Republic of the Marshall Islands - Digital Services Project

Deliverable 1: Assessment of the existing legal and regulatory enabling environment, gap analysis and recommendations

June 28, 2023

DRAFT FOR DISCUSSION

Contents

1. Executive Summary

This report supports the creation of an enabling environment to both promote digital transformation in the Republic of the Marshall Islands (RMI) and build citizen trust and confidence in the use of digital services, through laws and regulations that address 4 core areas:

- A digital identification (ID) system, to enable people to transact online and ensure secure identity verification and authentication;
- Privacy and data protection, to ensure personal data collection is limited and relevant for the purposes for which it is being collected, accurate and up to date and protected with adequate safeguards.
- Electronic transaction enabling laws, to support certainty in conducting commercial transactions online and to provide for efficient electronic government (e-government) services; and
- Cybersecurity and cyber-crime protections, to support the resilience of critical computer systems and data, secure critical information infrastructure and safeguard individuals and firms from crimes affecting digital transactions.

As a first step in this process, this report reviews and takes stock of existing legislation relating to the 4 core areas described above. Based on the assessment of the current situation, a gap analysis is conducted to support recommendation on specific areas where the legal framework must be strengthened having regard to the specific conditions of the RMI and international law and practices.

An initial finding of this assessment is that comprehensive legislation on these 4 core areas has yet to be enacted. Therefore, this report focuses on laws that may tangentially enable, limit, or impede the provision of digital ID and digital services in the RMI.

The key findings and recommendations of the report are summarized in the following subsections.

1.1. Digital ID

While the RMI has implemented several national ID systems, both foundational and functional, there is no legal framework in place to enable digital IDs in the country. Presently, the government issues different forms of ID to its citizens (and in some cases non-citizens), including national IDs, driver's licenses, passports, and social security cards. All forms of ID are currently applied for, processed, and issued in physical credentials and no express digital ID-related legislative provisions have been identified.

The government of the RMI may consider enacting digital ID legislation that specifically embeds elements such as inclusion, design, and governance. Such legislation should allow all citizens and other persons to access digital services and ensure universal coverage of these services. Further, security and privacy should be incorporated in the legislation. The RMI could enact legislation that allows citizens to request their digital ID from birth, integrating digital IDs into the current legislative framework. A determination should be made to assess whether digital IDs should be compulsory or voluntary. Notably, current ID card legislation does not make them compulsory.

Proposed actions in relation to digital ID

The RMI should consider: • Enacting specific legislation on digital ID, considering inclusion, security, and data protection matters (See further discussion Sections 4 and 6).

- Enacting legislation that provides for the use of digital IDs and electronic processes to engage in e-transactions with the public sector, institutions, and private organizations (See further discussion in Section 5).

1.2. Privacy and data protection

The right to privacy is enshrined in the Constitution of the RMI and can be defined as part of a universal right to live without external and unwanted interferences.

However, there is no general data protection law or privacy framework in the RMI. Several pieces of sectoral legislation establish varying degrees of privacy safeguards for personal data collected and stored by the government of the RMI, as well as certain private entities.

The government of the RMI may consider enacting a data protection and privacy legislative framework that is fit-for-purpose, considering national conditions and consistent with international practices. As a reference, this framework should reflect the privacy standard set forth in the Constitution. The proposed legislation should also expand upon recent legislation aimed at protecting determined categories of persons (e.g., persons with disabilities).

Proposed actions in relation to privacy and data protection legislation

The RMI should consider:

- Enacting specific legislation on data protection and privacy that aligns with international standards and the Constitution. The legislation should include definitions and set standards for best practices.
- The legislation should be designed to ensure inclusion and non-discrimination.
- The legislation should create a data protection authority or vest data protection functions onto an existing agency.

1.3. Electronic transactions

The current legal framework in the RMI does not establish comprehensive or sector-specific rules setting out the legal equivalence of electronic records and signatures as compared to paper and hand-signed documents. Similarly, no specific provisions addressing the use of digital technology for the provision of government services were identified.

Adopting an Electronic Transactions Act or similar legislation in the RMI would establish a governance framework for a range of activities that promote the digital economy by providing legal equivalence to electronic transactions, signatures, records, and commerce while enabling security mechanisms and user protections.

Proposed actions in relation to electronic transactions legislation

The RMI should consider:

- Enacting comprehensive e-transactions legislation that provides legal equivalence between electronic and paper record and applies widely to all types of transactions, contracts, signatures, and other records with limited exceptions which could include issues such as wills/testamentary trusts, real estate, or family law.

- The legal framework should also regulate e-government services, including equivalence provisions and mechanisms to phase in the provision of services by different ministries and agencies.
- The proposed legislation should take a technology-neutral approach to ensuring interoperability between systems, particularly in international commerce.
- To promote security and trust, the framework may include mechanisms that establish certification of providers to offer trust services that can serve to guarantee the origin and integrity of electronic records and signatures. The framework may also address intermediary liability that could be implemented through a self- or co-regulatory approach.
- Legislation could be based on various international models, such as the UN Convention on the Use of Electronic Communications in International Contracts,[1] UNCITRAL Model Law on Electronic Commerce,[2] and UNCITRAL Model Law on Electronic Signatures.[3]

1.4. Cybersecurity and Cybercrime

The government of the RMI may consider enacting cybersecurity legislation that specifically identifies and categorizes critical information infrastructure (CII), prescribes actions to enhance security for such infrastructure, sets forth processes to provide appropriate responses to cybersecurity incidents, and establishes specific offenses for attacks on CII with penalties that are adjusted and proportionate to the severity of the offenses.

The RMI should also consider enacting the necessary enabling framework for the creation of computer emergency response teams (CERTs) or similar structures to ensure expeditious responses to cybersecurity incidents. Taking account of the limitations inherent to the scale of the Marshallese market, this legislation could provide for a principles-based approach that is not prescriptive and allows for international good practices in cybersecurity measures.

Proposed actions in relation to cybersecurity legislation

The RMI should consider:

- Enacting comprehensive cybersecurity legislation to identify and categorize CII, enhance security measures for such infrastructure, enable appropriate responses to cybersecurity incidents, and create specific offenses for attacks on CII.
- Implementing provisions that establish CERTs or similar structures.

The government of the RMI may also consider enacting a cybercrime legislative framework that is fit-for-purpose considering national conditions and consistent with international practices. As a reference, this

[1] UNCITRAL, United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005),https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications#:~:text=Purpose,their%20traditional%20paper%2Dbased%20equivalents..

[2] UNCITRAL, Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

[3] UNCITRAL, Model Law on Electronic Signatures (2001) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.

framework could reflect the generally accepted standards set forth in the Convention on Cybercrime (Budapest Convention) of which the RMI is not a signatory. This would include enacting legislation criminalizing conduct, such as data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud, as well as introduce dissuasive and proportionate sanctions for such offenses. In addition, offenses, such as cyberstalking and cyberbullying, could also be considered.

The RMI should further consider updating its criminal procedure statute to create comprehensive provisions enabling, among other potential matters, the expedited preservation of stored computer data, its partial expedited preservation and partial disclosure of data, and the adoption of production orders. This would create a framework for law enforcement to combat cybercrime more effectively.

Lastly, the RMI could consider accession to the Budapest Convention to enable Marshallese law enforcement agencies to complement and expand on existing mutual assistance legislation with respect to cybercrime and electronic evidence.

Recommendation. Proposed Actions in relation to Cybercrime Legislation

The RMI should consider:

- Enacting specific legislation on cybercrimes that aligns with international practices and criminalizes internationally recognized cybercrimes.
- Enacting legislation that provides for criminal procedures to enable law enforcement agencies to effectively investigate crimes involving electronic evidence.
- Acceding to the Budapest Convention to facilitate Marshallese law enforcement agencies cooperation with other countries to further cooperate on cybercrime investigations.

2. Introduction

This report is the first deliverable of a project to establish a legislative framework for digital services in the Republic of the Marshall Islands (RMI).[4] This work supports the creation of an enabling environment to promote digital transformation, enable the digital economy and provide efficient electronic government (e-government) services. A key enabler to achieve these broader goals is implementing an identification (ID) system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.[5]

This report reviews and takes stock of existing legislation that would impact the establishment of a digital ID system in the RMI. This includes assessing current legislation establishing ID systems, as well as legislative provisions relating to or impacting privacy and data protection, electronic transactions (e-transactions), and cybersecurity in the RMI. Considering that specific legislation on digital services has yet to be enacted in the RMI, this report instead focuses on general laws that may tangentially enable, limit, or impede the provision of digital ID and digital services in the country. This includes laws covering a range of topics, such as civil registration, voter registration, health records, taxation, commercial agreements, and criminal conduct and procedure.

Our analysis first reviews existing legal frameworks related to digital ID and digital services in the RMI to assess the current situation and identify gaps. This assessment is aimed at supporting the development of a digital ID system by identifying where the legal and regulatory framework may need to be strengthened, having regard to the specific conditions of the RMI and international law and practices. It will also help inform the approach, focus, and support that may be required to achieve this objective.

The discussion included in this report is based on desk research and needs to be further validated with stakeholders in the RMI.

2.1. Overview of the legal and institutional framework in RMI

The RMI's legal system is grounded in its Constitution of 1979, as amended, which is the supreme law of the country.[6] The main sources of law are based on a mixed legal system of U.S. and English common law, customary law, and local statutes.[7] In particular, U.S. law strongly influences the RMI's law and practice. For example, as a former U.S. Trust Territory, the RMI modeled its Constitution on the U.S. Constitution.

