CONGRESS OF THE FEDERATED STATES OF MICRONESIA
P.O. Box PS 3
Palikir, Sokehs
Pohnpei State, FM 96941
Tel: (691) 320-2324/2325/2326/2327/2337/2338/2707
Fax: (691) 320-5122

COMMITTEE ON
JUDICIARY AND
GOVERNMENTAL OPERATIONS

STANDING COMMITTEE REPORT NO. 24-28

RE: C.B. No. 24-14/J&GO/T&C

SUBJECT: TO FURTHER AMEND TITLE 21 OF THE CODE OF THE FEDERATED STATES OF MICRONESIA (ANNOTATED), AS AMENDED, BY CREATING A NEW CHAPTER 4 ESTABLISHING A LEGAL FRAMEWORK TO PROMOTE CYBERSECURITY, PROTECT CRITICAL INFORMATION INFRASTRUCTURE, CREATE A COMPUTER EMERGENCY RESPONSE TEAM, AND PROVIDE FOR OTHER MATTERS CONCERNING CYBERSECURITY BOTH DOMESTIC AND INTERNATIONAL, AND FOR OTHER PURPOSES.

MAY 20, 2026

The Honorable Esmond B. Moses
Speaker, Twenty-Fourth Congress
Federated States of Micronesia
Fourth Regular Session, 2026

Dear Speaker:

Your Committee on Judiciary and Governmental Operations, to which was jointly referred Congressional Bill No. 24-14, entitled:

> "TO FURTHER AMEND TITLE 21 OF THE CODE OF THE FEDERATED STATES OF MICRONESIA (ANNOTATED), AS AMENDED, BY CREATING A NEW CHAPTER 4 ESTABLISHING A LEGAL FRAMEWORK TO PROMOTE CYBERSECURITY, PROTECT CRITICAL INFORMATION INFRASTRUCTURE, CREATE A COMPUTER EMERGENCY RESPONSE TEAM, AND PROVIDE FOR OTHER MATTERS CONCERNING CYBERSECURITY BOTH DOMESTIC AND INTERNATIONAL, AND FOR OTHER PURPOSES.",

begs leave to report as follows:

STANDING COMMITTEE REPORT NO. 24-28

RE: C.B. No. 24-14/J&GO/T&C

SUBJECT: TO FURTHER AMEND TITLE 21 OF THE CODE OF THE FEDERATED STATES OF MICRONESIA (ANNOTATED), AS AMENDED, BY CREATING A NEW CHAPTER 4 ESTABLISHING A LEGAL FRAMEWORK TO PROMOTE CYBERSECURITY, PROTECT CRITICAL INFORMATION INFRASTRUCTURE, CREATE A COMPUTER EMERGENCY RESPONSE TEAM, AND PROVIDE FOR OTHER MATTERS CONCERNING CYBERSECURITY BOTH DOMESTIC AND INTERNATIONAL, AND FOR OTHER PURPOSES.

MAY 20, 2026

The intent and purpose of this bill are expressed in its title.

Your Committee received Congress Bill No. 24-14 that proposes to establish a legal frame work to promote cybersecurity, protect critical information infrastructure, create a computer emergency response team, and provide for other matters concerning cybersecurity both domestic and international.

Your Committee held public hearings in Yap (November 25, 2025), Chuuk (November 28, 2025), and Kosrae (December 2, 2025) to meet with the Legislative branch, Executive branch, and the general public to brief them on all the cybersecurity bills and to solicit comments. Chairman of the J&GO Committee, Senator Andy P. Choor, who served as head of the delegation, and Senator Perpetua S. Konman. Senator Yoslyn G. Sigrah joined your Committee in Kosrae. Your Committee was joined by the Secretary of the Department of Transportation, Communications, and Infrastructure (hereafter "TC&I"), Carl Apis; Assistant Secretary for TC&I, Edward Albert for all the hearings and Assistant Secretary of the Department of Justice's Cybersecurity Division (hereafter "DOJ"), Minoru Stephen, joined the hearings in Yap and Kosrae. Your delegation was supported by Congress Staff Attorney Catherine Allen and Legislative Counsel for the Congress of the Federated States of Micronesia, Yancy Cottrill.

