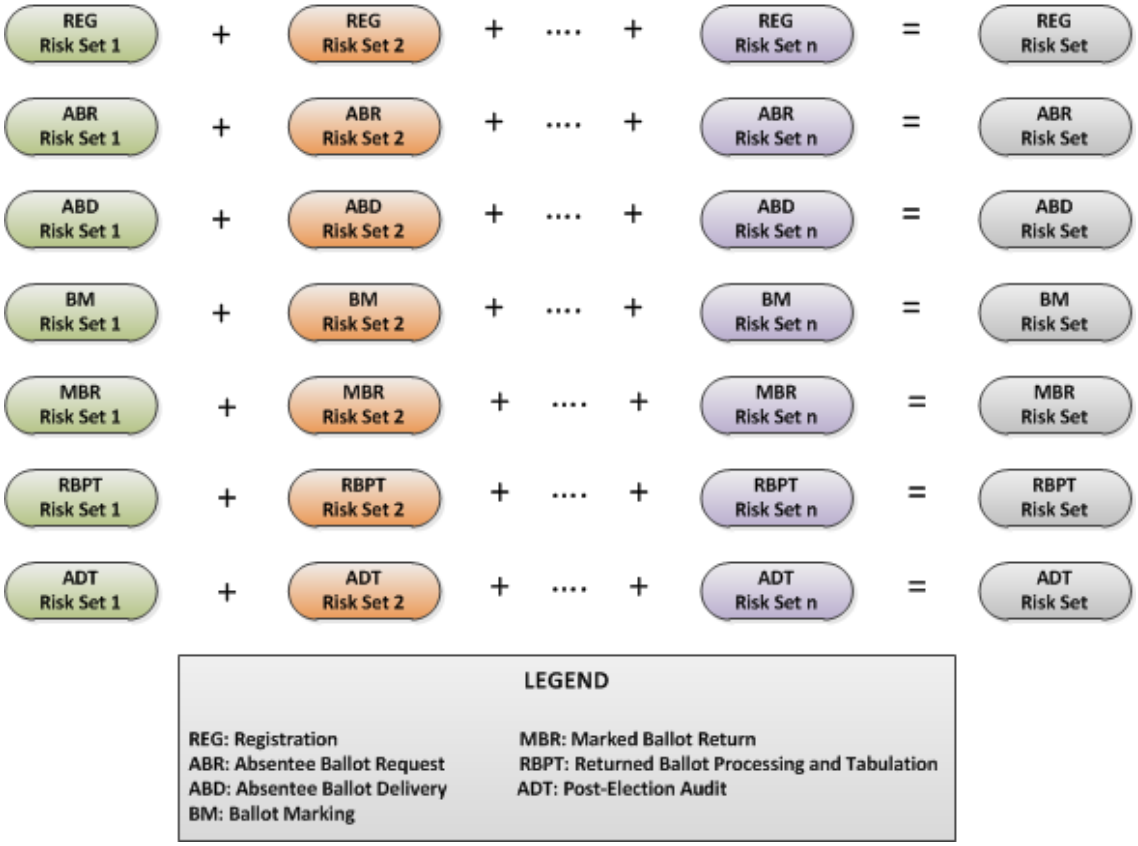


Figure 3.14: Risk Sets by Voting Step

3.6 Analysis of Individual Voting Systems

Once a risk estimate has been derived for each threat vector, risks can be compared by rank ordering the threat vectors according to their risk estimate to determine the highest associated risks. Risks can also be categorized by type of threats, e.g. attacks vs. errors, insider vs. outsider attacks or errors at the LEO vs. errors at the voter's location, or by voting step, e.g. registration vs. marked ballot return. This process is performed by averaging risk estimates across the categories of interest. Averaging is performed instead of summing at this stage of the

[i] Averaging is not performed due to the potential variability in risk estimates among the stakeholders. It would also inhibit the comparison of risk estimates between voting systems.

quantification to normalize the data given the various number of threat vectors in each category. In addition, the risks can be conveyed with respect to the voting system's security objectives, by determining the relevance of each of the security objectives to each threat vector. Table 3.2 shows an example of such determination, in a matrix format for the voting step "Marked Ballot Return." Based on this relevance matrix, the risk estimates computed for each threat vector are assigned to all the security objectives relevant to that threat vector, and can be averaged across all threat vectors to determine a risk estimate for each security objective in the context of the voting step of interest, as shown in Table 3.3 for the "Marked Ballot Return" step. As a result of this assignment, a security objective may not be assigned to a threat vector if it is deemed that this threat vector does not impact the security objective.

Table 3.2: Relevance of Security Objectives to Threat Vectors – Marked Ballot Return

			ASSIGNMENT MATRIX					
Threat Vector			Voter Authentication	Vote Secrecy	Vote Integrity	Vote Privacy	Auditability	Service Availability
Level 1	Level 2	Level 3						
Attacks	Insider	Attacks by Denial of Service						X
Attacks	Insider	Attacks During Transmission of Marked Ballots Packets			X			
Attacks	Outsider	Attacks by Denial of Service						X
Unintentional	Errors during Transmission of Election Materials	Errors in Transmission of Marked Ballot Packets		X	X	X		
Unintentional	Accidental Disruptions	Disruptions by Natural Events						X
Unintentional	Accidental Disruptions	Disruptions by Environmental Events						X
Unintentional	Accidental Disruptions	Disruptions by Human-Created Collateral Events						X

Table 3.3: Risk Estimates for Voting System Security Objectives – Marked Ballot Return
(The risk estimate values depicted are for illustration purposes only and do not reflect actual data)

Threat Vector			SECURITY RISK ESTIMATES						
Level 1	Level 2	Level 3	System 1 Risk Estimates	Voter Authentication	Vote Secrecy	Vote Integrity	Vote Privacy	Auditability	Service Availability
Attacks	Insider	Attacks by Denial of Service	0.650						0.650
Attacks	Insider	Attacks During Transmission of Marked Ballots Packets	0.173			0.173			
Attacks	Outsider	Attacks by Denial of Service	0.163						0.163
Unintentional	Errors during Transmission of Election Materials	Errors in Transmission of Marked Ballot Packets	0.233		0.233	0.233	0.233		
Unintentional	Accidental Disruptions	Disruptions by Natural Events	0.108						0.108
Unintentional	Accidental Disruptions	Disruptions by Environmental Events	0.059						0.059
Unintentional	Accidental Disruptions	Disruptions by Human-Created Collateral Events	0.047						0.047
		AVERAGES			0.233	0.203	0.233		0.205
		TOTALS SYSTEM 1			0.233	0.406	0.233		1.027

3.7 Comparative Analysis of Voting Systems

Within each voting step, risk values can be compared across voting systems for each threat vector at Level 3 in the format shown on Table 3.4 for the registration step, or individual risk values can also be "rolled up" by summing all Level 3 risk values under a Level 2 threat vector to obtain that threat vector risk estimate[i]. This process can be reiterated at Levels 2 and 1 to obtain a single risk value per voting step, allowing comparison of voting systems by major threat vectors (Level 1 and 2) as shown on Table 3.5. Voting step values can also be summed to obtain a single risk estimate for the whole voting system, as described on Figure 3.15, and the comparison of resulting risk estimates is performed in the format shown on Table 3.6, and can be illustrated as shown on Figure 3.16 or Figure 3.17 (The risk estimate values depicted are for illustration purposes only and do not reflect actual data). In addition, risks estimates for each voting system security objective can derived by summing all risk estimates across all threat vectors and comparing the results across voting systems, as shown in Figure 3.18. Since risk estimates for comparative analysis of voting systems are computed differently than risk estimates for individual voting system analysis, the estimates from the former cannot be compared to the estimates from the latter.

A user guide will be provided at a later date to guide FVAP in the use and customization of threat trees and the TIRA computational model.

[i] Summing is performed instead of averaging to allow comparative analysis of different voting systems.

Table 3.4: Comparison of Risk Estimates for the Registration Voting Step

THREAT VECTORS			RISK ESTIMATES			
			System 1	System 2	....	System n *
1	ATTACKS					
	1.1	INSIDER ATTACKS				
		1.1.1 Attacks Against VRDB				
		1.1.2 Attacks Against Voter's Assistance				
		1.1.3 Attacks Against Voting Access				
		1.1.4 Attacks by Denial of Service				
		1.1.5 Attacks Against Registration Forms and Instructions				
		1.1.6 Attacks During Transmission of Registration Forms and Instructions				
		1.1.8 Attacks During Transmission of Completed Registration Packets				
		1.1.9 Attacks Against Processing of Completed Registration Packets				
		1.1.10 Attacks During Transmission of Registration Rejections				
	1.2	OUTSIDER ATTACKS				
		1.2.1 Attacks Against Voter's Assistance				
		1.2.2 Attacks Against Voting Access				
		1.2.3 Attacks by Denial of Service				
		1.2.4 Attacks Against Marking of Registration Forms				
2	UNINTENTIONAL DISRUPTIONS					
	2.1	ERRORS AT LOCAL ELECTION OFFICE				
		2.1.1 Errors in VRDB				
		2.1.2 Errors in Voter's Assistance				
		2.1.3 Errors in Registration Forms and Instructions				
		2.1.4 Errors in Processing Completed Registration Packets				
	2.2	ERRORS DURING TRANSMISSION OF ELECTION MATERIALS				
		2.2.1 Errors in Transmission of Registration Forms and Instructions				
		2.2.2 Errors in Transmission of Completed Registration Packets				
		2.2.3 Errors in Transmission of Registration Rejections				
	2.3	ERRORS AT VOTER'S LOCATION				
		2.3.1 Errors in Voting Access				
		2.3.2 Errors in Obtaining Voter's Assistance				
		2.3.3 Errors in Registration Applications				
	2.4	ACCIDENTAL DISRUPTIONS				
		2.4.1 Disruptions by Natural Events				
		2.4.2 Disruptions by Environmental Events				
		2.4.3 Disruptions by Human-Created Collateral Events				

* n = number of voting systems being compared.

Table 3.5: Comparison of Risk Estimates across Voting Systems by Threat Vector

THREAT VECTORS		RISK ESTIMATES			
		System 1	System 2	....	System n *
1	ATTACKS				
1.1	INSIDER ATTACKS				
1.2	OUTSIDER ATTACKS				
2	UNINTENTIONAL DISRUPTIONS				
2.1	ERRORS AT LOCAL ELECTION OFFICE				
2.2	ERRORS DURING TRANSMISSION OF ELECTION MATERIALS				
2.3	ERRORS AT VOTER'S LOCATION				
2.4	ACCIDENTAL DISRUPTIONS				

* n = number of voting systems being compared.

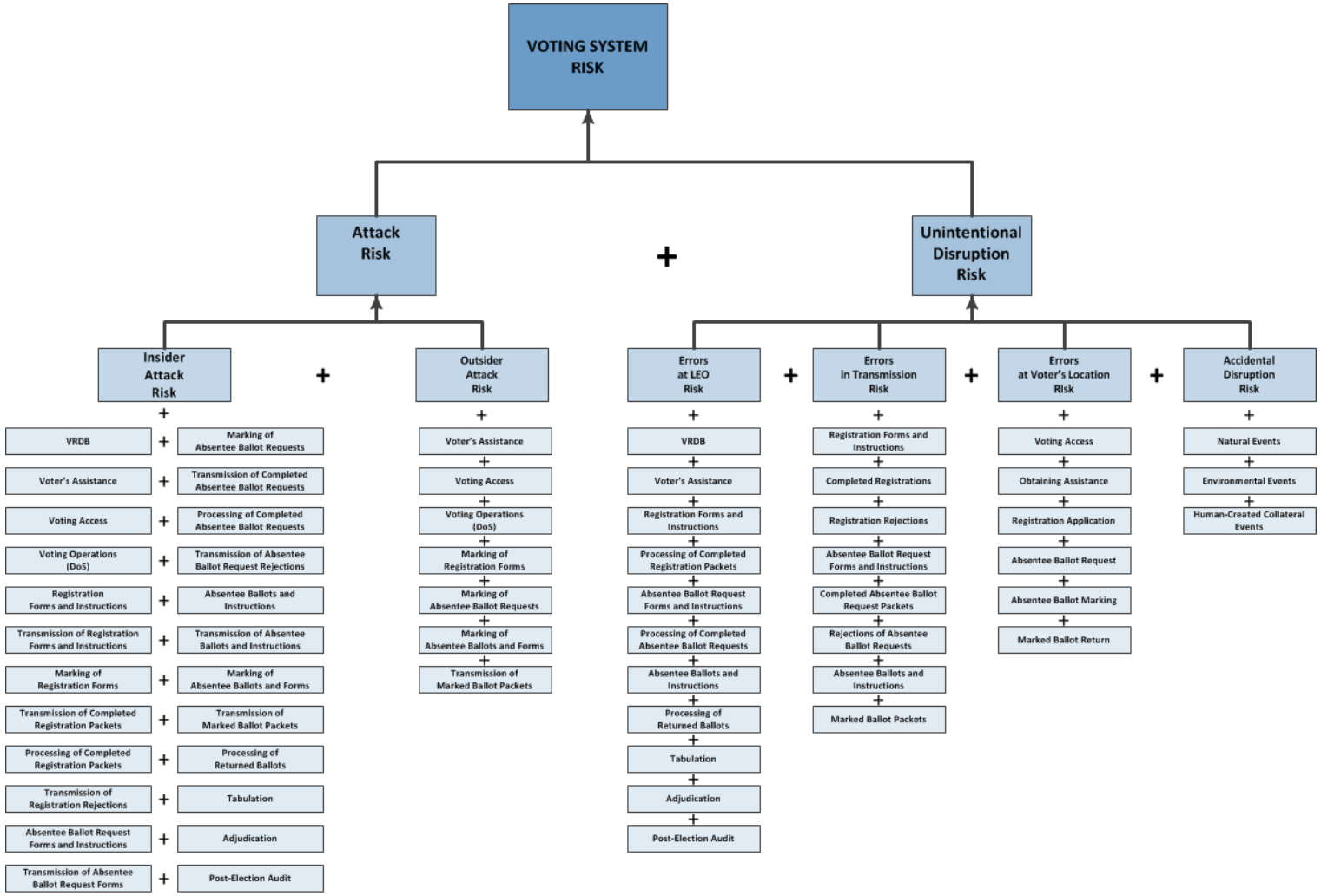


Figure 3.15: Process of Rolling Up Risk Estimates for Comparative Analysis

Table 3.6: Comparison of Risk Estimates across Voting Systems by Voting Step

THREAT VECTORS	RISK ESTIMATES			
	System 1	System 2	....	System n *
REGISTRATION				
ABSENTEE BALLOT REQUEST				
ABSENTEE BALLOT DELIVERY				
BALLOT MARKING				
MARKED BALLOT RETURN				
RETURNED BALLOT PROCESSING AND TABULATION				
POST-ELECTION AUDIT				
WHOLE VOTING SYSTEM				

* n = number of voting systems being compared.

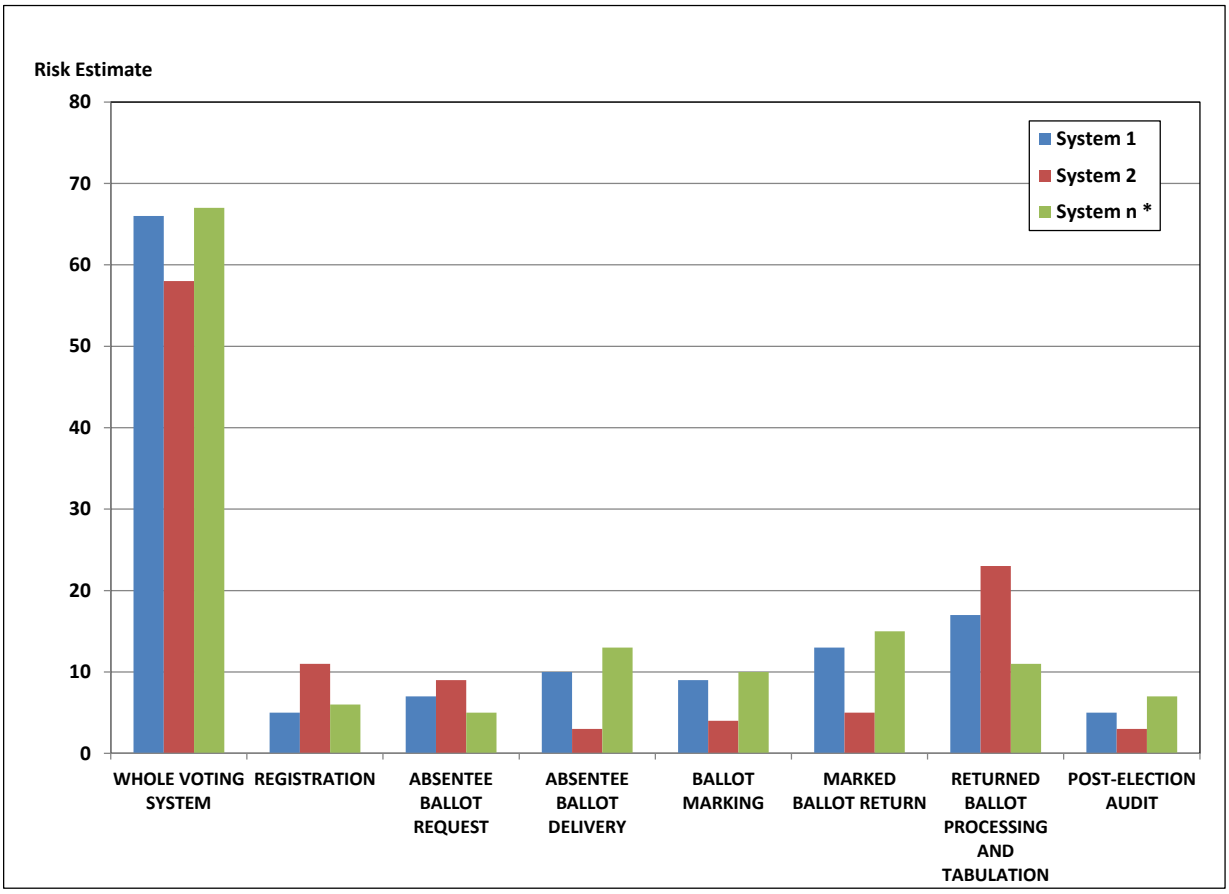


Figure 3.16: Illustration of Risks across Voting Systems by Voting Step
(The risk estimate values depicted are for illustration purposes only and do not reflect actual data)
* n = number of voting systems being compared

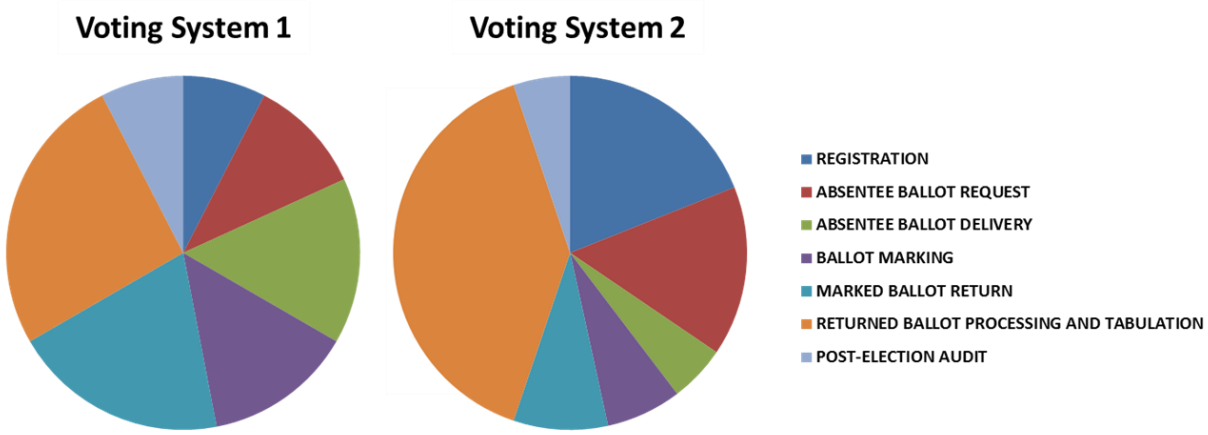


Figure 3.17: Comparison of Risks across Voting Systems by Voting Step
(The risk estimate values depicted are for illustration purposes only and do not reflect actual data)

