NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS
46TH CONSTITUTIONAL REGULAR SESSION, 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

DIGITAL TRANSFORMATION AND IDENTITY VERIFICATION ACT 2025

Index

Section **Page**

§101. Short title....3
§102. Purpose....3
§103. Interpretation....4
PART II –DIGITAL TRANSFORMATION UNIT....6
§104. Establishment of the Unit....6
§105. General functions and duties of the Unit....6
§106. Electronic identity verification functions....7
§107. Government Digital Plan....8
PART III –ELECTRONIC IDENTITY VERIFICATION....8
§108. Use of electronic identity credential....8
§109. Voluntary basis....8
§110. Covered electronic transactions....9
§111. Electronic identity credentials....10
§112. Identity trust framework....10
§113. Federated identity management....11
§114. Federated digital identity system....11
§115. Unit to act as federation operator....12
§116. Private sector participation....12
§117. Decentralized identity management....13
§118. Protection of personal data....13
PART V –OFFENSES AND PENALTIES....13
§119. Unauthorized Access and Fraudulent Use....13
§120. Identity Theft and Misrepresentation....14
§121. Abuse of Authority by Public Officials....14

§122. General Penalty. 14
PART IV – MISCELLANEOUS 15
§123. Regulations. 15
§124. Effective date. 15

NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS
46TH CONSTITUTIONAL REGULAR SESSION, 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

DIGITAL TRANSFORMATION AND IDENTITY VERIFICATION ACT 2025

AN ACT to promote digital transformation, establish the Digital Transformation Unit and to adopt an enabling framework for electronic identity verification.

BE IT ENACTED BY THE NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS

§101. Short title.

This Act may be cited as the Digital Transformation and Identity Verification Act 2025.

§102. Purpose.

The purpose of this Act is to:

(a) establish the Digital Transformation Unit to implement this Act and exercise other duties and responsibilities;

(b) establish an enabling legal framework for electronic identity verification to facilitate electronic government services including to:

(i) facilitate secure electronic transactions between individuals and participating public bodies for covered electronic transactions];

(i) ensure that participating public bodies are able to attain relevant identity assurance levels by providing individuals with the option of verifying their identity authoritatively and in real time by electronic means; and

(ii) provide a flexible framework for the use of federated and decentralized identity management systems to verify an individual's identity by electronic means while protecting the individual's privacy.

§103. Interpretation.

In this Act, unless context otherwise requires:

(a) 'biographical data' means personal data relating to the name, date of birth, address, and other aspects of the life of a person, excluding biometric data;

(b) 'biometric data" means photographic facial images, fingerprints, and specimen signatures;

(c) 'covered electronic transaction' means an electronic transaction identified by a participating public body for which the identity of an individual may be verified by electronic means;

(d) 'digital transformation' means the process of implementing digital, electronic or similar technologies and related practices to achieve improvements in security, productivity, efficiency and effectiveness in Government processes, culture and engagement with individuals and persons. This includes, but is not limited to, information management, equipment, software, operating systems, interface systems, interconnected systems, telecommunications, data management, networks, and network management, consulting, supplies, facilities, maintenance and training, ICT development and public sector ICTpractitioners coordination and collaboration;

(e) 'electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

(f) 'ICT' means information and communications technology;

(g) 'ICT practitioner' meansan employee of the public service tasked with ICT related functions;

(h) 'heads of departments and offices' mean all department secretaries, and shall include heads of any Government office or agency;

(i) 'identity assurance levels' means the certainty with which a claim to a particular identity during authentication can be trusted to actually be the individual's true identity;

(j) 'identity attributes' means identifying information associated with an individual which may include biographical data and biometric data and any other data relating to a person who can be identified or is identifiable, directly or indirectly by reference to such data;

(k) 'identity credential' means the data, or the physical object upon which the data may reside, that an individual may present to verify or authenticate his or her identity, or any related identity attributes, in a covered electronic transaction;

(l) 'identity proofing' means the collection, validation, or verification process for digital identity;

(m) 'identity provider' means a participating public body, or any third party acting on its behalf, certified by the Unit to provide electronic identity credentials that may be used by an identity credential holder to assert his or her identity, or any related attributes, in a covered electronic transaction;