STANDING COMMITTEE REPORT NO. 24-28

RE: C.B. No. 24-14/J&GO/T&C

SUBJECT: TO FURTHER AMEND TITLE 21 OF THE CODE OF THE FEDERATED STATES OF MICRONESIA (ANNOTATED), AS AMENDED, BY CREATING A NEW CHAPTER 4 ESTABLISHING A LEGAL FRAMEWORK TO PROMOTE CYBERSECURITY, PROTECT CRITICAL INFORMATION INFRASTRUCTURE, CREATE A COMPUTER EMERGENCY RESPONSE TEAM, AND PROVIDE FOR OTHER MATTERS CONCERNING CYBERSECURITY BOTH DOMESTIC AND INTERNATIONAL, AND FOR OTHER PURPOSES.

MAY 20, 2026

November 25, 2025, Yap State Legislative Chamber

At the November public hearing in Yap, Chairman Choor brought up several concerns that the Committee raised. He then opened up the floor for questions regarding C.B. 24-14.

A member of the Yap legislature raised a concern about people in the community being blackmailed over internet due to the publication of private images. He suggested that the National Government consider Private Public Partnerships to provide expertise for cybersecurity.

Assistant Secretary of the Cybersecurity Division Minoru Stephen, responded that they have international initiatives which provide cybersecurity trainings.

The members of the Yap legislature inquired about the history of these bills and why past Congresses did not pass them. It was explained that the bills were originally all included in one bill that encompassed and impacted many different areas of the code and committees. As a giant bill it was problematic and they needed to be broken down into simpler single subject bills.

A member of the Yap legislature expressed concern in having outside agencies being utilized to perform the functions of the cybersecurity unit. She mentioned the concern that private information will be in the hands of non-government entities.

Chairman Choor noted that there are no laws currently in place regulating 3rd party entities. He then noted that all

the bills are moving through the Committee together in order to address all the aspects of cybersecurity.

A member of the Yap legislature expressed a concern as to our capability to handle a cyberattack and suggested creating a division. There was a concern about the enforcement, how it would work, what outside agencies would be involved, the costs, what will happen if the outside agency or private partner merges or is bought out. Some ideas and theories about how these issues or potential problems could be addressed.

November 28, 2025 Chuuk State Legislative Chamber

During the November 28th hearing, Chairman Choor explained C.B. 24-14, the Cybersecurity Act. Assistant Secretary Albert then gave a background on the drafting history, a summary on the logic behind the bill and touched on the standards and policies that the bill will put into place. He laid out the division of powers amongst the Department of TC&I and The Department of Justice as they are envisioned under the bill.

Chairman Choor mentioned some concerns that the Committee had and some that were brought up in the previous meeting in Yap, such as, funding, what NGO's or foreign governments will be helping to implement these bills, and the capability to implement the measures under this bill.

A member of the Chuuk legislature stated that he had the same concerns over the funding. Assistant Secretary Albert explained that the World Bank is funding a part of the project initially. He was questioned as to whether the

World Bank was providing funding to the states as well or just the National Government. He responded that the World Bank funding is for the National Government offices, but reiterated that he is hopeful that sectors will work together to collaborate on a single system.

Secretary Apis clarified that the World Bank grant is part of the Digital Project. He stated that funding will not strictly be reserved for the National Government but will need to go to the states. He spoke generally about the census and conducting a real-time census.

The conversation evolved into the data protection and concerns over who could access the data arose. A member of the Chuuk Legislature asked if foreign companies would be collecting the data. Senator Konman commented on the health records in Chuuk and the necessity to keep that data with the state.

December 2, 2025 Kosrae State Legislative Chamber

Assistant Secretary Albert began the hearing by summarizing C.B. No. 24-14. He explained that it will establish a framework for the Department of TC&I and DOJ to work together. Chairman Choor listed several of the concerns which were brought up at the other hearings including, the structure of the CERT team and the costs. Assistant Secretary Albert explained a bit about the importance of centralizing everything on one standardized government platform.