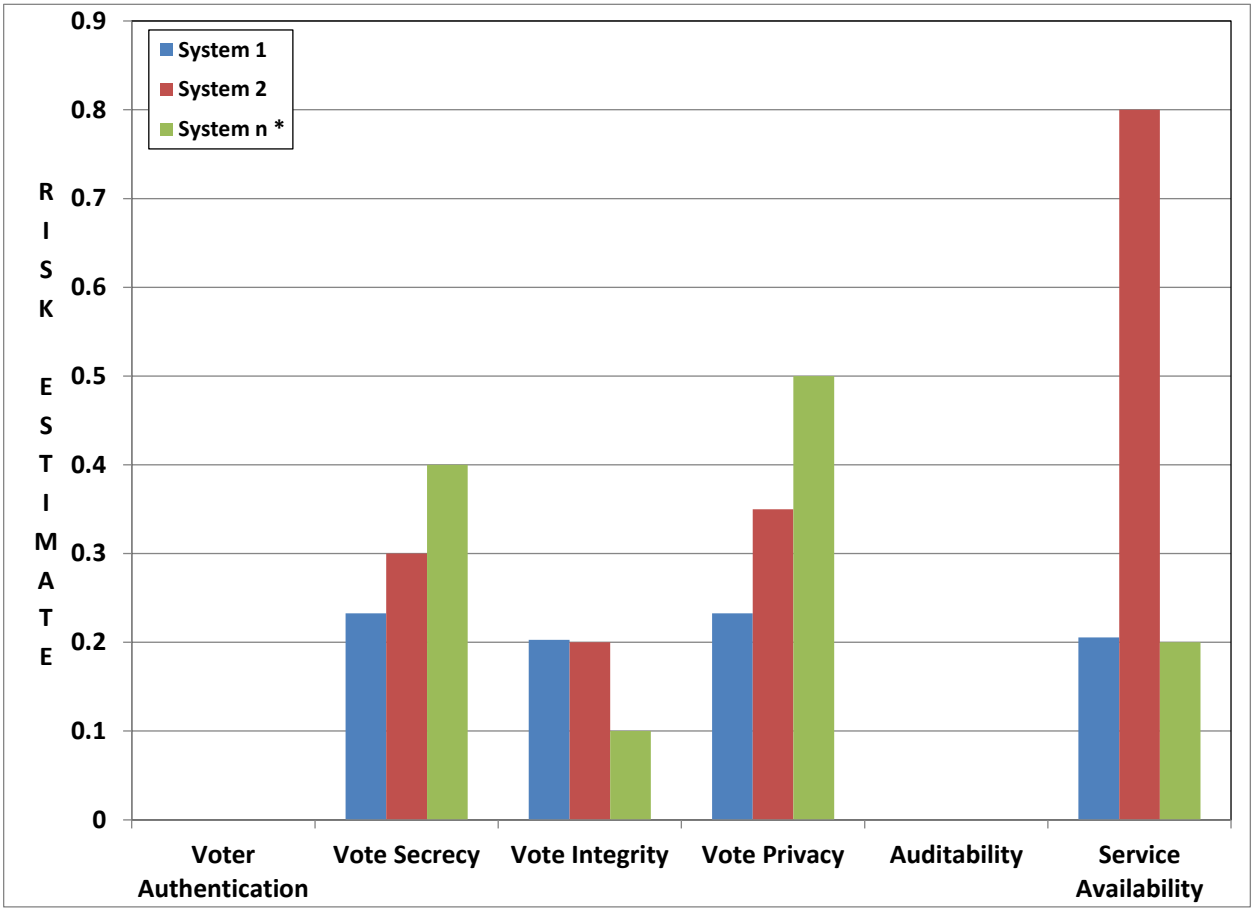


Figure 3.18: Comparison of Risk Estimates per Security Objective

4 Individual Risk Analyses

4.1 Current UOCAVA Voting System

4.1.1 System Definition

The architecture of the current UOCAVA by-mail absentee voting system is illustrated in Figure 4.1 and organized as follows:

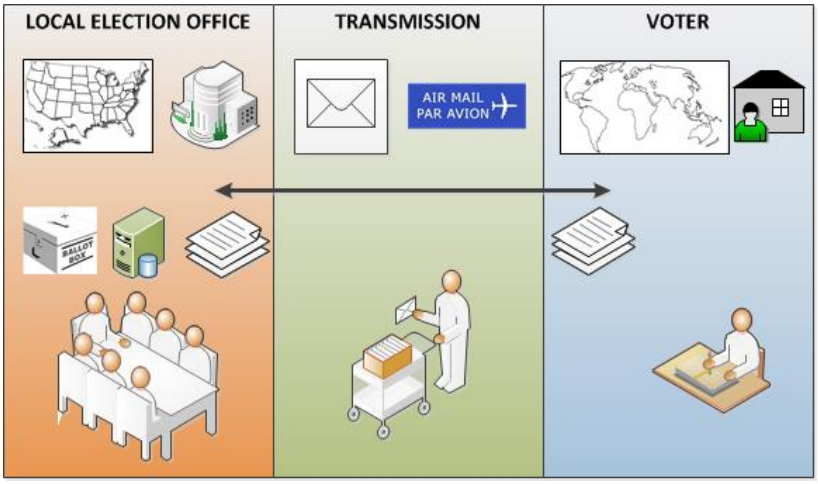


Figure 4.1: Architecture of the Current UOCAVA Voting System

- The voter communicates and submits ballots and forms to the local election office (LEO) via postal mail
- A Voter Registration Database (VRDB) is used for voter registration and ballot request
- The ballots and forms are physical and printed on paper
- The ballots and forms are physically completed and signed by the voter by hand
- The ballots and forms are handled by individuals during postal mail transmission between the LEO and the voter. Transmission involves transport by road and air
- The ballots are processed and tabulated at the LEO by hand
- Post-election audits are conducted by hand

4.1.2 Current UOCAVA Voting Process

The voting process within the current UOCAVA voting system is illustrated in Figure 4.2.

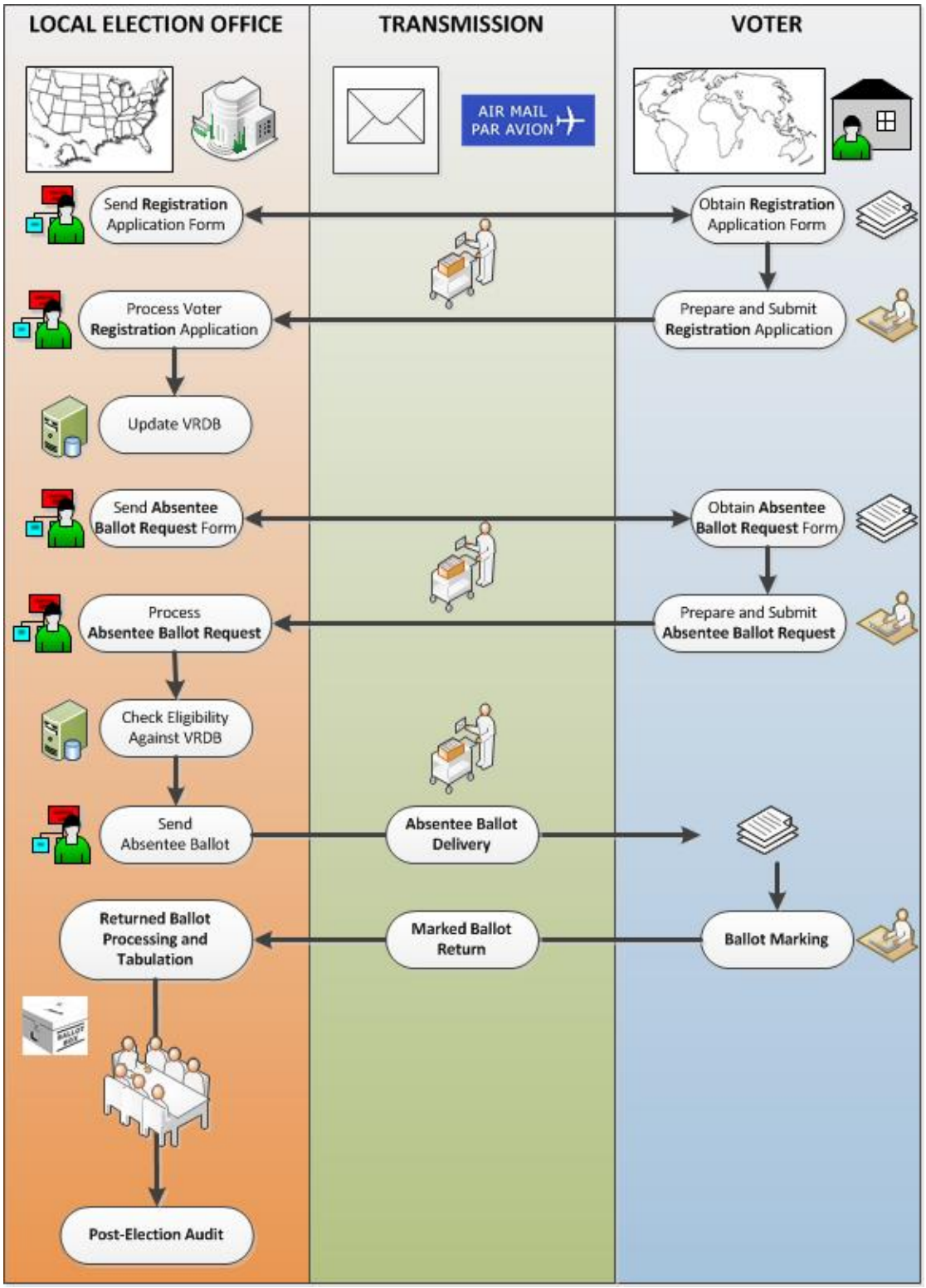


Figure 4.2: Voting Process Within the Current UOCAVA Mail System

4.1.3 Identification of Threats and Vulnerabilities

Specific threats and vulnerabilities associated with the current UOCAVA voting system were identified through an extensive literature review of academic peer-reviewed articles and technical reports from several federal, commercial, and grassroots organizations. The threat vectors and vulnerabilities related to this system are detailed in the voting step threat trees presented in Appendix B, and the vulnerability-threat database (VTDb) presented in Appendix C, respectively.

4.1.4 Quantitative Risk Analysis

4.1.4.1 Questionnaire Inputs and Risk Model Outputs

Inputs to the risk analysis questionnaires presented in Appendix B, were obtained from seven subject matter experts in the cyber security and election communities, and are detailed in Appendix C. These inputs are anonymously indexed as follows:

- Cyber Security Expert 1
- Cyber Security Expert 2
- Cyber Security Expert 3
- Cyber Security Expert 4
- Election Expert 1
- Election Expert 2
- Election Expert 3

These inputs were computed using the model detailed in Section 3.2.2, and the risk model outputs are detailed in Appendix C.

All risk model outputs are summed across all experts to derive a risk estimate for each threat vector and an assignment matrix is built for each security objective, as shown in Appendix C.

4.1.4.2 Rank Ordering of Threats

Risk estimates are first arranged in descending order to determine which threat vectors constitute the greatest risk to the voting system. This arrangement is shown in Figure 4.3 for the current UOCAVA voting system.

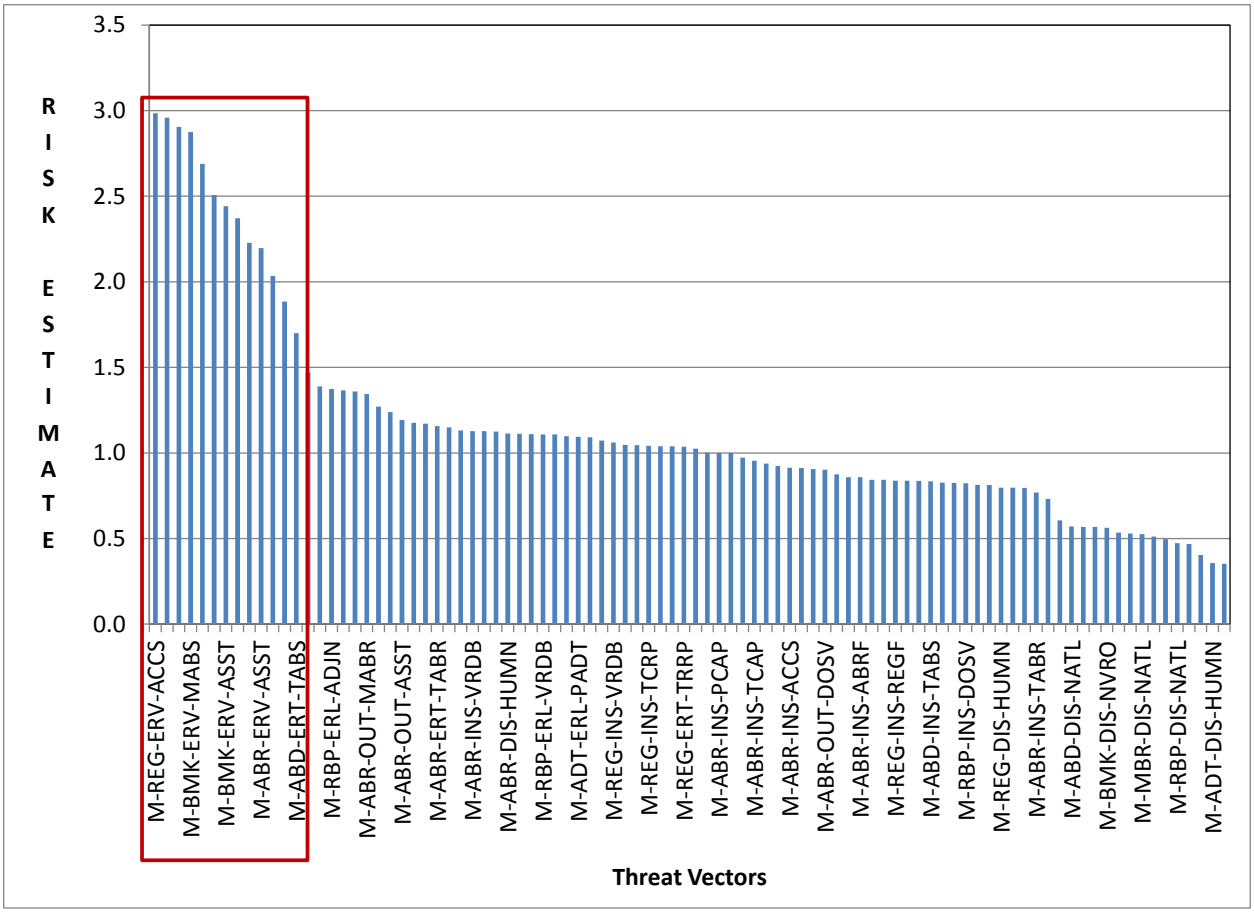


Figure 4.3: Risk Estimates for the Current UOCAVA Voting System

Figure 4.3 shows a group of 13 threat vectors in the upper 50th percentile with risk estimates significantly greater than the remaining 79 threat vectors. These threats, as highlighted above and detailed in Table 4.1 below, represent 14% of the total of 92 threat vectors and yield 30% of the total risk to the UOCAVA voting system. This figure reveals that these main threat vectors are all unintentional errors mainly committed at the voter's location, highlighting the propensity of human error in the current by-mail UOCAVA voting system. This trend is confirmed in Figure 4.4 where threat vectors are grouped at the second level of indentation of the threat tree. The greatest risks are present at the voter's location and during the transmission of election

materials, with the three most important risks to the system during the registration application, the physical marking of the ballot by hand and the request of an absentee ballot by the voter.

Table 4.1: Major Individual Threat Vector for the Current UOCAVA Voting System

Threat Vector				Risk Estimate
Voting Step	**Level 1**	**Level 2**	**Level 3**	
Registration	Unintentional	Error at the Voter's Location	Error in Voting Access	2.985
Registration	Unintentional	Error at the Voter's Location	Error in Registration Application	2.959
Absentee Ballot Request	Unintentional	Error at the Voter's Location	Error in Voting Access	2.905
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Marking the Absentee Ballot	2.874
Absentee Ballot Request	Unintentional	Error at the Voter's Location	Error in Completing the Absentee Ballot Request	2.689
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Voting Access	2.507
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Voter's Assistance	2.442
Marked Ballot Return	Unintentional	Error during Transmission of Election Materials	Error in Transmission of Marked Ballot Packets	2.371
Registration	Unintentional	Error at the LEO	Error in Voter's Assistance	2.228
Absentee Ballot Request	Unintentional	Error at the Voter's Location	Error in Obtaining Voter's Assistance	2.196
Registration	Unintentional	Error at the Voter's Location	Error in Obtaining Voter's Assistance	2.035
Absentee Ballot Request	Unintentional	Error at the LEO	Error in Voter's Assistance	1.884
Absentee Ballot Delivery	Unintentional	Error during Transmission of Election Materials	Errors in Transmission of Absentee Ballot and Instructions	1.700

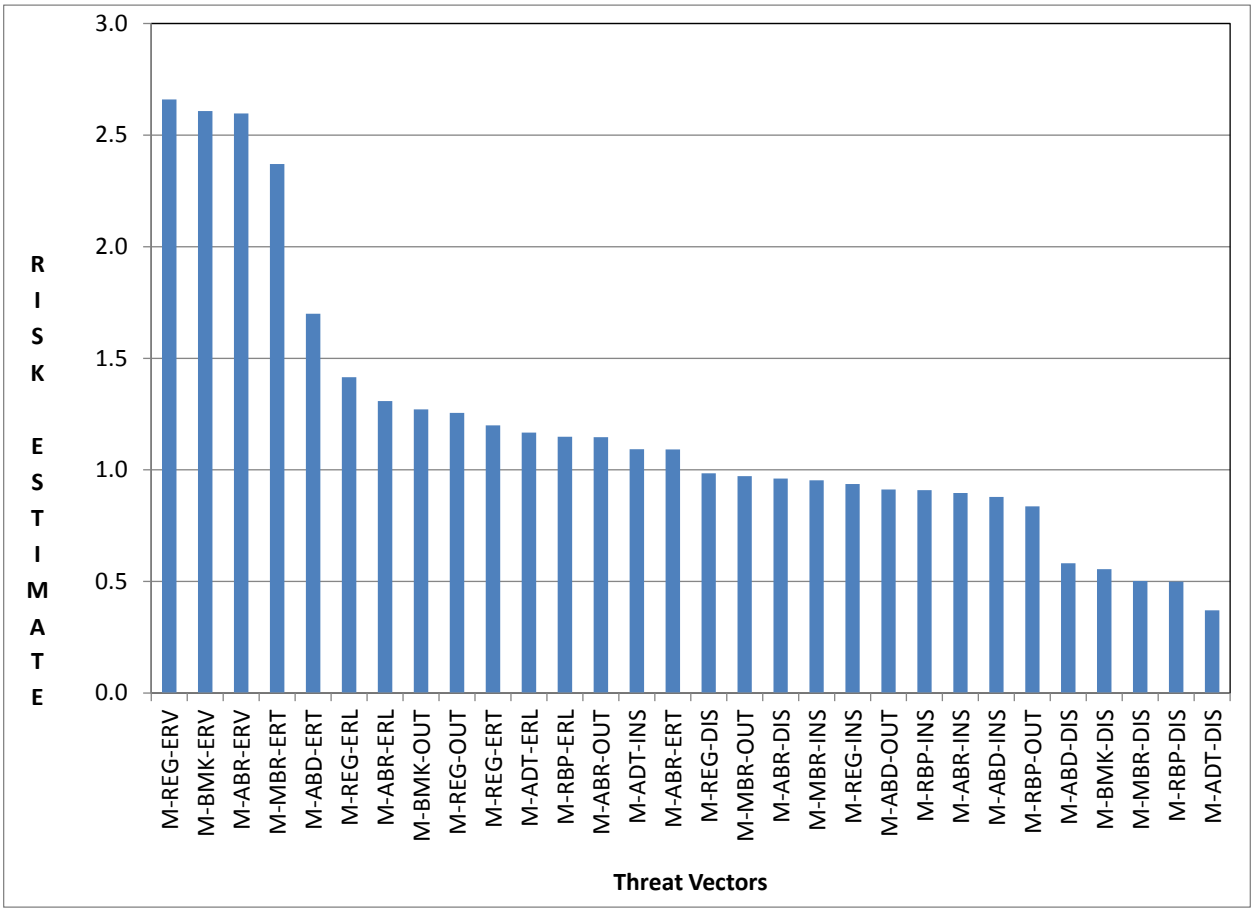


Figure 4.4: Sorted Threat Vectors Categorized at Level 2 for the Current UOCAVA Voting System

4.1.4.3 Analysis By Type of Threats

- **Level 2 Threat Types**
  Level 2 threat types are listed below with their 3-letter identifier, and their corresponding risks estimates are displayed in Figure 4.5 in chronological order by voting step (other key identifiers are listed in Table 3.1).

  - INS: Insider Attack
  - OUT: Outsider Attack
  - ERL: Error at the LEO
  - ERT: Error in Transmission of Election Materials
  - ERV: Error at the Voter's Location
  - DIS: Accidental Disruptions

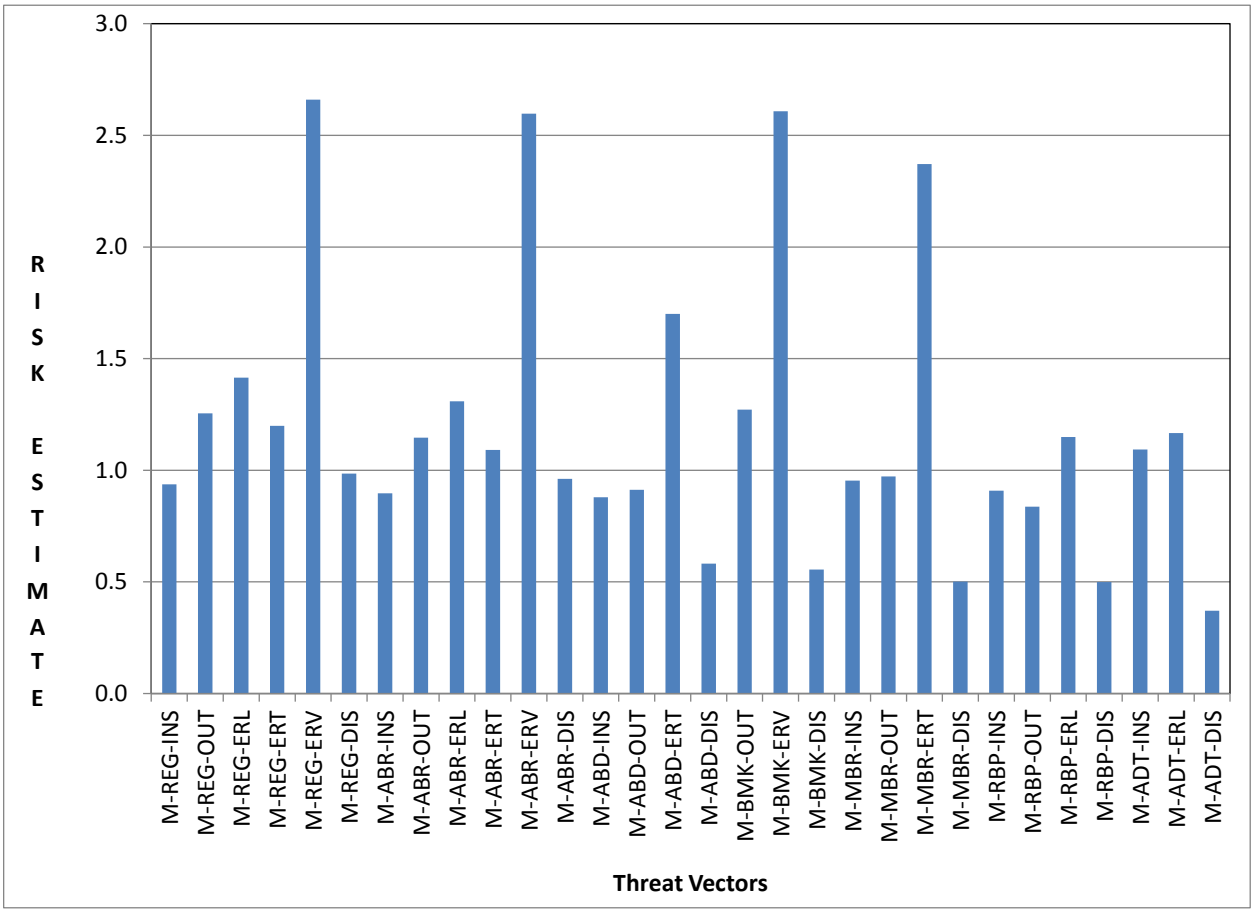


Figure 4.5: Level 2 Threat Vectors for the Current UOCAVA Voting System by Voting Step

These risks estimates can be rolled up across all voting steps to derive the Level 2 risk estimates for the whole system, as shown in Table 4.2, with the risk estimate for "Error at the Voter's Location" two fold greater than the other Level 2 risk estimates.

