Federal Voting Assistance Program

Secure Electronic Registration and Voting Experiment

Threat Risk Assessment - Phase 3

Version 0.5
March 23, 2004

Table of Contents

1 Introduction

1.1 Overview

The Secure Electronic Registration and Voting Experiment (SERVE) like any endeavor experiences risk. These risks need to be identified, classified and mitigated where feasible to provide a reliable, secure and trustworthy system. The SERVE system, UOCAVA Voting System (UVS) and its users are affected by all of the general security risks that any Internet connected system must address as well as risks specific to an Internet enabled electoral process.

The overall risk model that the UOCAVA Voting System operates under can in some ways be compared to the risk model that financial institutions face when they provide online services to their customer base (i.e., identification and authentication of clients and confidentiality, integrity and access to data). UVS labors under the same security requirements as the Citizen must be identified so that the confidentiality of the vote can be assured. The Citizen will also require UVS to assure the Integrity of the vote so that the intent of the voter can be transferred through the system to the local election office to its final destination the vote tally. Finally the Citizen will expect the system to be accessible to them so that they can vote at any time during the permissible voting period. The difference is that all of these goals must be accomplished while keeping the intent of the voter a secret.

Internet voting (I-Voting) also experiences some changes to the severity and type of risk that is inherent to the standard Internet accessible financial site. This modified risk portfolio is in many ways due to the secrecy of the voting process compared to the required knowledge of who both parties are in monetary transfers. Also it is possible that a government or group of individuals might feel they could affect US policy by either manipulating or blocking the voting process. These important issues must be held in mind while assessing each specific threat so that the true weight of the threat can be weighed and addressed to understand the overall projects threat risk portfolio.

This document is designed to lead the reader through all of the topics that must be covered to understand the entire portfolio of Internet voting security risks affecting SERVE and its systems. As such the document should be read from start to finish so that a full understanding of the broad issues can be applied to the more specific threats. The section you are currently reading will provide the base for reading the remainder of the sections including the risk assessment methodology used. Section 2 gives a broad overview of security threats that any Internet voting system will face. Section 3 describes the project information criticality to help the reader understand the various elements of the risk ratings. Section 4 discusses the specific threats that have been identified as affecting the SERVE systems. And section 5 lists the mitigations that are being used to address the threats that were identified in section 4.

1.2 Purpose

Security Risk Assessment is critical to the SERVE project as it provides a way to identify, document and deal with the inherent and unique risks involved in the registration and Internet voting process. The purpose of this document is to identify actual and perceived security threats affecting the SERVE system. Due to the new nature of Internet voting and the lack of experience the public has had with Internet voting the perception of risk is in many cases as dangerous to the project as the actuality of risk. Both real and perceived risks are covered in detail and compared with the whole body of risks to provide the reader a perspective of the overall level of risk and the possible mitigations.

To cover the field of possible risks this assessment deals with the security risks from the perspective of the Citizen, Local Election Official, VeriSign roaming certificate infrastructure, and UVS. This document is not limited to an overall discussion of Internet voting risks, but delves into the specific risk portfolio of the actual process used by the SERVE systems for Internet voting.

1.3 Risk Assessment Methodology

One of the difficulties encountered by this sort of risk assessment has to do with quantifying impact. Although the cost of equipment down time or service outage can be measured, other significant impacts, such as loss of public confidence or reputation (the intangibles) or the loss of a single vote, can be hard to calculate. To accomplish a meaningful security risk analysis of the SERVE project the Facilitated Risk Analysis Procedure (FRAP) methodology, as described by Thomas R. Peltier in his book "Information Security Risk Analysis" was used as the basis of this risk assessment. A brief description of the process is presented in Appendix A. In addition portions of the NSA (National Security Agency) Information Security Assessment Methodology have been incorporated into the FRAP where appropriate to provide the most appropriate risk analysis for the specific project.

The FRAP is designed to reduce the overall time it takes to create a meaningful risk assessment by using a diverse team of subject matter experts to identify the pool of risks and then rank them in a comparative fashion. The FRAP process is not designed to create hard risk values but comparative risk qualifiers giving management the ability to focus on the risks having the most priority to the project. It is entirely probable that a different team of experts would assign different levels of risk ratings to risk elements but the design of FRAP causes the overall ranking of the risks to stay generally the same.

The INFOSEC Assessment Methodology (IAM) is a detailed and systematic way of examining cyber vulnerabilities that was developed by NSA information security assessors. The portion of the IAM process used in this document deals with the value of data or systems. Specifically the creation of information criticality ratings so the document reviewer can understand some of the risk ratings applied by the FRAP participants. These ratings by definition are highly subjective and should be used only ass a guide to the authors perceptions of the value of data or a system.

1.4 Risk Rating Scales

To provide the assessment team with a meaningful means of assessing and quantifying the security risks associated with the UVS system the following scales have been defined:

1.4.1 Risk Impact

The following table explains how the impact that a risk item can have on the SERVE system is documented.

Risk Name	Risk Description
High Impact	Likely to severely damage SERVE or its reputation
Medium Impact	Risk could cause significant damage but SERVE will survive
Low Impact	Type of impact that is expected as part of normal operation

1.4.2 Risk Probability

The following table explains how the probability a risk item can have on the SERVE system is documented.

Risk Name	Risk Description
High Probability	A substantial likelihood of a weakness or threat exists
Medium Probability	Some likelihood of a weakness or threat exists
Low Probability	Very little likelihood of a weakness or threat exists

1.4.3 Priority Matrix

The following table describes the risk priority that is generated by the risk probability and impact.

Facilitated Risk Analysis Process (FRAP)
Priority Matrix

		Risk Impact		
		High	Medium	Low
Risk Probability	High	A	B	C
	Medium	B	B	C
	Low	C	C	D

1.4.4 Priority action table

The priority Action table gives the FRAP user an idea of the importance of action in relation to the risk element.

Priority Action Table
A - Corrective Action Must be Initiated
B - Corrective Action Should be Initiated
C - Requires Further Evaluation
D - No Action Required

2 Internet Voting Risk

The very nature of voting due to the complexity of the process, whether paper, mechanical, electronic, or Internet enabled, is inherently risky and labors under numerous threats. History has shown that people and organizations will try to thwart the process in order to sway the outcome in their favor. The election process has been demonstrated to be an attractive target for malicious actions. As such a requirement of any voting system especially an online voting system is that it must have public confidence, which could easily be undermined by an election horror story.

Before exploring the specific risks to the SERVE Internet voting project it is beneficial to cover the general risks and their associated entities that are inherent to the Internet voting process. Section 2.1 describes the general Internet voting risks and the entities associated with them to give the reader an introductory understanding of the basic risks associated with the voting process. The specific SERVE risks described in section 4.0 may then be considered within this broader context.

2.1 Threats to Internet Voting

Internet Voting breaks down the geographic barriers of traditional election systems. The election system is no longer confined to the local polling station; it is accessible world-wide, increasing the opportunity and in some cases the potential number and types of attacks.

This section makes no assumptions with regards to the specific configuration of the Internet voting system. This section of the assessment is based on the assumption that the Internet voting system will have at least one connection to the Internet affording external Internet specific access to the voting platform, the system will be made up of at least 2 parts a server and client and the voting related information will be available online and could be of a personal nature.

2.1.1 Potential Sources of attack

Internal
Legitimate users
Legitimate users of the Internet voting system may seek to misuse or damage the election system and may have significant technical resources and skills at their disposal, with a strong motivation to subvert the service. Since they are legitimate users, they are subject to legal or procedural sanctions if the subversive activity is traced to them.

System operators
The Internet voting system operators may seek to exploit their privileged position. They may include government employees or their agents or employees of outside organizations providing the systems services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation could be a desire to defraud the election process, either for financial gain or personal satisfaction. Contracted operators and government employees are readily subject to sanction in the event that security breaches are traced to them.

Other Insiders
Government employees and their agents, who may have access to the system or its documentation but who are not associated with the provisioning of election services, may conduct insider attacks. These individuals may possess a strong motivation to mount an attack for financial or personal gains. Such individuals, if discovered, will be readily subject to sanctions.

External

Hostile Individuals

Malicious entities may seek to cause disruption to systems because of a personal grudge, for the challenge of attacking the system or in protest against candidates and their parties or government policies. They may also wish to access, disclose, corrupt or steal data, either for personal gain or for publicity purposes.   These types of entities may be difficult to apprehend due to their location and ability to hide their actions.

Criminal Organizations

Criminals may also wish to access systems in order to obtain personal details for exploitation or to affect the outcome of an election. Organized crime is a larger target for law enforcement than single individuals but could still pose equally as difficult as the hostile individuals. It is interesting to note that some of the government security experts felt that this is the most likely group to attack an Internet voting system with specific aims of affecting a local election.

Protest Groups

Protest groups may seek to attack a voting system in order to demonstrate opposition to Internet voting, to disrupt the Internet voting mechanism or to obtain data to exploit, for information or aggrandizement purposes.   The protest groups depending on their size and nature will range in difficulty somewhere in between malicious entities and criminal organizations.

Foreign Intelligence Services

Foreign intelligence services may see an advantage in obtaining personal information, for intelligence-gathering and targeting purposes. They may also wish to access or block access to systems for political information-gathering purposes or to manipulate voting information in order to influence the election outcome.

Investigative Journalists

Investigative journalists may be interested in deliberately subverting the election system in order to prove that an Internet voting system has security flaws. Journalists are usually attached to organizations that are readily subject to sanction in the event that security breaches are traced to them.

Terrorist Organizations

Terrorist organizations may be interested in personal information stored on the system for targeting and intelligence-gathering purposes. They may also wish to interrogate the system in order to understand voting intentions, to affect the outcome or to cause disruption to the process. Terrorist organizations range in difficulty between the malicious entities and the foreign intelligence services in their ability and difficulty to protect against and prosecute.

