



The Senate
TWELFTH OLBIIL ERA KELULAU
P.O. Box 8, Ngerulmud
Republic of Palau 96940

Seventh Regular Session

July 2026

INTRODUCED AS SENATE BILL NO. 12-9, SD1, HD2

AN ACT

See Title Inside

INTRODUCED BY SENATOR (S) TJ Imrur Remengesau, Kerai Mariur, Mason N. Whipps,

Kazuki L. "Topps" Sungino and Lentcer Basilius ET, AL.,

DATE INTRODUCED January 28, 2025

SENATE ACTION

FIRST READING: January 28, 2025
REFERRED TO: Cybersecurity, Telecommunication & Technology
STANDING COMMITTEE REPORT NO.: 12-18
DATE ADOPTED: April 08, 2025
SECOND READING: April 08, 2025
LEGAL FORMAT: Proper
REVIEW: April 08, 2025
THIRD READING: October 14, 2025
FINAL READING: July 20, 2026

HOUSE ACTION

FIRST READING: October 23, 2025
REFERRED TO: CIP Energy, Communication & Public Utilities
STANDING COMMITTEE REPORT NO.: 12-24
DATE ADOPTED: April 21, 2026
SECOND READING: April 21, 2026
LEGAL FORMAT: Proper
REVIEW: April 21, 2026
THIRD READING: July 20, 2026
FINAL READING:

CONFERENCE COMMITTEE ACTION

DATE: NONE
COMMITTEE REPORT NO.: NONE
DATE PASSED: NONE
FINAL READING: NONE


Reagan Sidoi

CLERK OF THE SENATE


Leilani Senior

CLERK, HOUSE OF DELEGATES

AN ACT

To create a comprehensive cybersecurity system in the Republic of Palau; and to amend section 604 of Title 7 of the Palau National Code and for other related purposes.

THE PEOPLE OF PALAU REPRESENTED IN THE OLBIL ERA KELULAU DO ENACT AS FOLLOWS:

Section 1. Legislative findings. The Olbil Era Kelulau hereby finds that Palau has a unique opportunity to harness advancements in information and communications technologies. Increased connectivity to the internet has ushered in an era of inclusive, secure, and sustainable digital transformation in the country. Digital technologies and services have been integrated into all aspects of our daily lives, providing a pathway to enhance educational opportunities, enabling us to engage in commerce and to use public services more efficiently, and allowing us to remain informed of current events and be entertained. They are a tool for us to keep in touch with our family, friends, and our wider community. But these significant benefits are accompanied by risks; these technologies can be misused or can be leveraged by bad actors to harm users and vulnerable groups, including minors. Accordingly, the Olbil Era Kelulau finds that establishing a comprehensive cybersecurity government system has become essential. It is necessary that the Republic of Palau establish a system that ensures all citizens, consumers, and businesses in the Republic of Palau have equitable and affordable access to reliable, secure, and high-quality digital services and technologies that will promote socio-economic development and improve the quality of life in Palau. This will enable safe access to government services, participation in the national and global digital economy, and the development and expansion of digital skills.

Section 2. Amendment. Title 15 of the Palau National Code is amended to add a new Chapter 9 as follows:

“Chapter 9

Cybersecurity

§ 901. Short title.

§ 902. Definitions.

§ 903. Bureau of Cybersecurity; powers and duties.

§ 904. Chief Information Security Officer; powers and duties; appointment.

§ 905. Cybersecurity Advisory Committee; duties; constituents; meeting; reports; compensations.

§ 906. Data protection and confidentiality -- penalties.

§ 907. Temporary Provision.

§ 908. Rights Not Affected.

§ 909. Liabilities Not Affected.

§ 910. Severability.

§ 901. Short Title.

This Act may be cited as the “Cybersecurity Act.”

§ 902. Definitions.

