A Systematization of Voter Registration Security

Jack Cable*
Stanford University

Andrés Fábrega*
Cornell University

Sunoo Park
Columbia University

Michael A. Specter
MIT

Abstract

Voter registration is an essential part of almost any election process, and its security is a critical component of election security. Yet, despite notable compromises of voter registration systems, relatively little academic work has been devoted to securing voter registration systems, compared to research on other aspects of election security. In this paper, we present a systematic treatment of voter registration system security. We propose the first rigorous definitional framework for voter registration systems, describing the entities and core functionalities inherent in most voter registration systems, the jurisdictional policies that constrain specific implementations, and key security properties. Our definitions are configurable based on jurisdiction-specific parameters and policies. We provide a template for the structured presentation of detailed jurisdictional policy information, via a series of tables, and illustrate its application with detailed case studies of the voter registration systems of three U.S. states and Panama. Throughout our research, with the aim of realism and practical applicability, we consulted current and former U.S. election officials, civil society, and non-profits in the elections space. We conclude with a list of critical questions regarding voter registration security.

1 Introduction

Voter registration systems maintain a list of eligible voters, and are a crucial component of almost any election process. Starting well before election day, jurisdictions are tasked with enrolling eligible voters' information — either automatically or on a voter's initiative — and must keep that information up to date and verifiable for use throughout the democratic process. These voter lists serve many purposes, the most important of which is supporting eligibility checks during elections.

Public attention and academic research around election security often focus more intensely on the *casting and counting* processes that happen on and right after election day, rather than voter registration and other non-voting processes.

Yet voter registration security is critical to election security: a voter registration system failure can cause significant disruption to an election and the public's confidence. The results of failure could include disrupting voting processes (e.g., forcing voters to cast provisional ballots), preventing voters from receiving absentee ballots, and the leakage and misuse of sensitive personal and political information. (These issues are discussed more formally in Sections 3 and 5.) Recognizing the importance of voter registration system security, the U.S. Department of Homeland Security's

*Joint first authors.

designation of election infrastructure as critical infrastructure explicitly includes voter registration systems [1].

At least three U.S. states and numerous other countries and regions have suffered publicized compromises of their voter registration systems [2, 3, 4, 5, 6, 7], underscoring the value of registration systems as targets for attack and as potential sources of damage to electoral integrity and confidence. Some of these security incidents arose from software errors (e.g., [6]); others were perpetrated by foreign adversaries (e.g., [2]).

At first glance, the voter registration problem might appear to be addressed by known solutions in the distributed and accountable systems literature. For example, maintaining a canonical, audited database has been studied in a variety of settings including distributed consensus systems [8], the HTTPS ecosystem [9], and, most recently, decentralized currencies [10]. However, voter registration systems are complex and specialized systems with functionality requirements and security challenges not encapsulated by generalized database management and security. For example, the availability requirements of a voter registration database on election day[1] are unusually demanding and time-constrained. Voter registration systems also have unusual accessibility requirements, as they must accommodate *any eligible voter* in the relevant electorate: a highly diverse set of people of whom no technical expertise must be required (since that should not be a requirement to vote). Relatedly, voter registration is often facilitated by third-party intermediaries — neither the election office nor voters — that relay communication between the election office and voters, such as departments of motor vehicles[2] or nonprofit organizations. Election administrators are also often under-resourced, so it bears note that even basic security practices may be difficult to implement [12].

Currently, the security research community lacks a precise and systematic shared understanding of the scope and security challenges of voter registration. The infrequent security and cryptography publications that focus on voter registration have scoped out specific sub-problems and offered some valuable technical approaches, but hardly any prior work has addressed voter registration system security with a more holistic perspective alongside technical depth aimed for a research audience (see Section 2 for more discussion on prior work).

One barrier to such a systematic approach may have been the large variation between voter registration systems' implementations and requirements across jurisdictions. Even within the United States, every state manages its own voter registration system subject to its own state election law (in addition to federal law, which is fairly limited in scope), resulting in significant differences in implementation. The types of information collected and treated as public or confidential, registration methods offered, voter authentication methods, and conditions for updating or removing voter information are all subject to these jurisdiction-dependent regulations. Across countries, of course, an even wider range of laws apply.

This paper provides a systematic treatment of voter registration system security.[3] Our aim is to serve as a reference for the security research community in: (1) identifying research questions in voter registration security; (2) framing voter registration functionalities and security definitions in shared and precise terminology; (3) assessing the applicability of security approaches across different

[1] Or generally, while an election is ongoing.

[2] Under the U.S. National Voter Registration Act, states must offer voter registration opportunities at certain offices, including public assistance and disability offices. [11]

[3] In this paper, we scope voter registration systems as systems related to the process of maintaining an accurate list of voters and their eligibility. Often, other features are bundled with the term "voter registration" — such as ballot tracking, ballot configuration, and ballot design — which are outside the scope of this work.

jurisdictions; and (4) effectively organizing detailed information about a particular jurisdiction's voter registration requirements, to facilitate contextually tailored designs and security analyses.

To this end, we provide definitions of the *categories of entities*, *core functionalities*, and *security requirements* inherent to voter registration. These definitions, while rigorous, are formulated at a high enough level of abstraction to capture the features common to all fifty U.S. states and many other countries. We also provide a systematic exposition of the *jurisdiction-specific parameters* and *policies* that, when combined with the more abstract definitions just described, yield detailed lists of entities, functionality descriptions, and security requirements tailored to a particular jurisdiction.

The jurisdiction-specific parameters and policies effectively *instantiate* our general definitional framework to represent particular real-world implementations and security needs. The separation between the general definitions and the jurisdiction-specific parameters and policies highlights which aspects can be treated as common to most registration systems, and which aspects will need to be configured per jurisdiction.

To further illustrate how our framework yields jurisdiction-specific instantiations of our definitions, we provide detailed *case studies* of voter registration systems deployed in Colorado, Ohio, and Wisconsin (three U.S. states with different models of voter registration) and Panama (for an example outside the U.S.). Based on information from a range of public sources (such as a state's election code), we compile a detailed description of each jurisdiction's parameters and security policies as relevant to voter registration. These case studies provide concrete examples of how our framework facilitates organizing jurisdiction-specific voter registration parameters and policies, whether for research and analysis, or for transparency-minded election officials to publish (or internally examine) information in structured and detailed form amenable to comparison between jurisdictions.

To ensure that our work is grounded in the reality of how voter registration systems work in practice, we gathered feedback from a range of election experts, including current and former election officials. We checked our definitions' compatibility with a range of U.S. states' and other countries' voter registration systems using public compilations of comparative data, and confirmed our framework's applicability by conducting the detailed case studies mentioned above. See Section 3.2 for more details.

Finally, with a view to facilitating effective communication between security experts, election officials, and the public about security-relevant issues in voter registration, we provide a collection of critical questions as a starting point for those looking to gather information about strengths, weaknesses, and potential for improvement in the security of proposed or deployed voter registration systems.

In summary, our contributions are as follows:

1. We provide the first definitional framework for voter registration system security, comprising core technical functionalities, entities, jurisdictional parameters, and security policies (Sections 4–6).

2. We define a threat model (Section 5) and security properties (Section 6) for voter registration systems. Our definitions are *configurable* to accommodate jurisdictional policy variations.

3. We provide a template for the structured presentation of jurisdictional policy information (Section 8).

4. We conduct case studies of the voter registration systems of three U.S. states and Panama, showing the instantiation of our definitions with concrete jurisdictional parameters (Section 8).

5. We offer a collection of critical questions regarding security in voter registration systems (Section 9).

2 Relation to Prior Work

To our knowledge, there has been no systematic treatment of voter registration system security that provides precise problem definitions and system (security) requirements. Furthermore, there has been no treatment that captures the realistic constraints and operation of voter registration systems on the ground today. This paper aims to fill that gap: that is, to provide a detailed and systematic exposition of the challenges of voter registration security in practice, laying the groundwork for the security community to better contribute its expertise to pressing issues in voter registration.

2.1 Systematizing voter registration system security

The most extensive prior overviews of security considerations in voter registration systems are a 2006 report commissioned by the ACM U.S. Public Policy Committee on "accuracy, privacy, usability, security, and reliability issues" related to "statewide databases of registered voters" [13], and a 2019 report by the MITRE Corporation on "recommended security controls for voter registration" [14]. These two reports have very different emphases, as summarized next; they provide important perspectives complementary to our work.

The ACM report was produced at a time when U.S. states were adopting statewide voter registration databases to comply with then-new federal legislation [13]. The report's focus is much more policy-oriented, compared to our focus on definitions and systematization: for example, it lacks technical definitions of core functionalities or security properties. Within its broad policy-oriented scope, the ACM report is remarkably comprehensive, detailed, and thoughtful about security issues.

The MITRE report has a more technical focus. The bulk of the report overviews security measures and best practices[4] broadly applicable beyond the scope of voter registration. The MITRE report also presents a generalized voter registration system architecture and parties involved therein, in less detail than (but consistent with) our model; however, unlike this paper, it neither formalizes functionality and security requirements nor engages with variations in jurisdictional policy.

Additionally, the Electoral Knowledge Network's website on voter registration [15] is a rich source of information about how voter lists are operated across the world. Its focus is broader than security or technology: instead, it offers detailed information on operational and administrative issues, as well as a range of case studies and practitioners' perspectives on voter registration in specific regions.