2.1.2 Possible Methods of attack

Electronic Attack

Purposeful Unauthorized Access

Penetration of the Internet voting system would have very serious ramifications, both for public confidence in online voting and with regards to state and federal statutes. To be effective, such an attack does not have to modify the data stored in the system, but merely put it into the public domain. Penetration of the system need not take place during the polling period, but potentially any time before or after the event. Large amounts of personal information used by the Citizens to authenticate themselves in the registration phase might be divulged. This information could be used to link votes with individuals, undermining voter anonymity. There is also the potentially less serious threat of the appearance of the site being changed; this would undermine public confidence in the system though possibly not reduce its functionality. If the hyperlinks on the site were changed this could affect the integrity and confidentiality of the votes cast; this might result in an entire election being declared void.

Malicious Software (malware)
There is a risk of malicious software being introduced onto the system before or during the election. Furthermore, the connection of huge numbers of personal computers to the system may increase the chances of malware being spread to the Internet voting system if security is not properly designed into the system. This could cause damage to the server and potentially propagate to local election officials or Citizen PCs. The government or operators could potentially be liable for any resultant damage. If a program such as a Trojan Horse were to be installed on the systems web server, the confidentiality and integrity of the votes could be adversely affected, in the worst case resulting in all affected elections being declared void.

The insecurity of browsers and operating systems on client platforms will invariably make it possible to subversively install malicious software. It is possible for an attacker to introduce malware that has an activation delay on to the client platform, where it would remain undetected until activated on the date of the election or some period before. Installation of a program such as hostile mobile code could compromise the confidentiality and integrity of an individuals vote, by communicating information on how an individual voted to a third party, or by changing the vote before transmission without the users knowledge respectively.

Denial of Service (DOS)
An exceptionally high volume of Citizens using the Internet voting system might cause the system to become temporarily unavailable if appropriate provisions are not made for scale. A malicious DOS attack like the ones launched against Yahoo or mass unintentional misuse may also cause the system to become unavailable.

The client may be denied service by an attack on the Internet, such as the publicized root Domain Name Server (DNS) attacks. It is also possible that a number of client devices are attacked using a program to initiate a large number of redundant computations, which could render the client voting devices useless.

Domain Name Service (DNS) Attacks
It is possible that an attacker may alter an entry in a DNS lookup table to point to an alternate web address. This would enable the owner of the bogus site to modify or view the vote of the redirected Citizen. The same effect can be achieved by introducing a program that tells the browser to use a certain web address as a proxy, essentially affording a man-in-the-middle attack.

Routing Attacks
The client at the lowest level communicates with the IP (Internet Protocol) address of the internet service and if an attacker were to corrupt the routing tables near the Internet voting web server. All traffic could be redirected to an alternate site allowing the attacker to modify or view the vote of the redirected Citizen much like the DNS man-in-the-middle attack.

Other non technical attack approaches

Vote buying/ selling and coercion
Vote buying and selling are as possible electronically as they are with the current absentee voting postal based system. If a person wants to sell their vote currently there is no possible way to stop them. Coercion of the Citizen can be more effectively accomplished in the Internet and standard absentee system than in the polling place as more direct contact with the Citizen is available during the voting process but the effective scale is considerably smaller due to the number of resources required to watch each remote Citizen at his voting location.

An interesting effect of Internet voting is it might allow an enterprising Citizen to print multiple vote receipts from their screen (no system using home PCs can stop this) showing they had voted more than one way and using the multiple receipts collect from more than one candidate trying to buy their vote. This technique would still allow the Citizen to vote their mind while harvesting money from less reputable candidates or their sponsors.

Theft or forgery of election details
Theft and forgery of Citizen details is possible either electronically or from the postal system. Depending on the design of the Internet voting system and the location and security surrounding the storage of the Citizen related data this attack would most probably be detected. If this type of attack were accomplished it would provide a potent source of data for use by the attacker.

Multiple voter registrations
Registering to vote in multiple counties is a trivial effort in states without central voter registration databases and both the postal system and the electronic system are vulnerable to this type of attack. A central electronic system could be made more resistant to this risk but could not completely prevent multiple registrations as attackers would move to the next logical step and register in multiple states.

Deliberate repudiation of transaction
A malcontent Citizen or group of Citizens could potentially go to the Local Election Official or the media and claim they did not vote, they voted more than once or their vote was misinterpreted by the system. This could be used in an attempt to undermine the online voting process.

Accidental damage
Users
Legitimate users may unintentionally misuse the Internet based voting system and potentially cause damage to the system. Large numbers of Citizens using the system incorrectly could result in unnecessary loss in performance of the System or even cause it to crash. This risk can be mitigated by thorough testing with large numbers of trained and untrained users.

Operators
Operators may, through error, incompetence and/or inadequate training, cause damage to the system or loss of data. Such individuals are not specifically motivated to carry out such an attack but, due to their privileged access rights, may unwittingly cause significant damage.

Equipment
Equipment or software failure along any part of the Internet voting path may lead to suspension of service or loss of user or vote information.

Force Majeure
An accident or other natural disaster may destroy the Internet voting service or stored information.

3 Project Criticalities

The SERVE project has a number of systems and data types. Each of these elements needs to have its criticality defined to provide the areas defined in the threat risk assessment a frame of reference. This section defines the SERVE projects information criticality and the general subsystems in each of the SERVE Systems or areas.

3.1 *SERVE Information Criticality*

The following chart defines the SERVE information types that require risk mitigation and the level of their criticality to the project as defined by their impact values.

SERVE Information Criticality Matrix		Impact Attributes		
		Confidentiality	Integrity	Availability
SERVE Information Repositories	SERVE I&A data	High	High	Medium
	Registration data	High	Medium	Low
	VR data	Medium	High	Low
	Ballot Styles	Medium	High	Medium
	Vote Data	High	High	Medium
	Logs	Low	Medium	Low

From the SERVE Information Criticality Matrix we can derive the overall organizational criticality. As shown Confidentiality and Integrity both rate high and Availability rates medium. This demonstrates that to the project as a whole the confidentiality and integrity of the data is more important than the availability. This type of rating is indicative of a system that operates over a period of time and contains private personal data.

SERVE Organizational Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

3.2 *SERVE Central (UVS) Criticality*

Shown below are the criticality matrixes for the information types used in the UVS system aligned with their respective subsystems. These data are combined with the other sections to arrive at the tables in section 3.1.

Voter Registration Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low

Voter Registration Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
Medium	High	Low

Ballot Definition Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low
Ballot Styles	Medium	High	Medium

Ballot Definition Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
Medium	High	Medium

Voting Engine Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low
Ballot Styles	Medium	High	Medium
Vote Data	High	High	Medium

Voting Engine Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

Ballot Reconciliation Information Criticality Matrix			
	Confidentiality	Integrity	Availability
Ballot Styles	Medium	High	Medium
Vote Data	High	High	Medium

Ballot Reconciliation Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

I&A Information Criticality Matrix			
	Confidentiality	Integrity	Availability
SERVE I&A data	High	High	Medium

I&A Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

3.3 VeriSign Systems Criticality

Shown below is the criticality matrix for the information types used in the VeriSign system (Roaming Certificate Service) aligned with its respective subsystems. These data are combined with the other sections to arrive at the tables in section 3.1.

I&A Information Criticality Matrix			
	Confidentiality	Integrity	Availability
SERVE I&A data	High	High	Medium
Registration data	High	Medium	Low
Logs	Low	Medium	Low

I&A Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

3.4 LEO Systems Criticality

Shown below are the criticality matrixes for the information types used in the local LEO system aligned with their respective subsystems. These data are combined with the other sections to arrive at the tables in section 3.1.

Voter Registration Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low

Voter Registration Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
Medium	High	Low

Ballot Definition Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low
Ballot Styles	Medium	High	Medium

Ballot Definition Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
Medium	High	Medium

Ballot Reconciliation Information Criticality Matrix			
	Confidentiality	Integrity	Availability

Ballot Styles	Medium	High	Medium
Vote Data	High	High	Medium

Ballot Reconciliation Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

3.5 Citizen Workstation Criticality

Shown below are the criticality matrixes for the information types used in the Citizen system aligned with their respective subsystems. These data are combined with the other sections to arrive at the tables in section 3.1.

Voter Registration Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low

Voter Registration Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
Medium	High	Low

Voting Process Information Criticality Matrix			
	Confidentiality	Integrity	Availability
VR data	Medium	High	Low
Ballot Styles	Medium	High	Medium
Vote Data	High	High	Medium

Voting Engine Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

I&A Information Criticality Matrix			
	Confidentiality	Integrity	Availability
SERVE I&A data	High	High	Medium

I&A Criticality Matrix		
Impact Attributes		
Confidentiality	Integrity	Availability
High	High	Medium

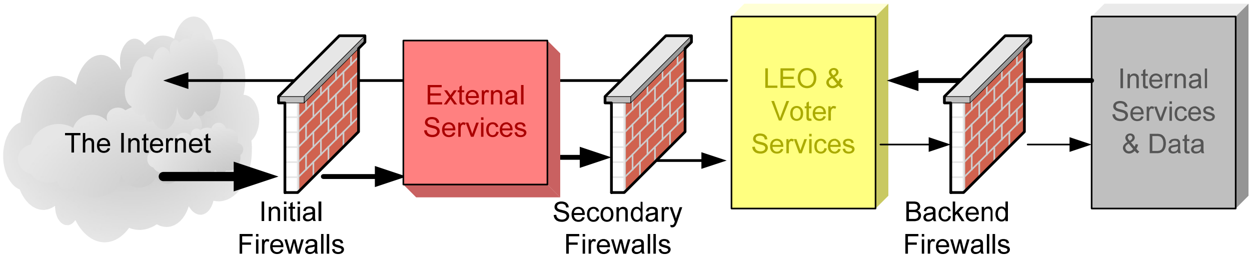
4 SERVE Security Risks

To provide a meaningful risk assessment the SERVE infrastructure has been separated into four distinct areas for the purpose of this assessment. The four major areas of the project listed in order of those being most under project control to least are SERVE site / UVS, VeriSign hosted roaming certificate infrastructure, State / LEO and Citizen. Most risks were found to be applicable to several of the areas with only a few exceptions that were area specific.

