# Securing Nigeria's Digital Future: E-Governance Practices at The Nigerian Immigration Service (NIS), 2015-2024

C. A. AKUJURU (PH. D)[1], NKWONTA, OBIANUJU STELLA (M.SC)[2]
[1, 2]*Department of Political Science (Public Administration), Faculty of Social Science Rivers state University, Nkpolu-Oroworukwo Port Harcourt, Nigeria*

***Abstract-*** ***This study examines the implementation of e-governance practices at the Nigerian Immigration Service (NIS) with a focus on digital transformation initiatives between 2015 and 2023. The NIS, as a critical agency responsible for border management, passport issuance, and immigration control, has experienced significant challenges in service delivery that could be addressed through effective e-governance strategies. These challenges include lengthy processing times, limited accessibility, operational inefficiencies, and vulnerability to corruption that undermine public trust and confidence in the immigration system. Using a descriptive research approach and secondary data analysis, this study explores the current state of digital transformation at the NIS, examining initiatives such as the e-passport system, online visa application platforms, border management information systems, and digitalized residence permit processing. The research is anchored on Institutional Theory and Network Governance Theory, which provide frameworks for understanding how the NIS's digital transformation is shaped by institutional pressures, legitimacy concerns, and the complex networks of stakeholders involved in immigration management. Findings reveal that while Nigeria has made notable progress in immigration service digitalization, particularly in urban centers and international airports, significant obstacles remain including substantial infrastructure deficits, digital literacy gaps among staff and service users, inadequate funding for technological development, cultural resistance to digital transformation, and weaknesses in data governance frameworks. The empirical evidence suggests that when effectively implemented, e-governance initiatives at the NIS can substantially improve service efficiency, enhance transparency, strengthen national security, and expand accessibility for citizens and foreign visitors. However, concerns about digital exclusion highlight the need for balanced strategies that ensure equitable access across geographical regions and socioeconomic groups. The study recommends comprehensive policy frameworks, sustained infrastructure investment, specialized training programs, robust data protection mechanisms, and periodic system evaluations to enhance digital service delivery at the Nigerian Immigration Service.***

***Indexed Terms-*** ***Nigerian Immigration Service, E-Governance, Digital Transformation, Border Management, National Security, Public Service Delivery.***

## I. INTRODUCTION

The Nigerian Immigration Service (NIS) represents a fundamental institution in Nigeria's governance architecture, entrusted with the critical responsibilities of border control, passport issuance, visa administration, and the management of foreign nationals within Nigerian territory (Adeola & Oluyemi, 2019). As Nwagwu (2020) observes, this agency plays an essential role in national security, identity management, and facilitation of legitimate travel and migration, functioning as both a service provider to citizens and visitors and a security organization safeguarding Nigeria's territorial integrity. The effective performance of the NIS directly impacts Nigeria's international relationships, tourism potential, diaspora engagement, and ability to manage migration flows in an increasingly interconnected global environment (Adedeji, 2021). According to Ocheni and Nwankwo (2022), the

Immigration Service represents one of the most citizen-facing agencies of the Nigerian government, with its operational effectiveness significantly influencing public perceptions of governance quality and administrative competence. The agency's performance therefore has far-reaching implications not only for security and migration management but also for Nigeria's economic development, international reputation, and public service delivery standards (Adepoju, 2018).

However, the traditional immigration administration system in Nigeria has been characterized by numerous challenges including lengthy processing times, cumbersome application procedures, limited accessibility, and operational inefficiencies that undermine service effectiveness. These systemic problems have developed over decades due to factors including outdated operational models, inadequate infrastructure, limited technological adoption, and resistance to procedural innovations within the organizational culture (Idowu, 2020). The continued reliance on paper-based processes created numerous vulnerabilities including document losses, data inconsistencies, opportunities for corrupt practices, and security weaknesses that compromised the integrity of Nigeria's immigration system (Ajibola, 2022). Manual verification procedures at border points created significant bottlenecks, increasing processing times while potentially allowing security threats to exploit system inefficiencies to circumvent proper controls (Ogbonna, 2021). The centralization of many immigration services necessitated multiple in-person visits and created geographical barriers for Nigerians living far from major service centers, imposing substantial time and financial costs on service users while undermining accessibility (Nwankwo, 2019). The accumulated effect of these challenges has contributed significantly to public frustration with immigration services and raised serious questions about the system's capacity to fulfill its dual mandate of service delivery and security enforcement in the twenty-first century.

In recent years, particularly during the 2015-2024 period, the emergence of information and communication technologies (ICTs) has presented unprecedented opportunities for transforming immigration management processes and enhancing service delivery. E-governance in immigration services refers to the application of digital technologies to streamline application processes, improve identity verification, enhance accessibility to services, strengthen security controls, and increase transparency in operations. When effectively implemented, digital immigration systems can significantly reduce processing times, minimize human intervention points that create corruption vulnerabilities, strengthen identity verification through biometric capabilities, and provide remote service access that overcomes geographical limitations (Eneanya, 2020). The integration of various immigration databases with other security and identity management systems creates powerful tools for intelligence gathering, security screening, and enforcement operations that were impossible under manual systems (Okafor & Nwaneri, 2021). The adoption of e-governance in Nigeria's immigration services represents a paradigm shift from traditional paper-based processes to digital systems that promise greater efficiency, security, accessibility, and transparency in both service delivery and enforcement functions.

The global COVID-19 pandemic during 2020-2022 accelerated the need for digital transformation across all sectors, including immigration and border management. With physical interactions restricted during lockdowns, the NIS was compelled to embrace technological solutions to ensure continuity in essential services while implementing new health screening requirements at borders (Oyedele, 2021). The pandemic-driven travel restrictions and health security measures necessitated more sophisticated systems for traveler tracking, health status verification, and contactless processing, highlighting both the potential of digital immigration management and the challenges of implementing such systems in the Nigerian context (Adebayo, 2022). This crisis-driven adaptation demonstrated the critical importance of digital readiness in ensuring institutional resilience during emergencies, while also revealing significant gaps in Nigeria's immigration technology infrastructure and digital capacity. The pandemic experience provided valuable lessons about both the possibilities and limitations of digital immigration services in Nigeria, offering insights that continue to inform ongoing transformation efforts through 2024.

This study examines the implementation of e-governance practices at the Nigerian Immigration Service between 2015 and 2024, focusing on the strategic approaches, current initiatives, challenges, and ethical considerations. By analyzing the trajectory of digital transformation in Nigeria's immigration system during this specific period, this research aims to contribute to the growing body of knowledge on public service digitalization and provide insights for enhancing e-governance in Nigeria's border management and immigration control. The study employs a descriptive research methodology based on comprehensive analysis of secondary data, including government reports, academic literature, policy documents, and case studies of digital immigration initiatives. In conducting this analysis, the research is guided by the Technology Acceptance Model (TAM) and Innovation Diffusion Theory (IDT) as theoretical frameworks for understanding the factors affecting the adoption and utilization of digital technologies within the NIS ecosystem during the 2015-2024 timeframe. The findings and recommendations from this study are intended to inform policy formulation, implementation strategies, and capacity development initiatives for advancing Nigeria's digital immigration agenda in alignment with global best practices and local contextual realities.

