Cybersecurity Roadmap
Federated States of Micronesia

December 2021

GOVERNMENT OF THE FEDERATED STATES OF MICRONESIA
PEACE UNITY LIBERTY

ocsc
Oceania Cyber Security Centre

MONASH University

APT

Contents

Executive Summary

The Cybersecurity Roadmap (Roadmap) of the Federated States of Micronesia (FSM) is intended as a guide to inform the FSM Government of the priorities for the development of a national cybersecurity strategy, supporting policies, laws and regulations.

Noting the recommendations from the 2020 Cybersecurity Capacity Maturity Model for Nations (CMM) review of the FSM and considering the results from the Roadmap consultations with local stakeholders in October 2021, several domains were identified as priorities for the Roadmap. The Roadmap is divided into three stages of actions to be taken across a total duration of six years.

Stage 1 focuses on building the National Cybersecurity Strategy and supporting cybercrime laws. Here, the priorities for the FSM will include:

- launching a National Cybersecurity Strategy to provide a clear vision for a cyber secure digital FSM and create a governance structure, with clearly defined roles and responsibilities for the development and oversight of the strategy. There is also a need for the strategy to include a program of awareness to build the general public's knowledge of the new cybercrime law and how to protect themselves online. It is also important for the strategy to address the protection of vulnerable citizens online, for example, protecting women and children from online abuse and exploitation;
- passing a classified information law to protect government information;
- passing the existing draft cybercrime law which is aligned with the Council of Europe's Convention on Cybercrime and providing training to enhance the capacity of cybercrime investigation.

Stage 1 activities should be completed within 2 years of the Roadmap being launched.

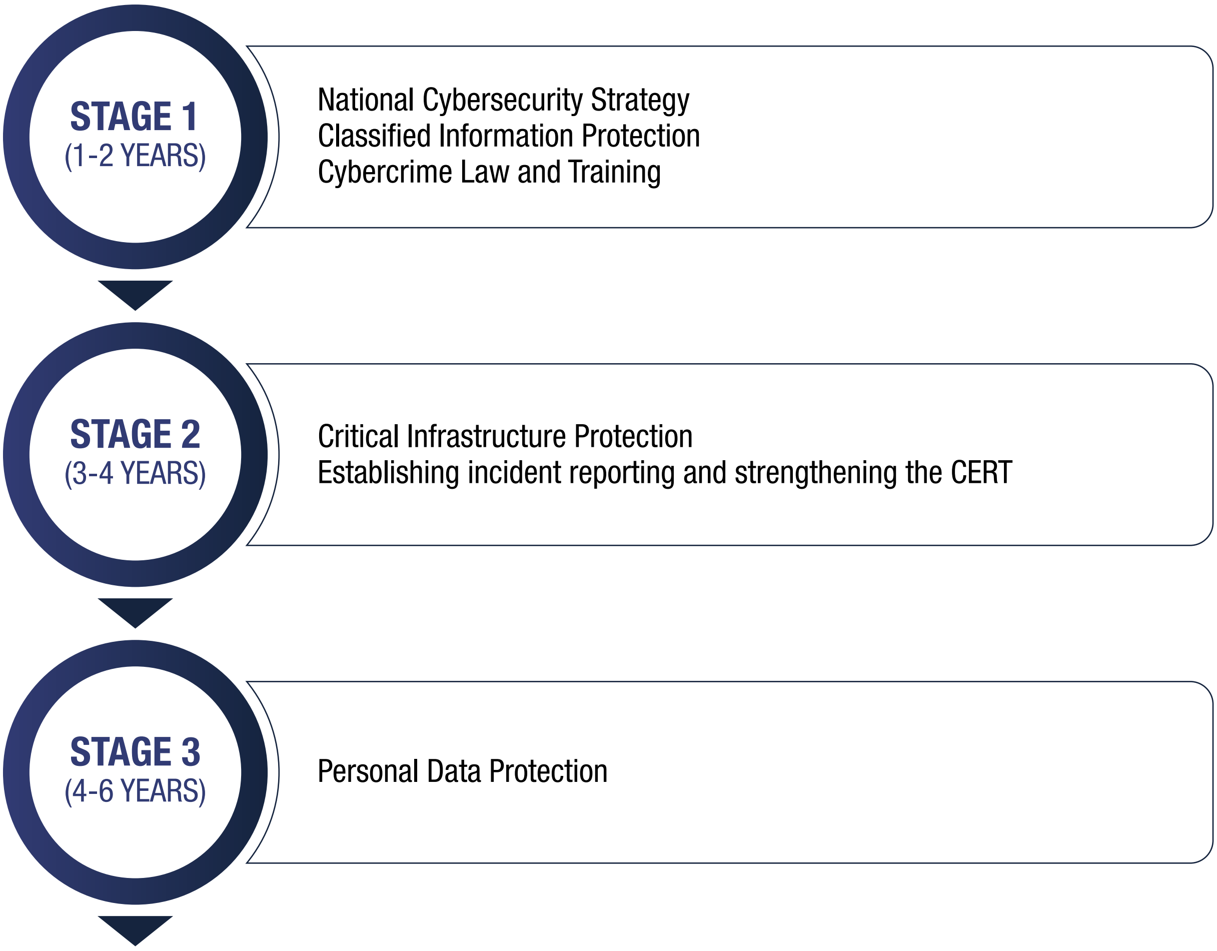
Stage 2 will focus on further developing critical infrastructure protection, establishing incident reporting and strengthening the national Computer Emergency Response Team (CERT). The FSM should, based on the National Cybersecurity Strategy, further develop strategies on critical infrastructure protection. These will include, but not be limited to, identifying organisations and assets that are considered to be critical to the FSM, and measures to protect them. Creation of an information security management and incident reporting process should also be prioritised to enable cybersecurity incident reporting to the national CERT. Finally, the FSM should provide resources to strengthen the national CERT. These strategies and processes should be adopted between 2-4 years after the Roadmap is launched.