Table 4.2: Level 2 Risk Estimates for the Current UOCAVA Voting System

Level 2 Threat Vectors	Risk Estimates
Insider Attack	0.926
Outsider Attack	1.104
Error at the LEO	1.292
Error during Transmission of Election Materials	1.320
Error at the Voter's Location	2.636
Accidental Disruptions	0.645

- **Level 1 Threat Types**
  Level 1 threat types are "Attacks" and "Unintentional Disruptions" with risk estimates over the whole voting system of 0.967 and 1.265, respectively. However, since "Unintentional Disruptions" includes both "Errors" and "Accidental Disruptions" that cannot be easily prevented or mitigated, it is more useful to present the data in terms of "Attacks" and "Errors" with associated risk estimates of 0.967 and 1.677, respectively demonstrating the preeminence of unintentional errors in the risks associated with the current UOCAVA voting system.

4.1.4.4 Analysis By Voting Step

This analysis aims at uncovering which voting step contributes the most to the risks associated with the voting system. Threat vectors can be rolled up at the voting step level and reveal that "Ballot Marking" is the voting step with the greatest associated risk, and the post-election audit constitutes the voting step with least associated risk, as illustrated in Figure 4.6.

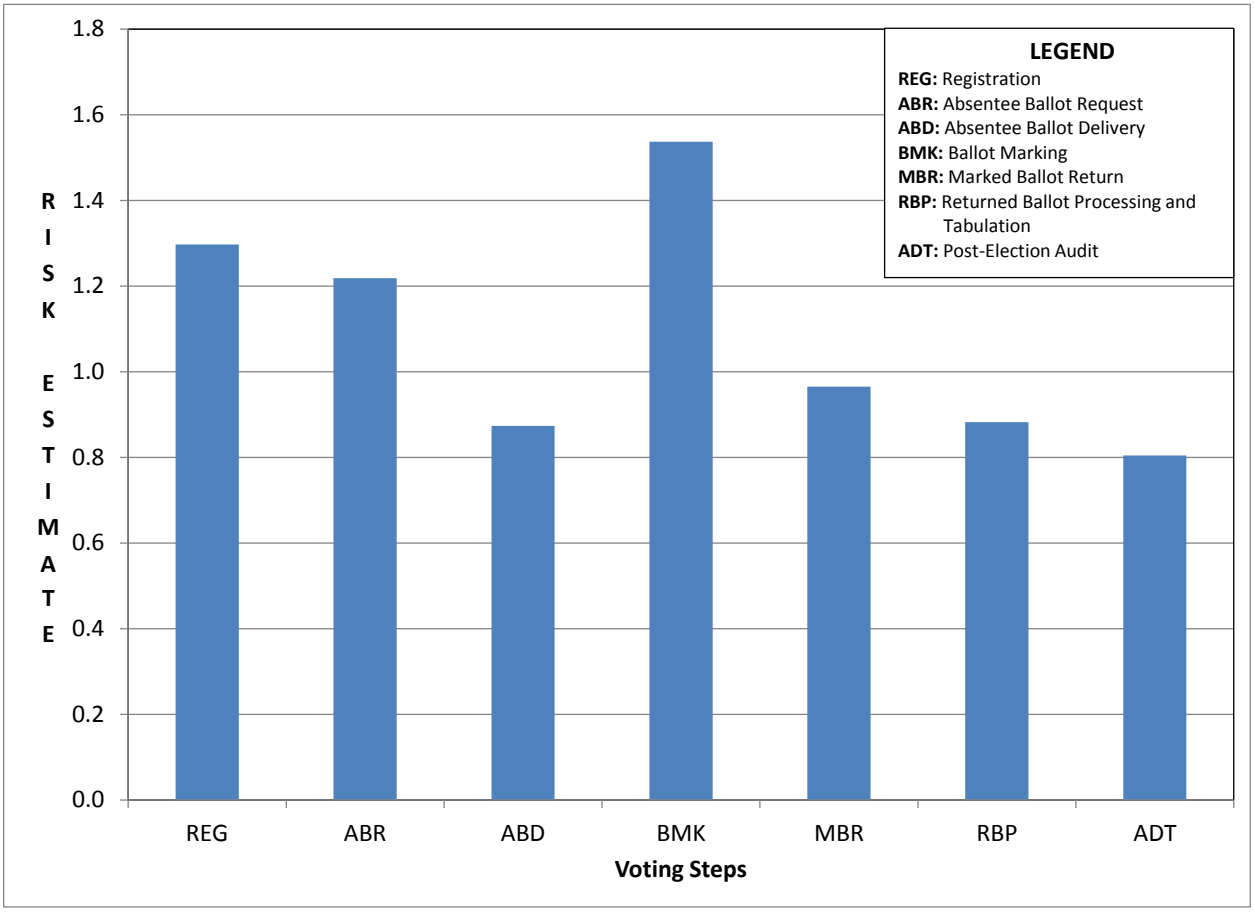


Figure 4.6: Risk Estimates by Voting Step for the Current UOCAVA Voting System

4.1.4.5 Analysis by Security Objective

The risk estimates associated with each security objective for each threat vector are presented in Appendix C. These estimates can be averaged at the second level of indentation of the threat tree by voting step to identify how each category of threat vector is affecting each security objective, as shown on Figure 4.7. A security objective may not be assigned to a threat vector if it is deemed that this threat vector does not impact the security objective, leading to gaps in the following figures.

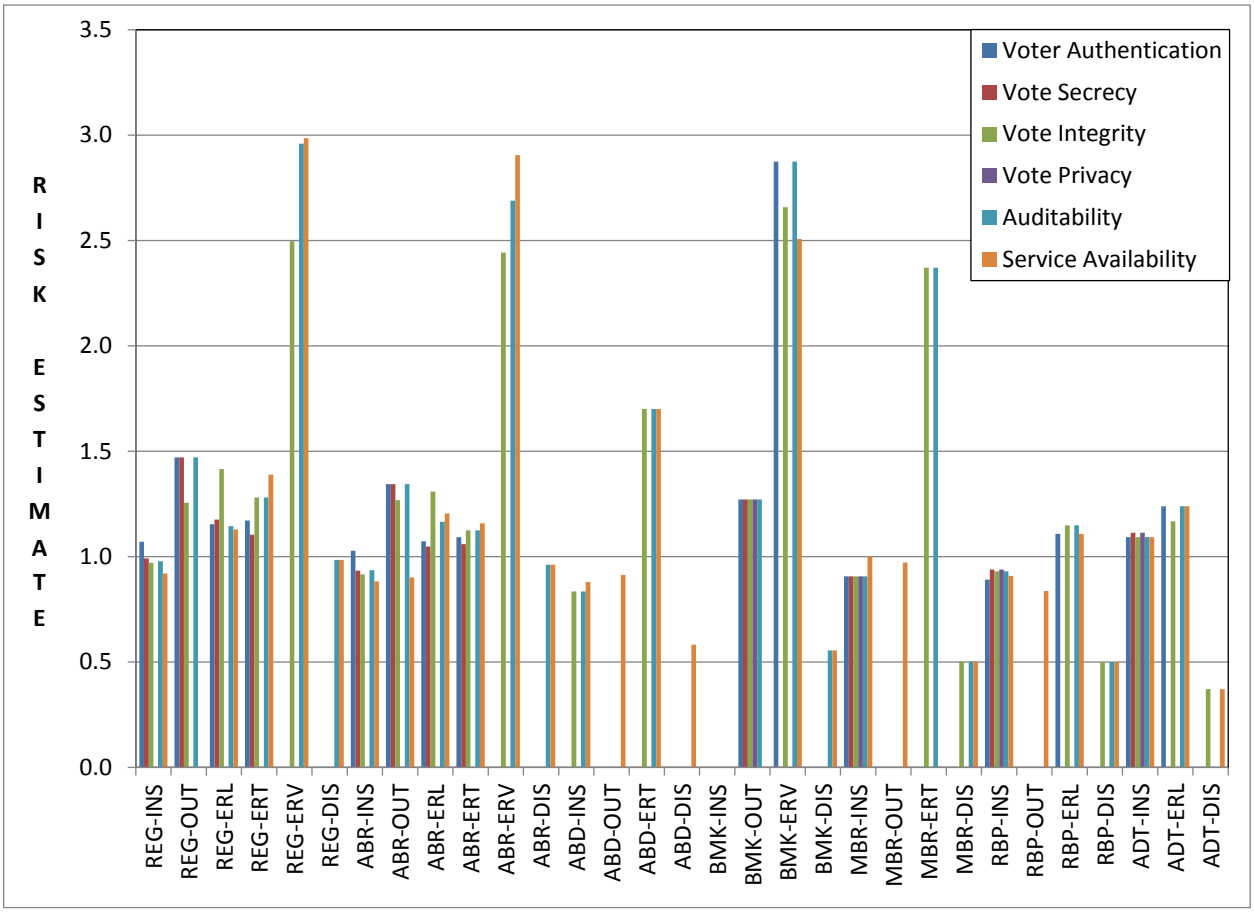


Figure 4.7: Security Risk Estimates for the Current UOCAVA Voting System

By averaging risk estimates over Level 2 threat categories, Figure 4.8 shows that security objectives are most affected by errors at the voter's location.

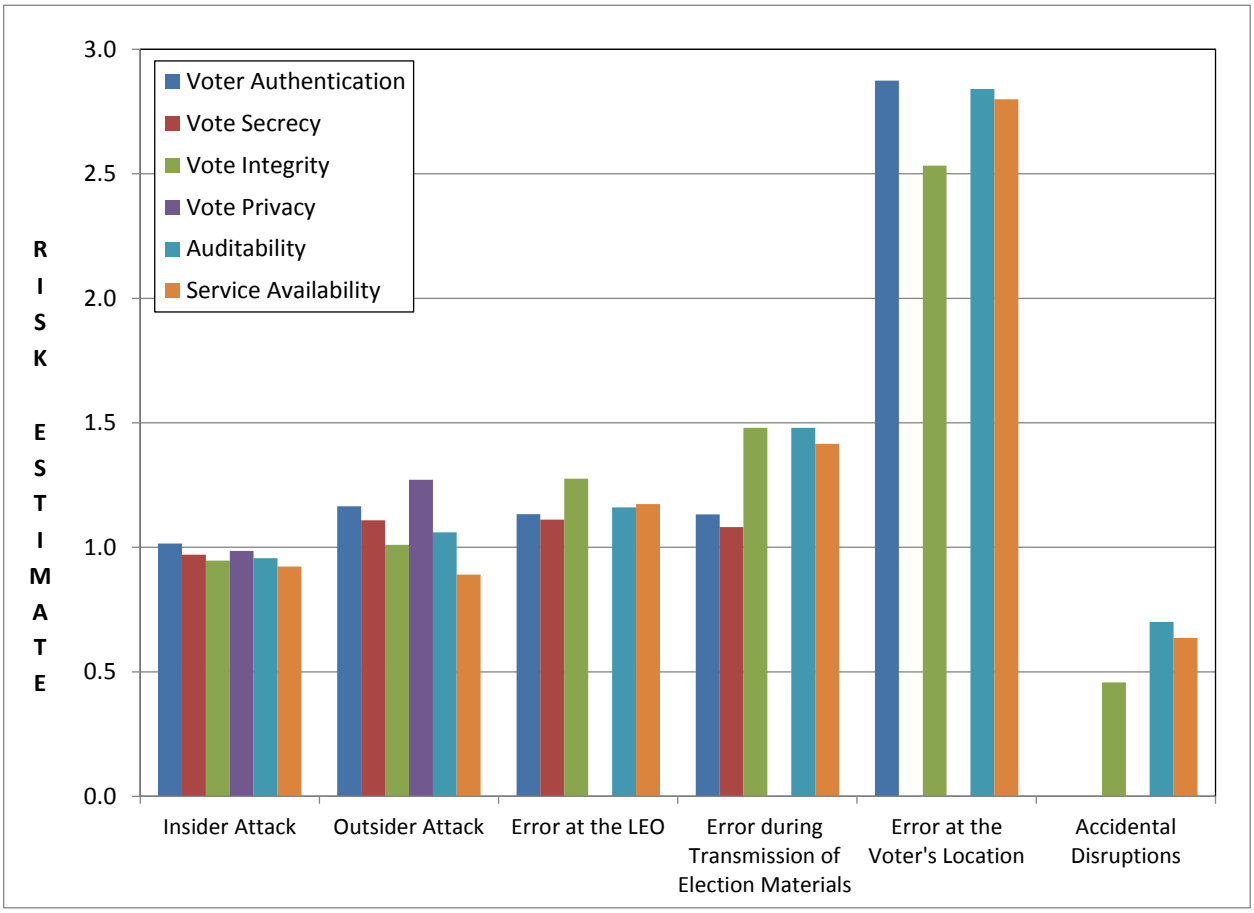


Figure 4.8: Security Risk Estimates by Voting Step for the Current UOCAVA Voting System

4.1.4.6 Summary for the Current UOCAVA Voting System

With regards to the current UOCAVA voting system, the results of the risk analysis demonstrate that unintentional errors constitute the greatest source of risk, as compared to intentional malicious attacks or accidental disruptions. Furthermore, errors at the voter's location appear most preeminent during the physical marking of the absentee ballot, the registration application, and the request of an absentee ballot by the voter.

This analysis emphasizes the areas where mitigation efforts must be focused to reduce the risks associated with the current UOCAVA voting system.

4.2 Remote Electronic Absentee Voting System

4.2.1 System Definition

The architecture of the electronic absentee voting system is illustrated in Figure 4.9 and organized as follows:

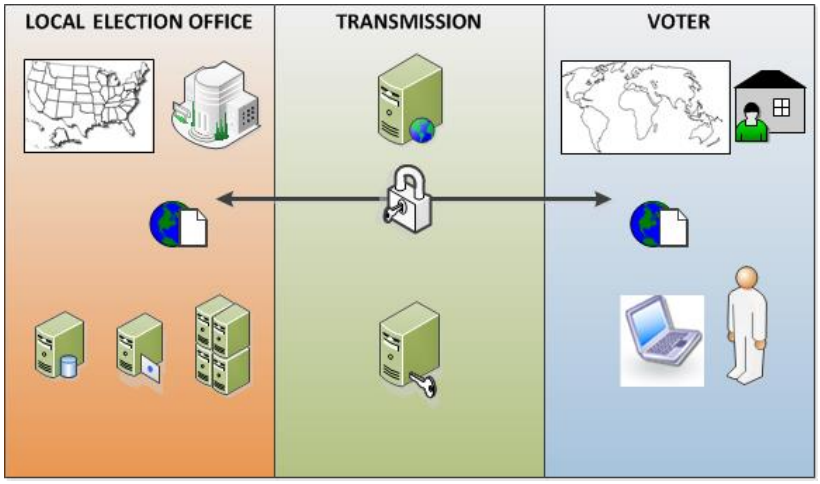


Figure 4.9: Architecture of the Electronic Absentee Voting System

- The voter communicates and submits ballots and forms to the LEO via a secure channel or virtual private network (VPN) on the Internet
- A Voter Registration Database (VRDB) is used for voter registration and ballot request
- The ballots are electronic in nature
- The ballots and forms are digitally completed and signed by the voter after logging in a voting software application running on the World Wide Web (the Web) using unique authentication credentials provided by the LEO
- The ballots and forms are electronically handled by servers and communication channels during transmission on the Internet between the LEO and the voter. Transmission involves transport by international land and satellite communication channels.
- The ballots are electronically processed and tabulated at the LEO on a tabulation server
- Post-election audits are conducted electronically

4.2.2 Remote Electronic Absentee Voting Process

The voting process within the remote absentee electronic voting system is illustrated in Figure 4.10.

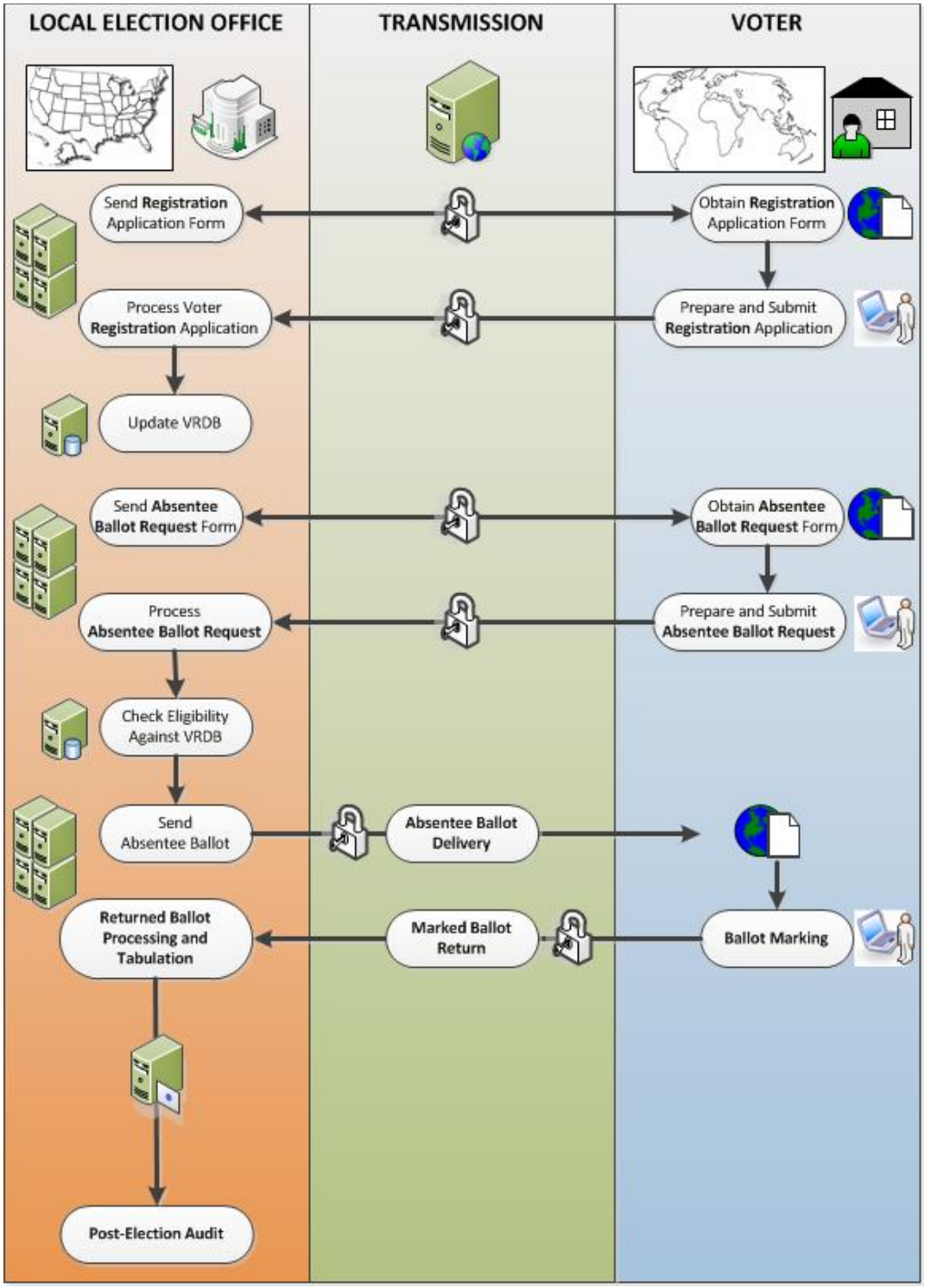


Figure 4.10: Voting Process Within the Electronic Absentee Voting Process

4.2.3 Identification of Threats and Vulnerabilities

Specific threats and vulnerabilities associated with the remote electronic voting system were identified through an extensive literature review of academic peer-reviewed articles and technical reports from several federal, commercial, and grassroots organizations. The threat vectors and vulnerabilities related to this system are detailed in the voting step threat trees presented in Appendix B, and the vulnerability-threat database (VTDb) presented in Appendix C, respectively.

4.2.4 Quantitative Risk Analysis

4.2.4.1 Questionnaire Inputs and Risk Model Outputs

Inputs to the risk analysis questionnaires presented in Appendix B, were obtained from seven subject matter experts in the cyber security and election communities, and are detailed in Appendix C. These inputs are anonymously indexed as follows:

- Cyber Security Expert 1
- Cyber Security Expert 2
- Cyber Security Expert 3
- Cyber Security Expert 4
- Election Expert 1
- Election Expert 2
- Election Expert 3

These inputs were computed using the model detailed in Section 3.2.2, and the risk model outputs are detailed in Appendix C.