The members of the Kosrae Legislature, the Governor, and the Lieutenant Governor all took turns making welcoming remarks

and stressing the importance of having good cybersecurity bills in place. The Governor stated that it will take time to digest these bills and asked for more time to submit written comments. The Speaker of the legislature stated that these laws are very new and very important, echoing the Governor's request for time to digest. The Lieutenant Governor weighed in stating that cybersecurity is what we need and that he would take a serious look into the bills as this is something that will help the Nation in the long run.

Secretary Apis explained the role of the Department of TC&I and the role of the DOJ. Assistant Secretary of Cybersecurity for DOJ Stephen stated that the costs to start up and maintain the program will outweigh the potential losses. The Governor stated that initially he sees no major concerns with C.B. 24-14.

Pohnpei and Comments

Your Committee was unable to schedule at time with the Pohnpei Legislature to hold a public hearing on Pohnpei. Your Committee sent a letter to the Pohnpei Legislature, the Pohnpei State Supreme Court, and to the Governor's office on April 8, 2026, soliciting comments on all the cybersecurity bills. As of date, your Committee has not received any comments from Pohnpei State.

Your Committee encouraged all the states to send us comments and formal suggestions to improve the cybersecurity legislation. Your Committee received detailed suggestions and comments from the Kosrae State Government on January 14, 2026. Please find their comments attached to this report. To date, your Committee has not received any correspondence

STANDING COMMITTEE REPORT NO. 24-28

RE: C.B. No. 24-14/J&GO/T&C

SUBJECT: TO FURTHER AMEND TITLE 21 OF THE CODE OF THE FEDERATED STATES OF MICRONESIA (ANNOTATED), AS AMENDED, BY CREATING A NEW CHAPTER 4 ESTABLISHING A LEGAL FRAMEWORK TO PROMOTE CYBERSECURITY, PROTECT CRITICAL INFORMATION INFRASTRUCTURE, CREATE A COMPUTER EMERGENCY RESPONSE TEAM, AND PROVIDE FOR OTHER MATTERS CONCERNING CYBERSECURITY BOTH DOMESTIC AND INTERNATIONAL, AND FOR OTHER PURPOSES.

MAY 20, 2026

from the Yap or Chuuk governments regarding any of the cybersecurity bills.

CONCLUSION

Your Committee on Committee on Judiciary and Governmental Operations has carefully reviewed C.B. No. 24-14, held public hearings in three of the states, solicited comments, and now defers to the Committee on Transportation and Communications , to which this bill is jointly assigned, to render a recommendation.

Respectfully submitted,

Andy P. Choor, chairman

Jermy W. Mudong, vice-chairman

Yoslyn G. Sigrah, member

Esmond B. Moses, member

Julio M. Marar, member

Perpetua S. Konman, member

Robson U. Romolow, member

GOVERNMENT OF
KOSRAE
Office of the Governor
Kosrae State
Post Office Box 158
Tofol, Kosrae FM
96944
Telephone (691) 370-
3002/3003/3009

January 14, 2026

Chairman Choor
FSM Congressman
FSM Congress
Palikir, Pohnpei FSM 96941

Re: Transmittal of State of Kosrae Submission on National Digital Governance Bills.

Dear Honorable Chairman Choor,

Warm greetings from the State of Kosrae.

On behalf of the Government of the State of Kosrae, I respectfully transmit herewith the State's formal submission on the package of national legislation presently before Congress concerning cybersecurity, cybercrime, electronic transactions, digital identity, electronic signatures, and personal data protection (C.B. Nos. 24-14, 24-15, 24-17, 24-23, and 24-94).

Kosrae supports the overarching objective of modernizing the Nation's digital legal framework to strengthen cybersecurity resilience, enhance digital trust, safeguard citizens, and promote reliable electronic government services and commerce. At the same time, the enclosed submission respectfully highlights the importance of maintaining constitutional balance between the National Government and the States, ensuring meaningful State participation in governance structures, avoiding unintended centralization, and providing adequate capacity and funding support for State-level implementation.