Stage 3 will focus on personal data protection. Personal data protection is critical for effective digital transformation. However, without the capacity built in the previous stages of the Roadmap, a personal data protection legal and regulatory framework will be ineffective. Therefore, it has been sequenced to occur in Stage 3. The FSM should develop personal data protection related laws within 4-6 years after the Roadmap is launched.

The Roadmap focuses on cybercrime and cybersecurity related laws and policies. It does not include e-government development or e-commerce. Though the developments of e-government and e-commerce are highly connected and dependent on cybersecurity, it is suggested that the FSM should develop the laws and policies of e-government and e-commerce separately. This is to make sure that there is a clear demarcation between cybersecurity and cybercrime related laws and e-government and e-commerce laws, ensuring that there is no delay in passing them.

To achieve sustainable change from within the FSM and provide protection to the country's critical functions and most vulnerable citizens, this Roadmap must be led and implemented by a senior government official who has sufficient authority, budget and resources.

Figure 1 below provides a high-level overview of the different stages of the roadmap, the expected duration and the key priorities for each stage.



STAGE 1 (1-2 YEARS)

National Cybersecurity Strategy
Classified Information Protection
Cybercrime Law and Training

STAGE 2 (3-4 YEARS)

Critical Infrastructure Protection
Establishing incident reporting and strengthening the CERT

STAGE 3 (4-6 YEARS)

Personal Data Protection

Figure 1: Summary of the Cybersecurity Roadmap for the FSM

This Roadmap is authored by Dr Lennon Chang, Dr James Boorman and Professor Jonathan Clough from Monash University and OCSC, based on their research. We thank Ms Luna Lourdes for her assistance in data collection.

Introduction

The Cybersecurity Roadmap of the Federated States of Micronesia (FSM) is intended as a guide to inform the FSM Government of the priorities for the development of a national cybersecurity strategy, supporting policies, laws and regulations.

In January 2020, in collaboration with the Asia-Pacific Telecommunity (APT), the not-for-profit Oceania Cyber Security Centre (OCSC) undertook a Cybersecurity Capacity Maturity Model for Nations (CMM) review of the FSM. The review was part of APT's work program 'APT Expert Mission'[1] at the invitation of the Department of Transportation, Communications and Infrastructure (TC&I), National Government of the FSM. The objective of the review was to enable the FSM to gain an understanding of its current cybersecurity capacity, identify priorities for the development of a national cybersecurity strategy and activities to strengthen capacity and resilience. Following the CMM review, the Government of the FSM requested support via APT Expert Mission in 2021 to develop a 'Roadmap on Cybersecurity and Cybercrime in FSM'. The OCSC was chosen as the appropriate expert organisation to work with the FSM to co-develop the Roadmap. The CMM considers that cybersecurity includes areas related to cyber capacity building: governance, policy, strategy, culture and society, education and training, regulation and legislation, standards and technical controls. To this end, regulation and legislation includes both substantive and procedural laws necessary for a more secure and safer digital environment.