All risk model outputs are summed across all experts to derive a risk estimate for each threat vector and an assignment matrix is built for each security objective, as shown in Appendix C.

4.2.4.2 Rank Ordering of Threats

Risk estimates are first arranged in descending order to determine which threat vectors constitute the greatest risk to the voting system. This arrangement is shown in Figure 4.11 for the remote electronic absentee voting system.

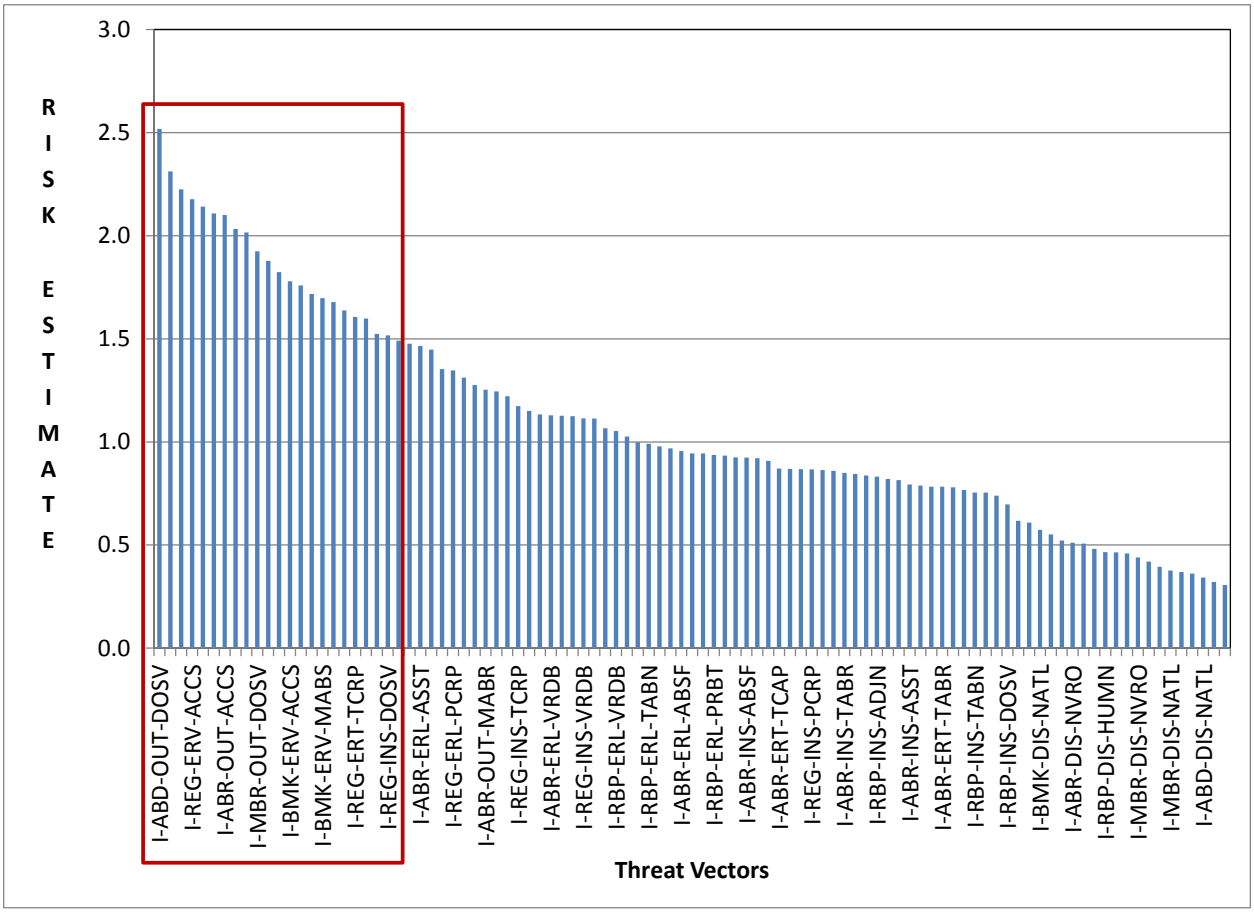


Figure 4.11: Risk Estimates for the Remote Electronic Absentee Voting System

Figure 4.11 shows a pattern of risks with accidental disruption of the post-election audit by a natural event exhibiting the least risk, and outsider attacks by denial of service during the "absentee ballot delivery" voting step constituting the source of greatest single risk to the remote electronic absentee voting system. As a parallel to the individual analysis of the current UOCAVA voting system, Figure 4.11 shows a group of 16 threat vectors, or 16% of the total of 99 threat vectors, yielding 30% of the total risk to the electronic voting system. These threats, as highlighted above and detailed in Table 4.3 below show that denial of service by malicious outsiders presents the most important risk to the system during the voting process, along with

unintentional errors at the voter's location in preparing the registration application, completing the absentee ballot request, obtaining access to the voting system and marking the absentee ballot. Specific to an online voting scenario, phishing attacks are also preeminent.

Table 4.3: Major Individual Threat Vector of the Remote Electronic Absentee Voting System

Threat Vector				Risk Estimate
Voting Step	**Level 1**	**Level 2**	**Level 3**	
Absentee Ballot Delivery	Attacks	Outsider Attack	Attack by Denial of Service	2.518
Absentee Ballot Request	Attacks	Outsider Attack	Attack by Denial of Service	2.312
Absentee Ballot Delivery	Attacks	Outsider Attack	Attack to Voting Access - Phishing Attack	2.225
Registration	Unintentional	Error at the Voter's Location	Error in Voting Access	2.177
Returned Ballot Processing and Tabulation	Attacks	Outsider Attack	Attack by Denial of Service	2.141
Registration	Unintentional	Error at the Voter's Location	Error in Registration Application	2.108
Absentee Ballot Request	Attacks	Outsider Attack	Attack to Voting Access - Phishing Attack	2.100
Absentee Ballot Request	Unintentional	Error at the Voter's Location	Error in Voting Access	2.032
Registration	Attacks	Outsider Attack	Attacks Against Marking of Registration Forms	2.016
Marked Ballot Return	Attacks	Outsider Attack	Attack by Denial of Service	1.924
Absentee Ballot Request	Unintentional	Error at the Voter's Location	Error in Completing the Absentee Ballot Request	1.878
Registration	Unintentional	Error at the Voter's Location	Error in Obtaining Voter's Assistance	1.824
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Voting Access	1.779
Marked Ballot Return	Attacks	Outsider Attack	Attack to Voting Access - Phishing Attack	1.759
Registration	Unintentional	Error at the LEO	Error in Registration and Instruction Forms	1.718
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Marking the Absentee Ballot	1.697

threat vectors exclusively specific to a remote electronic absentee voting scenario

This trend is confirmed in Figure 4.12 where threat vectors are grouped by the second level of indentation of the threat tree. The risk estimates yielding 30% of the total risk to the electronic voting system are composed by outsider attacks against the delivery of absentee ballots to the voters, the processing and tabulation of returned ballots, the return of marked ballots, and the request of absentee ballots. Unintentional errors at the voter's location are also included in this group with most preeminent errors during the registration application and the request of an absentee ballot by the voter.

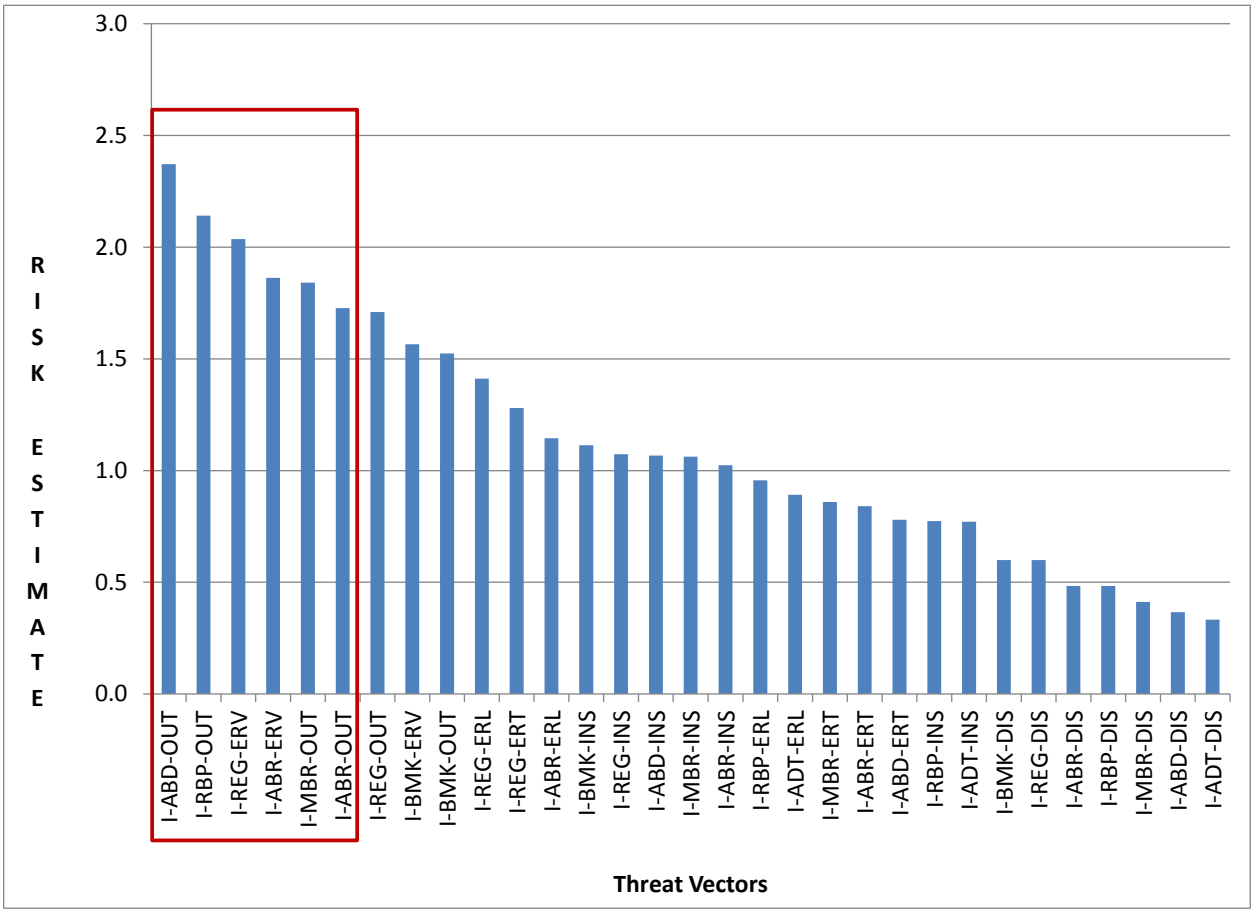


Figure 4.12: Sorted Threat Vectors Categorized at Level 2 for the Current UOCAVA Voting System

4.2.4.3 Analysis By Type of Threats

- **Level 2 Threat Types**
  Level 2 threat types are listed below with their 3-letter identifier, and their corresponding risks estimates are displayed in Figure 4.13 in chronological order by voting step (other key identifiers are listed in Table 3.1).

  - INS: Insider Attack
  - OUT: Outsider Attack
  - ERL: Error at the LEO
  - ERT: Error in Transmission of Election Materials
  - ERV: Error at the Voter's Location
  - DIS: Accidental Disruptions

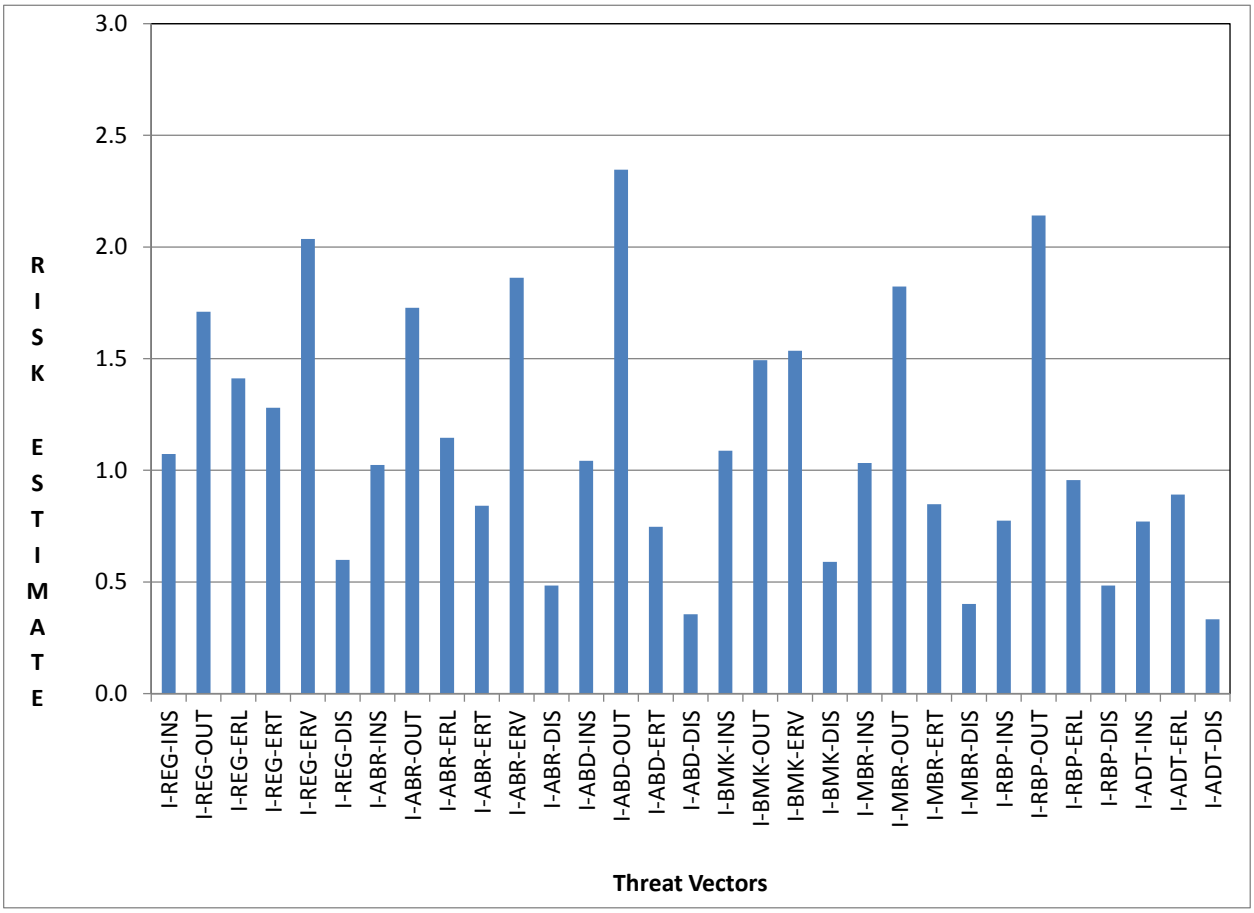


Figure 4.13: Level 2 Threat Vectors for the Remote Electronic Absentee Voting System by Voting Step

These risks estimates can be rolled up across all voting steps to derive the Level 2 risk estimates for the whole system, as shown in Table 4.4, with the risk estimates for "Outsider Attack" and "Error at the Voter's Location" 36 to 73% greater than the other Level 2 risk estimates.

Table 4.4: Level 2 Risk Estimates for the Remote Electronic Absentee Voting System

Level 2 Threat Vectors	Risk Estimates
Insider Attack	0.993
Outsider Attack	1.856
Error at the LEO	1.169
Error during Transmission of Election Materials	1.032
Error at the Voter's Location	1.827
Accidental Disruptions	0.485

- **Level 1 Threat Types**
  Level 1 threat types are "Attacks" and "Unintentional Disruptions" with risk estimates over the whole voting system of 1.237 and 0.966, respectively. However, since "Unintentional Disruptions" includes both "Errors" and "Accidental Disruptions" that cannot be easily prevented or mitigated, it is more useful to present the data in terms of "Attacks" and "Errors" with associated risk estimates of 1.237 and 1.293, respectively, demonstrating that the source of risk to the remote electronic absentee voting system is equally related to both intentional and malicious actions, i.e. attacks, and unintentional actions via human errors by the voter.

4.2.4.4 Analysis By Voting Step

This analysis aims at uncovering which voting step contributes the most to the risks associated with the voting system. Threat vectors can be rolled up at the voting step level and reveal that "Registration" is the voting step with the greatest associated risk, and "Post-Election Audit" constitutes the voting step with the least associated risk to the remote electronic absentee voting system, as illustrated in Figure 4.14.

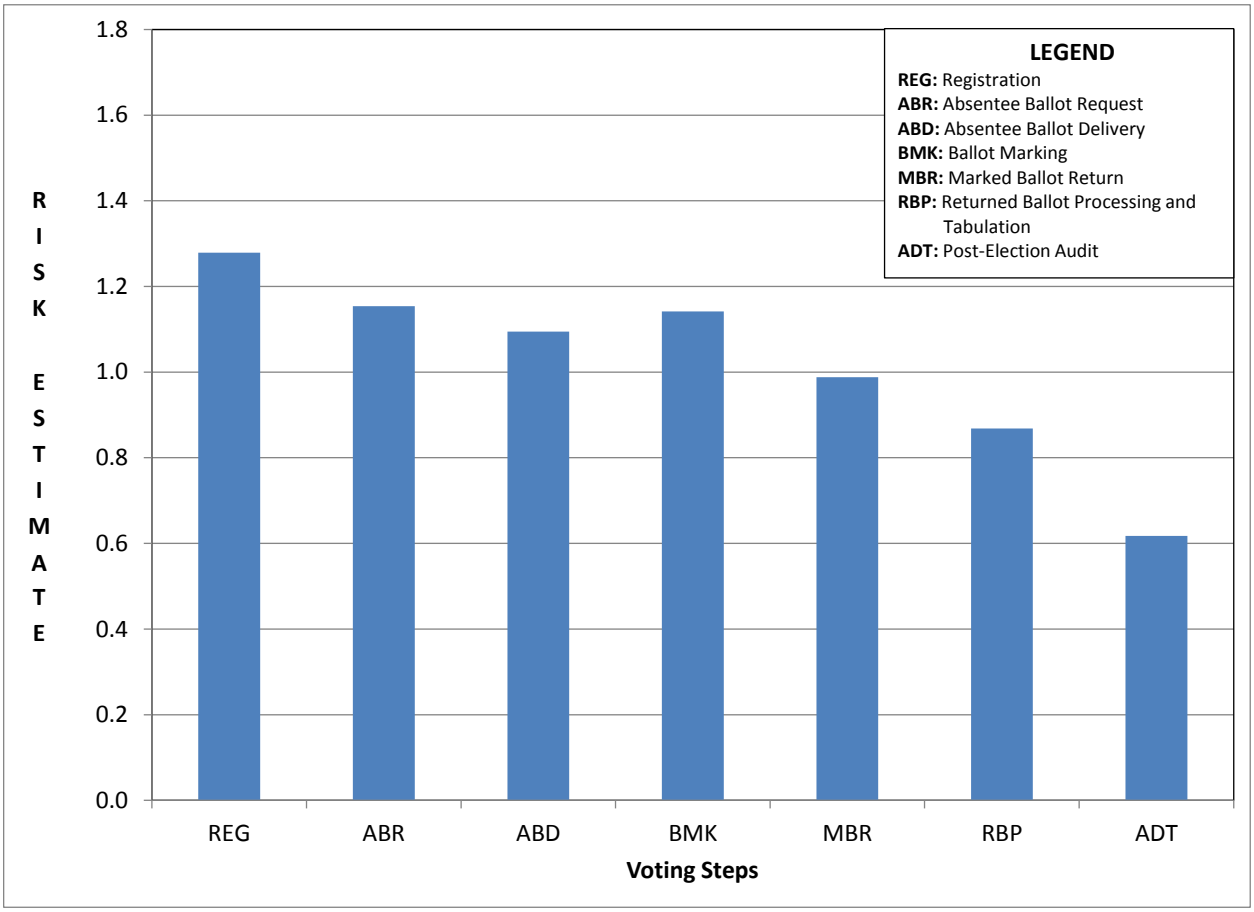


Figure 4.14: Risk Estimates by Voting Step for the Remote Electronic Absentee Voting System

4.2.4.5 Analysis by Security Objective

The risk estimates associated with each security objective for each threat vector are presented in Appendix C. These estimates can be averaged at the second level of indentation of the threat tree by voting step to identify how each category of threat vector is affecting each security objective, as shown in Figure 4.15. A security objective may not be assigned to a threat vector if it is

deemed that this threat vector does not impact the security objective, leading to gaps in the following figures.

