Voting Over the DISN-CAC Analysis Feasibility Evaluation

Submitted To:

October 5, 2012

Prepared by:

Dreifus Associates Ltd, Inc.

[redacted]

Table of Contents

Tables

Figures

Executive Summary

This report documents a review and evaluation of the feasibility of applying the Defense Information System Networks (DISN), specifically the Non-Classified Internet Protocol Router Network (NIPRNet), as a conduit to support Uniformed and Overseas Citizens Absentee Voting (UOCAVA) voters in the voting process, coupled with the Defense Department's primary form of identification, the Common Access Card (CAC), as an available, standardized means of asserting reliable identification of potential voters. In addition, an understanding is developed of considerations for protecting the privacy of personal identifiable information, and providing accountability, reliability and transparency.

The initial sections of the report detail the research and analysis performed on each of the key components; the NIPRNet, the CAC, Electronic Voting Systems and the remote voting client. The data elements and internal data structures of the CAC, including the underlying authoritative identity framework (that includes the vetting of CAC recipients), are evaluated for suitability and fit in asserting identity authentication for the purposes of enabling Local Election Officials (LEOs) to perform vetting and adjudication decisions regarding an individual's eligibility to vote. Comparability to analogous applications that apply the CAC and other digital electronic-based security architectures for the delivery of high-reliability services was also evaluated.

Based upon a review of each contributing component, current practices, policies, procedures, applicable standards, certifications, accreditations and security considerations, this report provides an assessment of the feasibility of applying the combination of the NIPRNet and CAC to facilitate a robust conduit to enable the prospect of future electronic voting. The evaluation takes into consideration the operating landscape within the DoD environment and constraints that the voting framework must be able to reliably support in order to reach the population of active duty UOCAVA voters.

A baseline conceptual framework is illustrated for the purpose of evaluating configurations and to enable the review of feasibility. It is not a representative design; it is solely used to facilitate the examination of options/considerations for the key components, both individually and collectively, that are required to support the voting process. A primary cornerstone assumption is that the Department of Defense will only be providing a positive assertion of identity and a known and characterized communications channel to the appropriate participating Local Election authorities within a network environment. The Local Election authorities have the sole responsibility for determining and adjudicating an applicant's right to vote and for any ensuing vote they may proffer.

The review was conducted using a methodical approach to individually evaluate each contributing component in the process and collectively as a whole. Key elements of the evaluation include:

- Information Assurance (IA) statutes, policies, instructions, practices and other data and security standards
- Advantages/disadvantages of the alternatives for each component
- Confidentiality, Privacy, Integrity and Availability of components and their integration
- Risks and Mitigations

The NIPRNet and CAC were also assessed against alternative approaches. This includes other PKI (and non-PKI) secured environments.

Crucial to the evaluation and assessment of an overall solution is the assessment and mitigation of risks associated with each of the components. A chain is only as strong as its weakest link and particular consideration is given to potential single points of failure with regard to security and integrity. The evaluation identifies the strengths and weaknesses surrounding each of the elements that comprise an overall solution. Potential mitigations are presented for discussion/further assessment.

The primary conclusion reached is that it is possible to provision a conduit for electronic voting using the DISN, more specifically the NIPRNet, and to use the CAC as the identity authentication mechanism of the voter. Key findings include:

1. DoD can support an electronic voting process for UOCAVA voters through the provision of positive identification of the voter to Local Election Officials and a secure communication channel through the use of the CAC.
2. The NIPRNet provides a managed, controlled and monitored network environment that can reduce exposure to exploits such as hacking, spoofing, and other forms of malicious activity. Other networks can also provide this environment but the NIPRNet is already established, supported and trusted within DoD.
3. The CAC is an existing, trusted identity credential used within an established, mature PKI framework in the DoD and it supports multi-factor authentication. Consideration needs to be given to the management of digital certificates within the voting framework to allow for turnover that can occur during the voting process due to standard CAC replacement cycles or lost/stolen cards.
4. A “clean boot” capability at the client site, such as provided by the Lightweight Portable Security (LPS) system, could help minimize the opportunity for malware and other exploits to corrupt the electronic voting process.

It is noted that the certification/approval processes regarding applications and connectivity to the NIPRNet can be lengthy – anecdotal accounts estimate a range from 6 months to over a year for certification. This should be taken into account in any forward planning.

A further consideration for forward planning is ensuring acceptance from each State of the framework, including the authentication methodology (such as CAC), as a trusted and accepted means of identification for voting.

Finally, it is noted that establishing an electronic voting framework around the NIPRNet and the CAC will restrict access/use to only those users who hold CAC’s with authorization for the NIPRNet. This framework would not be readily extensible to a

larger overseas voting population either not eligible for CAC's or not eligible for NIPRNet access. Wider issuance of CAC's is currently being considered, such as to family members and dependents, but this does not include access to the NIPRNet.

1. Objectives

The objective of this activity is to assess and document the feasibility of incorporating information age tools and capabilities in support of a potential remote electronic voting demonstration project for active duty personnel, pursuant to the National Defense Authorization Act of 2002 and as amended in 2005. Specifically, the Federal Voting Assistance Program (FVAP) wishes to evaluate the possibility of using the NIPRNet within the DISN in conjunction with a strong means of asserting online identification/authentication, such as provided by the CAC, to support UOCAVA voters in the voting process.

This feasibility assessment requires building an understanding of a number of elements and considerations, including security, privacy, accountability, reliability and transparency, and the associated risks, with respect to the key components: the Network, Authentication method, Electronic Voting Systems and client computer environment.

2. Defense Networks Background

The Defense Information Systems Agency[1] (DISA) provides, operates and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.

One of DISA's responsibilities is developing and operating the Global Information Grid[2] (GIG) networks and services utilized by the DoD.

Table 1 summarizes some of the GIG networks and services under DISA's management.

DISN Network/Service	Classification Supported
Cross Domain Solutions (CDS)	SECRET/Unclassified
Defense Red Switched Network (DRSN)	SECRET
Defense Switched Network (DSN)	Unclassified
DISN Leading Edge Services (DISN-LES)	SECRET
DISN Video Services (DVS)	SECRET/Unclassified
Non-Classified Internet Protocol Router Network (NIPRNet)	Unclassified
Office of the Secretary of Defense (OSD) Global Information Grid (GIG) Waiver Process	Unclassified
Real Time Services (RTS)	SECRET/Unclassified
Secret Internet Protocol Router Network (SIPRNet)	SECRET
Secure Mobile Environment-Portable Electronic Device (SME-PED) Provides wireless NIPRNet and SIPRNet access, includes email and web browsing in one device.	SECRET/Unclassified

Table 1: DISA Networks

DISA provides, and is responsible for, a variety of functions regarding these networks including, but not limited to, the following:

[1] See DISA *Our Mission*, Retrieved from website: http://www.disa.mil/
[2] Grimes, J. U.S. Department of Defense, Chief Information Office. (2007). *Department of defense global information grid architectural vision - vision for a net-centric, service oriented DoD enterprise.* Retrieved from website: http://www.msco.mil/documents/_7_GIG Architectural Vision - 200706 v1.0.pdf

- Analysis and laboratory evaluation of advanced technologies to support insertion into the DISN.
- Network management and systems engineering, implementation and consolidation required by DISN DoD worldwide strategic and special purpose circuit switched networks.
- Management and technical assistance to DISN special projects and programs which include: DoD support to the direct communications links; deployment license sharing among federal, state, local, and foreign mission partners; DISN transition to the DISN Core; DISN provisioning policies and process.

In this research report the focus is on the Unclassified, but Sensitive Internet Protocol Router Network, also known as the Non-Classified Internet Protocol Router Network (NIPRNet), and its feasibility to be utilized in the voting process in support of UOCAVA voters.

Information Assurance (IA)

The NIPRNet, as well as all DoD networks, follow Information Assurance (IA) practices (i.e., 8500 Series DoD Information Assurance and IA Implementation) as part of its information systems management strategies. The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the DoD process to ensure that risk management is applied to information systems (IS). The details of the strategies are continually updated to support the confidentially, integrity and availability of these information systems. The strategies focus on multi-layer security approaches to reduce the risk of an intruder exploiting any one weakness to gain access to information. Security is never done; it is constantly monitored, updated, added to and improved. The DoD has to balance the importance of access to the information and the support of the mission against threats, vulnerabilities and the effectiveness of IA solutions.

The Security Technical Implementation Guides (STIG)[3] and the NSA Security Configuration Guides[4] are the configuration standards for DoD IA and IA-enabled devices and systems. The STIG's contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to malicious attacks. DISA is presently in the process of moving the STIG's toward the use of the NIST Security Content Automation Protocol (SCAP) in order to be able to "automate" compliance reporting of the STIG's. The network personnel who manage the individual networks, which combine to form the NIPRNet, are responsible for ensuring that all configurations and guidelines are adhered to and properly reported.

Table 2 provides a sample of DoD Instructions (DoDI) along with DISA and NIST guidelines used by NIPRNet personnel for building and maintain these network systems.

Specifications / Standards	Description
DISA	Connection Process Guide
DoDI 8500.1	"all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines"
DoDI 8520.02	Public Key Infrastructure (PKI) and Public Key (PK) Enabling (May 24, 2011)
DoDI 8520.03	Identity Authentication for Information Systems (May 13, 2011)
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
NIST SP 800-119	Guidelines for the Secure Deployment of IPv6
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST SP 800-125	Guide to Security for Full Virtualization Technologies
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems
NIST SP 800-53	DRAFT Security and Privacy Controls for Federal

[3] See "Security Technical Implementation Guides (STIG), configuration standards for DoD IA", Retrieved from website: http://iase.disa.mil/stigs/
[4] See *National Security Agency "Security Configuration Guides",* Retrieved from website: http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml

	Information Systems and Organizations
NIST SP 800-63	Electronic Authentication Guideline
NIST SP 800-77	Guide to IPsec VPNs
NIST SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines
NIST SP 800-96	PIV Card to Reader Interoperability Guidelines
NIST SP 800-126	The Technical Specification for the Security Content Automation Protocol (SCAP)

Table 2: Sample of DoDI, DISA and NIST Guidelines for NIPRNet

NIPRNet

The Internet is currently governed under a "multi-stakeholder" approach that gives power to a host of nonprofits, rather than governments. It is a globally interconnected set of computers and networks with no single controlling body that is referred to as an untrusted network or public network. The present governing stakeholders consist of the Internet Corporation for Assigned Names and Numbers[5] (ICANN) and the World Wide Web Consortium[6] (W3C). The NIPRNet is also an interconnected set of computers and networks, but unlike the Internet, the NIPRNet is a controlled environment and considered a trusted network[7] or private network with a set of policies, procedures and controls that dictate its use, system configurations and security.

The individual networks within the NIPRNet are sometimes referred to as "Enclaves[8]" which in essence is any secured, self-contained computational system within a system of local area networks. This provides a level of security through the segregation or separation of network assets and or network users and is usually implemented through the use of technology (i.e. routers[9]).

The NIPRNet is utilized by the DoD to exchange sensitive but unclassified information between internal users as well as providing access to the Internet; it is the largest

[5] See Internet Corporation for Assigned Names and Numbers. (2012) *Retrieved from Website: http://www.icann.org/*
[6] See The World Wide Web Consortium. (2012) Retrieved from website*:* http://www.w3.org/
[7] See Duke University, Department of Computer Science. (2012).*CSI: Trusted and untrusted networks*. Retrieved from website: http://www.cs.duke.edu/csl/faqs/trust
[8] See Hyper Learning Technologies, (2012). *Dod instruction 8570*. Retrieved from website: http://www.hyperlearn.com/dod-military/dod-instruction-8570
[9] See Pacific Start Communication, *PacStar 4500 Commander Kit*, Retrieved from website: http://pacstar.com/pgs/products/deployable-communications/pacstar-4000-series

private network in the world[10]. Private networks are commonly referred to as Intranets[11] and function in a similar manner as the Internet but are private in nature and have a smaller address range.

Today there are two protocols utilized by both public and private networks; they are the Internet Protocol IPv4[12] and IPv6[13]. Each of the protocols can have different requirements when using encryption methods over a network, such as when utilizing IPsec[14] and Network Address Translation (NAT). Table 3 is the industry accepted Internet Protocol address ranges of IPv4 for private networks; the ranges are dictated by the network class or size of the network. The latest Internet Protocol (IPv6) was standardized to extend the address ranges available to the Internet. Neither IPv4 nor IPv6 private addresses may be routed on the public Internet. The IPv6 protocol is still in its infancy and not all DoD systems, including the NIPRNet, have been switched over to this protocol.

IPv4 Private IP Ranges
10.0.0.0 through 10.255.255.255
172.16.0.0 through 172.31.255.255
192.168.0.0 through 192.168.255.255

Table 3: IPv4 Private IP Ranges

NIPRNet Environment

A simplified example of the NIPRNet architecture consists primarily of tier one and tier two routers, separated by a firewall, with an Intrusion Detection System in its simplest form.

When compared to the Internet the NIPRNet maintains a higher level of control over its systems and users. This is achieved through the utilization of multiple managed networks following IA best practices, policy and STIG's but the NIPRNet remains only

[10] NIPRNet *Retrieved from Website:* http://www.websters-online-dictionary.org/definition/NIPRNET
[11] Intranet, (n.d.), Retrieved from website: http://compnetworking.about.com/cs/intranets/g/bldef_intranet.htm
[12] Ben Parr, See IPv4, (2011), Retrieved from website: http://mashable.com/2011/02/03/ipv4-ipv6-guide/
[13] Ben Parr, See IPv6, (2011), Retrieved from website: http://mashable.com/2011/02/03/ipv4-ipv6-guide/
[14] Steve Friedl, See IPSec, (n. d.), Retrieved from website: http://www.unixwiz.net/techtips/iguide-ipsec.html

as secure as its weakest link. A poorly managed network or application on the NIPRNet could expose a vulnerability to the entire system. As we have mentioned, security is never done and managers of the individual networks must continue to be diligent in securing their systems and who has access to them. The DoD is keenly aware of this and has over time surveyed the NIPRNet to create a roadmap to determine its size and find out what exists on the network. This mapping is also being used to update weak areas of network security and determine unauthorized users that may have gained access to the network.

Usage

The NIPRNet has specific guidelines for all users and groups that connect or use the network. At present, most users go through a National Agency Check with Local Agency Check and Credit Check[15] (NACLC) as part of the process. The Connection Approval Office[16] (CAO) is responsible for this access and the use of the networks. The Enterprise Connection Division's Information Assurance (IA) Branch has two distinctly different functions/teams; the Connection Approval and Cross Domain Solutions (CDS). The CAO is responsible for processing GIG waivers, reviewing and approving all routine DISN connection requests, which are primarily addressed in the Connection Process Guide[17] (CPG). The CAO also receives some other types of connection requests that are not routine, in the sense that they involve a higher level of risk to the DISN than the CAO is authorized to accept. Those requests (e.g., CDS) are reviewed and approved by the Defense IA/Security Accreditation Working Group[18] (DSAWG), and in cases of even higher risk, by the DISN/GIG Flag Panel. It is also important to point out that NIPRNet connections normally have expiration dates associated with their use; this could lead to a continual cycle of connection request during periods of voting.

[15] Defense Human Resource Activity, (n.d.). *Investigative standards for background investigations for access to classified information*. Retrieved from website: http://www.dhra.mil/perserec/adr/invstandards/invstandtext.htm
[16] See Defense Information System Agency. Enterprise Connection Division (n.d.), *Connection approval*. Retrieved from website: http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/Connection-Approval
[17] Defense Information Service Agency, Enterprise Connection Division. (2011). *Connection Process Guide*(v3.2). Retrieved from website: http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf
[18] See Defense Information System Agency. Enterprise Connection Division (n.d), *DSAWG*. Retrieved from website:, http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/DSAWG

Security

The NIPRNet by its design requirements is hardened to external attacks; this is partially achieved through using IA best practices, private IP addresses and the configurations along with the policies that the systems must abide by. Internet routers include rules to drop any traffic that is coming from or going to a private IP address, thus helping to provide a level of security. Configurations and reporting (STIG's) help in providing baselines for systems that will connect or be part of the NIPRNet. Polices can cover such items as:

- Protecting passwords
- Removing unnecessary accounts
- Disabling unneeded services
- Disabling unneeded applications
- Protecting management interfaces and applications
- OS configurations
- Network configurations
- Encryption

This is all part of the overall strategy in securing the NIPRNet and its systems. Security is a continual process that strives to mitigate risks by reducing the likelihood of a threat exploiting any vulnerability.

Client computers on the NIPRNet can pose a weak point in the networks as they are exposed to users who can either inadvertently or purposely expose the computer to virus and malware through downloading or installing unauthorized software. Both controls and authorization roles are used to help mitigate these potential issues. The control types and methods used follow three primary functions are preventative, detective, and corrective. Below are some examples of the control types employed.

- **Technical Controls** Uses technology to reduce vulnerabilities. (Antivirus, IDS's and firewalls)
- **Management Controls** Risk and Vulnerabilities assessments.
- **Operational Controls** Awareness and training, Configuration management, Contingency planning, Media protection, Physical environment protection.
- **Preventative Controls** security guards, change management, account disablement, system hardening.
- **Detective Controls** security audit, video surveillance.
- **Corrective Controls** Active IDS, backups, system recovery.

Access control models are also utilized to handle the user's access or authorization to specific information available on the network. The three most common models used are the following:

- Role-/Rule-based access control (RBAC)
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Security is critical to keeping the NIPRNet safe from both outside and inside threats and is a never ending process, items discussed above only cover a small portion of the security methods used to keep the network safe. With new protection methods emerging the NIPRNet will continue to be updated.