Kosrae offers these views in the spirit of constructive partnership and cooperative federalism. We respectfully request the Committee's consideration of the attached submission as it continues its review and deliberations on these important measures. The State remains available to provide clarification, technical assistance, or further engagement as the Committee may require.

We thank the Committee for its leadership and service, and we appreciate the opportunity to contribute to this important national legislative process.

With highest respect,

Tulensa W. Palik
Governor
State of Kosrae

The Honorable Chairperson
Judiciary and Governmental Operations Committee
Congress of the Federated States of Micronesia
Palikir, Pohnpei, FM 96941

RE: State Submission on Cybersecurity, Cybercrime, Electronic Transactions, Digital Identity, Electronic Signatures, and Personal Data Protection Bills (C.B. Nos. 24-14, 24-15, 24-17, 24-23, 24-94)

The Honorable Chairman Choor and Members of the Committee,

The Government of the State of Kosrae respectfully submits this position on the package of legislative measures currently before Congress relating to cybersecurity, cybercrime, electronic transactions, digital identity, electronic signatures, and personal data protection. These measures include **C.B. No. 24-14**, establishing a national cybersecurity and critical information infrastructure framework; **C.B. No. 24-15**, creating a comprehensive set of cybercrime offences and enforcement powers; **C.B. No. 24-17**, enacting the FSM Personal Data Protection Act of 2025 under Title 16; **C.B. No. 24-23**, providing a framework for electronic transactions, electronic records and an enabling digital identity and trust regime; and **C.B. No. 24-94**, recognizing electronic signatures as legally equivalent to handwritten signatures and providing for their implementation by regulation.

1. Appreciation and Recognition

Kosrae wishes at the outset to acknowledge and commend Congress for taking on this complex and important reform agenda. Together, these bills seek to modernize the legal framework of the Federated States of Micronesia so that it can better address cybersecurity threats, improve the safety and integrity of information systems, define and punish cyber-enabled crime, enable secure electronic transactions and records, recognize electronic signatures, and safeguard the personal data and privacy of natural persons.

C.B. 24-23 and **C.B. 24-94** are expressly directed toward increasing legal certainty and trust in electronic commerce and e-government. **C.B. 24-23** recognizes the validity and reliability of electronic records and transactions and sets out to provide a coherent legal basis for their use in government and the private sector. **C.B. 24-94** provides that electronic signatures may have the same legal effect as handwritten signatures, subject to implementing regulations that will set out technical and procedural safeguards. **C.B. 24-14** and **C.B. 24-15** respond to the growing threat environment by creating a cybersecurity governance framework and specific cybercrime offences with meaningful penalties. **C.B. 24-17**, the proposed Personal Data Protection Act, sets out a comprehensive framework for the protection of personal data held by core national government departments and agencies, including clear principles of legitimate purpose, data minimization, accuracy, retention, security and accountability, as well as a complaints and remedies structure for individuals.

Kosrae shares and supports the broad policy objectives of these measures: modernization of the legal framework, improved trust in digital systems, enhanced cyber resilience, protection of citizens, and stronger foundations for sustainable development and international engagement.

2. Overview of the Legislative Package and Its Institutional Effects

Taken together, these bills reshape the institutional landscape of digital governance in the Federated States of Micronesia.

C.B. 24-14 creates a national cybersecurity framework centered on national authorities. It empowers the Department of Justice to lead cybersecurity policy, designate and regulate critical information infrastructure, impose technical and organizational obligations on owners of such infrastructure, require reporting and audits, and develop regulations. It assigns technical and operational responsibilities, including management of the national Computer Emergency Response Team, to the Department of Transportation, Communications and Infrastructure. It establishes a National

Cybersecurity Committee which is chaired by national officials and is intended to coordinate policy and implementation across the national government and the States.