Other (mostly policy-focused) reports that discuss security in voter registration systems are generally less comprehensive, and tend to have less technical detail than the ACM and MITRE reports. These include: an excellent series by the Brennan Center for Justice, including but not limited to [16, 17, 18, 19, 20]; the U.S. Election Assistance Commission's resources on voter registration systems [21, 22]; a 2008 report by the National Research Council of the National Academies of

[4] E.g., firewalls, TLS, VPNs, and multifactor authentication.

Sciences, Engineering, and Medicine [23]; and a 2020 report by the Center for Election Innovation and Research [24]. These are valuable resources to understand specific aspects of modern voter registration systems, potential security issues, and the concerns of those managing the systems on the ground. Further information of this type may be found in policy-oriented resources discussing election infrastructure security more broadly, such as [25, 26, 12, 27].

2.2 Technical work

Another area of related work comprises technical proposals, such as secure protocols (e.g., [28]) or statistical techniques (e.g., [29]), that may improve voter registration system security. Beyond academia, a number of non-governmental organizations offer innovative technological solutions to improve the integrity of voter registration data. Examples include the Electronic Registration Information Center (ERIC), a non-profit that helps identify voters who have moved, died, or have duplicate registrations across U.S. states [30], and VoteShield, a non-profit that provides tools to monitor changes to voter data for anomalies [31].

There is also a body of technical work proposing approaches to improve the security of election infrastructure other than voter registration systems, such as approaches and systems for secure casting and tallying (e.g., [32, 33, 34, 35]) or post-election auditing (e.g., [36, 37, 38]). A related literature warns of serious security risks entailed by certain technical approaches — such as Internet voting — if used in high-stakes political elections, given the limitations of the current state of the art in computer security (e.g., [39, 40, 12]).

2.3 Beyond security

Many aspects of voter registration are beyond the scope of this paper, because our focus is on system security. Important security-adjacent considerations include usability, privacy practices, software engineering practices, and personnel training. For an overview of these broader topics, we recommend [13] (an ACM report on registration systems) and [12] (a National Academies report on election systems generally).

3 Background & Methodology

3.1 Background

Voter registration is the act of maintaining an accurate list of voters who are eligible to vote in an election for the purpose of (among other things) verifying eligibility at the time of voting. While most countries have some form of voter registration, practices vary widely. Countries may institute compulsory voter registration, in which voters are either automatically registered (such as in Argentina, Chile, Hungary, Israel, and the Netherlands) or required by law to register (such as in New Zealand and Tonga) [41]. In other cases, including the United States and India, qualified residents are not required to register to vote by law, though generally must be registered to vote in order to vote.

While a straightforward premise, maintaining voter registration databases (VRDBs) is complicated by a number of practical and legal concerns. Election administrators must allow voters to register or update their registration by a variety of means, which can include in person, mail, fax, email, and via web portals. This list must then be accessible to election officials when the

voter requests their ballot, both for access control, and to allow the official to customize the ballot for the various contests available to a particular voter in that election. Furthermore, jurisdictions may run multiple, overlapping elections in parallel, all supported by the same VRDB. Election administrators must also perform complicated maintenance on the database when voters become inactive or ineligible (e.g., when a voter dies or leaves the jurisdiction). Finally, the voter registration database may have a number of transparency requirements. Members of the public, including voters, candidates, or other entities, may be allowed to review (parts of) the VRDB contents to ensure accuracy.

Voter registration databases must therefore allow access and maintenance by a variety of entities of varying degrees of trust and technical ability. This includes state election officials, local election officials, and poll workers (many of whom are only temporarily employed). For instance, poll workers must have access to the voter registration database (or a local copy of it) in a pollbook[5] in order to check in voters on election day; this brings its own security challenges. States may also provide third parties[6] full or partial access to their VRDB (or copies of the data therein) for transparency, maintenance, or other purposes.

The law governing voter registration databases varies widely. In the United States, for instance, voter registration systems are run separately by each state.[7] Twenty-two U.S. states have implemented automatic voter registration, while in the remaining twenty-eight states registration occurs in solely on the initiative of the voter [44].[8] Like all election administration in the U.S., voter registration is heavily decentralized, with implementations dependent on state and local election laws and policies [22]. The National Voter Registration Act of 1993 (NVRA, also known as the "Motor Voter Act") required states to use a unified voter registration form for federal elections, allow voters to register to vote while applying for driver's licenses, and allow voters to register to vote by mail [11]. The Help America Vote Act of 2002 (HAVA) mandated that states base their voter registration systems on a computerized voter registration database [46]. U.S. states have taken three primary approaches: *top-down* databases maintain a central, authoritative database statewide; *bottom-up* databases have local jurisdictions maintain authoritative registration databases, which are compiled into a statewide database; and *hybrid* systems give local offices discretion to either maintain an authoritative list locally, or rely on a statewide database.

Voter registration information is made available to various third parties, often including the public, in all 50 states [47]. Laws and policies governing access vary widely: in some states, the voter registration list (excluding certain fields) is made publicly available for download (e.g., North Carolina [48]), while in others, data is restricted to political parties and other organizations (e.g., Maine [49]). The data may be available either for free or for purchase, and often, commercial vendors sell compiled "voter files" that contain records of most American voters for political outreach and advertising purposes [50].

Jurisdictions may also offer protections to voters whose safety would be threatened by the public release of their voter registration information, such as victims of domestic violence [47]. Most commonly known as an Address Confidentiality Program, voters may request to have a substitute address listed in their record. This is intended to allow participants to vote without fear for their

[5] A pollbook is an official register of people entitled to vote at a given election [42]. It may be paper-based or electronic [43].

[6] Such as the Electronic Registration Information Center (ERIC), a postal service, or a social security entity.

[7] All states, with the exception of North Dakota, require voter registration to vote. [44]

[8] "In many democracies, citizens are automatically registered to vote. The requirement in many states that citizens take the initiative by registering is not only atypical, but also costly to administer." [45]

safety; hence, protecting their private information is critical.

3.1.1 Threats to voter registration databases

Following the 2016 U.S. presidential election, attention has grown towards the security of voter registration databases. U.S. intelligence officials have confirmed that hackers from the GRU, Russia's foreign military intelligence agency, targeted all 50 states' voter registration systems in the run-up to the 2016 election, succeeding in two states, including Illinois [2]. In Illinois, the hackers exfiltrated hundreds of thousands of records — including social security numbers — before being caught. There is no evidence that the hackers modified voter records in these cases; that said, these incidents highlight the importance of securing voter records against surreptitious modification. Threats to the *availability* of voter registration databases may also pose a threat (e.g., preventing election officials from looking up voters on election day).

Additionally, voter registration databases may be subject to *inappropriate list modification* threats. This may include inserting, modifying, or removing voter records without authorization, or for illegitimate reasons. Large-scale illegitimate removal or modification of voter records has sometimes been referred to as *voter purges* [51]. In the U.S., as many states do not implement same-day voter registration, voters who are unaware that their records have changed may be forced to cast a provisional ballot (with less certainty of being counted). Another form of inappropriate list modification may involve surreptitiously adding fake or otherwise ineligible voter records. In practice, this is mitigated by a number of controls, including interstate programs such as ERIC and public transparency of voter registration lists, and numerous studies have found such incidents to be extremely rare [52, 53]. Our framework models inappropriate additions, removals, and other forms of inappropriate list modification.

3.2 Methodology

To construct our model, we began by performing a survey of publicly available documentation of voter registration systems used in the United States, including comprehensive overviews of systems in all fifty states and the District of Columbia via the National Conference of State Legislatures (NCSL) [47, 54, 44, 55, 51, 16, 17, 19, 20, 21].[9] We also reviewed compilations of information on international systems [18, 15, 56, 57, 58, 59, 60].

We also conducted a series of informal discussions with a variety of current and former U.S. elections officials, civil society organizations, and non-profits in the voter registration space. Discussions focused on understanding the voter registration process on the ground, perceived risks, and functional requirements of voter registration, filling in gaps from the available documentation. We then iteratively developed our framework through repeated feedback from these stakeholders to ensure that our models maps usefully and accurately to the real-world application of these systems.

Finally, we conducted several case studies focused on applying our model to Colorado, Ohio, Wisconsin, and Panama to both further validate our models, and provide a worked example of their practical application. These case studies involve states that employ top down (Colorado), bottom up (Ohio), and hybrid databases (Wisconsin) [22], as well as one example (Panama) beyond the U.S. We provide detailed compilations of information for each case study jurisdiction, containing

[9] Though our U.S. analysis mainly focuses on the 50 U.S. states, we note that the District of Columbia and U.S. territories also maintain voter registration lists.

jurisdictional parameters and security policies based on a review of publicly accessible laws, policies, and documentation. For more information, see Section 8.

4 Core Policies, Entities, and Functionalities

This section presents our definitional framework. First, we present definitions of the *types of entities* (Section 4.1) and *core functionalities* (Section 4.2) inherent to most voter registration systems. Then, turning to jurisdiction-specific aspects of voter registration, we define (non-exhaustive) *core parameters* (Section 4.3) and *security policies* (Section 4.4) whose details are determined according to jurisdictional policy. The jurisdictional parameters and policies serve to *instantiate* the core functionality definitions to match with concrete implementation and security needs in a particular jurisdiction.

Later, in Section 6, we present security definitions that build upon the entities, core functionalities, and jurisdictional policies defined in this section.

4.1 Entities

We identify six types of entities that are involved in most voter registration systems. The specific lists of entities that belong in each category will vary between jurisdictions.

We use the term "entity" to encompass individuals, organizations, and hardware/software systems (such as devices or databases). This is a convenient shorthand that is common in the security literature;[10] however, we emphasize that devices, systems, and organizations *do not act of their own accord*, and responsibility for their management and conduct must be ascribed to individuals via well-defined chains of responsibility according to jurisdictional policy (as further discussed in Section 4.4).