Public Key Infrastructure (PKI)

The DoD PKI[19] provides the data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature[20] services for programs and application, which use the DoD networks. The DoD Digital Certificate Policy[21] (i.e. X.509v3) provides the policy for binding the keys to individuals and

[19] Defense Information Service Agency. (n, d) *Public Key Infrastructure* Retrieved from website: http://iase.disa.mil/pki-pke/
[20] Digital Signature, See US ESign Act of 2000, (2000), Retrieved from website: http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
[21] Department of Defense, DoD Public Key Infrastructure Program Management Office (2005). *X.509 certificate policy for the united states department of defense* (v9). Retrieved from website: http://jitc.fhu.disa.mil/pki/documents/dod_x509_certificate_policy_v9_0_9_february_2005.pdf

hardware for identification purposes and the CAC provides the primary method for utilized the digital certificates.

The PKI technologies utilized on the NIPRNet are the same commonly used industry technologies used on the Internet. These include the use of industry standard asymmetrical and symmetrical encryption methods (i.e. “RSA, ECC, and AES”) and digital signatures that utilize common hashing methods (i.e. “MD5, SHA1, 2 and MAC”).

External PKIs that interact with the NIPRNet are approved for use by the ASD (NII)/DoD CIO. DoD partners use certificates issued by the DoD External Certification Authority (ECA) program or a DoD-approved PKI, when interacting with the DoD in unclassified domains. The DoD also maintains a cross certification with the Federal PKI to comply with Federal Information Processing Standards Publication 201-1.

The CAC is the primary hardware token used for identifying individuals for logical access to the NIPRNet resources; this is in accordance with DTM 08-003[22] and the DoD PKI issues the digital certificates that are stored on the CAC for its use in unclassified environments.

Internal Applications

Internal applications on the NIPRNet function in the same manner as those on the internet and utilize the same browsers, databases and operating systems that are commonly seen in commercial industry.

In some of the more common applications such as communications (i.e. email, messages), the CAC’s signing key is used to digitally sign messages or documents while other applications may use the CAC’s encryption key to encrypt sensitive data.

[22] Chu, D. S. Department of Defense, Under Secretary of Defense. (2011). *Memorandum for distribution: Directive-type memorandum (dtm) 08-003, “next generation common access card (cac) implementation guidance”*. Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-003.pdf

External Application Access

The NIPRNet is enabled for internal users to access the internet through a web browser, although certain content may be prohibited or denied. Information pertaining to this can be found in the DTM 09-026 “Responsibilities and Effective Use of Internet based Capabilities”[23]. Internal users are provided this access through an external gateway for access to the global internet and tunneling is used for encrypted data.

When an approved external NIPRNet application will utilize PKI methods either from an external PKI or comply with DoD PKI’s the following DoD instructions apply:

- DoDI 8500.01
- DoDI 8500.02
- DoDI 8520.02

[23] Department of Defense, Deputy Secretary of Defense. (2010). *Memorandum for distribution: Directive-type memorandum (DTM) 09-026, “responsible and effective use of internet-based capabilities* (DTM 09-026). Retrieved from website: http://www.defense.gov/news/dtm 09-026.pdf

3. Electronic Voting Systems Background

Electronic Voting Systems (EVS), or e-Voting, encompass a variety of different technologies from optical scanning to kiosk and internet based systems, here the research is focused on online based systems. E-voting[24] systems have been a center of contention for various groups and individuals for some time, in regards to their security and ability to protect privacy.

The frameworks that make up e-Voting systems are composed of many different parts such as Registration Systems, Client Voting Platforms, Election Management Systems, and Tabulators to name a few. Each of the individual components has the potential to introduce vulnerabilities into the voting process. Thus testing, standards and clear policies are key to establishing systems that can provide the confidentiality, integrity and availability that is necessary for a trusted e-Voting framework.

Because trust is a fundamental key in the voting process, industry vendors have spent many years refining their own techniques and methodologies to convey their frameworks are reliable and trustworthy, the latest terms in authentication, encryption and communications methods are often cited in their whitepapers (i.e. SSL, PKI, symmetric keys, and others)[25] [26].

High-Level Conceptual Internet Based Voting System Architecture

All internet based e-Voting systems have similar architectures and use similar technologies such as authentication, encryption and digital signatures in the voting process. Figure 1 is an example of a high-level conceptual internet based voting system architecture.

[24] E-Voting, (2011), Retrieved from website: http://whatis.techtarget.com/definition/e-voting-electronic-voting
[25] See Everyone Counts, *Whitepapers: Security*, Retrieved from website: http://www.everyonecounts.com/whitepapers/SecurityOverviewEveryoneCounts.pdf
[26] See Scytl, *Whitepapers: Secure Electronic Voting*, Retrieved from website http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf

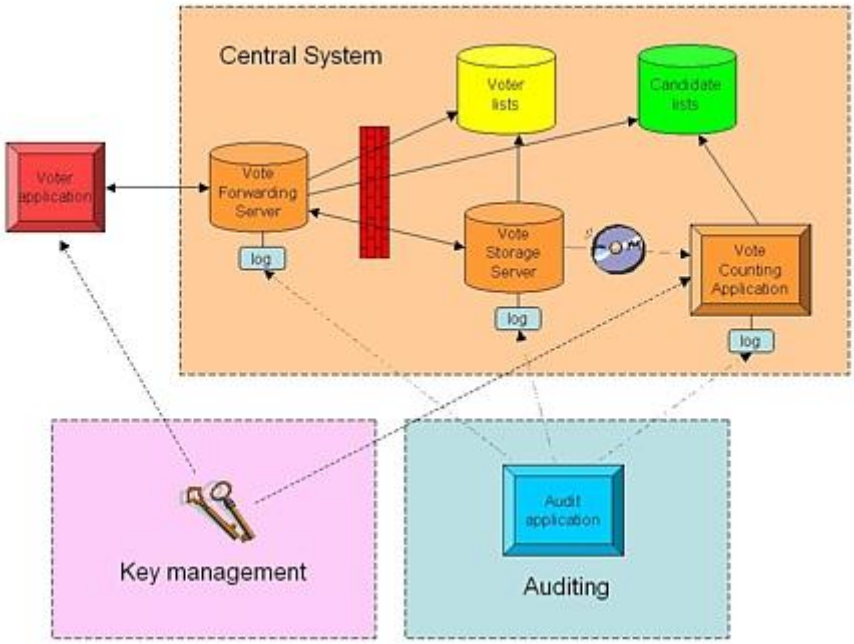

Figure 1: High Level Conceptual Voting System

Encryption plays a key role in these systems and is the primary method used to protect the end-user information. The most common encryption algorithms used in these internet e-Voting systems are listed in Table 5.

The internet based e-Voting systems are reliant on the total system to provide security for the voting process; this includes the operating system, hardware, software, configuration settings and the management of the computer that they operate on. To maintain the security of these systems requires diligence by IT staff in respect to having the latest OS updates along with proper configurations on the systems. Failure to maintain the entire system has the potential to open up vulnerabilities to the e-Voting platform.

Specification and Standards

Vendors of internet based voting systems have a multitude of computer industry standards that can be applied during the creation of their systems. The standards come from a variety of agencies and groups such as those listed below:

- NIST – National Institute for Standards and Technology
- IEEE - Institute of Electrical and Electronics Engineers
- ISO – International Organization for Standardization
- IEC - International Electrotechnical Commission
- IETF - Internet Engineering Task Force
- OASIS - Organization for the Advancement of Structured Information Standards
- FIPS – Federal Information Processing Standards
- IETF - Internet Engineering Task Force
- W3C - World Wide Web Consortium

These organizations are some of the major contributors to the foundation of the computer industry; the standards cover many areas such as electronics, communications, encryption, and protocols. In addition to these standards there are voting systems requirements that cover certifications and testing that must be done by each state/local jurisdiction in order for the system to be accepted for use in an election.

The Election Assistance Commission[27] (EAC) developed the 2005 Voluntary Voting System Guidelines[28] (VVSG) for testing of voting systems. Additional standards are emerging to provide interoperability between voting systems such as those being derived from the OASIS Election Markup Language[29] (EML) standard by NIST[30] and

[27] See Election Assistance Commission, Retrieved from website: http://www.eac.gov/
[28] Election Assistance Commission, (2005). *Voluntary voting systems guidelines* (v.1). Retrieved from website: http://www.eac.gov/assets/1/workflow_staging/Page/125.PDF
[29] See Advance Open Standards for the Information Society OASIS, Retrieved from website: https://www.oasis-open.org/standards#emlv5.0
[30] See NIST & HAVA, Retrieved from Website http://www.nist.gov/itl/vote/index.cfm

IEEE[31]. The EML standard(s) may help in simplifying EVS's by providing standardized methods for all voting client machines, to display information to voters and to pass information to the Local Election Officials (LEO's).

Specifications / Standards	Description
NIST/IEEE P-1622	EML for voting data.
EAC	Voluntary Voting System Guidelines

Table 4: Specifications and Standards

Security

The base methods used for security in internet voting systems are encryption methods, which provide a layer of confidentiality in the systems. Digital Signature methods are used to ensure the integrity of the data, such as the voting ballot information, to ensure data has not been modified. Common standards used in these processes can be seen in Table 5 below.

Specifications / Standards	Description
AES 128/192/256, (FIPS 197)	Advanced Encryption Standard
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
MD5	Message-Digest Algorithm (Cryptographically Broken)
RSA1024, 2048 (FIPS 186)	Ron Rivest, Adi Shamir and Leonard Adleman
SHA-1,2,3, (FIPS PUB 180-1,2,3)	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Table 5: Data Security Standards

The standards are used in different parts of internet based voting system[32]. As an example SSL can be used in browser based systems to provide secure transport of data to a server and back to the client. RSA public key technology is commonly used to

[31] IEEE, IEEE Standards Association. (2012). *Voting systems electronic data interchange project 1622: standard for electronic distribution of blank ballots for voting systems* (p-1622). Retrieved from website: http://grouper.ieee.org/groups/1622/

[32] See *Pnyx.core: The Key to Enabling Reliable Electronic Elections,* Scytl, Retrieved from website: http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf

digitally sign data or used in the authentication process through the use of digital certificates.

To protect the integrity of voting information, algorithms such as SHA can help ensure that data has not been modified during and after the voting process by creating a hash or checksum of the data. Vendors commonly use similar standards but have their own unique methods of how they are utilize to protect data and communications in their systems. In some cases, vendors split cryptographic keys and recommend that different individuals maintain control of only one portion of the key. This helps reduce the possibility of one insider being able to change information as it would require collusion with others in order to modify or affect the system.

As stated earlier e-Voting systems rely on many aspects of the platform they operate on so security must be applied across many areas such as the following:

- Applications (Browsers, etc)
- Network (Internet, Intranet, etc)
- Client Computer (User Authentication, OS)
- Configurations
- Data (Ballot Database)

In voting systems, security cannot be limited to just certain aspects of the system because even the best encryption methods can be thwarted by an insider with control of the cryptographic keys. Policy and procedures play just as critical a role as do the supporting technology used to protect the information. Although not necessarily a security related topic, redundancy/backup must also be a consideration in these systems as an insider could easily do physical damage to a system, making it difficult or impossible to obtain the data.

PKI in Voting Systems

PKI technologies provide a variety of services to protect e-Voting systems that cover authentication, secure communication and data signature. A common PKI method[33] used to insure the confidentiality of the communication[34] between a voter and a ballot server (LEO), happens through a secure exchange of a symmetric encryption key that is achieved by encrypting the symmetric key with the voter's private PKI key. The symmetric encryption key is then used to secure the communication during the voting process. Authentication is then used to identify the voter and ballot server through the use of a digital certificate (X.509). In the final process, the voter uses their digital signature key to sign their completed ballot. Although this is a simplification of the entire process that needs to transpire for a voting transaction, it is meant to convey the utilization of PKI in the process of internet based voting at a conceptual level.

How each voting system vendor utilizes the PKI methods, algorithms and the details related to key issuance, storage, exchange and revocation, are company dependent. These details may be proprietary for each vendor's product, and in many cases, are protected by a process patent.

When delving into the voting system details of communications between systems there is the potential for conflicts relating to network protocols. Some of these conflicts relate to the following protocols and system areas:

- IPv4
- IPv6
- IPsec
- NAT's
- VPN's

[33] See "How a secure key is agreed upon by two peers", Internet Computer Security, Retrieved from website: http://www.internet-computer-security.com/VPN-Guide/PKI.html

[34] See *Pnyx.core: The Key to Enabling Reliable Electronic Elections,* Secure Connection*, pg. 12.,* Scytl, Retrieved from website: http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf

- Availability of Encryption Methods (Key Sizes, Algorithms, etc.)
- OS versions
- Browser Versions

As an example, conflicts can occur when using IPSec and NAT's[35] which can cause conflicts for IP address translation thus making it impossible to use in certain situations.

The details regarding these conflicts require an in-depth knowledge of networks, protocols and security related topics; these details can be found through various publications and professional certification regarding security[36] and networks[37].

The conflicts will need to be addressed by each e-Vote vendor and reviewed on a case by case basis, but potential issues can be reduced or eliminated by standardizing the communication channel through the use of STIG's or voting systems standards. The STIG's provide technical guidance to help establish baseline configuration setting; for example if you are going to have a computer running the Microsoft Windows XP OS, there is a STIG that describes how to configure the baseline. In this same context a STIG could describe how to configure a system when using certain protocols or security technologies; this in turn helps avoid potential conflicts.

[35] See *2 Known Incompatibilities between NA(P)T and IPsec,* IPsec-Network Address Translation (NAT) Compatibility Requirements, Retrieved from website: http://www.ietf.org/rfc/rfc3715.txt
[36] See *CompTIA Security+*, Retrieved from website: http://certification.comptia.org/getCertified/certifications/security.aspx
[37] See *CompTIA Network+*, Retrieved from website: http://certification.comptia.org/getCertified/certifications/network.aspx

4. Common Access Card Background

The Common Access Card (CAC) is a type of smart card[38] used as the standard identification card for active-duty military personnel, selected Reserve, DoD civilian employees and eligible contractor personnel. It is a credit card sized (i.e. ISO/IEC 7810 ID-1 standard) card with an embedded integrated circuit commonly referred to as a smart card. Smart cards are typically used to provide identification, authentication, encryption, data storage and application processing for applications that require strong security, such as in financial transactions and security authentication for network sign-on. Smart Cards are commonly used to provide Two- or Three-factor authentication for both physical and logical access applications.

Two Factor:

- Something you know. (PIN number)
- Something you have. (Smart Card)

Three Factor:

- Something you know. (PIN number)
- Something you have. (Smart Card)
- Something you are. (Biometric)

The DoD uses the CAC for both physical access and logical access to defend computer networks and systems.

Smart cards just like any other computer based technology rely heavily on the information provided to it and its surrounding infrastructure or environment. The DoD utilizes IA practices to mitigate these risks throughout its organization and data systems which includes the CAC. The CAC is backed by a strong set of standards, policies and

[38] See Definition *Smart Card*, Retrieved from website: http://www.merriam-webster.com/dictionary/smart%20card

procedures to insure its full lifecycle process; this process includes manufacturing of the card, user vetting, key and certificate generation, issuance, usage, revocation and termination of the credential. See Table 6 for a list of CAC relevant specifications and standards.

Specifications / Standards	Description
DoDI 1000.13	"Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals"
DoDI 8520.02	Public Key Infrastructure (PKI) and Public Key (PK) Enabling (May 24, 2011)
DoDI 8520.03	Identity Authentication for Information Systems (May 13, 2011)
FIPS 201-1	Federal standard for Personal Identity Verification (PIV)
FIPS140-2	Security Requirements for Cryptographic Modules.
GSC-ISv2.1/NISTR 6887	Government Smart Card Interoperability Specification, National Institute of Standards Technical Regulation 6887 (July 2003)
HSPD-12	Homeland Security Presidential Directive
ISO/IEC 14443	Identification cards -- Contactless integrated circuit cards
ISO/IEC 7816-x	Electronic identification cards Pt. 1 Physical Characteristics Pt. 2 Dimensions and Locations for Contacts Pt. 3 Electronic signals and transmission protocols Pt. 4 Industry commands for interchange
NIST SP 800-76-1	Biometric Data Specification for Personal Identity Verification
NIST SP 800-79-1	Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers
NIST SP 800-104	Scheme for PIV Visual Card Topography
NIST SP 800-73-3	Interfaces for Personal Identity Verification –Part 1: End-Point PIV Card Application Namespace, Data Model and Representation. Pt. 2- PIV Card Application Card Command Interface. Pt. 3- PIV Client Application Programming Interface. Pt. 4- The PIV Transitional Interfaces & Data Model Specification.
NIST SP 800-78-3	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
NIST SP 800-85A-2	PIV Card Application and Middleware Interface Test Guidelines

Table 6: CAC and Smart Card Related Specifications and Standards

National Strategy for Trusted Identities in Cyberspace

Part of the CAC focus in this research report is on its use as an identity authentication credential for network access and or application access. The government has recently defined a national strategy regarding identity credentials for securing both government and public networks. The National Strategy for Trusted Identities in Cyberspace[39] (NSTIC) defines guidelines for establishing secure online credentials for the authentication of people and devices: the President's Cyberspace Policy Review established trusted identities as a cornerstone of improved cyber-security[40]. It is envisioned to include a vibrant marketplace that allows people to choose among multiple identity providers both private and public that would issue trusted credentials that prove identity. Some key benefits[41] described by NSTIC are:

- **Faster:** Once you use your credential to start an online session, you would not need to use separate usernames and passwords for each Web site. For example, your computer or cell phone could offer your "trusted ID" to each new site where you want to use the credential. The system would work much like your ATM card works now. By having the card and a PIN you can use your ATM card all over the world. By having a credential and a password you would be able to use your trusted ID at many different sites. This saves you time while enhancing security. No more searching in your drawer for your list of passwords.
- **More convenient:** Businesses and the government will be able to put services online that have to be conducted in person today like transferring auto titles or signing mortgage documents.
- **Safer:** Your trust credential will foil most commonly used attacks from hackers and criminals, protecting you against theft and fraud, safeguarding your personal information from cyber criminals.