C.B. 24-15 inserts a new cybercrimes chapter in Title 11. It defines offences such as unauthorized access to protected computer systems, unauthorized interception of computer data, unauthorized interference with systems or data, unlawful possession or supply of tools used to commit cyber offences, and computer-related forgery. It provides for increased penalties where critical information infrastructure or protected systems are compromised. Crucially, it grants the FSM Department of Justice primary authority to investigate and enforce these offences, to issue instructions and orders, and to make rules and regulations to implement the chapter.

C.B. 24-23 provides the legal underpinnings for electronic transactions and records, including electronic communications with public bodies and an enabling framework for digital identity and trust services. It confers regulatory, supervisory and standard-setting powers on national authorities to ensure the reliability, security and integrity of electronic systems and identity mechanisms.

C.B. 24-94 complements this by confirming that electronic signatures, when they meet prescribed requirements, will have the same validity and effect as handwritten signatures under FSM law, with the details to be elaborated in subordinate regulations.

C.B. 24-17, the Personal Data Protection Act of 2025, renames Title 16 as "Data Protection" and inserts a new chapter entitled "Personal Data Protection". It declares objectives that include establishing an enabling legal framework to protect the personal data and privacy of natural persons in a manner consistent with constitutional privacy rights, providing guidance to natural persons and public bodies on personal data collection and processing, promoting transparency and certainty regarding data sharing, identifying a competent authority, and promoting public confidence and trust in the handling of personal data by government.

Importantly, **C.B. 24-17** clearly states that the chapter applies to "core National Government departments and agencies" that collect, use, store, process, disclose or transfer personal data of natural persons. It also expressly states that nothing in the chapter requires a State to adopt similar laws, nor prevents or prohibits a State from adopting its own laws on personal data protection applicable to purely intrastate activities or to State agencies that handle personal data. The Bill sets out exclusions for purely intrastate activities, national law-enforcement and national security purposes, non-personal data, and certain categories of publicly available lawful information. It then provides detailed definitions, designates the National Statistics Office under the Department of Resources and Development as the competent authority, confers duties and powers on that authority to educate, coordinate, enter into agreements, require information from national agencies and make rules to implement the chapter, and sets out personal data protection principles and a complaints and remedies framework, including a private right of action and judicial remedies such as injunction and mandamus against core national departments and agencies, coupled with reporting and compliance obligations and rules for internal data sharing and guidance.

Kosrae welcomes the fact that **C.B. 24-17** is deliberately limited to core national institutions and explicitly preserves the freedom of States to develop their own data protection laws for State agencies and purely intrastate activities. This drafting approach is noteworthy because it demonstrates that it is possible to advance strong national standards while expressly respecting State autonomy.

3. Core Constitutional and Federal Balance Concerns

In supporting the policy goals of these measures, Kosrae must also respectfully express concerns about their implications for the constitutional balance between the National Government and the States.

The cybersecurity and cybercrime bills, **C.B. 24-14** and **C.B. 24-15**, together concentrate significant power over digital security policy, critical information infrastructure and

cybercrime enforcement in national agencies. The Department of Justice is empowered to designate which systems, including potentially systems owned or operated by State governments, constitute critical information infrastructure, and to impose mandatory technical and organizational requirements on their owners, as well as to require audits, reporting and remedial measures. The Department of Justice also has primary authority to investigate and prosecute cybercrime offences under the Cybercrimes chapter and to issue instructions, orders and regulations to implement that chapter.

The electronic transactions and digital identity bill, **C.B. 24-23**, similarly vests considerable rule-making, certification, supervisory and administrative powers in national bodies in relation to electronic records, transactions, and identity assurance frameworks. These authorities will, in practice, shape the technical and procedural environment within which both national and State systems will operate if they wish to interact fully with national platforms or participate in recognized electronic identity trust regimes.

Kosrae accepts that the National Government must have strong powers in areas of genuine national concern, such as cross-border cyber threats, international cooperation in cybercrime, and interoperability standards for national systems. However, there is a real risk that, absent clear statutory safeguards, these powers will be interpreted or applied in ways that intrude into areas traditionally falling within State administrative authority and public governance. This includes internal State government systems, State-owned utilities and infrastructure, and State-level service delivery platforms.