Statement of the Problem

The Nigerian Immigration Service faces significant challenges that impede effective service delivery and the fulfillment of its security mandate during the 2015-2024 period. These include lengthy processing times for passports and visas, cumbersome application procedures, inefficient border controls, limited accessibility to services, and vulnerability to document fraud and corruption. According to the 2022 NIS Performance Report, passport processing times averaged 8-12 weeks against the officially stipulated 3-week timeline, while visa approvals frequently exceeded the 48-hour service level agreement, creating significant inconveniences for applicants and potentially damaging Nigeria's business and tourism prospects. The manual verification procedures at many border crossings result in processing times of 45-60 minutes per traveler during peak periods, creating long queues, traveler frustration, and potential security vulnerabilities as officers face pressure to expedite checks (Presidential Enabling Business Environment Council, 2023). The geographical distribution of immigration offices and service centers has created significant accessibility disparities, with residents of rural areas and smaller states often required to travel long distances to access basic immigration services, imposing disproportionate costs in time and money on these populations. The combination of processing delays, accessibility limitations, and procedural inefficiencies has fostered perceptions of the NIS as bureaucratically cumbersome and service-deficient, undermining public confidence in this critical institution despite its essential national functions.

The traditional paper-based operations of the NIS have created numerous vulnerabilities that compromise both service quality and national security objectives. The manual documentation systems generate significant risks of data inconsistency, with applicant information often varying across different databases and paper records, creating identity verification challenges and potential security gaps. Physical document storage creates vulnerabilities to damage, loss, and unauthorized access, with a 2021 audit revealing that approximately 8% of paper files requested for verification could not be located in their designated storage locations (Office of the Auditor-General, 2021). Manual cash payment systems for various services create opportunities for financial irregularities, with studies indicating that unofficial "expedition fees" add 15-30% to the official cost of immigration services for many applicants (Transparency International, 2022). The limited integration between various immigration databases and other security systems creates information silos that prevent comprehensive verification checks, potentially allowing individuals with criminal records or security concerns to avoid detection during immigration processing. These operational vulnerabilities not only undermine service quality but also create potential national security risks by compromising the integrity of Nigeria's immigration controls.

While e-governance presents a potential solution to these challenges, its implementation at the NIS during the 2015-2024 period has been uneven and faces numerous obstacles. These include inadequate ICT infrastructure, insufficient funding, limited digital

literacy among immigration officers and service users, resistance to change, and concerns about data security and privacy. A 2023 assessment of digital readiness across NIS offices revealed that only 47% had reliable internet connectivity, 52% experienced power supply challenges affecting system uptime, and 63% reported insufficient computer hardware to fully digitalize operations (Ministry of Interior, 2023). The current budgetary allocation for ICT development at the NIS averages 5.8% of total expenditure, significantly below the internationally recommended minimum of 15% for agencies undergoing digital transformation (National Planning Commission, 2022). Surveys indicate that approximately 54% of immigration officers demonstrate inadequate digital competencies for effectively utilizing advanced border management systems, while over 40% express concerns about technology replacing human roles in the immigration process (Adebisi & Olatunji, 2023). Additionally, the absence of comprehensive legal frameworks specifically addressing digital immigration operations has created uncertainties regarding the legal validity of certain electronic processes, data protection responsibilities, and cross-border information sharing protocols. These implementation challenges have resulted in fragmented digitalization, with advanced systems operational at international airports and headquarters while many land borders and rural offices continue to rely predominantly on manual processes (Border Management Technology Assessment, 2022).

This study addresses the gap in understanding how e-governance has been effectively implemented at the Nigerian Immigration Service between 2015 and 2024 to overcome these challenges and enhance both service delivery and security operations. By examining the current state of digital immigration initiatives, identifying key implementation barriers, and analyzing successful strategies from comparable contexts, this research aims to provide evidence-based recommendations for sustainable digital transformation of Nigeria's immigration system. The study also explores the ethical dimensions of digital immigration management, including concerns about privacy, surveillance, digital divide, and the potential impacts of technology on vulnerable migrant populations. In focusing on both operational and ethical aspects of e-governance in immigration during this specific period, this research contributes to developing implementation approaches that balance technological innovation with core values of accessibility, efficiency, privacy, and security. Through this comprehensive examination, the study seeks to inform policy formulation, implementation strategies, and capacity development initiatives that can advance Nigeria's digital immigration agenda while maintaining alignment with human rights principles and international standards of migration management.

Aim and Objectives of the Study

The main aim of this study is to examine the implementation of e-governance practices at the Nigerian Immigration Service during the 2015-2024 period and extract lessons that can inform digital transformation of immigration management systems in Nigeria. The specific objectives include to:

1. Analyze the digitalization strategies and implementation approaches adopted by the NIS in its transition from paper-based to digital immigration management systems between 2015 and 2024.
2. Assess the impact of the NIS's digital transformation on service delivery efficiency, accessibility, security effectiveness, and user experiences during the study period.
3. Identify the key challenges encountered during the NIS's e-governance implementation from 2015 to 2024 and the strategies employed to address them.

Research Questions

Based on the objectives, this study seeks to answer the following research questions:

1. What digitalization strategies and implementation approaches were adopted by the NIS in its transition from paper-based to digital immigration management systems between 2015 and 2024?
2. How has the NIS's digital transformation impacted service delivery efficiency,

accessibility, security effectiveness, and user experiences during the 2015-2024 period?

3. What key challenges were encountered during the NIS's e-governance implementation from 2015 to 2024, and what strategies were employed to address them?

## Theoretical Framework

### Institutional Theory

The study is anchored on Institutional Theory propounded by scholars including Meyer and Rowan (1977), DiMaggio and Powell (1983), and Scott (1995), which explains how organizational structures and behaviors are shaped by normative, regulatory, and cultural-cognitive forces in their institutional environments. Institutional Theory conceptualizes organizations not merely as rational entities pursuing technical efficiency, but as social actors seeking legitimacy within their institutional contexts through conformity to established rules, norms, and belief systems. According to Scott (2008), institutions consist of "regulative, normative, and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life." In the context of public organizations like the Nigerian Immigration Service, institutional theory offers valuable insights into how digital transformation is influenced by formal regulations, professional standards, cultural expectations, and taken-for-granted assumptions about appropriate organizational forms and practices.

The basic assumptions of Institutional Theory include the premise that organizations seek legitimacy as much as efficiency, often adopting structures and practices that conform to environmental expectations regardless of their immediate technical value. The theory assumes that organizational fields develop shared understandings and practices through processes of institutional isomorphism, with organizations becoming increasingly similar as they respond to common regulatory, normative, and mimetic pressures. Institutional Theory further assumes that organizational structures often become decoupled from actual practices, with formal procedures sometimes serving ceremonial purposes rather than directly enhancing technical performance. Another core assumption is that institutions exert powerful constraints on organizational actors through taken-for-granted scripts, rules, and classifications that define appropriate behavior, making certain actions seem natural while others appear unthinkable. The model also assumes that while institutions are generally stable, they undergo processes of institutionalization, deinstitutionalization, and reinstitutionalization over time as new practices emerge, gain legitimacy, and potentially replace existing arrangements.

The underlying principles of Institutional Theory emphasize the social embeddedness of organizational behavior and the powerful role of cognitive frameworks in shaping perceptions of legitimacy and appropriateness. The theory incorporates the principle of institutional isomorphism, identifying three mechanisms through which organizations in a field become more similar: coercive isomorphism (resulting from political influence and legitimacy concerns), mimetic isomorphism (copying other organizations in response to uncertainty), and normative isomorphism (associated with professionalization). Another principle is the distinction between technical and institutional environments, recognizing that some organizations face stronger pressures for efficiency while others are more constrained by institutional expectations for conformity to societal norms. The theory further embraces the concept of institutional logics, acknowledging that organizations often operate within multiple, sometimes conflicting belief systems that provide guidelines for organizing and interpreting social reality.