4.1 SERVE Site Risks

The SERVE site / UVS provides the largest number of points of attack but is also directly under the project's control. Most of the risks that were described in section 2 can be applied to the SERVE site and its infrastructure and as such considerable time and effort must be taken to protect this vulnerable area. Shown below is a simplified view of the SERVE Site infrastructure.

4.1.1 SERVE Site Diagram



4.1.2 SERVE Site Priority Risk Discussion

The following section lists the UVS site risks in a narrative form and also discusses their mitigations. The risks have received either a rating of **A** (Corrective action must be initiated) or a Rating of **B** (Corrective action should be initiated) and have no current identified mitigations.

Risk: 103
Type: A
Risk title: Virus' / Worms / Trojans
Description: Malware that could affect the operation of the UVS infrastructure.
Mitigations: Antivirus software, Veracity, Patch management
Notes: This risk has a strong mitigation in the form of Antiviral software. Also UVS will employ Veracity to check the file integrity against a known hash. Another possible mitigating strategy is software updates or patches.

Risk: 46
Type: B
Risk title: DNS poisoning with site redirection
Description: This risk covers things like man in the middle attacks or blocking the voter from voting
Mitigations: Voter education, IP logging

Notes: DNS poisoning to redirect a target to an improper site is one of the oldest tricks in the malfeasants arsenal. A further wrinkle in the attack is to then use the bridge site to connect to the original site and translate the site content between the real user and real site. This attack is less effective when site certificates are used but the human factor comes into play and some people will ignore the displayed browser warning. A large scale attack of this sort would become evident though IP logging to an alert administrator or through a user calling the help desk.

Risk: 63
Type: B
Risk title: Inability of entities to access confidential data at a later date due to certificate revocation
Description: This risk is specific to the roaming certificate services. But since the user certificates are only used for access to the system this risk has been fully mitigated.
Mitigations: N/A
Notes: Non issue in current system design

Risk: 65
Type: B
Risk title: of user IDs on the system (administrative users)
Description: User level ID's on the SERVE UVS systems are only issued to administrators. These ID's could be shared among users if the administrators were acting inappropriately or by mistake.
Mitigations: User education, Management oversight
Notes: Through mistake or intent administrative accounts could be shared. This is a human nature problem and operations personnel must be schooled to the dangers inherent in this problem on a repeated basis. Also with sufficient management over site inappropriate actions by the administrators can be reduced.

Risk: 77
Type: B
Risk title: Release or exposure of Citizen personal data
Description: Through technical or personal error or intent Citizens data could be exposed.
Mitigations: SERVE Policy, Full complement of technical safeguards in system
Notes: Though every reasonable measure is being applied to the technology infrastructure and through policy it is still possible that leak could happen.

Risk: 82
Type: B
Risk title: New technologies leading to breaches of confidentiality
Description: Evolving technologies and ideas will lead to new abilities to defeat the current security measures.
Mitigations: None
Notes: Encryption is used through out the system but with all security related computer technology eventually it will be defeated. The current laws require certain classes of information to be stored for an extended period of time thus giving malfeasants the opportunity to decipher and protected material eventually.

Risk: 89
Type: B
Risk title: Disclosure of information and violation of privacy laws
Description: Depending on the location the Citizen is using the system the privacy laws could be more sever than in the US jurisdiction that the voter is voting in.
Mitigations: None

Notes: With any process where data of a personal nature is collected there is the possibility of disclosure. UOCAVA voters are by definition in other countries and in many cases are covered under local law. It is possible that an inadvertent exposure or a legal exposure of data in the US could be construed as illegal in another country.

Risk: 3
Type: Integrity
Risk title: Unauthorized internal access leading to data modification (Logical)
Description: An agent of SERVE with administrative equivalency could modify data.
Mitigations: Separation of duty, logging, oversight
Notes: Though internal threats are hard to combat they can be counteracted to the point that the amount of work and risk required to succeed is more than is warranted by the gain.

Risk: 13
Type: Integrity
Risk title: Unspecified In House Software Bugs
Description: Any large piece of software will have bugs.
Mitigations: Software testing (IV&V or ITA), Internal code reviews
Notes:

Risk: 19
Type: Integrity
Risk title: Modification of data due to Virus' / Worms / Trojans
Description: Malware could be crafted specifically for the SERVE system to modify its data or a piece of non specific malware could target one of the servers of services that SERVE uses and inadvertently damage data.
Mitigations: Antivirus software, Multi layered infrastructure, Backup
Notes: Data modification can happen in a number of ways and are covered elsewhere.

Risk: 27
Type: Integrity
Risk title: Data corrupted due to an incomplete transaction
Description: Due to the multi-tiered architecture of SERVE it is possible a transaction could fail before an activity was completed.
Mitigations: Logging, Citizen data checked by Citizen before it is marked as saved
Notes: The process that the vote follows before it is salved as the Citizens choice is an excellent example of the protections built into the system to combat this exact problem.

Risk: 39
Type: Integrity
Risk title: Unrecorded changes to system/application software or data
Description: A method of attack against systems is to modify the system in some fashion that causes it to work in a fashion other than was designed.
Mitigations: Logging, Veracity, IV&V or ITA
Notes: By using a combination of processes this risk can be reduced considerably though there will always be people who do not feel it has been reduced enough.

Risk: 43
Type: Integrity
Risk title: Personnel making changes who are not properly trained
Description: Well meaning but non trained personnel have reduced the working efficiency of many systems.
Mitigations: Operations training with management signoff.

Notes: By providing proper training and making management signoff on that training you can reduce the likelihood that errors will be introduced into and operating system significantly.

Risk: 45
Type: Integrity
Risk title: Operations processes so complicated they are ignored
Description: Effective operations processes must be short and easy to read. Complexity and length almost insure procedures written with the beast of intent are not used on a day to day basis.
Mitigations: Proper documentation, System training, Management signoff
Notes: Through the use of good documentation, training and placing the responsibility for conformance on management this risk can be reduced significantly.

Risk: 66
Type: Confidentiality
Risk title: Ability to assume another person's identity
Description: A system should be designed to reduce the ability of a person to steal another persons identity.
Mitigations: Roaming certificates, ID proofing process
Notes: The roaming certificate process is designed to make identity assumption hard and the ID proofing process used for SERVE is an in person process.

Risk: 70
Type: Confidentiality
Risk title: Ex staff still has access to secure data
Description: Staff that are no longer on the project must no longer have access to the system
Mitigations: Operational procedures, Security policy
Notes: This is a real problem with most systems. With the SERVE system we at least have protection that Administrative accounts cannot be used unless you are internal to the system providing some level of basic protection.

Risk: 108
Type: Availability
Risk title: Program bugs
Description: COTS software having unexpected bugs or errors
Mitigations: Software testing, Certification or IV&V, Patch management
Notes: All software including software bought for SERVE

Risk: 109
Type: Availability
Risk title: Application Design flaws may cause resource thrashing or internal resource contention
Description: IF an application is not designed and implemented correctly especially when distributed across many layers of infrastructure these faults can cause the system to perform a denial of service attack against its self.
Mitigations: Utilization monitoring, Code review, Testing
Notes: Performance testing is one of the best mitigations for this threat.

Risk: 132
Type: Availability
Risk title: DOS attacks against serve systems
Description: Denial of Service attacks can be applied to a system at almost any point. For this reason a well planned and executed attack can be very difficult to defend against.
Mitigations: IDS, Large quantity of bandwidth, Multiple Internet providers, Monitoring, Oversized equipment, Defined response procedures

Notes: Due to the large number of attack points many mitigations must be used to provide a reasonable ability to respond to this threat.

Risk: 134
Type: Availability
Risk title: Planned attack by protesters or hacktivists
Description: Organized attacks by people driven by their beliefs can be difficult to prevent. These types of groups are very active and the SERVE system would make a rich target for them.
Mitigations: All known system mitigations.
Notes: The large number of possible means for this type of motivated group makes any and all mitigations used by the system a possible mitigator for this attack.

4.1.3 SERVE Site Risk Elements

Priority	Risk #	Risk Title:	Mitigations	Risk Type	Risk Notes:
A	103	Virus' / Worms / Trojans	Antivirus software, Veracity, Patch management	Availability	
B	46	DNS poisoning with site redirection	Voter education, IP logging	Integrity	
B	63	Inability of entities to access confidential data at a later date due to certificate revocation	N/A	Confidentiality	After further system study it has been determined this is not a risk to SERVE
B	65	sharing of user IDs on the system (administrative users)	User education, Management oversight	Confidentiality	
B	77	Release or exposure of Citizen personal data	SERVE Policy, Full complement of technical safeguards in system	Confidentiality	Type of data collected changed
B	82	New technologies leading to breaches of confidentiality	None	Confidentiality	
B	89	Disclosure of information and violation of privacy laws	None	Confidentiality	
B	3	Unauthorized internal access leading to data modification (Logical)	Separation of duty, logging, oversight	Integrity	
B	13	Unspecified In House Software Bugs	Software testing (IV&V or ITA), Internal code reviews	Integrity	
B	19	Modification of data due to Virus' / Worms / Trojans	Antivirus software, Multi layered infrastructure, Backup	Integrity	