[39] *Cyberspace is the interdependent network of information technology components that underpins many of our communications; the Internet is one component of cyberspace*
[40] The White House, (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communication infrastructure.* Retrieved from website: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[41] SEE "Some Key Benefits", NSTIC, retrieved from website http://www.nist.gov/nstic/

- **Private:** This new "identity ecosystem" protects your privacy. Credentials share only the amount of personal information necessary for the transaction. You control what personal information is released, and can ensure that your data is not centralized among service providers.

The CAC is part of this identity ecosystem as it has already been accepted as a trusted identity credential, thus the CAC is already part of this national strategy. As NSTIC further refines the national strategy it would be advantageous that the guidelines be reviewed and kept in mind for use of the CAC and or other credentials for use in the voting process.

User Vetting

A key component to the strength of the CAC, or any ID credential, is the vetting process. It is imperative that before any credential is issued, there must be confidence that the individual receiving the credential is who they say they are; this process is commonly referred to as identity proofing. In order to be considered for a CAC[42], an individual must be sponsored by a person affiliated with the DoD or other federal agency who will take responsibility for verifying and authorizing the applicants need for an ID card. The CAC vetting process includes the following:

- Sponsorship
    - Applicants for a CAC must be sponsored by a DoD government official or employee.

- Registration in the Defense Enrollment Eligibility Reporting System (DEERS) by filling out a DD Form 1172-2.

- Sponsors will initiate a background check. This process involves the following steps:
    - A Federal Bureau of Investigation (FBI) fingerprint check

[42] See Department of Defense, Common Access Card. Retrieved from website: http://www.cac.mil/common-access-card/getting-your-cac/

- A National Agency Check with Written Inquiries (NACI) check

- Setting an appointment to visit a Real-Time Automated Personnel Identification System (RAPIDS) site for final verification and processing.

  - Two forms of ID in original form are required (listed on the I-9 Form). At least one form of ID must be a valid state or federal government-issued picture identification (for example, passport, driver's license, or current CAC).
  - Fingerprints will be taken to be biometrically scanned for identifying characteristics.

The importance of the vetting process cannot be understated because the level of trust in the ID credential is only as good as the vetting done on the individual receiving it. Other common forms of ID in many cases are not vetted to the same extent as the CAC and thus the trust or assurance levels are not the same for all credentials. The assurance levels are defined in the NIST SP800-63 guidelines[43] and are listed below; the CAC in its most commonly issued format is considered to have a level 4 assurance based on these definitions.

Assurance Levels	
Level	**Description**
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

Table 7: Assurance Levels

Level 1 - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is

[43] Burr, W., Dodson , D., Polk, W., U.S. Department of Commerce, National Institute of Standards and Technology. (2006). *Electronic Authentication Guideline* (v1.0.2). Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Level 2 - At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Level 3 - At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Level 4 - Authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and

since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Architecture

The internal architecture of the CAC has evolved since its first introduction, which was defined in the Government Smart Card Interoperability Specification (GSC-IS) or better known as NIST Interagency Report 6887[44] (NISTIR 6887). Part of the CAC evolving architecture came about when Homeland Security Presidential Directive number 12[45] (HSPD-12) was signed. This led to the creation of the Federal Information Processing Standard 201[46] (FIPS 201) that specifies the Personal Identify Verification's (PIV) technical requirements in support of HSPD-12. Part of the specification covers the use of smart cards for access to federal facilities and information systems, the details of which can be found in the Special Publication SP800-73-3. In order for the CAC to become compliant with the PIV specification a hybrid design has evolved. Today's version of the CAC is commonly referred to as the "next generation CAC" and the previous version is called the "Legacy CAC"; the "next generation CAC" is also referred to as the CAC PIV end Point, this is where the designs merge.

The present CAC environment now has a mixture of versions in circulation (CACv2 and CAC PIV end point) and will continue as new or changing requirements are introduced. The government workgroups and standards committees have made every effort to reduce the risk of non-interoperable cards as new versions are introduced into the environment.

A big part of the CAC architecture involves the layout of the containers that store data inside the CAC memory. In Appendix B – Common Access Card, Figure 8 depicts the available containers for data to be placed in and Table 17 lists the data elements that

[44] Schwarzhoff, T., Dray , J., Wack, J., Dalci, E., Goldfine, A., & Lorga, M. U.S. Department of Commerce, National Institute of Standards and Technology. (2003). *Government smart card interoperability specification* (v2.1). Retrieved from website: http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

[45] Bush, G. W. U.S. Department of Homeland Security, (2004). *Homeland security presidential directive 12: Policy for a common identification standard for federal employees and contractors*. Retrieved from website: http://www.dhs.gov/homeland-security-presidential-directive-12

[46] U.S. Department of Commerce, Computer Security Division. (2006). *Federal information processing standards publication personal identity verification of federal employees and contractors.* Retrieved from website: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

reside in these containers. Just as computers can limit access to data on a hard drive through the use of roles and access rights, the CAC provides these mechanisms through the use of Access Control Rules (ACR). ACR's define the rules for reading, updating and general authentication of the specific container and are established when the card is instantiated. As an ACR example, the PIV data model lists the mandatory containers and the ACR's required for the specified containers, these are shown in Table 8.

Data Object	Contact			Contactless			M/O
	Read	Upd	Gen Auth	Read	Upd	Gen Auth	
Card Capability Container	ALW	NEV	N/A	NEV	NEV	N/A	M
Card Holder Unique Identifier	ALW	NEV	N/A	ALW	NEV	N/A	M
X509 Certificate for PIV Authentication	ALW	NEV	PIN	NEV	NEV	NEV	M
Card Holder Fingerprints	PIN	NEV	N/A	NEV	NEV	N/A	M
Printed Information	PIN	NEV	N/A	NEV	NEV	N/A	O
Card Holder Facial Image	PIN	NEV	N/A	NEV	NEV	N/A	O
X509 Certificate for Digital Signature	ALW	NEV	PIN ALW	NEV	NEV	NEV	O
X509 Certificate for Key Management	ALW	NEV	PIN	NEV	NEV	NEV	O
X509 Certificate for Card Authentication	ALW	NEV	ALW	ALW	NEV	ALW	O
Security Object	ALW	NEV	NEV	NEV	NEV	N/A	M

Table 8: PIV Data Objects Access Control Rules
ALW-Always, NEV-Never, N/A-Not Available, M-Mandatory, O-Optional

The CAC ACR's for its defined containers function in the same manner as the PIV and CAC containers are combined with PIV containers in the CAC PIV End point data model. The CAC certificate containers have the following ACR's:

	Key Name	Key Purpose	Access Read / Usage
CAC Certificates	PKI Signature Key	PKI Logical Login (Outlook) Digital Signature with non-repudiation, logical access, PIN. Outlook requires special extension.	ALW/PIN
	PKI Identity Key	Can be used for non-repudiation signing outside Outlook.	ALW/PIN
	PKI Encryption Key	Key Encipherment (Email encryption)	ALW/PIN

Table 9: CAC Certificate Containers

Other containers in the CAC include the Person and Personnel containers, the data elements in these containers can be found in Table 17 of Appendix B.

Usage

The CAC is utilized for both physical and logical access as well as encryption and digital signature applications. Data contained on and in the card can also be useful depending on the application requirements. An important factor in the usage of the data provided by the card is the freshness of the information. The data placed on the physical surface of the card cannot be refreshed (i.e. barcodes, picture, etc.), unless a new card is issued thus this data is only fresh when the card is issued and grows older the longer the individuals has the card. Data internal or held in the memory of the card can be refreshed but is normally static in nature (i.e. Name, DOB, Fingerprints, Keys, etc.). The most common uses for the CAC are to log into computer systems or networks, digital signatures and encryption.

As a consideration in the voting process, the use of authentication for identification purposes and digital signatures provide the most attractive functions for the voting process. Additional information in the card may also provide a source of data for identification purposes, but will need to be reviewed for potential privacy concerns. It is important to point out that even though a data container (memory) in the card has ACR's for access; each individual data item in the container does not. When a data container ACR has been satisfied, an application has access to all the data stored in the

container; this may inadvertently expose data elements that could fall under privacy rights or regulations in regards to the voting process.

In the voting application usage considerations for the CAC, the card turnover rate needs to be part of the equation. Card turnover rates cover items such as hardware failure, expiration, lost and stolen card. Anecdotally this number appears to be minimal when compared to the total number of CACs in circulation, but it only takes one card to disrupt the voting process. Mitigation plans will need to be considered for these user circumstances, when looking at the potential disruptions to a voting process application.

Applications

The CAC is used in a variety of DoD applications, its core function in these applications is usually authentication into a network for access to resources. The DoD is continuing its CAC enabling of applications throughout its organizations; a good example is the recent CAC enabling of the Joint Personnel Adjudication System (JPAS) system. JPAS is a web-based application that provides access to information regarding security clearances. The application requires the use of the CAC for authentication purposes before any access is granted to the system and its information. In this application the authentication information is gathered from data in the memory of the card (i.e. Authentication Certificate) and cryptographic functions. Other applications, such as those being tested for airport gate entry by the Transportation Security Administration (TSA), utilize data printed on the outside of the card, such as bar codes.

The use of middleware is usually a requirement for smart cards in CAC enabled applications, but in recent times operating systems and browsers have included smart card driver software in their releases, thus making it easier for the end-user when enabling the client system for their use. This is still highly dependent on the version and manufacturer of the operating system; for example the Microsoft Windows 7 is compatible with smart cards[47] [48] out of the box.

[47] See *Windows 7 and Smart Cards*, http://www.windows7update.com/Windows7-Smartcard.html
[48] See *Information* section, Retrieved from website: http://militarycac.com/noactivclientwindows7.htm

CAC enabling of applications has become easier since the initial release of the CAC where many additional steps and software were required to enable an application for use with a smart card. Today most applications integrate the CAC utilizing standards based middleware; the type of middleware used is dependent on the application type (i.e. Web-based, Standard Client Application). ActivClient[49] middleware supports both web-based and application based interfaces through standardized protocols such as CryptoAPI, PKCS#11 and the SP800-85 interfaces.

Non-DoD Applications

The CAC is also being enabled for commercial use through the use of CAC middleware (NIST SP800-85) in software applications such as WinMagic's SecureDoc[50] product. SecureDoc supports single and multi-factor pre-boot authentication including password, smartcard, USB token, biometrics, the Trusted Platform Module (TPM) and PKI. The DoD CAC integrated with SecureDoc full-disk encryption software permits only authorized users to boot up their PCs or notebook computers, authenticating and authorizing users for secure access to their encryption hard drives. WinMagic has completed the certification process with the Department of Defense for the CAC interoperability with its SecureDoc full-hard disk encryption software.

PuTTY-CAC[51] is another commercially available product that is a freeware SSH client for Windows that supports smartcard authentication using the US Department of Defense Common Access Card as a PKI token. This software is provided through Forge.mil[52] which is a community consisting of project/program managers, software developers, testers, warfighters and other stakeholders responsible for the acquisition of Information Technology.

[49] See *ActivClient for Common Access Cards*, Retrieved from website: http://www.actividentity.com/products/securityclients/ActivClientforCommonAccessCards/
[50] See WinMagic SecureDoc, Retrieved from website: http://www.winmagic.com/market-segment/government/dod-cac-card
[51] See PuTTY-CAC, Retrieved from website: http://www.risacher.org/putty-cac/
[52] See Forge.mil, Retrieved from website http://www.forge.mil/Community.html

Security

The inherit design of smart cards is focused around security[53] and the protection of information that will be stored in the card (i.e. keys, data). Many smart cards undergo testing, to receive certification and to ensure they comply with the security standards such as FIPS140-2.

Both hardware and software methods are used to create this secure environment using hardware such as crypto-coprocessors, random number generators and secure memory as well as software that abides by Java Card[54] and GlobalPlatform[55]. The CAC also utilizes external security methods such as barcodes and tamper resistant surface materials; A CAC example can be seen in security policies provided by vendors[56] as part of the FIPS140-2 process.

The CAC architecture as stated previously utilizes defined containers to separate its data storage. Access Control Rules (ACR's) on each of the defined containers are used to control access to the data that resides in the container. The ACR's are determined at instantiation of the CAC applets; as an example, a container may require a PIN number before read access is granted to the specific container.

Smart Cards do not rely on just a single method to protect information, however it is the combination of policy, standards, hardware and software that make the environment secure.

Middleware

Smart Cards have their own protocol used to communicate with the cards called Application Protocol Data Units (APDU's). Parts of the NISTIR 6887 specification as

[53] Smart Card Alliance, (2008). *What makes a smart card secure?: A smart card alliance contactless and mobile payments council white paper* (CPMC-08002). Retrieved from website: http://www.smartcardalliance.org/resources/lib/Smart_Card_Security_WP_20081013.pdf
[54] See Java Card, Retrieved from website: http://www.oracle.com/technetwork/java/javacard/overview/index.html
[55] See Global Platform, Retrieved from website: http://globalplatform.org/
[56] Oberthur Technologies of America Corp., (2010).*Oberthur id-one cosmo 128 v5.5 for DoD common access card (CAC).* Retrieved from website: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1145.pdf

well as the SP800-73-3 specification define an Application Programming Interface (API) commonly referred to as the middleware which sits between an application and the smart card. The middleware allows applications to communicate with the card without having intimate knowledge of the card communication details. The DoD CAC middleware must go through a Joint Interoperability Test Command (JITC) test process to receive approval before the DoD will certify its use within government systems.

Middleware[57] makes interfacing with the CAC much easier for both web and system based applications but both applications and middleware have a common area of weakness in regards to user input. Key stroke loggers have the potential to capture user PIN numbers, depending on the CAC container access control rights; this can lead to the exposure of data on the card; the Sykipot[58] malware is a good example of this exploit

During the use of the CAC, while the smart card is still inserted in the smart card reader, a key stroke logger can capture the user PIN number when entered. Depending on the access control rights of the container, the malware can gain access to information, such as the digital certificates data. The information in the digital certificates can then be used in a spear-phising or zero-day exploit to gain access to the networks. This can only happen in a per-victim basis, but once the information has been obtained the potential for harm to the network goes up. This can be mitigated by hardening the middleware similar to how the payment card industry handles this, which uses a dynamic data element to ensure each transaction is authenticated.

Additional middleware commonly used by web browsers to interface with security tokens are used for web based applications via what is termed a plug-in or add-on. This middleware is dependent on the web browser manufacturer used but the two most

[57] See CAC Developers Technical Guides, Retrieved from website: http://www.cac.mil/common-access-card/developer-resources/
[58] Stephen Lawton, (2012,) SC Magazine, *DoD Cards Under Attack,* Retrieved from website: http://www.scmagazine.com/dod-id-cards-under-attack/article/223625/

common forms of middleware are the Public-Key Cryptography Standard (PKCS#11) and the Cryptographic Application Programming Interface (CryptoAPI).

Data Elements

The CAC has both external and internal data elements[59]; the figure below shows the external data elements that can exist on the card dependent on the card type issued.

External

The information presented on the surface of the card, just like the internal information held in the card memory, is dependent on the card type issued. Figure 2 shows all the externally available fields which may or may not be present depending on the card type issued[60]. The external elements that may be beneficial in the voting process are the following:

- Picture
- Expiration date
- DoD ID number

Figure 2: CAC External Data Elements

[59] See CAC Data Elements, Retrieved from website: http://www.cac.mil/common-access-card/developer-resources/
[60] See CAC Topology, Retrieved from Website: http://www.cac.mil/common-access-card/

Card Bar Code Information

- Name
- Social Security Number (to be removed in 2012 replaced with EDIPI number)
- Date of birth
- Personnel category
- Pay category
- Benefits information
- Organizational affiliation
- Pay grade

The bar code information can be used as an additional security measures in the authentication process for access to a voting system or network. As mentioned earlier the TSA has a pilot program that utilizes this information for airport gate access; this is only for active duty personnel. In the pilot, the bar code is scanned and used to look up data in the DEERS database allowing the verification of the individuals status, meaning are they active or not. An item of concern in regards to the data used in this process involves the freshness of the data in the system (both DEERS and or the CAC). In general the data has a typical refresh rate of 24 hours or less, meaning there is the potential for a lag in information used for any type of application.

Internal

The CAC's internal data is stored in predefined memory containers; these containers hold specific information defined by the data model in use. Access to the data containers is controlled by a set of ACR's that are predefined by the issuing agency and instantiated at issuance. For the CAC, most applications only provide read functions after the proper ACR has been accepted; only under certain conditions and with the use of specific applications (issuance, updates) can an update/write function occur. Appendix B includes the internal CAC PIV fields available. The internal data elements that may be beneficial in the voting process are highlighted in Table 17.

