Technical Risk Assessment: NIN as a Voter Authentication Factor for NBA 2026 National Elections

Background

A proposal has been made to incorporate the National Identification Number (NIN) into the voter authentication process for the 2026 NBA National Elections. The architecture proposed is real-time validation: the voter inputs their NIN at the point of voting, the system queries the NIMC database either directly via the NIMC API or through a NIMC-licensed third-party verification provider and the returned identity record is matched against the Voters Register before a ballot is issued.

This assessment evaluates that model against the realities of this election's technical environment.

The Existing Framework

The current authentication model is standard **Two-Factor Authentication (2FA):**

- **SCN** something the voter knows
- **OTP** a one-time password delivered in real time to the voter's registered phone or email at the moment of voting, expiring within minutes

This architecture is identical to what Nigerian banks and financial institutions deploy for high-value transaction authorisation. It is implemented, independently tested, certified, and operational. Every vote is bound to a verified identity through a live communication channel that only the legitimate voter can control at that precise moment.

Risk 1 API Access: Both Routes Have Unresolved Problems

Two access routes exist for querying the NIMC identity database in real time.

Route A Direct NIMC API: This requires a formal application to NIMC, execution of a data sharing agreement, regulatory approval, technical onboarding, sandbox testing, and production certification sequentially, each step contingent on the last, all operating on NIMC's timeline. The ECNBA has no existing

NIMC relationship, no credentials, and no pending application. This route cannot be completed before 18th July 2026. It is a closed door.

Route B NIMC-licensed third-party providers: Several private companies are licensed by NIMC to offer NIN verification as a paid service, typically charged per query. This route bypasses the direct NIMC regulatory process and is technically faster to onboard. It is the more credible of the two routes and deserves honest engagement.

However, selecting Route B does not resolve what the system must do with the API response once it arrives. Whether NIMC's own API or a licensed intermediary is used, the response is identical: the holder's biographic details as captured at NIN enrolment name, date of birth, gender. The response does not contain an SCN. It contains no field that directly maps to the NBA Voters Register.

The voting platform must therefore take the returned name and search the Voters Register to find the corresponding voter record a name-matching operation across two completely independent administrative databases. This is where the model breaks down, and it breaks down regardless of which API route is used. Third-party providers solve the access problem. They do not solve the matching problem. They do not solve the failure handling problem. They do not solve any of the risks below.

Risk 2 External Dependency: One Outage Can Halt the Entire Election

Inserting any external API call into the authentication path of a live election creates what systems architects call a **hard external dependency** a point at which the entire system's availability is contingent on the uptime of an outside service.

If the NIMC API or a licensed third-party provider experiences downtime during the 24-hour voting window, every voter attempting to authenticate at that moment is not slowed down. They are locked out. The voting window continues to expire. There is no SLA with any third-party provider that obligates them to guarantee uptime specifically for the NBA election, and no contractual remedy that restores a lost vote after the window closes.

This risk is not hypothetical. Third-party API services experience outages. The question is not whether it could happen it is what happens to eligible voters when it does. The SCN + OTP system carries no such exposure. Authentication runs entirely within infrastructure controlled and monitored by the ECNBA's designated service providers under binding contractual obligations. There is no external call in the authentication path and therefore no external point of failure.

Risk 3 Name Mismatch: The System Will Reject Eligible Voters

The NIMC database records a voter's name as submitted at enrolment. The NBA Voters Register records names as they appear on the Supreme Court Roll. These two records are maintained by entirely independent institutions with no data synchronisation between them.

Divergence between these records is not an edge case it is routine. A female member of the Bar who changed her surname upon marriage, updated her entry on the Supreme Court Roll, but has not updated her NIMC record, presents differently in each database. The system reads this as two different people and rejects her authentication. Her eligibility is not in question. Her NIN is genuine. She is rejected because of an administrative gap between two government databases that she has no obligation to keep in alignment and no means of correcting before Election Day.

The same problem applies to members with name corrections on the Roll, variations in how initials, hyphens, or prefix titles are recorded, and differences in field ordering between databases all of which are common in Nigerian naming conventions across administrative systems. Every mismatch is a live authentication failure during voting, with no human reviewer available to adjudicate it in real time and no mechanism to extend the voting window while it is resolved.