▦ B	27	Data corrupted due to an incomplete transaction	Logging, Citizen data checked by Citizen before it is marked as saved	Integrity	
▦ B	39	Unrecorded changes to system/application software or data	Logging, Veracity, IV&V or ITA	Integrity	Before or after certification
▦ B	43	Personnel making changes who are not properly trained	Operations training with management signoff	Integrity	
▦ B	45	Operations processes so complicated they are ignored	Proper documentation, System training, Management signoff	Integrity	
▦ B	66	Ability to assume another person's identity	Roaming certificates, ID proofing process	Confidentiality	
▦ B	70	Ex staff still has access to secure data	Operational procedures, Security policy	Confidentiality	
▦ B	108	Program bugs	Software testing, Certification or IV&V, Patch management	Availability	COTS
▦ B	109	Application Design flaws may cause resource thrashing or internal resource contention	Utilization monitoring, Code review, Testing	Availability	
▦ B	132	DOS attacks against serve systems	IDS, Large quantity of bandwidth, Multiple Internet providers, Monitoring, Oversized equipment, Defined response procedures	Availability	
▦ B	134	Planned attack by protesters or hacktivists	All system mitigations	Availability	
▦ C	8	Information accessed by individuals not authorized to access the data	Procedures, monitoring and reporting	Confidentiality	Just viewing data
▦ C	17	Code used to create or process the signature is compromised on the Server	Veracity	Integrity	
▦ C	18	Code used to encrypt or decrypt the vote is compromised on the server	Veracity	Integrity	
▦ C	47	Route poisoning with site redirection	None	Integrity	

▦ C	54	Access to backups is not properly controlled	SLA with VeriSign, VeriSign security policy	Confidentiality	VeriSign has procedures
▦ C	58	Authentication for access to sensitive information is inadequate	User training	Confidentiality	
▦ C	64	Allocation of security privileges not known to the organization	Security assessment	Confidentiality	
▦ C	68	Sensitive and non sensitive information is mixed	Policy and procedures, User training, ITA testing	Integrity	
▦ C	92	Encrypted copy of vote stored for retention period decrypted using new technology	None	Confidentiality	
▦ C	94	Information about system is inadvertently released for potential later use	Policy and procedures, User training	Confidentiality	
▦ C	96	Disgruntled admin staff with high security privileges	Management oversight	Confidentiality	
▦ C	99	Access to sensitive information through the test environment	Policy and procedure, User training, Security testing	Confidentiality	
▦ C	129	DNS poisoning (DOS)	None	Availability	
▦ C	130	Route poisoning (DOS)	None	Availability	
▦ C	133	Loss of users due to site unavailability	High level s of redundancy built into system	Availability	Project risk
▦ C	138	Disgruntled admin staff with high security privileges	Management oversight, User training	Availability	
▦ C	145	Code used to create or process the signature is compromised on the Server	Veracity	Availability	
▦ C	14	Citizen gets incorrect ballot from system	LEO testing, ITA testing	Integrity	
▦ C	23	Corrupted database	Backups	Integrity	
▦ C	26	Internal personnel deliberately modifying data for personal/group gain/reason	Management oversight, Training, Separation of duties	Integrity	
▦ C	36	Old versions of online data is not marked correctly	ITA testing, LEO testing	Integrity	
▦ C	37	Lack of change and version control process	Policy and procedures	Integrity	

▦ C	41	Use of an out of date version of backup data	Policy and procedures, Management oversight	Integrity	
▦ C	48	Ability to change data in transit	Data encryption, Data signing, Server checks, User reverification	Integrity	
▦ C	49	SERVE embarrassment due to changing of web content	Veracity, Hardware and software firewalls, Site monitoring	Integrity	
▦ C	73	Electronic eavesdropping of data (external to site) while in transit	Encryption	Confidentiality	
▦ C	74	Electronic eavesdropping of data (internal to site) while in transit	Separation of duties, encryption, Veracity, IDS	Confidentiality	
▦ C	76	Use of insecure systems to transmit data (Server systems)	ITA testing	Confidentiality	
▦ C	85	Keyboard logging Trojan	Antivirus software, Veracity	Confidentiality	
▦ C	97	Introduction of back doors into software, applications and data	Code reviews, ITA testing, LEO testing, Management oversight	Confidentiality	
▦ C	113	Insufficient monitoring of services may fail to report unavailability	SLA with VeriSign, Help desk procedures, Operations procedures	Availability	
▦ C	114	Backups are insufficient or not taken correctly	ITA testing, Internal testing, VeriSign testing	Availability	
▦ C	116	Technical resources lack proper training	Policy and procedures, User training	Availability	
▦ C	117	Planned maintenance will cause service outage	None	Availability	
▦ C	120	Unanticipated volumes or usage projections	Site designed to service 2 times projected number of users	Availability	
▦ C	122	Incorrectly made hardware or software changes	User training, Policy and procedures, Change control	Availability	
▦ C	123	Router or firewall failure or misconfiguration may cause inaccessibility to services	Change control, Redundant equipment, DR site	Availability	

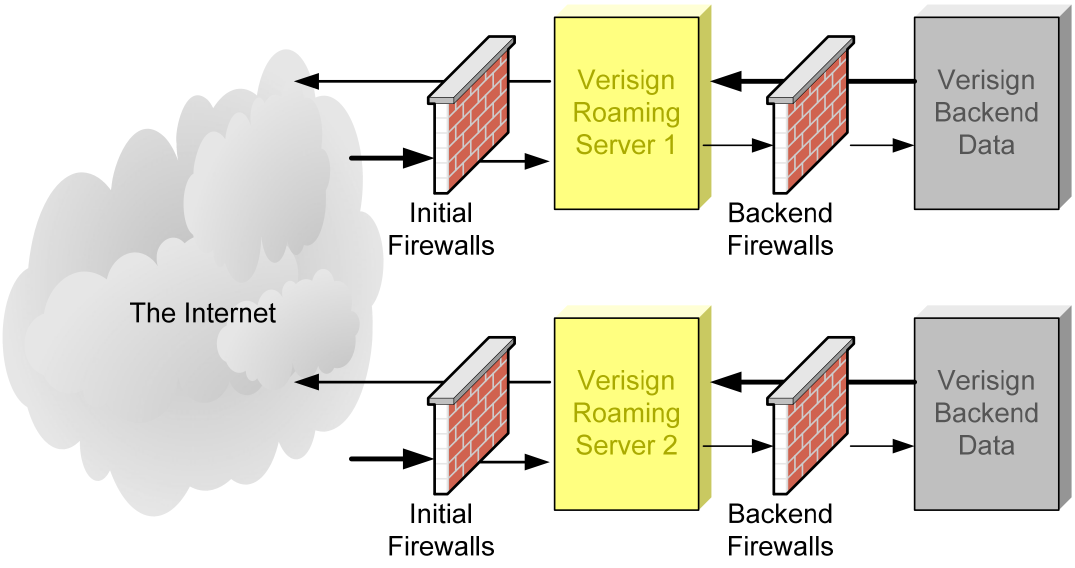
C	125	Links to back end systems fail	Redundant equipment, DR site	Availability	Server to server
C	128	Internet provider service outage blocks access for clients	Multiple Internet service providers	Availability	
C	148	Hardware failure of front end servers	Redundant equipment, DR site	Availability	
C	149	Hardware failure of backend servers	Redundant equipment, DR site	Availability	
C	140	Hackers bringing down SERVE site by attacking web servers	Multiple layers of firewalls, IDS, Software based firewall shim for IIS, ITA testing, VeriSign testing, Internal testing	Availability	
C	143	Software Fix breaks voting engine	Change control process	Availability	
C	144	Database holding votes is destroyed	Backup, DR site	Availability	
D	2	Unauthorized internal access leading to data modification (Physical)	Physical site security, separation of duties	Integrity	
D	51	Citizen registers in multiple locations (counties)	N/A	Integrity	This is an allowable action in current system by design
D	107	Intruders gaining physical access to servers and bringing them down	Physical site security	Availability	
D	136	Industrial action or strike at service provider	VeriSign SLA	Availability	
D	139	International ISP blocks access to SERVE voting site	None	Availability	
D	40	Incomplete or nonexistent documentation for system	ITA testing	Integrity	
D	57	Granting access to sensitive data to individuals who do not have business need	Policy and procedures, Management oversight, ITA testing	Confidentiality	System administration related
D	62	Developer access is not removed after the project is complete	Policy and procedures, ITA testing, Management oversight	Confidentiality	
D	72	No clear definition of confidentiality rules	Policy and procedures	Confidentiality	

D	79	Release or exposure of voted ballot	Encryption	Confidentiality	
D	110	Lack of application disaster recovery plan	Management oversight, Policy and procedures	Availability	
D	112	Lack of plan to restore backups	Testing, Policy and procedures	Availability	
D	118	Contingency planning procedures not tested	ITA testing	Availability	
D	147	Hardware configuration is insufficient for load	System designed for two times theoretical load	Availability	
A	100	Access Project data transferred among project members using insecure transfer methods	N/A	Confidentiality	Project risk transferred to risk tool
A	135	Inadequate funding for backup capability	N/A	Availability	Project risk transferred to risk tool
B	69	Hardcopy management (production, distribution and destruction)	N/A	Confidentiality	Project risk transferred to risk tool
B	50	Non overseas Citizen uses system to vote	N/A	Integrity	Citizen does not have to be overseas
N/A	81	Release or exposure of unvoted ballot	N/A	Confidentiality	Dynamically generated no concept of unvoted ballot

4.2 Roaming Certificate Infrastructure Risks

The VeriSign Roaming Certificate Infrastructure is utilized to provide the Identification and Authentication for the SERVE infrastructure. The central role this service plays to the SERVE infrastructure makes it a likely target for malicious activity. The SERVE team does not have control over the VeriSign infrastructure but VeriSign is providing an equivalent level of security as is provided for the UVS site. To make the risk assessment and documentation less complex the Roaming Certificate Infrastructure is referred to as VeriSign throughout the remainder of the document. Shown below is a simplified view of the VeriSign infrastructure.