Despite its explanatory power, Institutional Theory has faced criticism for sometimes underemphasizing agency and strategic action in institutional contexts, portraying organizations as overly passive recipients of institutional pressures (Oliver, 1991). Critics note that the theory has historically paid insufficient attention to how actors within organizations can strategically respond to institutional demands through tactics ranging from acquiescence to defiance (Lawrence & Suddaby, 2006). Some scholars argue that Institutional Theory has been challenged to adequately explain institutional change, particularly how new practices emerge and gain legitimacy within established institutional frameworks (Greenwood & Hinings, 1996). Additionally, the theory has been

criticized for sometimes treating institutions as overly stable and monolithic, underestimating the internal contradictions and ongoing contestation that characterize many institutional contexts (Seo & Creed, 2002). The Network Governance Theory addresses many of these limitations by focusing more explicitly on how diverse actors negotiate, coordinate, and collaborate in complex governance arrangements, providing a complementary perspective that enriches understanding of organizational change processes in networked environments like Nigeria's immigration system.

The relevance of Institutional Theory to this study lies in its ability to explain how the NIS's digital transformation is shaped by multiple institutional pressures, including regulatory mandates from government authorities, international standards for border management and immigration control, and prevailing norms about appropriate technological solutions in security agencies. The theory provides a framework for understanding how the NIS's digitalization efforts may reflect not only technical efficiency concerns but also legitimacy-seeking behavior as the organization strives to conform to expectations from stakeholders including government leaders, international partners, and the Nigerian public. Institutional Theory helps explain why certain digital solutions might be adopted ceremonially without full implementation, particularly when external pressures for modernization exceed organizational capacity for substantive change. The theory's emphasis on isomorphic pressures provides insights into how the NIS's digital transformation may be influenced by mimetic processes as it adopts systems similar to those in neighboring countries or international benchmarks.

The application of Institutional Theory to this study enables analysis of how different institutional mechanisms shape the NIS's e-governance implementation. The theory helps interpret regulatory changes such as the Immigration Act of 2015 and executive directives on service improvement as coercive pressures compelling digital adoption regardless of organizational readiness. Normative influences from professional networks, international organizations, and training institutions can be analyzed as sources of pressure for technological modernization. The concept of mimetic isomorphism provides a framework for understanding how uncertainty about appropriate digital solutions might lead the NIS to model its approaches on seemingly successful examples from other immigration authorities. By applying Institutional Theory's multi-level perspective, this study can systematically assess how the NIS's digitalization reflects and responds to regulative, normative, and cultural-cognitive elements in its institutional environment, extracting insights about the complex interplay between technical requirements and institutional pressures in Nigeria's immigration e-governance journey.

Network Governance Theory

The study also utilized Network Governance Theory developed by scholars including Rhodes (1997), Provan and Kenis (2008), and Sørensen and Torfing (2007) to provide a complementary theoretical framework for understanding the NIS's e-governance implementation. Network Governance Theory conceptualizes governance as occurring through networks of interdependent actors rather than through hierarchical authority or market mechanisms alone. This perspective views governance as "the self-organizing, interorganizational networks characterized by interdependence, resource exchange, rules of the game, and significant autonomy from the state" (Rhodes, 1997). In the context of immigration management, Network Governance Theory offers insights into how the NIS coordinates with diverse stakeholders including other government agencies, international partners, private technology providers, and civil society organizations to deliver integrated digital services and security functions.

The basic assumptions of Network Governance Theory include the premise that contemporary governance challenges often exceed the capacity of single organizations, requiring coordination across network structures that span organizational and sectoral boundaries. The theory assumes that actors within governance networks are interdependent, possessing different resources and capabilities that must be combined to address complex public problems effectively. Network Governance Theory further assumes that interactions within governance networks

involve ongoing negotiation and trust-building rather than simple command-and-control relationships, with network stability dependent on developing shared understanding and expectations among diverse participants. Another core assumption is that governance networks vary in their formality, scope, and structural arrangements, ranging from loosely coordinated partnerships to highly institutionalized collaboration systems with dedicated management structures. The theory also assumes that while networks can enhance governance capacity through resource sharing and coordinated action, they present distinct accountability and coordination challenges compared to traditional hierarchical governance.

The underlying principles of Network Governance Theory emphasize the relational nature of contemporary governance and the importance of collaborative approaches for addressing complex public challenges. The theory incorporates the principle of resource interdependence, recognizing that effective governance often requires combining dispersed knowledge, authority, and operational capabilities across multiple organizations. Another principle is the distinction between different network governance modes identified by Provan and Kenis (2008): participant-governed networks (managed collectively by members), lead organization-governed networks (coordinated by a dominant member), and network administrative organizations (managed by dedicated entities created specifically for network governance). The theory further embraces the concept of meta-governance, acknowledging the role of government in steering, facilitating, and regulating governance networks without reverting to direct hierarchical control. Additionally, Network Governance Theory recognizes the dynamic tension between flexibility and stability in governance arrangements, with networks requiring sufficient structure for effective coordination while maintaining adaptability to changing circumstances.

While powerful in explaining collaborative governance approaches, Network Governance Theory has faced criticism regarding potential democratic deficits in network arrangements where decision-making occurs through informal negotiations rather than formal democratic processes (Klijn & Skelcher, 2007). Critics note that governance networks sometimes lack transparency and clear lines of accountability, making it difficult for citizens to understand and influence decisions that affect them (Papadopoulos, 2007). The theory has also been challenged regarding assumptions about network effectiveness, with some scholars questioning whether networked approaches necessarily produce better outcomes than hierarchical or market-based alternatives in all contexts (Turrini et al., 2010). Additionally, some critics argue that Network Governance Theory sometimes understates power asymmetries within networks, presenting an overly consensual view of collaborative governance that masks how stronger actors can dominate agenda-setting and resource allocation (Davies, 2011). Despite these limitations, Network Governance Theory offers valuable insights that complement Institutional Theory, particularly in understanding how diverse actors coordinate digitalization efforts across organizational boundaries in Nigeria's immigration management system.

The relevance of Network Governance Theory to this study lies in its ability to explain how the NIS's digital transformation involves coordination across a complex network of stakeholders rather than occurring within organizational boundaries alone. The theory provides a framework for understanding how the NIS navigates relationships with multiple actors including the Ministry of Interior, security agencies, international organizations, technology vendors, and service users to implement integrated digital solutions. Network Governance Theory helps explain why certain digital initiatives succeed or struggle based on the quality of network coordination rather than just internal organizational factors. The theory's emphasis on resource interdependence provides insights into how the NIS leverages external resources including international technical assistance, private sector expertise, and inter-agency data sharing to overcome internal capacity limitations.

The application of Network Governance Theory to this study enables examination of how the NIS's implementation strategies reflect and respond to network governance challenges. The theory helps interpret the NIS's cross-agency coordination mechanisms as attempts to establish effective network governance arrangements for integrated identity

management and security information sharing. Network Governance Theory provides a theoretical basis for understanding the NIS's partnerships with international organizations and technology providers as networked approaches to accessing resources and capabilities beyond internal capacity. The model also helps explain implementation variations across different locations by considering how local network configurations affect resource availability and coordination quality. By applying Network Governance Theory alongside Institutional Theory, this study develops a more comprehensive understanding of how the NIS's e-governance implementation unfolds within both institutional constraints and network relationships, extracting richer insights for future digital transformation initiatives in Nigeria's security and immigration management ecosystem.

Conceptual Clarifications

E-Governance in Immigration Management

E-governance in immigration management represents the application of information and communication technologies (ICTs) to transform how immigration services are delivered and how border control functions are executed. The International Organization for Migration (2021) defines e-immigration as "the use of digital technologies to enhance the efficiency, security, and accessibility of immigration services while strengthening identity verification and border management capabilities." This definition encompasses both the service delivery and enforcement dimensions of immigration functions. Ibrahim (2020) offers a more comprehensive conceptualization, describing e-immigration as "the digitalization of immigration processes, identity management systems, and border control mechanisms to enhance national security, improve service delivery, and facilitate legitimate travel and migration."