While Marshallese courts are not bound by foreign law, the Constitution states that "[i]n interpreting and applying this Constitution, a court shall look to the decisions of the courts of other countries having constitutions similar, in the relevant respect, to the Constitution of the Marshall Islands (…)."[8] Similarly, the RMI closely follows U.S. law in other areas of substantive law. For example, regarding corporate law, the RMI's Business Corporations Act 1990 refers to "the laws of the State of Delaware and other states of the United States of America with substantially similar legislative provisions."[9] Recommendations and

[4] All RMI laws referenced in this report are available at: https://rmiparliament.org/cms/legislation.html?view=acts_alpha.
[5] *See* World Bank, ID Enabling Environment Assessment (IDEEA). Guidance Note, p. 9, https://documents1.worldbank.org/curated/en/881991559312326936/pdf/ID-Enabling-Environment-Assessment-Guidance-Note.pdf.
[6] *See* Constitution of The Republic of The Marshall Islands, Article I, §1(1).
[7] CIA, World Factbook, https://www.cia.gov/the-world-factbook/countries/marshall-islands/#government.
[8] *See* Constitution of The Republic of The Marshall Islands, Article I, §3(1).
[9] *See* Business Corporations Act 1990, §13.

analyses presented in this report take account of this approach to legislative sources and statutory construction where justified.

As the national legislative body of the RMI, the Nitijela is vested with the power to make, repeal, revoke, or amend laws and to "confer authority to promulgate rules and regulations, or other subordinate instruments pursuant to that Act and in furtherance of its stated purposes."[10] This clause recognizes the delegation doctrine, whereby the Nitijela may—by statute—delegate legislative power to executive branch agencies to make rules and regulations with the force of law, provided that the statute sets out an "intelligible principle" to guide such delegation.

The government is a parliamentary system with the executive authority vested in the Cabinet formed by the President and Ministers who must all be members of the Nitijela.[11] The Supreme Court is the superior constitutional court of record, having appellate jurisdiction with final authority to adjudicate all cases and controversies properly brought before it.[12] In addition, judicial powers are also granted to the High Court, Traditional Rights Courts, District Courts, and Community Courts.[13] The abovementioned institutional structure and their roles will also be taken into account in the consideration of legislative and regulatory options discussed in this report.

2.2. Policy framework and national strategic objectives

The National Strategic Plan 2020-2030 (NSP) provides a framework to coordinate the long-term development goals and objectives of the RMI government at the national level. It is the apex planning document in the country, which sets the strategic focus addressing all developmental activity, both public and private, including external projects.[14] The plan is structured into five key thematic pillars, each covering several strategic areas that include multiple policy objectives. It should be noted that the NSP does not explicitly mention or recognize a policy to leverage the use of digital technologies as a cross-sectoral lever to promote the country's economic or social development goals established in the plan. Despite this, among the key planning themes and objectives, the NSP identifies several policy objectives related to, or that may be affected by, the provision of digital services and digital ID discussed in this report.

The NSP establishes specific goals associated with the provision of high-quality, accountable, and transparent government services.[15] While the plan does not explicitly identify the use of digital technologies or mention the goal of promoting e-government services, it emphasizes modernizing the public service and introducing new public-sector management practices.[16] Among the policy objectives to meet these goals are to:

1) Improve practices to achieve an effective, ethical, and transparent public service, local governments, and related public agencies;
2) Strengthen oversight, audit, alignment and coordination across and within the public service and related public agencies;

[10] *See* Constitution of The Republic of The Marshall Islands, Article IV, §1(1)-(2).
[11] *See* Constitution of The Republic of The Marshall Islands, Article V, §1(1) and §2(1).
[12] *See* Constitution of The Republic of The Marshall Islands, Article VI, §1(1).
[13] *See* Constitution of The Republic of The Marshall Islands, Article VI, §1(1).
[14] National Strategic Plan 2020-20230, p. 1, 3, https://rmi-data.sprep.org/system/files/Marshall%20Islands%20National%20Strategic%20Plan%202020%20to%202030.pdf.
[15] National Strategic Plan 2020-20230, p. 18.
[16] National Strategic Plan 2020-20230, p. 18.

3) Strengthen the connection and cooperation with civil society, the private sector, and outer islands; and
4) Strengthen the capability of accountability and integrity institutions to address corruption and unethical practices.[17]

The RMI has yet to make progress in deploying digital technologies and services as an enabler to achieve efficient government services. Developing an enabling framework for these tools could be a relevant factor to achieve the NSP goals outlined above.

The NSP also recognizes the need for continued improvements in domestic telecommunications and information and communications technology (ICT) services in the RMI.[18] The plan emphasizes the goal of achieving modern, efficient, resilient, and affordable ICT infrastructure and services to underpin economic and social development.[19] The policy objectives proposed to achieve these goals are:

(1) Strengthening the legal and regulatory framework;
(2) Providing resilient platforms for efficient and affordable connectivity;
(3) Improving outer island connectivity; and
(4) Revising the ICT policy of 2012 and existing telecom laws and regulations.[20]

The RMI has yet to make significant progress in implementing several of these policy actions. While amendments to the legislation governing the telecommunications sector was passed in 2022[21] and market reforms are being considered in this sector, the ICT policy has yet to be updated. Further, specific legislation to strengthen digital services and digital ID and promote adoption of ICTs is still outstanding. To leverage the benefits of digital technologies and accelerate efforts toward digital transformation in line with the NSP's goals, this report presents specific recommendations and actions to adopt an enabling legal framework to support digital services and digital ID.

2.3. Overview of ID systems

An ID system comprises the databases, processes, technologies, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose.[22] A digital ID system, is also an identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.[23]

Successful and secure implementation of national digital ID systems is grounded on public trust. To achieve this, an ID system must be inclusive (i.e., not be used intentionally or otherwise to exclude any

[17] National Strategic Plan 2020-20230, p. 18.
[18] National Strategic Plan 2020-20230, p. 6.
[19] National Strategic Plan 2020-20230, p. 14.
[20] National Strategic Plan 2020-20230, p. 14.
[21] See Marshall Islands National Telecommunications Authority (Amendment) Act, 2022 [amending §107 (2)(d) of the Act by removing the National Telecommunications Authority's "exclusive" right to offer telecommunications services in the RMI].
[22] *See* World Bank, ID Enabling Environment Assessment (IDEEA). Guidance Note, p. 9, https://documents1.worldbank.org/curated/en/881991559312326936/pdf/ID-Enabling-Environment-Assessment-Guidance-Note.pdf.
[23] *See* World Bank, ID Enabling Environment Assessment (IDEEA). Guidance Note, p. 9 , https://documents1.worldbank.org/curated/en/881991559312326936/pdf/ID-Enabling-Environment-Assessment-Guidance-Note.pdf.

person from exercising rights or receiving services they are entitled to) and protect the privacy and personal data of individuals (i.e., ensure that the government will store, process, and share personal data responsibly).[24] The analysis in this report emphasizes both of these the key factors.

ID systems are sometimes described in terms of whether they are "foundational" or "functional" as shown in Table 1. This report follows this typology for the review of the RMI's current legislative framework. As noted below in section 3, the RMI has implemented both types of ID systems, including a national ID (foundational system), as well as driver's licenses and passports, among other forms of ID (functional systems). However, as far as has been ascertained from our desk review, no digital ID systems have been or are being implemented in the RMI at this time.

Table 1: Typology of ID systems

	Description	Examples
Foundational ID systems	Commonly used to provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials.	Civil registries, national IDs, universal resident ID systems, and population registers, among others.
Functional ID systems	Systems created to manage the identity lifecycle for a particular service or transaction. In some countries, these ID systems may be accepted as proof of identity for broader purposes outside of their original intent (i.e., "federated"), particularly when a foundational ID system is not available.	Voter IDs, passports, health and insurance records, tax ID numbers, ration cards, and driver's licenses, among others.

Source: TMG based on World Bank, ID Enabling Environment Assessment (IDEEA). Guidance Note.

2.4. Constitutional provisions relevant to ID systems and personal data protection in the RMI

The Constitution of the RMI does not explicitly provide for a national or other ID system to be implemented or for specific legislation on personal data protection. However, the Constitution does enshrine a Bill of Rights, which draws heavily from the U.S. Constitution, and recognizes the individual rights of persons before the law.[25] These provisions inform the establishment of current ID systems and sectoral data protection legislative provisions and include, among other enumerated rights, the rights to:

- **equal protection**: all persons are equal under the law and are entitled to equal protection of the laws;[26]
- **freedom from discrimination**: no law and no executive or judicial action shall, either expressly, or in its practical application, discriminate against any person "on the basis of gender, race, color, language, religion, political or other opinion, national or social origin, place of birth,

[24] *See* World Bank, ID Enabling Environment Assessment (IDEEA). Guidance Note, p. 7 , https://documents1.worldbank.org/curated/en/881991559312326936/pdf/ID-Enabling-Environment-Assessment-Guidance-Note.pdf.
[25] *See* Constitution of The Republic of The Marshall Islands, Article II.
[26] *See* Constitution of The Republic of The Marshall Islands, Article II, §12(1).

family status or descent," but non-arbitrary preferences may be established for citizens under the law;[27]

- **personal privacy**: all persons shall be free from unreasonable interference into their privacy;[28] and
- **access to judicial and electoral processes**: every person has the right to invoke judicial processes to vindicate any interest preserved or created by law and to participate in the electoral process as a voter or candidate for office, subject to qualifications required in the Constitution and the law.[29]

Similarly, the Constitution defines the requisites for citizenship, extending it to persons born after the effective date of the Constitution if (i) at the time of birth, either of the person's parents is a citizen of the RMI or (ii) that person is born in the RMI and is not at birth entitled to be or become a citizen of another country.[30]

The referenced constitutional framework will inform the implementation of any digital ID system and data protection framework in the RMI. In particular, special attention should be paid to ensuring that any such framework is non-discriminatory, ensures all persons have equal access to services and rights under the law, and is sufficiently secure as to protect the privacy of individuals.