4.2.1 VeriSign Diagram



4.2.2 VeriSign Priority Risk Discussion

The following risks received either a rating of **A** (Corrective action must be initiated) or a Rating of **B** (Corrective action should be initiated). These risks warrant attention as the project moves forward and may need to have further mitigations applied or may need to be accepted by management. The VeriSign risk portfolio is the smallest of the risk areas as VeriSign has a distinct area of operation and has tested policies and procedures in place.

Risk: 66
Type: B
Risk title: Ability to assume another persons identity
Description: We use the VeriSign Roaming Certificates to control and provide access to all external parities. If a malfeasant were to determine a way to misuse this authenticating infrastructure we could possibly have difficulty proving identity.
Mitigations: None
Notes: The VeriSign infrastructure houses one of the core security strengths of the SERVE project. This infrastructure is of such importance that a malfeasant who had gained access to an account with escalated privileges would be extremely detrimental to the project. For this reason this risk was highlighted by the review team and needs consideration throughout the project lifecycle.

Risk: 82
Type: B
Risk title: New technologies leading to breaches of confidentiality
Description: New ideas or technologies could allow an attacker to view the information sent between the VeriSign servers and a remote user in real time.
Mitigations: None
Notes: Encryption is used throughout the system but with all security related computer technology eventually it will be defeated. The current laws require certain classes of information to be stored for an extended period of time thus giving malfeasants the opportunity to decipher and protected material eventually. VeriSign provides the roaming certificate infrastructure and the initial

SERVE system user registration functions. The sanctity of these activities must be protected throughout the project through advancement of technology and strict adherence to policy.

Risk: 20
Type: Integrity
Risk title: Modification of data due to Virus' / Worms / Trojans
Description: Malware that is either specific to or compatible with the VeriSign infrastructure could destroy or make less effective the database or software that runs the roaming service.
Mitigations: Antivirus software
Notes: The roaming servers are Unix based and as such there are less malware writers attacking them currently. Also these servers are operated using best practices so the likelihood of a piece of malware being introduced is reduced.

4.2.3 VeriSign Risk Elements

Priority	Risk #	Risk Title:	Mitigations	Risk Type	Risk Notes:
B	66	Ability to assume another person's identity	None	Confidentiality	
B	82	New technologies leading to breaches of confidentiality	None	Confidentiality	
B	20	Modification of data due to Virus' / Worms / Trojans	Antivirus software	Integrity	
C	2	Unauthorized internal access leading to data modification (Physical)	Physical security measures	Integrity	
C	9	Information accessed by individuals not authorized to access the data	Physical security measures, Logical security measures	Integrity	
C	44	Personnel making changes who are not properly trained	User training, Management oversight	Integrity	
C	45	Operations processes so complicated they are ignored	Management oversight	Integrity	
C	46	DNS poisoning with site redirection	None	Integrity	
C	47	Route poisoning with site redirection	None	Integrity	
C	65	sharing of user IDs on the system	User training	Confidentiality	
C	115	Technical resources lack proper training	User training, Management oversight	Availability	
C	117	Planned maintenance will cause service outage	None	Availability	
C	129	DNS poisoning	None	Availability	

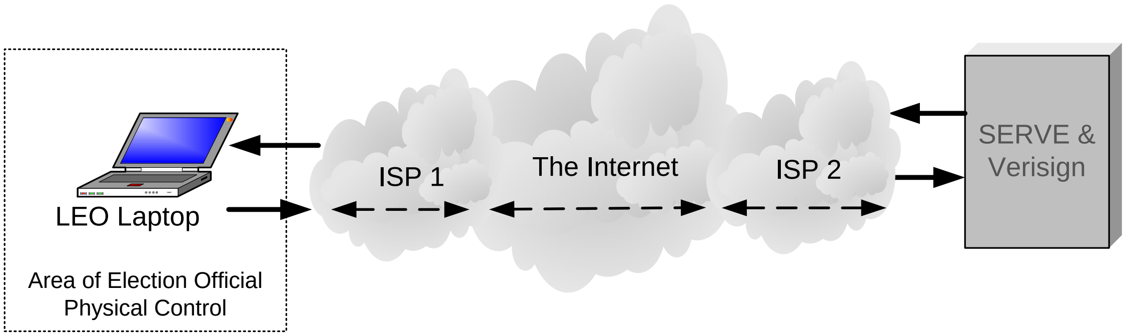
C	130	Route poisoning	None	Availability	
C	133	Loss of users due to site unavailability	24/7 monitoring and DR facility	Availability	
C	13	Unspecified In House Software Bugs	Internal testing, ITA testing	Integrity	
C	24	Corrupted database	Backup and DR facilities	Integrity	
C	73	Electronic eavesdropping of data (external to site) while in transit	Encryption	Confidentiality	
C	104	Virus' / Worms / Trojans	Purpose built platform with no other functions	Availability	
C	120	Unanticipated volumes or usage projections	Ability to add more server as needed	Availability	
C	123	Router or firewall failure or misconfiguration may cause inaccessibility to services	Redundant equipment	Availability	
C	132	DOS attacks against UVS system	Multiple Internet providers, Large quantities of bandwidth, Multiple servers	Availability	
C	134	Planned attack by protesters or hactivists	All SERVE security mitigations apply	Availability	
C	141	Hackers bringing down Roaming Certificate servers by attacking web servers	VeriSign testing, Backup servers	Availability	
C	147	Hardware configuration is insufficient for load	VeriSign internal testing, Multiple servers	Availability	
D	4	Unauthorized internal access leading to data modification (Logical)	Policy and procedure, Management oversight	Integrity	
D	38	Unrecorded changes to system/application software or data	Encryption, Logging	Integrity	
D	55	Access to backups is not properly controlled	Policy and procedure, Management oversight	Confidentiality	
D	59	Authentication for access to sensitive information is inadequate	Policy and procedure	Confidentiality	
D	70	Ex staff still has access to secure data	Policy and procedure, Management oversight	Confidentiality	

▦ D	75	Electronic eavesdropping of data (internal to site) while in transit	Separation of duties, Policy and procedure, Management oversight, Network segmentation	Confidentiality	
▦ D	96	Disgruntled admin staff with high security privileges	Management oversight	Confidentiality	
▦ D	111	Lack of application disaster recovery plan	Management oversight, Testing	Confidentiality	Tested every 6 months
▦ D	119	Contingency planning procedures not tested	Management oversight, Testing	Availability	Tested every 6 months
▦ D	122	Incorrectly made hardware or software changes	Operations procedures, Management oversight	Availability	
▦ D	136	Industrial action or strike at service provider	None	Availability	
▦ D	138	Disgruntled admin staff with high security privileges	Management oversight	Availability	
▦ D	148	Hardware failure of front end servers	Backup servers, DR site	Availability	Auto recovery of load balanced servers
▦ D	149	Hardware failure of backend servers	Backup servers, DR site	Availability	
▦ D	48	Ability to change data in transit	Encryption, Proprietary protocol	Integrity	
▦ D	85	Keyboard logging Trojan	Operations procedures	Confidentiality	
▦ D	113	Insufficient monitoring of services may fail to report unavailability	Operations procedures, Testing	Availability	
▦ D	128	Internet provider service outage blocks access for clients	Multiple internet providers	Availability	
N/A	63	Inability of entities to access confidential data at a later date due to certificate revocation	N/A	Confidentiality	Not relevant for roaming

4.3 State / LEO Risks

The State / LEO areas provide a more difficult set of attack points due to their distributed nature for malicious individuals from a remote standpoint but an easier area to attack due to the possible physical access to the locations. SERVE will provide the Local Election Officials with mobile computing platforms to perform their SERVE specific duties. Shown below is a simplified view of a LEO Site infrastructure.

4.3.1 State / LEO Diagram



4.3.2 State / LEO Priority Risk Discussion

The following risks received either a rating of **A** (Corrective action must be initiated) or a Rating of **B** (Corrective action should be initiated). These risks warrant attention as the project moves forward and need to have further mitigations applied or will need to be accepted by management. The State / LEO risk portfolio is one of the largest due to the budget constraints that reduce the number of highly trained technicians at these government levels to implement and maintain the strong security required. Also LEO locations are permanent and there are a limited number making them a more attractive target than the Citizen workstation.

Risk: 1
Type: B
Risk title: Unauthorized internal access leading to data modification (Physical)
Description: This risk specifically deals with a malfeasant physically acting within the LEO office.
Mitigations: LEO physical access controls
Notes: The local election office is staffed by paid professionals and unpaid staff. The paid staff are not trained to the levels of paranoia required to provide high levels of protection. It would be a reasonable task to infiltrate an office and gain access to SERVE related systems and information.

Risk: 10
Type: B
Risk title: Information accessed by individuals not authorized to access the data
Description: This could be physical, logical or any other means of access imaginable.
Mitigations: Leo physical access controls, Notebook hardening, Process
Notes: This risk is highly coupled with risk number 1.

Risk: 12
Type: B
Risk title: LEO being impersonated and accessing system
Description: This risk specifically addresses a Local Election Official being impersonated on the SERVE system.
Mitigations: Roaming certificates, Signing of data before transmission
Notes: Virtually any of the standard attacks against a user either technological or social would be effective against a LEO.

Risk: 13

Type: B
Risk title: Unspecified In House Software Bugs
Description: The software created by the SERVE project could experience a software fault.
Mitigations: Testing, Code review
Notes: Sufficient testing and code review can reduce this risk to an acceptable level

Risk: 21
Type: B
Risk title: Modification of data due to Virus' / Worms / Trojans
Description: Modification of data due to Virus' / Worms / Trojans
Mitigations: Antivirus software, Vote data stored on central server
Notes: Much of the data on the LEO machines is also stored on the Central server so it can be retrieved if failure is detected.

