

Respectfully submitted in response to the following White House Executive Order:

On March 25th of 2025 President Trump issued the Executive Order Preserving and Protecting the Integrity of American Elections¹. The EO states that the United States fails to enforce basic and election protections, many of which are afforded to citizens of other countries around the world. America, by comparison, relies on a “patchwork of voting methods that can lead to basic chain-of-custody problems” including mail-in voting that many states allow to be tabulated late.

The President states that elections should be unmarred by fraud, errors, and suspicion, and American citizens have the right to have their votes properly counted and tabulated. State governments are required by the Constitution to safeguard American elections in compliance with Federal Laws that protect voters.

The EO calls for the Election Assistance Commission to assist the various states with verifying eligibility and maintaining accurate lists of eligible voters. It calls for the Commission to be granted power to enforce policy at the state level, including improving the security of election systems, compliance with a National Election Day, the prevention of foreign interference in US elections, and the prosecution of election crimes.

These actions are designed to clean up legacy disparities between state electoral systems and create alignment with the current administration. However, to truly achieve the level of assurance called out by the President, the US electoral system needs to adopt Zero-Trust Architecture and implement IdentityCare as a Zero-Trust credentialing solution.

Zero-Trust Architecture (ZTA) is the current government recognized cybersecurity paradigm focused on resource protection and the premise that **trust is never granted implicitly and must be continually evaluated**. ZTA is a direct response to threats posed by cyber-attacks, replacing the legacy “castle wall” security designs that allows users to move unmonitored around a system once past the initial security login. Per NIST 800-207², ZTA assumes an attacker is always present in the environment, and no environment is safe. Protections include minimizing access to only those authorized and continually authenticating and authorizing identity, explicitly authenticating and authorizing all subjects, assets and workflows. By this definition, ZTA provides exactly the kind of protections the President says American citizens are entitled.

Today we are a nation online. We have a national crisis of identity fraud. The question of digital attestation is at the forefront of important conversations including chain-of-custody of the American vote, vetting citizens, legal issues around the collection and use of PII, and the elimination of identity theft.

IdentityCare is a touchless biometric attestation system for enterprise designed for ZTA. IdentityCare is essentially a transaction credential for ZTA. This means that it is perfectly suited for attesting to all transaction/interactions within a voting system, whether it be actual voting, any handling of data, or the maintenance of the voting machines, establishing Zero-Trust level traceability throughout the various chain-of-custody methodologies. IdentityCare is a proven enterprise biometric accurate and reliable enough to minimize errors, including false positives and false negatives, robust enough to resist spoofing attempts, and resistant to AI deepfakes. IdentityCare’s biometric is also patented for how it protects user privacy and is compliant with European GDPR legislation, making it suitable for use both within and outside the US.

¹ <https://www.whitehouse.gov/presidential-actions/2025/03/preserving-and-protecting-the-integrity-of-american-elections/> Income

² <https://csrc.nist.gov/pubs/sp/800/207/final>

Applied to US Citizenship, IdentityCare would enhance the safety and security for all US citizens by accurately recognizing any US citizen at the border or anywhere in the world. It would enable passport-less travel, secure digital transactions, personalized preferences and automatic settings based on individual profiles, integrated directly into any identity management function, bestowing all US citizens with the benefit of online identity safety and assurance.

There is a distinction between a national register of citizens vs a database of identifiers providing a citizenship credentialing system. The benefits of the latter to both the government and the individual citizen way outweigh the former, bringing an unparalleled almost “VIP-membership” aura to the idea of Citizenship, extensible to all areas of everyday life. Identification as a *benefit* of citizenship.

How It Works

IdentityCare technology offers a **frictionless** user experience with high accuracy and speed, exceeding 99.9% matching accuracy and less than one second of user interaction.

Millions of epidermal data points are collected from a participating user’s face in an instant, using a near-infrared light source, ensuring privacy, and **eliminating gender and race bias**. Proprietary algorithms discard all but around 5% of this data in the creation of an extremely accurate biometric identifier containing *no personal information*. Enrollment takes less than 15 seconds. Authentication is less than a second. This proprietary, patented near-infrared facial recognition technology has been tested and whitelisted by 45% of the Fortune 100, within direct access control. It has never been hacked, spoofed, or allowed a false entry, providing reliable and accurate frictionless access. IdentityCare is a FIDO2 compatible biometric solution ideally suited for passkey requirements, making it ideal for various applications, from devices to enterprise systems.³

IdentityCare holds IP in NIR biometrics with asynchronous keys, 1:N architecture (dynamic templates and collision detection), and privacy. To protect its IP and ensure licensing revenue, IdentityCare relies on U.S. patents based on asynchronous credential keys from biometric information. Subsequent U.S. utility patents were filed as continuations to become part of larger systems/apps like the “Pluggable Authorized Biometric” within FIDO2 standard adopted by Apple, Google, and Microsoft.

IdentityCare would give US citizens unparalleled protections when it comes to proving citizenship, including for purposes of income tax submission and refund collections, travel identification and of course, voting. A US Citizen Registry Identifier could be used as a ZTA-compliant, privacy compliant online identifier for all kinds of additional online commerce and transactions.

With IdentityCare used as a credential to attest to the identity of every voter, US elections would be unmarred by fraud, errors, and suspicions, and American citizens would have true Zero-Trust traceability of their votes, exactly as the President calls for in the EO. “Above all, elections must be honest and worthy of the public trust, requiring voting methods that produce a voter-verifiable paper record allowing voters to efficiently check their votes to protect against fraud or mistake.” Along with conformance with policy, a federally mandated migration to Zero-Trust Architecture with IdentityCare in the electoral is exactly the solution called for to achieve the President’s objective to preserve and protect the integrity of American elections.

Please contact Jason Townsend at IdentityCare for further information.

jason@identitycareid.com • 913 208-7224

³ No biometric before the IdentityCare credential has ever demonstrated the accuracy or reliability to be used for anything other than secondary verification in enterprise access control.