(a) “Agency” means any Palau National Government executive and administrative agencies, offices, boards, and commissions;

(b) “Cybersecurity” means acts, practices, or systems that eliminate or reduce the risk of loss of critical assets, loss of sensitive information, or reputational harm as a result of a cyber-attack or breach within a person’s or organization’s network;

(c) “Information security” means acts, practices, or systems that eliminate or reduce the risk that legally protected information or information that could be used to facilitate criminal activity is accessed or compromised through physical or electronic means;

(d) “Information technology” means computer hardware, storage media, networking equipment, physical devices, infrastructure, processes and code, firmware, software, and ancillary products and services, which include:

(1) Systems design and analysis;

(2) Development or modification of hardware or solutions used to create, process, store, secure, or exchange electronic data;

(3) Information storage and retrieval;

(4) Voice, radio, video, and data communications;

(5) Network, hosting, and cloud-based systems;

(6) Simulation and testing;

(7) Interactions between a user and an information system; and

(8) User and system credentials.

(e) “Legally protected information” means information explicitly protected by existing Palau law.

(f) “Personal data” means any information relating to an identified or identifiable natural person, including but not limited to names, identification numbers, location data, and online identifiers.

(g) “Proprietary and confidential data” means information pertaining to companies, institutions, and groups, including trade secrets, financial records, and other non-public or sensitive information.

(h) “Security Officer” means the chief information security officer.

§ 903. Bureau of Cybersecurity; powers and duties.

(a) There is hereby established the “Bureau of Cybersecurity,” and it is administratively attached to the Ministry of Public Infrastructure and Industries. The Security Officer manages the office.

(b) Except as provided by law, the Bureau of Cybersecurity must oversee, in a fiscally responsible manner, cybersecurity and information security-related functions for agencies and may:

(1) Adopt and implement rules establishing minimum security standards and policies to protect agency information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across information technology resources used by agencies, citizens, consumers, and businesses in the Republic of Palau to promote the availability, security, and integrity of the information processed, transacted, or stored by them in the Republic’s information technology infrastructure and systems;

1 (2) Develop minimum cybersecurity controls for managing and
2 protecting information technology assets and infrastructure for all entities that
3 are connected to an agency-operated or owned telecommunications network;

4 (3) Monitor agency information technology networks, consistent with
5 information security standards, to detect security incidents and support
6 mitigation efforts as necessary within capabilities;

7 (4) Obtain agency system event logs, as reasonably necessary to
8 perform its monitoring and detection duties, to support monitoring and
9 detection pursuant to paragraph (3) of this subsection;

10 (5) Create a model incident-response plan for agencies, in coordination
11 with state and national cybersecurity emergency management agencies as
12 appropriate, to adopt with the Bureau of Cybersecurity as the incident-response
13 coordinator for incidents that:

- 14 (i) Impact multiple public bodies;
15 (ii) Impact or involve citizens of the Republic;
16 (iii) Impact or involve consumers in the Republic; or
17 (iv) Impact or involve businesses in the Republic.

18 (6) Serve as a Cybersecurity resource for national and state
19 governments;

20 (7) Develop a service catalog of cybersecurity services to be offered to
21 agencies, citizens, consumers, and businesses in the Republic;

22 (8) Collaborate with agencies in developing standards, functions, and
23 services to ensure that agency regulatory environments are understood and
24 considered a part of a cybersecurity incident response;

25 (9) Establish core services to support minimum security standards and
26 policies;

27 (10) Establish minimum data classification policies and standards and
28 design controls to support compliance with classifications and report on
29 exceptions;

(11) Temporarily suspend the expenditure of monies if the office determines that the information technology project is at risk of failing to achieve its intended results or does not comply with the requirements of the Act;

(12) Continuously study emergent technology and evaluate its impact on the Republic's system;

(13) Maintain all confidential information as necessary;

(14) Provide staff support to the committee established by section 905 of this Act, and, as appropriate, retain the services of qualified consultants;

(15) Advise and make recommendations to the President of the Republic of Palau and the Olbiil Era Kelulau on all matters concerning its objectives;

(16) Manage enterprise-level information technology infrastructure;

(17) Temporarily suspend access to information technology infrastructure when directed by the Ministry of Finance, and consult with the Ministry of State regarding security policies, standards, and procedures;

(18) Develop and issue cybersecurity awareness policies and training standards and develop and offer cybersecurity training services; and

(19) Establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state. This reporting process must include a mandatory requirement for agencies to notify affected individuals, companies, institutions, or groups whose data has been compromised in a breach, consistent with the minimum security standards and policies adopted by the Bureau of Cybersecurity.