It is essential to note that no model provides a specific sequence for the development of laws that a country should follow, as this depends on the particular circumstances and priorities of the Government.[2] However, OCSC considers a National Cybersecurity Strategy (NCS) as the national plan that outlines how a nation will address both cybersecurity and cybercrime risk. The NCS should therefore include cybercrime and related cyber-laws, as well as basic principles for protecting critical infrastructure and vulnerable users, especially children.

To that end, OCSC has worked with the FSM to create a Roadmap that consists of 3 stages. The Roadmap is based on the steps taken by countries further along the cybersecurity maturity journey, as well as the first steps of other countries who are also working to strengthen their cybersecurity capacity.

Considering the efforts that the FSM has already taken in terms of Cybersecurity[3] and suggestions from local stakeholders, it is recommended the proposed Roadmap be followed over six years. The Roadmap will provide the FSM with a solid base to build capacity for the next steps of the cybersecurity maturity journey.

Overall, the Roadmap will allow the FSM to: i) design a NCS that fulfils the FSM's particular needs; ii) refine the FSM's governance structure for cybersecurity to support the development of a safer and more secure digital environment for all FSM citizens; iii) progressively develop the legal and regulatory framework; and, iv) embed awareness and education within the community and officials to effectively and sustainably address cyber-related issues into the future.

[1] APT Expert Mission aims to provide expert's assistance to address specific needs of APT Members in order to build capacity in ICT development in the region.<www.apt.int/APTHRD>

[2] According to the International Telecommunication Union (ITU) "National Cybersecurity strategies can take many forms and can go into varying levels of detail, depending on the particular country´s objectives and levels of cyber-readiness" International Telecommunication Union (ITU) et al, 'Guide to Developing a National Cybersecurity Strategy. Strategic Engagement in Cybersecurity' 13 <2021-NCS-Guide>.

[3] In the process of adjusting our proposed roadmap to the FSM's current needs, we became aware of several steps that the FSM has taken in regard to its Cybersecurity strategy; some of them made by the FSM itself and some with the guidance and support of the World Bank.

1. STAGE 1 (1-2 YEARS)

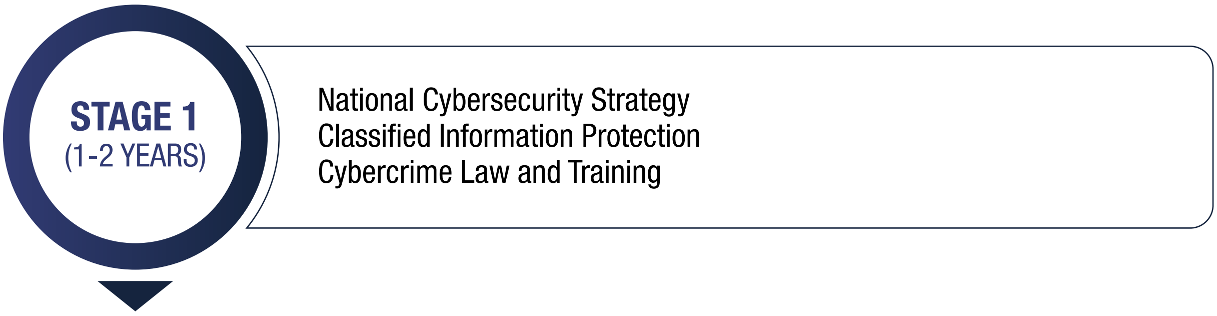

STAGE 1
(1-2 YEARS)
National Cybersecurity Strategy
Classified Information Protection
Cybercrime Law and Training

Figure 2: Stage 1 of the Cybersecurity Roadmap for the FSM

1.1 National Cybersecurity Strategy

A priority recommendation from the CMM review was for the FSM to develop a NCS.[4] Therefore, following the review and in line with good practice guidance, it is strongly recommended that the FSM focus its efforts on creating a NCS as the top priority.