- ***Voters:*** People who are legally allowed to cast a vote in the corresponding jurisdiction (possibly limited to particular kinds of elections).[11]
- ***Election infrastructure:*** All entities affiliated with — and controlled by or answerable to — the election office. We highlight three common types of sub-entities:
  - *election officials*, who are responsible for conducting elections, including maintaining the lists of voters and of those who are eligible to vote;
  - *poll workers*, who work for election officials to aid in conducting a specific election, and typically have much more limited expertise, system access, and responsibilities (e.g., confirming voter eligibility in pollbooks and issuing provisional ballots in case a voter's eligibility cannot be determined); and
  - the *voter registration database (VRDB)*, where voter records are stored.

  These sub-categories are non-exhaustive. Election infrastructure systems may be run by the government, external contractors, or a combination of both. Notably, in the U.S., the

[10] The security literature usually uses the term "parties" rather than "entities," but we prefer the term "entities" here in order to avoid confusion with political parties in the elections context.

[11] Some legal systems may define electors as those eligible to vote and voters as those who actually vote. This paper uses the colloquial definition of voter as one who is eligible to vote.

vendor of the VRDB or electronic pollbook often play a significant role in programming and maintaining the systems.[12]

- ***External maintenance entities:*** Entities external to the election office, who work with election officials to maintain voter registration lists. Each jurisdiction has its own list-maintenance strategies, but common external maintenance entities in the U.S. are the United States Postal Service (USPS) via the National Change of Address system (NCOA), a state's Department of Motor Vehicles and Bureau of Vital Statistics, and other states' VRDBs via the Electronic Registration Information Center (ERIC).

- ***Oversight entities:*** Entities external to the election office, who examine voter data or other components of a voter registration system, in order to verify that the voter registration system is operating as intended. There may be three types of oversight entities:

  - ***general*** *oversight entities* who, on their own initiative, examine publicly available information; and
  - ***designated*** *oversight entities* who, on their own initiative, examine non-public information that is available to them because they meet certain general criteria; and
  - ***official*** *oversight entities* who, on request from or under contract with an election office, examine non-public information made available to them for the purpose of a system review or audit.

  Designated and official oversight entities are relatively rare in practice, at least in the United States. Watchdog organizations interested in monitoring voter registration are more common, and can be considered general oversight entities. Definitionally, any member of the public can be a general oversight entity; however, we consider the term useful to refer to those entities that actually *do* (not only *could*) engage in oversight activities.

  Oversight mechanisms *within* the election office are also important: e.g., internal logging, auditing, and accountability procedures. We refer to entities involved in such internal oversight as part of the election infrastructure rather than as separate oversight entities.

- ***Intermediaries:*** All other entities that handle voter registration data at any point during registration, updating registration, proving registration, or maintenance and oversight of a voter registration system. (E.g., an organization like vote.org that helps register voters by mail.)

- ***The public***: All entities, whether listed above or not. (This term is not jurisdiction-specific and includes foreign entities.)

A given entity may fall within multiple of the above categories, depending on the context. For example, USPS serves as a external maintenance entity when aiding states in the process of finding voters who moved out of state, and it can also serve as an intermediary when a voter mails paper registrations to their election official.

[12] For simplicity, and to emphasize our focus on the *functionality* of these systems, we elide other entities that might be involved in voter registration such as the vendors that maintain the VRDB and/or electronic pollbook software.

4.2 Core functionality modules

Next, we define five *modules* that together make up the core functionality of a voter registration system. These modules represent the basic components that our research has found common to most voter registration systems. Real-world voter registration systems can be thought to *implement* these modules while taking into account jurisdiction-specific policy decisions and constraints. Real systems may also contain additional functionalities not described here; our model is intended to be inclusive rather than comprehensive.

The line between the voter registration system and other parts of an election system (e.g., casting and tallying systems) is not clear-cut, as many parts of the broader election system interact with the registration system. For this work, we focus on aspects of election infrastructure that more directly concern registration, as described by the following modules.

- Registration: The processes involved in checking an individual's eligibility to vote when their information is not already in the VRDB, and if they are determined to be eligible, entering their information into the VRDB.
- UpdateRegistration: The processes involved in applying voter-initiated edits to a voter record that is currently present in the VRDB. Note that this includes a voter removing themselves from the VRDB.
- ProveRegistration: The processes involved in determining whether an individual is registered to vote, based on information that the individual presents for this purpose (e.g., when "checking in" at a polling place). This module represents the main goal of a voter registration system.
- Maintenance: The processes involved in election officials (with the aid of external maintenance entities) editing, marking inactive, or removing voter records in the VRDB, without initiation by the concerned voter(s).
- Oversight: The processes involved in oversight entities assessing voter records and identifying discrepancies (such as voters who were incorrectly marked inactive), alerting either the public or election officials.

Section 6 describes each module in much more detail, framed as an interactive protocol parametrized by jurisdictional policies, and defines security properties for each module.

4.3 Jurisdictional parameters

In this section, we outline the core *jurisdictional parameters* of voter registration systems, which describe the variables of voter registration systems that vary across jurisdictions. Many of these parameters result from law or policy decisions that vary by jurisdiction. Jurisdictional parameters could include, but are not limited to, the following:

- p_{elig}: the voter eligibility criteria
- $p_{\text{reg-acts}}$: required actions from the voter in order to register
- $p_{\text{reg-methods}}$: the list of registration methods, such as the DMV, election office, registration website, etc. In particular, those that support automatic voter registration (typically only the DMV) get marked as such

- $p_{\text{voter-info}}$: the types of voter information that are collected and stored
- $p_{\text{freeze-reg}}$: the period before election during which new registrations may not be processed
- $p_{\text{freeze-db}}$: the period before election during which systematic registration removals or maintenance are not allowed
- $p_{\text{keep-logs}}$: the period after an election for which a snapshot and activity logs of the VRDB for that election are kept[13]
- p_{auth}: the voter registration authentication criteria: How voters are authenticated when registering to vote and checking or updating their voter registration record
- $p_{\text{auth(e)}}$: the election authentication criteria (parametrized by an election e)[14], i.e., how voters are authenticated when voting, both in-person and remotely (e.g., this may include checking fields of the VRDB or calling a subroutine to check if a voter has already voted)

We refer to [13] for a thoughtful policy perspective on how to set these parameters. To keep the scope manageable and to separate the technical from the policy aspects, in this paper, we do not suggest specific jurisdictional parameters. Instead, we focus on how to securely implement a voter registration system conditioned on given jurisdictional parameters. Whatever the jurisdictional parameters, secure implementation is an important goal.

4.4 Security policies

In addition to jurisdictional parameters, the rest of the jurisdiction specific details come in the form of *security policies*. A security policy governs the operations of a VRDB that affect its security. In the descriptions below, we outline a few items that would make sense to include in each security policy. We do not aim to provide an exhaustive list of items contained of each security policy: since these are different across jurisdictions, a "complete" description is not possible. Hence, we limit ourselves to a few important elements that serve as examples.

The different types of security policies relevant to voter registration are the following:

1. $\mathbb{P}_{\text{access}}$ denotes the ***access control policy***, which specifies which voter data specific entities may access.[15]
    - Types of voter information that are public
    - Description of which pieces of voter data are available to which entities
    - Whether there is an option to restrict dissemination of certain fields of a voter's information upon application (e.g., for address confidentiality program voters)
2. $\mathbb{P}_{\text{sys-chg}}$ denotes the ***system change control policy***, which specifies how election officials may modify the system, such as changing the system configuration, security policies, and database design.

[13] U.S. Federal law requires voter registration records to be kept for at least 22 months after a federal election [61].

[14] Multiple elections may take place in parallel within the same jurisdiction, so the election authentication criteria must be election-specific.

[15] Unlike the other security policies in this section, access control policies have been extensively studied, see, e.g. [62].

- How often is the system evaluated for upgrades?
- Who needs to grant authorization before a system change?
- What is the specific sequence of steps for implementing a system change?
- What are the backup plans in case parts of the system go down during a system change?

3. $\mathbb{P}_{\text{data-chg}}$ denotes the ***data change control policy***, which governs the changes of voter data, including authorization, execution, and logging.

   - Who needs to authorize a change of voter data?
   - What type of data can be changed?
   - Who triggers a change of voter data?
   - Who actually modifies the voter data?
   - How are such changes logged?

4. $\mathbb{P}_{\text{data-use}}$ denotes the ***voter data use policy***, which specifies guidelines related to uses to which public and non-public voter info can be put.

   - Which pieces of voter data are available for which uses?
   - What use cases are prohibited?

5. $\mathbb{P}_{\text{notif}}$ denotes the ***voter notification policy***, which specifies how jurisdictions notify voters when their data or registration status changes.

   - List of events for which a voter must be notified
   - Protocol by which voters are notified, including the amount of time a voter has to respond to a notification, if necessary, and the resulting action
   - Methods by which voters are notified

6. $\mathbb{P}_{\text{maint}}$ denotes the ***maintenance policy***, which specifies how election officials ensure voter records are accurate and up-to-date.

   - Reasons for which voter registrations may be updated (e.g., change of address), marked inactive (e.g., moved out of state, voter inactivity), or cancelled (e.g., death, incapacity)[16]
   - Specific events or thresholds that trigger such maintenance actions (e.g., time before voter is declared inactive)
   - Data sources used to inform maintenance

7. $\mathbb{P}_{\text{oversight}}$ denotes the ***oversight policy***, which specifies how third parties can review information in the VRDB.