Privacy Considerations

The CAC conforms to the regulations stated in the DoD Privacy Program[61] (5400.11-R, August 1983); additional CAC privacy[62] information can also be found on the CAC website. Through the design process of both the CAC and PIV, privacy has always been a priority and still is today. In recent time, the DoD decided to remove the Social Security[63] number from barcode and other areas of the CAC due to privacy concerns. The field value is being replaced by the Electronic Data Interchange Personal Identifier (EDIPI[64]) number, which is a unique number that is associated with the card owner and is recorded in the DEERS database. The number consists of ten-digits and is located in the barcode on the front of the card, the barcode on the back of the card, and stored in the card memory. The first 9 digits are unique numbers with the 10th digit being a check digit for the identifier. These changes will be implemented on newly issued CAC's starting on December 1, 2012.

[61] U.S. Department of Defense, Office of Assistant Secretary of Defense. (1983). *Privacy program* (DoD 5400. 11-R). Retrieved from website: http://www.cac.mil/docs/DOD-5400-11.pdf
[62] See CAC Privacy, retrieved from website: http://www.cac.mil/common-access-card/cac-security/
[63] See DoD DMDC, CAC, SSN Removal Communications Plan, Retrieved from website: http://www.cac.mil/docs/Information-Paper-SSN-Removal-Feb-11.pdf
[64] EDIPI, (n. d.), Retrieved from website: http://www.ako-webmail.com/faq/edipi/

5. Client Configurations

Voting is not an everyday event for UOCAVA voters; with this in mind, the conceptual framework in Section 6; takes into consideration a Voting Client that may only be a single use machine for the period or duration of the voting process. This allows for the possibility that a client computer can be utilized for other task/work during non-voting periods, as it may not be practical or cost effective to have a computer dedicated just for voting.

Consideration must also be given to NIPRNet connections, which have expiration dates and may reside in different locations between voting periods, making a dedicated Voting Client impractical. The Connection Process Guide[65] describes the details of expiration dates being assigned after the approved connection to the DISN through the granting of either an ATC or an IATC, which is normally assigned an expiration date to coincide with the Authorization Termination Date (ATD) of the customer. It is also important to note that some IA enabled products may need to be selected from the DoD UC Approved Products List[66] (APL) prior to connection.

Client Baselines

Following industries best practices it is recommended that the client computer used in the voting process begin with a well-known baseline free of malware and unnecessary applications; to better ensure this, a minimum set of baselines need to be considered for the voting client, such as those listed below.

- Security Baseline
- Configuration Baseline
- Performance Baseline

[65] Defense Information Service Agency, Enterprise Connection Division. (2011). *Connection Process Guide* (v3.2). Retrieved from website: http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf
[66] DISA APLITS, DoD UC Approved Products List, https://aplits.disa.mil.

The Security and Configuration baselines (STIG's) utilized by the NIPRNet should serve as a good starting point for consideration for Voting Client baselines. These baselines are built upon IA best practices and cover a variety of areas such as OS's and many other areas. The performance baselines will need to be determined based upon the throughput expected during the voting periods (number of users) and testing.

Security Baselines

Security baselines provide the starting point for the operating systems that will be utilized in the voting process; this includes both end-user operating systems and server systems. The baseline is used for System Hardening, which is the practice of making a system or application more secure from its default installation. This can include some of the following practices:

- Protecting passwords (Policy, strength, length, lockout, etc.)
- Disabling unneeded services
- Disabling unneeded applications
- Disabling unneeded ports
- Patch and Change Management (Testing)
- Protecting management interfaces and applications

By disabling unnecessary services[67] you eliminate attackers' abilities to attack these services, as an example, disabling the FTP service eliminates the exploitation of FTP vulnerabilities. Disabling unnecessary services and removing unneeded protocols provides key benefits including:

[67] See *Disabling Unnecessary and Dangerous Services*, Government Security Org, Retrieved from website: http://www.governmentsecurity.org/forum/topic/1480-disabling-unnecessary-and-dangerous-services/

- Protection against zero day attacks.
- Risks associated with open ports.

Removing unneeded applications helps eliminate vulnerabilities associated with software bugs that are frequent in software. Proper management of systems (servers, clients, routers, etc.) can also help to eliminate these issues.

The NIPRNet uses the Host Based Security System (HBSS)[68] which is a commercial-off-the shelf (COTS) suite of software applications used by the DoD to monitor, detect and counter attack against DoD computer networks and systems. The HBSS or parts of the software should be a consideration for use as part of a security baseline.

Client Operating System

The NIPRNet is a heterogeneous environment[69], utilizing hardware and system software from different vendors, like many modern day networks. This type of environment adds a level of complexity for any EVS that could be deployed on a client computer; areas of concern are the following:

- BIOS (Secure Boot)
- OS Versions
- Browser Versions
- Available Encryption libraries. (PKI Certificates, Key Sizes, Algorithms, etc.)
- IPv4 or IPv6 (issues related to NAT's and IPSec)

[68] Host Based Security System (HBSS) software used by the DoD to monitor, detect and counter attacks against the DOD computer networks and systems. Retrieved from website: http://www.disa.mil/Services/Information-Assurance/HBS/HBSS

[69] See heterogeneous environment , Retrieved from website: http://www.pcmag.com/encyclopedia_term/0,1237,t=heterogeneous+environment&i=44213,00.asp

Computer Basic Input/Output System (BIOS) or better known as the Systems BIOS on IBM PC compatible computers can provide methods for securing the Operating System and the applications that are allowed to run on the PC. In currently available computer systems the BIOS can be rewritten providing a mechanism for upgrades and patches but this can also add vulnerabilities. New technologies and standards are emerging in this area, such as the NIST BIOS Protection Guidelines[70] (NIST SP800-147) that provides guidance in this area. Secure Boot[71] and or the Unified Extensible Firmware Interface[72] (UEFI) is also another new technology. The Unified EFI Forum is a non-profit collaborative trade organization formed to promote and manage the UEFI standard. The UEFI Forum board of directors includes representatives from the following eleven leading companies:

- AMD
- American Megatrends Inc.
- Apple Computer, Inc.
- Dell
- Hewlett Packard
- IBM
- Insyde
- Intel
- Lenovo
- Microsoft
- Phoenix Technologies

Figure 3 provides a visual representation of how this interface fits into the BIOS chain.

[70] Cooper, D., Polk, W., Regenscheid, A., & Souppaya , M. U.S. Department of Commerce, National Institute of Standards and Technology. (2011). *Bios protection guidelines recommendations of the national institute of standards and technology* (Special Publication 800-147). Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

[71] Bottomley, J., & Corbet, J. The Linux Foundation, (2011).*Making UEFI secure boot work with open platforms*. Retrieved from website: https://www.linuxfoundation.org/sites/main/files/lf_uefi_secure_boot_open_platforms.pdf. also see, http://www.wired.com/wiredenterprise/2012/08/secure-boot/

[72] See UEFI, (n. d.), Retrieved from website: http://www.uefi.org/home/

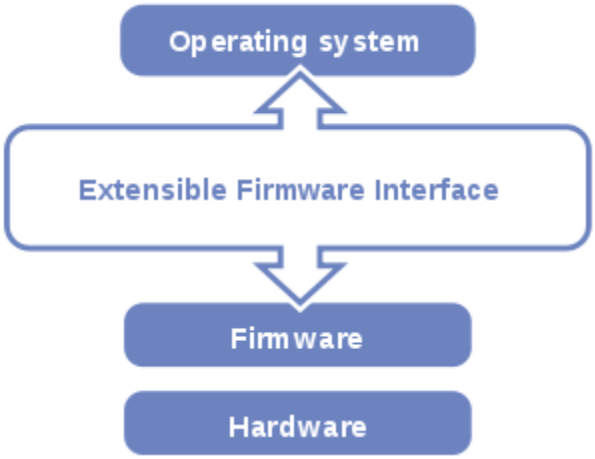

Figure 3: UEFI Interface Position in the BIOS Start up chain

The UEFI specification defines an interface between an operating system and platform firmware; the specification is primarily intended for the next generation of IA architecture–based computers.

OS vendors that are presently experimenting with the UEFI specification (Microsoft & Linux) have included the use of cryptographic keys as a means to link or allow only registered software and applications to run on the OS platform. This technology has the potential to provide additional benefits for EVS's and client systems as part of the security baseline, but may impose limits on the selection of computers and operating systems to just those that support the standards.

The Trusted Computing Group[73] (TCG) which is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms, has also provided specifications for a Trusted Platform Module[74] (TPM). Below is a list of the TCG contributing companies.

- Absolute Software
- Accenture
- Insyde
- InterDigital
- SanDisk
- Seagate

[73] See TCG, (n. d.), Retrieved from website: http://www.trustedcomputinggroup.org/
[74] See TPM, (n. d.), Retrieved from website: http://www.trustedcomputinggroup.org/developers/trusted_platform_module/

- American Megatrends, Inc.
- Mossys
- ARM
- ATMEL
- Battelle
- Bertin Technologies
- Broadcom Corporation
- Dell
- DMI
- DRS Technologies
- Enterasys Secure Networks
- Ericsson
- Freescale Semiconductor
- Gemalto
- General Dynamics
- Hitachi, Ltd.
- Huawei
- Infoblox
- Insight
- Communications, LLC
- Jetway
- Micron Technology, Inc.
- Nationz
- NetApp
- Nokia
- Nuvoton
- NVIDIA Corp
- NXP
- Oracle
- Panasonic
- Phoenix Technologies
- PMC
- Qualcomm
- Red Hat, Inc.
- Ricoh Company LTD
- SafeNet
- Samsung
- Security Innovation
- SK Hynix
- SMSC
- Sony Corporation
- SOPHOS
- STMicroelectronics
- Symantec Corporation
- Texas Instruments
- Thales Communications & Security
- The Boeing Company
- TOSHIBA
- TOYOTA
- ULINK
- VIA Technologies, Inc.
- ViaSat
- WD
- WINMAGIC Data Security
- SMSC

The group is recommending that TPM's be included with computers to enable trusted computing features. TCG also recently released a Trusted Network Connect[75] (TNC) protocol specification, based on the principles of Authentication, Authorization and Accounting[76] (AAA), by adding the ability to authorize network clients on the basis of hardware configuration, BIOS, kernel version, and which updates that have been applied to the OS and anti-virus software.

Microsoft has included parts of the TCG specifications in its Next-Generation Secure Computing Base[77] (NGSCB) architecture. NGSCB relies on hardware technology designed by the TCG which includes a number of security-related features, including the ability to hold cryptographic keys for various purposes of securing the OS platform. This technology would also be a consideration for EVS client systems but just like other technologies mentioned, could limit the selection of both hardware and OS's.

[75] See TNC, (n. d.), Retrieved from website: http://www.trustedcomputinggroup.org/solutions/network_security/
[76] See AAA, (n. d.), Retrieved from website: http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting
[77] See NGSCB, (n. d.), Retrieved from website: http://www.microsoft.com/resources/ngscb/default.mspx

OS versions

Because of the heterogeneous environment of networks and computers systems, there are no guarantees as to the consistency of OS's or OS versions within a network. Taking this into consideration the security baseline needs to focus on interoperability and the minimum requirements necessary to provide a secure operating environment.

Part of ensuring a secure environment begins with patch and change management on the operating systems. Strong consideration needs to be undertaken to ensure the proper scheduling and testing of patches on client computers that will be used in an election process. This statement holds true for both NIPRNet and non-NIPRNet based environments.

The operating systems must also meet minimum standards for encryption support and key strengths. Stakeholders involved in the creation of standards and secure internet-based EVS's will need to abide by a minimum set of guidelines as to acceptable encryption standards and time frames for the review of these guidelines at regular intervals. These guidelines will have a direct impact on the OS's and web-browsers used in the voting process; this is due to the cryptographic libraries[78] and the functionality they provide. As an example, if the guidelines require the use of an AES encryption algorithm utilizing a 256 bit key and the cryptographic library provided with the OS version only supports 3DES or AES with a 128 bit key, this will not pass the specification requirements. This can also impact the EVS manufacturers in their ability to protect data at the specified encryption strength and or not work with the vendor's software. In some cases a third party may need to supply an encryption library, this will requiring special instructions for installation and use on the OS version or web-browser, which may impose an unnecessary burden.

[78] Microsoft, Technet. (2012). *FIPS 140 evaluation*. Retrieved from website: http://technet.microsoft.com/en-us/library/cc750357.aspx

Virtualization

A Virtual Machine[79] is a software implementation of a machine (i.e. a computer) that executes programs like a physical machine. VM's provide the possibility of establishing a standardized configuration baseline for a voting client platform; this would allow most client computers to be standardized (OS and applications available on platform) regardless of the underlying physical machine used.

VM's provide a common method for reducing the cost of having multiple physical machines and are utilized by both companies and government agencies. Just like physical machines, they require maintenance and patch updates to keep them secure, but unlike a physical machine they are much easier to replicate and port to another machine. Through the process of copying, a baseline OS configuration, a VM would allow for an easier deployment of a secure operating environment for both a voting client and server. VM's are a very useful tool and should be a consideration for use in the voting process; they still have vulnerabilities such as a VM Escape attacks[80], which is an exploit that could give the attacker access to the host operating system and all other virtual machines VM's running on that host, but these can be mitigated through appropriate methods such as the following:

- Keeping virtual machine software patched.
- Installing only the resource-sharing features that you really need.
- Keeping software installations to a minimum because each program brings its own vulnerabilities.

[79] See Virtual Machine (VM), (n. d.), Retrieved from website: http://www.vmware.com/virtualization/virtual-machine.html
[80] See VM Escape Attack, TechTarget, Retrieved from: http://whatis.techtarget.com/definition/virtual-machine-escape

Bootable Media

Boot Disks[81] have been around since early operating systems such as DOS; they provide a convenient method for booting systems that may have problems, such as hard-drive boot sector errors and malware infected operating systems. Today, boot disks can be created using CD-R/DVD-R, Flash Drives[82] and other media. They are also commonly used when installing, replacing or updating OS's on computer systems. DISA provides information on this topic through its Bootable Media Program[83] which supports the operation and defense of the GIG by providing an operating environment to authorize home users to access the GIG utilizing bootable media.

Light versions of operating systems such as the Lightweight Portable Security[84] (LPS) product, available through the Software Protection Initiative[85] and those provided in Microsoft products provide a secure bootable version of an operating system. When these secure bootable operating systems are deployed on read-only media, such as CD-R's, which are Write Once Read Many (WORM) media, the associated risk with modification is reduced due to the inability to overwrite or change the software on the CD-R.

The LPS product was certified on June 15, 2011 by AFNIC[86] to connect to the GIG for general telecommuting use. An added benefit of LPS is that it was created using Open Source Software[87] (OSS) and thus has no license fees associated with it. Utilizing WORM[88] based media, as described above, in conjunction with a light weight OS can limit potential attacks, both externally and internally, by limiting the availability of write operations, ports, services, protocols and applications necessary to carry out specific

[81] Boot Disk, (n. d.), Retrieved from website: http://windows.microsoft.com/is-IS/windows7/What-is-a-boot-disk-startup-disk-and-why-would-I-need-one
[82] USB Flash Drive, (n. d.), Retrieved from website: http://bama.ua.edu/~gurle001/tutorial.htm
[83] See DISA's Bootable Media Program, Retrieved from Website: http://www.disa.mil/Services/Information-Assurance/HBS/BM
[84] Lightweight Portable Security (LPS), http://spi.dod.mil/lipose.htm, http://spi.dod.mil/docs/LPS_DS.pdf
[85] See Software Protection Initiative, Retrieved from website http://spi.dod.mil/index.htm
[86] Air Force Network Integration Center (AFNIC), retrieved at website http://www.afnic.af.mil/
[87] OSS, (n. d.), Retrieved from website: http://opensource.org/osd.html
[88] See "What is WORM storage", HP, Retrieved from website: http://h18006.www1.hp.com/products/storageworks/wormdps/index.html

exploits against client systems. When a light weight OS is booted from read-only media and no access is given to control the underlying hardware, the potential for malware on the system is essentially reduced. Adding additional layers of software to these OS's can also provide more security through the use of such items as software firewalls and active Anti-Virus programs.

To help reduce the threat of counterfeiting to these CD-R bootable media, additional measures can be applied, such as requiring a cryptographic key (PKI) to use the software; the key could then be verified either in an online or offline mode depending on the mechanisms chosen. In these cases the distributor of the CD-R bootable media would need to have a system in place for the process of verifying the key and enabling the software.

Web Browsers

Many EVS's utilize client based web-browsers to provide the presentation layer to the end-user for the voting experience. The modern web browser (i.e. Microsoft Internet Explorer, Mozilla Firefox, etc.) can be configured in "Kiosk Mode" [89] to limit the user's ability to navigate outside a network destination range or to access/run other applications. This prevents a malicious (or uninformed) insider from navigating to harmful sites. Using these web-browser configuration methods in combination with technologies described previously and or a light weight read-only media OS can offer a very secure baseline for a voting client.

Middleware

When considering the usage of certain technologies, such as smart cards and biometrics on client computers, additional levels of software are required. The software interfaces that allow applications to take advantage of these technologies are referred to

[89] See Web Browser "Kiosk Mode", Retrieved from website: http://support.microsoft.com/kb/154780, https://addons.mozilla.org/en-us/firefox/addon/r-kiosk/, http://think2loud.com/868-google-chrome-full-screen-kiosk-mode/, http://www.opera.com/support/mastering/kiosk/,

as middleware. Because this research is focused on the use of the CAC as an authentication method, the middleware associated with the CAC and other smart card based systems is twofold. The CAC middleware specification is described in an earlier section along with the API interface. The next layer of middleware also described in the CAC section of the report, provides functionality for cryptographic capabilities utilizing the PKCS#11 and the Microsoft CryptoAPI interfaces. Both of these interfaces can be utilized by web-browsers and other applications to provide the necessary cryptographic functions for an application. In the case of EVS's that utilize a web-browser, the CAC or other smart cards can provide services through vendor provided middleware.