Developing a NCS is a crucial element to sustainably strengthen cybersecurity within the FSM.[5] There are some models and handbooks that the FSM can use as guidance on how to develop the strategy, such as the Global Forum of Cyber Expertise (GFCE) catalogue[6] as well as the guides published by the International Telecommunication Union (ITU[7]) and the European Union Agency for Cybersecurity (ENISA[8]).

In order to simplify the strategy development process, the FSM can develop its NCS in two phases:

- Phase One is related to all the preparatory measures that the FSM should take to guarantee a smooth process.
- Phase Two is related to the actual activities and considerations to create the NCS.

Each phase will now be explained in the following paragraphs.

[4] Oceania Cyber Security Centre (OCSC), ‘National Cybersecurity Capacity Review, Federated States of Micronesia’ (March 2021) 8.

[5] National Centre of Incident Readiness and Strategy for Cybersecurity, ‘History of Governmental Framework of Cybersecurity’ <www.nisc.go.jp/eng/>.

[6] Global Forum on Cyber Expertise (GFCE), ‘Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle’ (2021) <cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/>.

[7] International Telecommunication Union (ITU) et al (n 2).

[8] European Union Agency for Cybersecurity (ENISA), ‘National Cyber Security Strategies Practical Guide on Development and Execution’ (December 2012) <www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>.

1.1.1 Phase One: preparing for NCS development

There are five main priorities for the FSM to complete in Phase One, before proceeding to develop the NCS in Phase Two. These priorities are detailed as follow:

a. Governance

It is vital for the FSM to define clear leadership that oversees and coordinates the development of cybersecurity laws, policies, and practices. This can be achieved either by appointing an existing entity or creating a new one for these purposes.[9]

Based on the documentation provided by the FSM, some progress has been made in this regard. The Unit on Information Technology and Support Services has been established by the Presidential Order released on 22 November 2019, under the Division of Communication in the Department of Transportation Communication & Infrastructure, to oversee critical technical cybersecurity matters.[10] This is an important step towards the consolidation of a governance structure.

However, to reflect the multi-dimensional nature of cybersecurity and its importance to the national security of the FSM, the role of National Cybersecurity Coordinator should be created and assigned to a minister or a higher-level individual. This role should be given responsibility for all dimensions of cybersecurity and developing the NCS and overseeing implementation. This senior leader should be a member of any national security council and report directly to the President. The ITU has created a detailed guide on how to structure this leadership scheme which the FSM could follow.[11]

b. Establishing the FSM CERT

Through the CMM review, the FSM has already assessed its capacity to respond to cybersecurity incidents. In accordance with the CMM review, the strategy should progress the FSM's capacity to respond to cybersecurity incidents by establishing entities or assigning responsibility to existing entities for: i) receiving cybersecurity incident reports and coordinating national incident response (commonly referred to as a national CERT); and ii) identifying and protecting critical infrastructure against cyber threats.

[9] International Telecommunication Union (ITU) et al (n 2) 35.

[10] The functions of this Unit are: "consolidation and centralization of IT support services operation at the National Government; Implementation and enforcement plans to support unified IT policies and procedures for further consideration and action through necessary regulation that would strengthen the ability of the National Government to address its internal IT needs; assessment and evaluation of IT personnel capacity building needs and user training; and, compilation of government services to be incorporated in the e-governance application."

[11] International Telecommunication Union (ITU) et al (n 2) 16–20. See also, the Cambodian experience, which has 2 agencies responsible for its Cyber-Strategy: i) the Ministry of Posts and Telecommunications of Cambodia and ii) NIDA (technical aspects).

There are guides that can assist the FSM with the process of starting up a national CERT[12] and identifying critical infrastructure.[13] As we will discuss the process for identifying critical infrastructure later in section 1.1.1.(c), at this point we will focus on the creation of a national CERT.

There are several advantages to having a national CERT rather than different teams per state. A national CERT can serve as a trusted point of contact, help various organisations within the nation to develop their own incident capabilities, as well as provide coverage of a broad spectrum of sectors within a nation's borders.[14] When the CMM report was drafted, there was no organisation in charge of the national cybersecurity response. Since the new Unit on Information Technology within TC&I has been established, it should take up the role. However, the Unit does not cover all roles that the national CERT should oversee. For example: the unit does not currently gather relevant information across the FSM for detecting, responding, and recovering from different cybersecurity incidents; nor does the unit have clear procedures and policies to share information and intelligence with other entities within the FSM. It is therefore recommended that the FSM provide additional annual budget, training, and sufficient resources (people and tools) for the IT Unit to provide such functions.