E-governance in immigration encompasses several distinct but interconnected dimensions:

1. E-Services: The delivery of immigration services through digital channels, enabling citizens and foreign nationals to access services such as passport and visa applications remotely, conveniently, and with reduced procedural complexity (Adeniran, 2020). The NIS's online application platforms exemplify this dimension.
2. E-Administration: The application of digital technologies to improve internal immigration operations, including documentation management, workflow automation, and administrative processes (Adesina, 2021). The NIS's digital file management and case tracking systems represent this dimension.
3. E-Identity: Digital systems for capturing, storing, verifying, and managing identity information of citizens and foreign nationals, often incorporating biometric components for enhanced security and reliability (Adebayo, 2019). The NIS's biometric passport system and electronic residence permits reflect this dimension.
4. E-Borders: Technological solutions for border surveillance, traveler processing, risk assessment, and cross-border information sharing to enhance security while facilitating legitimate movement (Oluwadare, 2022). The NIS's Border Management Information System exemplifies this dimension.
5. E-Intelligence: Digital systems that analyze immigration data to identify patterns, detect anomalies, and provide actionable insights for security operations and policy formulation (National Security Advisor's Office, 2021). The NIS's analytics capabilities for tracking overstays and identifying suspicious travel patterns represent this dimension.

The concept of e-immigration has evolved from early digitization efforts focused primarily on computerizing existing processes to more transformative approaches that reimagine immigration management for the digital age. Contemporary e-immigration emphasizes integrated identity management, risk-based processing, international interoperability, and data-driven decision-making (International Civil Aviation Organization, 2022). These advanced concepts have informed the later stages of the NIS's digital evolution, particularly its biometric systems and risk assessment capabilities.

Digital Identity and Border Management Systems

Digital identity systems represent a fundamental component of modern immigration management, providing the technological foundation for reliable identification and verification of citizens and foreign nationals. The World Bank (2022) defines digital identity as "a set of electronically captured and stored attributes and credentials that can uniquely identify a person," emphasizing the transformative potential of such systems for both service delivery and security functions. In the immigration context, digital identity systems enable the reliable linking of individuals to their travel documents, immigration history, and security profiles, significantly enhancing both processing efficiency and security effectiveness (Interpol, 2021).

Key components of digital identity systems in immigration include:

1. Biometric Enrollment: The capture of unique physical characteristics such as fingerprints, facial images, and (increasingly) iris patterns to create reliable identity records that are difficult to forge or misuse. The NIS's e-passport system incorporates ten fingerprints and digital facial imagery for enhanced identity assurance.
2. Identity Databases: Centralized or distributed repositories of identity information that enable verification against previously captured records, supporting both immigration service delivery and border control functions. The NIS maintains several identity databases including the passport database, visa records system, and foreigner registration database.
3. Identity Verification Mechanisms: Technologies that match presented credentials against stored identity information, ranging from simple document verification to sophisticated biometric matching systems. The NIS employs various verification technologies including document readers, fingerprint scanners, and facial recognition systems at various touchpoints.
4. Credential Issuance: The production and personalization of secure documents such as passports, visas, and residence permits that incorporate both physical and digital security features. The NIS's passport personalization centers represent this component.
5. System Integration: The interconnection of identity systems with other relevant databases such as watchlists, criminal records, and international information sharing mechanisms to enhance security capabilities. The NIS's growing integration with Interpol databases exemplifies this dimension.

Border management systems complement digital identity capabilities by providing technological platforms for processing travelers, assessing risks, and maintaining border security. Modern border management technologies include:

1. Advance Passenger Information/Passenger Name Record (API/PNR) Systems: Electronic systems that receive traveler information from carriers before arrival, enabling pre-screening and risk assessment. The NIS has implemented API capabilities at major international airports with plans for nationwide expansion.
2. Automated Border Control Gates: Electronic gates that use biometric verification to automate the border crossing process for eligible travelers, enhancing both efficiency and security. The NIS has piloted such systems at Lagos and Abuja airports.
3. Mobile Border Technologies: Portable devices that enable immigration officers to verify documents and identities away from fixed inspection points, enhancing coverage and flexibility. The NIS has deployed mobile verification units at various land borders and marine entry points.
4. Integrated Border Management Information Systems: Comprehensive platforms that bring together various border functions including traveler processing, document verification, and risk assessment in a unified technological environment. The NIS's Border

Management Information System represents this approach.

5. Surveillance Technologies: Systems including cameras, sensors, drones, and monitoring equipment that enhance awareness of border areas and support enforcement operations. The NIS has implemented various surveillance technologies at strategic border locations.

The integration of digital identity and border management systems creates powerful capabilities for immigration authorities to balance their dual mandate of facilitating legitimate travel while preventing unauthorized entry and identifying security threats. However, these technologies also raise significant privacy, ethical, and human rights considerations that must be addressed through appropriate governance frameworks (United Nations High Commissioner for Refugees, 2021).

The Nigerian Immigration Service and its Functions

The Nigerian Immigration Service was established in 1958 as a department within the Nigeria Police Force before becoming an independent agency in 1963. The Immigration Act of 2015 currently governs the Service's operations, providing the legislative framework for its activities and responsibilities. As Nigeria's designated authority for immigration matters, the NIS is responsible for a wide range of functions related to border management, citizenship administration, and regulation of foreign nationals in Nigeria.

The NIS's core functions include:

1. Border Control: Managing entry and exit points including land borders, seaports, and airports; examining travel documents; determining admissibility of travelers; and preventing unauthorized entry or exit (Immigration Act, 2015). This function involves both facilitation of legitimate travel and enforcement actions against unauthorized migration.
2. Passport Administration: Issuing and managing Nigerian passports and other travel documents, including determining eligibility, processing applications, producing secure documents, and maintaining the integrity of Nigeria's passport system (Presidential Executive Order on Ease of Doing Business, 2017).
3. Visa Administration: Processing visa applications, determining eligibility of foreign visitors, issuing various categories of visas, and managing visa policies in alignment with Nigeria's diplomatic, economic, and security objectives (Visa Policy of Nigeria, 2020).
4. Residence Permits: Registering foreign nationals residing in Nigeria, issuing and renewing residence permits, monitoring compliance with residence conditions, and maintaining records of foreigners within Nigerian territory (Immigration Regulations, 2017).
5. Investigation and Enforcement: Identifying and apprehending persons violating immigration laws, conducting investigations into immigration offenses, and enforcing compliance with immigration requirements (Immigration Act, 2015).
6. Border Surveillance: Monitoring Nigeria's extensive land and maritime borders to prevent unauthorized crossings, smuggling, and transnational crimes in collaboration with other security agencies (National Border Management Strategy, 2019).
7. Migration Management: Implementing Nigeria's migration policies, collaborating with international organizations on migration issues, and managing programs related to diaspora engagement, labor migration, and return migration (National Migration Policy, 2015).

The NIS's role has evolved significantly over time, particularly in response to changing security challenges, international obligations, and technological developments. The Service now plays a critical role in Nigeria's national security architecture, with responsibilities extending beyond traditional immigration functions to include counterterrorism, human trafficking prevention, transnational crime interdiction, and international intelligence

collaboration (National Security Strategy, 2019). This evolution has necessitated significant enhancements in technological capabilities, operational approaches, and international cooperation mechanisms.

Immigration Services and National Security

Immigration services and national security share a complex and interdependent relationship, with immigration management increasingly recognized as a critical component of comprehensive security strategies. The National Security Strategy of Nigeria (2019) explicitly identifies border security and migration management as key dimensions of national security, recognizing that ineffective immigration controls can create vulnerabilities to terrorism, transnational crime, and other security threats. This security-centric perspective has significantly influenced the evolution of immigration services globally, including Nigeria's approach to immigration management.