Deployment

Deployment is a key concern in the process for distributing software and or hardware for a client voting platform. The full process from beginning to end needs to be considered; in this section we will focus on a few of the major concerns.

With the use of web-browsers, the need to distribute an application becomes almost unnecessary for a web based voting application, but if we consider the use of bootable media and or middleware for smart cards or other technologies such as biometrics, software will have to be distributed at some level. When distributing software there are various considerations to take into account such as some of the following:

- Software Versions (Version Control)
- Integrity of the Software
- Software linkage to specified locations
- Distribution method (Mail, Electronic)
- Installation
- Configuration
- Counterfeiting

One consideration, based on the topics that have been covered previously, would involve the use of a VM. In this case, an entire machine configuration with all the security baselines could be provided to the voting locations by electronic means. Another consideration is the use of light weight OS bootable media, that would have the entire configuration and security baselines provided which also could be distributed by electronic means. Figure 4 is a representation of one way that software can be distributed by electronic means. A source system could be configured with the baseline configurations specified for the voting process; this could be in the form of either a VM or bootable media. An image server could be considered for the actual distribution process of the software image to the appropriate site locations utilizing PKI methods to provide a level of trust.

In the case of bootable media and or possibly a VM, the image would be copied to a CD-R/DVD-R for usage. This process may also require the use of PKI keys to ensure the software is only used on or can be installed on the designated machines.

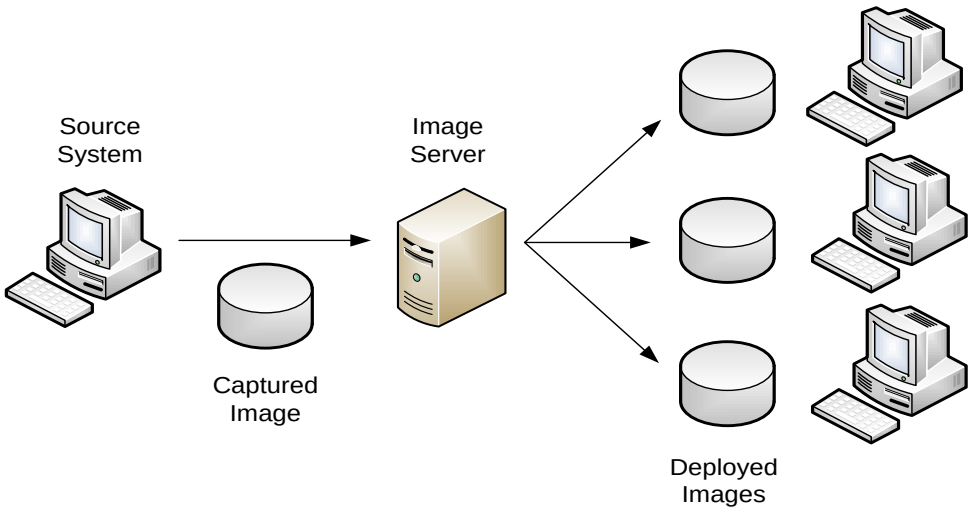

Figure 4: Deploying Secure Host Images

6. Feasibility Evaluation

This section reviews the feasibility of developing/deploying a secure framework in support of remote electronic voting.

Key Assumptions

In performing the feasibility evaluation, a number of key assumptions have been made:

List of Key Assumptions	
No.	**Assumption**
1.	The target population is UOCAVA voters
2.	Voters in the target population have been issued (or are eligible to receive) CAC's
3.	Voters in the target population will have access to computer workstations with network access
4.	Electronic Voting Systems will be used by the States to allow remote electronic voting by the target population
5.	The DoD intends to support the voting process only by providing authentication of system users to the appropriate Local Election authorities and by providing a secure communication channel between the voter and the appropriate Electronic Voting System as directed by the State
6.	The DoD is making no assertion of eligibility to vote – this is entirely retained by the State authorities.

Conceptual Framework

For the purposes of allowing review/discussion of options and considerations, a baseline conceptual framework is illustrated in Figure 5 from which the pros, cons and alternatives in each area can be discussed. It brings together each of the individual components evaluated throughout this report and is intended to enable review/analysis only – it is not intended as a representative framework design.

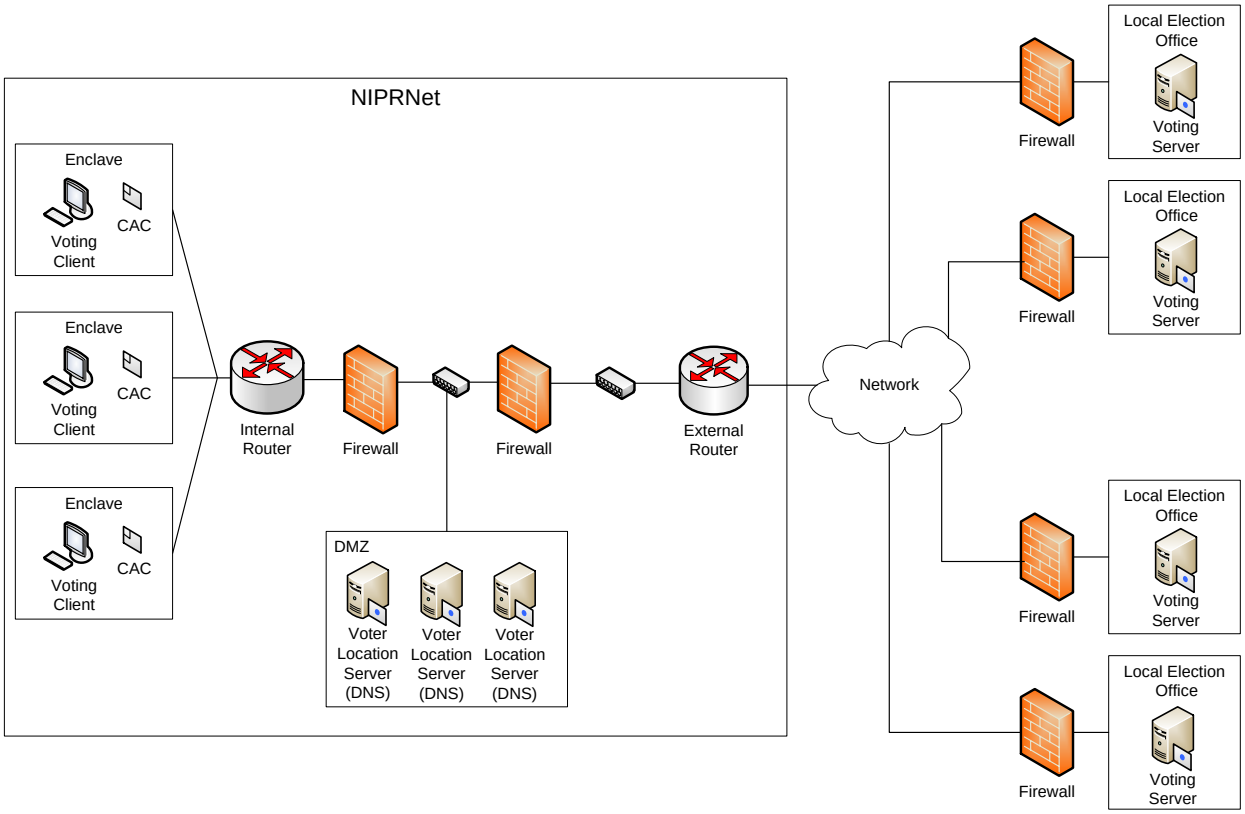

Figure 5: Pre-Decisional Baseline Conceptual Voting Framework

Network Discussion

In order for the eligibility of the potential voter to be established by the LEO, and in order for an eligible voter to cast a vote, an electronic connection must be established between the voter and the appropriate electoral jurisdiction. The Pre-Decisional Baseline Conceptual Voting Framework illustrates the NIPRNet being used to facilitate this connection for discussion purposes only - alternatives should be considered such as the Internet and dedicated private networks.

NIPRNet vs. Internet vs. Private Networks

As previously discussed in Section 2, the NIPRNet consists of a number of individual networks (enclaves) connected via a private backbone. These networks operate to a common set of strictly enforced rules and regulations, and public access is restricted[90].

The Internet is similar in nature and technical make-up to the NIPRNet; a number of smaller networks are connected via a backbone to create a much larger network[91]. The Internet is not as tightly managed or controlled as the NIPRNet and access is not restricted.

The NIPRNet is an example of a private network. A third option to consider is a dedicated, private network similar to the NIPRNet. This could be established and managed independently, either by the Government or an independent 3rd Party, to support the voting process exclusively.

Table 10 summarizes the key network parameters:

Parameter	**NIPRNet**	**Internet**	**Dedicated Private Network**
Network Type	Private	Public	Private
Managed (Controlled by)	DISA (DoD)	Multi-Stakeholder (ICANN, W3C, etc.)	Independent 3rd Party or Government
Configuration Standards	IA, STIG's, NSA Guidelines, NIST	Multiple (Organization dependent)	To be determined
Users	Restricted (Vetting required)	Anyone	Could be restricted (Authorization required)

[90] See "Sensitive But Unclassified IP Data", DISA, Retrieved from website: http://www.disa.mil/Services/Network-Services/Data/SBU-IP
[91] Kahn, R. E., & Cerf, V. G. (1999). What is the internet (and what makes it work). Retrieved from http://www.cnri.reston.va.us/what_is_internet.html

Network (Trust)	Trusted	Untrusted	Trusted
Access	Controlled (Location, Authentication, etc.)	Open	Could be controlled

Table 10: Network Distinctions

While the networks differ in terms of access and regulation, the computer equipment and individual sub-networks (enclaves) within them utilize similar, if not identical, components and technologies. These components and technologies may include:

- Access Control Models
- Authentication (one or more factors)
- Databases
- Encryption
- Firewalls
- Intrusion Detection Systems
- Load Balancers
- Operating systems (MS Windows, Unix, Linux, Apple, etc.)
- Peripherals (Smart Card Readers, Biometric Readers, etc.)
- PKI
- Protocols
- Proxies
- Routers
- Security Gateways
- Switches
- Virus Checkers
- Wireless Connectivity (802.11)

Having common components and technologies, the NIPRNet and other Dedicated Private Networks are susceptible to the same vulnerabilities and risks as the open Internet, but there are key distinctions that can be made because Dedicated Private Networks, the NIPRNet in particular, operate in a more controlled environment, particularly with regards to users and access. This is not to say that the NIPRNet does not have vulnerabilities; but by screening users, limiting access, certifying software applications, monitoring 'traffic' and enforcing strict rules and regulations per best

practice Information Assurance standards[92] [93], the exposure to vulnerabilities and/or security issues is reduced.

Standardization is critical within the network, in terms of the basic communication protocols (such as TCP/IP) and the security layers implemented for secure transmission of data (such as SSL, TLS, etc.) and/or the use of VPNs to allow servers to communicate seamlessly and securely with each other. An evolving challenge relates to the move from IPv4 to IPv6 on the Internet and other networks as a means to extend the addressing range. IPv6 is not backward-compatible with IPv4[94], but is the future direction for networks. A method for supporting both protocols in a voting platform will be necessary for a period of time as the transition continues. Networks that are strictly managed will have an advantage in this area. For example, systems that operate within the NIPRNet must be configured and certified as described in the STIG's and NSA Security Guidelines, as well as going through a formal connection process by requesting a connection as described in the DISA Connection Process Guide[95]. Although no specific timeframes for the certification process were documented, discussions with organizations that have been through the process indicate that it can be time-consuming, ranging from 6 months to over 1 year depending on the type of connection and certifications required. This is another consideration that must be taken into account when architecting a solution.

A summary of the key considerations for network infrastructure options, including potential advantages and disadvantages, is provided in Table 11.

Network Considerations		
NIPRNet	*Benefits / Advantages*	*Disadvantages / Gaps*
Security	• Managed and controlled environment	• Certification process can be long (anecdotally

[92] U.S. Department of Defense, (2007). *Information assurance (ia)* (8500.01E). Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf
[93] U.S. Department of Defense, (2003). *Information assurance (ia) implementation* (8500.2). Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf
[94] Kaushik , D. IPV6, (2008). IPv6 - *interoperability*. Retrieved from website: http://ipv6.com/articles/hardware/IPv6-Interoperability.htm
[95] U.S. Department of Defense, Defense Information Systems Agency. (2011). *Connection Process Guide* (v3.2). Retrieved from website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf

	• Enforced rules, regulations and policies for Information Assurance • All applications must be certified	6mths–1yr or longer) • NIPRNet connections typically have an expiration date – resulting in a cycle of connection request or reconnection request; this could potentially disrupt the voting process if connection scheduling is not adequately considered
Access	• No public access • Restricted to vetted, authorized users • Rules, regulations and requirements already established	• Potentially excludes some eligible overseas voters, such as those with CAC's but not authorized for NIPRNet access
Internet	*Benefits / Advantages*	*Disadvantages / Gaps*
Security	• None	• Open access – no vetting or restriction on users • No standardized Information Assurance practices • No certification of applications
Access	• Ubiquitous – available throughout the world with multiple means to connect	• None
Dedicated Private Network	*Benefits / Advantages*	*Disadvantages / Gaps*
Security	• Managed and controlled environment • Enforced rules, regulations and policies for Information Assurance	• Information Assurance rules, regulations and policies may not be government regulated/monitored/approved • Certification process undetermined
Access	• No public access • Restricted to authorized users	• Means of authorization/access have to be managed and distributed across the potential user base

Table 11: Network Considerations

Voter Authentication

The potential UOCAVA voter, the end-user, must be authenticated to enable access to the network and ultimately to the Local Election authority and electronic voting system.

For the NIPRNet, the CAC is an established, trusted identity credential within the US Government that allows voter access to the network (if authorized) and could provide the LEO with an elevated level of confidence in the identity of the voter due to the vetting process required prior to issuance. Accessing the NIPRNet with the CAC requires two-factor authentication (card & PIN), a best-practice for Information Assurance. The CAC can also support additional authentication factors if required and these are discussed in more detail in the following subsection. The DoD PKI infrastructure[96] over which the CAC operates is already deployed and proven.

The CAC can also provide additional functionality as required, such as encryption and digital signatures, either through the use of a pre-existing middleware API[97] or by the Voter application directly communicating with the card through standardized APDU commands. In the Baseline Conceptual Voting Framework presented for illustrative purposes at the start of this section, a CAC-authenticated login to the NIPRNet would be handled through an application running on the client operating system (or a web-based application) in conjunction with the existing DoD PKI (Certificate Authority, Revocation Server) infrastructure. For web-based login, an add-on or plug-in to the web-browser is used such as PKCS#11[98] or CryptoAPI[99].

Other end-user authentication methods and encryption/digital signature capabilities could be used with other Private Data Network systems or over the Internet. These include dedicated identity card/token PKI systems, soft-certificate PKI systems and non-PKI Knowledge Based Authentication (KBA) systems such as those used in the finance industry. Authentication methods have associated pros and cons and are often

[96] See Public Key Infrastructure and Public Key Enabling, Retrieved from Website: http://iase.disa.mil/pki-pke/
[97] See CAC Developer Support, Retrieved from Website: http://www.cac.mil/common-access-card/developer-resources/
[98] RSA Security Inc., (2009). *PKCS #11 v2.30: cryptographic token interface standard*. Retrieved from website: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf
[99] Microsoft CryptoAPI, (n. d.), Retrieved from website: http://msdn.microsoft.com/en-us/library/windows/desktop/aa380255%28v=vs.85%29.aspx

combined to provide greater assurity[100] [101]. As an example, passwords are easily to implement but are easily cracked and users tend to choose easy passwords such as "123456". Other popular authentication methods such as One-Time-Passwords (OTP) can provide a cost effective solution in certain environments and are more secure than just a regular password. By combining multiple authentication factors, risk can be reduced and single methods of authentication can become stronger when combined with an additional factor. Smart cards can be combined with biometrics to utilize three method of authentication thus providing three layers of protection and better overall security. There are many methods of authentication some are better than others but the selection of a specific technology needs to be based on the environment to protect.

A consideration with any 'token' based authentication method is that any issue with the token, be it a lost or stolen card, malfunctioning hardware or a revoked credential, will result in denied access to the system and the potential to vote. Similarly, a forgotten PIN may result in the token being 'blocked' by the system to prevent fraud and a recovery period to reset/re-establish the PIN[102]. This recovery period will be dependent on the location of the potential voter at the time of the error.

Any authentication method needs to establish trust, not only with the network for access purposes, but also with the local election authority as a trusted means of identification. The CAC is already established as a fully vetted, trusted identity credential by Federal Government agencies and can be used with non-NIPRNet applications. However, more research is required to determine if it will be a trusted form of identity for voting with all States, where voting eligibility and EVS access will be adjudicated.

Multifactor and Multilayer Authentication

In the example provided for discussion – the Baseline Conceptual Voting Framework – the CAC is used for authentication; providing access to the NIPRNet and to the State voter application. The CAC typically uses a two-factor authentication approach - "something you have" (the card) and "something you know" (the PIN number).