2.5. Structure of this report

This report reviews existing legislation in relation to digital services in the RMI, as follows.

- Section 3 discusses existing legislation on foundational and functional ID systems and its potential application to digital ID.
- Section 4 covers the evolution of privacy laws in the RMI to recommend a path forward in developing a data protection framework to ensure trust in digital services.
- Section 5 reviews existing legislation and proposes an approach to enable e-transactions, e-signatures and e-government services.
- Section 6 addresses cybersecurity and cybercrime to identify recommendations on these matters.
- Section 7 proposes an implementation plan for both the drafting and introduction of bills before the Nitijela, as well as the approach to phasing in of e-government services by ministries and government agencies.

[27] *See* Constitution of The Republic of The Marshall Islands, Article II, §12(2), (3).
[28] *See* Constitution of The Republic of The Marshall Islands, Article II, §13.
[29] *See* Constitution of The Republic of The Marshall Islands, Article II, §14(1), (2).
[30] *See* Constitution of The Republic of The Marshall Islands, Article IX, §1(1), (2).

3. Digital Identification

3.1. Current situation

The RMI has implemented several national ID systems, both foundational and functional. The government issues different forms of ID to its citizens (and in some cases non-citizens), including national IDs, driver's licenses, passports, and social security cards. All forms of ID are currently applied for, processed, and issued in physical credentials. No express digital ID related legislative provisions have been identified.

In several instances (see Table 2), legal provisions explicitly mention paper-based credentials or databases (e.g., books and registers) or reference actions that imply the paper-based form of the relevant ID credentials or processes (e.g., the physical transfer of the registers of birth, death, and marriage between Register-Generals).

In this context, as the government of RMI considers deploying a digital ID system to support e-transactions and e-government services, there is a need to assess existing ID systems, registers, processes, and databases and how (or if) those data can be used to support such transactions (see section 5). Most importantly, development of digital ID systems should also place special attention on inclusion, privacy, and data protection (see section 4) and data security considerations (see section6).[31]

The table below reviews legislation in force in the RMI that may impact the development of a digital ID system to differing degrees.

Table 2. Current legislation relating to digital ID

Digital Identification	
Policy/Legislation	No specific policy or law on, or in relation to, a digital ID system has been identified. A review of existing legislation relating to ID systems does not preclude the implementation of a digital ID system, provided that empowering legislation is adopted consistent with constitutional protections. General legislation on other ID systems, such as the issuance of national IDs under the Registration of Persons Act, 1989, has been enacted as further discussed below.
Institutional Structure/Governance	As noted, the RMI has no specific provision on the issuance of digital IDs, nor is there a ministry or agency tasked with developing or overseeing a digital ID system. That said, the Registrar-General is responsible for issuing national ID cards,[32] and other agencies are responsible for issuing other forms of functional IDs as further discussed below (e.g., the Chief of Police for driver's licenses). Considering the existing national ID card framework, the Registrar-General could be the government agency empowered with implementing or overseeing a future digital ID system.
Data protection and privacy	No specific provisions regarding data protection in relation to general ID systems and registries have been identified. Further discussion relating to privacy and data protection is included in section 4.

[31] World Bank, Guidelines for ID4D Diagnostics, https://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf.
[32] *See* Registration of Persons Act, 1989, §1613 (1).

Data security	No specific provisions on data security for general ID databases or registers have been identified. Further discussion relating to cybersecurity and cybercrime is included in section 6.
Data sharing/cooperation	No formal mechanisms of information sharing between domestic government agencies on data related to IDs were identified. No formal mechanisms of information sharing between the government—and its agencies—and trusted third parties were identified.
Inclusion	Existing ID systems appear to establish broad coverage and eligibility requirements to ensure non-discriminatory assignment and use of IDs in the RMI. Further review and validation of this matter is required with in-country visits and stakeholder engagement. Distinctions are made between citizens and non-citizens. As discussed below, in some cases, such as ID cards, non-citizens are excluded from registering and obtaining credentials. In others, such as driver's licenses or social security cards, non-citizens are eligible to obtain functional IDs.
Foundational ID systems – ID cards	**ID Cards:** the Registration of Persons Act, 1989, requires the Registrar-General to keep and maintain the Register of Persons,[33] and to issue ID cards to registered persons.[34] Only citizens, regardless of age, are eligible for registration;[35] however, registration is not compulsory.[36] No specific provisions exist in this Act in relation to the storage, management, protection, or usage of the Register of Persons. ID cards must: • be in the prescribed form and contain prescribed particulars, including but not limited to the applicant's name, address, and date and place of birth; • bear one copy of the applicant's photograph; • bear the signature of the facsimile of the signature of the Registrar-General or Assistant Registrar-General; • bear the signature of the applicant; and • contain any distinguishing mark imposed on that card by a machine or otherwise under the authority of the Registrar-General.[37] The text of Part IV of the Registration of Persons Act, 1989, assumes the physical nature of the ID card credential, as it may be replaced for loss or damages, and may not be altered by making "any mark, endorsement, or entry upon, or erase, cancel, or alter any such mark, endorsement or entry contained in any identity card or otherwise deface or destroy such card."[38] Based on the above, specific legislative provisions or amendments would be required to implement a digital ID system linked to the Registration of Persons Act, 1989, especially if additional personal information (e.g., biometric data) would be collected.

[33] *See* Registration of Persons Act, 1989, §1607.
[34] *See* Registration of Persons Act, 1989, § 1613 (1).
[35] *See* Registration of Persons Act, 1989, § 1606(1).
[36] *See* Registration of Persons Act, 1989, § 1608. [stating that "[a] person who is eligible to registration under this Chapter, may apply to the Registrar-General for such registration."]
[37] *See* Registration of Persons Act, 1989, § 1613 (2)-(3).
[38] *See* Registration of Persons Act, 1989, § 1614, § 1615, § 1620.

Foundational ID systems – Birth certificates	**Birth certificates**: the Births, Deaths and Marriages Registration Act, 1988, states that every Registrar must maintain separate registers with respect to births, deaths, and marriages in the Atoll for which she/he is appointed.[39] In addition, the Registrar-General must maintain separate General Registers for births, deaths, and marriages for the whole of the RMI.[40] Further, where a person ceases to hold the office of Registrar of any Atoll, the Act requires that "all registers, books, documents, and other material in the possession" of the office holder to be physically delivered to her/his successor.[41] Consistent with international law,[42] birth registrations are compulsory in RMI.[43] Upon registering a birth, the Registrar must give the informant "a certificate under his hand in the prescribed form" that the birth has been registered.[44] This credential is a physical document and is a key instrument to prove RMI citizenship for natural born persons. Note that while existing legislation does not recognize the possibility of keeping digital registers or issuing digital records of birth, there is also no explicit prohibition in the Births, Deaths and Marriages Registration Act, 1988 or other statutes to do so. Additional legislation would be required to support the application, processing, issuance, and recording of such digital birth records and registers.
Functional ID systems- Passports, driver's licenses, voter ID, social security numbers	**Passports**: the RMI Government issues passports to citizens under the Passport Act, 2020.[45] These are physical credentials that "shall serve as the official Government of the Republic of the Marshall Islands confirmation of the identity of the bearer."[46] Passports are not compulsory and are intended as proof of identity in order to facilitate the bearer's international travels.[47] **Driver's licenses:** the Motor Traffic Act, 1986 requires every eligible person, unless exempted, to be licensed to operate a motor vehicle by the Chief of Police.[48] The Chief of Police must also maintain "proper records" of all issued licenses, including name of operator, license number, and class.[49] Driver's licenses are compulsory to operate motor vehicles and every licensed person is required to have such license in their "immediate possession at all times when driving a motor vehicle."[50] **Social Security**: the Social Security Act, 1990, requires the RMI Social Security Administration to (i) issue each worker a social security number (SSN) and a social

[39] *See* Births, Deaths and Marriages Registration Act, 1988, § 405(2).
[40] *See* Births, Deaths and Marriages Registration Act, 1988, § 405(1).
[41] *See* Births, Deaths and Marriages Registration Act, 1988, § 406.
[42] *See* UN Convention on the Rights of the Child, Article 7; International Covenant on Civil and Political Rights, Article 24(2). The RMI is a signatory of both treaties. *See* UN Treaty Collections, Convention on the Rights of the Child, status as of June 9, 2023, https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en and UN, Human Rights treaty Body Database, Ratification Status for CCPR - International Covenant on Civil and Political Rights, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en.
[43] *See* Births, Deaths and Marriages Registration Act, 1988, § 407. [stating that "[s]ubject to the provisions of this Part, the birth of every child born in the Marshall Islands shall be registered by the Registrar for the Atoll in which the child was born (…)."]
[44] *See* Births, Deaths and Marriages Registration Act, 1988, § 418.
[45] *See* Passport Act, 2020, §1115(1).
[46] *See* Passport Act, 2020, §1115(2).
[47] *See* Passport Act, 2020, §1108 (1)(b).
[48] *See* Motor Traffic Act, 1986, §111.
[49] *See* Motor Traffic Act, 1986, §111.
[50] *See* Motor Traffic Act, 1986, §119.

security card,[51] and (ii) maintain a "permanent register" of workers' account numbers.[52] This ID system is aimed at supporting social benefits of covered persons (e.g., pensions, old age insurance, and disability insurance).[53] Social security cards must state the name and SSN of each worker.[54] The law allows information exchange with the Division of Revenue and Taxation, requiring the "strictest security of these records and documents and information."[55]

Voter registration: the Elections and Referenda Act, 1980 makes voter registration compulsory for all eligible voters in the RMI.[56] The process to register must be done in person before the Board of Elections assigned to her/his electoral district, or to the person that the district authorizes to administer the oath and subscribe the application.[57]

Upon registration of the applicant, the Chief Electoral Officer must issue to the applicant a voter ID number and such ID number must be displayed on the voter's national identification card.[58]

The Chief Electoral Officer is responsible for compiling and maintaining the electoral register,[59] which must show the following personal information for each voter:[60]

- name and sufficient other detail to allow the voter to be identified;
- place and date of birth or, if unknown, the voter's apparent age at the date of registration;
- address of the residence or the location and nature of the land rights by virtue of which the voter is registered:
- nature of the voter's citizenship of the Republic;
- date of registration as a voter under the Elections and Referenda Act, 1980; and
- any further information required to establish the right of the voter to vote in a local government election, as such further information or as the regulations require.