Risk 4 Diaspora Members: Disproportionate Exposure to Authentication Failure

NIN enrolment has historically required physical presence at a NIMC centre in Nigeria. Remote enrolment capability has been introduced for a limited number of countries but remains inconsistently available and operationally immature across most jurisdictions where Nigerian lawyers in the diaspora reside.

Nigerian lawyers practising or resident abroad who are on the Final Voters Register and constitutionally entitled to vote face a disproportionate vulnerability under the proposed model. Some will not possess a NIN at all, having left Nigeria before or shortly after NIN enrolment became mandatory. Others will have a NIN but face the name mismatch problem described above with the additional disadvantage that updating a NIMC record from outside Nigeria is significantly more difficult than doing so in person at a local NIMC office.

The proposed model does not categorically bar diaspora members from voting. It does, however, expose them to a substantially higher rate of authentication failure than their counterparts based in Nigeria through no fault of their own and with no practical remedy available before 18th July 2026. That is a disproportionate and unjustifiable burden on a specific cohort of fully eligible voters.

Risk 5 System Security: Integration Creates a New Attack Surface on the ECNBA Platform

The ECNBA voting platform has been independently built, security-tested, and certified as a standalone system. It operates within a defined and audited technical perimeter. Integrating it with an external API whether NIMC's own or a licensed third-party provider requires opening a live data channel between that perimeter and an outside environment.

Members of the Bar will be aware of the data breaches that have affected Nigerian financial institutions and government-linked platforms in recent years incidents, including those involving Sterling Bank and other organisations, in which the breach entered not through the institution's own core systems but through an integration point with a third-party service that carried a weaker security posture. This is a documented and recurring pattern in Nigerian enterprise IT security.

The third-party NIN verification providers licensed by NIMC operate their own infrastructure with their own security controls, their own patch cycles, and their own vulnerabilities none of which the ECNBA can audit, enforce, or contractually guarantee before Election Day. Connecting the voting platform to such a service under time pressure, without the security review, penetration testing, and integration audit that responsible production deployment requires, opens a channel into the ECNBA system that did not previously exist.

The established principle in information security is unambiguous: **a system is only as secure as its weakest integration point.** Introducing an untested external connection into a certified election platform days before polling opens is not a security enhancement. It is a liability introduced at the worst possible moment.

Risk 6 API Failure During Voting: There Is No Safe Default

Every API integration must specify what the system does when the external service fails or returns an error mid-election. In a live voting context, NIN API failure produces a binary choice with no good answer:

Fail closed deny authentication until the service recovers. Eligible voters are locked out for the duration of any outage with no extension of the voting window and no means of recourse.

Fail open bypass NIN verification and fall back to SCN-only authentication when the API is unavailable. This means NIN verification is silently suspended whenever the external service is under stress making it not a security control at all, but a check that disappears precisely when system pressure is highest.

There is no third option. No technical design resolves this dilemma within the constraints of a fixed 24-hour election window. The SCN + OTP framework does not face this problem because it carries no external dependency that can place the system in this position.

The Fundamental Point

The OTP already accomplishes what NIN is being proposed to accomplish. Even if an attacker possesses both a voter's SCN and their NIN, they cannot cast a vote without live access to that voter's registered phone or email inbox at the exact moment of authentication. That constraint is what the OTP enforces. NIN introduces a static, permanent identifier into a system whose security is grounded in a dynamic, time-limited one and adds no meaningful protection against any realistic threat that the OTP does not already defeat.

Summary

Risk	Severity	Resolved Before 18 July
Both API routes leave the matching problem unsolved	High	No
External API dependency single point of failure	Critical	No
Name mismatch eligible voters wrongly rejected	High	No
Diaspora members disproportionately exposed	High	No
Integration opens new attack surface on ECNBA platform	Critical	No
No safe API failure handling within election window	Critical	No

Three critical risks. Three high-severity risks. No improvement in authentication assurance over the existing framework. The case against NIN integration is technically conclusive.