Memorandum

To: Honorable Members, Rules Committee, San Francisco Board of Supervisors

From: John Arntz, Director

Date: May 10, 2024

RE: File No. 240029 Report in advance of hearing on impact of artificial intelligence in local elections

---

The Department of Elections (Department) is providing this memorandum in response to Supervisor Preston's request that the Department report on artificial intelligence (AI) in local elections.

The Department acknowledges the concern regarding the application of AI to potentially negatively impact an election or election-related processes such as voter registration, voting, and results reporting. As the November 2024 election approaches, the Department continues to consider methods to identify and then mitigate potential negative AI-related impacts on the integrity of the election.

Although AI may bring new concerns regarding the interference with the conduct of an election, the Department along with many state and federal agencies have been collaborating for several years on safeguarding elections. AI-related issues are now becoming incorporated into this joint effort to ensure elections are conducted in a manner that are free, fair, and functional.

While the Department remains steadfast in safeguarding the integrity of the City's elections, the Department has no legal authority to monitor or regulate campaign speech. This means the Department focuses on preserving the integrity of election processes and voting, and issues that may rupture voters' or the public's trust in the conduct or the outcome of an election. Should the Department become aware of false or misleading campaign speech the Department's recourse would be to report such instances to other agencies.

This memorandum provides an overall summary of the safeguards the Department has implemented and is considering regarding election security both in relation to AI and to the overall integrity of the election processes and voting system. The four areas discussed are 1) the Department's collaboration with several state, federal, and local agencies that monitor possible AI- and cyber-related threats and that organize coordinated responses to such threats, 2) a description of some of the Department's efforts to identify possible misinformation and the response protocols the Department would follow, 3) an overview of the type of content included in the Department's voter outreach efforts and published materials to provide voters with trusted information, 4) the Department's review and expansion of its social media guidelines and messaging that more explicitly highlights the Department's content as being trusted sources of election information, and, 5) an overview of the security protocols and actions the Department follows to safeguard the voting system

1. Collaboration with State, Federal and Local Agencies

The Secretary of State's Office (SOS) established its Office of Elections Cybersecurity (OEC) to support county election officials in defending against cyber-related threats. This support occurs through the OEC's focus on coordinating efforts between the SOS and local election officials to expand cyber-attack prevention capabilities and establish improved cyber incident responses. The OEC also collaborates with a number of federal, state, and local partners – including the Department of Homeland Security, the Federal Bureau of Investigation (FBI), the Attorney General's Office, the CA

Department of Technology, the CA Office of Emergency Services, the California Highway Patrol, and county elections officials – to share election security information and best practices and monitor and counteract false or misleading information.

As part of this coordinated effort, the OEC responds to reports of attempts to propagate election-related misinformation at **VoteSure@sos.ca.gov** and the Department encourages people to use the address for reporting any AI- or cyber-related concerns affecting elections. Similarly, the Department collaborates directly with both the FBI and OEC to report any false election related information and to prevent election interference and the spread of false claims in the City and County of San Francisco. The Department has also established contacts with local law enforcement entities, including the District Attorney's Office, to report any false and misleading election information meant to create distrust in election processes or undermine the integrity of San Francisco elections. Additionally, the Department can amplify its messaging through local media and community leaders should it be necessary to circulate information to the public regarding an election or its conduct.

2. Information Evaluation and Response Protocols

Relatedly, the Department has developed protocols for monitoring its own social media accounts so that personnel can better identify false or misleading election information, respond to false claims, and to further escalate any possible instances. The Department is preparing to implement a social media management tool with a monitoring feature to further alert Department personnel about the possible mis-use of relevant election-related words mentioned in public social media posts.

Further, when the Department becomes aware of a possible incident involving Mis-, Dis-, or Mal-information (MDM), the Department will activate its MDM Evaluation and Response Plan (see Attachment A). By developing and following this plan, which focuses primarily on broadcasting accurate information to the public, the Department seeks to appropriately respond to or curb the effects of information adverse to the integrity of the election.