The electoral register may include either a number assigned for purposes of voter registration or, if available, that voter's SSN, or both.[61] Further, the Chief Electoral Officer may, from time to time, correct errors and omissions in the register, delete

[51] *See* Social Security Act, 1990, §133(1). The term "workers" covers all employees (i.e., a natural person who has entered into or works under contract with an employer in the RMI), including both citizens as well as nationals of other countries (with certain exclusion for U.S. personnel). S*ee* Social Security Act, 1990, §103(s), (pp) and §104.
[52] S*ee* Social Security Act, 1990, §133(2).
[53] S*ee* Social Security Act, 1990, Part VI.
[54] S*ee* Social Security Act, 1990, §133(1).
55 *See* Social Security Act, 1990, § 160.
[56] *See* Elections and Referenda Act, 1980, §130. A citizen who has attained the age of 18 years is eligible to vote, provided she/he has not been "certified as insane;" or "convicted of a felony and is serving sentence of imprisonment or is released on parole or probation." *See* Constitution of The Republic of The Marshall Islands, Article IV, §3(1), (2).
[57] *See* Elections and Referenda Act, 1980, §132.
[58] *See* Elections and Referenda Act, 1980, §133(3).
[59] *See* Elections and Referenda Act, 1980, §126(1).
[60] *See* Elections and Referenda Act, 1980, §126(2).
[61] *See* Elections and Referenda Act, 1980, §126(5).

	entries of persons who are dead or no longer eligible, and rearrange the register.[62] Persons are entitled to apply for corrections and omissions to the register.[63]
	Senior citizens: the Senior Citizens Act, 2018 charges the Office of Senior Citizens Affairs with maintaining and updating a list of senior citizens and issuing national individual Senior Citizen Identification Cards.[64] This form of ID applies both to RMI citizens and non-citizens that have reached the age of retirement.[65]

3.2. Gap analysis

Based on the analysis of the various legislative frameworks governing current ID systems, no law governing a digital ID system has been identified in the RMI that could broadly support implementation of e-government services and processes. Current law reviewed is neutral on the matter, neither supporting nor proscribing the use of digital IDs in the RMI.

In addition, existing legislation does not provide a comprehensive privacy framework to safeguard personal information collected, processed, and stored by the government should it implement a digital ID system. Similarly, no specific legislation on security and criminalization of data breaches and other such conduct exists in the RMI. Further assessment of these two issues is provided in sections 4 and 6 below.

Against this backdrop, implementation of digital ID systems by the RMI government would require enactment of an enabling legislative framework. In developing such framework, consideration should be given in terms of (i) how inclusive the system will be; (ii) how the system will be designed—from a structural, technological, procedural, and operational point of view—to determine security, robustness, and sustainability; and (iii) the governance of the system, including the protection of citizens' data to promote trust and accountability.

Digital ID systems can strengthen how the public and private sectors deliver services and create a foundation on which to build new systems, services, and markets, including e-government, cashless payments, and the digital economy.[66] Creating a digital ID can also control how much information (e.g., identity data, certificates) that the user is sharing with the services that require data to operate. The exchange of information can be achieved through the government (e.g., name, date of birth, nationality) and implemented by trusted private sources.[67] When trusted services are involved, both businesses and citizens can benefit in terms of reductions in time and cost for obtaining services.[68]

For example, a digital ID can be used to deliver multiple government services, including:

- obtaining birth, death, marriage, adoption certificates;
- accessing health data and requiring services and certificates;
- filling tax returns;

[62] *See* Elections and Referenda Act, 1980, §127(2).
[63] *See* Elections and Referenda Act, 1980, §129(1).
[64] *See* Senior Citizen Act, 2018, §507(2)(b).
[65] *See* Senior Citizen Act, 2018, §502(1)(e).
[66] World Bank Group, Guidelines for ID4D Diagnostics, p.1, https://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf.
[67] European Commission, Digital Identity for all Europeans. A personal digital wallet for EU citizens and residents, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.
[68] European Commission, Digital Identity for all Europeans. A personal digital wallet for EU citizens and residents, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

- applying and enrolling in schools; or
- making payments.

Digital IDs not only will allow citizens to access digital services offered in the RMI, but also contribute to building trust in international cross-border transactions.

3.3. Recommendations

The government of the RMI may consider enacting digital ID legislation that specifically embeds elements of inclusion, design, and governance. Such legislation should allow all citizens and other persons to access digital services and ensure universal coverage of such services. Further, security and privacy should be incorporated by design into the legislation. The RMI could enact legislation that allows citizens to request their digital ID from birth, integrating digital IDs into the current legislative framework. A determination should be made to assess whether digital ID should be compulsory or voluntary, following current ID card legislation.

Recommendation 1. Proposed actions in relation to digital ID

The RMI should consider:

- Enacting specific legislation on digital ID, considering inclusion, security, and data protection matters (See also Section 4 and 6).
- Enacting legislation that provides for the use of digital IDs and electronic processes to engage in e-transactions with the public sector, institutions, and private organizations (See also Section 5).

4. Privacy and Data Protection

4.1. Current situation

There is no general data protection law or privacy framework in the RMI. However, several pieces of sectoral legislation establish varying degrees of privacy safeguards for personal data collected and stored by the government of the RMI as well as certain private entities.

The right to privacy in the RMI can be described as part of a universal right to live without external and unwanted interferences. As noted in section 2.4, the RMI Constitution states that privacy is protected from "unreasonable intrusions." [69] The Constitution does not identify the source of the intrusion, instead broadly protecting persons in the RMI from unwanted invasion of their personal sphere. While the concept of privacy itself is multifaceted, especially as different societies have a different sense of what should be kept private and secured,[70] over the years the RMI has defined the scope of the right to privacy through legislation.

Privacy laws in the RMI have evolved in response to the nation's experience and needs. Starting in the 1980s, privacy provisions included in RMI legislation were sectoral in nature, focused on banking and taxation, and key terms such as "information," "privileged information," "disclosure," and "secrecy" were progressively introduced into the legislative framework. This sectoral approach resulted in certain gaps in privacy law. For instance, during this initial period, areas of the law where one would expect to find privacy protections, such as healthcare legislation (e.g., the Health Service Act), lacked any such privacy and data protections.

However, moving forward into the 2010s, the scope of privacy was expanded to cover concepts, such as "dignity," "reputation," "consent," and "disaggregation," and focused on specific mechanisms to protect certain categories of personal data. Laws, such the Persons with Disabilities Act, 2015, limit disclosure of personal, health, or rehabilitation data without consent, and set a framework to protect dignity, reputation, and physical or mental integrity of the involved persons.

Even if RMI's legislative framework has not regulated privacy with a uniform approach over time, the constitutional right to privacy has always been foundational in legislative choices. That constitutional right appears to have slowly evolved into a data protection regime, albeit sectoral. As a result, the RMI presents an evolving concept of privacy, which impacts individuals differently based on the regulated matter and the time of the enactment of the legislation.

As further discussed below, the rights of data subjects in the RMI vary widely based on various factors, such as socio-economic condition, gender, age, and type of data involved in the regulated process. While this system allows great flexibility in modifying specific pieces of legislation, it does not provide a uniform framework on which persons in the RMI may rely.

In this context, the table below reviews legislation in force in the RMI impacting privacy and data protection to differing degrees.

---

[69] *See* Constitution of the Republic of the Marshall Islands, art. 2, §13,["All persons shall be free from unreasonable interference in personal choices that do not injure others and from unreasonable intrusions into their privacy".]

[70] James Q. Whitman, The two western Cultures of Privacy: Dignity versus Liberty, Yale Law School (2004), at 1153. At https://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty.

Table 3. Current legislation relating to privacy and data protection

Privacy and Data Protection	
Policy/Legislation	No general policy or law on data protection has been identified. While the RMI has not established a comprehensive approach toward data protection and privacy legislation, recent sectoral legislation has expanded protection to specific groups.
Institutional Structure/Governance	There is no data protection authority in the RMI. No other ministry or agency is explicitly tasked with general data protection functions. Different ministries and agencies, such as the Ministry of Finance or the Ministry of Health, are responsible for sectoral data protection functions in the matters under their purview.
Definitions	The RMI lacks a uniform framework defining key privacy and data protection-related terminology. There is a lack of uniform identification regarding the nature of the data processed.
Data life cycle	There are no common provisions on data collection, storage, and processing. There is no general provision that requires data to be adequate, relevant, and limited for the purpose (i.e., data minimization). Only three acts were identified that establish a data retention period, the Banking Act, 1987, Income Tax Act, 1989,[71] and the Tax Collection Act (1966). [72] There are few provisions on the integrity and confidentiality of data. For example, the Exchange of Information Act, 1989 provides for confidential treatment of tax related information under the Compact of Free Association Agreement with the United States. [73] The Cancer Registry Act, 2009 provides for information on cancer incidence and related data to be considered confidential. [74]
Data subject rights	The law does not provide any mechanism for users to have control over their data. The legislation lacks privacy and cookies policies requirements. There are no general provisions on the right to access, right to ratification, right to erasure, right to information, right to data portability, right to object, and right to avoid automatic decision-making.
Information sharing	There is no general provision regarding data sharing with third parties. Mechanisms of information sharing between domestic agencies were identified between the Division of Revenue and Taxation and the Social Security Administration. Mechanisms of information sharing between the RMI and other countries are regulated by treaties (e.g., anti-money laundering (AML), antiterrorism legislation, taxation).