Risk: 16
Type: B
Risk title: Code used to encrypt or decrypt the vote is compromised on the client
Description: The encryption and decryption routines on the LEO machine could be broken by advances in technology or replaced with a rogue version.
Mitigations: None
Notes: A strong cipher is less susceptible to the issue of new technology. Also with an effective cipher the code could be modified in such a way to invalidate a few votes which might not be noticed or even the whole batch of votes requiring a new notebook be delivered to the LEO.

Risk: 25
Type: B
Risk title: Corrupted database
Description: Any of the Hart software could experience a corrupted database
Mitigations: Votes stored on central server
Notes: After the software is written to CD it will not matter what shape the database us in.

Risk: 33
Type: B
Risk title: Ballot data is modified on the LEO workstation
Description: The shape of this attack is dependent on timing. If it were done before the ballot data were uploaded then bad ballots might be delivered. If it were done after the ballots were delivered the Hart tabulation software might have difficulty reading the ballots.
Mitigations: LEO Procedures
Notes: If a malicious individual were to gain control over the LEO workstation they could modify the ballot data to either affect the ballots issued or the votes stored on the machine. This risk can be mitigated through both procedure and technology.

Risk: 34
Type: B
Risk title: Vote data is modified maliciously on the LEO workstation
Description: After the encrypted vote blob is downloaded it could be modified on the LEO notebook.
Mitigations: Votes stored on central server
Notes: Same as risk 33.

Risk: 37
Type: B

Risk title: Lack of change and version control process
Description: LEO notebooks will need to be updated during their lifetimes. These updates must be tested and rolled out in a controlled fashion. It is possible a well meaning notebook operator could update the machine prematurely causing unknown damage.
Mitigations: LEO Processes, Training
Notes: Process and training are the most effective prevention to this risk.

Risk: 39
Type: B
Risk title: Unrecorded changes to system/application software or data on the LEO notebook
Description: The LEO notebook system could be modified either by accident or malice in a way that could affect its operation.
Mitigations: None
Notes: Due to the attractive target that the LEO makes for a malfeasant the possibility of improper changes to the LEO system is great. This should be explored further to identify possible mitigations that can be applied to the LEO system.

Risk: 42
Type: B
Risk title: Personnel making changes who are not properly trained
Description: Personnel making changes who are not properly trained
Mitigations: Training, LEO processes
Notes: Due to the human element at the LEO location the human element risks were of great concern to the team. With proper LEO personnel training and process many of these risks can be reduced.

Risk: 56
Type: B
Risk title: Access to backups is not properly controlled
Description: The LEO will press to CD their vote information from the notebooks. This information will the need to be stored in a safe fashion.
Mitigations: LEO procedures
Notes: There is no way to determine if this process will work as each ELO office is operated in a different fashion.

Risk: 60
Type: B
Risk title: Authentication for access to sensitive information is inadequate
Description: Authentication for access to sensitive information is inadequate
Mitigations: Roaming certificates
Notes: The most current understanding of this process would make this risk a “C” if a new FRAP meeting were held.

Risk: 65
Type: B
Risk title: Sharing of user IDs on the system
Description: LEO personnel should not share user ID’s as they may have different roles in the system and this practice would reduce the accountability of their respective actions.
Mitigations: LEO procedures, Training
Notes: Due to the human element at the LEO location the human element risks were of great concern to the team. With proper LEO personnel training and procedures many of these risks can be reduced.

Risk: 66

Type: B
Risk title: Ability to assume another persons identity
Description: This risk addresses the possible confidentiality issues of identity assumption.
Mitigations: None
Notes: Both sociological and technology issues affect this risk. The attractive target potential of the LEO office makes this threat very concerning. With proper LEO personnel training and possibly some technological solutions this risks can be reduced.

Risk: 67
Type: B
Risk title: Shoulder surfing of data
Description: Shoulder surfing of data
Mitigations: Training, LEO procedures
Notes: Due to the human element at the LEO location the human element risks were of great concern to the team. With proper LEO personnel training many of these risks can be reduced.

Risk: 71
Type: B
Risk title: Ex staff still has access to secure data
Description: Staff in the LEO offices are not all paid employees making the likelihood of staff being removed from the active roles less than in the standard corporate setting.
Mitigations: Training, LEO procedures
Notes: Due to the human element at the LEO location the sociological risks were of great concern to the team. Through process and LEO personnel training many of these risks can be reduced.

Risk: 80
Type: B
Risk title: Release or exposure of voted ballot
Description: This is a confidentiality issue only in that it would provide bad press for the SERVE program as printed ballots have no way to be traced back to the voter..
Mitigations: Training, LEO procedures
Notes: This risk is one of perception. The perception that a ballot was exposed even it if provides no valid benefit to any party is sufficient to damage the public trust.

Risk: 86
Type: B
Risk title: LEO office key compromised
Description: If a LEO office key were compromised someone might have the ability to modify a ballot.
Mitigations: Training, LEO procedures, Ballots stored on central servers
Notes: The LEO office private key is expected to reside on a hardware token or smart card. This certificate is the key to all of the Citizen votes and must be protected from disclosure and loss at all costs.

Risk: 105
Type: B
Risk title: Virus' / Worms / Trojans
Description: General Malware threat
Mitigations: Antivirus software
Notes: N/A

Risk: 116
Type: B

Risk title: Technical resources lack proper training
Description: Technical resources lack proper training
Mitigations: Training, LEO procedures
Notes: Funding at the LEO level creates this risk and is one of the largest sources of unease for the team.

Risk: 126
Type: B
Risk title: Internet provider service outage blocks access to UVS facilities
Description: If the LOE Internet connectivity were shut down or blocked the LEO would have no ability to retrieve ballots.
Mitigations: Alternate Internet connectivity
Notes: Internet access is a best effort service and as such cannot be fully depended on. In locations that vote tabulation has time elements a second Internet access method should be employed (Dial up).

4.3.3 State / LEO Risk Elements

Priority	Risk #	Risk Title:	Mitigations	Risk Type	Risk Notes:
▦ B	1	Unauthorized internal access leading to data modification (Physical)	LEO physical access controls	Integrity	
▦ B	10	Information accessed by individuals not authorized to access the data	Leo physical access controls, Notebook hardening, Process	Integrity	
▦ B	12	LEO being impersonated and accessing system	Roaming certificates, Signing of data before transmission	Integrity	
▦ B	13	Unspecified In House Software Bugs	Testing, Code review	Integrity	
▦ B	21	Modification of data due to Virus' / Worms / Trojans	Antivirus software, Vote data stored on central server	Integrity	
▦ B	16	Code used to encrypt or decrypt the vote is compromised on the client	None	Integrity	
▦ B	25	Corrupted database	Votes stored on central server	Integrity	
▦ B	33	Ballot data is modified on the LEO workstation	LEO Procedures	Integrity	No control over notebook after delivered to LEO
▦ B	34	Vote data is modified maliciously on the LEO workstation	Votes stored on central server	Integrity	
▦ B	37	Lack of change and version control process	LEO Processes, Training	Integrity	

B	39	Unrecorded changes to system/application software or data	None	Integrity	
B	42	Personnel making changes who are not properly trained	Training, LEO processes	Integrity	
B	56	Access to backups is not properly controlled	LEO procedures	Confidentiality	
B	60	Authentication for access to sensitive information is inadequate	Roaming certificates	Confidentiality	This risk should be downgraded
B	65	sharing of user IDs on the system	LEO procedures, Training	Confidentiality	
B	66	Ability to assume another persons identity	None	Confidentiality	
B	67	Shoulder surfing of data	Training, LEO procedures	Confidentiality	
B	71	Ex staff still has access to secure data	Training, LEO procedures	Confidentiality	
B	80	Release or exposure of voted ballot	Training, LEO procedures	Confidentiality	
B	86	LEO office key compromised invalidating all current ballots	Training, LEO procedures, Ballots stored on central servers	Confidentiality	
B	105	Virus' / Worms / Trojans	Antivirus software	Availability	
B	116	Technical resources lack proper training	Training, LEO procedures	Availability	
B	126	Internet provider service outage blocks access to SERVE facilities	Alternate Internet connectivity	Availability	
C	5	Unauthorized internal access leading to data modification (Logical)	LEO procedures	Integrity	
C	7	User denied access to information/services they are authorized to access	ITA testing, Internal SERVE testing	Integrity	
C	32	Authentication data is modified on the LEO workstation	Hardening procedures, LEO procedures	Integrity	
C	45	Operations processes so complicated they are ignored	LEO procedures	Integrity	
C	46	DNS poisoning with site redirection	Ability to use alternate ISP	Integrity	
C	47	Route poisoning with site redirection	Ability to use alternate ISP	Integrity	
C	53	Unattended workstation	LEO procedures, Time based dead man lock	Confidentiality	Per activity lock in sec req