By contrast, **C.B. 24-17** demonstrates a different approach. It confines the scope of the Personal Data Protection Act to core national departments and agencies and expressly states that it neither compels nor precludes the adoption of State-level data protection laws. It also excludes purely intrastate activities from its scope. Kosrae considers this an example of good federal legislative technique. It protects individuals' privacy when dealing with national institutions while affirming the separate sphere of State competence. Kosrae respectfully suggests that similar clarity and restraint be incorporated into **C.B. 24-14, C.B. 24-15** and **C.B. 24-23**, so that national powers are clearly limited to national

institutions and matters of national and international concern, unless a State has formally agreed to be bound.

4. Concerns Regarding Cybersecurity Governance and Representation

Kosrae is particularly concerned about the governance structure of the National Cybersecurity Committee in **C.B. 24-14**. While the intention to include State representatives is welcomed, the Committee is co-chaired by national officials, its quorum rules require the presence of those officials, decisions are taken by simple majority, and in the event of a tie a deciding vote is reserved to a national officer. Additional members may also be appointed beyond the State representatives.

In practice, this ensures that national representatives will always retain control over outcomes, even if all State representatives share a different position. This structure risks turning what appears on paper to be a national–State coordinating body into a centrally dominated decision-making organ with only consultative roles for the States. Given that cybersecurity designations and policies can significantly affect State-owned infrastructure and services, Kosrae considers such imbalance to be constitutionally and practically problematic.

Kosrae therefore respectfully urges Congress to reconsider the composition and voting arrangements for the National Cybersecurity Committee so that they provide for equitable State participation and shared decision-making, and to ensure that no decisions affecting State systems are made without the meaningful input and agreement of the affected States.

5. Administrative and Implementation Realities

The successful implementation of these bills will require substantial administrative and technical capacity on both the national and State sides. Cybersecurity obligations for

critical information infrastructure, such as risk assessments, security controls, incident reporting and audit responses, require specialist expertise, modern equipment, and sustained budget support. Cybercrime enforcement demands trained investigators, prosecutors, digital forensics capabilities, and judicial familiarity with novel forms of evidence. Electronic transactions and electronic signatures frameworks require secure systems, reliable identity verification mechanisms, and well-governed registries or trust services. Personal data protection entails the development of policies, training and internal controls, and mechanisms to respond to complaints and access requests.

Kosrae is concerned that, without explicit provision for capacity building and financial support for the States, these measures may result in unfunded obligations or create dependence on centrally operated systems in which States have little say. In particular, if State systems are designated as critical information infrastructure or are expected to connect to national identity or transaction platforms, the State will be expected to meet standards and obligations that may not be achievable without assistance.

6. Data Privacy and Citizen Protection

Kosrae strongly supports the objective of enhancing citizen protection, both in relation to cybercrime victimization and in the safeguarding of personal data and privacy. **C.B. 24-15** provides an important legal basis for the prosecution of serious cyber offences, including offences that target children and other vulnerable persons. **C.B. 24-17** establishes a principled framework for the protection of personal data held by core national departments and agencies, built around legitimate purpose, data minimization, accuracy, retention, integrity and security, and accountability. It creates a competent authority, sets out obligations on that authority and on national agencies, and provides for complaints, reporting and remedies, including a private right of action and judicial remedies.

Kosrae notes positively that **C.B. 24-17** is carefully crafted to apply only to core national institutions and explicitly preserves State freedom to enact analogous protections for State agencies and intrastate activities. However, many of the public services through

which citizens most regularly interact with government—such as education, local health services, utilities and local administration—are administered at the State level. In the absence of coordinated State-level frameworks, citizens may enjoy robust protection in their dealings with national agencies, but weaker or more fragmented protection in their dealings with State systems. Kosrae therefore views **C.B. 24-17** as a useful national model, but believes that there should also be explicit recognition and support for the development of complementary State personal data protection regimes, if and when States choose to adopt them.

