ETSI TR 103 741 V1.1.1 (2021-05)

CYBER;
Elections Infrastructure Cybersecurity

Reference
DTR/CYBER-0054

Keywords
cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides a comprehensive examination of public elections infrastructure cybersecurity which includes the existing ecosystem, important cybersecurity capabilities together with both technical and non-technical best practices. The recommendations are also useful for all elections infrastructure. Although e-Voting is encompassed, its use remains widely unaccepted by most nations for definitive voting legal consequences [i.3].

Introduction

Elections infrastructure has emerged over the past two decades to describe a diverse array of systems, products, and techniques used to assist the voting process, that is, the expression of a preference by people or entities for a choice among entities or specific courses of action. These expressions may be advisory, or have legal consequences - especially in governance activities. The systems can be part of an electronic communication network.

These infrastructures include e-Voting which has been promoted in diverse jurisdictions and organizations for many governance purposes worldwide - often with little or no understanding of the technologies, the limitations, the cybersecurity vulnerabilities or necessary steps to reduce risks. The promotion of e-Voting has also led to significant numbers of largely unknown providers of on-line software and e-Voting services, with a user population that has minimal capability to evaluate the security or securely use the products and services. Although e-Voting may have value for informal polls and private sector organizations, it creates significant risks for public elections [i.3].

The present document provides a consistent, widely agreed-upon set of best practices for the security of systems infrastructure that supports elections. It includes both a general explanation of the threats that exist for the various components of the elections process and examples of known mitigations for these threats. The aim is to establish a baseline of protection for all aspects of the elections infrastructure ecosystem that leverage digital tools and applications.

1 Scope

The present document examines existing public elections infrastructure, the threats faced, and provides a set of best practices for the security for both public and private infrastructure.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: Whilst any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Center for Internet Security: "Handbook for Elections Infrastructure Security," Ver. 1.0, February 2018.

NOTE: https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

[i.2] Center for Internet Security: "Handbook for Elections Infrastructure Security".

NOTE: https://www.cisecurity.org/elections-resources/elections-infrastructure-handbook-best-practices/.

[i.3] Council of Europe, European Committee on Democracy and Governance (CDDG), Review Meeting on Recommendation CM/Rec(2017)5 on Standards for e-Voting, 5 December 2019.

[i.4] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.5] ISO/IEC 27005: "Information technology - Security techniques - Information security risk management".

[i.6] NIST Special Publication 800-30: "Guide for Conducting Risk Assessments".

[i.7] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security controls".

[i.8] Center for Internet Security: "Election Security Best Practices".

NOTE: https://www.cisecurity.org/elections-resources/

[i.9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

e-pollbook: electronic pollbook used to assist election officials by providing voter registration information to workers at each polling location

e-Voting: expression of a preference by people or entities for a choice among entities or specific courses of action using a public electronic communications network

elections infrastructure: components of elections systems that define the risk landscape, consisting of network connected systems and components, indirectly connected systems, and non-digital elections components

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations:

CIS	Center for Internet Security
COTS	Commercial-off-the-shelf
CSV	Comma-Separated Values
DRE	Direct Record Electronic
EAC	Election Assistance Commission
EMS	Election Management System
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
ISAC	Information Sharing and Analysis Center
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information technology
NIST	National Institute of Standards and Technology (USA)
PDF	Portable Document Format
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
USB	Universal Serial Bus
XML	eXtensible Markup Language

4 Introduction

4.1 Overview

A common way of describing an organization's cybersecurity posture is in terms of risks that have been mitigated and risks that have been accepted. Those outside the information security community will often think of security in terms of stopping all possible threats. Both within the community and in the legal domain, practitioners understand that perfect cybersecurity is not possible. Rather, organizations seek to achieve "reasonable" security that involves accepting some level of risk given the threats and potential consequences, whilst maintaining an ability to recover should any of those consequences be felt.

4.2 Elections systems risk

The IT systems infrastructure that supports elections processes has myriad risks, and these risks vary from one organization to the next. There are a number of commonly used risk assessment approaches that can be used by election officials and their technical staff to help assess risk (ETSI TR 103 305 [i.4], ISO/IEC 27005 [i.5], NIST SP 800-30 [i.6], CIS Hub [i.8]). The most popular tools for understanding and managing cybersecurity risk consist of frameworks that organizes cybersecurity activities in five functions: identify, protect, detect, respond, and recover.

Unfortunately, many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems.

In its simplest form, a risk assessment is used to identify and assess the impact of vulnerabilities - weaknesses that an attacker can exploit - whilst being mindful of the compensating controls that exist in a system. These risks can be mitigated with appropriate physical, process, and technical safeguards. In this way, risk and potential impacts can be reduced to a level deemed acceptable by the accountable election officials, often called a balanced risk posture. The potential impact or consequence of a successful exploit is an important part of a risk assessment as elections officials want to focus first on exploits that have the greatest potential consequence.

Whilst some risks vary from one election jurisdiction to another, many are common across the wide variety of elections systems configurations. As part of producing the present document, experts have collaborated to assess the common risks to elections systems. This common baseline risk assessment has influenced the prioritization of security best practices in the present document.

Examples of threats and consequences are described in the following two scenarios:

- Scenario 1: A nation-state uses a public internet to access and disrupt one or more voter registration databases such that legitimately registered voters are denied the ability to vote on election day, or are required to file a provisional ballot.

  Consequence: Although no votes are manipulated, this attack would likely be a major national news story that results in reduced confidence by the public in the integrity of the voting process and the election results. Additionally, this slows the voting process, creating the risk of long lines and making in-person voting less efficient.

- Scenario 2: An adversary gains access through the internet to one or more election night vote displays and changes the displayed results such that the real winner of the election is now the reported loser in the election.