[71] *See* Income Tax Act, 1989, §132 (1).
[72] *See* Tax Collection Act, §306.
[73] *See* Exchange of Information Act, 1989, §302.
[74] *See* Cancer Registry Act, 2009, §1805.

Privacy provisions in first wave of legislation – initial phase (1980-2000s)	**Banking:** the Banking Act, 1987 broadly addresses "information" as a key feature of the sectoral banking framework but does not define the term. Information must be submitted correctly by clients and can be shared for AML procedures and policies, customers' due diligence, customers' files, samples of accounts, and transaction information.[75] Bank employees must keep secret all matters relating to the affairs of clients or operations, except when disclosure is required by law. [76] Every bank and financial services provider must keep records of several types of data on all transactions, which should be in a "readily recoverable form."[77] These records should be retained in the banks or financial services provider's buildings for at least six years after the last relevant transaction.[78] Records on customers' identification, account files, and financial transactions should be kept for six years by financial institutions after the account is closed.[79] The Banking Act, 1987 covers several key matters related to privacy, such as the importance of secrecy and the use of terminology like "information." The act also introduced data management provisions, such as data retention periods and the ability of the data controller to access and manage the data subjects' data. The act is sufficiently broad to allow an electronic database even without modifying the act's wording. **Income taxation**: the Income Tax Act, 1989 requires the Secretary of Finance and every employee of the Department of Finance to ensure the secrecy of all information concerning individual taxpayers.[80] Some information is defined as "privileged" and must undergo special treatment.[81] A data retention period of three years is required for privileged information, after which information can be deleted.[82] Information can be shared with the Social Security Administration, or to an appointed committee or to law enforcement only for investigation of specific criminal offenses.[83] Data from tax returns can be used to compile and publish statistics or public information, as "long as there is no reference to a particular return" or it does not in effect divulge the content of any one return.[84] As such, the Income Tax Act, 1989 recognizes taxpayers' information as secret and defines some data as privileged. The act also provides a data management policy setting the data retention period. This piece of legislation, moreover, defines when and how data can be shared between national agencies and how data can be processed in order to respect persons' privacy rights and provide anonymized information to the public for research. **Tax collection**: the Tax Collection Act (1966) establishes a data retention period of three years by persons, corporations, or association for every record of a

[75] *See* Banking Act, 1987, §163(2)(c).
[76] *See* Banking Act, 1987, §154.
[77] *See* Banking Act, 1987, §169(1)-(2).
[78] *See* Banking Act, 1987, § 169(4).
[79] *See* Banking Act, 1987, §169(2).
[80] *See* Income Tax Act, 1989, §132(2).
[81] *See* Income Tax Act, 1989, §132.
[82] *See* Income Tax Act, 1989, §132 (1).
[83] *See* Income Tax Act, 1989, §132 (3) and (5).
[84] *See* Income Tax Act, 1989, §132 (7).

transaction subjected to a tax, fee, or charge levied or imposed by the law.[85] The Secretary of Finance is responsible for maintaining the records of each of the Atoll's accounts.[86]

This act establishes the existence of different kinds of data for taxation purposes. It establishes procedures on data management, such as setting the data retention period for both privileged information and other information, creating a process to delete and update data, establishing a process to share information between national agencies, and identifying the subject responsible of the data. The act also sets standards for statistical or research use of data.

Information exchange: the Exchange of Information Act, 1989 provides for the confidentiality of tax-related information under the Compact of Free Association Agreement with the United States.[87] The information collected is considered confidential and can only be disclosed for law enforcement purposes.[88] Data can be used for statistical purposes, without disclosing the identity of any person in relation to their income.[89] Employees cannot disclose in any court information regarding return of income, assessment or notice of assessment, or any information related to the work performed, except when in the scope of the agreement.[90]

The act provides a definition of confidentiality and creates a process that allows the use of data for statistical purposes while protecting persons' privacy. The act also establishes a policy to ensure that data are properly shared for pre-determined purposes.

Statistics: the Statistics Act, 1986 allows authorized officers to require any person to fill in specific forms for statistical purposes.[91] The office collects, processes, and presents statistical information.[92] When approved by the relevant Minister, the act requires any person having custody or control of data needed for statistical purposes to grant access to the National Statistician office.[93] An officer cannot ask to share information regarding a third person.[94] However, the act does not require the disclosure of "privileged information" defined as "official, secret or confidential [...] technical process or trade secret."[95]

Under the Statistics Act, 1986, the Statistics Office has the power to collect, process, and share data. Despite this, the act does not provide any information regarding data retention and security measures applied to the stored data. The legislation is sufficiently broad to include an electronic database of the data and to allow implementation of data-security protocols.

Social Security: the Social Security Act, 1990 requires that the Social Security Administration maintain records of workers' personal data.[96] The act allows

[85] *See* Tax Collection Act, §306.
[86] *See* Tax Collection Act, §307A, 307B, 307C.
[87] *See* Exchange of Information Act, 1989, §302.
[88] *See* Exchange of Information Act, 1989, §304.
[89] *See* Exchange of Information Act, 1989, §305.
[90] *See* Exchange of Information Act, 1989, §309.
[91] *See* Statistics Act, 1986, §1010 (1).
[92] *See* Statistics Act, 1986, §1004 (1)(d).
[93] See Statistics Act, 1986, §1011.
[94] *See* Statistics Act, 1986, §1017(1).
[95] *See* The Statistics Act, 1986, §1016.
[96] *See* Social Security Act, 1990, §133(2).

	information exchange with the Division of Revenue and Taxation, requiring the "strictest security of these records and documents and information."[97] See Table 2 for more context related to SSN as a form of ID. The legislation is sufficiently broad to include an electronic database of workers' account numbers, data, and benefits. The legislation does not provide security measures for data storage or data life cycle provisions. **Healthcare**: the Health Services Act, 1983 regulates health care professionals and the licensing of heath care providers. Notably, however, this act does not contain any duty of confidentiality, or any provision related to privacy and data protection in relation to health information or health records in general.
Privacy provisions in second wave of legislation – current phase (2010s)	**Cancer registry**: the Cancer Registry Act, 2009 requires the Ministry of Health to establish a database to collect information on cancer incidence and related data.[98] All data are considered confidential and "private information." An *ad hoc* protocol was created to ensure confidentiality and privacy.[99] All information that can identify a patient contained in "records of interviews, written reports, letters, or statements" in connection with cancer morbidity and mortality should be confidential and privileged and used only for study purposes.[100] Studies on the matter can be published but cannot identify individuals or the specific sources of information.[101] The Secretary of Heath can implement agreements to exchange confidential information with foreign cancer registers or healthcare facilities to obtain a report of RMI residents.[102] Guidelines and control measures for providing statistical information to other nations' cancer registries, control agencies, or health researchers to collaborate in studies and establish prevention must be in place to allow the sharing of data.[103] Confidential information can only be released after the approval of MOH IRC or an academic committee for the protection of human subjects.[104] This legislation is sufficiently broad to allow an electronic database of the cancer incidence and related data. The act identifies procedures for data sharing and guidelines to treat confidential data, and identifies how and when data can be used for study purposes **Persons with disabilities**: the Rights of Persons with Disabilities Act, 2015 recognizes equal rights for people with disabilities and recognizes equal accessibility to information and communication technology systems.[105] The act further states that the respect of persons with disabilities' privacy should be maintained "equally with others" and includes the right to be protected from unlawful interference and disclosure of personal, health, or rehabilitation information without consent. The act protects dignity, reputation, and physical or

[97] *See* Social Security Act, 1990, §160.
[98] *See* Cancer Registry Act, 2009, §1803.
[99] *See* Cancer Registry Act, 2009, §1805.
[100] *See* Cancer Registry Act, 2009, §1805(2).
[101] *See* Cancer Registry Act, 2009, §1805(2).
[102] *See* Cancer Registry Act, 2009, §1806(1).
[103] *See* Cancer Registry Act, 2009, §1806 (2).
[104] *See* Cancer Registry Act, 2009, §1806 (2).
[105] *See* Rights of Persons with Disabilities Act §1106 (c).

mental integrity of the data subjects.[106] Further, the law explicitly requires the confidentiality of medical records or information of persons with disabilities.[107]

The Ministry of Internal Affairs' role is to collect information— including from reliable and internationally comparable statistical and research data—to implement policies and give effect to the act.[108] The Ministry maintains the collected information and applies safeguards, "including legislation on data protection, in order to ensure confidentiality and respect for privacy."[109] The data collected must be disaggregated "as appropriate" and include disaggregated gender data.[110] The records may be in electronic format, provided the information is readily retrievable and is protected against loss and unauthorized alteration.[111]

The Right of Persons with Disabilities Act, 2015 is the piece of legislation that most directly focuses on data protection in the RMI, requiring the application of different safeguards to protect sensitive data.

Gender equality: the Gender Equality Act, 2019 aims to improve gender statistics, "including sex-disaggregated data" in all areas of women's and girl's lives and to ensure gender equality across policies in all sectors.[112] The government collects gender disaggregated data and information related to all areas and identifies where inequality, underrepresentation, and disadvantages occur.[113] The act requires data on women's lives to be collected, disaggregated by sex, age, disability, ethnicity, socio-economic background, sexual orientation, gender identity, and any other status.[114] Notably, the act provides a detailed list of data to be collected and how to properly use them to reach the goal of gender equality.[115]

The act is sufficiently broad to allow the creation of an electronic database. However, the act lacks policies and procedures establishing rules on the life cycles of data and safeguards to protect the security of data.