(n) 'individual' means a natural person, except a deceased natural person;

(o) 'information' means data, text, images, sounds, codes, computer programs, software, databases, or similar;

(p) 'national government identity management standards' means the minimum specifications and standards that must be included in an identity trust framework so as to meet the requirements of this Act and are set forth in policy documents approved pursuant to this Act;

(q) 'participating public body' for the purpose of electronic identity verification means a public body that acts as an identity provider, as a relying party, or both, in accordance with this Act;

(r) 'person' means an individual, public body, commercial, or non-commercial organization, or other legal or commercial entity;

(s) 'personal data' means any information relating to an identified or identifiable natural person that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, whether directly or indirectly, with a particular natural person, including by reference to an identifier, such as name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

(t) 'public body' means any ministry, division, bureau, office, agency, or other instrumentality of the Government of the Republic of the Marshall Islands;

(u) 'relying party' is a participating public body that relies on the validity of an identity credential or an accreditation mark;

(v) 'Unit' means the Digital Transformation Unit established in section 4.

PART II –DIGITAL TRANSFORMATION UNIT

§104. Establishment of the Unit.

(1) The Digital Transformation Unitis hereby established within the Office of the Chief Secretary.

(2) The Unit shall be headed by a director who will be the Chief Information Officer of the Republic of the Marshall Islands and shall be supported by staff, experts and analysts with such qualifications and experience as may be prescribed by the director. The director and the staff may be members of the public service or contracted based on specific needs, expertise and qualifications as determined by the Chief Secretary from time to time.

§105. General functions and duties of the Unit.

The Unit shall have the following general functions and duties:

(a) develop and recommend to Cabinet the Government Digital Plan;

(b) lead the planning and delivery of whole of government digital infrastructure as set out in the Government Digital Plan to enable government to citizen digital services;

(c) develop, consult on and issue relevant ICT policies and standards for ministries, departments, offices, or other agencies of the Government for improving coordination, administration, security, confidentiality, program effectiveness, integration and interoperability of the Government technology systems, data management, training, acquisition and deployment of technology for digital transformation;

(d) develop and coordinate the efforts of the Government ICT practitioners to ensure ministries, departments, offices, or other agencies of the Government, act in a manner that is consistent with

the Government Digital Plan, and any relevant ICT policies and standards issued by the Unit;

(e) support operations with agencies responsible for national intelligence and national security to ensure cybersecurity and safety are maintained across whole of government;

(f) undertake such other planning and coordination actions as required for the advancement of digital transformation and perform all necessary and appropriate services required to fulfill these duties;

(g) perform technology reviews pertaining to digital transformation initiatives within Government;

(h) enter into agreements with third parties, to undertake some or all of the functions of the Unit;

(i) in consultation with the heads of departments and offices, mobilize ICT practitioners as the need arises to assist the Unit any other ministries, departments, offices, or other agencies of the Government in ICT technical support and help desk matters;

(j) undertake such other functions granted or delegated to the Unit under this Act or otherwise under law.

§106. Electronic identity verification functions.

The Unit shall have the following general functions and duties under this Act:

(a) adopt national government identity management standards in accordance consistent with recognized international standards to ensure security;

(b) certify participating public bodies as identity providers to issue electronic identity credentials;

(c) adopt policies and standards on the levels of identity assurance, authentication assurance, and federation assurance;

(d) establish the national digital identity trust framework and act as the identity trust operator in accordance with section 12;

(e) make rules and policies to implement one or more of the following identity management frameworks:

(i) a federated identity management framework and act as the federation operator for electronic identity management in accordance with section 15;

(ii) a decentralized identity management framework in accordance with section 17; and

(f) take any other actions and make decisions under this Act as required or that are necessary for the Unit to effectively implement this Act.

§107. Government Digital Plan.

(1) The Government Digital Plan shall be a multiyear, cross-government strategy developed by the Unit and approved by Cabinet with the objective of:

(a) promoting digital transformation of the Government of the Marshall Islands;

(b) expanding access to high-quality digital government information and services;

(c) enabling the use of government data to spur innovation; and

(d) delivering whole of government digital infrastructure.

(2) The Unit shall consult relevant stakeholders to develop the Government Digital Plan.