  Consequence: Again, whilst no votes have been changed, and the erroneous posting of election results by an authoritative source will subsequently be republished correctly, there is likely to be a significant loss of voter confidence.

4.3 Baseline elections risk assessment

The baseline assessment of risk for elections is summarized for the purpose of helping election officials and their technical staffs understand the major areas of risk that can serve as their primary focus. Each organization should augment the baseline elections risk assessment to address the risks that might be unique to their elections processes, systems, and threats.

A top-level assessment of vulnerabilities and potential consequences to the elections systems infrastructure identifies network connectivity - devices or systems that work with other devices or systems to achieve their objectives - as the major potential vulnerability. The reason is simple: given an adversary with sufficient time and resources, systems that can be accessed via a network cannot be fully protected against compromise. There are ways to improve the security of network connected systems with additional controls, but the inherent complexity of network connectivity results in significant residual vulnerabilities.

Therefore, risks for system components that are connected to a network should be treated differently than for components that are never connected to a network. In the present document the present document, the definition of "network" includes connections to the internet as well as connections to both local wired and wireless networks.

Whilst systems that are continuously connected to a network have a somewhat higher risk than systems that are only intermittently connected to a network, experts have demonstrated that any network connectivity, even if only for a limited period of time, results in a significantly larger vulnerability profile. An access path to these components can be available through the internet if any connected component can access the internet, and thus an attack can be orchestrated from anywhere in the world.

On the other hand, systems that have a digital component but are not network connected have a reduced vulnerability profile. Specifically, there are fewer ways to attack such systems and devices, but it does not mean the consequences of a successful attack are any lower - indeed, an attack can still be executed without geographic boundaries. The methods used to upload and download information (e.g. USB sticks, memory cards) still have vulnerabilities, but there are fewer vectors of attack to mitigate.

4.4 Classes of elections systems

In the present document, best practices are organized into two classes based on the different threat characteristics associated with levels of connectedness. A third class, that of processes that are executed without a digital component, such as hand-counted paper ballots is out of scope.

Whilst there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analysing the manner in which they connect to networks and other devices. Throughout the present document, components of elections systems are classified based on three types of connections that most clearly define the risk landscape:

1) **Network connected systems and components.** Network connected components are interconnected with other devices to achieve their objectives. The level of interconnection, whilst providing various benefits, also introduces additional risks to be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means extra efforts are necessary to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. As an example, an Election Management System (EMS) connected to a private county network would still be classified as a network connected system.

2) **Indirectly-connected systems.** Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives or other flash media. Whilst the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive.

3) **Non-digital election components.** These are aspects of the elections process that have no digital component and are out of scope for the present document. An example would be the mailing, completing, and returning of a paper mail-in ballot. Whilst aspects of the overall process - such as an online request for the ballot - can leverage digital infrastructure, the aspect of this process that is purely paper-based is out of scope.

In clause 5, each major component of an election system is briefly described and then placed into one of these classes, providing a method to simplify the risk landscape and assist officials and their technical staff in determining the most effective and efficient approaches to managing risk. In some cases, major components are divided into the primary approaches to executing a process, such as the different approaches to conducting vote capture, each of which is classified individually. This classification analysis becomes the foundational basis for an election organization selecting the appropriate technical best practices for that component described in clause 6 of the present document.

4.5 Vulnerabilities created by transmission between components

Whilst securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack - attack vectors in cybersecurity parlance - lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected. For instance, whilst paper pollbooks would not typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks to be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e. vote capture) devices. clause 5 addresses transmission risks of this nature and the best practices that can mitigate them.

5 Election systems and risk

5.1 Introduction

This clause provides a generalized elections systems architecture showing each major component of the systems and:

1) a discussion of the risks and threats for each major component;

2) for some components, a description of the different types of deployment in use; and

3) a classification of the component based on how it connects to other devices, and thereby a mapping to controls and recommendations in clause 6 of the present document.

5.2 A generalized elections systems architecture

There are many flavours of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. That said, many experts have studied the elections process at length, and there are several fundamental components common to nearly all elections systems.

In some jurisdictions, the owner of various aspects of the architecture can differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices. Those accountable for elections infrastructure should understand these basic processes and identify the parts where they have purview. A description of major system components that comprise the elections infrastructure are shown in Figure 5-1.

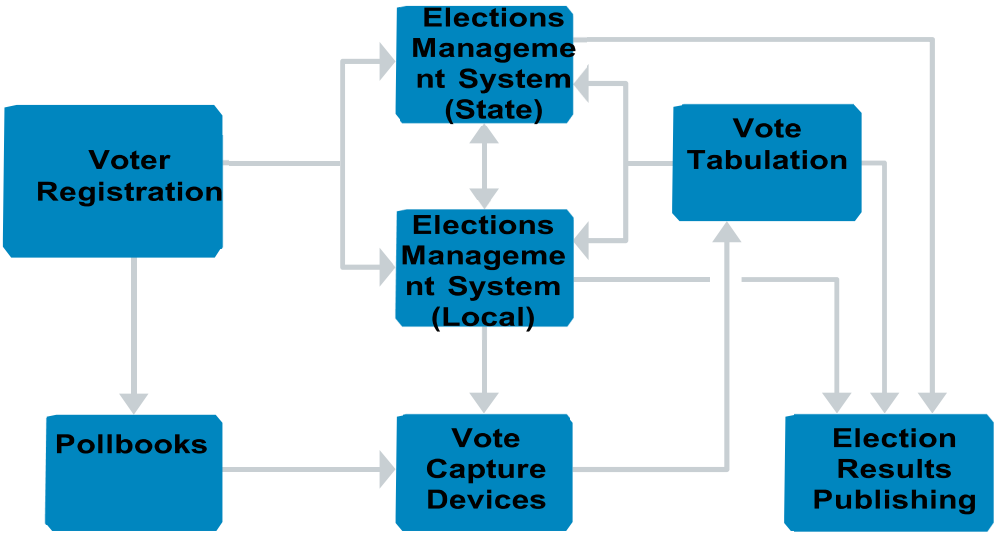

Figure 5-1: A generalized elections systems architecture

While each of these systems has IT components that require security best practices, the present document addresses a subset that are, the highest risk targets of attack by adversaries and thus deserve the bulk of the attention. For digital components not covered in the present document, the analysis methods used here can be applied to determine the appropriate set of technical best practices for that component.

Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components can exist in multiple jurisdictions and some will not be applicable in certain jurisdictions. Nonetheless, all will exist in most jurisdictions and are addressed in order to provide a comprehensive best practices guide. This is especially true for local jurisdictions, given the extent to which elections are administered locally. Even where there is a substantial amount of legacy infrastructure - old systems that are difficult or impossible to update - much can be done to mitigate risks. These systems are described in clauses 5.3 through 5.9 and appropriate best practices and controls are provided in clause 6.

5.3 Voter registration

Different jurisdictions can have unique approaches to voter registration - including some with automatic voter registration - but there are several commonalities shared by all of them. Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks - paper and electronic - as well as provide information back to the voter as they verify their registration and look up polling locations and sample ballots.

The inputs to voter registration systems are registrations, removals due to ineligibility (e.g. an individual moving out of the jurisdiction, death of a voter), and record updates, most often due to an individual moving within the jurisdiction. The outputs include facilitating voter lookups - such as a voter verifying they are registered, seeking a sample ballot, or finding their polling place - and transfer of voter information to pollbooks.

In all of these cases, there is a master voter database in the jurisdiction. Research describes these databases as populated in one of three broad ways:

1) a top-down system in which the data are hosted on a single, central platform of hardware and maintained by the jurisdiction with data and information supplied by local jurisdictions;

2) a bottom-up system in which the data are hosted on local hardware and periodically compiled to form a jurisdiction-wide voter registration list; or

3) a hybrid approach, which is a combination of a top-down and bottom-up system.

For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on Commercial-Off-The-Shelf (COTS) hardware and software. Because they use these common computing platforms, voter registration systems can be part of a shared computing system, though in many cases they are dedicated systems with dedicated software.

Additionally, voters' connection to the voter registration system can run through direct means such as a national or regional registration portal, or through indirect means like mailing in a registration on paper. To address this risk, many voter registration systems with which the voter would interact are separated from the "official," or production, voter registration system. Periodically, a report of changes is generated and undergoes a quality assurance review that is certified before being entered into the production system. This can substantially reduce, for instance, an online portal as a vector of attack, though the production system can still be network connected in other ways.

In general, voter registration systems exhibit the risk characteristics of a general-purpose computing system and, more specifically, any network connected database application. To properly mitigate risks, each voter registration system within a jurisdiction, and links to the voter registration system, needs a comprehensive assessment of its technical characteristics and the application of appropriate security controls.

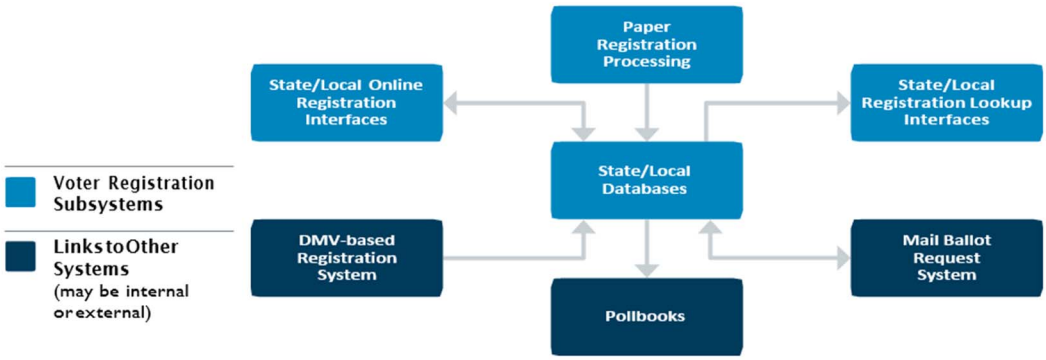

Figure 5-2: Major functions or subsystems of a voter registration system

Types of voter registration

Voter registration generally occurs in one of two ways, each of which is recorded in a jurisdiction wide registration system.

1) Online registration: a website or other web application allows prospective voters to register electronically and have election officials review their registration for validity, which, if valid, is entered into the voter registration database. Same-day registration, because of the need for live updating and cross checking, usually falls into this category.

2) Paper-based registration: prospective voters submit a paper voter registration form that is reviewed by election officials and, if valid, entered into the voter registration database. Registration of this type is out of scope in the present document.

The type of voter registration should typically be viewed as a form of online registration.

Risks and threats

As noted in clause 4, the ability to access voter registration systems through the internet results in a significant increase in vulnerability and resulting risk. There are well known best practices to mitigate these risks, but the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components.

While the attacks on voter registration systems can have a specific purpose not found outside the elections domain, the vectors for those attacks, and thus the primary risks and threats associated with voter registration systems, are similar to those of other systems running on COTS IT hardware and software, and include:

- risks associated with established (whether persistent or intermittent) internet connectivity;
- network connections with other internal systems, some of which can be owned or operated by other organizations or authorities;
- security weaknesses in the underlying COTS products, whether hardware or software;
- errors in properly managing authentication and access control for authorized users;
- difficulty associated with finding, and rolling back, improper changes found after the fact; and
- infrastructure- and process-related issues associated with backup and auditing.

