BRIEFING TO THE CHIEF ELECTORAL OFFICER

From: Political Image Verification Project Team

Date: February 2026

Title: Deployment of a Political Image Verification System for the 2026 General Election: Strengthening Public Trust in Political Communications

PROPOSAL

1. This briefing seeks the Chief Electoral Officer's agreement to support the deployment and operational integration of a Political Image Verification System (PIVS) for the 2026 General Election, enabling registered political parties to authenticate campaign imagery and providing the public with a tool to verify whether political images are genuine.
2. Advances in generative AI mean that anyone — including foreign state actors, interest groups, or individuals — can now create realistic political imagery that falsely appears to originate from a New Zealand political party. This fundamentally threatens voters' ability to trust the political communications they encounter. Providing a verification mechanism falls squarely within the Electoral Commission's mandate to promote public confidence in the electoral process.
3. The system is under development and will be available for contracted deployment or IP transfer to the electoral commission, depending on the Commission's preference. The project team is open to discussing arrangements for ongoing technical support during the campaign period. The Commission would need to fund testing, security audit, and operational hosting — estimated at 40,000−100,000 across the election cycle, with infrastructure hosted on Catalyst Cloud under the All-of-Government Cloud Framework Agreement.

RELATION TO THE ELECTORAL COMMISSION'S STRATEGIC PRIORITIES

3. This proposal supports the Electoral Commission's:
    - **statutory obligation** under the Electoral Act 1993 to promote public confidence in the electoral process and administer parliamentary elections;
    - **2026 General Election programme**, including the $61.9 million Budget 2025 allocation for election delivery and modernisation;
    - **voter education function**, by providing a practical tool the Commission can direct the public to use when they encounter political imagery of uncertain origin;
    - **integrity responsibilities**, aligned with the $18.7 million Budget 2025 allocation for election integrity improvements over four years.

EXECUTIVE SUMMARY

4. Advances in generative artificial intelligence now allow the rapid creation of realistic synthetic images, audio, and video. Globally, AI-generated political content has been used to mislead voters in elections in the United States, Romania, Slovakia, India,

Taiwan, Canada, and the Netherlands. In Romania, the Constitutional Court annulled a presidential election in December 2024, in part due to coordinated AI-generated content and cyberattacks against electoral infrastructure.

5. New Zealand is not immune. Generative AI tools are freely available, and anyone can create convincing political imagery that falsely appears to originate from a New Zealand political party. Voters encountering such content have no way to verify whether it is genuine. The Commission does not regulate the content of election advertisements, and no verification infrastructure currently exists to help the public assess the authenticity of political imagery.
6. The Political Image Verification System provides a practical, technology-based safeguard. Political parties register campaign images through authenticated accounts. The system stores cryptographic and perceptual hashes of each image. Members of the public, media organisations, and platform operators can verify any political image against this registry. The system uses a privacy-first encrypted architecture and requires no personal information from users performing verification.
7. The system has been developed and is available for intial testing by the Commission. The project team is open to discussing arrangements for contracted maintenance of the system or intellectual property transfer and/or ongoing technical support during the campaign period. The Commission would need to fund testing, security audit, and operational hosting — estimated at $40,000-$100,000 across the election cycle, with infrastructure hosted on Catalyst Cloud under the All-of-Government Cloud Framework Agreement.

BACKGROUND

AI-generated content and the erosion of public trust

8. Generative AI tools capable of producing photorealistic images, convincing audio deepfakes, and synthetic video are now widely accessible at low or no cost. Anyone — including foreign state actors, domestic interest groups, or individuals — can now create political imagery that convincingly appears to originate from a specific party. This fundamentally undermines voters' ability to trust the political communications they encounter.
9. Globally, more than 80 percent of countries with elections in 2024 experienced AI-generated content that eroded public trust in electoral processes. Key incidents demonstrating the impact on voter trust include:
   a. **United States (2024):** An AI-generated robocall mimicking President Biden's voice told New Hampshire voters not to vote. The perpetrator was fined USD $6 million and criminally indicted. Russian operatives created deepfake videos of Vice President Harris making fabricated statements. AI-generated images falsely depicted Black Americans supporting a candidate.
   b. **Romania (2024):** The Constitutional Court annulled the presidential first-round election results on 6 December 2024, the first European country to cancel a presidential election due to cyber and information warfare. Investigations uncovered over 85,000 cyberattacks against electoral IT infrastructure, coordinated AI content, bot networks, and troll farms.
   c. **Slovakia (2023):** An AI-generated audio recording fabricated a phone call between a journalist and an opposition leader, purportedly discussing election rigging. The opposition lost the subsequent election.
   d. **Canada (2025):** A deepfake video of Prime Minister Carney reached over one million views. Canada's election watchdog classified AI use as a "high" risk.
   e. **Taiwan (2024):** Microsoft identified China-based deepfake operations as the first confirmed use of AI-generated material by a nation-state to influence a foreign election.

The "liar's dividend"

10. Academic researchers have identified a secondary threat to trust: the "liar's dividend." The mere existence of deepfake technology allows public figures to dismiss authentic evidence as AI-generated, evading accountability. Trust is eroded in both directions: voters cannot trust that content is genuine, and genuine content can be dismissed as fake. A verification system that can positively confirm the provenance of genuine political images helps restore trust in both directions.