Regardless of the path adopted, we strongly recommend the FSM to create a national CERT in this NCS development Phase One. However, the services offered by the national CERT in this initial phase do not have to be complete or comprehensive. The important step is to create the national CERT, as time and resources allow, so that additional services can be added as required.

[12] Netherlands Organisation for Applied Scientific Research (TNO), 'Getting Started with a National CSIRT' <cybilportal.org/tools/getting-started-with-a-national-csirt-guide>; Global Forum on Cyber Expertise (GFCE), 'Global CSIRT Maturity Framework' (April 2021) <cybilportal.org/tools/global-csirt-maturity-framework>; Netherlands Organisation for Applied Scientific Research (TNO); Commonwealth & Development Office et al, 'Commonwealth NCSIRT Capacity Building Programme: Self-Help Guide' <www.gov.uk/government/publications/commonwealth-ncsirt-capacity-building-programme-self-help-guide>; Organisation of American States (OAS), 'Best Practices for Establishing a National CSIRT by the Organisation of American States (OAS)' <cybilportal.org/tools/best-practices-for-establishing-a-national-csirt-by-the-organisation-of-american-states-oas>.

[13] European Union Agency for Cybersecurity (ENISA), 'Methodologies for the Identification of Critical Information Infrastructure Assets and Services' (2015) <www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis>.

[14] Carnegie Mellon Software Engineering Institute, 'Steps for Creating National CSIRTs' (August 2004) <resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf>; Global Forum on Cyber Expertise (GFCE) (n 6).

The following process, based on the Carnegie Mellon Software Engineering Institute report,[15] can assist the FSM with developing the national CERT:

Process	Activities
Education and information gathering (ongoing) This first step focuses on the key stakeholders and makes them fully aware of what a CERT implies, its relevance, and its challenges.	The following activities are essential:[16] • Understand the business drivers and motivations to create a national Computer Emergency Response Team. • Understand what is needed to develop a national team (staff, regulatory and legal requirements, funding, among others). Finally, create a plan to obtain each of them (e.g. determine funding strategies and which one will be used). • Identify the relevant actors to develop the national team, such as government agencies, critical infrastructure representatives, military organisations, among others. • Identify critical resources and critical infrastructure within the FSM. See 1.1.1(c) section for further considerations in this regard. • Identify the types of communication channels. • Identify international best practices for developing a CERT. • Discuss basic response plans across a variety of sectors within the FSM.
Planning (0-5 months) This second step identifies the decisions necessary to plan the national CERT, such as identifying its constituency, the services it will provide (and how they will expand), the budget, and personnel needed to create and operate it within a reasonable timeline.	The activities the FSM should take are the following:[17] • Outline the requirements for the national CERT to respond to the current situation in the FSM based on the information gathered in the previous step. • Develop a vision and objectives for the national CERT. • Identify the correct senior level government official with delegation to approve, lead and sponsor the establishment of an ongoing national CERT. • Identify the responsibilities and roles that the national CERT staff will need, including what skills (technical and non-technical)[18] are required. • Set a consistent terminology and criteria to identify incident activity and threats. • Set incident handling guidelines, reporting requirements, and outline how the CERT will interact with other external partners.

[15] Carnegie Mellon Software Engineering Institute (n 14) 9.

[16] Ibid 10.

[17] Ibid 11–12.

[18] Carnegie Mellon Software Engineering Institute (n 14) 22.

Process	Activities
	• Determine integration with existing disaster recovery, incident response plans, business continuity plans, crisis management or other emergency management plans. • Determine methods for building trusted relationships and collaboration agreements with other key resources and critical infrastructures. • Design communication and coordination processes for disseminating threat and vulnerability intelligence, receiving incident reports and coordinating response to incidents. A relevant experience that the FSM may consider is the suggestion made by Kiribati to create their national CERT.[19] This country strengthened its cyber-maturity by creating a 'CERT Kiribati' supervised by the Ministry of Information and Communications, Transport and Tourism Development. The process analysed how business and Government were affected by cybersecurity incidents and cybercrime. Further, it had to identify the local point of contact to facilitate the gathering of information. Other relevant experiences may be from Papua New Guinea[20] and Vanuatu.[21]
Implementation (9 -15 months) Based on the gathered information from step 1 and the plan designed during step 2, the FSM team should implement the CERT.	As part of this step, the following activities are required:[22] • Secure funding. • Announce the creation of the national CERT within the FSM community. • Coordinate between stakeholders and the national CERT (establishing the point of contact between them, defining policies, procedures, and standards for the protection of information exchanged, among others). • Implementing secure information systems and network infrastructures to operate the national CERT. • Set operational policies and procedures for the national CERT staff. • Identify and hire personnel with the appropriate training and education and providing adequate training for staff.