Management of these items is important to ensure proper management of voter registration systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats. Based on their type of connectedness to digital systems, these controls are listed in clause 6.

In practice: protecting the voter registration database

Cybersecurity practitioners constantly face a difficult balance between convenience for users and strong security. With voter registration databases, some approaches allow elections officials to have it both ways.

Practice #1:

Officials in one jurisdiction leverage what's called a "sneakernet" to move information from an internet-facing copy of the voter registration database and a master version of the database that is not connected to the internet. Officials physically move data from one machine to another - usually by moving their sneakers to walk it across the room. This does not eliminate all risks, but can help protect sensitive information from attack through internet-based vectors, while still allowing individuals to access their information over the internet.

Officials can only access the database from a special application. This application makes periodic copies of the database in a tightly controlled environment and these copies are used to populate all other interfaces. Similarly, changes to the master database are limited to this application. Thus, updates do not directly access the database. They are carefully checked for corruption and moved to the master database through this controlled process.

Practice #2:

Some jurisdictions do not air gap their master voter database but use other methods to balance strong security and real-time election official access to the database. In one jurisdiction, the master database is accessible via networks due to needs such as facilitating same-day registration. Experienced cybersecurity professionals leverage appropriate protections including strong vulnerability and risk management programs coupled with robust access controls, intrusion detection and prevention systems, web application firewalls, and security information and event management integration. Multiple layers of defences - both computerized and human - are used to sustain operations while minimizing risk.

How these components connect

Each type of voter registration, along with the master voter registration database, should have risks evaluated individually based on its type of connectivity and employ controls and best practices found in clause 6 that correspond to the type of connectivity and are appropriate to address risks. That said, aspects of the voter registration systems, and the types that can be implemented, have general characteristics that can be classified by connectivity. Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks. See table 5-1.

Table 5-1: Voter registration mitigations based on types of network connectivity

Network Connected 1) Online registration. In addition, the master registration database or system itself should be considered network connected.
Indirectly Connected N/A
Not connected, out of scope 2) Paper-based registration.
Additional transmission-based risks Transmission of a registration via email or fax leverages a digital component and should incorporate the relevant transmission-based mitigations in Clause 6.

5.4 Pollbooks

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this clause focuses primarily on electronic pollbooks (e-pollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These e-pollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These e-pollbooks are typically dedicated software built on COTS hardware and riding on COTS operating systems.

The primary input to e-pollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, e-pollbooks can require additional inputs and outputs to allow for election day changes.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer - in the jurisdiction, or via commercial printing services - protects the integrity of the information in printed pollbooks.

Risks and threats

Attacks on e-pollbooks would generally serve to disrupt the election day process by one of these three situations:

1) attacking the integrity of the data on the pollbook by altering the information displayed from voter rolls;

2) disrupting the availability of the e-pollbooks themselves; or

3) in some cases, causing issues with the vote capture device by altering an activation token.

Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that prevents them from casting a ballot or forces them to use the provisional ballot process, but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook.

An e-pollbook may or may not be connected to a network. If they are network connected, they are treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an e-pollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- risks associated with established (whether persistent or intermittent) internet connectivity;
- network connections with other internal systems, some of which can be owned or operated by other organizations or authorities, including private networks for e-pollbooks;
- security weaknesses in the underlying COTS products, whether hardware or software;
- security weaknesses in the dedicated components, whether hardware or software;
- errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media; and
- difficulty associated with finding, and rolling back, improper changes found after the fact.

The management of these primary risks is important to ensure proper management of pollbooks. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Managing risks associated with e-pollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data (see table 5-2). Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks.

Table 5-2: Pollbook mitigations based on types of network connectivity

Network Connected Pollbook connects via a wired or wireless network.
Indirectly Connected Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).
Not connected, out of scope Paper-based pollbooks.
Additional transmission-based risks Transmission of data for paper-based pollbooks for formatting or printing. If this transmission incorporates a digital component, it should incorporate the relevant transmission-based mitigations in Clause 6.

5.5 Jurisdiction Election management systems

Jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each jurisdiction has an EMS, and each local jurisdiction will typically have a separate EMS that can, but will not always, connect to the jurisdiction's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A jurisdiction EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of the present document, vote tabulation is broken out into its own clause.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties among jurisdiction levels and the manner in which they handle particular aspects of the election process.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware that operate in a networked environment. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and include:

- network connections with other internal systems, some of which can be owned or operated by other organizations or authorities;
- security weaknesses in the underlying COTS products, whether hardware or software;
- security weaknesses in the dedicated components, whether hardware or software;
- errors in properly managing authentication and access control for authorized users;
- difficulty associated with finding, and rolling back, improper changes found after the fact; and
- infrastructure- and process-related issues associated with backup and auditing.

Significant consequences can result from successful attacks on an EMS. These potential consequences include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a jurisdiction EMS is network connected and whether communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP). Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks.

Table 5-3: EMS mitigations based on types of network connectivity

Network Connected Unless known definitively to have no network capabilities, treat an EMS as network connected.
Indirectly Connected If known definitively to have no network capabilities, treat an EMS as indirectly connected.
Not connected, out of scope N/A
Additional transmission-based risks N/A

5.6 Vote capture

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place can give voters the choice of electronic machines or paper ballots. Another instance, voters with language needs or voters with disabilities can necessitate the use of additional components or a separate device.

To this end, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other national jurisdictions, vendors, and others in the election community, maintain standards and a certification program for vote capture devices. Those recommendations are not replicated or altered here, but a generalized set of recommendations is provided that can help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security - and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But, as documented throughout the present document, they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

The primary inputs to vote capture devices are the ballot definition file - which describes to the device how to display the ballot - as well as an activation key (for some electronic machines) and the ballot itself for scanning of a paper ballot. The primary output is, of course, the cast vote record.