Also attached to this memorandum are two examples of how the Department's homepage may appear should it become aware of an action or incident adverse to an election. The Department's website provides a widely available format and promptly posting information on the homepage, following the issuance of a press release, is an effective and low-barrier method to inform the public on election matters.

The homepage example in Attachment B considers a scenario that rises to 'Level 2' in the Department's MDM Evaluation and Response Plan. In response, the Department would place a noticeable alert-style banner on the homepage, with a link to more information about the incident.

Attachment C contemplates a potential 'Level 3' incident, where a deepfake video with serious voter-suppression implications is circulating on social media three days before the November 2024 election. In this situation, the Department's site would include a graphic clarifying that voting continues through Election Day, an acknowledgment that the Department is aware of the situation, and a link to more information about all the steps the Department is taking. In these situations, the Department would focus on providing the accurate information first, before explaining details of the incident, which could have the unintended consequence of elevating the misinformation.

3. Providing Accurate and Trusted Election Information

The Department consistently provides voters with accurate information before and during every election cycle. Voter education and outreach on election related topics, including information on the Department's implementation of steps to protect the conduct of local elections. Before each election, the Department develops multilingual, multiformat outreach strategies intended to maintain the Department's presence as a trusted source of accurate election-related information. The strategies are comprised of numerous print and digital materials, presentations at live and virtual events, regular postal notices, placement of newspaper ads, broadcasting of public service announcements via television and radio, regularly updated copy on *sfelections.gov* and social media channels, and the issuance of press releases and public notices.

The Department is developing content in its outreach presentations that alerts voters in identifying reliable election-related information. Department personnel provide a multilingual presentation at community events and distribute it to hundreds of local outreach partners (e.g., community-based organizations, government agencies). The informational presentation will include slides 1) advising San Francisco voters and other interested parties to be informed by being vigilant about all the election information they consume and share on social media; 2) encouraging viewers to check all election information against official sources, and 3) asking them to report any suspected false or misleading information regarding voter registration, election-related processes, or the Department's operations to both the source medium (e.g., Facebook, TV news) and to the Department of Elections. This presentation will encourage viewers to sign up to receive official news, updates, and public notices from the Department.

The Department recently developed an informational brochure, *San Francisco Elections: Safe and Secure,* that describes some of the key security measures protecting voter registration data, vote-by-mail ballots, voting technology, and elections results reporting processes. The brochure also describes key ballot processing security measures, including the post-election canvass which the Department undertakes to audit election materials and to verify and validate election results. The brochure references several transparency-related polices that the Department follows to increase the public's understanding of election processes. This further highlights that the Department's digital and hard copy materials are the best, trusted source for election-related information, and encourages voters to sign up to receive official news, updates, and public notices from the Department at ***sfelections.gov/trustedinfo***.

The Department has also created a page on the topic of election security at ***sf.gov/election-security***. This page provides an overview of the Department's actions to ensure the integrity of elections in San Francisco. The webpage highlights rules and protocols the Department follows to protect voting systems and technology, and to protect voter data and ballots. The page is organized according to current concerns regarding election integrity and security and provides short statements responsive to specific topics. For example, the Department realizes people may have concerns that the Accessible Vote-by-Mail system allows for "online voting." The response to this concern explains that the system only allows locally registered voters to receive a PDF of their ballot which voters must then print, mark, and either mail or otherwise return this hard copy ballot to the Department for counting.

The Department receives inquiries from members of the public regarding election processes, in particular during the voting period for an election. Department staff will continue to manually review and respond to all inquiries the Department receives to provide accurate and relevant information to voters and the public. Further, the Department does not intend to utilize automated systems such as "chatbots" to review inquiries or generate automated responses using AI. Additionally, the Department continues to provide materials and information in non-English languages that have been translated by staff or trusted vendors. The Department does not intend to utilize AI machine translations (e.g. Google Translate) to develop translated documents for public consumption. This practice helps ensure that all information disseminated to the public by the Department is accurate, consistent, and accessible to both English and non-English speakers.