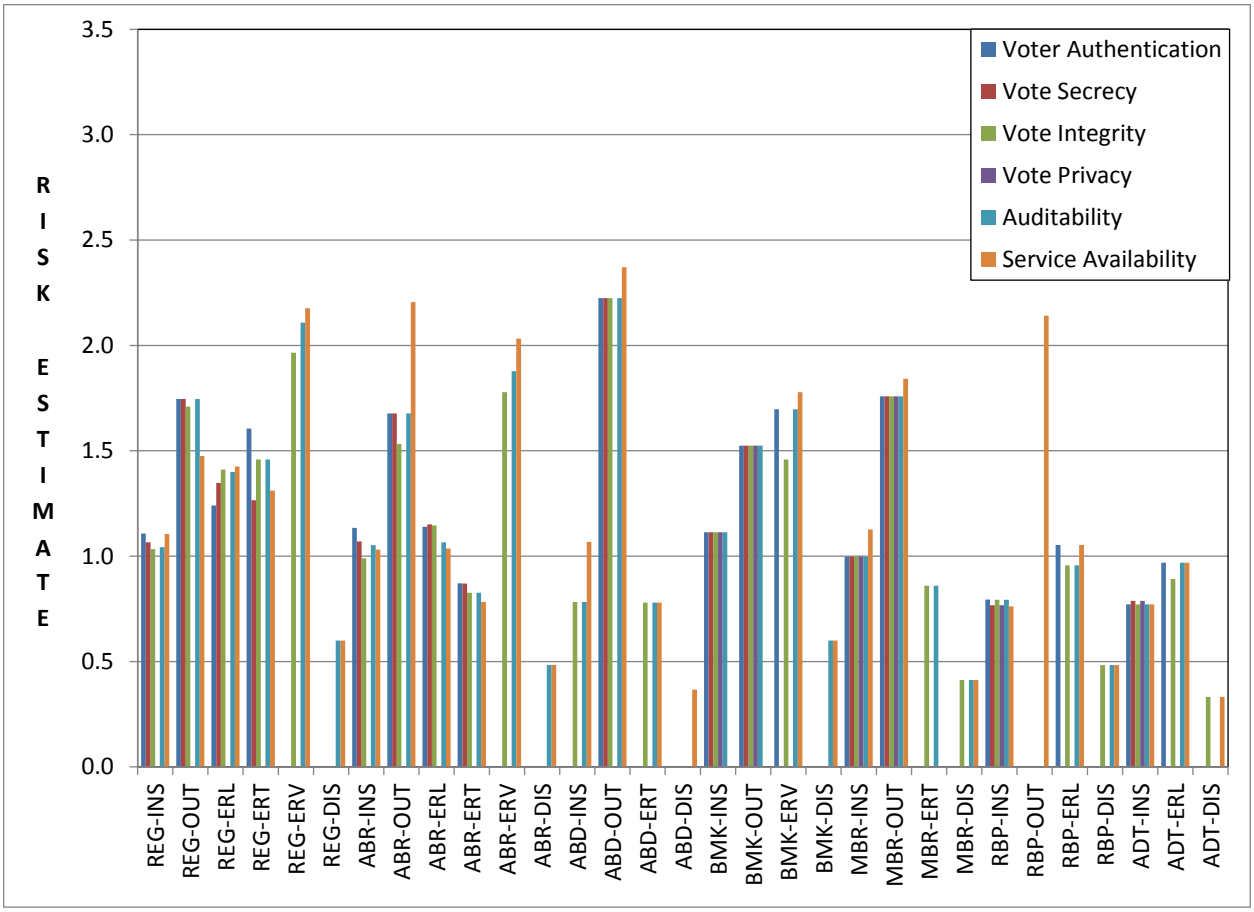


Figure 4.15: Security Risk Estimates for the Remote Electronic Absentee Voting System

By averaging risk estimates over Level 2 threat categories, Figure 4.16 shows that security objectives are most affected by errors at the voter's location, and attacks by malicious outsiders.

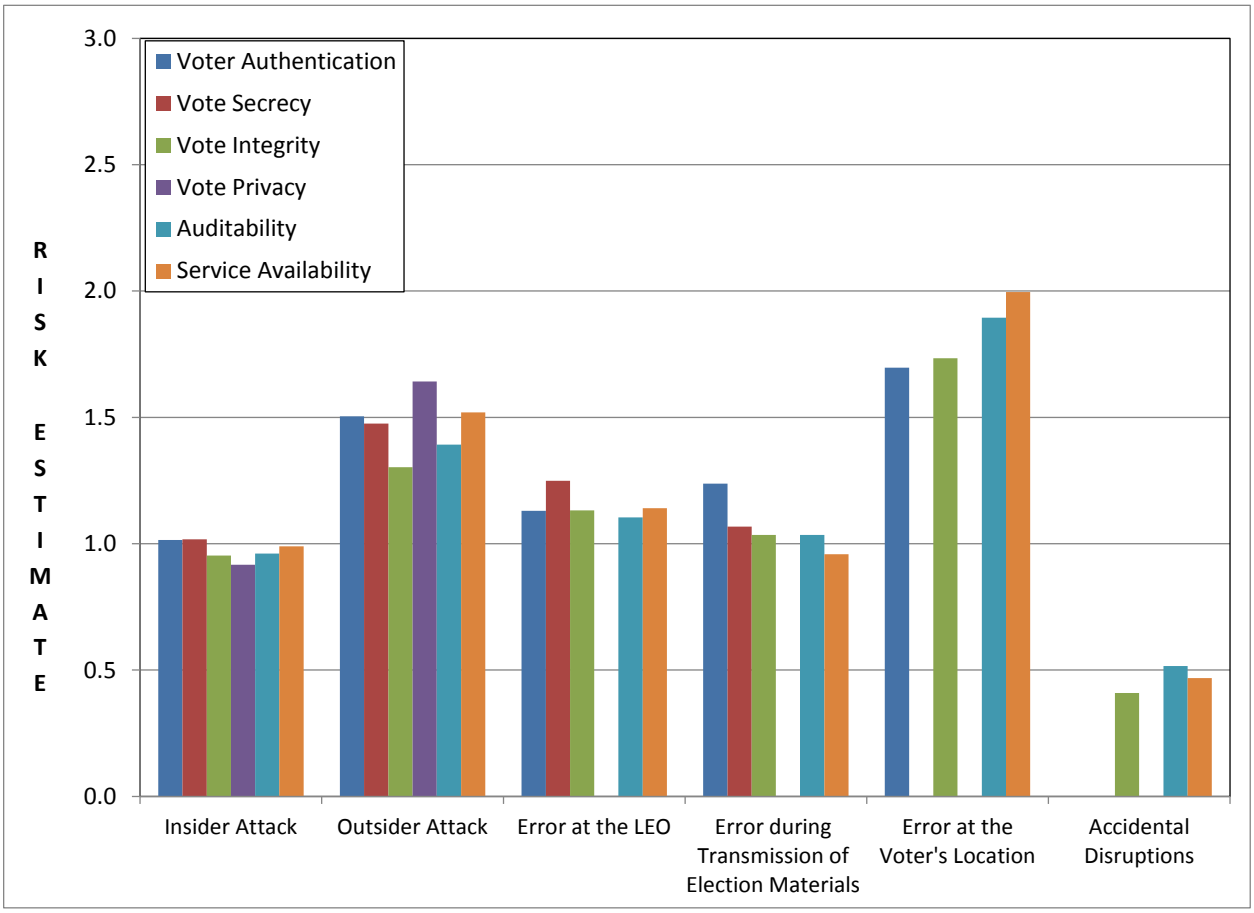


Figure 4.16: Security Risk Estimates by Voting Step for the Remote Electronic Absentee Voting System

4.2.4.6 Summary for the Remote Absentee Electronic Voting System

With regards to the remote electronic absentee voting system, the results of the risk analysis demonstrate that the system is equally subjected to unintentional human errors and architecture-specific threats by malicious outsiders (e.g. denial of service).

This analysis emphasizes the areas where mitigation efforts must be focused to reduce the risks associated with the remote electronic absentee voting system described in this report.

5 Comparative and Quantitative Risk Analysis

The purpose for this analysis is two-fold. First, it aims at resolving the inherent risks of the current UOCAVA voting system, which have not been previously addressed in a systematic fashion. Second, it uses the risk analysis of the current by-mail system as a baseline and reference for comparison with a theoretical remote electronic absentee voting system, which architecture is modeled on currently commercially available online voting solutions, as described on Figure 4.9. Similarly to individual voting system analysis, the comparative analysis draws on the computation of inputs to risk analysis questionnaires completed by subject matter experts listed in Section 4. However, the process of rolling up risk estimates to higher levels is different between the two types of analysis. Individual system analysis aims at comparing the risks associated with different threat vectors within one voting system, and comparative analysis aims at revealing differences or similarities between the risks associated with threat vectors or groups of threat vectors across voting systems. As a result, risk estimates under Level 1 and 2 threat vectors are summed instead of averaged to allow comparison of risks across voting systems. Furthermore, the risk estimates derived for each voting system and described in this section should not be compared with the risk estimates discussed in Section 4. Detailed information regarding the rationale for this calculation process is provided in Section 3.7.

5.1 Dataset Statistical Analysis

In this section, the whole dataset of risk estimates is examined for both systems under consideration and statistical analysis is performed to derive general observations on the behavior of the data. The results of the statistical analysis are detailed in Appendix C, while the main conclusions are presented hereafter.

The current UOCAVA voting system exhibits greater risk estimates with greater minimum, maximum, and sum values than its electronic alternative.

Figure 5.1 illustrates the relative behavior of the datasets with each other.

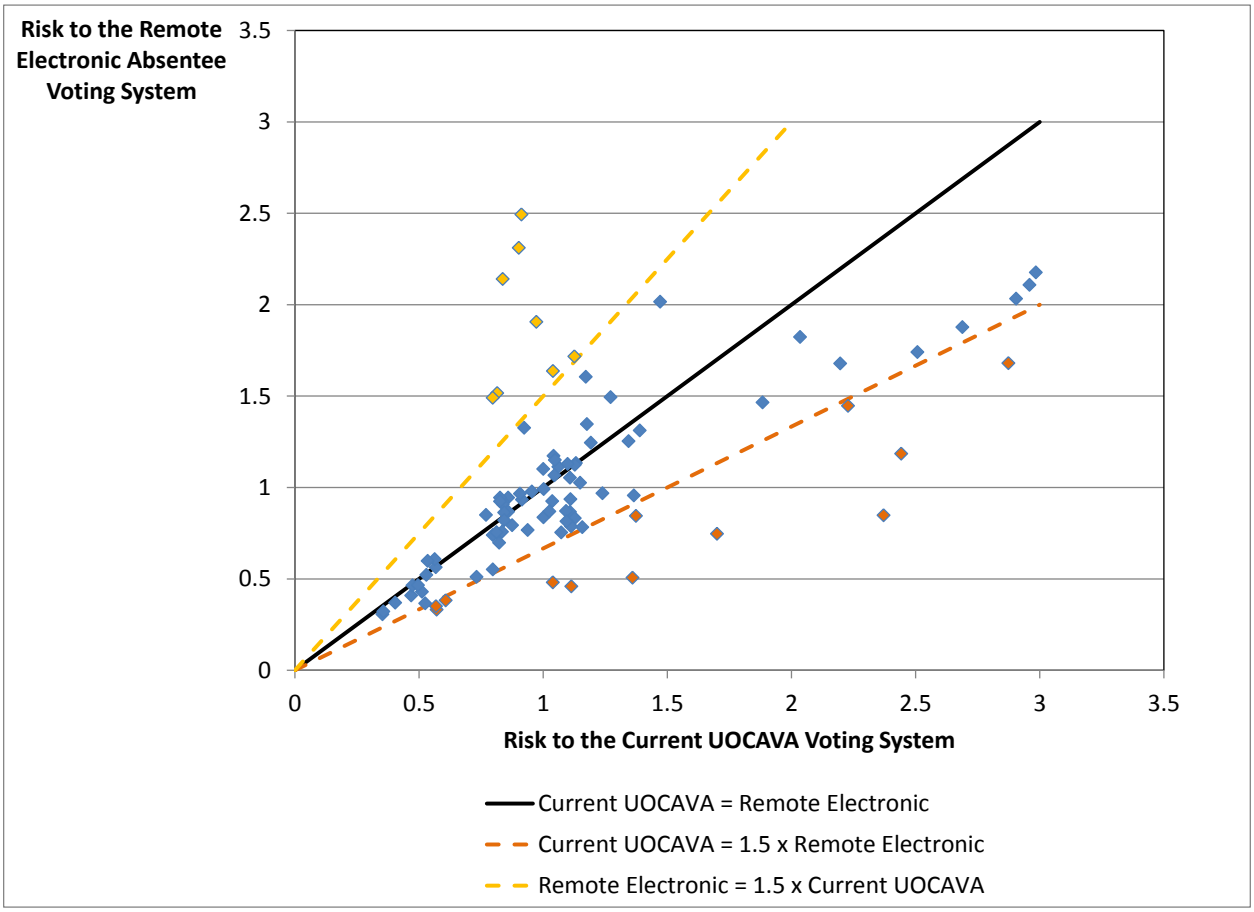


Figure 5.1: Plot of the Comparison of Risk Estimates between Voting Systems

In addition, several threat vectors stand out with risk estimates significantly different from one system to another. The yellow diamonds highlight threat vectors that exhibit lower risk estimates in the current UOCAVA voting system and higher risk estimates in the electronic alternative. The orange diamonds highlight the opposite behavior. All other threat vectors exhibit similar risk estimates from one system to another (i.e. their respective data points are close to the black identity line on Figure 5.1). These threat vectors are detailed in Table 5.1 and discussed further below. The first category corresponding to risks significantly greater for the remote electronic voting system is dominated by denial of service attacks, which are intrinsically linked to the specific architecture of the remote absentee voting system. The second category exhibits mainly unintentional errors, preeminent in the current by-mail UOCAVA voting system, and also shows that this by-mail system is more susceptible to accidental disruptions from unexpected events. These observations confirm that the specific architecture of a voting system has a direct impact on the nature of the risks it will experience. It also highlights that the current

UOCAVA voting system is more prone to unintentional human errors while its electronic counterparts is more subjected to intentional attacks by malicious individuals. These observations support empirical observations made by the election community on both system's architectures, and validate the original risk analysis framework developed for the comparative analysis of voting systems.

Table 5.1: Threat Vectors with Different Risk Estimates across Voting Systems

Threat Vector				Risk Estimate	
Voting Step	Level 1	Level 2	Level 3	Current UOCAVA Voting System	Remote Electronic Absentee Voting System
Absentee Ballot Delivery	Attacks	Outsider Attack	Attack by Denial of Service	0.912	2.494
Absentee Ballot Request	Attacks	Outsider Attack	Attack by Denial of Service	0.901	2.312
Returned Ballot Processing and Tabulation	Attacks	Outsider Attack	Attack by Denial of Service	0.836	2.141
Marked Ballot Return	Attacks	Outsider Attack	Attack by Denial of Service	0.972	1.907
Registration	Unintentional	Error at the LEO	Error in Registration and Instruction Forms	1.125	1.718
Registration	Attacks	Outsider Attack	Attack to Voting Assistance	1.039	1.638
Registration	Attacks	Insider Attack	Attack by Denial of Service	0.814	1.517
Absentee Ballot Request	Attacks	Insider Attack	Attack by Denial of Service	0.796	1.491
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Marking the Absentee Ballot	2.874	1.681
Ballot Marking	Unintentional	Error at the Voter's Location	Error in Obtaining Voter's Assistance	2.442	1.185
Marked Ballot Return	Unintentional	Error during Transmission of Election Materials	Error in Transmission of Marked Ballot Packets	2.371	0.848
Registration	Unintentional	Error at the LEO	Error in Voter's Assistance	2.228	1.447
Absentee Ballot Delivery	Unintentional	Error during Transmission of Election Materials	Errors in Transmission of Absentee Ballot and Instructions	1.700	0.747
Returned Ballot Processing and Tabulation	Unintentional	Accidental Disruption	Error in Adjudication	1.373	0.845
Registration	Unintentional	Accidental Disruption	Disruption by a Natural Event	1.360	0.507
Absentee Ballot Request	Unintentional	Accidental Disruption	Disruption by a Human-Created Collateral Event	1.113	0.459
Absentee Ballot Request	Unintentional	Accidental Disruption	Disruption by a Natural Event	1.039	0.481
Absentee Ballot Delivery	Unintentional	Accidental Disruption	Disruption by an Environmental Event	0.607	0.383
Absentee Ballot Delivery	Unintentional	Accidental Disruption	Disruption by a Natural Event	0.570	0.332
Absentee Ballot Delivery	Unintentional	Accidental Disruption	Disruption by a Human-Created Collateral Event	0.568	0.351

Risks associated with the remote absentee electronic voting system >= 1.5 x Risks associated with the current UOCAVA voting system

Risks associated with the current UOCAVA voting system >= 1.5 x Risks associated with the remote absentee electronic voting system

5.2 Comparative Analysis by Type of Threats

5.2.1 Level 2 Threat Type

Level 2 threats types are listed below with their 3-letter identifier, and their corresponding risks estimates are displayed in in chronological order by voting step on Figure 5.2. This figure shows that insider attacks during the registration and absentee ballot request voting steps exhibit the greatest risk estimates to both voting systems while the current UOCAVA voting system displays greater risk estimates from errors at the voter's location than its electronic alternative.

- INS: Insider Attack
- OUT: Outsider Attack
- ERL: Error at the LEO
- ERT: Error in Transmission of Election Materials
- ERV: Error at the Voter's Location
- DIS: Accidental Disruptions

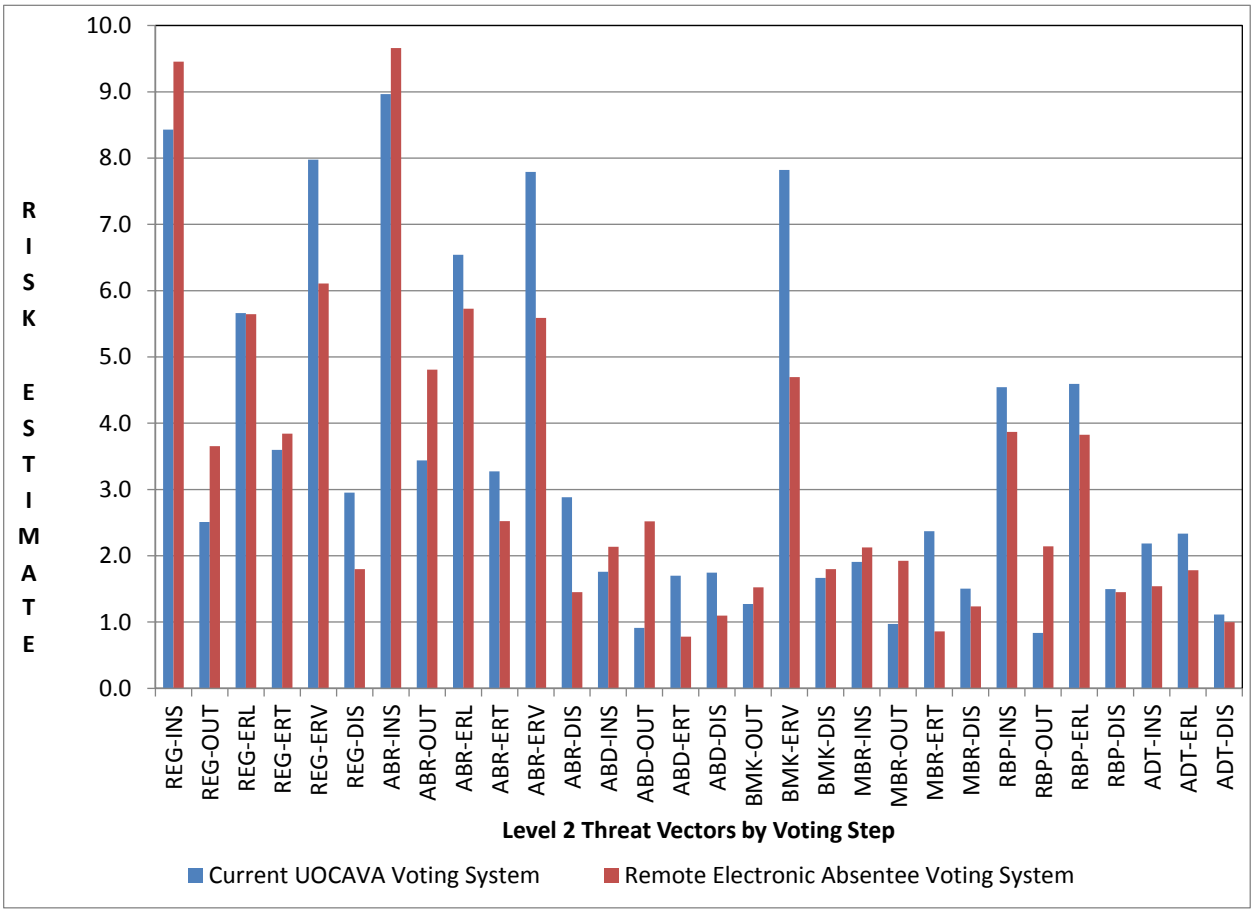


Figure 5.2: Comparison of Level 2 Threat Vectors across Voting Systems by Voting Step

These risks estimates can be rolled up across all voting steps to derive the Level 2 risk estimates for the whole system, as shown in Table 5.2. It shows that the current UOCAVA voting system is more prone to insider attacks and errors at the voter's location while its electronic counterpart exhibits greater risks from attacks and errors at the LEO and at the voter's location.

Table 5.2: Comparison Level 2 Risk Estimates across Voting Systems

Level 2 Threat Vectors	Risk Estimates	
	Current UOCAVA Voting System	Remote Electronic Absentee Voting System
Insider Attack	27.791	28.791
Outsider Attack	9.940	16.572
Error at the LEO	19.131	16.980
Error during Transmission of Election Materials	10.942	8.004
Error at the Voter's Location	23.593	16.394
Accidental Disruptions	13.363	9.831

5.2.2 Level 1 Threat Types

Level 1 threat types are "Attacks" and "Unintentional Disruptions". However, since "Unintentional Disruptions" includes both "Errors" and "Accidental Disruptions" that cannot be easily prevented or mitigated, it is more useful to present the data in terms of "Attacks" and "Errors, as shown on Table 5.3. These results confirm previous observations regarding the preeminence of errors in the risk associated with the current UOCAVA voting system, while both attacks and errors contribute equally to the risks associated with the electronic absentee voting system.

Table 5.3: Comparison Level 1 Risk Estimates across Voting Systems

Level 1 Threat Vectors	Risk Estimates	
	Current UOCAVA Voting System	Remote Electronic Absentee Voting System
Attacks	37.731	45.363
Errors	53.666	41.378

5.3 Comparative Analysis By Voting Step

This analysis aims at uncovering which voting step contributes the most to the risks associated with the voting systems.