In cybersecurity, non-repudiation is the inability to deny having taken an action. Voting is founded in the opposite principle: the ballot is secret; no one should be able to prove who or what was voted for - or against - in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. Voter anonymity is intentionally created through a breakpoint between the fact that an individual voted and what votes they actually cast. The ability to look at a marked ballot and track it back to a specific voter should exist.

Instead, the integrity and secrecy of the vote cast is protected through the capture process and into the process of tabulation. To do this, best practices call for applying a series of controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

5.7 Types of vote capture processes

Vote capture generally occurs in one of six ways:

1) **Voter marked and hand counted paper balloting.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.

2) **Voter marked paper balloting with scanning**. Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots.

3) **Electronic marking with paper ballot output.** Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a ballot marking device.

4) **Electronic voting with paper record.** The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a direct record electronic (DRE) device with voter verifiable paper audit trail.

5) **Electronic voting with no paper record.** The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as a DRE device.

6) **Electronic receipt and delivery of ballots conducted remotely.** The majority of ballots received by voters using this method are voters located in another jurisdiction. Though most votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. When this approach is used, the balloting itself is out of scope as it is via paper means. However, this type of voting can carry transmission-based risks.

Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject - in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, the jurisdiction entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The type of vote capture device known as electronic receipt and delivery of ballots conducted remotely, can take on a large number of flavours. In terms of cybersecurity-related risks, for activities like emailing ballots, election officials consider especially risks involved in the transmission of the ballot. Whether during distribution or return, if the transmission of the ballot is done via digital means, it is subject to the risks of that transmission mode. In clause 6, there is a set of control measures that provide mitigations for risks in transmission.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- if ever networked, risks associated with established (whether persistent or intermittent) network connectivity;
- risks associated with the corruption of removable media or temporary physical connections to systems that are networked;

- security weaknesses in the underlying COTS products, whether hardware or software;
- security weaknesses in proprietary products, whether hardware or software;
- errors in properly managing authentication and access control for authorized users; and
- difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity. Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks.

Table 5-4: Vote capture mitigations based on types of network connectivity

Network Connected

If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network.

Also, many central count scanners, used for *Voter marked paper balloting with scanning* in batches (usually vote by mail ballots) are similarly networked on a closed-LAN.

Some electronic vote capture machines also directly transmit data for election night reporting.

Indirectly Connected

2) *Voter marked paper balloting with scanning.* Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they are programmed to understand the ballot format and transmit captured vote data to another, usually network connected, device.
3) *Electronic voting with paper ballot output.* In addition to the role of the scanners, the vote capture machines are typically not network connected, but are programmed to display the ballot and print the ballot in the correct format.
4) *Electronic voting with paper record.* The vote capture machines are typically not network connected but are programmed to understand the ballot format and transmit captured vote data to another, usually network connected, device.
5) *Electronic voting with no paper record.* The vote capture machines are typically not network connected but are programmed to understand the ballot format and transmit captured vote data to another, usually network connected, device.

note: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Not connected, out of scope

1) *Voter marked and hand counted paper balloting.* Out of scope in this the present document as the vote capture process does not include a digital component.

Additional transmission-based risks

6) *Electronic voting conducted remotely.* These methods vary greatly and addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations in Clause 6. Aspects definitively executed without a digital component are *not connected, out of scope.*

5.8 Vote tabulation

In its broadest definition, vote tabulation is any aggregation or summation of votes. Vote tabulation is the aggregation of votes (e.g. cast vote records and vote summaries) for the purpose of generating totals and results report files. For the purposes of the present document, this clause on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Vote tabulation in the present document is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g. results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across the jurisdiction through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- network connections with other internal systems, some of which can be owned or operated by other organizations or authorities;
- security weaknesses in the underlying COTS products, whether hardware or software;
- security weaknesses in proprietary products, whether hardware or software;
- errors in properly managing authentication and access control for authorized users;
- lack of confidentiality and integrity protection for transmitted results;
- difficulty associated with finding, and rolling back, improper changes found after the fact; and
- infrastructure- and process-related issues associated with backup and auditing.

The management of these primary risks is important to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network. Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks.

Table 5-5: Vote tabulation mitigations based on types of network connectivity

Network Connected In some cases, vote tabulation equipment will be *network connected,* whether through a wired or wireless connection.
Indirectly Connected If vote tabulation equipment is not *network connected,* it is indirectly connected through removable media.
Not connected, out of scope N/A
Additional transmission-based risks N/A

5.9 Election results reporting and publishing

After votes are tabulated, results are communicated both internally and to the public. In any given jurisdiction, this can take many forms, but, in most cases, the basic process goal remains: getting results as quickly and accurately as possible. This clause focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing tabulated votes as described in clause 5.8. The systems used for reporting and publishing are likely networked, and, in many cases, have public facing websites.

The outputs are the unofficial election results, typically published on a website, often in multiple formats such as extensible Markup Language (XML), Hypertext Markup Language (HTML), Portable Document Format (PDF), and Comma-Separated Values (CSV). There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results can be kept on a system that is not persistently connected to a public internet.

How these components connect

Depending on the approach to submitting tabulated votes, the reporting component can be network connected. The publishing component is almost certainly network connected, but can be indirectly connected, depending on the implementation. Based on the type of connectivity for a given implementation, clause 6 provides mitigations for these risks.