Public trust in New Zealand's electoral process

11. Public trust in electoral communications is a foundation of New Zealand's democracy. That trust is now at risk. The Department of the Prime Minister and Cabinet's national security surveys in 2022 and 2023 found that more than 80 percent of New Zealanders are concerned about the impacts of disinformation. Ipsos polling shows 63 percent of New Zealanders are nervous about AI, though only 35 percent understand where it is being used.
12. The risk to trust is straightforward: any person or entity can now create realistic political imagery that falsely appears to originate from a New Zealand political party. A fabricated campaign image, indistinguishable from a genuine one, could be circulated on social media and attributed to any party. Voters encountering this content have no way to verify whether it is genuine. This erodes confidence not only in the specific content but in political communications generally.
13. Cybersecurity experts have warned that the 2026 election will face serious challenges as bad actors leverage AI to increase the realism and volume of misinformation. Without a verification mechanism, voters are left to judge authenticity on their own — a task that is increasingly impossible as AI-generated content becomes more sophisticated.

Absence of trust infrastructure

14. The Electoral Commission currently has no mechanism to help the public assess the authenticity of political imagery. The key gaps are:
    a. The Commission has stated: "We do not regulate the content of election advertisements, so do not have a position on the use of AI in election ads." This means the body responsible for electoral integrity is currently playing no role in helping voters assess the authenticity of political imagery.
    b. No verification infrastructure exists. Promoter statements (section 204F, Electoral Act 1993) identify who is responsible for an advertisement, but do not verify that the visual content is genuinely from that party. A fabricated image can carry a real promoter statement.
    c. The DPMC-funded monitoring initiatives (Hate and Extremism Insights Aotearoa, Logically, the Disinformation Project) have ended, creating a monitoring gap ahead of the 2026 election.
    d. New Zealand's AI Strategy (July 2025) adopted a "light-touch" regulatory approach, placing responsibility on existing agencies and mechanisms. No new trust infrastructure was established.
15. While the Commission does not regulate advertisement content, it does have a statutory obligation to promote public confidence in the electoral process. Providing the public with a verification tool is consistent with this obligation and the Commission's voter education function, without requiring the Commission to become a content regulator.
16. Internationally, jurisdictions have recognised the threat to electoral trust and taken steps to protect the integrity of political communications:
    a. **South Korea** amended the Public Official Election Act to ban election-related deepfakes within 90 days of election day, recognising that fabricated content destroys voter trust.
    b. **Singapore** passed the Elections (Integrity of Online Advertising) Amendment Bill, protecting voters from digitally generated content that could mislead them about candidates' positions.
    c. **The European Union** classified AI systems used for influencing elections as high-risk under the AI Act (fully enforceable from August 2026), requiring transparency measures to maintain public trust.
    d. In the **United States**, 28 states have enacted laws addressing deepfakes in political communications, driven by concern for voter trust and electoral integrity.

ANALYSIS

The proposed system

17. The Political Image Verification System (PIVS) is a privacy-first platform that allows political parties to register authentic campaign imagery and enables the public to verify that imagery. The system is being developed and consists of three

components:
a. **Party submission portal:** Authorised party representatives submit campaign images through authenticated accounts with multi-factor authentication. The system computes cryptographic and perceptual hashes of each image before encrypting and storing it.
b. **Public verification portal:** Any member of the public can upload a political image or scan a QR code to check whether it has been registered by a political party. No personal information or account is required.
c. **Verification API:** Media organisations and platform operators can integrate verification into their own systems through a documented programming interface.
d. **Administrative dashboard:** Commission staff can monitor system performance, manage party accounts, and review verification logs.

How verification works

18. The system uses a dual-hashing approach to handle the practical reality that political images are modified as they circulate:
a. **Cryptographic hash (SHA-256):** Provides exact-match verification for unmodified original images. This is fast and deterministic.
b. **Perceptual hash (PDQ, developed by Meta):** Provides fuzzy matching that tolerates visual modifications commonly introduced by social media platforms, including JPEG recompression, resizing, minor cropping, screenshot capture, and the addition of verification badges or QR codes. PDQ uses a 256-bit hash with a Hamming distance threshold; images scoring within this threshold are identified as matching. pHash provides a secondary fallback algorithm. This is processed locally to avoid privacy concerns of sending images to a third-party service. Generative AI is not used in the verification process to avoid the risk of hallucination and to maintain transparency and auditability.
19. This dual approach means that an image originally registered by a party will still be verified even after it has been shared on Facebook, screenshotted, or printed on a hoarding with a QR verification code added.

Privacy and security

20. The system is designed with a privacy-first architecture:
a. All stored images are encrypted with AES-256-GCM using envelope encryption, where each image has a unique data encryption key.
b. The public verification process exposes only hash comparisons, never the stored images themselves.
c. Verification is anonymous. No login, personal information, or tracking is required.
d. IP addresses are hashed in system logs and cannot be reversed.
e. Party user personal information (email addresses) is encrypted at rest.
f. The system is designed to comply with the Privacy Act 2020, notwithstanding the political party exemption.