[100]Review, Duncan, R. Reading Room SANS, (2001). *Sans institute InfoSec reading room*. Retrieved from website: http://www.sans.org/reading_room/whitepapers/authentication/overview-authentication-methods-protocols_118
[101] RSA Security Inc, (2011). *The RSA authentication decision tree: select the best authentication solution for your business*. Retrieved from website: http://www.rsa.com/products/securid/whitepapers/9687_DECTRE_WP_0711.pdf
[102] See Military CAC, Retrieved from Website: http://militarycac.com/CAC.htm

For stronger authentication, the CAC and other token-based authentication can also support additional factors for authentication, typically through the addition of biometrics ("something you are"). The CAC architecture (see Appendix B – Common Access Card) includes biometric data containers for both fingerprint and facial images. Use of these would enhance the strength of authentication, but would incur costs through the client system requiring additional peripherals such as fingerprint readers to be used.

A layered approach to authentication increases the associated level of confidence and could be considered. This could include the addition of Knowledge Based Authentication ("what you know") or One-Time-Passwords, as currently used by financial institutions and credit bureaus.

Behavioral Biometric Characteristics[103] (BBC) is an emerging authentication method that uses biometric characteristics based on behavior, not personal information. BBC bases authentication verification on recognition of previously experienced stimuli and/or biometric data as the information is entered. This includes areas such as graphic object selections, keystroke dynamics and biometric signatures.

Key considerations for Voter Authentication options, including potential advantages and disadvantages, are summarized in Table 12:

Voter Authentication		
	Benefits / Advantages	*Disadvantages / Gaps*
CAC	• Existing credential with PKI infrastructure established • Fully vetted and trusted by the Federal Government for access to the NIPRNet and many other functions • Supports multi-factor authentication • Token based "something you have"	• May not yet be officially accepted by the States as a formal means of identity for voting • Malware introduced key loggers can capture PIN numbers utilized for authentication and signing • Any issues with the card potentially delay the voting process or

[103] Gamby, R. Vermont, Office of Chief Information Officer. (2010). *Alternatives to password-reset questions tackle social networking cons*. Retrieved from website: http://itsecurity.vermont.gov/Alternative_Passwords

	and PIN-based "something you know" security • Recurring face-to-face vetting is required on a periodic basis for re-issuing CAC – ongoing assurance of a positive and verified individual ID as opposed to a one-time 'static' process	prevent an individual from participating, for example: ○ Expired/revoked card ○ Lost card ○ Forgotten PIN ○ Failed hardware (card or reader) • Cards are reissued (and the associated digital certificates) on a periodic basis due to lost, malfunctioning, expiry, etc. This may happen during the request/ eligibility determination/ voting cycle as determined by local election rules and must be managed/ accounted for in the framework
Other Token-Based PKI authentication	• Token based "something you have" can be supplemented by PIN or other factor for additional security • Supports multi-factor authentication	• Status of trust – relating to vetting and issuance control would need to be established • Relatively high PKI infrastructure and maintenance costs[104] • Issues with the token potentially delay the voting process or prevent an individual from participating, including: ○ Expired/revoked ○ Lost ○ Failed hardware (token or reader)
Other Non-Hardware-Based PKI authentication	• Soft certificates eliminate potential issues with lost/malfunctioning	• Vetting requirements not as rigorous for the issuance of soft certificates – do not

[104] See Exploring authentication methods: How to develop secure systems, SearchSecurity, http://searchsecurity.techtarget.com/tutorial/Exploring-authentication-methods-How-to-develop-secure-systems

	tokens • Available from a wide number of commercial suppliers • Can be implemented with a second authentication factor (PIN)	typically require face-to-face interviews
Knowledge Based Authentication (KBA)	• Relatively low infrastructure and maintenance costs • Dynamic KBA more secure than Static KBA	• Dynamic KBA has developing concerns: ○ Privacy ○ Increasing availability of public records • Only provides single factor authentication ("something you know")

Table 12: Authentication Considerations

Voting Client

A Network Enclave is defined[105] [106]as a segment of a network that is defined by common security policies. An enclave is used in situations where the confidentiality, integrity and availability of resources differ from those of the general environment. It typically features limited access (not publicly accessible) through the use of firewalls, VPN's, etc.

Within the context of the NIPRNet, a Network Enclave maintains a similar definition[107] as a segment of the network that is defined by common security policies and is not publicly accessible. NIPRNet Network Enclaves are typically made up of multiple computers and systems but can consist of only a single system.

Establishing Voting Client(s) within Enclaves on the Network allow the definition and enforcement of the required security policies, rules and regulations and access control.

[105] *Where trust is key*. (2009, August 13). Retrieved from website: http://trustcc.wordpress.com/2009/08/13/network-enclaves-–-enhanced-internal-network-segmentation/
[106] *Department of Defense* (2003) Instruction 8500.2, E2.1.17.2,
[107] *Department of Defense, DISA* (2011) Connection Process Guide v3.2, p2-1, Retrieved from Website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf

In the Baseline Conceptual Voting Framework, this was illustrated as an Enclave on the NIPRNet with the CAC being used for authentication. A similar architecture could be implemented on any network.

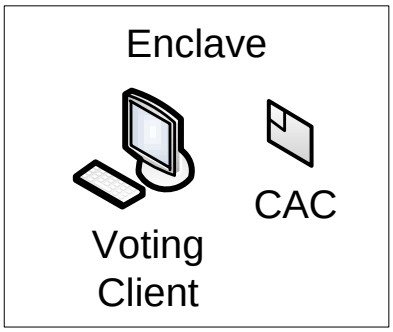

Figure 6: Illustrative Network Enclave with Voting Client(s)

One advantage of implementing the Enclave within the NIPRNet is the established access control, monitoring and isolation the NIPRNet provides. This helps reduce the opportunity for exposure to attacks and vulnerabilities without having to establish and prove new security measures within another network. In addition, for operation on the NIPRNet, software must be certified per the DISA Connection Process Guide[107]. Consideration can be given to creating a specific STIG for the Voting Client Enclave to ensure the proper configuration and management.

The physical environment where the Voting Client resides can also impact security and trust. Unrestricted access to a Voting Client elevates the opportunity for malicious activity when compared to restricted access, such as that provided if the Client is located on a Military base where physical access is strictly controlled and reduces the number of individuals who could gain access to the system.

In order to further limit the potential for malware and malicious code being introduced on the Voting Client, consideration should be given the Client operating under a specialized, limited Operating System (OS) such as the Lightweight Portable Security (LPS) product discussed previously. This type of OS is booted from a read-only medium such as a CD-R/DVD-R and can be configured to limit the availability of the typical functions (writes, ports, services, protocols and applications) used to carry out

malicious exploits.[108] [109] It can also be restricted to only allow access to the voting application and no other. This can be achieved by having the OS boot into a standardized web browser (such as Microsoft Internet Explorer, Mozilla Firefox, etc.) configured in "Kiosk Mode" [110] to limit the user's ability to navigate outside a limited network destination range (a white list) or to access/run other applications. This prevents a malicious (or uninformed) insider from navigating to harmful sites. The OS and Voting Client application may also be configured for a limited 'write' capability to the hard drive; only allowing recording of a date/time stamp of the voting transaction for audit purposes. A 'clean boot' of the OS between each voting session could further minimize the opportunity for malicious exploits.

Under ideal circumstances, the Voting Client would be dedicated to the voting process only, even if just for the voting period – this would limit the opportunity for malicious exploits to be introduced by eliminating activity on potentially non-secure sites.

[108] Gibson, Darril (2011) *CompTIA Security+,* pp223-226, http://www.ebay.com/ctg/CompTIA-Security-Get-Certified-Get-Ahead-SY0-301-Study-Guide-Darril-Gibson-2011-Paperback-/111415005
[109] Techterms, Hardening (computing), (n. d.), http://www.techterms.com/definition/systemhardening
[110] See, Web Browser "Kiosk Mode", Retrieved from Websites: http://support.microsoft.com/kb/154780, https://addons.mozilla.org/en-us/firefox/addon/r-kiosk/, http://think2loud.com/868-google-chrome-full-screen-kiosk-mode/, http://www.opera.com/support/mastering/kiosk/,

Key considerations for the Voting Client are summarized in Table 13:

Voting Client Considerations		
Item	**Benefits / Advantages**	**Disadvantages / Gaps**
Enclave	• Provides a consistent and managed set of rules and regulation for security and operation • Use of digital certificates can assure end-to-end authentication of the client and the Election system	• Time and cost associated with approvals/certifications and management • Established process, rules and enforcement with the NIPRNet; not necessarily established with other networks. • Cost associated with the management and distribution of digital certificates
Bootable OS	• Bootable OS from read-only media limits exposure to exploits • Implementable on a wide range of hardware platforms to support a broad range of voter environments	• Management and costs associated with distribution of media • Custom configuration requirements to meet voting application specifics • Hardware/media failure delays the voting process or prevents an individual from participating[111]

Table 13: Voting Client Considerations

Electronic Voting Systems and Voting Location Servers

Local Election Officials in each State are responsible for determining eligibility to vote and for providing Electronic Voting Systems according to State-specific regulations. The voting rules and voting systems are not standardized from State to State. Each State (and potentially voting precincts within the State) can use equipment from different vendors and with different capabilities, as long as the equipment meets the minimum requirements set forth by the State and Federal regulations.

[111] Mcmillan, R. (2012, August 30). Your pc just crashed? don't blame Microsoft. *Wired Magazine*, Retrieved from http://www.wired.com/wiredenterprise/2012/08/your-pc-just-crashed-dont-blame-microsoft/

Voting Location Servers

Regardless of the Network being used or the Voting Client configuration, a secure connection needs to be established from the Voting Client to the appropriate State voting location. To provision this, the Baseline Conceptual Voting Framework illustrated a number of Voting Location Servers (virtual or physical) that act similarly to DNS servers found on the internet. These servers would map the voter request in the Voting Application through to the appropriate State location, establishing and maintaining a secure communication channel for the online session.

The Baseline Conceptual Voting Framework illustrated the application of these within the NIPRNet, but the principles apply to other network configurations.

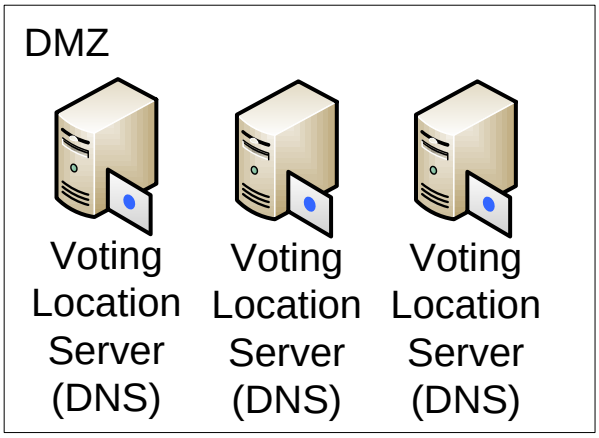

Figure 7: Voting Location Servers

Specifically for the NIPRNet, implementing the Location Servers within the DMZ could help maintain a high level of trust in the system. They could also be implemented externally, although consideration would need to be given to how this might impact the established trust level with the States. There are commercial organizations (e.g. OpenDNS[112]) that provide this type of secure DNS service.

Since the Voting Location Servers are responsible for ensuring the NIPRNet Voting Client (end-user) reaches and connects to the appropriate voting State precinct web-server, it is essential a level of trust is established to ensure neither the Voting Location

[112] See Open DNS, Retrieved from Website: http://www.opendns.com/

Server nor the State precinct web-server are being 'spoofed'. This can be achieved through the use of digital certificates. The issuing/managing authorities for these certificates would depend on the location of the systems. Certificates for the State web servers/Voting systems could be issued/managed by each State. If Voting Location Servers are implemented within the NIPRNet DMZ, those certificates could be issued/managed under DoD PKI. The Federal PKI Bridge[113] would allow for cross-certification of certificates in this scenario.

Electronic Voting Systems

Section 3 of this report provides details on Electronic Voting Systems. Remote e-Voting systems function over a network such as the Internet or a Dedicated Private Network utilizing standard industry based technologies such as client OS's, web browsers, encryption, biometrics, PKI and others. With regard to the feasibility assessment, the key considerations surround the communication protocols and standards used by the EVS systems.

Standards in electronic voting are emerging and being adopted (such as OASIS EML[114] [115]) for information display and communication. However, due to the slow commercial adoption and continuing evolution of these standards, consideration needs to be given in any framework development to the different standards employed by the EVS and their potential impact e.g. the current migration from IPv4 to IPv6 in many networks creates communications challenges that need to be addressed. In addition, items such as digital signature standards, key lengths for encryption, etc. have not yet been fully standardized for a voting process.

Initially, until standards are complete and ubiquitously adopted, any conflicts must be addressed on an individual basis. Consideration can be given to reducing or eliminating the number of conflicts through the use of very specific electronic voting framework

[113] See Appendix X, http://iase.disa.mil/pki-pke/interoperability/index.html , http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/index.html, http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-welcome-page

[114] OASIS, (2008). *Election mark-up language*. Retrieved from website: https://www.oasis-open.org/committees/download.php/30366/EML-Top-Reasons.pdf

[115] See OASIS Election and Voter Services Technical Committee, Retrieved from Website: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election

rules and regulations. These could be defined under the NIPRNet using specific voting STIGs.

Key considerations for Electronic Voting Systems and Voting Location Servers are summarized in Table 14:

Electronic Voting System Considerations		
Item	**Benefits / Advantages**	**Disadvantages / Gaps**
Electronic Voting Systems – lack of standardization	• Each State (and/or local jurisdiction) is free to select the certified voting system that best meets their requirements. • Having multiple vendors/system types creates a heterogeneous environment that reduces the possibility of a single voting system exploit compromising all systems.	• Challenges with different communication protocols • Challenges with different digital signature and encryption standards • Challenges with enforcing a common standards for EVS on States with regard to the UOCAVA voting process
Voting Location Servers	• Allows user-agnostic mapping of voter requests to appropriate State locations	• Must establish and maintain trust with the States • Certification and maintenance would be essential although time-consuming and with associated cost

Table 14: Electronic Voting System Considerations

Security Considerations

The security, integrity and privacy of the voting process are of paramount concern. UOCAVA voters must be provided a secure, private and reliable environment within which to participate in the election process and the Local Election authorities must be able to trust the identity of the voter.

The CIA principle[116]

An accepted and widely-applied principle for secure information systems is C.I.A. – Confidentiality, Integrity and Availability. Attempts to compromise any one of these three core factors can result in serious consequences such as loss of privacy, data corruption or manipulation and the inability to access a voting system, for the parties concerned.

Confidentiality

Confidentiality relates to preventing unauthorized access to data within the system – particularly important in maintaining the privacy of the voting process. Data is vulnerable to intercept both at rest within the system and in transit between systems. Guidance is available from a number of sources on protecting the confidentiality and privacy of information[117], including the use of robust access controls help maintain confidentiality for data at rest. Encryption methods help maintain confidentiality of information both in transit and at rest (even if the system is subject to unauthorized access).

Integrity

Integrity relates to ensuring that the data within the system is accurate and remains unchanged, an important factor in any data system but critical to a voting system. As with Confidentiality, data is under threat both in motion and at rest and similarly robust access controls, encryption and digital signature techniques can be used to help maintain integrity.

Availability

Availability relates to ensuring the system is readily accessible to authorized users when required. For a voting system, this is important to both the voter casting a vote and to the election official. Many security attacks focus on denying access to a system to authorized users. Techniques such as Network Behavior Analysis (NBA)

[116] Security Analysis, See website http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm
[117] McCalisster, E., Grance, T., & Scarfone, K. U.S. Department of Commerce, National Institute of Standards and Technology. (2012). *Guide to protecting the confidentiality of personally identifiable information (pii)*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

can be used to examine network traffic to identify threats such as Distributed Denial of Service attacks, scanning, and other forms of malware[118].

Additional security considerations for a framework used for electronic voting are accountability, non-repudiation and legality.

[118] U.S. Department of Commerce, National Institute of Standards and Technology. (2012) *Special publication 800-94, guide to intrusion detection and prevention,* Retrieved from website: http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

7. Risks and Mitigations

In performing the research behind this report, a number of risks have been identified with respect to utilizing the NIPRNet as a conduit to support Uniformed and Overseas Citizens Absentee Voting (UOCAVA) voters in the voting process, and in using the Common Access Card (CAC) for authentication. These are broken into a number of key areas and summarized in the table below.

Where possible or applicable, a potential mitigation is provided for consideration to address each risk.