Key dimensions of the immigration-security nexus include:

1. Border Security: Effective border management prevents unauthorized entry of individuals who may pose security threats while maintaining territorial integrity. Nigeria's extensive land borders (approximately 4,000 kilometers) present significant security challenges, with the NIS working to enhance technological and human capabilities for border protection (Presidential Committee on Small Arms and Light Weapons, 2021).
2. Identity Security: Reliable identification systems prevent the fraudulent acquisition or use of identity documents for criminal or terrorist purposes. The NIS's biometric passport system represents a key enhancement in identity security, with features designed to prevent forgery and misuse (African Union Passport Policy Framework, 2020).
3. Terrorist Mobility Interdiction: Immigration systems play a critical role in identifying and intercepting terrorist suspects through watchlist checking, suspicious travel pattern analysis, and international information sharing. The NIS's growing integration with Interpol databases enhances these capabilities (Counterterrorism Center, 2022).
4. Transnational Crime Combating: Immigration controls help identify and disrupt criminal networks involved in human trafficking, drug smuggling, and other cross-border crimes. The NIS's specialized units for trafficking interdiction represent this security function (UNODC, 2021).
5. Critical Infrastructure Protection: Immigration facilities themselves constitute critical national infrastructure requiring protection from physical and cyber threats. The NIS has enhanced security measures at key facilities including data centers, passport production sites, and border posts (Critical Infrastructure Protection Strategy, 2020).

While the security dimension of immigration is increasingly prominent, balancing security imperatives with service delivery objectives presents significant challenges. Excessive security focus can compromise efficiency, accessibility, and human rights considerations in immigration management. The International Organization for Migration (2021) advocates for a "facilitation-security balance" that protects national security while ensuring that legitimate travelers and migrants are treated with dignity and efficiency. This balance is particularly important for Nigeria, where economic development objectives require facilitating tourism, business travel, and skilled migration while addressing genuine security concerns.

The digitalization of immigration services presents both opportunities and challenges for this balance. Digital systems can enhance security through more reliable identity verification and information sharing while simultaneously improving service delivery through faster processing and enhanced accessibility. However, digital security measures must be implemented with appropriate oversight and safeguards to prevent misuse, discrimination, or disproportionate impacts on vulnerable populations (United Nations High Commissioner for Human Rights, 2020).

Technology Adoption in Public Security Organizations

Technology adoption in public security organizations like the NIS presents unique challenges and considerations that significantly influence e-governance implementation outcomes. Unlike typical government agencies focused primarily on service delivery, security organizations must balance operational efficiency with mission-critical security requirements, creating distinctive adoption dynamics (Bruneau & Matei, 2021). Understanding these contextual factors is essential for analyzing the NIS's digitalization journey and extracting transferable lessons.

Key dimensions of technology adoption in public security organizations include:

1. Security-Efficiency Tension: Security organizations must constantly balance the potential efficiency gains of new technologies against security considerations including confidentiality, integrity, and reliability (Loveday, 2018). The NIS faces this tension in determining appropriate access controls, system interconnections, and information sharing protocols for its digital systems.
2. Institutional Culture: Security organizations often exhibit distinctive cultural characteristics including hierarchical authority structures, procedure orientation, and risk aversion that can influence technology acceptance patterns (Chan, 2021). The NIS's organizational culture, shaped by its dual service-security mandate, creates specific adoption challenges that require contextually appropriate change management approaches.

3. Specialized Operational Requirements: Security technologies must meet distinctive operational needs including 24/7 reliability, field usability, interoperability with other security systems, and resilience under adverse conditions (Interpol, 2020). The NIS's border management technologies must function effectively in diverse environments ranging from high-traffic international airports to remote land borders with limited infrastructure.
4. Command Structure Influences: Hierarchical command structures typical in security organizations can significantly impact adoption processes, with senior leadership support critical for successful implementation (Peterson, 2019). The NIS's experience demonstrates the importance of securing buy-in across command levels to ensure consistent implementation throughout the organizational structure.
5. Security Classification Constraints: Information security requirements can limit technology testing, evaluation, and modification processes that are standard in other contexts (Nigerian Office of National Security, 2022). The NIS must navigate these constraints while still ensuring that systems meet operational requirements and user needs before full deployment.

Public security organizations like the NIS often exhibit distinctive technology adoption patterns characterized by thorough vetting before adoption, standardized implementation approaches, and significant emphasis on training and standard operating procedures (Adebayo & Omotoso, 2021). These patterns reflect the critical nature of these organizations' missions and the potential consequences of technology failures in security contexts. The NIS's digitalization journey must be understood within this specialized adoption context, recognizing that approaches suitable for regular government agencies may require significant adaptation for effective implementation in the immigration security environment.

Empirical Review

Adeyemo & Olufemi (2020) conducted a comprehensive assessment of digital transformation at the Nigerian Immigration Service between 2016 and 2019, examining implementation approaches and operational impacts across multiple service areas. The research employed a mixed-methods approach combining analysis of operational data from the NIS,

surveys of 420 service users (citizens, foreign nationals, and immigration consultants), and interviews with 35 NIS officers at various command levels. The study documented significant improvements in processing times following digitalization, with standard passport processing reduced from an average of 35 days in 2016 to 12 days by 2019, though still exceeding the officially targeted 3-day turnaround. Visa processing showed more dramatic improvement, with online applications processed within 48 hours in 78% of cases compared to 23% under the previous manual system. However, the researchers identified substantial variations in digital service performance across different NIS offices, with the five main passport issuing centers in Lagos and Abuja demonstrating significantly better metrics than smaller state commands. Survey results revealed moderate satisfaction rates among users of digital services, with 58% reporting positive experiences compared to 26% satisfaction with previous manual systems, though recurring complaints about system downtime, technical glitches, and limited customer support persisted across user groups. The study concluded that while the NIS's digital transformation had yielded substantial efficiency improvements, significant work remained to address infrastructure limitations, standardize service quality across locations, and enhance user support systems to maximize the potential benefits of digitalization.

Nwagwu & Ibrahim (2021) examined the implementation and effectiveness of digital border management technologies at Nigeria's international entry points, with particular focus on the Border Management Information System (BMIS) deployed at airports and select land borders. The study utilized a case study methodology incorporating border post observations, document analysis, and interviews with 42 stakeholders including immigration officers, border community representatives, and international partners supporting border technology initiatives. The research documented significant disparities in technology implementation across different border categories, with international airports achieving 85-92% digitalization of passenger processing, major land borders averaging 40-55% digital coverage, and remote land borders showing minimal digital presence with under 15% of crossings captured in electronic systems. At digitalized entry points, processing times decreased by an average of 76% for standard travelers, with particular efficiency gains in verifying travel document authenticity and checking against watchlists. However, the study identified critical challenges including power supply instability affecting system availability, connectivity limitations particularly at land borders, inadequate technical support for maintenance and troubleshooting, and integration gaps between the BMIS and other security databases. The researchers observed that effective digital border management was achieved only where comprehensive implementation approaches addressed infrastructure, training, and operational procedure modifications simultaneously. The study concluded that Nigeria's digital border management implementation demonstrated promising results at well-resourced entry points but required substantial additional investment to achieve consistent coverage across Nigeria's extensive borders, particularly the more remote land boundaries where security challenges are often most acute.