[19] Ministry of Information Communication Transport & Tourism Development, 'Kiribati National Cybersecurity Strategy 2020' (March 2021) 5 <www.micttd.gov.ki/download/file/fid/300>.

[20] 'The Papua New Guinea Computer Emergency Response Team' <www.pngcert.org.pg>.

[21] The Office of the Government Chief Information Officer (OGCIO), 'Vanuatu National Cyber Security Strategy' <cert.gov.vu/index.php/resources/policies-and-strategies>.

[22] Carnegie Mellon Software Engineering Institute (n 14) 14.

Process	Activities
Operation (ongoing)	At the start, the national CERT will have an essential incident management capability whose primary purpose will be receiving incident reports and coordinating responses to them. This stage will take place once the framework detailed in the planning phase has been established. During this phase it is vital that the FSM continue training its existing and new staff, as well as developing and enhancing its policies and procedures to become a fully operational national CERT in the long term. Further, the national CERT should be independently assessed annually to determine which aspects should be improved, and priority given to making the required amendments.
Collaboration (ongoing)	A key concept for the maturity of the national CERT is enhancing and developing trusted relationships with key stakeholders, partners, and other CERTs.[23]

Apart from the Carnegie Mellon Software Engineering Institute report, the following guidelines may also be helpful at the time to develop the CERT: ENISA's 'Good Practice Guide for Incident Management'[24] and 'CSIRT Setting up guide'[25] as well as the 'CSIRT Services framework' by FIRST[26] and the Netherlands Organisation for Applied Scientific Research (TNO) 'Getting started with a National CSIRT guide'.[27]

c. Defining critical infrastructure and the process for identification

It is important to address the need to protect critical infrastructure in the NCS. The FSM has two different definitions of critical infrastructure. The first is in The FSM National Disaster Response Plan 2016 and refers to sectors. The second is in the draft Cybercrime Bill and refers to "electronic systems, devices, networks, computer programs, electronic data so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters".

The CMM review reported that no stakeholders were aware that their organisations were critical. Therefore, the NCS should include an agreed definition of critical infrastructure that includes all essential services and functions that the country and its people rely on. Once defined, the FSM should raise awareness of this definition with all relevant stakeholders. This will help to inform the identification of critical infrastructure owners and assets.

[23] Forum of Incident Response and Security Team (FIRST), 'FIRST Members around the World'.

[24] European Union Agency for Cybersecurity (ENISA), 'Good Practice Guide for Incident Management' <www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>.

[25] European Union Agency for Cybersecurity (ENISA), 'CSIRT Setting up Guide' (2006) <www.enisa.europa.eu/publications/csirt-setting-up-guide>.

[26] FIRST, 'Computer Security Incident Response Team (CSIRT) Services Framework' <www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1>.

[27] Netherlands Organisation for Applied Scientific Research (TNO) (n 12).

The critical infrastructure identification process takes considerable time and effort. It is suggested that the process is developed and agreed to in Stage 1 of the Roadmap and continued through to implementation in Stage 2 of the Roadmap. The FSM may follow the ENISA – Methodologies when developing and agreeing the process to identify critical Infrastructure assets and services.[28] A relevant criterion that the FSM may follow is one based on sectors. ENISA provides a list of 11 critical sectors that the FSM may consider during its analysis[29] and determine which ones are relevant to the FSM (e.g. Chemical, Commercial Facilities, Communication Sector, among others). This approach is adopted by the United States, as well as[30] Japan[31] Kiribati[32] and Vanuatu.[33]

d. Risk Management

A priority recommendation from the CMM review was to conduct a national risk assessment. This fourth group of activities aims to: i) undertake a national risk assessment, and ii) validate that analysis and the FSM's capacity to address the identified risks. Identifying, quantifying, and managing the cyber-threats the FSM currently faces regarding the national risk assessment is crucial for the FSM's cyber maturity.