   - Who can oversee which parts of the database
   - How oversight entities authenticate to the election official
   - Level of access given to oversight entities

[16] For a list of maintenance practices by U.S. states, see NCSL's compilation [54].

- Points at which oversight entities may review the VRDB (e.g., pre-election, post-election, continuously)
- How jurisdictions conduct internal audits, including security incident detection and response protocols

In summary, this section introduced the core elements of a voter registration system in the form of functionality modules. We also described the main entities involved, and defined security policies and parameters that enclose the fundamental differences across jurisdictions. In the subsequent sections, we will tie these elements together as we expand on the descriptions of these modules as a function of entities and policies.

5 Threat Model

A *threat model* characterizes the key security threats to a system. Developing a detailed threat model is helpful to design systems resilient to particular threats of interest, and to systematically analyze systems for potential security flaws. No simplified model will capture all possible threats; as such, a threat model should be treated as an essential analytical tool, not as a comprehensive characterization of threats.

Our approach aims broadly to capture the main threats of interest to most voter registration systems. Given the diversity of contexts and system requirements of deployed voter registration systems, threat models are likely to vary by jurisdiction. Some threats will be more important to mitigate in certain contexts than others, whether due to system design, local laws, societal norms, political stakes, specific threat actors, or other factors. When considering a particular jurisdiction's voter registration system security, we encourage a context-specific inquiry into how our basic threat model could be modified to better fit the situation.

We organize the threats that our voter registration framework models into three key categories:

- *Threats on completeness.* Any party being unable to use the voter registration system in a permitted way (e.g., an eligible voter being unable to register).
- *Threats on soundness.* A party being able to use the voter registration system in a prohibited way (e.g., someone registering an ineligible voter).
- *Threats on secrecy.* Any party being able to access information in the voter registration database that they are not permitted to access under the circumstances.

These correspond to the common cryptographic security requirements of *completeness*, *soundness*, and *secrecy*. We provide detailed definitions of completeness, soundness, and secrecy guarantees for voter registration systems in Section 6.6. Each of these three categories can be elaborated into potential threats towards each of the core functionality modules defined in Section 4.2, as summarized in Table 1. Later, in Section 7 we will show how concrete examples of threats (e.g., inappropriate list modification) are instantiations of the threat categories we identify here.

6 Detailed Model and Security Properties

This section provides a detailed modeling of each core functionality module (introduced in Section 4.2) of a voter registration system. First, we specify the categories of interacting entities,

	Registration	Updating registration	Proving registration	Maintenance	Oversight
Completeness	An eligible voter is not able to register.	An eligible, registered voter is not able to update their existing registration.	A registered voter is not given access to the casting process.	A voter's record is flagged for review during a maintenance procedure but the voter is not notified and given a chance to appeal. Or, otherwise unauthorized modifications to voter records are made during VRDB maintenance.	A valid oversight entity is not given access to the information that they are authorized to learn.
Soundness	Someone registers incorrect information or ineligible voters.	Someone updates a record that they are not authorized to update, or with incorrect information.	An ineligible voter is given access to the casting process.	VRDB maintenance routines fail to make timely updates to voter information where flagged and appropriately verified (e.g., change of address).	A party learns information associated with the oversight process which they are not authorized to access.
Secrecy	A party learns information that they are not authorized to access.				

Table 1: **Informal examples of threats to voter registration systems, organized by core functionality modules.**

jurisdictional parameters, and communication patterns inherent to each module. Then, for each module, we enumerate security properties parametrized by jurisdictional security policies.

We model each core functionality module as a simple interactive protocol between entities: e.g., between a voter and the voter registration database (VRDB), possibly via intermediaries. Entities communicate with each other via *communication channels*: e.g., online, mail, or in-person communication. The VRDB can (typically) only be *directly* accessed by election infrastructure entities. Each protocol (i.e., module) is parametrized by relevant entities and communication channels,[17] and takes as input voter data. For example, the registration module is parametrized by T, the entity through whom the voter is registering, and C the channel through which the voter communicates with T, and takes as input some voter data S.

6.1 $\mathsf{Registration}^{T,G}_{C,C',C'',C'''}(S)$

A member of the public, acting either directly by interacting with an election official or communicating via an intermediary, submits an application containing required information. The information is then reviewed by the election official, and if the voter is determined to be eligible and the submitted data determined to be accurate, the election official adds the voter's information to the VRDB. Information about the outcome of this process may then be communicated back to the applicant. Voters may only be permitted to register during certain time periods, as defined in the jurisdictional policy. In detail:

[17] For variables that appear more than once, the apostrophes denote the order in which they are used in the protocol. For example, C' and C'' are two communication channels used in that order.

1. The voter sends some personal information S that contains a signature[18] S' (determined by p_{auth}, $p_{\text{voter-info}}$, and $\mathbb{P}_{\text{access}}$) to an intermediary T (contained in $p_{\text{reg-methods}}$) via a communication channel C (e.g., in-person, mail, or the Internet, as determined by $p_{\text{reg-methods}}$). If registering in person at the election office or via an official web portal, T is empty ($\perp$).

2. If $T \neq \perp$, then T forwards S and S' to an election infrastructure entity G via communication channels C' and C'', respectively. (If $T = \perp$, the voter is communicating their data directly to G.)

3. G verifies that the submitted data meets the criteria outlined in p_{elig}, and that the registration was submitted during an eligible timeframe, as defined in $p_{\text{freeze-reg}}$.

4. G then calls Maintenance (S), i.e., it triggers a subroutine to verify the registration information via third parties (if needed), following the list maintenance protocol defined in Section 6.4 for the specific voter[19].

5. If all checks pass, G stores the voter's data in the VRDB, following the guidelines from $\mathbb{P}_{\text{data-chg}}$. Lastly, G sends a notification N to the voter through a communication channel C''', as outlined in $\mathbb{P}_{\text{notif}}$, confirming that the registration was successful (if unsuccessful, the verification subroutine from the prior step would send a notification to the voter).

The workflow of the Registration module is shown in Figure 1. Note that in practice, registrations may not be sent directly, one at a time, from T to G: e.g., they might be sent in batches instead. Our model captures the basic information flow of the module and omits such implementation details, for clarity of presentation.

6.2 UpdateRegistration$^{T,G}_{C,C',C'',C'''}(I, N)$

In order to update their record, the voter notifies the election official of a desired change, such as a change of address or name. Operating within the data change control policy $\mathbb{P}_{\text{data-chg}}$, the election official authenticates this change and updates the voter's record accordingly.

The workflow of updating a registration is much like that of the registration module defined above, with some small differences: instead of sending all their data in step (1), voters send an identifier I and just their new data N (e.g., a new address); T then uses I to authenticate the voter, and proceeds with the rest of the steps in the registration module. Given its similarity to the Registration module (Figure 1), the workflow of the UpdateRegistration module is not depicted separately.

[18] Here and throughout, we use the term "signature" to refer to information authenticating the voter's identity which is accepted by the relevant jurisdiction as proof of identity for voter registration purposes. This could be a physical ink-based signature or any other voter authentication method used by the system.

[19] The process of verifying voter data during registration is very analogous to the list maintenance process. For example, verifying that a voter's address is correct and checking if a voter changed states may involve processing data from USPS in both cases. Even though the specific information used may change, the high-level behavior of these two processes is similar. For simplicity, we model the verification subroutine as a call to the Maintenance module.

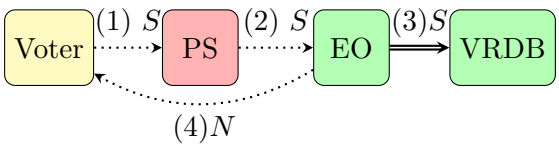

Figure 1: Example Registration flow. Here, T = Postal Service (PS) and G = Election Officials (EO). Dotted and double arrows indicate using mail and internal networks as communication channels, respectively. The call to Maintenance is left implicit.

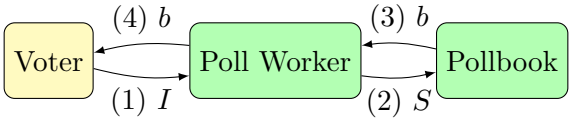

Figure 2: Example ProveRegistration flow. Here, G = Poll Worker and G' = Pollbook. All communication channels are in person.

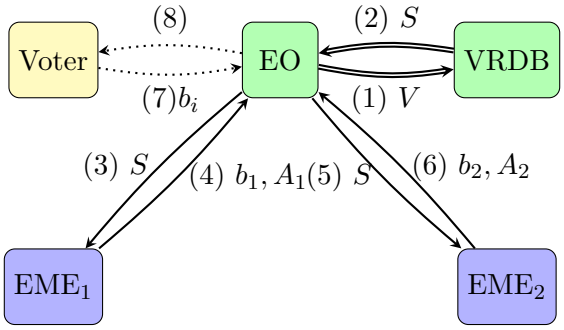

Figure 3: Example Maintenance flow. Here, G = election office, M_1 = Election Maintenance Entity 1 (EME$_1$), and M_2 = Election Maintenance Entity 2 (EME$_2$). Dotted, double, and bold arrows indicate using mail, internal networks, and the Internet as a communication channels, respectively.

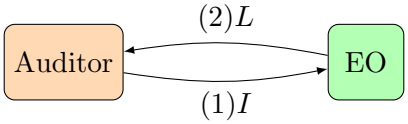

Figure 4: Example Oversight chain. In this case, A = Auditor and G = EO (election officials). All communication channels are the Internet.