Okafor & Nwachukwu (2019) investigated the relationship between immigration digitalization and national security outcomes in Nigeria, examining how electronic systems affected security screening effectiveness, identity verification reliability, and enforcement capabilities. The research utilized statistical analysis of enforcement data from 2014-2018, classified security assessments from relevant agencies, and interviews with 28 security officials from the NIS and partner organizations. The study documented significant security enhancements following digital implementation, with watchlist matches increasing 380% after integration of immigration systems with Interpol databases, detection of fraudulent documents improving by 215% following deployment of electronic document verification systems, and identification of suspicious travel patterns enhancing by 140% through analytics capabilities. Additionally, the study identified substantial improvements in interagency information sharing, with digital systems enabling the NIS to provide actionable intelligence to partner security agencies in 68% less time than under paper-based systems. However, the researchers also identified significant security vulnerabilities including incomplete biometric enrollment of the resident population, limited coverage of digital systems at

smaller entry points, and inadequate cybersecurity measures protecting immigration databases. The study concluded that while digitalization had significantly enhanced Nigeria's immigration security capabilities, the irregular implementation pattern created security asymmetries where strengthened controls at major entry points potentially diverted threats toward less-monitored border areas. The researchers emphasized the need for comprehensive rather than point-based digital security implementation to avoid creating "digital security gaps" that could be exploited by those seeking to evade proper immigration controls.

Adepoju & Adegoke (2022) examined user experiences with Nigeria's digital immigration services, focusing on accessibility, usability, and satisfaction across different demographic and geographic segments. The study employed a comprehensive survey methodology, collecting data from 1,830 users of various NIS digital services including passport applications, visa processing, residence permit management, and border crossing. The researchers supplemented quantitative survey data with focus group discussions involving 87 participants across six geopolitical zones. The study revealed significant disparities in service experiences based on location, digital literacy, and socioeconomic status. Urban users reported 74% satisfaction with digital services compared to 41% among rural users, while those with higher education reported 68% satisfaction versus 37% among users with limited formal education. The research identified specific user challenges including complex interface design (reported by 58% of users), limited local language support (affecting 43% of users), difficulties with required document uploads (experienced by 62% of users), and payment processing complications (affecting 51% of users). Digital literacy emerged as a critical factor, with 67% of users reporting that they required assistance from others to complete online applications. Importantly, 72% of users still reported interacting with middlemen or agents despite the availability of direct digital channels, suggesting that intermediaries had adapted to the digital environment rather than being eliminated by it. The researchers concluded that while digital services had improved accessibility for digitally literate, urban populations, significant barriers remained for rural, less educated, and older users. The study recommended comprehensive user experience enhancements including simplified interfaces, local language options, improved help systems, and community access points to ensure more equitable benefits from Nigeria's digital immigration services.

Eneanya & Adebayo (2020) analyzed the change management approaches employed during the NIS's digital transformation, examining how organizational, cultural, and human resource factors influenced implementation outcomes. The research utilized document analysis, semi-structured interviews with 46 NIS personnel across ranks, and observation of change management activities at headquarters and five state commands. The study identified critical success factors in the NIS's change management approach, including: involvement of respected senior officers as digital champions; practical demonstration of system benefits rather than theoretical explanations; phased implementation allowing for adjustment and learning; and integration of digital metrics into performance evaluation systems. The research documented significant variations in acceptance levels across different officer segments, with younger officers (under 40) demonstrating 82% acceptance of digital systems compared to 47% among older officers (over 50). Educational background also proved influential, with officers possessing computer-related qualifications showing 78% acceptance versus 51% among those without such background. The researchers identified several implementation challenges including insufficient communication about system changes, inadequate training before deployment, limited involvement of frontline officers in system design, and concerns about job security among personnel performing tasks targeted for automation. The study concluded that effective change management in security organizations like the NIS requires balanced attention to both technical and human dimensions, with particular emphasis on addressing security-specific concerns about system reliability, procedural modifications, and command structure impacts. The researchers recommended more comprehensive stakeholder engagement throughout the digitalization process, enhanced training programs tailored to different officer segments, and clearer communication about how digital systems would affect roles and responsibilities within the organization.

## Methodology

This study employs a qualitative research approach utilizing secondary data to examine the NIS's digital transformation journey. The research is based on documentary analysis of various sources providing insights into the implementation, impact, and challenges of the NIS's e-governance initiatives, including: official NIS documents (annual reports, strategic plans, policy documents); government publications (e-governance policy documents, ministry reports, legislative materials); international agency reports (International Organization for Migration assessments, UNDP e-governance surveys); academic literature (peer-reviewed journal articles, books, conference papers); industry and professional reports (security technology assessments, digital identity studies); and media reports providing contemporaneous accounts of the NIS's digital initiatives. The data analysis utilizes thematic content analysis to identify patterns, extract insights, and develop evidence-based conclusions regarding the NIS's e-governance implementation, with triangulation across multiple sources enhancing the reliability of findings by corroborating information and identifying areas of consensus or divergence in assessments of the NIS's transformation. This methodological approach is appropriate given the historical nature of the case study, the availability of substantial documentary evidence, and the objective of extracting transferable lessons rather than generating primary data.

## Findings and Discussions

### Implementation Strategies and Digital Initiatives

The analysis of the NIS's digital transformation reveals several key implementation strategies that contributed to successful e-governance adoption in Nigeria's immigration system. The phased implementation approach identified by Eneanya & Adebayo (2020) emerged as a significant factor in managing transition complexities and building acceptance within the hierarchical organizational structure. Rather than attempting comprehensive digitalization simultaneously across all functions and locations, the NIS adopted a sequential approach beginning with passport application processing, followed by visa administration, and eventually expanding to border management systems. This incremental strategy allowed for learning, adaptation, and capacity building while minimizing disruption to critical security operations and essential public services. The approach aligns with Rogers' (2003) Innovation Diffusion Theory, particularly the principles of trialability and observability, by allowing stakeholders to experience benefits in one functional area before expanding to others. The prioritization of international airports and headquarters operations for initial digital deployment demonstrated a strategic focus on high-volume, high-visibility service points that could demonstrate clear efficiency gains and build momentum for broader implementation.

The NIS's digital initiatives evolved from basic computerization to increasingly sophisticated integrated systems over time, with core components including: the e-passport system incorporating biometric identification and enhanced document security features; the online visa application platform enabling remote application submission and electronic approval processes; the Border Management Information System (BMIS) supporting traveler processing and security screening at entry points; and the digitalized residence permit system for managing foreign nationals within Nigerian territory. The leadership commitment to digital transformation, manifested through policy consistency despite changes in service leadership, provided critical continuity for long-term implementation efforts. However, Adeyemo & Olufemi's (2020) identification of significant variations in digital service performance across different NIS offices highlights implementation inconsistencies that have created an uneven digital landscape, with well-resourced command centers demonstrating substantially better performance than smaller offices. These findings suggest that while the NIS's implementation strategy successfully established digital foundations, insufficient attention to standardization and resource equalization across locations has limited the full potential of the transformation. The ongoing challenge remains extending the benefits of digital immigration services beyond major urban centers to create consistent nationwide coverage, particularly at remote border points where security concerns are often most acute.

Impact and Outcomes

The evidence indicates that the NIS's digital transformation has delivered substantial improvements in both service delivery and security effectiveness, though with significant variations across service areas and locations. Adeyemo & Olufemi's (2020) documentation of reduced processing times for passports (from 35 days to 12 days) and visas (78% processed within 48 hours) demonstrates meaningful efficiency gains, though still falling short of official targets in some areas. These improvements align with broader public service modernization objectives while enhancing Nigeria's attractiveness for tourism, investment, and business travel. The enhanced security capabilities documented by Okafor & Nwachukwu (2019) represent equally important outcomes, with significant increases in watchlist matches (380%), fraudulent document detection (215%), and suspicious pattern identification (140%) following digital implementation. These security enhancements contribute directly to Nigeria's counter-terrorism, transnational crime prevention, and border security objectives, demonstrating how effectively implemented e-governance can simultaneously improve service quality and security effectiveness.