§ 904. Chief Information Security Officer; powers and duties; appointment.

(a) There is hereby created the position of "Chief Information Security Officer."

(b) The Security Officer must, subject to the approval of the President, have powers to make regulations as he deems necessary for cybersecurity. However, such regulations must be promulgated by the President of the Republic of Palau.

(c) The President of the Republic of Palau must appoint the Security Officer, subject to the advice and consent of the Senate.

(d) The Security Officer must:

(1) Serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance, and the technologies impacting executive branch cybersecurity programs;

(2) Ensure the Bureau of Cybersecurity resources assigned or provided to executive branch agencies are in compliance with applicable laws and regulations;

(3) Coordinate cybersecurity efforts between executive branch agencies;

(4) Provide guidance to executive branch agencies when compromise of personal information or computer resources has occurred or is likely to occur as the result of an identified high-risk vulnerability or threat;

(5) Act as the primary point of contact for international cybersecurity cooperation and enter into information-sharing agreements with foreign Computer Emergency Response Teams (CERTs) and international law enforcement bodies to mitigate cross-border cyber threats; and

(6) Perform such other functions and duties as provided by law.

(e) While absent, the Security Officer can delegate the authorities prescribed herein to his or her designee.

(f) The designee executes the Security Officer's duties in the absence of the officer.

§ 905. Cybersecurity Advisory Committee; duties; constituents; meeting; reports; compensations.

(a) There is hereby established the "Cybersecurity Advisory Committee" within the Bureau of Cybersecurity, and it must assist the office in the development of:

(i) a national cybersecurity plan;

(ii) statewide cybersecurity plans;

(iii) guidelines for best cybersecurity practices for agencies; and

(iv) recommendations on how to respond to a specific cybersecurity threat or attack.

(b) The Security Officer or the Security Officer's designee must chair and be an advisory non-voting member of the committee. The remaining members consist of:

(1) One (1) member appointed by the Ministry of Finance who is experienced with cybersecurity issues;

(2) Two (2) members appointed by the Senate who are experienced with cybersecurity issues;

(3) One (1) member appointed by the House of Delegates who is experienced with cybersecurity issues; and

(4) Three (3) members appointed by the President of the Republic of Palau who are experienced with cybersecurity issues.

(c) The Cybersecurity Advisory Committee may invite representatives of unrepresented agencies or other public entities to participate as advisory members of the committee.

(d) Pursuant to the Act or other statutory authority, the Security Officer may issue orders regarding the compliance of agencies with guidelines or recommendations of the Cybersecurity Advisory Committee. Compliance with those guidelines or recommendations by non-executive agencies or state governments must be strictly voluntary.

(e) The Cybersecurity Advisory Committee must hold a meeting every two (2) months at minimum, provided that the Security Officer shall have the discretion to call for more frequent meetings as necessary. At the discretion of the Security Officer, the committee may issue advisory reports on cybersecurity issues.

(f) The Cybersecurity Advisory Committee must submit an annual report to the presiding officers of the Olbiil Era Kelulau and to the President of the Republic of Palau regarding the status of cybersecurity preparedness within agencies and elsewhere in the country. Every September 30, the Bureau of Cybersecurity must present updated reports to the committee and the President.

(g) The members of the Cybersecurity Advisory Committee must receive no payment for their services as members of the committee.

§ 906. Data protection and confidentiality -- penalties.

(a) An agency must ensure that all information technology systems and information technology practices are, at a minimum, consistent with international best practices standards as to security and confidentiality regarding:

- (1) personal data;**
- (2) proprietary and confidential data; and**
- (3) legally protected information.**

(b) Right to Privacy and Security. The policies, standards, and practices adopted under § 903(b)(1) and (8) must explicitly prioritize and protect the right to privacy of all citizens and consumers in the Republic of Palau, ensuring that the collection, processing, storage, and exchange of electronic data are conducted securely and lawfully.