Child welfare: the Child Rights Protection Act, 2015 recognizes that children have the right to privacy, described as the right to not suffer from "arbitrary or unlawful interference with his/her privacy or family, nor to unlawful attacks on his/her reputation" and "to protection of the law against such interference or attacks."[116] This right also allows the minor to have their identity protected and not disclosed to the public during a proceeding.[117]

The act formally recognizes the right to privacy and the respect of confidentiality of children's data in sensitive matters. The language defining the right to privacy is similar to the one used in the Constitution.

[106] *See* Rights of Persons with Disabilities Act §1114.
[107] *See* Rights of Persons with Disabilities Act §1117 (g).
[108] *See* Rights of Persons with Disability Act, §1138 (1).
[109] *See* Rights of Persons with Disabilities Act §1138 (2)(a).
[110] *See* Rights of Persons with Disabilities Act §1138 (3)(a).
[111] *See* Rights of Persons with Disabilities Act §1139 (3).
[112] *See* Gender Equality Act, 2019, §704 (3)(d), (e).
[113] *See* Gender Equality Act, 2019, §708 (1), (2).
[114] *See* Gender Equality Act, 2019, §725 (2)(b).
[115] *See* Gender Equality Act, 2019, §725 (1), (2).
[116] *See* Child Protection Act, 2015, §1010.
[117] *See* Child Protection Act, 2015, § 1007(2) (c).

4.2. Gap analysis

Data protection and privacy are cornerstones of modern society. Protecting personal data and ensuring the respect of a person's right to privacy is a challenge that countries have been facing for decades. As noted above, the RMI has not enacted comprehensive or sectoral data protection and privacy legislation. While specific data protection or privacy provisions exist in some acts, such as the Rights of Persons with Disabilities Act or the Income Tax Act, those provisions are dispersed and lack a cohesive policy approach and legislative framework.

Many terms used in current legislation are not consistently defined. For example, "privileged data" refers to both banking information and sensitive data (e.g., on cancer morbidity and mortality). Further, most laws that include privacy provisions recognize the collection of personal data made by the government and identify a responsible agency to safeguard and manage it. Those agencies are often also in charge of ensuring the accuracy and integrity of data.

There are few provisions on the life cycle of data in the RMI's current legislative framework. Only three laws—the Banking Act, 1987, Income Tax Act, 1989, and the Tax Collection Act (1966)—establish a data retention period. The existing framework does not provide common guidelines regarding data collection, processing, storage, and cancellation.

Few laws explicitly state how and for which purposes national agencies can exchange data. For example, the Social Security Act and the Tax Collection Act allow respective agencies to exchange data for pre-determined purposes. One piece of legislation in particular, the Cancer Registry Act, 2009, provides protocols to exchange data with international health providers and sets safety measures to ensure both privacy and data protection of the patients covered.

Relatedly, the legislative framework does not differentiate between identified or identifiable data. This can be an issue when the population is particularly small, as it can be easier to identify a data subject based on a relatively few pieces of information. Moreover, the lack of definitions can impact the protection of a smaller portion of that population, which is already more fragile based on gender, age, or health conditions.

As newer legislation has been enacted by the Nitijela over the last 15 years, greater attention has been paid to data protection. Laws such as the Persons with Disabilities Act, 2015 and the Gender Equality Act, 2019, incorporate new concepts and create policies and safeguards to gather, process, and use data. Over time, new terminology has been introduced, such as confidentiality, data disaggregation, authorized/unauthorized access, loss, and alteration of data. As a result, acts enacted in the 2010s provide higher level and broader protection of personal data than in prior years. For example, this is the case of the Rights of Persons with Disability Act, which allows the Ministry of Internal Affairs to enact data protection laws and policies to ensure confidentiality and the respect of privacy.

While the RMI lacks a comprehensive legal framework on data protection matters, additional steps have more recently been taken to protect a broader number of categories of data than in the past, leveraging the constitutional provision that protects persons' privacy rights.

4.3. Recommendations

The government of the RMI may consider enacting a data protection and privacy legislative framework that is fit-for-purpose based on national conditions and consistent with international practices. As a reference, this framework should reflect the privacy standard set forth in the Constitution. The proposed

legislation should also expand upon recent legislation aimed at protecting determined categories of persons.

The proposed legislation should include general definitions of terms such as “data,” “anonymization,” “minimization,” “violation of personal data,” or “transparency,” as well as setting standards for best practices in the private and public sectors.

Moreover, the proposed legislation should follow international standards, such as the OECD Privacy Framework guidelines. Consequently, the collection of data should be limited, and data should be obtained lawfully and—when appropriate—with the knowledge or consent of the data subject. Personal data should be relevant for the purposes for which it is being collected and should be accurate and up to date. Personal data should be protected with adequate safeguards, both physical and electronic, in order to avoid loss, unauthorized access, destruction, improper use, modification or disclosure.

Lastly, the RMI should consider assigning data protection functions to a specific agency. This could be done by establishing a new data protection authority or vesting an existing agency with the power to enforce data protection legislation, as well as cooperate with foreign authorities. This important step will create a framework for national and international agencies to work together and will support the ability of the RMI government, including law enforcement agencies, to protect citizens’ personal data more effectively.

Recommendation 2. Proposed Actions in relation to Privacy and Data Protection Legislation

The RMI should consider:

- Enacting specific legislation on data protection and privacy that aligns with international standards and the Constitution. The legislation should include definitions and set standards for best practices.
- The legislation should be designed to ensure inclusion and non-discrimination.
- The legislation should create a data protection authority or vest data protection functions with an existing agency.

5. Electronic Transactions

5.1. Current situation

The current legal framework in the RMI does not establish comprehensive or sector-specific rules setting out the legal equivalence of electronic records and signatures as compared to paper and hand-signed documents. For example, there is no mention of e-transactions or electronic signatures (e-signatures) in sectoral legislation including the Banking Act, 1987, Consumer Protection Act (1970), Foreign Investment Business License Act, 1990 or Notaries Public Act (1966). The only provisions identified in our review on e-transactions and e-signatures are included in special legislation governing secured transactions and voidable transactions, which has a limited scope of application.

Similarly, no specific provisions addressing the use of digital technologies for the provision of government services was identified. For example, as discussed in section 3.1 above, existing legislation on issues such ID cards or birth registrations explicitly or implicitly assumes paper-based processes and documentation.

The table below reviews current RMI legislation that may impact electronic transactions, signatures, contracts, commerce, and other records.

Table 3. Current legislation relating to electronic transactions

Electronic transactions	
Policy/Legislation	No specific policy or law on e-transactions has been identified.
Institutional Structure/Governance	Responsibility for e-transactions is uncertain. The Ministry of Transport, Communications and Information Technologies oversees the ICT sector, but no specific powers have been granted regarding e-transactions. In limited instances, other ministries may be involved, such as the Ministry of Resources and Development under the Secured Transactions Act, 2007,[118] or the Minister of Finance under the Business Corporation Act, 1990.[119]
Electronic Transactions	No specific provisions have been identified that enable widespread use of e-transactions. However, limited examples of legislation recognizing the validity of e-transactions have been identified. **Secured transactions**: the Secured Transactions Act, 2007 provides a very limited example of e-transactions regarding security interests in movable property that applies to "transactions that secure an obligation with collateral."[120] The law defines a record as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form" and allows for a "security agreement" to be in an electronic record that is "effective between the parties and against purchasers and creditors."[121] Thus, in the limited manner prescribed by the Secured Transactions Act, 2007, electronic records may be considered legally effective. **Voidable transactions**: the Uniform Voidable Transactions Act, 2018 provides another limited example of e-transactions in relation to the legal framework for

[118] *See* Secured Transactions Act, 2007, §528(1).
[119] *See* Business Corporation Act, 1990, §5(3).
[120] *See* Secured Transactions Act 2007, §503(1).
[121] *See* Secured Transactions Act 2007, §502(aa) and §510.

	creditor protections. This law defines a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[122] Such "records" are sufficient for an "obligation" to be incurred if the record is "signed by the obligor [and] is delivered to or for the benefit of the obligee."[123] Note that this act, which is taken verbatim from a U.S. model law with the same tittle,[124] applies narrowly to mechanisms aimed at strengthening creditor protections by providing remedies for certain transactions by a debtor that are unfair to the debtor's creditor.
Electronic Signatures	No specific provisions have been identified that enable widespread use of e-signatures. However, two limited examples have been identified. **Corporate records**: the Business Corporation Act, 1990 establishes e-signatures as legally binding, albeit in a narrow capacity. In particular, the act requires all instruments to be signed by an officer, director, or other authorized person of the corporation and specifies that the "signature on any instrument authorized to be filed with a Registrar of Corporations under this Act may be a facsimile or an electronically transmitted signature."[125] **Voidable transactions**: the Uniform Voidable Transactions Act, 2018 recognizes the validity of e-signatures, noting that to "sign" a record includes attaching or logically associating with the record "an electronic symbol, sound or process."[126] **Commercial code**: the Uniform Commercial Code (Reference) Act, 2018 repealed and replaced the Sale of Goods Act, 1986 and permits (but does not require) the national courts to reference Articles 1 to 8 of the Uniform Commercial Code (UCC) of the United States.[127] The UCC generally permits electronic or digital signatures. For example, Section 3-401 of the UCC authorizes a signature for negotiable instruments to be made "manually or by means of a device or machine."[128] However, it is not clear whether the courts have interpreted this provision to allow for e-signatures in the RMI.
Electronic Contracts	No specific provisions regarding electronic contracts (e-contracts) have been identified.
Electronic Commerce	No specific provisions have been identified that enable widespread use of electronic commerce (e-commerce).
Electronic Government	No specific provisions regarding the equivalence of government documents and the provision of e-government services were identified.