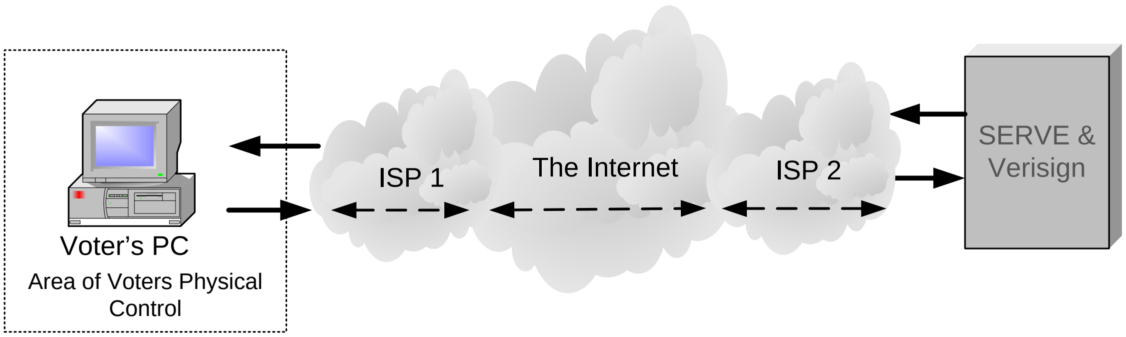
C	95	Disgruntled admin staff with high security privileges	None	Confidentiality	
C	121	Incorrectly made hardware or software changes	None	Availability	
C	129	DNS poisoning	Ability to use alternate ISP	Availability	
C	130	Route poisoning	Ability to use alternate ISP	Availability	
C	137	Disgruntled admin staff with high security privileges	None	Availability	
C	142	Lack of qualified LEO's to do tabulation ((due to attrition) do not have required 2 to access office certificate)	LEO procedures	Availability	
C	48	Ability to change data in transit	Encryption, LEO procedures	Integrity	
C	84	Keyboard logging Trojan	Antivirus software	Confidentiality	
C	91	SERVE Site spoofed and then info retransmitted to gain information about Citizen and vote	Random signing of data sent to SERVE during LEO procedures	Confidentiality	
C	108	Program bugs (COTS)	ITA testing, SERVE testing, Code review	Availability	
C	123	Router or firewall failure or misconfiguration may cause inaccessibility to services	None	Availability	
D	63	Inability of entities to access confidential data at a later date due to certificate revocation	N/A	Confidentiality	N/A as data is stored on LEO notebook/ workstation
D	78	Release or exposure of Citizen personal data	None	Confidentiality	In many jurisdictions this is done as a matter of policy so this risk may not apply
D	81	Release or exposure of unvoted ballot	N/A	Confidentiality	In most jurisdictions this is dome as a matter of policy
D	82	New technologies leading to breaches of confidentiality	None	Confidentiality	
D	101	Unauthorized internal access causing site outage	None	Availability	
D	102	Unauthorized external access (logical) causing site outage	LEO procedures, OS hardening	Availability	

▦ D	131	Internet DOS attacks against users	None	Availability	
▦ D	136	Industrial action or strike at service provider	Ability to use any ISP	Availability	
N/A	15	Code used to create or process the signature is compromised on the client	N/A	Integrity	Changes to system have removed
N/A	35	Registration data is modified maliciously on the LEO workstation	N/A	Integrity	Registration data is not stored on SERVER provided LEO workstation
N/A	92	Encrypted copy of vote stored for retention period decrypted using new technology	N/A	Confidentiality	Votes stored in unencrypted form at LEO
N/A	93	Process used to separate vote from person at LEO does not lead to vote confidentiality	N/A	Confidentiality	Vote striped at server from identity

4.4 *Citizen Risks*

The Citizen area has been argued to be the most vulnerable of any of the areas. It is probable from a theoretical viewpoint that this is true. But from a practical standpoint the effort required to locate and successfully compromise enough Citizen workstations to make a noticeable effect on the voting process would be considerably more expensive and time consuming than using non technical means to affect an election outcome. Shown below is a simplified view of a Citizen infrastructure.

4.4.1 Citizen diagram



4.4.2 Citizen Priority Risk Discussion

The following risks received either a rating of **A** (Corrective action must be initiated) or a Rating of **B** (Corrective action should be initiated). The Citizen risk portfolio is the second largest due to the known lack of security on most client machines. But the number of SERVE participants versus the total number of Internet users makes the SERVE user base a difficult target. In many cases it would be easier to physically identify and affect a Citizen than it would be to electronically identify the Citizen and affect their voting process.

Risk: 11
Type: B
Risk title: Information accessed by individuals not authorized to access the data
Description: This risk is specific to data leakage in a close knit computing environment.
Mitigations: User training, Enrollment process
Notes: Due to the close nature of many computer users with their cohabitants and the predictability of many people it is possible for a person to identify sufficient information about a Citizen to be able to access their SERVE related data.

Risk: 29
Type: B
Risk title: Ballot data is maliciously modified on the client
Description: This could be done by the Citizen workstation user themselves in an attempt to discredit SERVE or an external entity who has installed software designed to perform this task.
Mitigations: User training, Voted ballot approval process
Notes: There is very little possibility of stopping a malicious individual from modifying ballot data on an unprotected client. But the design of the system allows a Citizen to detect this modification and in the worst case call the help desk and in the best case just log on at a later time and receive an unmodified ballot.

Risk: 30
Type: B
Risk title: Vote data is modified maliciously on the client
Description: This could be done by the Citizen workstation user themselves in an attempt to discredit SERVE or an external entity who has installed software designed to perform this task.
Mitigations: User training, Voted ballot approval process
Notes: There is very little possibility of stopping a malicious individual from modifying vote data on an unprotected client. But the design of the system allows a Citizen to detect this modification and in the worst case call the help desk and in the best case recast their vote.

Risk: 52
Type: B
Risk title: Unattended workstation
Description: Unattended workstation
Mitigations: User training
Notes: With the number of Citizens that SERVE is trying to attract it is highly likely that a Citizen will abandon their workstation during the voting process for the small amount of time it will take for a local individual to disrupt their current process. Though unfortunate this person will need to either repeat their interrupted process or call the helpdesk for assistance.

Risk: 65
Type: B
Risk title: Sharing of user IDs on the system
Description: Sharing of user IDs on the system
Mitigations: User training

Notes: The sociologic elements of the voting process demand that certain individuals will misconstrue the process or attempt to thwart it. These people will hopefully realize their mistake and get their own separate user accounts to allow them to vote.

Risk: 66
Type: B
Risk title: Ability to assume another persons identity
Description: Various means could be employed to assume another persons identity on the system
Mitigations: User training, Enrollment process, VeriSign roaming certificates
Notes: This is a very broad risk assumed by any multi-user system.

Risk: 67
Type: B
Risk title: Shoulder surfing of data
Description: Citizens who do not take precautions to protect their privacy during the voting process could be overseen either physically or electronically.
Mitigations: User training
Notes: The distributed nature of Internet voting does not allow the voting process to be monitored and places the requirement of a private voting location on the shoulders of the Citizen.

Risk: 82
Type: B
Risk title: New technologies leading to breaches of confidentiality
Description: The advancement of computer science inevitably leads to older technology becoming obsolete.
Mitigations: None
Notes: This risk is not specific to SERVE but is a problem all systems are affected by equally.

Risk: 83
Type: B
Risk title: Keyboard logging Trojan
Description: Keyboard loggers can come in many forms and essentially capture the keystrokes typed by a user.
Mitigations: User training, Antivirus software, Ballot design
Notes: Through educating the Citizen it is possible to reduce the likelihood of this threat. Also the design of the ballot (clicking on choices not typing them) makes the keyboard logger less effective of a tool that it could be.

Risk: 90
Type: B
Risk title: Remote management software loaded on client machine by controlling entity
Description: In corporate environments it is very common to have remote management softwar loaded on all corporate assets. Though this provides an efficient way to remotely assist users it could be used to view how a voter was voting or even vote for them.
Mitigations: User training
Notes: Through malice or purpose there is a high level of likelihood that at least one Citizen will have remote management software loaded on their PC. This risk is made more real through the fact that most major manufacturers enable remote management software on the PC's they ship to ease support burdens. Also many companies load remote management software on PCs they provide to their employees for support purposes. This risk can only be reduced through educating the Citizen in sound security principles.

Risk: 108
Type: B
Risk title: Program bugs
Description: Any software no matter how carefully it was written can have errors.
Mitigations: Software testing, Code review
Notes: N/A

Risk: 124
Type: B
Risk title: Congestion on the Internet causes user dissatisfaction
Description: This risk deals with a perception that the SERVE system is malfunctioning or down
Mitigations: None
Notes: The perception that SERVE is slow through no fault of the UVS system must be combated through the judicious use of the help desk and keeping the footprint of the serve client software small. The perception of the system by the user is in many cases more important than the reality and perception issues should be reviewed and tested throughout the system lifecycle.

4.4.3 Citizen Risk Elements

Priority	Risk #	Risk Title:	Mitigations	Risk Type	Risk Notes:
▦ B	11	Information accessed by individuals not authorized to access the data	User training, Enrollment process	Integrity	
▦ B	29	Ballot data is maliciously modified on the client	User training, Voted ballot approval process	Integrity	
▦ B	30	Vote data is modified maliciously on the client	User training, Voted ballot approval process	Integrity	
▦ B	52	Unattended workstation	User training	Confidentiality	
▦ B	65	sharing of user IDs on the system	User training	Confidentiality	
▦ B	66	Ability to assume another persons identity	User training, Enrollment process, VeriSign roaming certificates	Confidentiality	
▦ B	67	Shoulder surfing of data	User training	Confidentiality	
▦ B	82	New technologies leading to breaches of confidentiality	None	Confidentiality	
▦ B	83	Keyboard logging Trojan	User training, Antivirus software, Ballot design	Confidentiality	

B	90	Remote management software loaded on client machine by controlling entity	User training	Confidentiality	
B	108	Program bugs	Software testing, Code review	Availability	
B	124	Congestion on the Internet causes user dissatisfaction	None	Availability	
C	1	Unauthorized internal access leading to data modification (Physical)	None	Integrity	
C	7	User denied access to information/services they are authorized to access	ITA testing, SERVE testing	Integrity	
C	15	Code used to create or process the signature is compromised on the client	User education	Integrity	
C	22	Modification of data due to Virus' / Worms / Trojans	User education	Integrity	
C	28	Authentication data is modified on the client	None	Integrity	
C	46	DNS poisoning with site redirection	User education, Ability to use any Internet connection	Integrity	
C	47	Route poisoning with site redirection	User education, Ability to use any Internet connection	Integrity	
C	61	Authentication for access to sensitive information is inadequate	ITA testing, SERVE testing	Confidentiality	
C	87	Information on clients is unprotected	None	Confidentiality	
C	88	Information on client remains after voting process has ended on client	None	Confidentiality	XML data may be problematic to flush
C	98	Vote selling	User education	Confidentiality	
C	106	Keyboard logging Trojan	None	Availability	
C	127	Internet provider service outage blocks access to SERVE facilities	Ability to use any Internet connection	Availability	
C	129	DNS poisoning	Ability to use any Internet connection	Availability	
C	130	Route poisoning	Ability to use any Internet connection	Availability	
C	131	Internet DOS attacks against users	Ability to use any Internet connection	Availability	
C	136	Industrial action or strike at service provider	Ability to use any Internet connection	Availability	