(3) The Government Digital Plan shall be updated and amended from time to time.

PART III –ELECTRONIC IDENTITY VERIFICATION

§108. Use of electronic identity credential.

An individual may use an electronic identity credential for the purpose of verifying his or her identity by electronic means in order to meet the identification requirements established under law or by a participating public body in relation to a covered transaction in accordance with this Act.

§109. Voluntary basis.

(1) Nothing in this Act requires or prevents an individual:

(a) to apply for an electronic identity credential to be issued to him or her; or

(b) to use an electronic credential that has been issued to him or her to access a covered electronic transaction.

(2) An individual may continue to access a covered transaction of a participating public body by means other than by using an electronic identity credential even though an electronic identity credential has already been issued to him or her.

§110. Covered electronic transactions.

(1) Participating public bodies may identify from time to time covered electronic transactions subject to the provisions of this Act.

(2) Participating bodies must determine the level of identity assurance for each covered electronic transaction identified under subsection (1) in line with international standards and using the following reference framework:

(a) identity assurance level 1 (IAL1): provides some confidence, where identity attributes are self-asserted by the individual and there is no identity proofing;

(b) identity assurance level 2 (IAL2): provides high confidence, where identity proofing is required, either in-person or remotely; and

(c) identity assurance level 3 (IAL3): provides very high confidence, where in-person or supervised-remote identity proofing is required. Identifying attributes must be verified through examination of physical documentation.

(3) The Unit may adopt policies or standards on:

(a) the levels of identity assurance;

(b) the processes to be performed by participating public bodies to determine specific identity assurance levels for each covered electronic transaction;

(c) identity proofing processes, including the types of acceptable documents and verification methods; and

(d) security standards and attack detection requirements, particularly in the case that biometric data is used for identity proofing.

(4) In adopting policies and standards under subsection (3), the Unit shall ensure consistency with standards issued by recognized international or national standard setting organizations to facilitate interoperability.

§111. Electronic identity credentials.

(1) Participating public bodies may act as identity providers to provide electronic identity credentials to an individual that may be used by that individual to assert his or her identity, or any related identity attributes, in relation to covered electronic transactions.

(2) Prior to issuing an identity credential to an individual in accordance with subsection (1), the participating public body must, directly or indirectly, undertake identity proofing in a manner consistent with the level of identity assurance established for each covered electronic transaction in accordance with section 10.

(3) Identity providers and relying parties shall adopt effective measures to ensure security and avoid fraud in a manner consistent with this Act.

§112. Identity trust framework.

(1) The Unit may establish a national digital identity trust framework with established identity, security, privacy, technology, and enforcement rules and policies that shall be binding to certified identity providers that are members of the identity trust framework.

(2) Members of an identity trust framework include:

(a) the Unit, which shall act as the identity trust framework operator;

(b) identity providers; and

(c) relying parties.

(3) The identity trust framework adopted in accordance with subsection (1) shall comply with standards issued by recognized international or national standard setting organizations.

§113. Federated identity management.

(1) The Government may implement a federated identity management framework for covered electronic transactions to enable a centralized approach to be taken in relation to the verification of an individual's identity by electronic means while protecting the individual's privacy.

(2) The federated identity management is a process that allows the conveyance of identity credentials and authentication information across digital identity systems managed by participating public bodies through the use of a common and binding set of policies, practices, and protocols for managing the identity of users and devices across security domains.

(3) The federated identity management framework shall use secure communications protocols and undertake regular security assessments as may be required by the Unit by written order.

§114. Federated digital identity system.

(1) The Government may implement a federated digital identity system in accordance with this Act.

(2) The federated digital identity system shall:

(a) utilize federated identity management to enable the use of identity information across otherwise autonomous security domains;

(b) be compliant with the Government identity management standards and with the provisions of the governing identity trust framework;

(c) have established identity, security, privacy, technology, and enforcement rules and policies, which shall be binding on the certified identity providers and relying parties that are members of the federated digital identity system; and

(d) include as members the federation operator, identity providers, and relying parties.

§115. Unit to act as federation operator.

(1) If, pursuant to section 14, the Government implements a federated identity management system for covered electronic transactions, the Unit shall act as the federation operator.