Although the Department is the official source for nonpartisan election information, the Department realizes that voters may use unofficial sources for election-related information. The Department is monitoring updates on AI-related instances that might affect elections and considering resources that can eventually be used by the Department or even the public to detect manipulated media. With this in mind, the Department is determining if tools are available that could assist members of the public in identifying possible misinformation such as "deepfakes". An example of such tools is **detect.resemble.ai** which allows users to drop a file into the site for analysis.

4. Expanded Social Media Guidelines and Topical Messaging

The Department has implemented *Social Media Access and Use Guidelines* for personnel to follow. The purpose of the *Guidelines* is to ensure voters continue to rely on the Department's social media sites to obtain trusted election-related content. These guidelines require personnel to review and approve all content prior to posting, and only personnel authorized by the Director or Deputy Director have access to the sites to post the content. These steps also protect the Department's social media accounts from third-party interference since access is closely monitored and restricted.

These guidelines require personnel to utilize strong passwords and multi-factor authentication; limit the posting of external links to the Department's social media sites; limit "friending" or "following" to reduce the risk of leading readers to inaccurate information; prohibit the posting of unapproved videos or pictures, restrict reposting or retweeting posts; prohibit the release of any confidential information, prohibit the use of personal mobile devices to access Department social media accounts; and mandate that any Department-issued computer, laptop, cellphone or other mobile device used to access Department social media accounts has up-to-date protective software, including anti-virus and anti-spyware applications.

In addition, the Department has increased security-related updates and news via its social media channels: Facebook, X, Instagram, and Nextdoor. As part of this ongoing effort, the Department has incorporated "Myth Buster Mondays" (*#mythbustermonday*) into its regular social media posting schedule with the goal of addressing common misconceptions about election processes. Most recent such postings are responsive to common queries such as whether ballot drop boxes are secure, whether and how vote-by-mail ballots are counted, and whether the Department reviews the voters' signatures on the return envelope containing vote-by-mail ballots.

5. Election Technology Security Protocols

To safeguard the integrity of local elections, including from AI-generated effects, the Department employs multiple layers of cybersecurity protection, which are reviewed and updated on an ongoing basis. All of the Department's cybersecurity protocols follow best practices and recommendations from: 1) the San Francisco Office of Cybersecurity; 2) the Office of Elections Cybersecurity and Enterprise Risk Management, California Secretary of State; 3) U.S. Department of Homeland Security; 4) National Institute of Standards and Technology (NIST); and 5) Election Assistance Commission (EAC).

State elections law requires counties to only use voting systems certified by the SOS. Further, before every election, counties must re-install a "trusted build" of the software used by their voting systems. The trusted build is identifiable by the cryptographic HASH applied to the content to ensure the approved version has not been modified. The Department provides for the physical security of the voting system and its components, and Department personnel comply with prescribed chain of custody rules when using any voting equipment. These rules were drafted with guidance from the Department of Justice, the Cybersecurity and Infrastructure Security Agency, and the EAC.

Besides limiting physical access to the voting system and its components, the system is isolated from all connections to the internet. The system is air-gapped and kept separate from not only internet connections, but also the City's network. All components of the voting system are incapable of connecting via Wi-Fi or Bluetooth with any device. The Department also utilizes and enforces strong cybersecurity protocols, including multifactor authentication (MFA) and end point detection and

response software (EDR). The Department's IT personnel have implemented zero trust principles to prevent unauthorized access to data and services by utilizing role-based access control (RBAC) across the entire system. IT personnel regularly review up-to-date security recommendations and threat research alerts from US-CERT, MS-ISAC, EI-ISAC, and the City's cybersecurity team. Similarly, the Department regularly participates in penetration tests conducted by City, state, and federal agencies to audit the security posture of its website, including all applications, forms, tools, and internal processes. Finally, the Department monitors daily threat assessments issued by the City, state, and federal agencies and implements any recommendations appropriate to the Department's site.