Verification badges and QR codes

21. When a party registers an image, the system generates:
a. A small verification badge (under 5 percent of image area) that can be overlaid on the image. The badge is deliberately sized to remain within the perceptual hash tolerance so that badged images still verify against the original.
b. A QR code encoding a verification URL. This is particularly useful for physical media such as hoardings and billboards, enabling voters to scan and verify on their mobile device.
c. A unique verification ID and URL for each registered image.

Promoter statement management

22. The system includes integrated support for Electoral Act promoter statements (section 204F). Each party account can store a promoter statement, and the system provides tools to:

a. **Add promoter statements to images:** Authorised party users can overlay their party's promoter statement onto campaign images during registration. The overlay uses contrast-aware text placement (meeting WCAG 2.1 AA legibility standards with a minimum 4.5:1 contrast ratio) and configurable corner positioning, with automatic adjustment for portrait and landscape orientations.
b. **Verify promoter statements using OCR:** The system can scan submitted images using optical character recognition to check whether a promoter statement is already present and whether it matches the party's registered statement, using fuzzy text matching to account for OCR imprecision. This is locally processed so information is not sent to a third-party service.
c. **Batch processing:** Party users can add promoter statements to images in batch mode (upload and download directly) or via email, without registering images as verified assets. This supports high-volume campaign workflows.
d. **Email interface:** Images can be submitted as email attachments to a processing address. Anti-spoofing verification ensures that images are processed only after the registered user confirms the submission via a verification email sent to their authenticated address.

23. This feature directly assists parties in meeting their existing legal obligations under the Electoral Act, reducing the barrier to compliance and ensuring that promoter statements are consistently legible and correctly placed.

Complementary role to Commission functions

24. PIVS does not replace any existing Commission function. It complements the Commission's work:
a. The promoter statement requirement (section 204F, Electoral Act 1993) establishes who is responsible for an advertisement. PIVS establishes whether the visual content of that advertisement is genuinely from the claimed party, and directly assists parties in meeting the promoter statement requirement by providing tools to add legible, contrast-aware promoter statements to campaign imagery.
b. The Advertising Standards Authority's fast-track complaints process addresses misleading content after the fact. PIVS provides proactive, real-time verification before complaints are made.
c. The Commission's voter education programme can direct the public to the verification tool as a practical action they can take when they encounter political imagery. This strengthens the Commission's existing voter education mandate without expanding its regulatory scope.
d. The system could be presented as part of the Commission's broader 2026 election modernisation programme, demonstrating proactive steps to address emerging technology risks.

Development status and readiness

1. The system is ready for early testing. The current status is:
a. **Core application:** Complete. FastAPI backend, Next.js frontend, PostgreSQL database, and containerised Docker deployment are all built and functional.
b. **Hashing and verification:** Complete. SHA-256, PDQ, and pHash algorithms are integrated and tested against common image transformation scenarios.
c. **Encryption and security:** Complete. AES-256-GCM envelope encryption, JWT authentication, TOTP multi-factor authentication, and role-based access control are implemented.
d. **Party registry:** Complete. Pre-seeded with New Zealand's seven registered parliamentary parties.
e. **Promoter statement tools:** Complete. Contrast-aware text overlay with WCAG 2.1 AA legibility, OCR verification via Tesseract, batch processing mode, and email processing interface with anti-spoofing verification.
f. **Production deployment configuration:** Complete. Gunicorn application server, Nginx reverse proxy with rate limiting, security headers, and TLS termination are configured.
2. The system is ready for acceptance testing, security audit, and deployment either as a contracted deployment on Catalyst Cloud or to the Commission's operational environment.

Risks and mitigations

25. The following risks have been identified:

Risk	Mitigation
Low party adoption reduces usefulness	Early engagement with major parties; simple onboarding process; system pre-seeded with seven registered NZ parties
False positive matches (incorrect verification)	Multiple hash algorithms with configurable thresholds; confidence scoring; human review pathway
System targeted by cyberattack	Rate limiting; web application firewall; encrypted storage; security audit before launch; nginx reverse proxy with rate limiting zones
Late election traffic spike overwhelms system	CDN deployment; auto-scaling infrastructure; load testing before election
Public confusion about what verification means	Clear user interface messaging; verification means "registered by a party" not "factually accurate"
Adversarial image manipulation to evade detection	PDQ is resistant to common transforms; multiple hash algorithms reduce evasion; DINOv2-based hashing available for future enhancement
Reputational risk to Commission if system fails	Thorough testing and security audit; soft launch with limited publicity; staged rollout

POPULATION IMPLICATIONS

26. The system is designed to benefit all New Zealanders who engage with political advertising. Specific population implications include:
a. **Maori:** AI models trained on Western data present specific risks of culturally offensive or stereotyping content in political contexts. Fabricated imagery purporting to represent Maori positions or interests could be created by any actor and circulated without accountability. The verification system helps Maori communities confirm whether political imagery purporting to represent Maori interests is genuinely from the claimed party.
b. **Pacific peoples:** Similar risks of AI-generated stereotyping apply. Verification provides a practical tool for Pacific communities to check political imagery targeting them.
c. **Older New Zealanders:** Research indicates lower digital literacy among older populations, making them more susceptible to AI-generated misinformation. The QR code system on physical media (hoardings, printed material) provides an accessible verification method.
d. **Rural communities:** Political advertising on physical media (hoardings, billboards) is prevalent in rural areas. QR code verification is particularly relevant for these communities.
e. **Disabled people:** The web portal will be designed to meet WCAG 2.1 AA accessibility standards.