Table 5.4 shows that the risks associated with each voting steps are fairly similar between the two voting systems, with the exception of the "Ballot Marking" step, which exhibits a greater relative risk in the current UOCAVA voting system. In both systems, the "Registration" and "Absentee Ballot Request" voting step represents the greatest risk to the overall system.

Table 5.4: Comparison of Risk Estimates by Voting Step across Voting Systems

Voting Step	Risk Estimates	
	Current UOCAVA Voting System	Remote Electronic Absentee Voting System
Registration	31.131	30.503
Absentee Ballot Request	32.896	29.761
Absentee Ballot Delivery	6.115	6.533
Ballot Marking	10.760	8.021
Marked Ballot Return	6.755	6.145
Returned Ballot Processing and Tabulation	11.472	11.287
Post-Election Audit	5.632	4.322

5.4 Comparative Analysis by Security Objective

The risk estimates associated with each security objective for each threat vector are presented in Appendix C.

Figures 5.3 through 5.8 show the effect of attacks and unintentional errors on the voting system security objectives. Attacks have a greater effect than errors on the voter authentication objective for both systems; however the remote absentee electronic voting system is more affected relatively with a risk estimate for attack two fold greater than its risk estimate for errors. Both systems exhibit similar risk estimates from errors associated with the voter authentication objective.

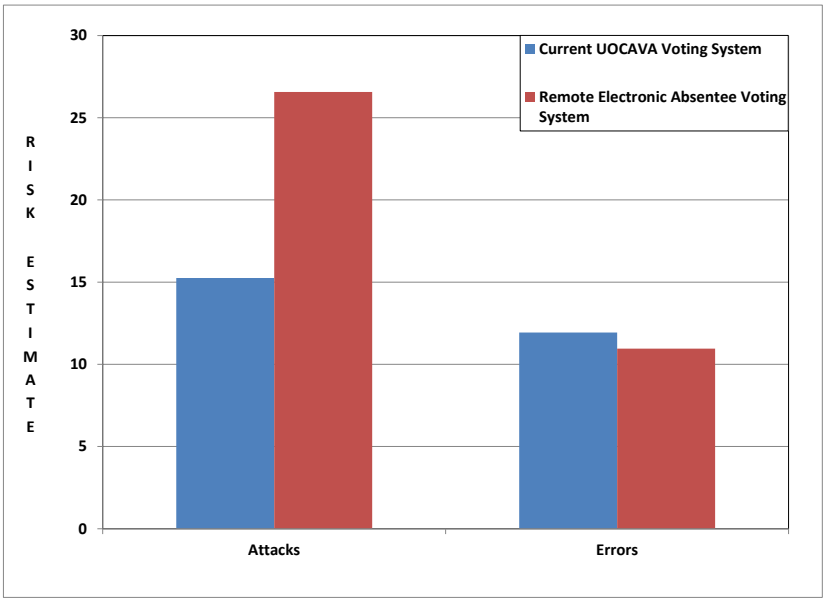


Figure 5.3: Effect of Attacks and Unintentional Errors on Voter Authentication across Voting Systems

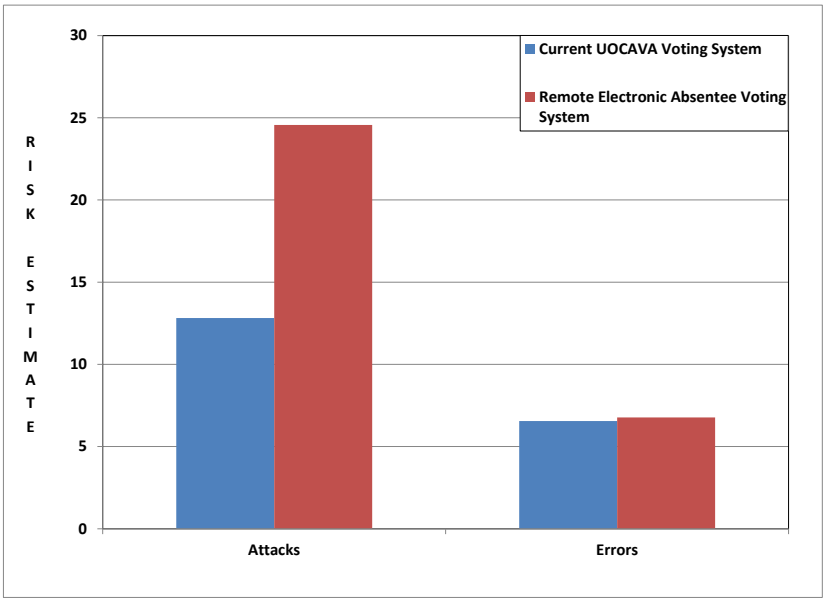


Figure 5.4: Effect of Attacks and Unintentional Errors on Vote Secrecy across Voting Systems

Similarly to the voter authentication objective, errors have similar effect on the vote secrecy security objective for both systems while attacks have a predominant effect on this objective in the context of the remote electronic absentee voting system.

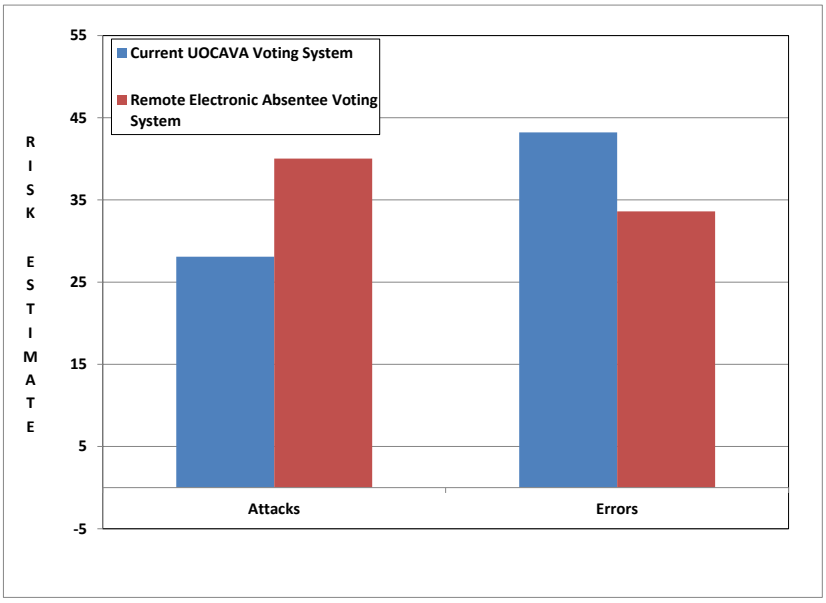


Figure 5.5: Effect of Attacks and Unintentional Errors on Vote Integrity across Voting Systems

The effect of errors on the vote integrity objective is greater for the current UOCAVA voting system than for its electronic alternative, while the opposite is observed for the effect of attacks, concurrent with previous observations.

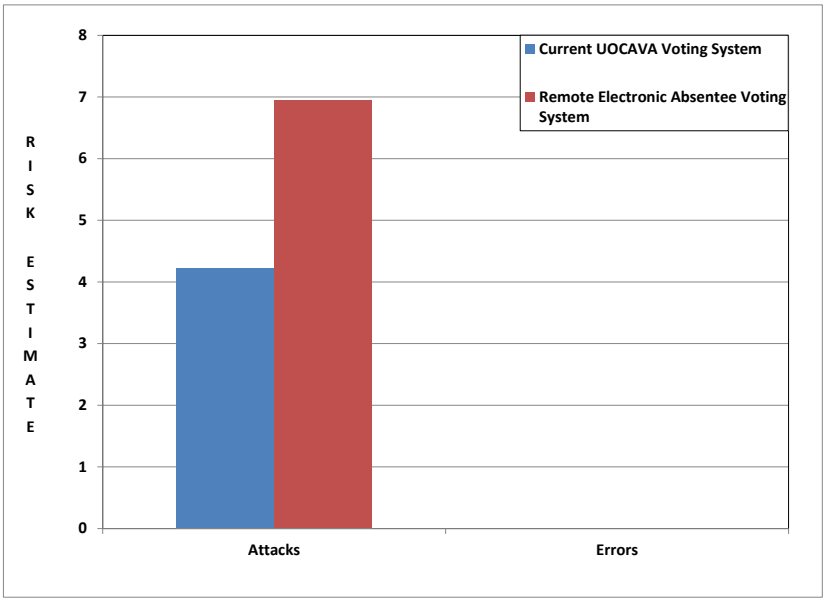


Figure 5.6: Effect of Attacks and Unintentional Errors on Vote Privacy across Voting Systems

It was considered that errors do not affect the vote privacy security objective for either system, so no risk estimates from errors were assigned to this security objective. However the effect of attacks on this factor is greater in the context of the remote electronic absentee voting system.

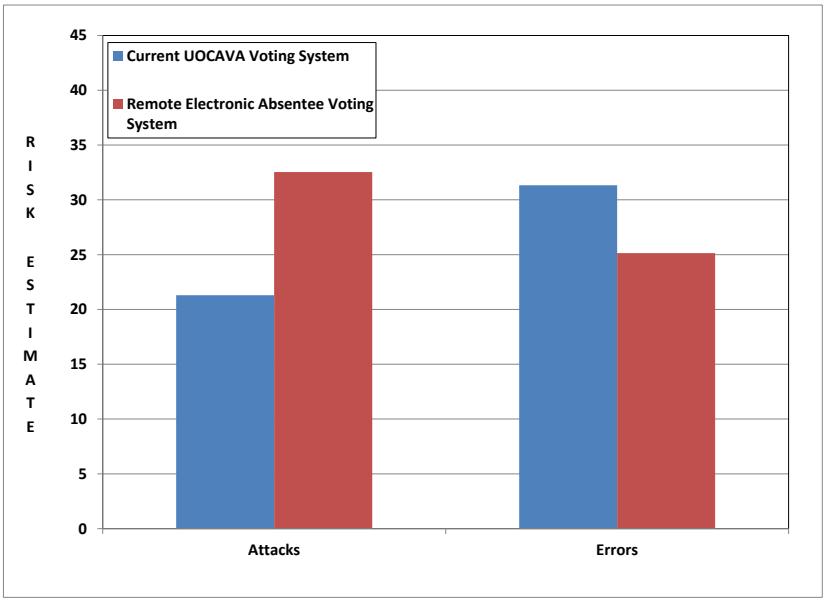


Figure 5.7: Effect of Attacks and Unintentional Errors on Auditability across Voting Systems

The effect of errors on the auditability objective is greater for the current UOCAVA voting system than for its electronic alternative, while the opposite is observed for the effect of attacks, concurrent with previous observations.

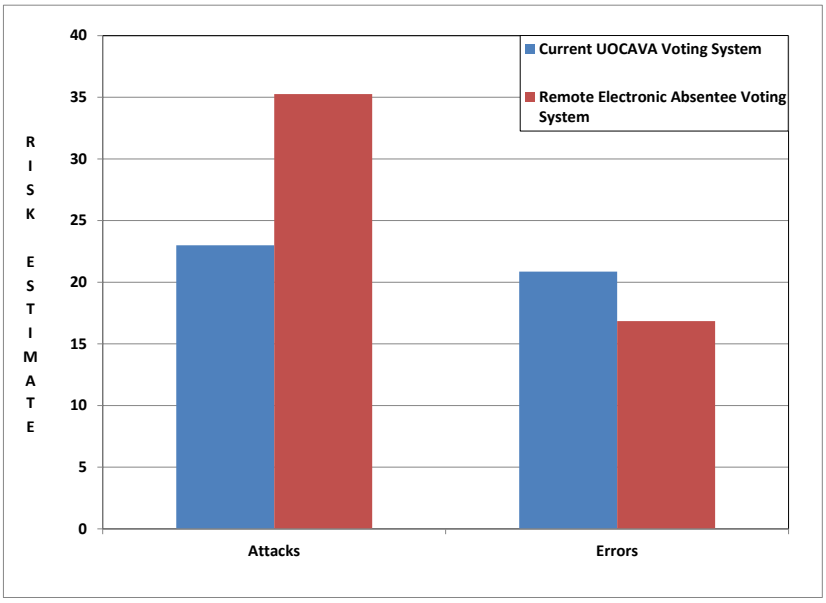


Figure 5.8: Effect of Attacks and Unintentional Errors on Service Availability across Voting Systems

Attacks have a greater effect than errors on the voter authentication objective for both systems; however the remote absentee electronic voting system is more affected relatively with a risk estimate for attack two fold greater than its risk estimate for errors. The service availability objective seems more affected by errors for the current UOCAVA voting system than its electronic alternative.

5.5 Comparative Risk Analysis By Voting System

By summing all the risk estimates across all threat vectors, a single risk estimate can be derived for each system. In the context of the system architectures and the analysis framework described in this report, the remote absentee electronic voting system appears to exhibit a lower overall absolute risk than the current UOCAVA voting system (

). However, the results of the statistical analysis described in Appendix C show that there is no statistical difference between the means of the two datasets.

Table 5.5: Comparison of Comprehensive Risk Estimates across Voting Systems

VOTING SYSTEM	RISK ESTIMATES
Current UOCAVA Voting System	104.8
Remote Electronic Absentee Voting System	96.6

As a result, both systems exhibit similar overall risks and the absolute values presented in Table 5.5 should not be construed as a demonstration of any significant difference between the overall risks associated with each system. This observation is a direct result of the opinions of a diverse panel of election and cyber security experts, whose answers to the risk analysis questionnaire were used to derive these estimates. The result of this analysis is also related to the format of the questionnaire itself, which can impact the provided answers. It denotes that the overall opinion of the panel assigned a greater risk to the current UOCAVA by-mail system than to its electronic alternative. However, from a process perspective and a statistical standpoint, these two systems appear to yield similar risks.

5.6 Summary

To date, the risks associated with the current UOCAVA voting system have not yet been quantitatively compared side-by-side to the risks associated with an electronic alternative. As a result, FVAP aimed at conducting a quantitative comparison of risks between the current UOCAVA voting system, as a baseline and reference system, and an electronic alternative

system for the implementation of a remote electronic voting demonstration project, as mandated by Congress. This report represents the first systematic risk analysis of the current UOCAVA by-mail voting system in an original analysis framework allowing quantitative comparison with other voting systems. The analysis was focused on the existing by-mail voting system and an online-based remote absentee voting system. In order to capture the risks between purely physical and purely digital absentee voting systems, the current UOCAVA voting system architecture was restricted to paper ballots and transmission of election materials through postal systems, while the architecture of its electronic counterpart featured voting via a Web application and transmission via the Internet. Thanks to an original risk analysis framework, a threat tree architecture tailored to voting systems, and inputs from a diverse panel of subject matter experts, the risks associated with each system were systematically compared across common threat vectors.

The findings of this analysis are as follows:

- The threats observed to incur the greatest risks on each voting system are linked to the system's inherent architecture, in accordance with opinions from the election community, thus validating the original risk analysis framework designed for this study
- The current UOCAVA voting system appears more susceptible to unintentional errors at the voter's location and accidental disruptions than its electronic alternative.
- The remote electronic absentee voting system appears to exhibit an equal subjectivity to malicious attacks and unintentional errors.
- From a process perspective, the risks to the voting system by voting step are similar for both architectures with "Registration" and "Absentee Ballot Request" representing the greatest risk to the overall system. The physical ballot marking by hand in the current UOCAVA voting system appears to exhibit a slightly greater risk than its digital alternative.
- From a security standpoint, authentication, vote secrecy, vote privacy and service availability are relatively more affected by attacks than unintentional errors when a digital absentee voting system is concerned, as opposed to its physical by-mail alternative. In addition, the effect of errors on vote integrity and auditability is greater for the current UOCAVA voting system than for its electronic alternative, while the opposite is observed for the effect of attacks.
- Based on the format of the questionnaire and associated inputs from subject matter experts, the current UOCAVA voting system appears to exhibit a greater risk than the remote electronic absentee voting system, when absolute risk estimates are examined. However, from a process perspective and a statistical standpoint, these two systems appear to yield similar risks.

6 Conclusions and Recommendations

To assist FVAP in better understanding the inherent risks associated with both the current UOCAVA voting system, as a baseline and reference system, and a remote absentee electronic voting system, and establish a foundation for quantitative comparison of risks across voting systems, this report described:

1. The creation of a risk analysis framework for quantitative analysis of the risks associated with absentee voting systems, with applicability to any voting scenario, including an original comparative risk analysis model and an original computational model derived from the EAC Election Operations Assessment TIRA model.
2. The identification of vulnerabilities and threats associated with the current UOCAVA by-mail voting system and a remote electronic absentee voting system.
3. A quantitative analysis of the risks associated with the current UOCAVA by-mail voting system.
4. A quantitative analysis of the risks associated with a remote electronic absentee voting system.
5. A side-by-side quantitative comparison of risks between the current UOCAVA by-mail voting system and a remote electronic absentee voting system.

This report presents the first systematic risk analysis of the current UOCAVA by-mail voting system with an electronic alternative. It offers a baseline and a reference for future comparative analysis and an original analysis framework allowing quantitative comparison with other voting systems to be evaluated during the research and development phase of the mandated demonstration project.

Aside from the quantitative results discussed in this report and summarized below, the risk analysis framework provides FVAP with:

- A dynamic tool for the evaluation of any voting system of interest.
- A threat tree architecture amenable to high level comparison of risks between voting systems.
- A means to perform individual in-depth analysis of components within voting systems, e.g. the comparison of risks between the "absentee ballot delivery" and "marked ballot return" steps within the current UOCAVA voting system.

In light of the Congressional mandate for a demonstration project, this analysis framework will allow FVAP to analyze and quantitatively compare risk within the identified processes for any

voting system architecture, thereby facilitating the discussion of comparative risk vis-à-vis the current postal mail absentee voting process. As a first step towards a quantitative comparison with a web-based voting interface transmitting voting materials through the Internet, this report examined the current UOCAVA voting system restricted to paper ballots transmitted by postal mail, and a remote electronic absentee voting system restricted to voting via an online software interface with transmission of election materials over the Internet. Due to the originality of the risk analysis framework and the preliminary nature of this initial risk analysis, the results derived from the work presented in this report should not be construed as conclusive statements, but rather observations drawing the potential towards such conclusions. These observations are detailed below:

Risk Analysis of Voting Systems

- Voting systems can be defined through a specific system architecture and a common voting process adapted to that architecture.
- A threat tree approach can be used to assess voting system risks once both system and process have been defined.
- Systematic and side-by-side comparison of risks across voting systems requires a common analysis framework.
- The risk analysis framework is validated by the concurrence of the risk outputs with empirical observations from the election community.

Risk Analysis of the Current UOCAVA Voting System

- Unintentional errors constitute the greatest source of risk, as compared to intentional malicious attacks or accidental disruptions.
- Errors at the voter's location appear most preeminent, especially during the physical marking of the absentee ballot by the voter.

Risk Analysis of the Remote Electronic Absentee Voting System

- Unintentional human errors and architecture-specific threats by malicious outsiders (e.g. denial of service) constitute the greatest source of risk.
- Conversely, insider attacks for this architecture yield a risk estimate fifty percent lower than the risk estimate for outsider attacks.

Quantitative Comparison of Risks across Voting Systems

- The current UOCAVA voting system appears to exhibit a greater risk from unintentional errors, while its electronic counterpart is equally subjected to attacks and errors.
- Security objectives are more affected by attacks in the context of the remote absentee voting system, and by errors in the context of the current UOCAVA voting system.
- Overall, the remote electronic absentee voting system and the current UOCAVA voting system exhibit similar risks, from a statistical standpoint.

With regards to the risk analysis framework, the following recommendations are made:

- This tool should be further validated and optimized by a wider panel of election and security experts to ensure that its outputs reflect the diverse opinions of the election community at large.
- This tool can and should be continuously updated with any new relevant threat-vulnerability pairings upon discovery.

Due to the diverse landscape of risk modeling, the following precautions should be used when using the risk analysis framework:

- Risk estimates must be used in the context of a defined risk management strategy.
- Risk estimates should not be compared to other estimates from different models.
- Risk estimates are dependent on the panel's expertise.

In light of the pending pilot demonstration project mandated by Congress, the following recommendations are made regarding the use of this tool as a first step in a risk management strategy crucial to a successful pilot deployment:

1. The current threat tree architecture presented in this report should be used for high level comparison of risks between pilot candidates and the current UOCAVA by-mail voting system. This comparison will provide a first level of selection across voting system native architectures.
2. Upon refinement of the voting system architectures, individual in-depth analyses of these systems should be performed using this tool by refining the threat tree and procuring specialized expert inputs relevant to the system's component under scrutiny. Such individual analyses will assist FVAP in assessing the risks associated with vulnerability-threat pairings specific to a particular component or subsystem, and will

constitute a guide for the design of a voting system's architecture with the least residual risk.

3. Once a voting system architecture has been finalized, the risks associated with the selected pilot system should be compared to the baseline risks of the current by-mail voting system to assist FVAP in the design of a coherent and tailored mitigation strategy for the pilot demonstration project.

Appendix A: Definitions

All definitions provided in this Appendix are constrained to the voting process unless otherwise noted.

A.1 Voting Process Definitions

A.1.1 Registration

Voter registration is the first step towards participating in the voting process[i] for any election. Registration is defined as being entered into a public record as eligible to vote in the city or county of legal residence. The legal voting residence for absentee voters is defined as their last physical address[46] within the fifty states, the District of Columbia, and the four territories (Guam, Northern Mariana Islands, Puerto Rico, and the United States Virgin Islands) hereafter referred to as "the states," whether they have maintained formal ties to that residence or not. Eligible voters living overseas who have never resided in the U.S. may use their parents' residence as their own for voting purposes in 24 states and the District of Columbia.[47] Military personnel and their family members may change their legal residence when changing permanent duty stations, or may retain their residency without change. Some states also have specific rules for voting eligibility aimed at excluding particular individuals, such as felons, and those recognized as mentally incompetent according to the regulations of their local residence.