6.3 $\mathsf{ProveRegistration}^{G,G',\mathrm{e}}_{C,C'}(I)$

A voter must prove that they are registered to vote (in order to cast a ballot in a particular election e).[20] The voter supplies information in accordance with the election authentication criteria (for election e) to the poll worker, who authenticates the voter and confirms the voter's registration or eligibility in reference to a pollbook or the VRDB. In the case that an election official is unable to confirm a voter's registration, they may provide the voter with a provisional ballot,[21] in which case the voter's registration is validated after the ballot is provisionally submitted. In the case of remote voting, a voter remotely authenticates themselves to the election official, e.g., by providing a signature on the envelope of an absentee ballot. In more detail:

1. The voter sends some identifying information I (determined by $p_{\mathrm{auth(e)}}$ and $\mathbb{P}_{\mathrm{access}}$) to election infrastructure entity G (e.g., a poll worker, election official or a web portal) via a communication channel C.

2. G forwards I (as indicated in $\mathbb{P}_{\mathrm{access}}$) to another election infrastructure entity G' (such as an electronic pollbook or the election office), which verifies if I corresponds to a valid, eligible voter by interacting with the VRDB via a communication channel C' (either an internal network or the Internet) or doing a local check (in the case of a pollbook). The specific authentication checks that take place are outlined in $p_{\mathrm{auth(e)}}$, such as verifying that the voter has not already cast a ballot.

3. G then sends a bit b to the voter through the original channel C; if $b = 1$, the voter proceeds to vote (we treat the vote casting process as outside the scope of voter registration). If $b = 0$, G may provide the voter with a provisional ballot, and the voter's registration is validated after the ballot is cast. After the ballot is received, there may be some other authentication checks (e.g., signature verification in the case of remote voting).

Starting the voting process through mail or the Internet represents requesting an absentee ballot, while in-person represents physically going to the polling center. For the latter, information verification tends to happen with an (e-)pollbook, which either checks the information locally (if the VRDB is downloaded a priori) or contacts the VRDB via the Internet. The workflow of the ProveRegistration module is shown in Figure 2.

6.4 $\mathsf{Maintenance}^{G,\{M_i\}}_{C,\{C_i\},C'}(V)$

Election officials perform maintenance activities on their VRDB. In the United States, certain maintenance is required under the National Voter Registration Act [11]. Maintenance activities may include updating records of voters who have moved and removing ineligible or inactive voters, and often occur based on communication with external maintenance entities. Maintenance activities may be paired with notifications to voters, as determined by the voter notification policy. In more detail:

1. When indicated by $\mathbb{P}_{\mathrm{maint}}$, an election infrastructure party G acquires some information S (following $\mathbb{P}_{\mathrm{access}}$) for a specific voter (specified by an identifier V, e.g., an SSN, following

[20] e is an optional parameter, since a voter may need to prove they are registered to vote outside the context of a specific election.

[21] Provisional ballots are required by federal law in the U.S. [46].

p_{auth}) from the VRDB via a communication channel C (internal network). If the input to the module is the full voter data S itself (in the case of a voter verification subroutine), skip this step.

2. G sends S (following the guidelines of $\mathbb{P}_{\text{access}}$) to zero or more external maintenance entities $M_1, ..., M_n$, defined in $\mathbb{P}_{\text{maint}}$, via communication channels $C_1, ..., C_n$. Each M_i, after doing local checks, replies with a bit b_i (which identifies if, for example, the voter is alive or still at their same address) and some auxiliary data A_i (e.g., the voter's new address). G also performs local checks and replies with a bit b_*, which may be 0, 1, or null (e.g., if no checks are performed).[22]

3. If $b_i = 0$, G updates, marks inactive, or removes the voter from the VRDB via C (following $\mathbb{P}_{\text{data-chg}}$), and sends b_i to the voter via a communication channel C' (i.e., upon seeing $b_i = 0$, the voter knows that their registration got deleted from the VRDB). If $b_i = 1$, G does not do anything. If $b_i = null$ then a *voter-confirmation subroutine* gets triggered in accordance with $\mathbb{P}_{\text{notif}}$: contact the voter some number of times to try to confirm registration info; fails if no response or bad response.

The Maintenance module's workflow is shown in Figure 3. In practice, the maintenance protocol may be non-interactive (e.g., the external maintenance entity simply sends their data to G).

6.5 $\mathsf{Oversight}_C^{A,G}(I, L)$

Oversight entities (as defined by the oversight policy) may access voter data in accordance with the jurisdiction's oversight and access control policies. The oversight entities may assess voter records and identify discrepancies (such as voters who were incorrectly marked inactive), and inform the public and/or election officials of their findings. Election officials may accept the claims and issue corrective actions or refute the claims (ideally, with supporting evidence). Next, we describe this process in more detail for designated or official oversight entities (putting aside general oversight entities since they only access public information, as defined in Section 4.1):

- An oversight entity A sends some identifying information I to an election infrastructure entity G via a communication channel C.
- G checks if the request is coming from a valid oversight entity (as specified in $\mathbb{P}_{\text{oversight}}$), and verifies I. In addition, G also confirms that this oversight entity is allowed to review the database at this point in time, as specified in $\mathbb{P}_{\text{oversight}}$, too.
- If all checks pass, G sends a subset L of the voter registration list (as permitted by $\mathbb{P}_{\text{access}}$ and $\mathbb{P}_{\text{oversight}}$) to A through the original channel C.

The workflow of the Oversight module is shown in Figure 4.

6.6 Security Properties

Next, we present security properties applicable to each of the core functionality modules. As usual, since jurisdictions differ in their voter registration policies, these are a function of the relevant jurisdiction's parameters and security policies.

[22] Such checks may include, for instance, identifying voters who have not voted for a certain period of time.

The three security requirements of *completeness*, *soundness*, and *secrecy* for each module correspond to the three threat types identified in Section 5. Essentially, the security definitions that follow provide a more detailed and formal definition of how a system must behave in order to prevent each of the three threat types, organized by each of the five key functionalities. There is a one-to-one relationship between each of the identified threats and each of the security properties below, representing the fact that each threat represents a violation of the corresponding security property, and, conversely, that mitigating each threat guarantees the corresponding security property.

- Registration
  - ***Completeness:*** An eligible voter possessing the requisite proof of eligibility must be able to register their accurate information in the VRDB only once and only during the periods in which new registrations are allowed, as determined by $\mathbb{P}_{\text{data-chg}}$ in accordance with p_{auth}, p_{elig}, and $p_{\text{freeze-reg}}$.
  - ***Soundness:*** Nobody must be able to register incorrect information or ineligible voters to the VRDB. This is governed by $\mathbb{P}_{\text{data-chg}}$, and assessed by voters (via $\mathbb{P}_{\text{notif}}$), election officials (via p_{elig} and $\mathbb{P}_{\text{maint}}$) and by oversight entities (via $\mathbb{P}_{\text{oversight}}$).
  - ***Secrecy:*** Only entities authorized under $\mathbb{P}_{\text{access}}$ to access (specific types of) information submitted by applicants may learn such information during the registration process.
- UpdateRegistration
  - ***Completeness:*** Any eligible, registered voter must be able to update their existing registration with their correct information, and to delete their VRDB record, subject to $\mathbb{P}_{\text{data-chg}}$ in accordance with p_{auth}.
  - ***Soundness:*** Nobody must be able to (1) update a VRDB record that they are not authorized to update under $\mathbb{P}_{\text{data-chg}}$, or (2) edit any VRDB record to contain incorrect information. As with soundness of registration, this is governed by $\mathbb{P}_{\text{data-chg}}$, and assessed by voters (via $\mathbb{P}_{\text{notif}}$), election officials (via $\mathbb{P}_{\text{maint}}$) and by oversight entities (via $\mathbb{P}_{\text{oversight}}$).
  - ***Secrecy:*** Only entities authorized under $\mathbb{P}_{\text{access}}$ to access (specific types of) information submitted by applicants for updates, and to access (specific types of) VRDB data, may learn such information during the update process.
- ProveRegistration
  - ***Completeness:*** Any registered voter should be given access to the casting process according to p_{auth}.
  - ***Soundness:*** No ineligible voter should be given access to the casting process, according to p_{auth}.
  - ***Secrecy:*** Only entities authorized under $\mathbb{P}_{\text{access}}$ to access (specific types of) VRDB data may learn such information during the process of proving registration.
- Maintenance
  - ***Completeness:*** After a list maintenance update,

    - any VRDB record that a external maintenance entity flags as possibly containing incorrect or incomplete information or corresponding to a person who is not eligible to vote should trigger a voter communication as specified in $\mathbb{P}_{\text{notif}}$, and the voter's record must otherwise remain unchanged;
    - any other VRDB record must remain unchanged in the VRDB; and
    - if a voter notification about a flagged record results in timely voter feedback that demonstrates (in accordance with p_{auth}) that the voter is still eligible, and either confirms the information in the record is correct or provides updated correct information, then the record must remain in the VRDB.
  - ***Soundness:*** After a list maintenance update,
    - any record that all external maintenance entities flag as possibly incorrect or ineligible must be marked as such in the VRDB;
    - any record that an external maintenance entity flags as incorrect or ineligible must have appropriate reasoning in accordance with $\mathbb{P}_{\text{maint}}$ for being flagged as such; and
    - any record flagged by a external maintenance entity as possibly incorrect or ineligible, where the follow-up voter communication does *not* result in timely voter feedback that demonstrates eligibility and correct information must be marked as such in the VRDB in accordance with $\mathbb{P}_{\text{maint}}$, and the voter's record must be preserved.
  - ***Secrecy:*** Only entities authorized under $\mathbb{P}_{\text{access}}$ to access (specific types of) VRDB data may learn such information during list maintenance.
- Oversight
  - ***Completeness:*** Any oversight entity must be able to learn the information that $\mathbb{P}_{\text{oversight}}$ authorizes it to access for oversight purposes. There should be an appeal process in case they cannot do so.
  - ***Soundness/secrecy:*** No oversight entity must be able to learn any information that it is not authorized to access under $\mathbb{P}_{\text{oversight}}$ and $\mathbb{P}_{\text{access}}$.