HUMAN RIGHTS

27. The proposal is consistent with the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993. The system:
a. does not restrict the publication of any content (section 14, freedom of expression);
b. is voluntary for political parties to adopt;
c. does not collect or process personal information from members of the public performing verification;
d. supports informed participation in elections by enabling voters to assess the authenticity of political communications (section 12, right to vote).

FINANCIAL IMPLICATIONS

Estimated image volumes

28. Based on data from the 2023 General Election, the system would need to handle the following image volumes:

    a. In the 2023 election, the six main parliamentary parties ran approximately 9,000 paid Facebook advertisements across a three-month regulated period: National ran 4,073 Facebook ads, ACT ran 844 Meta ads, and the remaining parties ran a combined total of approximately 4,100 ads (Victoria University of Wellington; RNZ; The Spinoff). However, the number of **unique images** is substantially smaller than the number of ads, as each image is reused across multiple ad variants with different demographic and geographic targeting.

    b. Physical campaign materials add further volume. Labour's 2023 expense return recorded 130 large, 40 medium, and 200 small hoardings for a single electorate, with similar volumes across other parties and electorates (Electoral Commission, 2023 Party Expenses Returns). Parties also produce flyers, billboards, social media graphics, and print collateral.

    c. Based on these volumes, the estimated number of **unique images** that parties would register with the system is:

Category	Major Party (×3)	Minor Party (×4)
Party-wide campaign graphics (policy, leader, attack ads)	30–80	15–40
Electorate candidate materials	150–400	30–100
Social media originals	50–150	20–50
Hoardings and billboard designs	10–30	5–15
Print collateral (flyers, DLs)	20–50	10–20
Subtotal per party	**260–710**	**80–225**

    d. **System-wide totals:** Conservative estimate: ~1,300 images (3 major parties × 300 + 4 minor parties × 100). Moderate estimate: ~2,100 images. High estimate (including individual candidate submissions): 3,000–5,000 images.

    e. **Storage requirement:** Each registered image generates up to four encrypted variants (original, badge overlay, QR code, promoter-stamped version) at approximately 3 MB each, totalling ~12 MB per image. At 5,000 images, total encrypted storage is approximately 60 GB — a modest volume for cloud object storage.

    f. **Verification query volume:** During the campaign period, each registered image may be verified multiple times by the public, media, and automated integrations. Peak verification traffic is estimated at 5,000–20,000 queries per day during the final weeks of the campaign, based on the volume of social media political advertising observed in 2023.

Financial implications

29. The system has intial development to alpha testing, with this cost invested by the project team. The project team is open to discussing arrangements for contracted deployment, intellectual property transfer and/or technical support during the campaign period; however, the costs below relate only to the Commission's operational hosting and deployment requirements.
30. **Recommended hosting platform:** Catalyst Cloud, the only All-of-Government Cloud Framework provider with 100% New Zealand-based infrastructure. Catalyst Cloud is ISO 27001 and ISO 27017 certified, PCI DSS compliant, and all three data centres are located in New Zealand, ensuring data sovereignty under New Zealand law. Cloud usage by government agencies is aggregated under the AoG framework, providing volume discounts regardless of individual agency spend. All prices below are sourced from Catalyst Cloud's published price list (catalystcloud.nz/pricing/price-list/, effective 1 June 2025) and are in NZD exclusive of GST unless otherwise noted.
31. The Commission's costs for testing, security assurance, and operational hosting are estimated as follows:

Item	Estimated Cost (NZD)	Notes
Security audit and penetration test if needed	$20,000$–40,000	Pre-launch independent security assessment; recommended to be conducted by a GCSB-approved provider
Acceptance and integration testing	$10,000$–20,000 *	Commission staff or contracted testers to validate functionality against Commission requirements
Load and stress testing	$5,000$–10,000 *	Simulate election-day traffic volumes to validate system capacity
WCAG accessibility audit	$1,000$–2,000 *	Confirm the public-facing portal meets WCAG 2.1 AA standards
Privacy Impact Assessment	0–5,000 *	Required under the Privacy Act 2020; a draft PIA can be provided with the system
Infrastructure hosting (see breakdown below)	$1,000$–2,500/month	Catalyst Cloud hosting for the deployment period (estimated 8 months, April–November 2026)
Total estimated operational cost	$44,000$–**99,000**	Across the 2026 election cycle (including 8 months' hosting at $8,000$–20,000)

* These items could be conducted in-house by Commission staff with existing capabilities, reducing costs to staff time only. The privacy impact assessment, acceptance testing, load testing, and accessibility audit do not require external contractors if the Commission has qualified personnel available.