Item	Area	Risk	Mitigation
1	NIPRNet	Voter does not have access to the NIPRNet preventing access to the voting application	The system should only be used to supplement – not replace – existing methodologies that allow UOCAVA voters to vote. In the event that the NIPRNet is not available, or access is denied, the voter can use existing methodologies instead
2	NIPRNet	Costs to implement, certify, manage and maintain the framework on the NIPRNet are burdensome	N/A
3	CAC	Voter does not have a CAC that provides access to the NIPRNet	The system should only be used to supplement – not replace – existing methodologies that allow UOCAVA voters to vote. In the event that the voter does not have a CAC that provides access to the NIPRNet, the voter can use existing methodologies instead
4	CAC	The voter's CAC is lost, stolen, expired or otherwise non-functional (e.g. high turnover rates in CAC replacement cards)	The system should only be used to supplement – not replace – existing methodologies that allow UOCAVA voters to vote. In the event that the voter does not have a CAC that provides access to the NIPRNet, the

			voter can use existing methodologies instead
5	CAC	Cards are reissued (and the associated digital certificates) on a periodic basis due to lost, malfunctioning, expiry, etc. This may happen during the request/ eligibility determination/ voting cycle as determined by local election rules.	Framework must allow for the management of re-issued digital certificates during the voting cycle.
6	Client	A hardware or software failure prevents access to the voting application and/or the NIPRNet	The system should only be used to supplement – not replace – existing methodologies that allow UOCAVA voters to vote. In the event that the voter does not have a CAC that provides access to the NIPRNet, the voter can use existing methodologies instead
7	Client	Distribution of bootable OS media is disrupted	The system should only be used to supplement – not replace – existing methodologies that allow UOCAVA voters to vote
8	EVS	Lack of standardization of communication and signature protocols	DoD define standard.
9	EVS/Voting Location Servers	State does not have a PKI system cross-managed with the Federal Bridge	States to implement PKI and get cross certified with Federal Bridge.
10	Security	The framework is subject to hacking attempts	1. Strictly managed and maintained security of the network 2. Bootable OS limits the opportunity for malware or other exploits to be insinuated into the voting system
11	Security	The framework is subjected to a DDOS attack not allowing it to be used for voting	Strictly managed and maintained security of the network
12	Security	A stolen CAC is used to gain access to the voting system or a CAC is spoofed	Use multi-factor authentication beyond just CAC and PIN

Table 15: Framework Risk Summary

8. Conclusions and Recommendations

The primary objective of this study was to evaluate the feasibility of using DISN and the CAC to support UOCAVA voters in the voting process. From that perspective, the primary conclusions reached are:

(1) The DoD can support UOCAVA voters in an electronic voting process using the NIPRNet with DISN to provide an existing, managed and monitored environment for communication with the LEO (including casting a ballot), and

(2) CAC's are a trusted, vetted readily available means to assert positive identification and authentication of a potential voter for the LEO, allowing the LEO to proceed with the voter eligibility determination/voting process with an elevated level of confidence in the identity of the voter.

It should be fully understood that at no point in this evaluation is it assumed that the DoD is providing anything more than an assertion of identity to State election officials. The determination of eligibility and the provision of the opportunity to vote remains entirely under the control of the LEO in the state/jurisdiction that the voter is registered to vote in.

By using the NIPRNet to enable the electronic voting process for UOCAVA voters, the ability for hacking, spoofing and other forms of fraudulent online activity is limited due to the enforced management controls, certification requirements and regulations enforced by DISA. Other networks can be used to provide a similar environment, such as the Internet or another dedicated Private Network, but the NIPRNet is an existing resource that is already trusted within the DoD.

Using the NIPRNet at the client end of the voting 'transaction' eliminates the use of public networks, particularly on foreign soil. While it is possible to securely transmit information over public networks, the opportunities for interception and interference with the data are inherently greater in an open, unmonitored network environment. Using the NIPRNet to host the client computer workstation limits the potential exposure to

malicious interference due to the established access controls, management and monitoring.

If the NIPRNet is used to support the client environment, specific Security Technical Implementation Guide(s) (STIGs) can be developed under the existing DISA guidelines[119]. The STIGs would define the installation, configuration and maintenance of hardware and software for the voting-specific application. STIGs typically include recommended administrative processes and lifecycle policies and procedures to be developed / managed in addition to the baseline NIPRNet security policies. The STIGs can be coordinated with all stakeholders in the voting process, including election officials, to ensure meeting federal as well as State-specific requirements.

The CAC is a vetted, trusted identity credential already in use to gain access to the NIPRNet and other applications/environments. It provides a benefit over other PKI/authentication systems for the voting application in that it is already established, deployed, understood and supported as an authentication credential within DoD. A 2-factor authentication process is presently used to gain access to the NIPRNet (the physical card and the PIN number) and this may be augmented to provide 3-factor authentication if/as desired. The CAC utilizes established middleware to provide support for digital signatures that could be used in the voting process. Further consideration would need to be given to establishing the CAC as a trusted, accepted identity credential for voting with each of the States - however, there is no identified alternative authentication system that would not be subject to the same process.

To help limit the exposure to risks associated with exploits from a constantly changing electronic environment (both hardware and software related) consideration can be given to creating a 'clean' client environment for voting through the use of a "clean boot" capability at the client workstation as discussed in Section 5. An example is provided of the family of Lightweight Portable Security (LPS)[120] system products that help prevent work activity or malware to be written to the local computer resources, and limits the

[119] U.S. Department of Defense, DISA. (2011). *Network services directorate (ns) enterprise connection division (nsc) connection process guide (v.3.2)*. Retrieved from website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf

[120] See Lightweight Portable Security, Retrieved from websitehttp://spi.dod.mil/lipose.htm

client exposure to potential threats by not making available the ports, services, protocols and applications necessary to carry out specific exploits. The LPS or similar boot system can also be engineered to boot into a standard web browser configured to only allow access to the web-based voting application that directs the user to the appropriate LEO destination. This eliminates potential exposure to threats associated with deliberate or accidental navigation to untrustworthy websites.

To further reduce exposure to exploits from malware, either accidental or intentional, consideration can be given to dedicating a workstation to the voting process only. While a clean boot capability will reduce exposure, particularly if a boot is performed between each voting session, it is still feasible that a sophisticated threat could circumvent the protection this provides. Dedicating a workstation to the voting process, even if just for the voting period, will provide additional risk mitigation by restricting access of the client to potentially hazardous sites. This limits the ability of an insider to add new software or hardware to the workstation and allows a clean baseline to start with. The workstation can then be easily checked between usages or daily for variations in configuration as well as any changes to existing software they may reside on the machine; through the use of cryptographically signed software.

If considering security/integrity considerations only in developing an e-voting framework, locating the Electronic Voting Systems within the managed NIPRNet network environment (in the NIPRNet DMZ for example) could also help reduce exposure to malicious exploits. However, as discussed in Section 3, a number of significant obstacles exist with this approach, including the maintenance and management of the vast number of unique configurations and options that would be required by each state along with the additional certification/maintenance requirements needed for inclusion in DISN. The associated costs and logistics could become prohibitively expensive to manage and maintain, this is due to a variety of reasons including but not limited to each state having different ballots, states having their own requirements for voting system certification, and additional software for formatting voting data to provide for state tabulation. Alternatively, consideration can be given to maintaining the Electronic Voting Systems with the State and Local authorities, not within the DISN, and that

instead a secure communications channel only is established / supported between the LEO and the UOCAVA voter through the NIPRNet.

If a DNS-like 'switch' is required in the framework, similar to that depicted as the Voting Location Server in the Baseline Conceptual Voting Framework, establishing that within the NIPRNet DMZ could be considered to benefit from the more secure and controlled environment. Any decision in this regard would also have to include consideration of the associated certification, maintenance and management costs. Digital certificates at both the switch and the LEO system(s) could be used to prevent spoofing and establish a secure communication channel.

For future consideration, it is noted that if the NIPRNet and CAC are used as part of an electronic voting framework, only CAC holders with authorized access to the NIPRNet will have the ability to use the framework to vote. This framework would not be readily extensible to a larger overseas voting population either not eligible for CAC's or for NIPRNet access. Wider issuance of CAC's is being considered, such as to family members and dependents, but this does not include access to the NIPRNet.

Recommended Additional Research

1. What is required to have the CAC accepted as a trusted (and legal) means of identification at the State level?
2. What is the timeframe required to complete the certification/approval processes necessary for software applications and connectivity to the NIPRNet?

Appendix A – Abbreviations and Acronyms

Acronym	Description
AAA	Authentication, Authorization and Accounting
ACR	Access Control Rights
AFNIC	Air Force Network Integration Center
APDU	Application Protocol Data Units
API	Application Programming Interface
APL	Approved Products List
ATD	Authorization Termination Date
BBC	Behavioral Biometric Characteristics
CAC	Common Access Card
CAO	Connection Approval Office
COTS	Commercial-Off-The Shelf
CPG	Connection Process Guide
DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DIACAP	DoD Information Assurance Certification and Accreditation Process
DMZ	Demilitarized Zone
DoDI	Department of Defense Instruction
DSAWG	Defense IA/Security Accreditation Working Group
EAC	Election Assistance Commission
EDIPI	Electronic data interchange personal identifier
EML	Election Markup Language
EVS	Electronic Voting Systems
FBCA	Federal Bridge Certificate Authority
FIPS	Federal Information Processing Standard
FVAP	Federal Voting Assistance Program
GIG	Global Information Grid
GSC-IS	Government Smart Card Interoperability Specification
HAVA	Help America Vote Act of 2002
HBSS	Host Based Security System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
JPAS	Joint Personnel Adjudication System
KBA	Knowledge Based Authentication

LEO	Local Election Official
LPS	Lightweight Portable Security
MOVE	Military and Overseas Voting Empowerment Act of 2009
NACLC	National Agency Check with Local Agency Check and Credit Check
NACI	National Agency Check with Written Inquiries
NAT	Network Address Translation
NBA	Network Behavior Analysis
NGSCB	Next-Generation Secure Computing Base
NIPRNet	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
NSTIC	National Strategy for Trusted Identities in Cyberspace
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RAPIDS	Real-Time Automated Personnel Identification System
SCAP	Security Content Automation Protocol
SPI	Software Protection Initiative
STIG	Security Technical Implementation Guides
TCG	Trusted Computing Group
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSA	Transportation Security Administration
UEFI	Unified Extensible Firmware Interface
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act
VM	Virtual Machine
VPN	Virtual Private Network
VVSG	Voluntary Voting System Guidelines
W3C	World Wide Web Consortium

Table 16: Abbreviations and Acronyms

Appendix B – Common Access Card

Internal architecture of CACv2 combined with PIV to create the next generation CAC.

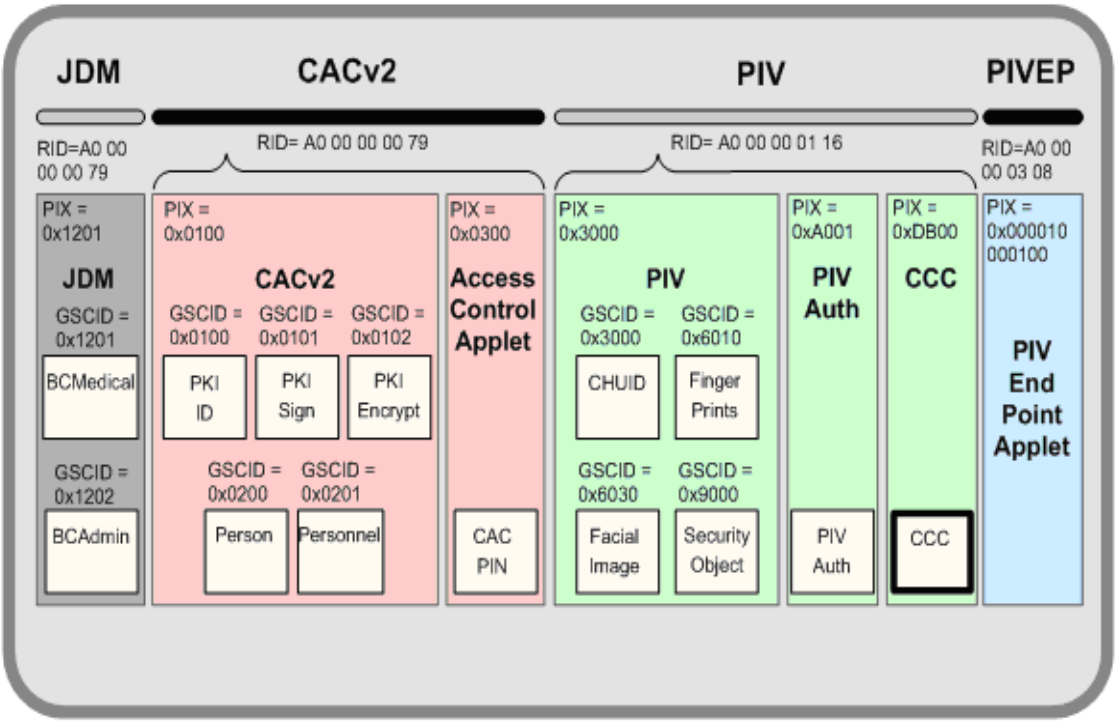

Figure 8: CAC Data Architecture

CAC (Containers) and their internal data elements, the highlighted areas are data elements for consideration in the voting process; privacy must be a consideration with any of these.

Category	Alias	Data Element	Element Definition
ID	First Name	Person Forename Text	The text of a person forename.
ID	Gender	Sex Category Code	The code that represents a sex category.
ID	Person Designator	Person Designator Type Code	The code that represents a specific kind of person designator.
ID	Last Name	Person Surname Text	The text of a person surname.
ID	Middle Name	Person Middle Name Text	The text of a person middle name.

ID	Social Security Number	Person Designator Identifier	The identifier that represents a person designator. (Being replaced with DoD Identification Number. June 1, 2011)
ID	Suffix	Person Cadency Name Text	The text of a person cadency name.
ID	Person Identifier	DoD Electronic Data Interchange (EDI) Person Identifier	The identifier that represents a person within the Department of Defense Electronic Data Interchange.
ID	Blood Type	Blood Type Code	The code that represents a person's blood type
ID	Organ Donor	Organ Donation Agreement Indicator Code	The code that indicates whether a person has agreed to donate their internal organs after death.
Benefits	Date of Birth	Person Birth Calendar Date	The calendar date when a person was born.
Benefits	Contractor Code	DoD Contractor Function Code	A code that indicates the type of work a DoD contractor does or agency they work for.
Benefits	Entitlement Condition	Personnel Entitlement Condition Type Code	The code that represents the type of condition that occurred while a sponsor was in a personnel category and organization that affects the entitlements of the sponsor and/or the sponsor's dependents.
Org	Branch	Uniformed Service Branch Classification Code	The code that represents a Uniformed Service branch classification.
Org	Personnel Category	Personnel Category Code	The code that represents how the DoD personnel and/or finance center views the sponsor based on accountability and reporting strengths.
Org	Government Agency	US Government Agency/Sub agency Code	The code that indicates the government agency a "Non-DoD civil services employee, except Presidential appointee", works for.
Org	Non-Government Agency	US Non-Government Agency Code	The code that indicates the non-government agency a "Non-government agency personnel" works for.
Org	Pay Category	Pay Plan Code	The code that represents a category or a schedule for monetary compensation.
Org	Pay Grade	Pay Plan Grade Code	The code that represents a pay category or schedule for monetary compensation.
Org	Rank	Uniformed Service Rank Short Name	The abbreviated name of a Uniformed Service rank.
CM	Date Demographic Data was Loaded on Chip	CAC Demographic Data Update Calendar Date	The date when the last update was made to the demographic data; is independent of benefit dates.
CM	Date Demographic Data on Chip Expires	CAC Demographic Data Expiration Calendar Date	The date when demographic data is expected to expire; is independent of benefit dates.

CM	Card Security Code	Card Instance Identifier	The identifier used to uniquely identify each card issued to a person
CM	Card Issue Date	Identification Card Issue Calendar Date	The date when the person's current or former ID card was issued.
CM	Card Expiration Date	Identification Card Expiration Calendar Date	The date when the person's current ID card is expected to expire.
PKI	Identity Certificate	DoD PKI Authentication Certificate Data	The data contained in a person's authentication certificate used for the DoD private key infrastructure.
PKI	Signature E-Mail Certificate	S/MIME Certificate Signature Data	The data contained in a person's public signature key for the secure multipurpose Internet mail extension certificate.
PKI	Encryption E-Mail Certificate	S/MIME Certificate Encryption Data	The data contained in a person's public encryption key for the secure multipurpose Internet mail extension certificate.
PKI	PIV Auth Certificate	Federal PIV Authentication Certificate	The data contained in a PIV Auth Cert
CM	CCC (Card Capability Container)	Card Capability Container	For discovery of Object ID and App ID discovery
ID	Fingerprint Biometric	Fingerprint captures from RAPIDS	N/A
ID	Facial Image biometric	JPEG 2000 Facial Image	N/A
ID	CHUID	Card Holder Unique Identifier	N/A
CM	Security Object		
ID	Personnel Entitlement condition begin date	Personnel Entitlement condition Begin Date	N/A
ID	Personnel Entitlement condition end date	Personnel Entitlement condition End Date	N/a

Table 17: CAC Data Elements

Appendix C – LPS Light Weight Portable Security

Screen shot showing the LPS bootable operating system environment.

Figure 9: LPS Operating System Environment

Lightweight Portable Security (LPS) creates a secure end node from trusted media on almost any Intel-based computer (PC or Mac). LPS boots a thin Linux operating system from a CD or USB flash stick without mounting a local hard drive. Administrator privileges are not required; nothing is installed. The LPS family was created to address particular use cases: LPS-Public is a safer, general-purpose solution for using web-based applications. The accredited LPS-Remote Access is only for accessing your organization's private network.

.LPS-Public allows general web browsing and connecting to remote networks. It includes a smart card-enabled Firefox browser supporting CAC and PIV cards, a PDF and text viewer, Java, and Encryption Wizard - Public. LPS-Public turns an untrusted system (such as a home computer) into a trusted network client. No trace of work activity (or malware) can be written to the local computer. Simply plug in your USB smart card reader to access CAC- and PIV-restricted US government websites.