Table 5-6: Election results reporting and publishing mitigations based on types of network connectivity

Network Connected In some cases, election night reporting will be *network connected,* whether through a wired or wireless connection. The publishing component of election night reporting is almost certainly *network connected,* whether through a wired or wireless connection.
Indirectly Connected If the election night reporting process is not network connected, it is indirectly connected through removable media.
Not connected, out of scope N/A
Additional transmission-based risks N/A

6 Mitigating election system risk

6.1 Introduction

Mitigating risk is, ultimately, about decisions and actions that establish trust in aspects of a system, leading to confidence in the outcome. Risk is considered at every stage of a system - requirements, design, development, operation, and even for disposal or retirement (e.g. removal of sensitive information).

Like many systems, for election systems this involves establishing trust in users, devices, software, and processes. Many systems are "composed," or built up from a variety of commercial and purpose-built parts, devices, and software connected via processes and user actions. The results in security decisions about trust are made across many components and brought together at a system level. In other cases, key election system components or services functions are contracted out. This does not change the security responsibility for decision-makers, but forces them to think about how the desired security properties can be specified in contract language and service specifications, rather than implemented directly.

Clauses 6.2 to 6.7 contain:

1) a set of critical risk-mitigating activities from which all organizations can benefit;

2) recommendations for best practices in contracting for IT services; and

3) a set of best practices in the form of recommendations and controls for network connected and indirectly connected devices, as well as for transmission of information.

6.2 Critical risk-mitigating activities

Auditing

Election officials conduct many audits of all aspects of the election process (e.g. vote by mail processing, training, equipment delivery) and election systems (e.g. voter registration transactions, audit log data). However, the focus of this clause is on auditing vote capture and tabulation in an election.

Included in this is to validate that the aggregated results reflect the actual ballots cast. One auditing approach is to select a sample of the ballots and, applying a structured process, do a partial recount of the ballots. This controlled audit is intended to provide confidence that the voting results are accurate based on the results of that partial recount. Moreover, audits provide information to election officials that go beyond the requirements for audit and recounting results; audits are the "production time" opportunity for election officials to know that the systems they are using are working properly.

The approach to auditing can vary based on a number of factors, including requirements that can be established within elections jurisdictions. Some auditing requirements call for a manual recount of a set percentage of ballots, others - including risk limiting audits described below - leverage statistical methods to determine the extent of the recount. Auditing requirements typically also have a trigger for a larger recount or full recount based on the outcome of the initial audit. Given the potential expense of auditing, it is critical to properly design audit procedures to reduce costs while achieving the goals of the audit.

Almost all jurisdictions have provisions for a full recount of a contest should the result of that contest fall within the jurisdiction required recount margin (for instance, many jurisdictions require a recount for a jurisdiction-wide race if that race is within one half of one percent after certification).

The initial audit size and recount triggers are critically important to a good audit. As important is the method by which the audited ballots are selected. Establishing proper methods for random selection of ballots can have a tremendous impact on the audit's ability to confirm election results or show evidence of tampering.

For election officials, the first step to a good audit is to keep records to make an audit possible. This means allocating resources to support an audit, along with procedures for efficiently executing the audit and making it sufficiently transparent for interested parties. While audits are not inherently digitally-based efforts, establishing an audit process, with resources, ballot selection methods, audit size rules, and recount triggers, is a critical aspect of mitigating risk across all aspects of elections.

A best practice: risk limiting audits

A possible weakness in some traditional auditing methods is that often either more ballots or fewer ballots are recounted than necessary to validate the results. This can either produce an audit that does not fully validate the outcome of the election, or an audit that is more costly than necessary without increasing confidence in the results.

More recently, the concept of risk limiting audits has been introduced as an approach to auditing election results that is both effective and efficient. In addition to those characteristics necessary in a traditional audit - resources, good ballot selection methods, and prior-determined rules - in a risk limiting audit the size of the audit and recount triggers are based on a "stopping rule" determined by the likelihood that the actual election outcome differs from the reported outcome. Put another way, additional ballots are recounted in the audit until there is a pre-determined statistical level of confidence that the reported result is correct. As an example, a very large margin of victory will typically result in a relatively small audit size, as a very large error would have to occur to change the outcome. A very close election, on the other hand, would require a larger audit.

In a risk limiting audit, the size of the audit is determined by the results of the audit itself. That is, the closer the audited results are to the actual outcome, the sooner the audit ends. This is termed the statistical confidence in an election's results. As soon as a previously-determined confidence threshold is met, the audit can stop. As in all audits, units - precincts, machines, batches of paper records - should be selected using random sampling methods. In a risk-limiting audit, the sample size will depend on the margin of victory and other factors; these other factors can include the number of ballots in each precinct and the overall number of ballots in the contests. In general, smaller margins of victory and fewer total votes cast require auditing a larger percentage of the ballots cast. These methods are well-documented and replicable through sources such as ElectionAudits.org.

Incident response planning

Despite the best efforts of election officials and their technical staff, there is some likelihood that there will be an incident at some point during an election cycle. This is the nature of cybersecurity; the true measure of success is often the resiliency of an organization in the face of these incidents.

Incidents can be minor, having no real potential for impacting the election results or public perception of the elections process, or they could be major incidents requiring prompt action to ensure the actual or perceived integrity of the election results. An incident could be a direct attack on some portion of the election system, or it could be a potential threat that might affect confidence in the system (e.g. a reported major flaw in a foundational COTS component of many election systems).

Experience shows that successful incident response depends almost entirely on planning and preparation - the work done before any incident occurs. Good technical and process controls will minimize the attack surface and also help to enable timely analysis of the incident. Identifying key decision- makers and their roles ahead of time allows for effective response.

Planning and preparing begins with creating a plan for diagnosing and recovering from incidents and exercising this plan. To properly develop and exercise these plans, efforts include a wide variety of stakeholders - ideally all stakeholders that would be involved in response to and recovery from the incident itself. All stakeholders, including seemingly sovereign jurisdiction, need to collaborate in incident response and recovery; they need also to collaborate in preparing for those incidents. As the threats change, so do plans. Officials should update documentation regularly and include specific plans for addressing modern cybersecurity risks, such as those presented throughout this clause.