Prior to every election, the Department conducts logic and accuracy testing on every component of the of the voting system. Staff mark batches of ballots, process them, and then compare the actual results to expected results in order to verify each unit and the system as a whole is functioning a) mechanically (i.e., ballots are fed correctly through belts and rollers without jamming), b) logically (i.e., the unit recognizes the ballot type), and c) accurately (i.e., the system reads, tabulates, and reports the correct total vote numbers). After each election, the Department conducts a post-election manual tally. As part of this public process, Department staff manually count all of the standard ballots cast in 1% (one percent) of randomly chosen San Francisco precincts, as well as 1% of randomly-chosen citywide vote-by-mail and provisional ballots. This manual tally verifies that the voting equipment properly tabulated ballots and accurately reported results. The Department applies SHA-512 cryptographic hashing to all election results reports to protect the integrity of the results in a verifiable manner.

As mentioned, no part of San Francisco's voting system receives or transmits electronic election data through an external network, and every local voter uses a paper ballot to cast their vote. As an added layer of transparency, and to create an auditable vote record, the voting system also produces publicly verifiable and sortable digital image files of voted ballots, with annotations regarding how the system interpreted each ballot's vote-marks. In order to protect vote secrecy, the Department redacts any private personal information (PPI) on these files.

To protect voter data, the Department's web applications – which provide voters information such as the status of their vote-by-mail or provisional ballot, registration, or polling place location – reside on a server protected by Cloudflare, which offers several important security features:

A. Caching information from the host server onto alternative servers so users never directly access the host server.
B. Ensuring the Department's *sfelections.gov* website itself is not attacked through use of a distributed network of servers that remain online and perform optimally during peak times.
C. Preventing website defacement that can result from brute force login attacks, which might result in the Department's site inaccurate information (at least until such time as the attack can be resolved by Department staff).
D. Protecting against denial-of-service attacks by replicating Department data on multiple servers to reduce the effects of any bad actor's concentration of requests that might degrade responsiveness. For similar reasons, upon receiving repetitive requests, Cloudflare is designed to block the associated actor's IP address(es) across its system.
E. Preventing attacks on a host server that seek to obtain voter information and providing automated security monitoring and network intrusion protection for the Department's website.

The Department maintains documented, multi-person chains of custody for all of its ballot handling and processing tasks. The Department's ballot processing protocols are designed to protect the overall integrity of the election (e.g., one person, one vote) as well as individual voter rights (e.g., the right to cast a secret ballot). All elections workers handling ballots are required to review current security rules and sign an acknowledgement of those rules. All elections workers are required to complete the cybersecurity awareness and phishing trainings and their work is continuously monitored by supervisors and observers.

The Department follows strict protocols in verifying the eligibility and identity of every registered voter. For example, the Department manually reviews all of the electronically-submitted voter registration applications to validate eligibility and potential duplication, before processing and adding any new records to the voter rolls. As another example, when a mail ballot envelope is returned by a voter, Department personnel verify the sender's identity using a rigorous three-person signature verification process. Only if the signature on a return envelope compares to the signature(s) in the recipient voter's registration record will the ballot be accepted for further processing and counting. Personnel will contact voters using hard copy mail, email, and phone calls when unable to verify a signatures on returned vote-by-mail ballot envelopes with signature samples on file for the voter. Contacting the voters provides them with an opportunity to update their registration record or provide an updated signature sample. If the voters resolve the matter before the Department certifies the election, the voters' ballots will be counted and their votes included in the results for the election.