7 Threat Examples

In this section, we briefly illustrate how the threats described in the introduction can be expressed in terms of the security properties we have defined. These examples are concrete instantiations of the threat categories introduced in Section 5.

Inappropriate list modification. Inappropriate list modification can involve unauthorized additions or modifications to or deletions from a voter registration list.

- ***Additions***. *Invalid voter registrations are submitted and entered into the VRDB.* This violates the soundness of Registration, which states that no ineligible voters may be registered. Such threats may be mitigated by ensuring that p_{elig} is enforced when processing new registrations.
- ***Deletions***. *Voter records corresponding to active eligible voters are removed from the VRDB.* This violates the soundness property of Maintenance: election officials must have a valid

reason for flagging voters in accordance with laws and allow voters who have been incorrectly flagged to remediate. Such threats can be mitigated by flagging voters in accordance with best practices and properly notifying voters.

- ***Modifications***. *Voter data is modified in an unauthorized manner.* This violates the soundness property of UpdateRegistration, which states that no changes to voter data may occur that are not authorized under $\mathbb{P}_{\text{data-chg}}$. Such threats may be mitigated by ensuring that p_{auth} is strong enough when updating voter registration records and consistently enforced, and by ensuring that voters and oversight entities are sufficiently able to monitor for unexpected changes.

Voter data breach. A voter data breach involves the unauthorized access to voter data by any entity. This could be a violation of the Secrecy property of any module. This may be mitigated by ensuring that $\mathbb{P}_{\text{access}}$ adequately protects voter information and that it is adhered to at all steps.

8 Policy Implementations

We demonstrate, using case studies, how our model of voter registration systems (presented in Sections 4 and 6) can be instantiated with concrete jurisdictional parameters to represent a real-world system. We propose a structured table-based format for jurisdictional information and provide case studies for Colorado, Ohio, Wisconsin, and Panama. The tables may be expanded and customized for different jurisdictions; we present just the core components needed to capture the jurisdictional parameters and policies described in Sections 4 and 6. As one illustration, the detailed tables for Colorado are provided in Appendix A. Template tables and complete tables for Colorado, Ohio, Wisconsin, and Panama are available at `https://github.com/cablej/voter-reg-tables/`.

Our definitions encapsulate jurisdiction-specific details in general jurisdictional parameters and security policies. This approach is beneficial to provide a generalized model of features common to most voter registration systems. Then, when analyzing voter registration in a particular jurisdiction, we can fill in the details of these generalized policies and parameters as a function of specific jurisdictional parameters, as illustrated in Table 2.

In conducting the case study, we consulted existing laws, policies, and documentation in each jurisdiction. For instance, in Colorado, Part 5 of Title 1, Article 2 in the Colorado Revised Statutes governs voter registration [63]. As part of a rulemaking process, the Colorado Secretary of State publishes its election rules, of which Rule 2 governs voter registration [64]. Beyond these, we consulted Colorado's voter registration form and technical requirements of its voter registration database [65]. We proceed similarly for the other states and Panama.

In all cases, we were able to complete most information in the policy tables with public information. This suggests that policy tables could either (preferably) be published by the jurisdiction itself, and/or be constructed independently by the public.

By conducting case studies across multiple states, we can begin to observe differences between jurisdictions. As each state operates a different type of database — Colorado uses a top-down database, Ohio uses a bottom-up database, and Wisconsin uses a hybrid database [22] — some differences are inevitable. Wisconsin's tables rely heavily on municipal election officials, of which there are more than 1,800 local clerks [66], who must consistently enforce state law and policy. Likewise, there are notable differences in the access control policy for the state VRDBs. For

p_{elig}	U.S. Citizen, resident of Colorado for at least 22 days, at least 16 years old, and not serving felony sentence
$p_{\text{reg-acts}}$	None (for automatic voter registration), otherwise submit voter registration application
$p_{\text{reg-methods}}$	Online, email, fax, mail, in person
$p_{\text{voter-info}}$	See access control policy table
$p_{\text{freeze-reg}}$	8 days before election (mail/online), up to and on election day (in person). County election officials may choose to process registrations submitted later than 8 days.
$p_{\text{freeze-db}}$	N/A
$p_{\text{keep-logs}}$	At least 2 years
p_{auth}	Updating record: Date of birth/driver's license number or last 4 digits of social security number, signature. Looking up record online: Name, zip code, birthday
$p_{\text{auth(e)}}$	Checking in at pollbook: 1 form of ID Vote by mail: signature, if first time may need to provide copy of ID

Table 2: **Jurisdictional parameters for Colorado.**

instance, voter email addresses and phone numbers are available to the public in Wisconsin, while only phone numbers are available in Colorado, and neither in Ohio.

We hope that organizing jurisdictional information in the structured form that we propose, as demonstrated via these case studies, may be helpful in order to:

- specify detailed jurisdictional-specific *threat models* for voter registration systems, which is helpful for security analyses and research;
- organize voter registration policy information for *convenient comparison* between jurisdictions, and learn about common and uncommon approaches;
- enhance *transparency* of voter registration systems, thereby promoting civic engagement and accountability;
- *identify strengths and weaknesses* of a particular jurisdiction's approach to voter registration security, which can inform where to focus resources for improvement;
- *identify underspecified aspects* of a particular jurisdiction's voter registration policies;
- *identify mismatches* between a jurisdiction's stated policies and its implementation of voter registration; and
- *encourage constructive dialogue* between election officials and the security research community regarding details of voter registration systems that are important to security analyses and research.

International case study: Panama. Our model of voter registration is general enough to encompass the systems of many other countries. We give one example of our framework's generality by showing how it can be instantiated with Panama's parameters.

Panama has public documentation outlining many of their procedures and practices, in a manner that corresponds remarkably well with our framework. As such, Panama's example could be viewed

as a positive indication of the realism of election officials publicizing detailed jurisdictional voter registration parameters as we advocate.

In Panama, general elections occur once every 5 years, when the vast majority of public officials are elected. Unlike the U.S., Panama's voter registration system is at the national level instead of at lower jurisdictional levels. The Tribunal Electoral, Panama's main entity in charge of electoral matters, issues identity cards to all adult (18+) citizens, which is the only process by which nationals are added to the electoral registry. Then, it is each citizen's responsibility to inform the relevant authorities of changes to their address, name, or other relevant details. As such, there is no routine and extensive list maintenance at the scale of voter registration maintenance in the U.S. That said, more limited maintenance operations are performed based on the national census and some other corner cases (e.g., using a public service that requires declaration of residence). Finally, voters are removed (after a notification) from the electoral registry if they fail to vote in three consecutive general elections or do not participate in any processes (related to voting or not) through the Tribunal Electoral.

We outline Panama's jurisdictional parameters and policies at `https://github.com/cablej/voter-reg-tables/blob/main/panama.md`. We constructed these primarily based on public documentation available on the Tribunal Electoral's website, particularly the Código Electoral (CE) [56] (the main code of law for the Tribunal Electoral), confirmed by informal consultations with Panamanian nationals. Interestingly, Panama has public documentation outlining the specific steps that must be followed to make system changes, the most notable of which are the procedure manuals of the Infrastructure Management [67] and the Information Security Management [68]. Thus, this represents their specific implementation of the ***system change control policy***. We omitted an independent construction of this table for Panama, as it is covered by these documents.

9 Critical Questions

In this section, we propose questions that policymakers, election officials, security practitioners, and researchers may wish to ask to evaluate candidate systems. We categorize our questions with respect to our varying policies presented above. We note that this list is incomplete; our goal is for these questions to help foster discussion and in-depth evaluation of proposed and already deployed systems.

- ***General questions:***
  - Main question: **is there a (security) mechanism enforcing each item of every security policy?**
  - Who is responsible and/or accountable for maintaining each security property?
  - Is the voter registration system compatible with (1) the jurisdiction's expressed policy choices? (2) the framework's rigorous security definitions?
  - Are there undefined or incomplete portions of any policies?
  - Do the policies completely encompass how the voter registration system should work?
  - Is the voter registration database regularly audited to ensure that the policies outlined are enforced programmatically?
  - Are there reliability mechanisms in place in case any of the security policies gets violated?

  - How might external developers, researchers, and government agencies help improve the system?
  - Are there security mechanisms in place to enforce the security properties of each module?

- ***Access control policy:***
  - Is the access control policy in compliance with laws regulating voter data access?
  - Are there fields of voter data that are made accessible to third parties even though they are not required to by law?
  - Does the access control policy follow the *principle of least privilege*?

- ***System change control policy:***
  - Are system changes regularly audited to ensure that no unauthorized changes have been made?
  - Is the system change control policy followed every time there is a system change?
  - Does the system change control policy follow the *principle of least privilege*?
  - Is the system (including security policies) constantly evaluated for potential updates?

- ***Data change control policy:***
  - Are changes to voter data regularly audited to ensure that no unauthorized changes have been made?
  - Is there sufficient logging (at the application, network, and operating system level) to determine who made a change in the case of an unauthorized change being detected?
  - Is the data change control policy followed every time data gets changed?
  - Are there enough reliable backups of the VRDB in case voter data gets tampered with?