Some of the current threats that the FSM faces have been identified in the CMM review.[34] Nonetheless, a regular (at least annual) update on the analysis of threats would allow identification of the trend of threats facing the FSM, set the priorities that should be included in the strategy, and adjust or reinforce the strategy's objectives.[35]

Further details of actions to be undertaken by the FSM to identify threats and manage risk are detailed as follows:

- The regular (annual) update of the national risk assessment should include a list of the assets that may be affected, known weaknesses, dependencies, and different risk scenarios, following Information Security Management – ISMS criteria.[36] A tool that the FSM may use to update its analysis is the joint report released by Cybersecurity agencies from the United States, United Kingdom and Australia[37] which summarises the routinely exploited vulnerabilities based on data from 2020 and 2021. This report possesses technical recommendations to detect and mitigate those exposures. For further reference, see also the ENISA guideline.[38]
- Establish a process for the collection and sharing of cyber threat intelligence. This will enable the FSM to collect data to respond more effectively to cyber threats. The FSM should consider joining regional CERT networks such as APCERT and PaCSON to obtain threat and vulnerability information and alerts. Additional threat feeds may be obtained from commercial suppliers or by exploring what threat and vulnerability information can be shared by allies.

[28] European Union Agency for Cybersecurity (ENISA), Methodologies for the Identification of Critical Information Infrastructure Assets and Services (n 13).

[29] Ibid 4–5.

[30] Cybersecurity & Infrastructure Security Agency, 'Critical Infrastructure Sectors' <www.cisa.gov/critical-infrastructure-sectors>; National Institute of Standards and Technology (NIST), 'Critical Infrastructure Resources' <www.nist.gov/cyberframework/critical-infrastructure-resources>.

[31] 'Cybersecurity Strategy -Japan Provisional Translation' (2018) 24 <www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf>.

[32] Ministry of Information Communication Transport & Tourism Development, 'Kiribati National Cybersecurity Strategy 2020' (March 2021) <www.micttd.gov.ki/download/file/fid/300>.

[33] The Office of the Government Chief Information Officer (OGCIO), 'Vanuatu National Cyber Security Strategy' <cert.gov.vu/index.php/resources/policies-and-strategies>.

[34] Oceania Cyber Security Centre (OCSC) (n 4) 40.

[35] ENISA (n 8) 8.

[36] European Union Agency for Cybersecurity (ENISA), 'ISMS Framework' <www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework>.

[37] Cybersecurity & Infrastructure Security Agency, 'Alert (AA21-209A)' (July 2021).

[38] ENISA (n 8) 10.

- Gather information on trends regarding near misses and reported incidents within the FSM and across partners.
- Seek advice from local and international partners on protecting critical national infrastructure and critical information infrastructure.

Finally, regarding specific threats that the FSM is exposed to, protecting children continues to be a national priority for the FSM, as demonstrated both by the revival of the President's National Advisory Council for Children[39] and as a priority in the CMM review. Therefore, it is important for the FSM government to address this issue in the strategy. A good starting point to address this issue, in accordance with a priority recommendation from the CMM report, is for the FSM to establish an entity, or assign responsibility to an existing entity, for establishing an awareness program with resources to inform parents and children of how to stay safe online.

Another relevant consideration that requires an updated assessment is the impact on the FSM of cyber-threats associated with COVID-19.[40] For example, Australia, in its 2020 Cyber strategy, focused on protecting citizens, businesses, and Government against COVID-19 themed scams (for example, to distribute malicious software).[41]

e. Urgent Issues

Based on our discussions before developing the current Roadmap, the FSM expressed concern about the need to adopt prompt measures to strengthen cyber security. In this regard, we consider that the FSM can adopt the following two measures concurrently while developing the NCS.

- The FSM should connect with a network of professionals or organisations in charge of online child protection, such as ECPAT International and UNICEF. Partnering with these organisations does not require a legal framework to operate.
- The FSM should have a national plan on cybersecurity awareness raising. The FSM might be able to learn from Myanmar's experience (Cyber Baykin)[42] and take part in awareness websites (e.g. Get Safe Online).

[39] Embassy of the Federated States of Micronesia, 'President Panuelo Revives the President´s National Advisory Council for Children' (June 2021) <fsmembassy.fm/president-panuelo-revives-the-presidents-national-advisory-council-for-children/>.