Incident response generally follows a lifecycle of: prepare; detect and analyse; contain, eradicate, and recover; and manage post-incident. Again, it begins with documenting and exercising, but in recovery this includes specific information about the systems and processes that can be impacted, such as knowing the hardware and software comprising specific systems, as well as things such as hashes of critical files - a way to validate whether a file has been tampered with from its last known good state. In preparing for incident recovery, one of the most critical mitigation strategies is to ensure proper backups that are secured separately from the affected systems and networks in advance of a potential incident.

The process of actually recovering starts with understanding the incident. As part of that analysis, decision-makers need to understand the impact of the incident so they can prioritize resources appropriately. Recovery is about getting back to a viable state - in some cases, the priority is not to directly fix the problem, but rather to work around it to get to the desired outcome without the affected system. This is nothing new in the election context: when a vote capture device breaks, it can be desirable to fix it, but it can be better at the moment to move to paper ballots so votes can be cast efficiently. The same logic can apply in a cybersecurity context across the election ecosystem; the most important reaction is often to return to an operational state, even if it is not the optimal jurisdiction.

Recovery, then, is about getting to the best possible outcome in light of the current circumstances. With proper planning and exercising, officials can avoid the impact of an incident that could prevent successfully executing an election, even when seemingly all has gone wrong.

Attacks such as those that would be directed at an election come with a motivation to impact the election in some way. Nothing serves as a greater disincentive to an attacker than knowing that their target will recover quickly and completely. And little serves to build trust with the public like a plan to achieve an accurate result even if an attack is successful. Just as with other aspects of cybersecurity, by taking the time to prepare before an incident occurs, election officials can actually turn away attackers before they arrive.

6.3 Contracting for systems or services

Many organizations use contractors or vendors to provide election system components and services to support elections processes or elections system operations. Election officials should assess the contracted supply chain in addition to support provided internally. In instances where there is contract support, officials should carefully analyse requirements for security and clearly define them in the contract. The government organization that is doing the contracting has the responsibility to assess the security risks for the component or service based on an evaluation of potential threats and security weaknesses or vulnerabilities as well as the probability of occurrence and resulting consequences. Security considerations should be an important consideration in the process of evaluating and selecting a contractor.

If the elections staff is contracting for services that are managed by a contractor or vendor, such as hosting of elections-related software or operations of elections systems, the contract should require that the company providing managed services also provide documentation of their cybersecurity processes and controls, including security metrics that are being collected and monitored. Contractor controls can then be compared to the controls listed in the present document.

The contract should include a definition of services to be delivered (called a service level agreement or SLA) that includes security controls identified in the present document. Moreover, a best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits.

For elections system components that are subject to elections system certification requirements, evidence of certification is required. Ideally, there should also be a provision for the contractor to provide security updates to the component over its lifecycle to ensure that vulnerabilities that are discovered are corrected and the component is recertified. For system components or services that are not subject to certification, security requirements will need to align with the particular capabilities or services provided in the contract. Many of the best practices listed in the present document can be appropriate to include as contract requirements.

In general, the contract should require that the contractor provide a security plan as one of the initial contract deliverables. The security plan should describe how the contractor will meet the security obligations of the contract and specify the security practices and procedures that will be used. Of particular importance in specifying security requirements for contractors will be to address how elections-sensitive information (e.g. ballot layout, voter personal information, vote results) is protected during the execution of the contract and how information records are destroyed.

Additionally, contracts should address the obligations of contracted system operators and public sector clients in regards to identity theft liability, control of and access to public and private data under open records laws, and incident response plans and processes. Where possible, contracts also should specify that vendors transmit network, system, and application logs to the client's security information and event management tools if the client requests. This would allow election officials and their staffs to review and monitor activity instead of being solely reliant on the vendor's capacity for monitoring.

Guidelines for ensuring security of contracted support should be followed pursuant either to ISO/IEC 27002 [i.7] or the CIS Hub [i.8], section 15 of the ISO/IEC standard describes security issues that should be addressed in dealing with suppliers, and the Appendix to reference [i.1] contains a reproduction of this clause.

Contracting and technical personnel are encouraged to use this or a similar resource to help identify and assess potential risks as well as responsibilities that will need to be addressed in contract documents and in managing suppliers.

6.4 Election Infrastructure Security Best Practices

The extensive table of Election Security best practices together with a related appendix of references and resources are found in [i.2] and [i.8]. This material is derived from extensive experience understanding the types of vulnerabilities found and attacks experienced across a very wide variety of enterprises, and then translating that into specific and positive steps to mitigate those vulnerabilities and threats. Those recommendations are tailored based on the system and "mission" issues that are unique to elections systems, and the confidence expected for successful outcomes. The process used also examined the various guidelines and specifications used in this sector in order to maintain consistency and minimize overlap.

All of the recommended practices are grouped by class of connectedness (i.e. network connected, indirectly connected, transmission), which was identified as the key factor in assessing security risk. In addition, recommended practices that specifically deal with transmission (electronically or manually) are grouped as a collection for ease of reference.

Network connected

Network connected components work directly with other devices or systems to achieve their objectives. These connections provide many benefits (e.g. remote diagnostics and management, simple data transfer, rapid updating), but also introduce additional risks to be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means to accessing and managing the devices, which means organizations take extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet.

Indirectly connected

Indirectly connected components are not persistently interconnected with other devices. They do, however, exchange information in order to complete their objectives in the election process. While these devices do not carry the same risks associated with being connected to a network or the internet, connecting these components to other devices, either through the use of removable media or direct wired connects, can introduce threats. Mitigating these risks requires a particular set of controls and recommendations when managing the device.