32. The monthly infrastructure hosting estimate of $1,000$–2,500 is based on the following Catalyst Cloud configurations:
    a. **Application compute:** 285–570/month. Two application servers for the verification API, hash computation (SHA-256, PDQ, pHash), Tesseract OCR processing, and image overlay processing. Lower bound: 2× c1.c2r4 instances (2 vCPU, 4 GB RAM each, at $95.05/montheach).Upperbound : 2 \times c1.c4r8instances(4vCPU, 8GBRAMeach, at$190.09/month each) for election-day capacity. One additional worker instance for background processing (c1.c2r4 at $95.05/monthtoc1.c4r8at$ 190.09/month).
    b. **Managed PostgreSQL database:** 180–360/month. Catalyst Cloud Managed Database Service with automated backups and replication. A db.c1.c2r4 instance (2 vCPU, 4 GB RAM) provides sufficient capacity for the party registry, asset index, and verification logs. The upper estimate includes a read replica for high-availability during election peak.
    c. **Encrypted image storage:** 5–20/month. Object storage for AES-256-GCM encrypted images, verification badges, QR codes, and promoter-stamped versions. At 60 GB (5,000 images × 12 MB), geo-replicated object storage costs $0.10/GiB/month =$ 6/month. Single-region storage at $0.05/GiB/monthhalvesthiscost.Blockstorageforthedatabaseat$0.21/GB/month for 50 GB adds ~$10.50/month.
    d. **Network and load balancing:** 75–150/month. Load balancer $(24.62/month), publicIPv4addresses($4.50/month each), and outbound data transfer at $0.12/GB.At200GB/monthoutbound(verificationresponses, imagedownloads, APItraffic), bandwidthcosts$ 24/month. CDN for static frontend assets may be provided externally (e.g., Cloudflare free tier) or via Catalyst's network.
    e. **Operational overhead (15% contingency):** 80–165/month. Covers monitoring, alerting, SSL/TLS certificates (free via Let's Encrypt), DNS, log aggregation, automated backups, and a buffer for unexpected traffic scaling or incident response during the election period.
33. All prices above are exclusive of GST (15%). Including GST, the monthly hosting cost is approximately $1,150$–2,875/month, or $9,200$–23,000 for an eight-month deployment period.
34. **Cost drivers and scaling:** The primary cost driver is compute, not storage. Image storage at the volumes estimated for a New Zealand general election (60 GB) is negligible on Catalyst Cloud — under $10/month even with geo-replication. The upper hosting estimate accounts for running redundant application servers and a database read replica during the peak election period (August–October), with the option to scale down to the lower configuration outside the peak.

35. These costs represent a fraction of the Budget 2025 allocations available to the Commission ($18.7 million for integrity improvements;$61.9 million for election delivery). The total is modest compared to the potential cost of an electoral integrity incident. Romania's annulled election required a full re-run at significant public expense and lasting damage to democratic legitimacy.
36. By deploying a system that has already been developed rather than commissioning bespoke development, the Commission avoids the typical software procurement costs and timeframes that would otherwise make deployment ahead of the 2026 election impractical.

LEGISLATIVE IMPLICATIONS

32. No legislation is required to deploy the system. The system operates within existing regulatory settings as a voluntary verification tool. The Commission's statutory functions under the Electoral Act 1993, particularly the obligation to promote public confidence in the electoral process and to conduct voter education, provide sufficient basis for offering this tool to the public.
33. The Chief Electoral Officer may wish to note that:
    a. Future legislative consideration could make registration of political advertising images mandatory rather than voluntary, providing stronger assurance to the public.
    b. The Independent Electoral Review recommended expanding the undue influence offence and considering microtargeting regulations. A verification system would complement any such future legislative changes.
    c. Deployment now as a voluntary tool establishes operational experience and public familiarity that would ease any future transition to a mandatory regime.

CONSULTATION

34. The following agencies have interests relevant to deployment:
    - **Ministry of Justice:** As the policy agency for electoral law and the Minister's office.
    - **Department of the Prime Minister and Cabinet:** As the lead agency for national security and disinformation resilience.
    - **Government Communications Security Bureau:** For cybersecurity review of the system prior to deployment.
    - **Office of the Privacy Commissioner:** To confirm the privacy-by-design approach meets best practice.
    - **Department of Internal Affairs:** As the lead for the Government's digital strategy and AI framework.
35. Engagement with registered political parties would be required before deployment to ensure uptake. The system is pre-seeded with accounts for all seven registered parliamentary parties, and onboarding can commence as soon as the Commission confirms operational readiness.

PROPOSED DEPLOYMENT TIMELINE

36. Given that the system is already developed, the following timeline is indicative:

Phase	Activity	Indicative Period
1. Acquisition	Engage with project team on IP transfer and/or support arrangements; receive source code and documentation	February - March 2026
2. Testing	Acceptance testing; integration with Commission infrastructure; accessibility audit	March - April 2026

Phase	Activity	Indicative Period
3. Security	Independent security audit and penetration test; GCSB review	April - May 2026
4. Remediation	Address any findings from testing and security audit	May - June 2026
5. Party onboarding	Engage registered parties; set up authenticated accounts; provide training	June - July 2026
6. Soft launch	Limited public availability; monitor system performance	July 2026
7. Full deployment	Public launch integrated with Commission voter education programme	August 2026
8. Election operations	Full operational support through election day and post-election period	August - November 2026

37. This timeline provides adequate time for thorough testing and security assurance while ensuring the system is operational well before the regulated election advertising period commences.