6. Conclusion

The Department will continue to monitor any additional information regarding AI and its possible impacts on San Francisco's elections. Additionally, the Department will also continue to consider how to best identify and respond to any AI-related incidents.

I will be glad to provide additional information and answer questions the Committee may have.

Topics of Discussion

1. Possible impacts of AI in local elections
2. Department's role in relation to misinformation, disinformation, and mal-information
3. Protocols for responding to misinformation, disinformation, and mal-information

San Francisco Department of Elections

Impact of Artificial Intelligence (AI) in Local Elections

Rules Committee, San Francisco Board of Supervisors
May 13, 2024

1. Possible impacts of AI in local elections

Examples of using AI to affect local elections could include:

1. **"Deepfakes"**
   - **An example would be using AI to generate inauthentic audio of someone making false statements, and using such audio to make phone calls to voters.**

2. **False or Misleading Content**
   - **Using AI to generate content that appears authentic or official and provides inaccurate messaging.**

3. **Social Media Accounts and Websites that resemble official sources.**
   - **Using AI to create social media accounts and websites that imitate the look and tone of official sites and provide inaccurate information.**

1. Possible impacts of AI in local elections

Current security measures safeguard voting systems from AI-related threats:

1. The voting system and all equipment are not able to connect to the internet.
2. The system software obtained in person from the Secretary of State (SOS) is reinstalled onto the system before every election.
3. All equipment is tested before every election, verifying the system accurately scans ballots, tabulates votes, and reports election results.
4. The Department cryptographically hashes all results reports which ensures the results from the Department's website are authentic.
5. After each election the Department manually tallies ballots to compare against the system's election results reports, and the Department conducts a risk-limiting auditing of contests with the closest vote totals.

2. Department's role in relation to misinformation, disinformation, and mal-information

The Department's primary role is to be a trusted source of information regarding election-related processes such as voter registration, voting, and results reporting.

The Department focuses on preserving the integrity of election processes and voting, and on issues that may impact the public's trust in the conduct or the outcome of an election.

The Department does not monitor or regulate campaign speech. Should the Department become aware of false or misleading statements, the Department can alert other agencies of the situation.

2. Department's role in relation to misinformation, disinformation, and mal-information

The Department develops multilingual, multiformat outreach strategies intended to maintain the Department's presence as a trusted source of accurate election-related information.

Clear and Direct Communication: We prioritize publishing clear, easy-to-understand information on our website and in printed materials. We inform all San Francisco registered voters about key election dates, rules, and any operational changes.

Comprehensive Outreach: We engage in robust, multilingual, outreach efforts through notices, press releases, social media channels, and live and virtual presentations.

Community Engagement: We actively participate in over 100 community events to engage with residents, community organizations, and other outreach partners before and during an election cycle.

2. Department's role in relation to misinformation, disinformation, and mal-information

The Department continuously provides notices and updates to local media and community organizations throughout an election cycle.

The Department has ongoing communication with local media and community organizations, which increases the number of people who receive the Department's accurate information regarding election-related topics.

2. Department's role in relation to misinformation, disinformation, and mal-information

Before each election the Department meets with and receives information from state, federal, and local agencies regarding election security and responses to possible issues.

The California Secretary of State's Office (SOS) and its Office of Elections Cybersecurity (OEC) organizes meetings with counties and provides updates throughout an election cycle. The OEC is connected to several other agencies that organize their resources around election security such as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the California Department of Technology, and others.

The OEC has established a dedicated email address, votesure@sos.ca.gov, for the public to use to alert the agency of possible adverse impacts on an election, and which the Department also provides in its materials.

The Department collaborates directly with both the OEC and FBI to report any false election related information and to prevent interference of an election in San Francisco.

3. Protocols for responding to misinformation, disinformation, and mal-information

The Department has developed protocols for identifying and responding to false or misleading election information.

When the Department becomes aware of a possible incident involving mis-, dis-, or mal-information (MDM), the Department will activate its MDM Evaluation and Response Plan.