- ***Voter data use policy:***
  - How are third parties assessed and held accountable for incorrect uses of voter data?
  - Is there a rigorous evaluation process to authorize external entities to use non-public voter data, if applicable?
  - Are voters given the option to opt-out of their data being used for specific purposes, especially if it would threaten their safety?

- ***Voter notification policy:***
  - Is there enough redundancy in the notifications sent to voters in case they missed the first one(s)?
  - Is the notification policy working in harmony with the data change control policy and the maintenance policy?
  - Are replies from voters processed in an efficient and timely manner?

- ***Maintenance policy:***

  - What transparency practices are in place to allow third parties to audit maintenance activities?
  - Is voter data verified in-depth when maintenance activities indicate it should be removed/updated?
  - Are state-of-the art maintenance technologies like ERIC being used?
  - Are external maintenance entities (e.g. ERIC or other states) regularly assessed for correct behavior?

- ***Oversight policy:***
  - Is external oversight encouraged and advertised?
  - Is there a proper channel through which oversight entities can notify election officials of suspected irregularities?
  - Is there a timely and well-defined procedure to investigate and resolve potential irregularities found by oversight entities?

10 Conclusion

We provide the first systematic formalization of *voter registration systems* as they exist today. We define the entities and core functionalities inherent in most voter registration systems, the jurisdictional policies that constrain specific implementations, and key security properties. As a tool for adapting our general definitions to specific jurisdictions and implementations, we provided a series of tables organizing jurisdiction-specific policy information, illustrated with case studies of three U.S. states and Panama. Finally, we offer a list of critical questions.

Though voter registration is a fundamental part of secure elections, it is often comparatively understudied. One contributing factor may be the lack of detailed understanding of problem definitions, practical constraints, and security issues. Precise threat modeling and security definitions have long been an essential foundation of secure system design: as such, we hope that our work will promote the study, development, and adoption of more secure voter registration systems.

Acknowledgments

We are grateful to Jared Dearing, Joseph Lorenzo Hall, Jennifer Morrell, Ronald L. Rivest, and Trevor Timmons for helpful discussions, and to our anonymous reviewers for helpful feedback. Sunoo Park's research was supported by a 2021–22 Computing Innovation Fellowship under National Science Foundation grant #2127309 to the Computing Research Association, and by Cornell Tech's Digital Life Initiative.

References

[1] Statement by Secretary Jeh Johnson on the designation of election infrastructure as a critical infrastructure subsector. `https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical`, Jan 2017.

[2] Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf, 2019.

[3] James Temperton. The Philippines election hack is 'freaking huge'. https://www.wired.co.uk/article/philippines-data-breach-fingerprint-data, April 2016.

[4] Ivan Martin. It firm C-Planet fined €65,000 over massive voter data breach. https://timesofmalta.com/articles/view/it-firm-c-planet-fined-65000-over-massive-voter-data-breach.92848, Jan 2022.

[5] Software glitch discloses Wokingham edited electoral register. https://www.bbc.com/news/uk-england-berkshire-27304885, May 2014.

[6] Three Welsh councils' electoral roll data breaches probed. https://www.bbc.com/news/uk-wales-south-east-wales-27159648, April 2014.

[7] Dustin Volz. Iran probed state election websites since September, U.S. says. https://www.wsj.com/articles/iran-probed-state-election-websites-since-september-u-s-says-11604104649, 2020.

[8] Diego Ongaro and John Ousterhout. In search of an understandable consensus algorithm. In *2014 USENIX Annual Technical Conference (Usenix ATC 14)*, pages 305–319, 2014.

[9] Ben Laurie. Certificate transparency. *Communications of the ACM*, 57(10):40–46, 2014.

[10] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[11] National Voter Registration Act of 1993, 1993.

[12] National Academies of Sciences, Engineering, and Medicine. Securing the vote: Protecting American democracy, 2018. Consensus Report.

[13] Association for Computing Machinery. Statewide databases of registered voters: Study of accuracy, privacy, usability, security, and reliability issues commissioned by the U.S. public policy committee of the association for computing machinery, 2006.

[14] Carter Casey, Johann Thairu, Susie Heilman, Susan Prince, Brett Pleasant, and Marc Schneider. Recommended security controls for voter registration systems. https://www.mitre.org/sites/default/files/publications/pr-19-3594-recommended-security-controls-for-voter-registration-systems.pdf, December 2019. Report, MITRE Corporation.

[15] ACE Electoral Knowledge Network. Voter registration. https://aceproject.org/ace-en/topics/vr.

[16] Justin Levitt, Wendy R. Weiser, and Ana Muñoz. Making the list: Database matching and verification processes for voter registration. https://www.brennancenter.org/our-work/research-reports/making-list-database-matching-and-verification-processes-voter, 3 2006. Report, Brennan Center for Justice at NYU Law.

[17] Wendy Weiser, Michael Waldman, and Renée Paradis. VoterRegistrationModernization: PolicySummary, 2009. Report, Brennan Center for Justice at NYU Law.

[18] Jennifer S. Rosenberg and Margaret Chen. ExpandingDemocracy:VoterRegistrationAroundtheWorld, 2009. Report, Brennan Center for Justice at NYU Law.

[19] Christopher Ponoroff. Voter registration in a digital age. https://www.brennancenter.org/sites/default/files/2019-08/Report_Voter-Registration-Digital-Age.pdf, 2010. Report, Brennan Center for Justice at NYU Law.

[20] Holly Maluk, Myrna Pérez, and Lucy Zhou. Voter registration in a digital age: 2015 update. https://www.brennancenter.org/our-work/research-reports/voter-registration-digital-age-2015-update, 2015. Report, Brennan Center for Justice at NYU Law.

[21] Election Assistance Commission. Voluntary guidance on implementation of statewide voter registration lists. https://www.eac.gov/sites/default/files/eac_assets/1/1/Implementing%20Statewide%20Voter%20Registration%20Lists.pdf, July 2005.

[22] Election Assistance Commission. Statewide voter registration systems. https://www.eac.gov/statewide-voter-registration-systems, Aug 2017.

[23] National Research Council of the National Academies of Sciences, Engineering, and Medicine. State voter registration databases: Immediate actions and future improvements. https://www.eac.gov/sites/default/files/document_library/files/State_Voter_Registration_Databases_-_Interim_Report.pdf, 2008. Interim Report.

[24] Center for Election Innovation and Research. Voter registration database security. https://electioninnovation.org/wp-content/uploads/2020/08/2020_VRDB_Security_Report.pdf, Aug 2020.

[25] Center for Internet Security. A handbook for elections infrastructure security. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf, Feb 2018.

[26] Belfer Center for Science and International Affairs at Harvard Kennedy School. The state and local election cybersecurity playbook. https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf, 2018.

[27] Sam van der Staak and Peter Wolf. Cybersecurity in elections: Models of interagency collaboration. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf, 2019. International Institute for Democracy and Electoral Assistance.

[28] Louis-Henri Merino, Simone Colombo, Jeff Allen, Vero Estrada-Galiñanes, and Bryan Ford. TRIP: trustless coercion-resistant in-person voter registration. *CoRR*, abs/2202.06692, 2022.

[29] Jian Cao, Seo young Silvia Kim, and R. Michael Alvarez. Bayesian analysis of state voter registration database integrity. *Statistics, Politics and Policy*, 13(1):19–40, 2022.

[30] Electronic Registration Information Center. https://ericstates.org.

[31] VoteShield. https://voteshield.us.

[32] Ben Adida. Helios: Web-based open-audit voting. In Paul C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 335–348. USENIX Association, 2008.

[33] Ronald L. Rivest. On the notion of 'software independence' in voting systems. *Philosophical Transactions of the Royal Society*, 366:3759–3767, 2008.

[34] Susan Bell, Josh Benaloh, Michael D. Byrne, Dana Debeauvoir, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. STAR-Vote: A secure, transparent, auditable, and reliable voting system. In *2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13)*, Washington, D.C., August 2013. USENIX Association.

[35] Josh Benaloh, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, and Poorvi L. Vora. End-to-end verifiability. *CoRR*, abs/1504.03778, 2015.

[36] Mark Lindeman and Philip B. Stark. A gentle introduction to risk-limiting audits. *IEEE Secur. Priv.*, 10(5):42–49, 2012.

[37] Josh Benaloh, Douglas W. Jones, Eric Lazarus, Mark Lindeman, and Philip B. Stark. SOBA: secrecy-preserving observable ballot-level audit. In Hovav Shacham and Vanessa Teague, editors, *2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '11, San Francisco, CA, USA, August 8-9, 2011*. USENIX Association, 2011.

[38] Mark Lindeman, Philip B. Stark, and Vincent S. Yates. BRAVO: ballot-polling risk-limiting audits to verify outcomes. In J. Alex Halderman and Olivier Pereira, editors, *2012 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '12, Bellevue, WA, USA, August 6-7, 2012*. USENIX Association, 2012.

[39] Barbara Simons. Why internet voting is dangerous. *Georgetown Law Technology Review*, 4:543–563, 2020.

[40] Sunoo Park, Michael A. Specter, Neha Narula, and Ronald L. Rivest. Going from bad to worse: from internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1), 2021.

[41] From voter registration to mail-in ballots, how do countries around the world run their elections? https://www.pewresearch.org/fact-tank/2020/10/30/from-voter-registration-to-mail-in-ballots-how-do-countries-around-the-world-run-their-elections/, 2020.