Transmission

In addition to the level of network connectedness, recommendations to address the broader risk of transmission of information across systems are listed separately. These can provide different and sometimes unexpected avenues of attack. These can also involve information transmitted to or from supporting systems that are easy to overlook in terms of security criticality (e.g. the printing of pollbooks, scheduling systems).

6.5 Structure of the best practices

Each best practice includes the following information:

- Asset Class (Device, Process, Software, User) - the portion of the overall system to which the practice applies.
- Priority (High, Medium, Low) - from a security perspective (only High and Medium practices have been included).
- Applicable Critical Security Controls [i.4] - a cross-reference to the most applicable of the CIS Controls (which can provide a deeper description of this type of practice, and pointers to other information).

Information is also provided that is intended to help decision-makers calibrate the potential challenges of implementation. However, these should be treated as rough guidelines for a "typical" situation - not a rule that can be applied to every election system.

- Potential User Resistance (Yes/No) - Would implementation of the practice be expected to cause resistance or complaints by users and operators of the system? If so, extra care might be needed for rollout or training; and care should be taken so that implementation does not encourage the use of risky "work-arounds".
- Upfront Cost (High, Medium, Low) - Does this practice typically require the purchase of new technology, or other significant capital expenditure (High)? Items can be listed as Low when no separate purchase is needed, often because the recommendation can be implemented using existing technology, into the basic configuration of the purchased system, or through operator action.
- Operational Cost (High, Medium, Low) - What are the expected post-purchase costs of this practice? Are there high costs associated with things like supplies (e.g. media, special licensing)?

6.6 Summary of connectedness in elections infrastructure components

Clause 5 describes the components of a generalized elections system. The end of each clause classified the different approaches to implementing each component based on the extent to which the component is connected to networks. These connectedness classifications are summarized in table 6-1 and form the basis of the best practices. Depending on specific implementation, some of these classifications can vary. However, unless compelling information suggests otherwise, components should be protected at the level indicated.

From clause 5, election officials and others should be able to step through each component to determine the manner (or manners) in which it is implemented in a given election jurisdiction. Once the approach is known, the connectedness classification, summarized here, maps to specific sets of best practices found in the remainder of clause 6.

As noted in clause 5, the components below are a subset that reflect the highest risk targets. For digital components not listed below, the analysis methods described in clause 5 can be applied to determine the appropriate correctness class and the associated best practices applicable to that component.

Practitioners can implement these best practices in any order. However, one should begin with the high priority best practices.

Table 6-1: Summary of connectedness for election infrastructure components

Component		Type within component	Connectedness Class
Voter registration		Master systems and databases	Network connected
	1	Online	Network connected
	2	Paper-based	Not connected
		Transmission of a registration via email or fax	Transmission-based
Pollbooks		e-Pollbook, connects via a wired or wireless network	Network connected
		e-Pollbook, connects via a physical media connection or removable media	Indirectly connected
		Transmission of data for printing via a network connection, website portal, or email	Transmission-based
		Transmission of data for printing via a wired media connection or removable media	Transmission-based
EMS	1	Unless definitively known to have no network capabilities	Network connected
	2	If known definitively to have no network capabilities	Indirectly connected
Vote capture		Vote capture device transmits data for any reason—or if the functionality is enabled regardless of whether it is used	Network connected
	1	Voter marked and hand counted paper balloting	Not connected
	2	Voter marked paper balloting with scanning	Indirectly connected
	3	Electronic voting with paper ballot output	Indirectly connected
	4	Electronic voting with paper record	Indirectly connected
	5	Electronic voting with no paper record	Indirectly connected
	6	Electronic receipt and delivery of ballots conducted remotely	Transmission-based
Vote tabulation	1	Connects via a wired or wireless connection	Network connected
	2	All others	Indirectly connected
Election night reporting	1	If receiving tabulated votes via a wired or wireless connection	Network-connected
	2	If receiving tabulated votes via a wired media connection or removable media	Indirectly connected
Election night publishing	1	All	Network connected

6.7 General Data Protection Regulation

The application of GDPR requirements to public election systems is a complex legal matter within the competence of jurisdiction government authorities [i.9]. The practices described in this clause generally further compliance with GDPR. However, full compliance with GDPR requirements, where applicable, is essential.

Annex A: Bibliography

Global Governmental

International Telecommunication Union

- Report by the Secretary-General, Doc. C17/70, 12 April 2017.
- Draft Recommendation ITU-T X.stov: "Security threats to online voting using distributed ledger technology," SG17-TD2817, Mar 2020.

Council of Europe

- Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, (Adopted by the Committee of Ministers on 30 September 2004).
- Recommendation CM/Rec(2017)5, of the Committee of Ministers to member States on standards for e-voting, (Adopted by the Committee of Ministers on 14 June 2017). See News 2017.
- Review meeting on implementation of Recommendation CM/Rec(2017)5 on standards for e-voting, Dec 2019.

CIS Elections Infrastructure ISAC

- Elections Infrastructure Information Sharing and Analysis Center™ (EI-ISAC®) has links to related resources and provides support.

NGO and Academic

ACE e-Voting Project. On-line knowledge network. The Project consists of partner organizations: Election Canada, Electoral Institute for Sustainable Democracy in Africa, International Institute for Democracy and Electoral Assistance, International Foundation for Electoral Systems, Instituto Nacional Electoral - Mexico, The Carter Center, The United Nations Development Programme, The UN Electoral Assistance Division. It has produced for reference, Cybersecurity in Elections, Literature review, 2018.

Harvard Kennedy School Belfer Center Defending Digital Democracy project. It has produced for reference The State and Local Election Cybersecurity Playbook, February 2018.

History

Document history		
V1.1.1	May 2021	Publication