(c) It is unlawful for an officer, employee, or agent of any agency to intentionally or recklessly access, disclose, misuse, or otherwise compromise personal data, proprietary and confidential data, or legally protected information that the officer, employee, or agent obtains or processes in the course of that individual's duties, resulting in a breach of confidentiality or security.

(d) The penalties for breach of confidentiality and security are as follows:

(1) Any person who commits a prohibited act under this section is subject to administrative discipline, including termination of employment, and may be liable for a civil penalty of up to \$10,000 for each instance of a breach of confidentiality or security, as determined by a court. These penalties shall be in addition to any other civil remedies provided by law.

(2) Any person who commits a prohibited act under this section with the intent to defraud or with the intent to cause harm shall be guilty of a felony and, upon conviction, is subject to a fine of not less than \$10,000 or imprisonment for a term not to exceed five (5) years, or both.

(e) Notwithstanding the foregoing, it shall not be a violation of this section for an individual to access an information technology system solely for the purpose of good-faith security research, provided that the individual does not cause harm, does

not disclose personal data, and reports the vulnerability to the Bureau of Cybersecurity within a reasonable timeframe.

§ 907. Temporary Provision.

(a) All functions, personnel, money, appropriations, records, furniture, equipment, supplies, and other property pertaining to cybersecurity or information security are transferred to the Bureau of Cybersecurity;

(b) All contractual obligations for cybersecurity or information security services are binding on the Bureau of Cybersecurity; and

(c) All references in law to the Chief Information Security Officer must be deemed to be references to the Security Officer, unless context demands otherwise.

(d) The sum of \$150,000, or so much thereof as may be required, is authorized and appropriated as organizational and initial operational funding for the Bureau of Cybersecurity. The sum appropriated in this subsection shall come from local revenues and shall not lapse.

(e) The Bureau of Cybersecurity shall, in coordination with the Ministry of Finance, submit a recurring annual budgetary request to the Olbiil Era Kelulau to ensure the continued maintenance of national cybersecurity infrastructure and the retention of qualified technical personnel.

§ 908. Rights Not Affected.

The Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

§ 909. Liabilities Not Affected.

The enactment of the Act must not have the effect of terminating or in any way modifying any liability, civil or criminal, which is already in existence before its effective date.

§ 910. Severability.

If any provisions of the Act or the application of it to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the Act that can be given effect without the invalid provision or application, and to this end, the provisions of the Act are severable.

1 Section 3. Effective date. Except otherwise as provided by law, the Act takes
2 effect upon its approval by the President of the Republic of Palau or upon becoming
3 law without such approval.

4 Section 4. Amend Section 604 of RPPL 12-4 as follows:

5 “Section 604. Appointment of Ship Registry Administrator; duties of
6 Administrator; temporary exemption.

7 (a) ...

8 (b) To ensure the continued and uninterrupted operation of the Registry in the
9 event of a lapse in contractual arrangements, the President is hereby authorized to
10 enter into a contract for the operation of the Republic of Palau Open Ship Registry,
11 established pursuant to Chapters 6 through 13 of Title 7 of the Palau National Code.
12 The contract authorized in this subsection shall not be subject to the public notice and
13 competitive bidding requirements contained in Chapter 6 of Title 40 of the Palau
14 National Code, shall be for a term of six (6) months or less, and shall provide that the
15 Republic of Palau must receive not less than fifty percent (50%) of all revenue
16 generated by the Registry. The contract may be extended for one (1) additional term
17 of not more than six (6) months, provided that the procurement process for a
18 subsequent contract has been initiated prior to such extension and that the extension is
19 solely for the purpose of allowing sufficient time to complete the evaluation and award
20 of the long-term contract. Any subsequent contract for such services shall adhere to all
21 requirements contained in Chapter 6 of Title 40 of the Palau National Code.”

Passed on: July 20, 2026

Approved this 21st day of July, 2026.



H. E. Surangel S. Whipps, Jr.
President, Republic of Palau