COMMUNICATIONS

38. If the Chief Electoral Officer agrees to progress this proposal, officials recommend:
    a. An announcement framed around election integrity and public trust, positioning the system as part of the Commission's broader 2026 election modernisation programme.
    b. Engagement with major media organisations to encourage integration of the verification tool into their election coverage workflows.
    c. Inclusion in the Commission's 2026 voter education programme, with clear messaging about what verification means and how to use the tool.
    d. A public-facing website with clear, plain-language guidance, integrated with the Commission's existing elections.nz domain.
    e. Engagement with social media platforms operating in New Zealand to encourage adoption of the verification API.

PROACTIVE RELEASE

39. The Chief Electoral Officer is advised to proactively release this briefing, with any redactions necessary to protect security-sensitive technical details, within 30 business days of decisions being confirmed.

RECOMMENDATIONS

The Chief Electoral Officer is recommended to:

Context

40. **note** that advances in generative AI now allow the rapid creation of realistic synthetic political images, audio, and video at low cost and with minimal technical skill;
41. **note** that AI-generated political content has been used to mislead voters in elections in the United States, Romania, Slovakia, India, Taiwan, Canada, and the Netherlands, and that Romania annulled a presidential election in December 2024 due in part to AI-enabled interference;

42. **note** that no mechanism currently exists for voters to verify whether political imagery is genuinely from the party it claims to represent, and that anyone can now create convincing fake political content at minimal cost;
43. **note** that the absence of verification infrastructure poses a direct risk to public trust in electoral communications, and that the Electoral Amendment Act 2025 did not address this gap;
44. **note** that the Commission's statutory obligation to promote public confidence in the electoral process and to conduct voter education provides a sufficient basis for offering a voluntary image verification tool;
45. **note** that Budget 2025 allocated $18.7 millionoverfouryearsforelectionintegrityimprovementsand$61.9 million for 2026 General Election delivery and modernisation;
46. **note** that a fully developed Political Image Verification System is available for transfer to the Commission, with operational hosting and deployment costs estimated at $40,000–$10,000 across the election cycle based on Catalyst Cloud pricing under the All-of-Government Cloud Framework Agreement;

Decisions

47. **agree** that a practical, technology-based safeguard for verifying the authenticity of political campaign imagery is necessary to protect electoral integrity for the 2026 General Election;
48. **agree** that the Political Image Verification System, which enables parties to register authentic campaign images and the public to verify them using cryptographic and perceptual hashing with a privacy-first encrypted architecture, is a suitable solution;
49. **agree** to engage with the project team on arrangements for intellectual property transfer and/or technical support during the campaign period, and to proceed with testing and deployment;
50. **agree** that the system should be deployed as a voluntary tool available to all registered political parties ahead of the 2026 General Election;

Next steps

51. **direct** officials to engage with the project team on arrangements for intellectual property transfer and/or technical support, and to receive source code, documentation, and deployment configurations;
52. **direct** officials to commission an independent security audit and penetration test of the system, and to engage the Government Communications Security Bureau for review;
53. **direct** officials to conduct acceptance testing and integration of the system with Commission infrastructure, including a WCAG 2.1 AA accessibility audit;
54. **direct** officials to engage with registered political parties on voluntary adoption and to commence account onboarding;
55. **direct** officials to integrate the verification tool into the Commission's 2026 voter education programme;
56. **direct** officials to report back to the Chief Electoral Officer by April 2026 on testing outcomes, security audit results, and confirmed deployment timeline.

Prepared by: Political Image Verification Project Team

Approved by: [Senior Official Name and Title]

APPENDIX A: Technical Summary of the Political Image Verification System

System Architecture

The system comprises a FastAPI (Python) backend with PostgreSQL database, a Next.js web frontend, and containerised deployment via Docker. The architecture follows a three-tier model:

Layer	Technology	Purpose
Frontend	Next.js (React)	Public verification portal and party submission portal
API	FastAPI (Python)	RESTful API with OpenAPI documentation
Data	PostgreSQL + encrypted file storage	Party registry, hash index, encrypted image storage

Hashing Approach

Method	Purpose	Detail
SHA-256	Exact match	256-bit cryptographic hash; detects unmodified originals
PDQ (Meta)	Perceptual match	256-bit perceptual hash; tolerates compression, resizing, badge overlays; Hamming distance threshold of 31 or fewer differing bits for a confident match
pHash	Fallback match	64-bit perceptual hash; secondary matching algorithm

Encryption

- **Envelope encryption:** Each image encrypted with a unique AES-256-GCM data encryption key (DEK), which is itself encrypted by a key encryption key (KEK).
- **PII encryption:** Party user email addresses and contact details encrypted at rest.
- **Transport:** TLS for all connections.