[122] *See* Uniform Voidable Transaction Act, §901(13).
[123] *See* Uniform Voidable Transaction Act, §906(5).
[124] *See* National Conference of Commissioners on Uniform State Laws, Uniform Voidable Transaction Act (Formerly Uniform Fraudulent Transfer Act) (As Amended in 2014), at https://higherlogicdownload.s3-external-1.amazonaws.com/UNIFORMLAWS/8326748f-1240-842e-9a13-aad3853c6eba_file.pdf?AWSAccessKeyId=AKIAVRDO7IEREB57R7MT&Expires=1686596029&Signature=jQHByqT8uDpZ5VOCNSs8tESEIWo%3D.
[125] *See* Business Corporation Act 1990, §5(3).
[126] *See* Uniform Voidable Transaction Act, §901(15).
[127] *See* Uniform Commercial Code (Reference) Act 2018, §102. Note that the UCC (upon which RMI's law is based) is not itself a law of the United States but is a collection of proposed model laws drafted by the American Law Institute and the U.S. National Conference of Commissioners on Uniform State Laws and intended to guide U.S. state legislatures when drafting statutes involving commercial contracts and transactions.
[128] *See* Uniform Commercial Code, §3-104, https://www.law.cornell.edu/ucc/3/3-401.

Legal equivalence	No specific provisions have been identified that establish the legal equivalence of electronic records and signatures as compared to paper and hand-signed documents.
Trust Services	No specific provisions regarding trust services have been identified.
International recognition	No formal mechanisms for cross-border or international use of electronic records or trust services have been identified.

5.2. Gap analysis

E-transaction legislation, which recognizes "the legal equivalence between paper-based and electronic forms of exchange," is the global norm.[129] Such legislation may be comprehensive or sector specific. Whereas an overarching e-transactions law establishes a comprehensive framework that applies across all sectors, countries may also adopt sector-specific laws (e.g., financial services, consumer protection, or business licensing legislation) that address e-transactions and e-signatures in certain areas.

According to the United Nations Conference on Trade and Development (UNCTAD), e-transactions laws are a "prerequisite for conducting commercial transactions online."[130] As of December 2021, UNCTAD identified that 81 percent of countries worldwide have adopted e-transaction legislation while another 7 percent of countries were in the process of finalizing such laws. Only 12 percent of countries were identified as having no law or no data on e-transaction legislation. Notably, RMI was identified as one of the countries with no data on such laws.[131]

In line with UNCTAD's findings, RMI's current legal and regulatory frameworks do not establish comprehensive or sector-specific rules setting out the legal equivalence of electronic records and signatures as compared to paper and hand-signed documents.

5.3. Recommendations

Adopting an Electronic Transactions Act or similar legislation in the RMI would establish a governance framework for a range of activities that promote the digital economy by providing legal equivalence to electronic transactions, signatures, records, and commerce while enabling security mechanisms and user protections.

Recommendation 3. Proposed actions in relation to electronic transactions legislation

The RMI should consider:

- Enacting comprehensive e-transaction legislation that provides legal equivalence between electronic and paper record and applies widely to all types of transactions, contracts, signatures, and other records with limited exceptions to be determined following consultation with key stakeholders, but which could include a limited range of matters, such as for wills/testamentary trusts, real estate, or family law.

[129] UNCTAD, E-transactions Legislation Worldwide (2021), https://unctad.org/page/e-transactions-legislation-worldwide#:~:text=A%20prerequisite%20for%20conducting%20commercial,29%20are%20Least%20Developing%20Countries..
[130] UNCTAD, E-transactions Legislation Worldwide (2021), https://unctad.org/page/e-transactions-legislation-worldwide#:~:text=A%20prerequisite%20for%20conducting%20commercial,29%20are%20Least%20Developing%20Countries..
[131] UNCTAD, E-transactions Legislation Worldwide (2021).

- The legal framework should also regulate e-government services, including equivalence provisions and mechanisms to phase in the provision of services by different ministries and agencies.
- The proposed legislation should take a technology-neutral approach to ensuring interoperability between systems, particularly in international commerce.
- To promote security and trust, the framework may include mechanisms that establish certification of providers to offer trust services that can serve to guarantee the origin and integrity of electronic records and signatures. The framework may also address intermediary liability that could be implemented through a self- or co-regulatory approach.
- Legislation could be based on various international models, such as the UN Convention on the Use of Electronic Communications in International Contracts,[132] UNCITRAL Model Law on Electronic Commerce,[133] and UNCITRAL Model Law on Electronic Signatures.[134]

[132] UNCITRAL, United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005),https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications#:~:text=Purpose,their%20traditional%20paper%2Dbased%20equivalents..

[133] UNCITRAL, Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

[134] UNCITRAL, Model Law on Electronic Signatures (2001) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.

6. Cybersecurity and Cybercrime

6.1. Current situation

The National Strategic Plan 2020-2030 recognizes the relevance of cybersecurity, among other security dimensions, as a key policy goal for the protection of the people and the country,[135] as well as calls for continued steps to strengthen law enforcement institutions to address cybercrimes.[136]

To date, however, the RMI has yet to adopt a national cybersecurity strategy or policy or enact specific cybersecurity or cybercrime legislation. Such a policy, together with a draft Cybercrime Bill, appear to have been developed and laid before the Nitijela in 2020,[137] but these documents were not available for review for this report. Even before then, a Computer Crimes Bill also appears to have been developed in 2011 but did not progress.[138]

In this context, the table below reviews legislation in force in the RMI that may impact cybersecurity and cybercrimes in differing degrees.

Table 4. Current legislation relating to cybersecurity and cybercrime

Cybersecurity	
Policy/Legislation	No specific policy or law on cybersecurity has been identified.
Institutional Structure/Governance	Responsibility for cybersecurity is uncertain.[139] No Computer Emergency Response Team (CERT) has been established in the RMI. The Ministry of Transport, Communications and Information Technologies has purview over ICTs, but no specific powers in relation to cybersecurity threats or incidents. Other law enforcement agencies, such as the Attorney General and the RMI police, are granted law enforcement functions.[140]
Protection of Critical Information Infrastructure (CII)	No specific provisions in relation to the protection of CII have been identified.
Incident reporting/response	No specific provisions for reporting or responding to cyber threats or incidents have been identified.

[135] National Strategic Plan 2020-20230, p. 20, https://rmi-data.sprep.org/system/files/Marshall%20Islands%20National%20Strategic%20Plan%202020%20to%202030.pdf.
[136] National Strategic Plan 2020-20230, p. 19-20.
[137] *See* World Bank, Republic of the Marshall Islands e-Government Pathway, Draft for Consultation, April 2021, para. 115.
[138] *See* Pacific Region Infrastructure Facility (PRIF), Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands, October 2019, p. 169, https://www.theprif.org/sites/default/files/documents/cyber_security_report_low_res_rev_5.pdf.
[139] The Maritime Administrator has issued a Marine Guidance on Maritime Cyber Risk Management, providing for mitigation of cyber risks that may result in shipping-related operational, safety, or security failures. This guidance also provides for a voluntary framework of maritime cyber incident reporting to the Maritime Administrator. *See* Republic of the Marshall Islands Maritime Administrator, Marine Guidance, No.2-11-16, Rev. March 2023, https://www.register-iri.com/wp-content/uploads/MG-2-11-16.pdf.
[140] The Attorney General is tasked with discharging the duties of the "head of any Department or office dealing with the administration of justice". *See* Article VII, section 3(b) of the Constitution of the Marshall Islands.

Information sharing/cooperation	No formal mechanisms of information sharing between domestic agencies on cyber threats/incidents were identified.
Cybercrime	
Policy/Legislation	No specific policy or law on cybercrimes has been identified. The section below identifies provisions of general criminal acts that establish offenses that could be applied to certain cybercrimes.
General substantive criminal provisions	**Violation of privacy:** the Criminal Code, 2011 criminalizes harassment, which covers repeatedly making "electronic mail transmissions without the purpose of legitimate communications."[141] Unlawful eavesdropping or surveillance in "private places" is also criminalized. These are understood as places where there is a reasonable expectation of privacy, that is, where the public does not have access.[142] Similarly, the Criminal Code, 2011 criminalizes the interception of private communications, including messages by "telephone, telegraph, facsimile, electronic mail, letter or other means of communicating privately."[143] **Forgery and fraudulent practices:** The Criminal Code, 2011 criminalizes traditional forgery, defined as altering "any writing" without authorization with the intent to defraud, deceive or injure anyone.[144] A "writing" is defined broadly to include "printing or any other method of recording information," which reasonably can be read to include digital information.[145] **Terrorist acts**: the Counter-Terrorism Act, 2002 identifies the disruption or destruction of electronic systems of as a "terrorist act" if "intended, or by its nature or context can be reasonably regarded as intended, to intimidate the public or any portion of the public, or to compel a government or an international or regional organization to do or refrain from doing any act." [146] This includes acts that affect: "(i) an information system; (ii) a telecommunications system; (iii) a financial system; (iv) a system used for the delivery of essential government services; (v) a system used for, or by, an essential public utility; (vi) a system used for, or by, a transport system".[147] This offense would not cover cybercrimes affecting CII for reasons unrelated to terrorist actions.
Procedural criminal provisions	The Criminal Procedure Act has general provisions on process, criminal searches, and seizures.[148] This includes the ability to search the premises where an arrest is made for "instruments, fruits, and evidences of the criminal offense for which the arrest is made, and, if found, seize them."[149] While these provisions could be read as extending to the search and seizure of electronic evidence, no procedural provisions specifically aimed at cybercrime investigations and proceedings have been enacted.

[141] *See* Criminal Code, 2011, § 250.4(1).
[142] *See* Criminal Code, 2011, § 250.12(1).
[143] *See* Criminal Code, 2011, § 250.12(2)(a).
[144] *See* Criminal Code, 2011, § 224.1(1)(a).
[145] *See* Criminal Code, 2011, § 224.0(1).
[146] *See* Counter-Terrorism Act, 2002, § 105(38).
[147] *See* Counter-Terrorism Act, 2002, § 105(38)(g).
[148] *See* Criminal Procedure Act, Part II and III.
[149] *See* Criminal Procedure Act, §123(1).