LPS differs from traditional operating systems in that it isn't continually patched. LPS is designed to run from read-only media and without any persistent storage. Any malware that might infect a computer can only run within that session. A user can improve security by rebooting between sessions, or when about to undertake a sensitive transaction. For example, boot LPS immediately before performing any online banking transactions. LPS should also be rebooted immediately after visiting any risky web sites, or when the user has reason to suspect malware might have been loaded. In any event, rebooting when idle is an effective strategy to ensure a clean computing session. LPS is updated on a regular basis (at least quarterly patch and maintenance releases). Update to the latest versions to have the latest protection.[121]

[121] U.S Department of Defense (2012) *Light weight portable security*: Retrieved from website: http://spi.dod.mil/lipose.htm

Appendix D – DoD PKI External Interoperability Landscape

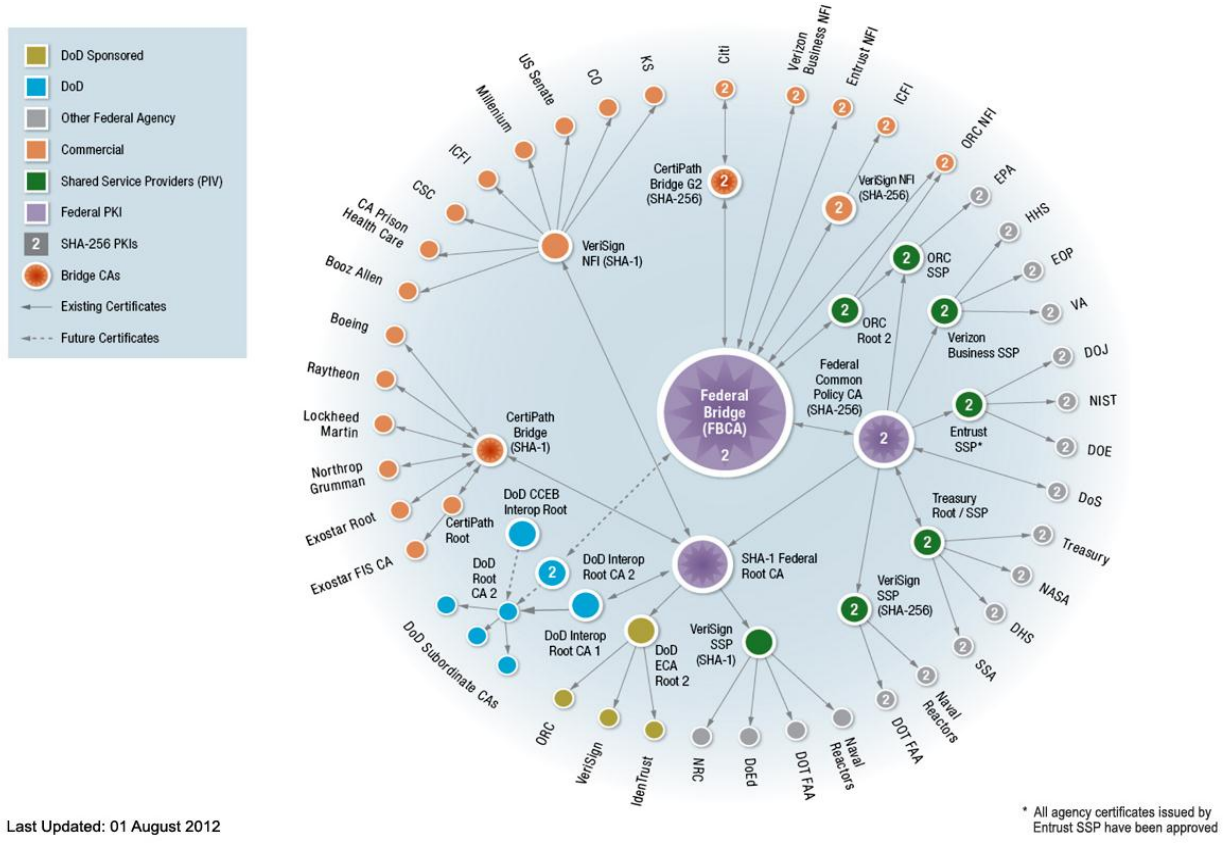

Figure 10: DoD PKI External Interoperability Landscape[122]

[122] U.S Department of Defense (2012) *The DoD PKI external Interoperability landscape*. Retrieved from website: http://iase.disa.mil/pki-pke/interoperability/fed_crosscert.html

Appendix E – Source References

Department of Defense, (2006). *DoD Implementation Guide for CAC Next Generation* (ng). Retrieved from website: http://www.idmanagement.gov/iab/documents/CACngImplementationGuide.pdf

Information assurance support environment. (2012, August 24). Retrieved from http://iase.disa.mil/

Department of Defense, (2008). *DoD Information Assurance Certification and Accreditation Process Handbook*. (Vol. 1.0).

Information assurance workforce improvement program (8570.01-M). Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

Department of Defense, (2008). •*DoD Implementation Guide For CAC Piv End-Point, version 1.22.* Retrieved from website: http://www.cac.mil/docs/ref 1.c.i-CAC_End-Point_Implementation_Guide_v1 22.pdf

"*Beyond Flash Value", A User's Quick Guide To Using The CAC (2003).* Retrieved from website: http://www.cnic.navy.mil/navycni/groups/public/@hq/@cacpmo/documents/document/cnicd_a064701.pdf

Department of Defense, (2006). •*DoD Implementation Guide for Transitional Piv ii SP 800-73 v1, version 1.01*. Retrieved from website: https://www.dmdc.osd.mil/smartcard/docs/DoD PIV Transitional Implementation Guide.pdf

Department of Defense, (2006). •*DoD CAC Middleware Requirements Release 3.0, version 1.0.* Retrieved from website: http://www.idmanagement.gov/iab/documents/DoDcacMiddlewareRequirements.pdf

Department of Defense, (2011). •*Department of Defense Instruction, ID Cards for Members of Uniformed Services, Their Dependents, and Other Eligible Individuals*. Retrieved from website: http://usmilitary.about.com/od/publicationsregulations/p/i100013.htm

(2011). •*x.509 certificate policy for the u.s. federal pki common policy framework, version 3647-*

1.17. Retrieved from website: http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf

(2011). *•x.509 certificate policy for the fbca, version 2.25*. Retrieved from website: http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

(2005). *•systems & software technology conference: Ports, protocols, and service management process for the department of defense*. Retrieved from website: http://www.mitre.org/work/tech_papers/tech_papers_05/04_1281/04_1281.pdf

(2012). *•chairman of the joint chiefs of staff instruction, defense information systems network responsibilities*. Retrieved from website: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf

(2010). *•department of defense, approval of external public infrastructures, july 22, 2008 department of defense, external interoperability plan, version 1.0,* . Retrieved from website: http://jitc.fhu.disa.mil/pki/documents/dod_external_interoperability_plan_aug_2010.pdf

(2010). *Dod public key infrastructure (pki) partner pki interoperability test plan, version 2.0*. Retrieved from website: http://jitc.fhu.disa.mil/pki/documents/DoD_PKI_Interoperability_Test_Plan_v2_0_15Nov10.pdf

(2009). *•deputy assistant secretary of defense for cyber, identity, and information assurance strategy*. Retrieved from website: http://dodcio.defense.gov/Portals/0/Documents/DoD_IA_Strategic_Plan.pdf

(2003). *Department of defense instruction, information assurance (ia) implementation, number 8500.2*. Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

(2011). *•department of defense instruction, public key infrastructure and public key enabling*. Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf

(n.d.). *•dod programs, public key infrastructure (pki) increment 2*. Retrieved from website: www.dote.osd.mil/pub/reports/FY2011/pdf/dod/2011pki.pdf

(2011). *Connection process guide, version 3.2*. Retrieved from website: http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Library/disn_cap_04272011.pdf

DISA, (2012). *Connection process guide, version 4.0*. Retrieved from website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/DISN-Connect/Library/cpg_june2012.pdf

DISA, (2011). *Fiscal year 2012 budget estimates*. Retrieved from website: http://comptroller.defense.gov/defbudget/fy2012/budget_justification/pdfs/02_Procurement/DISA_PB12_PDW_Final.pdf

DISA, (2012). *Network services: Private internet protocol (ip) service, establish a virtual private network (VPN) customer ordering guide, version 1.0*. Retrieved from website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/Network-Services/Private IP/EstablishVPNCustomerOrderingGuidev10.pdf

DISA, (2009). *The changing nature of data center security*. Retrieved from website: http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/Network-Services/Private IP/EstablishVPNCustomerOrderingGuidev10.pdf

(2011). *•GIG 3.0 design factors, an architecture proposal for aligning netops to the operational chain of command*. Retrieved from website: http://www.afceahawaii.org/docs/gig3_0_2011.pdf

DISA, (2007). *Network infrastructure, security technical implementation guide, version 7, release 1*. Retrieved from website: http://www.sentekglobal.com/solutions/downloads/Network STIG.pdf

(2006). *•federal information processing standards publication, minimum security requirements for federal information and information systems*. Retrieved from website: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

ATSPI Technology Branch, (2011). *Software protection initiative, lightweight portable security*. Retrieved from website: http://spi.dod.mil/lipose.htm

ATSPI Technology Branch, (2012). *Lightweight portable security (lps) product family*. Retrieved from website: http://pdf.101com.com/GCN/2010/GCN_101018DSD.pdf

Department of Defense Washington Headquarters Services Federal Voting Assistance Program, (2011). *Voting over the internet pilot project assessment report*. Retrieved from website: http://www.fas.org/sgp/crs/misc/RS20764.pdf

SERVE, (2004). *A security analysis of the secure*. Retrieved from website: http://www.servesecurityreport.org/paper.pdf

Jarzombek, J. (2011, March). *Building in security as a requisite enabler for highly reliable, safety-critical software-intensive systems*. Software assurance. Retrieved from http://www.omg.org/news/meetings/tc/agendas/va/SysA_pdf/Jarzombek.pdf

Defense Information Systems Agency, (2012). Retrieved from website: http://www.disa.mil

Department of Defense, (1983). *Department of defense privacy program,"*. Retrieved from website: http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf

NIST, (2003). *Government smart card interoperability specification* (Interagency Report 6887). Retrieved from website: http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

FVAP, (2011). *2010 post-election survey report to congress*. Retrieved from website: http://www.fvap.gov/resources/media/2010report.pdf

FVAP, (2010). *Strategic plan for fiscal years 2010-2017*. Retrieved from website: http://www.fvap.gov/resources/media/strategic_plan.pdf

FVAP, (2011). *2011 initiatives, uocava solutions summit*. Retrieved from website: http://www.fvap.gov/resources/media/UOCAVA_Solutions_Summit_AUG_2011_Slides.pdf

FVAP, (2012). *2010 results and 2012 preparedness*. Retrieved from website: http://www.fvap.gov/resources/media/06JAN2012FVAP_JEOLC.pdf

United States Election Assistance Commission, (2005). *Voluntary voting system guidelines: Volume ii, vesion 1.0*. Retrieved from website: http://www.eac.gov/assets/1/workflow_staging/Page/124.PDF

U.S. Election Assistance Commission, Military Heroes Initiative. (2012). Pilot project plan for providing voting assistance and electronic ballot delivery to Georgia veterans with disabilities. Retrieved from website: http://www2.itif.org/2012-mhi-demonstration-proposal.pdf

Entrust, (2000). Cross-certification and pki policy networking (Verision 1.0). Retrieved from website: https://www.netrust.net/docs/whitepapers/cross_certification.pdf

The U.S. Election Assistance Commission, (2010). Report to congress on eac's efforts to establish guidelines for remote electronics absentee voting systems. Retrieved from website: http://www.eac.gov/assets/1/AssetManager/2010-04-26 Report Congress EAC Efforts Establish Remote Electronic Absentee Voting Systems.pdf

IEEE, (2004). Analysis of an electronic voting system. Retrieved from website: http://avirubin.com/vote.pdf

IEEE , (2011). Voting systems electronic data interchange (P-1622). Retrieved from website: http://www.nist.gov/itl/vote/upload/Keller-P1622-Presentation-2011-02-08-1.ppt

SCYTL, Secure Electronic Voting. (2011). *Usage of eml* (V.2). Retrieved from website: http://www.nist.gov/itl/vote/upload/Scytl-EML-Usage-v2.ppt

Backend Authentication Work Group, (2006). Framework for inter-agency authentication of federal personal identity verification (piv) cards (Version 1). Retrieved from website: http://www.idmanagement.gov/iab/documents/FrameworkInteragencyAuthenticationFederalPIV.pdf

United States Government Accountability Office, (2005). *Elections: Additional data could help state and local elections officials maintain accurate voter registration lists*. Retrieved from website: http://www.gao.gov/new.items/d05478.pdf

United States Government Accountability Office, (2006). *Elections: Absentee voting assistance to military and overseas citizens increased for the 2004 general*

election, but challenges remain. Retrieved from website: http://www.dodig.mil/SPO/Reports/DODIG-2012-123.pdf

National Institute of Standards and Technology, (2006). Electronic authentication guideline (Version 1.0.2). Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

National Institute of Standards and Technology, (2008). *E-authentication: What technologies are effective?*. Retrieved from website: http://www.ists.dartmouth.edu/docs/e-auth_tokens-2.ppt

National Institute of Standards and Technology, (2011). Common date format (cdf) update. Retrieved from website: http://www.nist.gov/itl/vote/upload/CDF-Overview-P1622-Workshop-v1.ppt

National Institute of Standards and Technology, (2003). *Guideline on network security testing*. Retrieved from website: http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf

National Institute of Standards and Technology, (2003). *Guideline on network security testing*. Retrieved from website: http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf

National Institute of Standards and Technology, (2011). *Bios protection guidelines*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

National Institute of Standards and Technology, (2011). *Guide for conducting risk assessments*. Retrieved from website: http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

National Institute of Standards and Technology, (2009). *Recommended security controls for federal information systems and organizations*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

National Institute of Standards and Technology, (2008). *Volume 1: Guide for mapping types of information and information systems to security categories*. Retrieved

from website: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

National Institute of Standards and Technology, (2008). *Volume 2: Appendices to guide for mapping types of information and information systems to security categories*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

National Institute of Standards and Technology, (2011). *Electronic authentication guideline*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

National Institute of Standards and Technology, (2010). *Guide to protecting the confidentiality of personally identifiable information (pii)*. Retrieved from website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

National Institute of Standards and Technology, (2011). *Overview of july tgdc meeting*. Retrieved from website: http://www.nist.gov/itl/vote/upload/Collins-overview-7-11-2.ppt

National Institute of Standards and Technology, (2011). *Enhancing online choice, efficiency, security, and privacy*. Retrieved from website: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Frum, D. (2012). A national id card that protects voting rights. *CNN*, Retrieved from http://www.cnn.com/2012/03/26/opinion/frum-identity-cards/index.html

Ovf research newsletter. (2009, May). *Overseas Vote Foundation*. Retrieved from https://www.overseasvotefoundation.org/research-intro-newsletter-volume1_May2009

Smart Card Alliance, (2011). *Personal identity verification interoperability (piv-i) for non-federal issuers: Trusted identities for citizens across states, counties, cities and businesses*. Retrieved from website: http://www.smartcardalliance.org/pages/publications-piv-i-for-non-federal-issuers

Voting Technology Project, (2008). *Uocava: A state of research*. Retrieved from website: http://www.vote.caltech.edu/sites/default/files/WP_69.pdf

NISTIR 7551, (2008). *A threat analysis on uocava voting systems*. Retrieved from website: http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf

NISTIR 7770, (2011). *Security considerations for remote electronic uocava voting,*. Retrieved from website: http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011.doc

Executive Office of the President, (2003). *Office of management and budget, e-authentication guidance for federal agencies*. Retrieved from website: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

ECAR Research Study 2, (2006). *Establishing identity and user authentication*. Retrieved from website: http://net.educause.edu/ir/library/pdf/ers0602/rs/ers06025.pdf

EAC, (2009). *Roadmap for the development of remote electronic absentee voting guidelines*. Retrieved from website: http://www.nist.gov/itl/vote/upload/UOCAVA-Roadmap-Final.pdf

Ohio Secretary of State, (2012). *Request for proposals uocava ballot delivery & tracking system*. Retrieved from website: http://www.sos.state.oh.us/sos/upload/about/RFP/2012-07-02.pdf

(2010-2011). *Air force voting plan* . Retrieved from website: http://www.fvap.gov/resources/media/afvap.pdf

Coesys egov 2.0 v3 . (n.d.). Retrieved from http://www.gemalto.com/govt/coesys/coesys_egov2_0_version3.html

RSA, (2012). *Combating advanced attacks and protecting high risk transactions with layered authentication*. Retrieved from website: http://www.rsa.com/products/consumer/datasheets/8898_OOB_DS_0212.pdf

RSA, (2011). *The rsa authentication decision tree, select the best authentication solution for your business*. Retrieved from website: http://www.rsa.com/products/securid/whitepapers/9687_DECTRE_WP_0711.pdf

ARDA, (n.d.). *Cewas (cyber early warning system): Evaluation on deter*. Retrieved from website: http://www.isi.edu/deter/community.meetings/Workshop28sep05/ghosh.CEWAS.pdf

SCYTL, (2007). *Okaloosa distance ballot pilot*. Retrieved from website: http://www.itif.org/files/odbp_slides.pdf

Operation BRAVO Foundation. (2008). *Okaloosa distance balloting pilot: Procedures and system description for secure remote electronic transmission of ballots for overseas civilian and military voters*. Retrieved from http://www.operationbravo.org/pilot_projects.html

MasterCard, (2011). *E-commerce security, advantages of a risk based authentication strategy for mastercard securecode*. Retrieved from website: http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf

ID Analytics for Authentication, (2010). *Risk-based identity proofing, a new approach to online identity verification*. Retrieved from website: http://www.idanalytics.com/assets/whitepaper/Risk-Based-IdentityProofing.pdf

Appendix F – Source Organizations

ActivIdentity, Inc.

DISA

DMDC

Dominion Voting Systems

Election Systems & Software (ES&S)

Equifax

Everyone Counts, Inc

Gemalto, Inc

Microsoft

NIST

Scytl

TSA

USAF AFRL/RYWA