▦ C	139	International ISP blocks access to SERVE voting site	Ability to use any Internet connection, User education	Availability	
▦ C	146	Web voting application designed to work with a limited set of clients	None	Availability	That is by designed
▦ C	150	Failure of client machine	Ability to use any Internet connection	Availability	
▦ C	48	Ability to change data in transit	Encryption, User education	Integrity	
▦ C	91	Site spoofed and then info retransmitted to gain information about Citizen and vote	User education	Confidentiality	
▦ D	63	Inability of entities to access confidential data at a later date due to certificate revocation	N/A	Confidentiality	Not applicable to user
▦ D	123	Router or firewall failure or misconfiguration may cause inaccessibility to services	Ability to use any Internet connection	Availability	Home rtr (dsl)
N/A	16	Code used to encrypt or decrypt the vote is compromised on the client	N/A	Integrity	
N/A	121	Incorrectly made hardware or software changes	N/A	Availability	No software or hardware rolled out to client

5 SERVE Risk Mitigation

Controls are the active processes, procedures, and system features that serve to detect and / or reduce the probability of a threat, or the impact of a vulnerability, causing a reduction of the system or processes total risk. There can be a very large number of specific controls or in some cases none contributing to the mitigation or acceptance of threats and vulnerabilities. The controls are used to implement security features in the UVS system and its related components.

During phase 1 of the assessment only the project security requirements were considered as possible controls. During phase 2 and 3 a number of controls were identified from the completed design and possibly created during phase 2 to fulfill any needs where applicable. It is possible that some identified risk elements cannot be mitigated using current technology.

5.1 Accepted Risks

Due to early project termination no risks have or will be marked as accepted.

5.2 Controls

Due to early project termination the controls section has been removed and combined with the risks section so as to provide a simpler format for a wider reading audience.

6 References

References
“A Report on the Feasibility of Internet Voting” by The California Internet Voting Task Force - California Secretary of State Bill Jones
“Internet Voting” by David Jefferson - Compaq Systems Research Center
"Security Criteria for Electronic Voting" by Peter G. Neumann - Computer Science Laboratory SRI International
“Electronic Voting - Evaluating the Threat” by Michael Ian Shamos
“BGPv4 Security Risk Assessment” by Barry Raveendran Greene, and Philip Smith - The ISP Essentials
“Security Considerations for Remote Electronic Voting over the Internet” by Avi Rubin AT&T Labs - Research Florham Park, NJ
“Client encryption pros and cons.doc” by Chris Dahl of Election.com – SERVE project internal
“Client vs Server risk comparison” by Carl Almond – SERVE project internal
“Will High-Tech save or sink future elections” – MSNBS News
“A Better Ballot Box? New electronic voting solutions pose risk as well as solutions” – IEEE Spectrum Online
“Information Security Risk Analysis” by Thomas R. Peltier – Auerbach Publications

7 Glossary of Terms and Acronyms

Term	Definition
DOD	United States Department of Defense
DOS	Denial of Service
FRAP	Facilitated Risk Analysis Process
Impact	The effect of one thing on another.
LEO	Local Election Official
Malware	Software that is Viral or Trojan in nature. Malicious software designed with ill intent.
Risk	A factor, thing, element or course involving uncertainty. The danger or probability of loss.
SERVE	Secure Electronic Registration and Voting Experiment.
Threat	An indication of impending danger or harm.
Vulnerability	Open or susceptible to attack.

8 Appendix A – FRAP Description

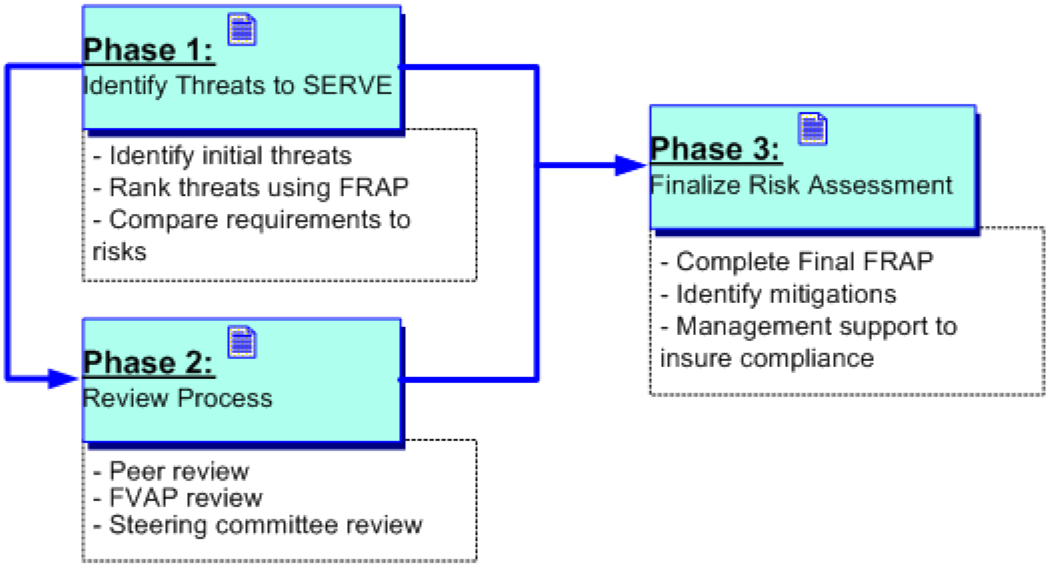
8.1 Risk Assessment Process

The Facilitated Risk Analysis Process was developed as an efficient and disciplined process for insuring that information security related risks to a system or process are considered and documented. The standard process consists of analyzing one system or process at a time and convening a team of subject matter experts who have a detailed understanding of potential vulnerabilities and related controls. The sessions are lead by a participating team member from a project management or security discipline.

During the session the team of experts starts with an initial list of risks and expands the list further to identify any potential threats, vulnerabilities and their resultant impacts on Confidentially, Integrity and Availability. The team then analyzes the effects of such impacts on systems or processes and categorizes the risks according to their priority level. The team does not have, as one of its goals, to develop specific estimates for the threat likelihood or an annualized loss estimate as are created in other risk assessment methodologies. Instead the team draws from its knowledge of threats and vulnerabilities obtained from external sources and personal experience to provide meaningful risk analysis.

After identifying and qualifying the risks, the team specifies controls that could be implemented to reduce the risk. The team's conclusions as to what risks exist; the priority of the risk and what controls need to be applied are documented and passed to the projects management. Management then identifies the risks they wish to accept and the risks that will be mitigated with the specific mitigations used. All of this is then documented and the system or project owners sign off on their sections.

The modified Facilitated Risk Analysis Process that is being used for SERVE is split into three phases to fit the size and complexity of the project. The three phases are outlined below.


Phase 1:
Identify Threats to SERVE
- Identify initial threats
- Rank threats using FRAP
- Compare requirements to risks
Phase 2:
Review Process
- Peer review
- FVAP review
- Steering committee review
Phase 3:
Finalize Risk Assessment
- Complete Final FRAP
- Identify mitigations
- Management support to insure compliance

8.1.1 FRAP Phase 1

In this phase the project security architect determines a base set of security risks after reviewing all project documentation and any external sources on Internet voting risk. The base security risks are developed into a set of FRAP forms that can be used by the team of experts as the basis of their meeting. The SERVE project security requirements are also reviewed for use as possible mitigations against the identified risks. After the FRAP risk forms and the current security requirements are ready the team is convened to perform the initial assessment.

During the initial assessment the team of experts works to identify potential threats, vulnerabilities and their resultant impacts on Confidentially, Integrity and Availability. The team adds any new threats to the FRAP forms and begins analyzing the effects of such impacts on the planned SERVE systems and categorize the risks according to their priority level. The team does not develop specific estimates for the threat likelihood or an annualized loss estimate. Instead the team draws from its combined knowledge of threats and vulnerabilities obtained from external sources and personal experience to provide meaningful risk analysis.

After identifying and quantifying the risks the project security architect reviews the security requirements that will be implemented to reduce the risk. The research, risks and requirements are then combined into a document to form the “Initial Threat Risk Assessment – Phase 1”. It should be noted that this phase of the document is being produced during the early design phase of the SERVE project and as such is very preliminary in nature and only the security threats can currently be identified.

8.1.2 Phase 2

The second phase provides time for the review committee, Federal Voting Assistance Program (FVAP) and the SERVE team to review the security assessment and make comments. This phase will run concurrently with the SERVE projects design phase and includes these steps:

a. Peer review
b. FVAP review
c. Steering committee review

After all of the listed reviews have been completed the recommendations, risk modifications, new risks and controls are added to the “Threat Risk Assessment – Phase 2” document. Phase 2 also gives the project architects the ability to view their systems’ threats and modify the design of those systems to reduce the project’s overall security risk.

8.1.3 Phase 3

Phase 3 creates the final security risk assessment and can begin after the SERVE project design phase and the two initial risk assessment phases have been completed. During this phase the FRAP forms are completed with the new risk and control information and an enhanced subject mater expert team is reconvened to reassess all of the project security threats. Unlike in phase 1 the team might also identify controls or mitigations to the systems threats.

The teams conclusions as to the total risk portfolio, the priority of each threat, and what controls are needed to mitigate the threats are documented in the “Final Threat Risk Assessment – Phase 3” document which includes the risk mitigations.