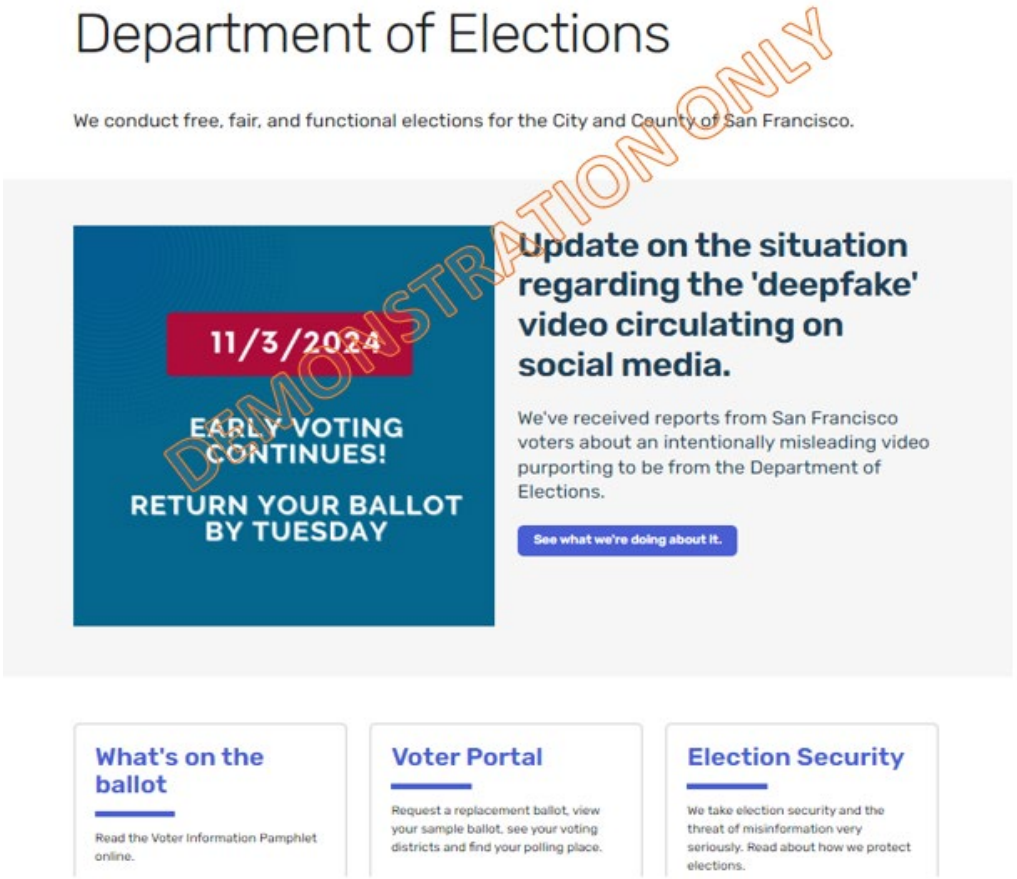
By following this plan, the Department can methodically provide accurate information to voters and alert the public in response to a potential situation. This plan also guides Department personnel to collect information on the situation that may assist investigatory and law enforcement agencies in relation to their responses.

3. Protocols for responding to misinformation, disinformation, and mal-information

One example of the Department's response to a potential situation involving video intending to suppress voter participation circulating on social media.

The Department would inform and reassure the public and local voters by posting 1) a statement on its website clarifying that voting continues through Election Day, 2) an acknowledgment that the Department is aware of the misinformation and its details, and 3) a link to more information about the steps the Department is taking.

Such notices would be in addition to press releases and briefings, posting updates on the Department's social media accounts, and informing community partners.



3. Protocols for responding to misinformation, disinformation, and mal-information

The Department would alert its partner agencies of the incident to increase the scope of the response to the incident.