However, the accessibility and equity dimensions of the transformation reveal more complex outcomes. Adepoju & Adegoke's (2022) finding of significant disparities in satisfaction between urban (74%) and rural users (41%) highlights how digitalization can potentially reinforce or exacerbate existing social inequalities without specific measures to ensure inclusive implementation. The persistence of intermediaries despite direct digital channels, with 72% of users still reporting agent interactions, suggests that digital systems have altered rather than eliminated traditional service access patterns. The digital literacy barriers identified, with 67% of users requiring assistance to complete online applications, underscore the importance of user capacity considerations alongside technological development. These findings demonstrate that while the NIS's digital transformation has yielded substantial benefits, these advantages have not been equally distributed across Nigeria's population. The challenge moving forward involves extending digital benefits to underserved populations through targeted accessibility measures, simplified interfaces, and community support systems that can help bridge the digital divide in immigration service access. Additionally, the integration of immigration systems with other government databases has enhanced identity verification capabilities while creating a more coherent digital government ecosystem, though significant interoperability challenges remain, particularly with local government and informal identification systems that many Nigerians still primarily rely upon.

Challenges and Limitations

Despite documented successes, the NIS's digital transformation encountered several significant challenges that offer important lessons for e-governance implementation in security-focused organizations. Infrastructure limitations emerged as a persistent obstacle, with Nwagwu & Ibrahim's (2021) research highlighting how power supply instability and connectivity constraints affected system availability, particularly at land borders where digital coverage remained limited to 40-55% at major crossings and below 15% at remote points. These findings emphasize how underlying infrastructure deficiencies can fundamentally constrain digital government effectiveness regardless of system sophistication, underscoring the need for robust infrastructure development alongside digital system implementation. Digital literacy limitations among both staff and users created significant adoption barriers, with Eneanya & Adebayo (2020) documenting substantial variations in technology acceptance across officer demographics and Adepoju & Adegoke (2022) identifying user capability gaps that limited self-service utilization. These challenges highlight the importance of human capacity development as a critical complement to technological investment.

The security-specific adoption challenges identified by Eneanya & Adebayo (2020) reveal how the NIS's organizational character as a security institution influenced digitalization processes, with officers expressing concerns about system reliability for security-critical functions, procedural modifications that might compromise established security protocols,

and command structure impacts from changing information flows. Okafor & Nwachukwu's (2019) identification of cybersecurity vulnerabilities, including inadequate protection for immigration databases, highlights the new risk categories introduced by digitalization that require specialized expertise and resources to address. The uneven implementation pattern documented by multiple studies has created "digital security gaps" where strengthened controls at major entry points potentially divert threats toward less-monitored areas, demonstrating how partial digitalization in security contexts can create new vulnerabilities even while addressing others. These challenges collectively highlight the complexity of e-governance implementation in security-focused organizations like the NIS, where digitalization must address not only traditional service delivery concerns but also mission-critical security requirements. The findings suggest that successful digital transformation in such contexts requires balanced attention to infrastructure readiness, human capacity development, organizational culture considerations, comprehensive security coverage, and evolving cybersecurity requirements.

Conclusion and Recommendations

The Nigerian Immigration Service's digital transformation journey provides valuable insights into the potential, process, and challenges of e-governance implementation in security-focused public institutions. The evidence demonstrates that the NIS has achieved substantial improvements in both service delivery and security capabilities through strategic implementation of digital technologies. The reduction in processing times for passports and visas, expanded service accessibility through online platforms, enhanced detection of fraudulent documents and security threats, and improved information sharing with partner agencies represent significant public value creation through digital transformation. These outcomes align with Nigeria's broader ambitions for enhanced security, improved public services, and greater international competitiveness, while demonstrating the feasibility of effective digital government implementation despite contextual challenges.

The NIS's experience highlights several critical success factors for e-governance implementation in Nigeria's security agencies, including phased implementation approaches, leadership commitment across command levels, strategic prioritization of high-impact service areas, and practical demonstration of benefits to enhance acceptance. However, the challenges encountered—including infrastructure limitations, digital literacy gaps, uneven implementation across locations, cybersecurity vulnerabilities, and digital divide concerns—highlight the complexity of digital transformation in security contexts. These challenges require specific attention in future initiatives to ensure that digitalization enhances rather than compromises security capabilities while delivering equitable service improvements across all population segments. The significant variations in digital performance and access documented by researchers underscore the need for more balanced implementation approaches that extend benefits beyond major urban centers to create consistent nationwide coverage.

Based on these findings, the following recommendations are proposed for enhancing e-governance implementation at the Nigerian Immigration Service and similar security-focused institutions:

1. That the Nigerian Immigration Service should develop a comprehensive digital infrastructure strategy addressing power supply reliability, network connectivity, and hardware requirements across all operational locations to ensure consistent system availability nationwide.
2. That the Federal Government should establish a dedicated funding mechanism for immigration technology that protects critical security system investments from budgetary fluctuations, with specific allocations for extending digital capabilities to currently underserved border areas.
3. That the NIS should implement a segmented training program addressing the diverse digital literacy needs of different officer categories, with specialized modules for senior officers focused on strategic oversight, mid-level officers emphasizing operational

integration, and junior officers concentrating on tactical system utilization.

4. That policymakers should develop comprehensive legal frameworks specifically addressing digital immigration operations, including clear provisions for data protection, electronic evidence, cross-border information sharing, and cybercrime in immigration contexts.
5. That the NIS should redesign digital service interfaces based on user experience research, incorporating simplified workflows, multiple language options, enhanced help features, and offline capabilities to improve accessibility across different user segments.
6. That the service should establish community access points in partnership with local governments, providing assisted digital services in locations with limited internet connectivity or low digital literacy to ensure equitable access to immigration services.
7. That the NIS should implement comprehensive cybersecurity measures specifically tailored to immigration contexts, including enhanced database protection, officer access controls, secure international information sharing protocols, and regular security audits.
8. That the service should adopt an integrated border digitalization approach ensuring consistent technological coverage across entry points, with mobile and portable solutions deployed at remote locations where fixed infrastructure is impractical.
9. That the NIS should establish formal coordination mechanisms for system interoperability with other security agencies and international partners, ensuring seamless information exchange while maintaining appropriate security controls.
10. That the service should implement a formal monitoring and evaluation framework for digital systems, incorporating both performance metrics (processing times, error rates) and outcome measures (user satisfaction, security effectiveness) to guide continuous improvement.

REFERENCES

[1] Adebayo, A. (2019). Digital identity systems in developing countries: A comparative analysis. Journal of Information Technology for Development, 25(2), 148-172.

[2] Adebayo, O. (2022). Pandemic impacts on border management: Lessons from Nigeria's COVID-19 response. Security and Border Management Review, 14(3), 87-102.

[3] Adebisi, A., & Olatunji, F. (2023). Digital competencies among Nigeria's immigration workforce: A capability assessment. African Journal of Public Administration, 15(2), 112-130.

[4] Adedeji, T. (2021). Immigration policy and economic development in Nigeria: Historical perspectives and current challenges. Development Policy Review, 39(3), 415-433.

[5] Adelakun, A. (2022). Judicial interpretations of Nigeria's immigration laws in the digital age. Nigerian Law Journal, 28(2), 157-178.

[6] Adeniran, O. (2020). E-service implementation in Nigerian government agencies: Comparative case studies. International Journal of Electronic Government Research, 16(4), 78-96.

[7] Adepoju, A. (2018). Migration dynamics in Africa's largest democracy: Policy, practice and governance implications. African Affairs, 117(469), 543-565.

[8] Adepoju, A., & Adegoke, E. (2022). User experiences with Nigeria's digital immigration services. Journal of E-Government Studies and Best Practices, 2022(1), 1-18.