While voter eligibility may be defined differently by each state, the following requirements typically apply:

- United States citizenship;
- Residency in the state where registration is sought;
- 18 years of age or older on Election Day; and,

Registration in the voter's state of legal residence is carried out through various means depending on allowances and instructions dictated by the voter's state of legal residence and jurisdiction,[48] as illustrated in Table A.1:

[i] While it is recognized that several states allow for Election Day registration, the sole exception to this general rule is the state of North Dakota, which does not require any voter registration prior to obtaining and casting a ballot.

Table A.1: Registration Options for UOCAVA Voters

The UOCAVA voter can register to vote by:	and transmit this form to the LEO through
▪ Completing a registration form obtained through either: ✓ their local election office (LEO) ✓ US embassies ✓ National Voter Registration offices[49]: ○ Division of Motor Registration offices (i.e. "Motor Registration"); ○ offices in the state of legal voting residence that provide public assistance or state-funded programs primarily engaged in providing services to persons with disabilities;	▪ Postal mail, or ▪ Electronic means (e.g. email or fax)
▪ Completing a Federal Post Card Application (FPCA) form[i]	▪ Postal mail, or ▪ Electronic means (e.g. email or fax)

A.1.2 Absentee Ballot Request

To participate in a specific election, eligible and registered UOCAVA voters must request an absentee ballot[ii], formatted according to the requirements set forth in the jurisdiction where they are registered, and by the appropriate deadline dictated by that jurisdiction. This request can be carried out through various means depending on allowances and instructions dictated by the voter's state of legal residence and jurisdiction,[50] as illustrated in Table A.2:

[i] The FPCA is a form for both voter registration and absentee ballot request for elections for federal offices (President/Vice President, U.S. Senator, U.S. Representative, Delegate or Resident Commissioner). Most states also allow the FPCA to be used to register and request ballots for state and/or local elections.

[ii] Some states allow for permanent absentee status, thus not requiring absentee ballot request for each election.

Table A.2: Means of Requesting an Absentee Ballot for UOCAVA Voters

The UOCAVA voter can request an absentee ballot by:	and transmit this form to the LEO through
▪ Completing a specific request form obtained through their LEO	▪ Postal mail, or ▪ Electronic means (e.g. email or fax)
▪ Completing the FPCA form[51]	▪ Postal mail, or ▪ Electronic means (e.g. email or fax)

A.1.3 Absentee Ballot Delivery

This step is defined as the transmission of the blank absentee ballot and relevant election materials to the voter, either by postal mail or electronic means. Once a valid absentee ballot request has been received and the voter registration status has been confirmed by the local election office, the absentee ballot is transmitted by postal mail or electronic means to the voter's address of record included in their registration. When the voter uses the FPCA to request an absentee ballot, he/she has the option to choose how the absentee ballot will be delivered: either by postal mail to a different physical address or by electronic means (e.g. personal email address). For the purpose of the risk analysis presented in this report, this transmission step is constrained to the absentee ballot and election materials, immediately after they leave the LEO (e.g. received at the post office), and immediately before they reach the voter (e.g. in the hands of the mail service on route for delivery to the voter).

A.1.4 Ballot Marking

Ballot marking consists of marking the voter's selection onto the blank ballot, either by physical (ink) or electronic (web interface) means, according to the specific instructions set forth in the jurisdiction where the voter is registered.

A.1.5 Marked Ballot Return

This step is defined as the transmission of the marked ballot from the voter to the local election office, either by postal mail or electronic means, according to the specific instructions and by the appropriate deadline set forth in the jurisdiction where the voter is registered. This transmission step is constrained to the marked ballot immediately after it leaves the voter (e.g. received at the post office), and immediately before it reaches the local election office (e.g. in the hands of the mail service on route for delivery to the LEO).

A.1.6 Returned Ballot Processing and Tabulation

Processing of the returned ballots comprises the following steps:

- receipt at the LEO
- sorting
- validation by precinct, i.e. verifying that the postmark or digital timestamp complies with the deadline set forth in the jurisdiction where the voter is registered, and matching the voter's signature, whether physical or digital, with the registration rolls
- formal acceptance
- privacy separation, i.e. separating the voters completed affidavits confirming their identity from the cast ballots, either by physical (separation of signed envelope from the privacy envelope) or electronic means

Once the voter's identity has been separated from the cast ballot, tabulation is carried out along with inspection for mismark, legibility, or evidence of fraud, and according to the preferred means of that LEO, whether it be manual or electronic. Those ballots considered invalid during inspection are set aside for adjudication. Ballots deemed valid are entered into the official election tally.

Across the states, reasons for adjudication and disqualification may include:

- Marked ballot received after the assigned deadline
- Lack of eligibility and/or registration (as defined in Section 2.1)
- Mismatch between signature on cast ballot and registration rolls
- Illegible ballot, including voting choices and signature
- Mismarks (the ballot is not completed according to the instructions)
- Violated privacy, with marks identifying the voter on the cast ballot
- Evidence of voting fraud (e.g. multiple voting, voter's impersonation, ballot stuffing, vote buying)

A.1.7 Post-Election Audit

The post-election audit consists of randomly selecting a sufficiently large subset of cast ballots – this proportion is dictated by state and local regulations – from randomly selected precincts across a jurisdiction for recount, in order to validate the individual and total tallies, and verify the integrity of the voting system. This step is typically carried out after all valid ballots have been counted, and is followed by the certification of the election results. Post-election audits should not be confused with the term "recount" in that the post-election audit primarily checks the accuracy of voting process, rather than yielding solutions to contested elections. Many states

have enacted mandatory audit requirements, although such audits are not necessarily required for certification of the election results.

A.2 Definitions for Voting-Related Risks

A.2.1 Vulnerability

A vulnerability is defined as a weakness in any part of the voting system that could be exploited by a threat agent through a threat vector. For example, the susceptibility of voters to bribery by malicious individuals constitutes a vulnerability to the voting system, since such susceptibility, if acted upon, could result in modified selections on ballots cast by bribed voters, thus affecting the results of the election.

A.2.2 Threat

A threat is defined as any action with the potential to adversely impact any or all parts of the voting system. As such, it encompasses both malicious and unintentional threats. A threat constitutes any action carried out by a threat agent via a threat vector with the potential to exploit a vulnerability in the voting system.

A.2.2.1 Threat Agent

A threat agent is defined as an individual or group of individuals who intentionally or accidentally exploit a vulnerability in the voting system via a threat vector. Threat agents encompass:

- Insider threat agents: individuals that have authorized access to election artifacts and responsibilities related to the voting process, whether it is handling of registrations and absentee ballot requests, or transmission of election materials, or handling and processing of marked ballots (e.g. local election officials)

- Outsider threat agents: individuals not affiliated with the voting process (e.g. voters, and foreign countries)

A.2.2.2 Threat Vector

A threat vector is defined as the intent and method targeted at the intentional exploitation of a vulnerability (i.e. attack), or a situation and method that may accidentally exploit a vulnerability (i.e. error or disrupting event). For the purpose of the quantitative risk analysis of voting systems, threat vectors have been categorized into the following two groups and six subgroups:

- **Attacks**

  An attack is defined as the intent and method targeted at the intentional exploitation of a vulnerability in the voting system. It encompasses both insider and outsider attacks.

  - Insider Attacks
    Attack carried out by an insider threat agent as defined above. An example of insider attack is the deletion of a batch of marked ballots on the LEO's server or theft of a bag of marked ballots by an election official.
  - Outsider Attacks
    Attack carried out by an outsider threat agent, as defined above. An example of outsider attack is the coercion of voters by malicious individuals with the intent to force specific selections on absentee ballots.

- **Unintentional Disruptions**
  - Errors at Local Election Office

    An error is defined as a method that may accidentally exploit a vulnerability in the voting system. An example of error at the LEO is a computing error during tabulation on the LEO server or by an election official.
  - Errors during Transmission of Election Materials
  - Errors at the Voter's Location
  - Accidental Events

    An accidental event is defined as a situation that may accidentally exploit a vulnerability in the voting system. Accidental events comprise natural events (e.g. storms), environmental events (e.g. accidental toxic spill), and human-created activities resulting in unintentional collateral compromise of the voting system (e.g. civil unrest). An example of accidental event is the Superstorm Sandy, which severely impacted the New Jersey voting system in 2012.

A.2.3 Likelihood

Likelihood is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability of the voting system.

A.2.4 Impact

An impact is defined as the adverse consequence of a threat vector being carried out by a threat agent on any or all parts of the voting system. The magnitude of impact to the voting process is categorized in three levels, as shown in Table A.3. For example, the level of impact with respect to the voting process could be considered high, depending on the threat vector being exercised, if the voting step "marked ballot return" were to be compromised.

Table A.3: Definition of Levels of Impact to the Voting System

Impact Level	Impact Definition
High	Severe or catastrophic adverse effect on the voting system potentially resulting in contest failure, with the effectiveness of the process severely reduced, and major damage to privacy, integrity, and/or auditability.
Medium	Serious adverse effect on the voting system not resulting in contest failure, with the effectiveness of the process significantly reduced, and significant damage to privacy, integrity, and/or auditability.
Low	Limited adverse effect on the voting system not resulting in contest failure, with the effectiveness of the process noticeably reduced, and minor damage to privacy, integrity, and/or auditability.

To further understand the notion of impact to the voting process, it is important to acknowledge that the existence of threats and vulnerabilities to the process does not preclude an impact. For an impact to occur, four factors are required:

1. a threat agent,
2. a threat vector,
3. a vulnerability, and
4. an action, i.e. the exercise of a threat by a threat agent via a threat vector (whether intentional or accidental) upon an existing vulnerability.

The following figure demonstrates how these four factors must combine to result in an impact:

				Threat Agent	+	Vulnerability	=	No Impact
				Threat Vector	+	Vulnerability	=	No Impact
		Threat Agent	+	Threat Vector	+	Vulnerability	=	No Impact
Threat Agent	+	Threat Vector	+	**Action**	+	Vulnerability	=	**Impact**

A.3 Definitions of Voting Security Objectives

A.3.1 Authentication

Authentication is defined as the process of identifying the voter's identity while he/she is using the voting system. In the context of the current UOCAVA voting system, this verification is performed by asking the voters to provide a signature on their registration application. This signature is then entered in the VRDB for archiving. Subsequently, this signature is used to compare with the required signature provided on the absentee ballot request form and on the marked ballot packet submitted to the LEO. In the context of the remote absentee electronic voting system, a unique pair of username and password is provided to each voter to access the online voting application. The use of these credentials provides a first line of defense against fraudulent activities on the application. A secondary last line of defense consists of requiring the voter to digitally sign his/her registration application. This signature is archived in the VRDB and subsequently used to compare with the required digital signature provided on the absentee ballot request form and on the marked ballot packet submitted to the LEO.

A.3.2 Vote Secrecy

Vote secrecy is defined as the concealment of the voting activity. Ensuring vote secrecy consists of the prevention of eavesdropping activities while the voter conducts voting activities, i.e. registration, absentee ballot request, ballot marking, and returning a marked ballot. In any voting scenario, the voter is requested to conduct his/her voting activities in person, or through a trusted delegate if he/she is physically unable. In the context of the current UOCAVA voting system, this prevention is carried out by sealing documents inside envelopes when transmitting ballots and forms to the LEO. In the context of the remote absentee electronic voting system, transmission of ballots and forms to the LEO is performed via a secure network connection, e.g. a VPN. In addition, activities on the voting application are concealed from unauthorized view by providing security measures, e.g. firewalls, and encryption.

A.3.3 Vote Integrity

Integrity is defined as the quality of an undamaged and unmodified vote. Hence, protecting the vote integrity consists of preventing against tampering, wrongful loss or destruction of votes. In the context of the current UOCAVA voting system, this prevention is carried out by ensuring the trustworthiness and integrity of the personnel handling election materials via background checks and other measures, as well as requesting that the voter conducts his/her voting activities in person, or through a trusted delegate if he/she is physically unable. Voters are also requested to verify their selections on their marked ballot before transmitting them to the LEO, where ballots are secured in a physical ballot box, with restricted access to authorized and vetted local election officials.

A.3.4 Vote Privacy

Vote privacy is the separation of the voter's identity from the marked ballot, to ensure its anonymity. In the context of the current UOCAVA voting system, this quality is preserved by sealing the marked ballot inside a secrecy envelope, it sealed in a secondary envelope containing the voter's affidavit. Upon reception at the LEO, the secrecy envelope is separated from the affidavit after validation of the voter's signature. In the context of the remote absentee electronic voting system, this separation is performed on the tabulation server via a coded instruction.

A.3.5 Auditability

Auditability is defined as the required ability of a vote and voter's registration to be examined for accuracy to ensure that all votes are cast as intended and counted as cast, and safeguard the transparency of the voting system. The definition of a post-election audit is provided in Section 1.7 of this appendix.

A.3.6 Service Availability

Service availability consists of the quality of voting resources to be accessible and obtainable to voters throughout the election cycle. Protecting this quality consists of ensuring adequate staffing and training at the LEO, and accessibility of these resources to all disabled voters. Transmission of election materials between the voter and the LEO is also required to be performed in a timely fashion, to allow voter's registrations and absentee ballot requests to be carried out and votes to be cast within the mandated deadlines.

Appendix B: Methodology

All definitions provided in this Appendix are constrained to the voting system unless otherwise noted.

B.1 Individual Risk Analysis Methodology

B.1.1 Voting System Characterization

B.1.1.1 Architecture Definition

Defining the voting system's architecture consists of determining the relationships and the nature of the interactions between the three voting-related elements composing the system, i.e. the local election office, the transmission element, and the voter, as defined in Section 2.1.

B.1.1.2 Definition of the Voting Process

The voting process consists of the seven steps described in Section 2.2, and generally defined in Appendix A. To conduct a risk analysis of a voting system, these definitions need to be specified by clarifying how each of these steps is carried out in the context of the voting system's architecture previously delineated, as shown in Section 4.

B.1.1.3 Identification of Security Objectives

Voting security objectives are listed in Section 2.3, and defined in Appendix A. For a risk analysis, it is important to understand the relationship of these objectives to each step in the voting process of a specific voting system.

B.1.2 Identification of Vulnerabilities

The goal of this step is to develop a list of system vulnerabilities (as defined in Appendix A) that could be exploited by potential threat agents through various threat vectors, for a given voting system architecture. It is performed through a thorough literature review, as described in Section 3.2.1.

B.1.3 Identification of Threats

The goal of this step is to develop a list of potential threats (as defined in Appendix A) to the voting system, for a given voting system architecture. A threat poses a risk to the system, only if it can exploit an existing system vulnerability. In the absence of such vulnerability, the potential

threat does not constitute a risk to the system. The identification of threats to a particular voting system is performed through a thorough literature review, as detailed in Section 3.2.1. A threat amounts to a threat agent using a particular method or threat vector to carry out a threat.

B.1.3.1 Threat Agent

A threat agent is defined as an individual or group of individuals who intentionally or accidentally exploit a vulnerability in the voting system via a threat vector. Threat agents can be categorized as follows:

- **Insider threat agents**

  Individuals that have authorized access to election artifacts and responsibilities related to the voting system, whether it is access to resources at the LEO, or involvement with the transmission of election materials.

- **Outsider threat agents**

  Individuals not affiliated with the voting system (e.g. voters, and foreign countries).

B.1.4 Likelihood Determination

To measure risks to the voting system, the likelihood (as defined in Appendix A) of each identified threat to be exercised on existing vulnerabilities needs to be assessed. It takes into account the nature of the threat and the associated vulnerability.

B.1.5 Impact Evaluation

The second major parameter in assessing risk is the impact a given exercised threat has on the system, as defined in Appendix A.

B.2 Framework for Comparative and Quantitative Risk Analysis

B.2.1 Literature Review

The linked document contains a reference list of supporting documentation on voting and risk analysis.

B.2.1 Literature Review.pdf

B.2.2 Comparative Risk Analysis Model

B.2.2.1 Voting Step Threat Trees

Voting step threat trees are derived from the universal voting system threat trees detailed in Figure 3.3 and Figure 3.4, and adapted to each voting system under consideration. In this work the current UOCAVA voting system and a remote electronic absentee voting system are examined. The voting step threat trees associated with these systems are provided in attached Excel spreadsheets below.

B2.2.1 Voting Step Threat Trees.xlsx

B.2.3 Computational Model for Risk Analysis

B.2.3.1 Risk Analysis Questionnaires

- **Current UOCAVA Voting System**

  Current UOCAVA Risk Assessment Que

- **Remote Electronic Absentee Voting System**

  Electronic Voting Risk Assessment Question

B.2.3.2 Statistical Simulation for Risk Analysis

The TIRA model uses a Monte Carlo simulation to derive estimates of risks for each threat vector in the voting step threat trees. The Monte Carlo simulation is a stochastic simulation, i.e. it uses variable inputs generated from random number distributions to simulate an output.

The inputs to the model are the numerical answers to the likelihood and impact questions submitted to the stakeholders, as defined in Section 3.2.3.

A simulation is used to build an experimental model to describe a real system. In this case the Monte Carlo simulation is used to randomly sample from distributions created from the reasonable ranges of likelihood and impact values over potentially thousands of iterations. These iterations allow for a description of the risk of a threat being exercised over a wide range of values for impact and likelihood. The steps of the Monte Carlo simulation are described below.

First, cumulative distribution functions are built for each input variable, i,e. likelihood and impact. It must be noted that the cumulative distribution function for likelihood is continuous, while it is discrete for impact.

- **Likelihood**

1. Generate random numbers within the numerical range for likelihood, i.e. minimum, most likely, and maximum values.
2. Create a cumulative distribution function by:
    a. Dividing the range [0,1] in adjacent increments or bins of equal size. Here a bin size of 0.005 is chosen, as most appropriate for this application. Therefore the bin values displayed on the x-axis or horizontal axis are 0.005, 0.010, 0.015… up to 1, and a bin is defined as the interval between two bin values, e.g. 0.255 to 0.260 or 0.950 to 0.955.
    b. Calculating the frequency distribution of the random numbers generated in Step 1, by calculating how many random numbers fall within each bin or interval between two bin values.
    c. Creating a relative frequency distribution from the frequency distribution built in Step 2b by dividing the frequency of the random numbers by the sum of all frequencies. This normalizing step ensures that the sum of all relative frequency values is equal to 1.
    d. Creating a cumulative frequency distribution by incrementally adding the normalized relative frequency in one bin with the normalized frequency in the previous bin.

e. Transforming bin values created in Step 2a into probabilities by using the following formula:

- If the bin value is below the minimum value for likelihood, this minimum value is assigned to that bin.
- If the bin value is above the maximum value for likelihood, this maximum value is assigned to that bin.
- If the bin value falls within the minimum and maximum values for likelihood, the bin value is used for probability.