This includes the SOS' Office of Elections Cybersecurity, and likely the FBI since federal contests appear on the November 2024 ballot.

The Department would issue the appropriate notices to the media and on social media, and provide ongoing updates.

Mis-, Dis-, and Malinformation (MDM) Evaluation and Response Plan

This document provides guidance to Departmental staff on how to evaluate and respond to incidents involving mis-, dis-, and malinformation (MDM) during the November 5, 2024 election cycle. Although these general protocols have been developed with different scenarios in mind, including AI-related incidents, staff should be aware that the Director may need to modify these general protocols on short notice in order to respond to unforeseen circumstances.

Level	Incident Characteristics	Response Protocol
1	- MDM was spread by a source with little to no established credibility or public reach (e.g., MDM fewer than 10 "likes" or views on social media)	1. Conduct internet and social media search to confirm the incident was limited in reach. 2. Post related factual information in relevant social media accounts. 3. Create and update an incident report (see instructions below). 4. Continue monitoring incident topic via searches for at least a week
2	- MDM was spread by a source with credibility only in one or more smaller communities (e.g., MDM impacted only a Facebook group comprised of neighbors who volunteer at a community garden in Potrero Hill))	1. Conduct search to confirm only a small group was affected. 2. Post responsive information to relevant social media accounts. 3. Create and update an incident report (see instructions below). 4. Notify appropriate City offices and Secretary of State's office. 5. Continue monitoring incident topic via searches for at least 2 weeks.
3	6. MDM was spread by a very popular source (e.g., major media, government, NGO, influencer) or is a "deepfake" from the same; the incident was widespread and visible to many San Francisco voters.	1. Reassign staff from other divisions as necessary to help respond to the public. 2. Schedule phone/email bank staff to work overtime as necessary. 3. Update Department voicemail message with summary of incident. 4. Update Department website homepage with summary of incident. 5. Send summary of incident via MDM's method (mass text or robocall). 6. Ask City and non-profit partners to distribute summary of incident. 7. Place signs with summary of incident at all voting sites and ballot boxes. 8. Ensure poll workers understand how to educate voters on the topic. 9. Create and update an incident report (see instructions below). 10. Notify appropriate City offices, Sheriff, City Attorney, and Secretary of State's office. 11. Issue press release (ensure details match incident report details). 12. Continue monitoring incident topic via searches for at least 3 weeks.

MDM incident reporting instructions: Staff must use the designated form to create a report with all of the following:

1) Evidence, (screenshot, audio file, or PDF scan of MDM), 2) date and time incident was first reported, 3) name of the person who notified the Department and how, 4) a description of the Department's response, 5) a description of the Department's planned further actions, if any. After election certification, this report can be updated with a Supplemental MDM Incident Report *if any further actions were taken. Finally, the report(s) must be archived for at least six months.*

SF.GOV

Services Departments Search

Department of Elections

We conduct free, fair, and functional elections for the City and County of San Francisco.

We've received reports of misleading information about the upcoming election. See our update on the situation.

Make a plan to vote!

There are many ways to vote in this election, by mail or in person.

Ways to vote

What's on the ballot

Read the Voter Information Pamphlet online.

Voter Portal

Request a replacement ballot, view your sample ballot, see your voting districts and find your polling place.

Election Security

We take election security and the threat of misinformation very seriously. Read about how we protect elections.

SF.GOV

Services Departments Search

Department of Elections

We conduct free, fair, and functional elections for the City and County of San Francisco.

Update on the situation regarding the 'deepfake' video circulating on social media.

We've received reports from San Francisco voters about an intentionally misleading video purporting to be from the Department of Elections.

See what we're doing about it.

What's on the ballot

Read the Voter Information Pamphlet online.

Voter Portal

Request a replacement ballot, view your sample ballot, see your voting districts and find your polling place.

Election Security

We take election security and the threat of misinformation very seriously. Read about how we protect elections.