(2) The federation operator shall undertake the following functions:

(a) define the rules and policies for member parties to the federation, including fees, if applicable;

(b) certify participating public bodies as identity providers to issue electronic identity credentials pursuant to the federation;

(c) evaluate participation in the federation to ensure compliance by members of the federation with its rules and policies, including the ability to undertake audits of participating public bodies for verification of compliance; and

(d) take such other actions or issue such other decisions as may be necessary to implement this Part.

§116. Private sector participation.

(1) Notwithstanding the definition set forth is section 4(t), persons other than public bodies may opt in to be members of the identity trust framework and the federated digital identity system as relying parties by presenting an application that must be approved by the Unit.

(2) Prior to approving an application received in accordance with subsection (1), the Unit shall verify that the person filing the application has sufficiently demonstrated that it meets or is reasonably capable of meeting all obligations applicable to relying parties in accordance with this Act.

(3) A person that is approved as a member of the identity trust framework and the federated digital identity system in accordance with subsection (2) shall be subject to the rights, obligations and requirements set forth under this Act in relation to relying parties, including payment of fees, if applicable.

§117. Decentralized identity management.

(1) Nothing in this Act should be construed as limiting the ability to implement decentralized identity management in the Republic of the Marshall Islands.

(2) Decentralized identity management is the process of managing and controlling digital identities without the need for a central authority or intermediary.

(3) The Unit may issue rules, policies, and standards for the implementation of decentralized identity management by participating public bodies in a manner consistent with standards issued by recognized international or national standard setting organizations.

§118. Protection of personal data.

(1) A participating public body, or any third party acting on behalf of a participating public body, and such persons that have been approved pursuant to section 16, must ensure that personal data processed in connection with this Part complies with the principles set out in section 9 of the Personal Data Protection Act 2025, as if they formed part of this Act.:

(2) A participating public body, or any third party acting on behalf of a participating public body, and such persons that have been approved pursuant to section 167, must implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data in its possession or under its control in accordance with this Part, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure, or access.

PART V –OFFENSES AND PENALTIES

§119. Unauthorized Access and Fraudulent Use.

(1) A person knowingly and wilfully gains unauthorized access to any digital identity system established under this Act commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding five (5) years, or both.

(2) A person who fraudulently obtains, uses, or misrepresents an electronic identity credential of another person commits an offense and shall be liable upon conviction to a fine not exceeding $15,000 or imprisonment for a term not exceeding seven (7) years, or both.

§120. Identity Theft and Misrepresentation.

(1) A person who intentionally provides false information or misrepresents their identity in order to obtain an electronic identity credential under this Act commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding five (5) years, or both.

(2) A person who engages in identity theft using an electronic identity credential commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding five (5) years, or both.

§121. Abuse of Authority by Public Officials.

(1) A public officer who knowingly misuses their authority to improperly issue, revoke, or manipulate electronic identity credentials commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding five (5) years, or both.

(2) Any public officer who, in the course of performing their duties under this Act, accepts bribes, engages in corrupt practices, or unlawfully denies a person access to electronic identity verification services commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding five (5) years, or both.

§122. General Penalty.

Where no specific penalty is provided for an offense under this Act, a person who contravenes any provision of this Act commits an offense and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding three (3) years, or both.

PART IV – MISCELLANEOUS

§123. Regulations.

The Chief Secretary may promulgate regulations necessary to ensure the effective administration of the provisions of this Act and may further issue regulations prescribing additional enforcement mechanisms, and administrative procedures necessary for its effective implementation.

§124. Effective date.

This Act will take effect on the date of certification in accordance with Article IV, section 21 of the Constitution.

CERTIFICATE

I hereby certify:

1. That Nitijela Bill No: 41ND1 was passed by the Nitijela of the Republic of the Marshall Islands on the 7th day of April 2025; and

2. That I am satisfied that Nitijela Bill No: 41ND1 was passed in accordance with the relevant provisions of the Constitution of the Republic of the Marshall Islands and the Rules of Procedures of the Nitijela.

I hereby place my signature before the Clerk this 21st day of April 2025.

Brenson S. Wase
Speaker
Nitijela of the Marshall Islands

Attest:

Morean S. Watak
Clerk
Nitijela of the Marshall Islands