An example is shown below:

- The likelihood input values for a given threat vector are:

  Minimum: 0.1

  Most likely: 0.25

  Maximum: 0.3

- Table B.1 and Figure B.1through Figure B.4 below illustrate Step 2:

Table B.1: Building of a Normalized Cumulative Distribution Function
(risks estimates are for informational purpose only and do not reflect actual risk analysis outputs)

Bins	Frequency	Relative Frequency	Cumulative Frequency	Probability
0.22	0	0	0	0.22
0.225	1	0.00332	0.00332	0.225
0.23	2	0.00664	0.00997	0.23
0.235	0	0.00000	0.00997	0.235
0.24	11	0.03654	0.04651	0.24
0.245	12	0.03987	0.08638	0.245
0.25	20	0.06645	0.15282	0.25
0.255	21	0.06977	0.22259	0.255
0.26	32	0.10631	0.32890	0.26
0.265	42	0.13953	0.46844	0.265
0.27	36	0.11960	0.58804	0.27
0.275	33	0.10963	0.69767	0.275
0.28	24	0.07973	0.77741	0.28
0.285	20	0.06645	0.84385	0.285
0.29	19	0.06312	0.90698	0.29
0.295	7	0.02326	0.93023	0.295
0.3	10	0.03322	0.96346	0.3
0.305	8	0.02658	0.99003	0.3
0.31	2	0.00664	0.99668	0.3
0.315	1	0.00332	1	0.3
0.32	0	0	1	0.3
0.325	0	0	1	0.3
Sum	301	1		

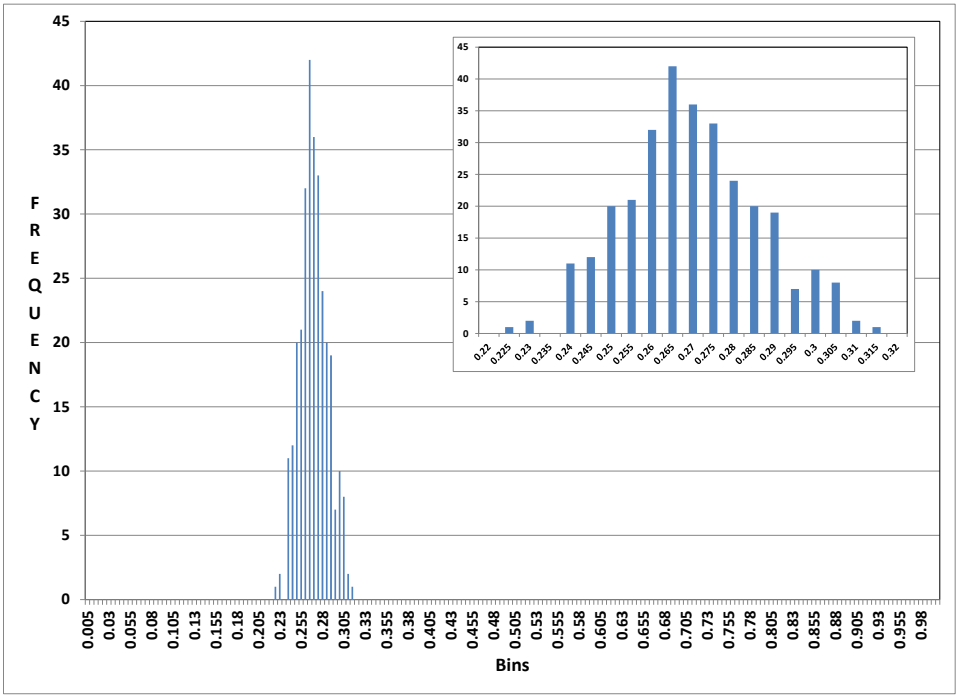


Figure B.1: Step 2b - Frequency Distribution

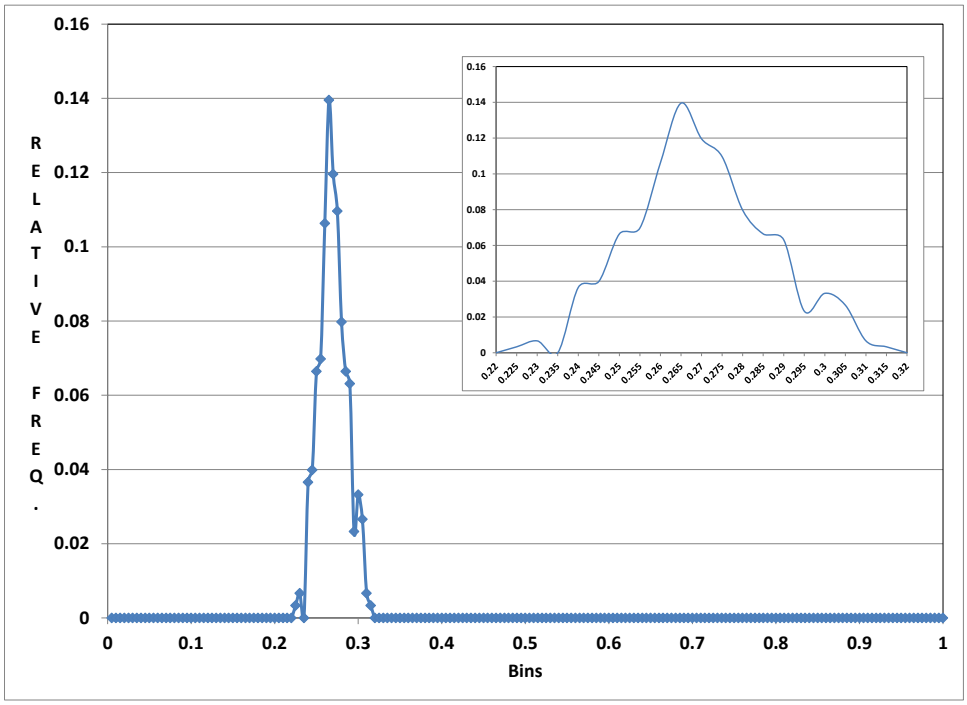


Figure B.2: Step 2c - Relative Frequency Distribution

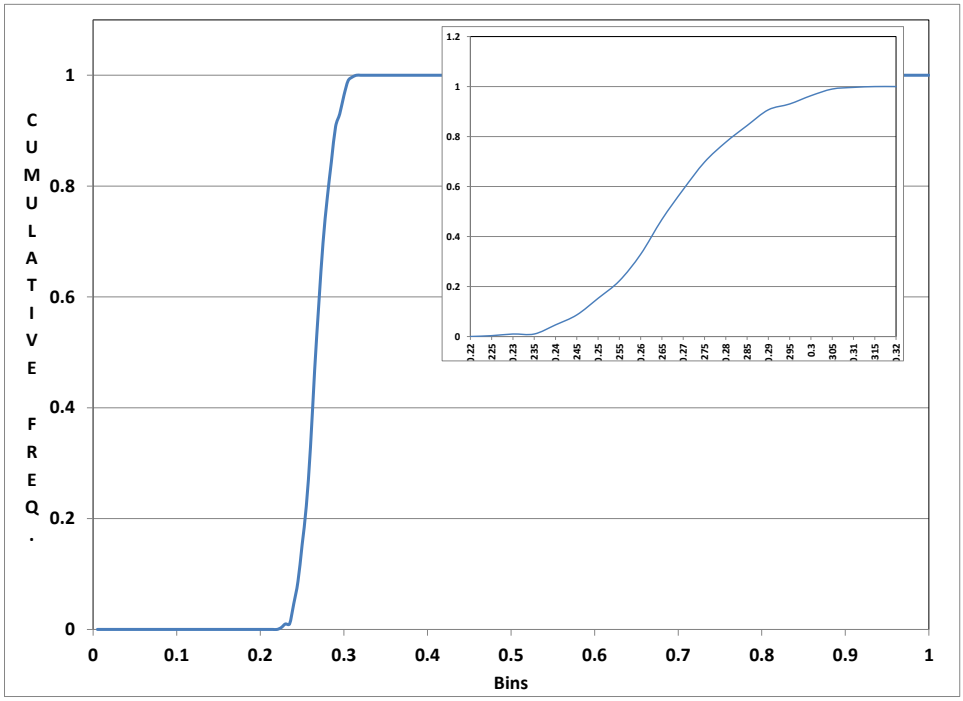


Figure B.3: Step 2d - Cumulative Frequency Distribution

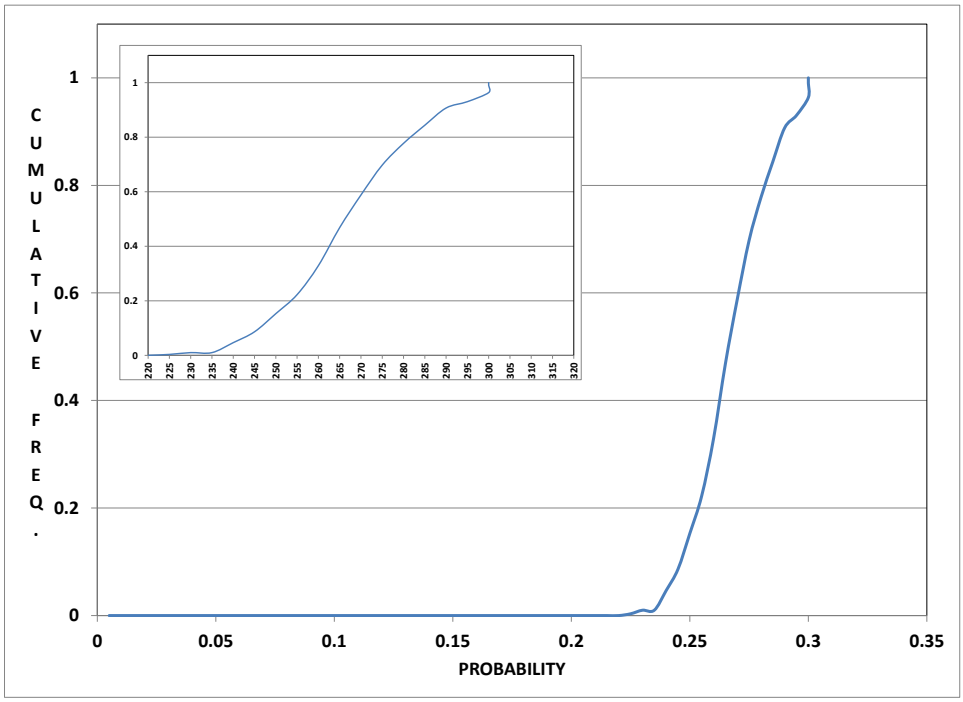


Figure B.4: Cumulative Distribution Function for Likelihood

- **Impact**

For this input parameter and the threat vector of interest, the creation of the cumulative distribution function follows the steps below

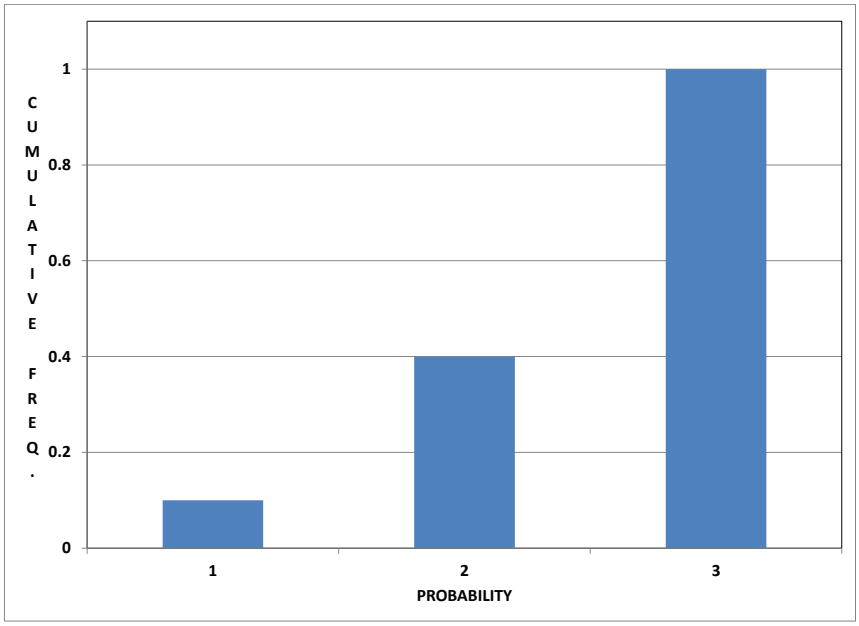
1. Low, moderate and high impact are assigned discrete probability values as follows:
   - Low = 1
   - Moderate = 2
   - High = 3
2. The discrete values for cumulative frequencies are as follows:
   - $\frac{Low\ Impact\ Value}{Sum\ of\ all\ Impact\ Values}$
   - $\frac{Low\ Impact\ Value + Moderate\ Impact\ Value}{Sum\ of\ all\ Impact\ Values}$
   - 1

   An example is shown below:
   - Impact values are as follows:

     Low Impact: 10

     Moderate Impact: 30

     High Impact: 60
   - The cumulative distribution function for impact is shown on Figure B.5 :



[redacted]

Figure B.5: Cumulative Distribution Function for Impact

Second, a set of two random numbers is generated for iteration j for impact and likelihood within their respective ranges of input values for the threat vector of interest.

Third, these random numbers are plotted onto the respective cumulative distribution function to determine their assigned probability, as shown in the example below:

- Random number for likelihood: 0.48956

  Since this number falls between the cumulative frequencies 0.46844 and 0.58804 on Table B.1, it is assigned the probability 0.265, as shown on Figure B.6:

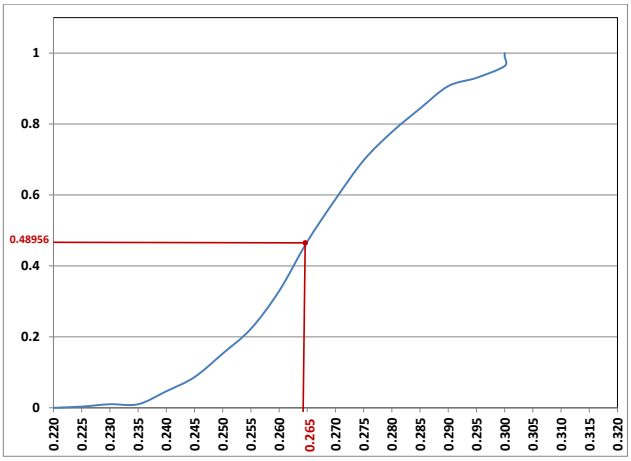


Figure B.6: Determination of Likelihood Estimate

- Random number for impact: 0.21387

  Since this number falls between 0.1 and 0.4 (Figure B.5), it is assigned the value 2, as shown on Figure B.7:

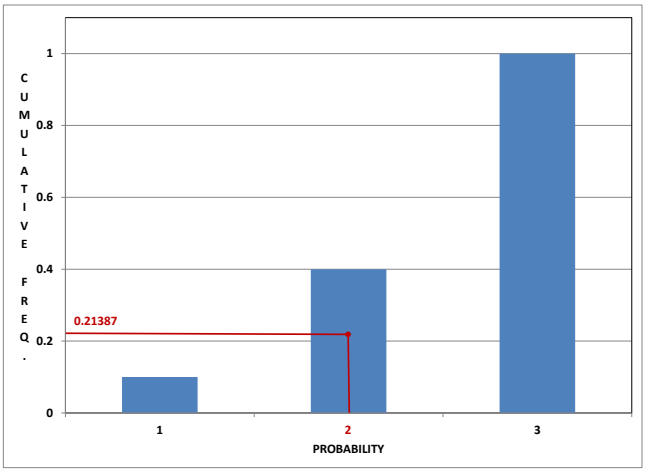


Figure B.7: Determination of Impact Estimate

Finally, the risk estimate for iteration j is calculated, as follows:

$$Risk_j = Likelihood_j \times Impact_j$$

$$Risk_j = 0.265 \times 2$$

$$Risk_j = 0.53$$

This process is performed at each new iteration, and the average of the resulting set of risk estimates is calculated. This averaged estimate is the risk value assigned to the threat vector under consideration (risks estimates are for informational purpose only and do not reflect actual risk analysis outputs).

Appendix C: Risk Analysis

C.1 Vulnerability Database

C1 VTDb FINAL.pdf

C.2 Questionnaire Inputs

CSE1-Current UOCAVA Risk Assessı

CSE1-Electronic Voting Risk Assessme

CSE2-Current UOCAVA Risk Assessı

CSE2-Electronic Voting Risk Assessme

CSE3-Current UOCAVA Risk Assessı

CSE3-Electronic Voting Risk Assessme

CSE4-Current UOCAVA Risk Assessı

CSE4-Electronic Voting Risk Assessme

EE1-Current UOCAVA Risk Assessı

EE1-Electronic Voting Risk Assessment Que

EE2-Current UOCAVA Risk Assessı

EE2-Electronic Voting Risk Assessment Que

EE3-Current UOCAVA Risk Assessı

EE3-Electronic Voting Risk Assessment Que

C.3 Risk Model Outputs

C3 Risk Model Outputs FINAL.pdf

C.4 Risk Estimates and Assignment Matrices

C4 Security Risk Estimates and Assignı

C.5 Statistical Analysis of the Risk Dataset

Table C.1 shows that the variance associated with the risk data from the current UOCAVA voting system is greater than for the data from the remote electronic absentee voting system. The Z statistic value of 1.077, greater than 1 demonstrates that the mean values of both datasets are not significantly different from each other, as confirmed with the value of "P(Z<=z) one tail" of 0.141 above the alpha statistic of 0.05. The positive covariance value of 0.188 shows that the datasets vary similarly with each other, i.e. a large risk estimate for a given threat vector for the current UOCAVA voting system leads to a large risk estimate for its electronic counterpart.

Table C.1: Side-by-Side Statistical Analysis of Voting System Risk Estimates

Statistical Data	Current UOCAVA Voting System	Absentee Voting System
Variance	0.366	0.262
Minimum	0.352	0.307
Maximum	2.985	2.518
Sum	104.760	96.572
z-stat	1.077	
P(Z<=z) one-tail	0.141	
Covariance	0.188	

References

[1] United States Code. 1986. Registration and Voting by Absent Uniformed Service Voters and Overseas Voters in Elections for Federal Office (Uniformed and Overseas Citizens Absentee Voting Act). 42 USC Sec. 1973ff. Retrieved from: http://www.justice.gov/crt/military/uocava_statute.htm

[2] United States Public Law. 2001. National Defense Authorization Act for Fiscal Year 2002. 107-107 115 Stat. 1012. Retrieved from: http://www.dod.gov/dodgc/olc/docs/2002NDAA.pdf

[3] United States Public Law. 2004. National Defense Authorization Act for Fiscal Year 2005. 108-375 115 Stat. 1811. Retrieved from: http://www.gpo.gov/fdsys/pkg/PLAW-108publ375/pdf/PLAW-108publ375.pdf

[4] United States Code. 2010. Uniformed and Overseas Citizens Absentee Voting Act As amended by the Military and Overseas Voter Empowerment Act. Retrieved from: http://www.fvap.gov/resources/media/uocavalaw.pdf

[5] U.S. Election Assistance Commission. 2007. UOCAVA Voters and the Electronic Transmission of Voting Materials in Four States. October 2007.

[6] U.S. Election Assistance Commission. 2009. Election Operations Assessment – Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA). EAC Advisory Board and Standards Board Draft. December 23, 2009. Retrieved from: http://www.eac.gov/assets/1/Documents/eoathreattrees.pdf

[7] U.S. Election Assistance Commission. 2011. A Survey of Internet Voting. Testing and Certification Technical Paper #2. September 14, 2011.

[8] National Institute of Standards and Technology. 1995. Special Publication 800-12. An Introduction to Computer Security The NIST Handbook. October 1995.

[9] National Institute of Standards and Technology. 2002. Special Publication 800-30. Risk Management Guide for Information Technology Systems. July 2002.

[10] National Institute of Standards and Technology ITL. 2003. An Overview of Issues in Testing Intrusion Detection. June 2003.

[11] National Institute of Standards and Technology. 2007. Interagency Report 7435. The Common Vulnerability Scoring System and its Applicability to Federal Agency Systems. August 2003.

[12] National Institute of Standards and Technology. 2008. Special Publication 800-53A Rev.1. Guide for Assessing the Security Controls in Federal Information Systems and Organizations. July 2008.

[13] National Institute of Standards and Technology. 2008. Special Publication 800-115. Technical Guide to Information Security Testing and Assessment. September 2008.

[14] National Institute of Standards and Technology. 2009. Special Publication 800-53 Rev.3. Recommended Security Controls for Federal Information Systems and Organizations. August 2009.

[15] National Institute of Standards and Technology. 2010. Special Publication 800-34 Rev.1. Contingency Planning Guide for Federal Information Systems. May 2010.

[16] National Institute of Standards and Technology. 2011. Special Publication 800-39. Managing Information Security Risk. March 2011.

[17] National Institute of Standards and Technology. 2008. Interagency Report 7551. A Threat Analysis on UOCAVA Voting Systems. December 2008.

[18] National Institute of Standards and Technology. 2010. TGDC Presentation. Risk Methodology for UOCAVA Voting Systems. July 2010.

[19] National Institute of Standards and Technology. 2011. Interagency Report 7770. Security Considerations for Remote Electronic UOCAVA Absentee Voting. February 2011.

[20] National Institute of Standards and Technology. 2011. Interagency Report 7682. Information System Security Best Practices for UOCAVA-Supporting Systems. September 2011.

[21] National Institute of Standards and Technology. 2011. Interagency Report 7711. Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. September 2011.

[22] Constitutional Convention. 1787. Constitution of the United States. Philadelphia, Pennsylvania. September 17, 1787.

[23] Federal Voting Assistance Program. 2012. www.FVAP.gov. Voting Assistance Guide. June 2012. Retrieved from:
http://www.fvap.gov/resources/media/vag2012.pdf

[24] NIST. 2002. SP 800-30.

[25] Council on National Security Systems (CNSS). 2010. Instruction No 4009. National Information Assurance Glossary. April 26, 2010.

[26] NIST. 2002. SP 800-30.

[27] NIST. 2002. SP 800-30.

[28] NIST. 2008. IR 7551.

[29] NIST. 2010. TGDC Presentation.

[30] Alberts, C., Dorofee, A. 2002. Managing Information Security Risks – The Octave Approach. Ed. Addison Wesley, Boston, MA.

[31] National Infrastructure Advisory Council. 2004. Common Vulnerability Scoring System.

[32] Wallach, D.S. 2008. Voting System Risk Assessment via Computational Complexity Analysis. William and Mary Bill of Rights Journal. 17:325-349.

[33] EAC. 2009. Election Operations Assessment.

[34] Lazarus, E.L., Dill, D.L., Schneier, B. 2010. Quantitative Security Analysis of Internet Voting vs. Two Other Voting Systems. Workshop on UOCAVA Remote Voting Systems. Aug 6-7, 2010.

[35] Pardue, H, Yasinsac, A., Landry, J. 2010. Towards Internet Voting Security: A Threat Tree for Risk Assessment.

[36] Lazarus, E.L., Dill, D.L., Epstein, J., Lorenzo Hall, J. 2011. Applying a Reusable Election Threat Model at the County Level.

[37] Alberts, C., Dorofee, A. 2002.

[38] NIAC. 2004. CVSS.

[39] Wallach. 2008.

[40] Lazarus et al. 2010.

[41] EAC. 2010. Election Operations Assessment.

[42] Pardue, H, Yasinsac, A., Landry, J. 2010.

[43] EAC. 2010. Election Operations Assessment. Informational Videos for the Election Operations Assessment. Retrieved from: http://archives.eac.gov/extlnk/lnkframehead.htm?http%3A//www.hp.isc.usouthal.edu/BOASB_PhaseII_Presentation.htm

[44] Jones, Doug W. 2005. Threats to Voting Systems. NIST workshop on Threats to Voting Systems. 7 October 2005. Gaithersburg, MD. Retrieved from: http://homepage.cs.uiowa.edu/~jones/voting/nist2005.shtml

[45] Jones. 2005.

[46] Federal Voting Assistance Program. www.FVAP.gov. Frequently Asked Questions. "Where is my legal voting residence?". Retrieved from: http://www.fvap.gov/faq.html#usmq2

[47] Federal Voting Assistance Program. www.FVAP.gov. Never Resided in the US. Retrieved from: http://www.fvap.gov/reference/nvr-res.html

[48] NIST. 2011. IR 7711.

[49] United States Code. 1993. National Voter Registration Act. 42 USC Sec. 1973gg-5. Retrieved from: http://www.fvap.gov/resources/media/nvralaw.pdf

[50] NIST. 2011. IR 7711.

[25] NIST. 2011. IR 7711.

[51] FVAP. Voting Assistance Guide.