[42] Merriam-Webster Dictionary. Pollbook. https://www.merriam-webster.com/dictionary/pollbook [https://perma.cc/7D58-GYQB].

[43] National Conference of State Legislatures. Electronic poll books, Oct 2019. https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx [https://perma.cc/G4YJ-7DCD].

[44] National Conference of State Legislatures. Automatic voter registration. https://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx, Jan 2022.

[45] Douglas W. Jones and Barbara Simons. *Broken Ballots*. Center for the Study of Language and Information, 2012. pg. 243.

[46] The Help America Vote Act of 2002, 2002.

[47] National Conference of State Legislatures. Access to and use of voter registration lists. https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx, Aug 2019.

[48] North Carolina State Board of Elections. Voter registration data. https://www.ncsbe.gov/results-data/voter-registration-data.

[49] Maine Department of the Secretary of State. Voter registration data, election data and online forms. https://www.maine.gov/sos/cec/elec/data/index.html.

[50] Commercial voter files and the study of U.S. politics. https://www.pewresearch.org/methods/2018/02/15/commercial-voter-files-and-the-study-of-u-s-politics/, Feb 2018.

[51] Jonathan Brater, Kevin Morris, Myrna Pérez, and Christopher Deluzio. Purges: A growing threat to the right to vote. https://www.brennancenter.org/sites/default/files/2019-08/Report_Purges_Growing_Threat.pdf, July 2018.

[52] Sharad Goel, Marc Meredith, Michael Morse, David Rothschild, and Houshmand Shirani-Mehr. One person, one vote: Estimating the prevalence of double voting in U.S. presidential elections. *American Political Science Review*, 114(2):456–469, 2020.

[53] Lorraine Minnite. Election day registration: A study of voter fraud allegations and findings on voter roll security. https://www.brennancenter.org/sites/default/files/analysis/edr_fraud.pdf, 2007.

[54] National Conference of State Legislatures. Voter registration list maintenance. https://www.ncsl.org/research/elections-and-campaigns/voter-list-accuracy.aspx, Oct 2021.

[55] National Conference of State Legislatures. Same day voter registration. https://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx, Sept 2021.

[56] Código Electoral de Panamá. https://www.tribunal-electoral.gob.pa/publicaciones/codigo-electoral/, 2022.

[57] GOV.UK. Register to vote. https://www.gov.uk/register-to-vote.

[58] Law Commission of England and Wales and Scottish Law Commission. Electoral law: A joint final report, 2020.

[59] Service-Public.fr. Listes électorales : nouvelle inscription. https://www.service-public.fr/particuliers/vosdroits/F1367, 2022.

[60] Le ministre de l'intérieur. Instruction relative à la tenue des listes électorales complémentaires. https://www.eure.gouv.fr/content/download/29070/193726/file/circulaire%20minist%C3%A9rielle%20du%2021%20novembre%202018.pdf, 2018.

[61] 52 USC 20701: Retention and preservation of records and papers by officers of elections; deposit with custodian; penalty for violation.

[62] Donald C Latham. Department of Defense trusted computer system evaluation criteria. *Department of Defense*, 1986.

[63] Colorado Revised Statutes 2021 Title 1, 2021.

[64] Colorado Department of State. Election Rules [8 ccr 1505-1]. https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule2.pdf, 2021.

[65] Colorado Department of State. Statewide voter registration system requirements. https://www.sos.state.co.us/pubs/elections/SCORE/files/systemrequirementsv10.doc, 2006.

[66] About the WEC. https://elections.wi.gov/about-the-wec, 2022.

[67] Procedimiento Gestión para la Seguridad Informática. https://www.tribunal-electoral.gob.pa/wp-content/uploads/2021/11/Proc.-Gral.-Gestio%CC%81n-para-la-Seguridad-Informatica-Enero-2021.pdf, June 2018.

[68] Procedimiento General Gestión de Infraestructura. https://www.tribunal-electoral.gob.pa/wp-content/uploads/2020/07/Proc.-Gral.-Gesti%C3%B3n-de-Infraestructura.pdf, January 2021.

A Tables for Colorado case study

Category	Entity	Name	Home address, Mailing address	Birth year	Birth day	Phone	Email	Driver's License/ ID card number	SSN last four digits	Party, Affiliation date, Gender	Signature	Voting activity history
REGISTER/ UPDATE	Voter being registered	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VRDB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Online registration/update portal	✓	✓*	✓	✓	✓*	✓	✓	✓	✓	✓	✓
	NVRA agency (e.g., DMV)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	County clerk	✓	✓†	✓	✓	✓†	✓	✓	✓	✓	✓	✓
USE REG TO VOTE	County official (polling place)	✓	✓†	✓	✓	✓†	×	✓	×	✓	✓	×
	County official (mail-in ballots)	✓	✓†	✓	✓	✓†	×	✓	×	✓	✓	×
LIST MAINTENANCE	NCOA	×	×	×	×	×	×	×	×	×	×	×
	Department of Revenue	×	×	×	×	×	×	×	×	×	×	×
	ERIC	✓	✓	✓‡	✓‡	✓	✓	✓‡	✓‡	×	×	✓
TRANSPARENCY	The public	✓	✓*	✓	×	✓*	×	✓	×	✓	×	✓

Table 3: **Colorado Access Control Policy.** The access control policy determines which entities can access certain fields. We represent the access control policy as a table that maps entities to registration fields, with binary values in each cell denoting whether the entity in that row is allowed to view the data point in that column, for any voter.
*Hidden for address confidentiality program voters
† only accessible by designated address confidentiality program election staff
‡ hashed before sending to ERIC

For the **system change control policy**, Colorado does not publish information related to the system change control policy. See `https://github.com/cablej/voter-reg-tables/` for a template table. This policy specifies all guidelines that must be followed when making meta changes to the voter registration system. We represent the system change control policy as a table that maps "types of changes" to stages of a change's lifecycle. Each cell specifies the directives that are in place at a particular stage of a (type of) change.

Oversight entity	Voter data	VRDB logs	VRDB code	Interactive access	Time periods
Nonprofit	Yes, as public in accordance with access control policy	No	No	No	Continuously
Political organization	Yes, as public in accordance with access control policy	No	No	No	Continuously
Third party pentester	No	Yes	Yes	Yes	Over 90 days before election
VoteShield	Yes, as public in accordance with access control policy	No	No	No	Continuously
Department of State	Yes	Yes	N/A	N/A	Continuously

Table 4: **Colorado oversight policy.** The oversight policy governs how third parties can review information in the VRDB. We represent the oversight policy as a table mapping oversight entities to the type of voter data and other information they can access, along with time periods for oversight.

Category	Entity	Type of Data
AUTHORIZATION	Voter	Personal data
	State and county election officials	Data from list maintenance update
TRIGGER	Online update portal	Data from voter who started update
	Mail	Data from voter who started update
	ERIC	Data of voters in other states
	Department of Revenue (DMV)	Data of new/updated license
	Other NVRA agency	Data of new voter
	NCOA	Data of voter move
	Department of Public Health and Environment, Social Security Death Index	Data of death
	Colorado Department of Corrections, Colorado U.S. Attorney's office	Voters who committed crime
EXECUTION	State election officials	
	County election officials	

Table 5: **Colorado data change control policy.** The data change control policy includes information about the entities involved in updating the VRDB or associated policies. We represent the data change control policy as a table that specifies the entities allowed to authorize/start updates, trigger updates (send updated data to election officials), and execute the update (directly modify the data inside the VRDB). In this table, we map these entities to the type of data they update, and if there is a notification involved in this type of update.

Prohibited uses	Not specified
Approved entities	Public
Information released	See access control policy table
Opt out policy	Address Confidentiality Program (ACP) participants

Table 6: **Colorado voter data use policy.** The voter data use policy specifies limitations on how (and by whom) the data can be used. We represent the voter data use policy following the structure of [47].

Notification reasons	Notification protocol	Notification methods
Incomplete registration	Send notice via notification methods	Mail, Email (by county)
New registration	Send notice via notification methods. If returned as undeliverable, do not register. If not returned as undeliverable, register.	Mail, Email (by county)
Inactive registration	Send elector voter confirmation card at least 60 days before election via notification methods. If not returned or not marked undeliverable, and voter has not voted in two general elections, cancel registration.	Mail, Email (by county)
Address change	Send notice to new address.	Mail, Email (by county)
Cancelled registration	None	N/A

Table 7: **Colorado voter notification policy.** The voter notification policy governs how jurisidictions notify voters of various changes to their records. We represent the voter notification policies as a table mapping notification reasons to notification protocols and methods.

Reason	Data source	Threshold	Action
New driver's license or updated address	Department of Revenue	New driver's license or updated address	Register voter or update existing record
Moved in state	NCOA	Address changes in state	Update address
Moved out of state	NCOA / ERIC	Address changes out of state	Mark inactive – NCOA
Returned mail	County	Returned mail	Mark inactive – returned mail
Undeliverable ballot	County	Ballot could not be delivered	Mark inactive – undeliverable ballot
Voter inactivity	VRDB	Has not voted in past two elections	Mark inactive; cancel reg after two more inactive elections
Death	Dept. of Public Health and Env., Social Security Death Index	Voter dies	Cancel registration - deceased
Crime	Dept. of Corrections, CO U.S. Attorney's office	Voter currently incarcerated for a felony conviction	Cancel registration - convicted felon

Table 8: **Colorado maintenance policy.** The maintenence policy governs how jurisdictions keep their VRDB accurate and up-to-date. We represent the voter maintenance policy as a table mapping maintenance reasons and their associated data sources to maintenance thresholds and actions.