Authentication

- JWT-based authentication for party users.
- TOTP multi-factor authentication mandatory for party administrators.
- Role-based access control (admin, submitter, viewer).

API Endpoints

Endpoint	Auth	Purpose
`POST /api/v1/verify/image`	None	Upload image for verification
`POST /api/v1/verify/hash`	None	Verify by pre-computed hash
`GET /api/v1/verify/{id}`	None	QR code / verification ID lookup
`GET /api/v1/parties`	None	List registered parties
`POST /api/v1/assets`	Party	Submit image for registration (with optional promoter statement overlay and OCR check)
`POST /api/v1/assets/add-promoter`	Party	Add promoter statement to image and return (batch mode)
`GET /api/v1/assets`	Party	List registered assets
`PUT /api/v1/parties/{id}/promoter-statement`	Admin	Set or update party promoter statement
`POST /api/v1/email/verify/{job_id}`	Token	Confirm an email-submitted processing job

Production Deployment

The system is containerised with Docker Compose and includes:

- Gunicorn application server with Uvicorn workers
- Nginx reverse proxy with rate limiting (30 verifications/minute, 10 submissions/minute)
- Security headers (X-Frame-Options, Content-Security-Policy, X-Content-Type-Options)
- TLS termination at the reverse proxy
- PostgreSQL with encrypted connections

Pre-seeded Parties

The system is pre-configured with New Zealand's seven registered parliamentary parties:

1. New Zealand Labour Party
2. New Zealand National Party
3. Green Party of Aotearoa New Zealand
4. ACT New Zealand
5. New Zealand First
6. Te Pati Maori
7. The Opportunities Party (TOP)

APPENDIX B: International Comparisons

Jurisdiction	Measures to Protect Electoral Trust	Status
South Korea	Ban on election deepfakes within 90 days of polling; up to 7 years' imprisonment	In force (2023)
Singapore	Prohibition on digitally generated content depicting candidates during elections	In force (2024)
European Union	AI Act classifies election-influencing AI as high-risk; Digital Services Act requires platforms to label manipulated content	Full enforcement August 2026
United States	No federal legislation; 28 states have enacted laws; FCC fines for AI robocalls	Patchwork
Australia	No binding AI-specific laws; AEC acknowledges it cannot combat AI misinformation; "Stop and Consider" campaign only	Voluntary
Canada	No AI-specific election legislation; election watchdog rates AI as "high" risk	Gap
New Zealand	No verification infrastructure; Electoral Commission does not regulate ad content; no trust mechanisms	**Significant gap**

APPENDIX C: Key Statistics

Statistic	Source
80%+ of countries with elections in 2024 experienced AI-related electoral incidents	Harvard Ash Center
63% of New Zealanders are nervous about AI	Ipsos

Statistic	Source
80%+ of New Zealanders are concerned about disinformation impacts	DPMC National Security Survey
550% increase in known deepfake videos globally since 2019	Deepstrike
57% of Americans are worried about AI generating false political content	Pew Research Center
97% of Americans agree AI should be subject to safety rules	Gallup/SCSP
87% of voters support AI disclosure requirements for political ads	Public Citizen
Up to 8 million deepfake videos projected on social media by 2025	Industry projections
$18.7 million allocated in Budget 2025 for election integrity improvements	NZ Budget 2025
$61.9 million allocated for 2026 election delivery and modernisation	NZ Budget 2025

APPENDIX D: Cost Comparison - Acquisition Approaches

Approach	Estimated Operational Cost	Timeline	Risk
Transfer of existing system (recommended)	$20,000 IPaquisition+$60,000–$110,000 hosting and deployment on Catalyst Cloud	2 months to deployment	Low — system already has basic functionality; NZ data sovereignty assured
Contracted Deployment	$100,000$–150,000 for managed system deployed on Catalyst Cloud	2 months to deployment with managed updates and security during the election	Low — system already has basic functionality; NZ data sovereignty assured
Bespoke development via government procurement	$500,000$–1,000,000+	12–18 months	High — impossible for 2026 election
Commercial SaaS solution	$200,000$–400,000/year	3–6 months	Medium — data sovereignty concerns with offshore providers; vendor lock-in; ongoing costs

The transfer approach provides the Commission with full ownership of the source code and infrastructure, avoids vendor lock-in, and ensures data sovereignty through hosting on Catalyst Cloud's 100% New Zealand-based infrastructure under the All-of-Government Cloud Framework Agreement. The operational cost estimate of $60,000$–110,000 covers Catalyst Cloud hosting ($8,000$–20,000 for 8 months), security audit and penetration testing ($30,000$–50,000), and acceptance, load, and accessibility testing ($20,000$–40,000). Image storage for the estimated 2,000–5,000 campaign images across all parties is a negligible cost component at under $10/month on Catalyst Cloud object storage. Arrangements for intellectual property transfer and/or technical support during the campaign period can be discussed separately with the project team.

APPENDIX E: Privacy Impact Assessment

A draft Privacy Impact Assessment (PIA) has been prepared for the system and is provided as a separate document (*Privacy Impact Assessment: Political Image Verification System*, February 2026). The PIA assesses the system against all 13 Information Privacy Principles under section 22 of the Privacy Act 2020.