International cooperation / Mutual assistance	**Mutual Assistance**: the Mutual Assistance in Criminal Matters Act, 2002 enables Marshallese law enforcement agencies to cooperate with foreign countries in criminal investigations and proceedings.[150] This legislation is sufficiently broad to cover cybercrime investigations. The RMI's law enforcement agencies tend to seek assistance from U.S. law enforcement, particularly through the Federal Bureau of Investigation (FBI) in Guam or Hawaii.[151] **Extradition**: the Criminal Extradition Act provides rules for the extradition of persons charged with felonies or other crimes who have fled from justice and are found in the RMI.[152] This legislation is sufficiently broad to cover extraditions for cybercrimes.

6.2. Gap assessment

6.2.1. Cybersecurity

With the increased diffusion of digital technologies and services, there is a marked need to protect CII against threats and attacks that may severely impact basic functions of modern societies. A strong cybersecurity legislative framework supports the resilience of critical computer systems and data, allow the identification and categorization of CII, sets forth measures to enhance security measures for such infrastructure, and enables appropriate responses to cybersecurity incidents.

As noted above, the RMI has not enacted a cybersecurity policy or cybercrime legislation. No centralized authority has been tasked with the mandate to ensure cybersecurity of CII in the RMI. Existing legislation criminalizes as terrorist acts any conduct aimed at destroying or disrupting certain types of CII. This requires meeting higher evidentiary standards linked to terrorist acts and does not cover criminal acts against the availability, integrity, and confidentiality of CII.

6.2.2. Cybercrime

As digital transformation advances and societies adopt digital technologies for everyday social and commercial interactions, a comprehensive legislative framework criminalizing globally recognized cybercrimes becomes critical to protect citizens and support the development of digital transactions, both in the public and private sectors.

Such legislation should encompass, for example, offenses against the availability, integrity, and confidentiality of computer systems and computer data, as well as criminalize computer-related offenses such as electronic forgery and electronic fraud. Similarly, procedural safeguards specifically tailored to support the investigation of cybercrimes should also be considered, including investigative tools for the collection of electronic evidence for specific criminal investigations. Given the typical cross-border nature of cybercrime, the RMI should set forth the necessary arrangements for cooperation with other jurisdictions.

As noted above, the RMI has not enacted comprehensive, substantive cybercrime legislation. While provisions in the Criminal Code, 2011 and the Counter-Terrorism Act, 2002 arguably cover certain types

[150] *See* Mutual Assistance in Criminal Matters Act, 2002, §402.
[151] *See* Pacific Region Infrastructure Facility (PRIF), Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands, October 2019, p. 170.
[152] *See* Criminal Extradition Act, §203.

of cybercrimes, this framework is incomplete. For example, the legislation does not cover computer-related offenses regarding data interference (i.e., damage, deletion, deterioration, alteration, or suppression of computer data without right); system interference (i.e., the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data); or computer-related forgery or fraud, among others.

Likewise, the RMI has yet to enact procedural legislation with specialized provisions for the collection and preservation of electronic evidence for criminal law enforcement purposes. As discussed, general search and seizure provisions in the Criminal Procedure Act may extend to the search and seizure of electronic evidence, but do not specifically empower law enforcement agencies to make and retain a copy of computer data, maintain the integrity of data, or render inaccessible or remove computer data in an accessed computer system.

Comprehensive substantive and procedural cybercrime legal provisions in line with international best practices are necessary to support digital security and usher in digital transformation and technology adoption in the RMI. This framework will be particularly relevant considering the broader scope of the digital services project and is a key building block to build trust in digital transactions and the roll-out of a digital ID program.

6.3. Recommendations

6.3.1. Cybersecurity

The government of the RMI may consider enacting cybersecurity legislation that specifically identifies and categorizes CII, prescribes actions to enhance security for such infrastructure, sets forth processes to provide appropriate responses to cybersecurity incidents, and establishes specific offenses for attacks on critical infrastructure with aggravated penalties.

The RMI should also consider enacting the necessary enabling framework for the creation of CERTs to ensure expeditious responses to cybersecurity incidents. Taking account of the limitations inherent to the scale of the Marshallese market, this legislation could establish a principles-based approach that is not prescriptive and allows for international good practices in cybersecurity measures.

Recommendation 4. Proposed actions in relation to cybersecurity legislation

The RMI should consider:

- Enacting comprehensive cybersecurity legislation to identify and categorize CII, enhance security measures for such infrastructure, enable appropriate responses to cybersecurity incidents, and create specific offenses for attacks on critical infrastructure.
- Implementing provisions that establish CERTs.

6.3.2. Cybercrime

The government of the RMI may consider enacting a cybercrime legislative framework that is fit-for-purpose considering national conditions and consistent with international practices. As a reference, this framework could reflect the generally accepted standards set forth in the Convention on Cybercrime

(Budapest Convention).[153] This would include enacting legislation criminalizing conduct, such as data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud, as well as introduce dissuasive and proportionate sanctions for such offenses. In addition, online-based offenses, such as cyberstalking and cyberbullying, could also be considered.

In addition, the RMI should consider updating its criminal procedure statute to create comprehensive provisions enabling, among other potential matters, the expedited preservation of stored computer data, its partial expedited preservation, partial disclosure of data, and the adoption of production orders. This would create a framework for law enforcement to combat cybercrime more effectively.

Lastly, the RMI could consider accession to the Budapest Convention to enable Marshallese law enforcement agencies to complement and expand on existing mutual assistance legislation with respect to cybercrime and electronic evidence.

Recommendation 5. Proposed actions in relation to cybercrime legislation

The RMI should consider:

- Enacting specific legislation on cybercrimes that aligns with international practices and criminalizes internationally recognized cybercrimes.
- Enacting legislation that provides for criminal procedures to enable law enforcement agencies to effectively investigate crimes involving electronic evidence.
- Acceding to the Budapest Convention to facilitate Marshallese law enforcement agencies cooperation with other countries to further cooperate on cybercrime investigations.

[153] *See* Convention on Cybercrime, Budapest 23.XI.2001, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

7. Implementation plan

Implementation of digital transformation initiatives in the RMI should proceed on parallel tracks. This should involve (i) the adoption of a legislative package to create trust in the use of digital IDs and to support e-transactions and e-government services and (ii) the creation of a framework to empower ministries and agencies to map and roll-out digital services and processes.

7.1. Legislative reform package implementation

As described in sections 3, 4, 5 and 6 of this report, the RMI lacks a comprehensive framework to support and provide legal certainty to the implementation of digital ID systems, as well as e-transactions and e-government services. Enacting a legislative package to enable digital services should be a key policy objective to support such services and ensure inclusion, security, and trust in digital technologies and services in the RMI.

Considering the current situation assessment and recommendations included in this report, a set of four different laws should be considered:

1. legislation on e-transactions and e-government;
2. legislation on data protection;
3. legislation on digital IDs; and
4. legislation on cybercrime and cybersecurity.

To advance the process of drafting and enacting of this legislative package, we propose a phased process as described in Figure 1 to prepare draft bills and introduce them in the Nitijela. The expectation with this proposed approach and timeline is to provide the RMI government and legislature sufficient time to develop and enact the legislative package. Introducing the e-transactions bill in the September 2023 session is aimed at laying the legal foundation for ministries and agencies in the RMI to begin preparatory work toward mapping and implementing e-government services and processes, as further discussed in section 7.2. The expectation is that, by the January 2024 session, further foundational bills may be drafted to support implementation of such e-government services in a manner that ensures trust, security, and inclusion.

Figure 1. Proposed approach to develop digital services legislative framework and introduce bill before the Nitijela

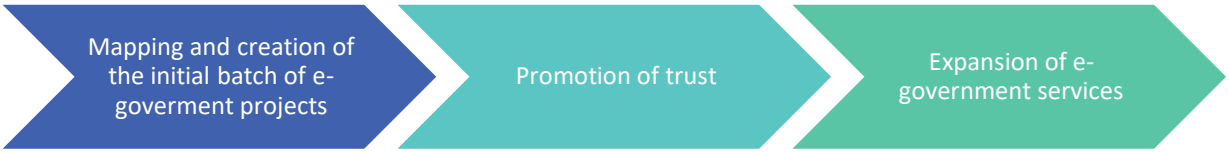
Source: TMG

7.2. E-government service implementation

A strategy to roll-out digital public services in the RMI should be aimed at leveraging technology to enhance citizen services. Rethinking how governmental services are offered will lead to new and efficient ways of serving the public in the RMI. As noted in this report, a key component of this process will be ensuring trust and inclusive services, which counsels that this initiative should focus first on users' needs, taking a human-centric approach that promotes equal access.

Considering limited experience and capacity with e-government services in the RMI, we propose to follow a voluntary approach to phase in such services with a backstop for mandatory adoption for certain services. This opt-in approach will allow ministries and agencies to map and develop digitalization projects based on perceived internal capabilities and needs. The expectation is that implementation of key proof of concept projects could—once successful—create an environment of trust for both ministries and agencies and among the general public, allowing additional digital services to be implemented over time (Figure 2). Ideally, success of initial projects will encourage other agencies to opt-in to providing e-government services and collaborate to offer additional services.

Figure 2: Proposed approach to encourage governmental agencies to opt-in a e-government platform.



Source: TMG

Telecommunications Management Group, Inc.
1600 Wilson Blvd, Suite 660
Arlington, Virginia 22209
USA
Tel + 1 (703) 224-1501
Fax + 1 (703) 224-1511

www.tmgtelecom.com