7. Proposal for Cooperative Federal Implementation and Capacity Support

Kosrae believes that the long-term success of this legislative package depends on a cooperative federal model. Under such a model, the National Government would focus on setting principles, minimum standards, interoperability requirements and international cooperation arrangements, and on regulating national institutions, while the States would retain clear regulatory and administrative authority over their own systems and services. In practical terms, Kosrae respectfully proposes that the bills should:

i. Make clear that national regulatory and enforcement powers are directed at national institutions and matters of national or international concern, and do not automatically extend to State institutions without formal State consent.

ii. Incorporate statutory language comparable to that used in **C.B. 24-17** to affirm that nothing in the Acts requires a State to adopt particular laws, nor prevents or prohibits a State from adopting its own laws in areas such as data protection, cybersecurity and electronic transactions as they apply to State agencies and purely intrastate activities.

iii. Reform the governance structures, particularly the National Cybersecurity Committee, to ensure balanced State representation and genuine shared decision-making.

iv. Establish a formal National–State Cyber and Data Governance Council or strengthen existing committee mandates to provide a structured forum for

critical information infrastructure, such as risk assessments, security controls, incident reporting and audit responses, require specialist expertise, modern equipment, and sustained budget support. Cybercrime enforcement demands trained investigators, prosecutors, digital forensics capabilities, and judicial familiarity with novel forms of evidence. Electronic transactions and electronic signatures frameworks require secure systems, reliable identity verification mechanisms, and well-governed registries or trust services. Personal data protection entails the development of policies, training and internal controls, and mechanisms to respond to complaints and access requests.

Kosrae is concerned that, without explicit provision for capacity building and financial support for the States, these measures may result in unfunded obligations or create dependence on centrally operated systems in which States have little say. In particular, if State systems are designated as critical information infrastructure or are expected to connect to national identity or transaction platforms, the State will be expected to meet standards and obligations that may not be achievable without assistance.

6. Data Privacy and Citizen Protection

Kosrae strongly supports the objective of enhancing citizen protection, both in relation to cybercrime victimization and in the safeguarding of personal data and privacy. **C.B. 24-15** provides an important legal basis for the prosecution of serious cyber offences, including offences that target children and other vulnerable persons. **C.B. 24-17** establishes a principled framework for the protection of personal data held by core national departments and agencies, built around legitimate purpose, data minimization, accuracy, retention, integrity and security, and accountability. It creates a competent authority, sets out obligations on that authority and on national agencies, and provides for complaints, reporting and remedies, including a private right of action and judicial remedies.

Kosrae notes positively that **C.B. 24-17** is carefully crafted to apply only to core national institutions and explicitly preserves State freedom to enact analogous protections for State agencies and intrastate activities. However, many of the public services through

which citizens most regularly interact with government—such as education, local health services, utilities and local administration—are administered at the State level. In the absence of coordinated State-level frameworks, citizens may enjoy robust protection in their dealings with national agencies, but weaker or more fragmented protection in their dealings with State systems. Kosrae therefore views **C.B. 24-17** as a useful national model, but believes that there should also be explicit recognition and support for the development of complementary State personal data protection regimes, if and when States choose to adopt them.

7. Proposal for Cooperative Federal Implementation and Capacity Support

Kosrae believes that the long-term success of this legislative package depends on a cooperative federal model. Under such a model, the National Government would focus on setting principles, minimum standards, interoperability requirements and international cooperation arrangements, and on regulating national institutions, while the States would retain clear regulatory and administrative authority over their own systems and services. In practical terms, Kosrae respectfully proposes that the bills should:

i. Make clear that national regulatory and enforcement powers are directed at national institutions and matters of national or international concern, and do not automatically extend to State institutions without formal State consent.

ii. Incorporate statutory language comparable to that used in **C.B. 24-17** to affirm that nothing in the Acts requires a State to adopt particular laws, nor prevents or prohibits a State from adopting its own laws in areas such as data protection, cybersecurity and electronic transactions as they apply to State agencies and purely intrastate activities.

iii. Reform the governance structures, particularly the National Cybersecurity Committee, to ensure balanced State representation and genuine shared decision-making.

iv. Establish a formal National–State Cyber and Data Governance Council or strengthen existing committee mandates to provide a structured forum for