Key findings:

- **Overall privacy risk: Low.** The system collects minimal personal information (party user accounts only — approximately 50–100 individuals). Public verification is fully anonymous.
- **No personal information is collected from the public.** Verification requires no login, account, or identifying information. Uploaded images are processed in memory and not stored.
- **All personal information is encrypted at rest.** Email addresses use AES-256-GCM encryption; passwords are bcrypt-hashed; IP addresses are SHA-256 hashed in logs (irreversible).
- **No offshore data transfer.** When hosted on Catalyst Cloud, all personal information remains within New Zealand.
- **Recommendations:** The hosting agency should establish a data retention schedule, a documented process for access and correction requests, and consult with the Office of the Privacy Commissioner before deployment.

The full PIA is available for review by the Commission's privacy officer and for consultation with the Office of the Privacy Commissioner as required by the Cabinet Manual.

REFERENCES

1. Electoral Commission of New Zealand. *Ensuring election integrity for 2026 and the future.* https://elections.nz/media-and-news/2025/ensuring-election-integrity-for-2026-and-the-future/
2. Electoral Commission of New Zealand. *About election advertising.* https://elections.nz/guidance-and-rules/advertising-and-campaigning/about-election-advertising/
3. Elections NZ. *2026 General Election.* https://elections.nz/about/about-the-electoral-commission/our-work/2026-general-election/
4. Department of the Prime Minister and Cabinet. *Strengthening resilience to disinformation in Aotearoa New Zealand.* https://www.dpmc.govt.nz/our-programmes/national-security/strengthening-resilience-disinformation
5. Ministry of Justice. *Electoral law changes.* https://www.justice.govt.nz/about/news-and-media/news/electoral-law-changes/
6. Ministry of Business, Innovation and Employment. *New Zealand's Strategy for Artificial Intelligence: Investing with confidence.* July 2025.
7. DPMC Multi-Stakeholder Group. *Strengthening civil society resilience to mis- and disinformation in Aotearoa New Zealand.* March 2024.
8. Ministry of Justice. *Independent Electoral Review: Final Report.* November 2023.
9. International Foundation for Electoral Systems. *The Romanian 2024 Election Annulment.* https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity
10. NPR. *How deepfakes and AI memes affected global elections in 2024*. December 2024.
11. Centre for Governance Innovation. *Then and Now: AI Electoral Interference in 2025.* https://www.cigionline.org/articles/then-and-now-how-does-ai-electoral-interference-compare-in-2025/
12. Harvard Ash Center. *The Apocalypse That Wasn't: AI in 2024 Elections.* https://ash.harvard.edu/articles/the-apocalypse-that-wasnt/
13. University of Waikato. *Playing politics with AI: Why NZ needs rules on the use of fake images in election campaigns.* https://www.waikato.ac.nz/news-events/news/playing-politics-with-ai/
14. Pew Research Center. *Views of AI Around the World.* October 2025.
15. Advertising Standards Authority. *Spotlight on General Election Advertising.* https://asa.co.nz/2023/08/09/spotlight-on-general-election-advertising/

16. Broadcasting Standards Authority. *Election Programmes Code.* https://www.bsa.govt.nz/broadcasting-standards/election-code/
17. Carnegie Endowment for International Peace. *Can Democracy Survive the Disruptive Power of AI?* December 2024.
18. Brennan Center for Justice. *Gauging the AI Threat to Free and Fair Elections.* March 2025.
19. Catalyst Cloud. *Price List.* https://catalystcloud.nz/pricing/price-list/ (Prices effective 1 June 2025.)
20. Catalyst Cloud. *All-of-Government Cloud Framework Agreement.* https://catalystcloud.nz/customers/public-sector1/
21. New Zealand Government Procurement. *Catalyst Cloud Framework Agreement.* https://www.procurement.govt.nz/contracts/catalyst-cloud-framework-agreement/
22. Krewel, M. (Victoria University of Wellington). *Five weeks, 4,000 Facebook posts: social media campaigning in the 2023 election.* November 2023. https://www.wgtn.ac.nz/news/2023/11/five-weeks-4-000-facebook-posts-social-media-campaigning-in-the-2023-election
23. RNZ. *The campaign for social media supremacy in Election 2023.* October 2023. https://www.rnz.co.nz/news/political/500672/the-campaign-for-social-media-supremacy-in-election-2023-who-the-parties-targeted-and-their-key-messages
24. The Spinoff. *Who spent most on online ads this election?* October 2023. https://thespinoff.co.nz/politics/20-10-2023/who-spent-most-on-online-ads-this-election
25. Electoral Commission of New Zealand. *2023 General Election Party Expenses.* https://elections.nz/democracy-in-nz/historical-events/2023-general-election/party-expenses/
26. NZ Herald. *Election 2023: Who spent most on online advertising?* October 2023. https://www.nzherald.co.nz/business/election-2023-who-spent-most-on-online-advertising-act-tops-parties-in-meta-google-data/3GCHJGIJNRGLNKTGNGFTPUBIIQ/