[9] Adesina, T. (2021). Digital transformation of administrative processes in Nigerian government departments. Journal of Public Administration and Governance, 11(2), 45-63.

[10] Adeyemo, K., & Olufemi, T. (2020). Digital transformation at the Nigerian Immigration Service: Implementation approaches and operational impacts. International Journal of Public Sector Management, 33(4), 431-448.

[11] Adeyemo, R., & Omotoso, F. (2021). Technology adoption patterns in Nigerian security agencies: A comparative assessment.

Journal of Science and Technology Policy Management, 12(2), 210-227.

[12] African Union. (2020). African Union passport policy framework. African Union Commission.

[13] Ajibola, T. (2022). Document fraud and identity theft in West African migration: Implications for Nigeria's immigration control. Journal of Migration Studies, 8(2), 178-195.

[14] Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. Journal of the Association for Information Systems, 8(4), 244-254.

[15] Benbasat, I., & Barki, H. (2007). Quo vadis TAM? Journal of the Association for Information Systems, 8(4), 211-218.

[16] Border Management Technology Assessment. (2022). Technology deployment at Nigeria's borders: Current state and future directions. Federal Ministry of Interior.

[17] Bruneau, T., & Matei, F. (2021). Security sector digital transformation: International perspectives. Journal of Strategic Security, 14(1), 78-96.

[18] Chan, J. (2021). Digital transformation challenges in hierarchical security organizations. Public Management Review, 23(4), 567-584.

[19] Counterterrorism Center. (2022). Terrorist mobility and border control effectiveness in West Africa. Office of National Security Adviser.

[20] Critical Infrastructure Protection Strategy. (2020). National critical infrastructure protection strategy (2020-2025). Office of National Security Adviser.

[21] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

[22] Eneanya, A. (2020). E-governance implementation in Nigerian public institutions: Policy challenges and prospects. International Journal of Public Administration in the Digital Age, 7(2), 1-17.

[23] Eneanya, A., & Adebayo, P. (2020). Change management in Nigeria's digital immigration transformation. International Journal of Public Sector Reform, 5(2), 112-131.

[24] Federal Government of Nigeria. (2015). Immigration Act 2015. Federal Government Printer.

[25] Federal Government of Nigeria. (2015). National Migration Policy. Federal Ministry of Interior.

[26] Federal Government of Nigeria. (2017). Immigration regulations 2017. Federal Government Printer.

[27] Federal Government of Nigeria. (2017). Presidential executive order on ease of doing business. Federal Government Printer.

[28] Federal Government of Nigeria. (2019). National border management strategy. Federal Ministry of Interior.

[29] Federal Government of Nigeria. (2019). National security strategy. Office of National Security Adviser.

[30] Federal Government of Nigeria. (2020). Visa policy of Nigeria. Nigerian Immigration Service.

[31] Ibrahim, A. (2020). Digital transformation of immigration processes in developing countries: A framework for analysis. Information Technology & People, 33(3), 1091-1108.

[32] Idowu, O. (2020). Bureaucratic resistance to reform in Nigerian public institutions: Case studies from the security sector. Public Administration and Development, 40(3), 146-159.

[33] International Civil Aviation Organization. (2022). Digital travel credentials: Technical specifications and implementation guidelines. ICAO Publications.

[34] International Organization for Migration. (2021). Border management in the digital age: Balancing security and facilitation. IOM Publications.

[35] Interpol. (2020). Technology requirements for law enforcement in developing contexts. Interpol Research Series.

[36] Interpol. (2021). Digital identity in cross-border security: Best practices and implementation challenges. Interpol Technical Reports.

[37] Loveday, K. (2018). Balancing security and efficiency in digital government transformations. Public Management Review, 20(6), 899-918.

[38] Lundblad, J. P. (2003). A review and critique of Rogers' diffusion of innovation theory as it

applies to organizations. Organization Development Journal, 21(4), 50-64.

[39] Lyytinen, K., & Damsgaard, J. (2001). What's wrong with the diffusion of innovation theory? The case of a complex and networked technology. In Proceedings of the IFIP TC8 WG8.1 Working Conference on Diffusing Software Product and Process Innovations (pp. 173-190).

[40] MacVaugh, J., & Schiavone, F. (2010). Limits to the diffusion of innovation: A literature review and integrative model. *European Journal of Innovation Management, 13(2), 197-221.*

[41] Ministry of Interior. (2023). Digital readiness assessment of immigration facilities nationwide. Federal Ministry of Interior.

[42] National Planning Commission. (2022). Public sector digitalization budget allocation report. Federal Government of Nigeria.

[43] National Security Advisor's Office. (2021). Integrated security data analytics: Implementation framework for Nigerian security agencies. Office of National Security Adviser.

[44] Nigerian Office of National Security. (2022). *Security classification guidelines for digital systems*. Office of National Security Adviser.

[45] Nwagwu, E. (2020). The evolving role of immigration agencies in national security architecture: A Nigerian perspective. *African Security Review, 29(3), 249-267.*

[46] Nwagwu, E., & Ibrahim, T. (2021). Border management digitalization in Nigeria: Implementation and effectiveness of the border management information system. *Journal of Borderlands Studies, 36(4), 567-585.*

[47] Nwankwo, B. (2019). Geographical barriers to government service access in Nigeria: Assessment and policy options. *International Journal of Public Administration, 42(15), 1290-1304.*

[48] Ocheni, S., & Nwankwo, B. (2022). Public perceptions of administrative competence in Nigerian government agencies: An empirical assessment. *Public Administration and Policy, 25(1), 73-89.*

[49] Office of the Auditor-General. (2021). Performance audit of document management at the Nigerian Immigration Service. Office of the Auditor-General of the Federation.

[50] Ogbonna, E. (2021). Security implications of inefficient border management in Nigeria's north-eastern region. *Journal of African Security Studies, 15(2), 112-131.*

[51] Okafor, C., & Nwachukwu, J. (2019). E-immigration and national security in Nigeria: Examining the relationship between immigration digitalization and security outcomes. *International Journal of Cyber Security Intelligence, 2(1), 78-96.*

[52] Okafor, E., & Nwaneri, A. (2021). Digital platforms for intelligence gathering in Nigerian security agencies. *African Journal of Security Management, 4(2), 45-62.*

[53] Oluwadare, O. (2022). Electronic borders: Technology applications in border management. *Border Security Review, 8(3), 112-130.*

[54] Oyedele, A. (2021). Technology-enabled pandemic response: Nigerian immigration service's adaptation to COVID-19 restrictions. *Journal of Crisis Management, 7(2), 145-162.*

[55] Peterson, R. (2019). Digital leadership in security organizations: Balancing innovation and operational continuity. *Leadership Quarterly, 30(2), 201-217.*

[56] Presidential Committee on Small Arms and Light Weapons. (2021). Border security assessment: Northeast and Northwest Nigeria. Office of National Security Adviser.

[57] Presidential Enabling Business Environment Council. (2023). Service delivery assessment of priority government agencies. Office of the Vice President.

[58] Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.

[59] Transparency International. (2022). Corruption risks in immigration services: Assessment of Sub-Saharan African countries. Transparency International.

[60] United Nations High Commissioner for Human Rights. (2020). Digital border technologies and human rights: Guidelines for states. OHCHR.

[61] United Nations High Commissioner for Refugees. (2021). Digital identity for refugees: Benefits, risks and standards. UNHCR Reports.

[62] United Nations Office on Drugs and Crime. (2021). Assessing trafficking interdiction capabilities at Nigerian borders. UNODC Regional Office for West Africa.

[63] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

[64] World Bank. (2022). Digital identity for development: Principles and country experiences. World Bank Group.