[40] Council of Europe, 'Cybercrime and COVID-19' <www.coe.int/en/web/cybercrime/cybercrime-and-covid-19>.

[41] Commonwealth of Australia, 'Australia´s Cybersecurity Strategy 2020' 14 <www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.

[42] See Lennon Y.C. Chang and Nicholas Coppel, 'Building cyber security Awareness in a developing country: Lessons from Myanmar', Computers & Security, 97 (2020).

1.1.2 Phase Two: NCS Development

Once the FSM achieves the initial activities described in Phase One, it can proceed to design the National Cybersecurity Strategy and its implementation.

a. Strategy design

There is no single model to define a NCS or its content; however, some of the steps that the FSM should consider include:

i. Set the goals to develop national capabilities[43]

Conducted by the leading authority, a group of key stakeholders[44] (from the public, private sector, and civil society[45]) should work together to define the strategy's objectives, priorities, vision, and scope.[46] This objective should also incorporate the findings of the previous activities (see sections 1.1.1(c) and 1.1.1(d)).

The Vanuatu[47] and Kiribati[48] experience may be helpful for the FSM in defining objectives and priorities because, like the FSM, both are Pacific Island Countries strengthening their cybersecurity capacity. It may also be relevant for the FSM to align its goals to those set by its key partners when setting the objectives. For example, the first Cybersecurity Strategy developed by the United States was mainly focused on protecting critical infrastructure at a Federal and State level.[49]

ii. Define a Governance Framework

Even though the leadership was set within the first step (see section, 1.1.1), it is essential to complement leadership with other entities that will enhance the governance structure and oversee the strategy within the proposed six-year timeframe.[50] To this extent, it is also essential to identify the need to commit sufficient resources and ensure that communication and collaboration is operating effectively between all relevant agencies.[51]

iii. Define and establish a trusted information-sharing mechanism[52]

Create a plan for sharing information regarding Cybersecurity among the essential public, private stakeholders, and owners of critical infrastructure. For further details, see section 2.2 of this Roadmap.

iv. Define and establish security requirements

Create a plan to identify the minimum-security requirements that relevant public, private sectors and owners of critical infrastructure should implement.[53] For further details, see section 2.2 of this Roadmap.

[43] Commonwealth of Australia (n42) 19.

[44] European Union Agency for Cybersecurity (ENISA), National Cyber Security Strategies Practical Guide on Development and Execution (n 8) 13–14.

[45] Following "a public–private partnership (PPP) establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals ENISA." Ibid 27–28.

[46] Several key performance indicators have been recommended by ENISA to evaluate the set objectives. Ibid 31.

[47] The Office of the Government Chief Information Officer (OGCIO) (n 33).

[48] Ministry of Information Communication Transport & Tourism Development (n 18) 4.

[49] 'The National Strategy to Secure Cyberspace' (February 2003) <us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf>.

[50] ENISA (n 8) 12.

[51] International Telecommunication Union (ITU) et al (n 2); International Telecommunication Union (ITU) and American Bar Association (n 17) 38; Homeland Security, 'State Cybersecurity Governance Case Studies' (December 2017) 6 <www.cisa.gov/sites/default/files/publications/Cross_Site_Report_and_Case_Studies_508.pdf>.

[52] ENISA (n 8) 15–16.

[53] See also, International Telecommunication Union (ITU) et al (n 2) 38-39.

v. **Develop national cyber contingency plans**

Based on the risk assessment findings made under NCS Development Phase One (see 1.1.1 (d)), the FSM should include a plan to address identified cyber threats. Among others, a definition of what a crisis is and instructions to follow in that scenario may be necessary.[54]

As mentioned previously, we propose that the responsible entity for coordinating responses to cyber-attacks[55] should be the national CERT. Therefore, it is essential to sufficiently empower national CERT to effectively fulfill this role.[56] In addition, as cybersecurity threats are constantly changing, it is vital to include in the plan an approach that allows the FSM to establish a single and shared understanding of the cyber threat environment.[57]

vi. **Establish a plan to protect critical infrastructure services (CIS) and essential services**[58]

Now that the definition and process for identifying critical organisations and assets has been agreed in NCS development Phase One, the FSM will require a comprehensive plan to protect the services it provides. The guidelines for the critical infrastructure plan should be included within the NCS (see sections 1.1.1(c) and 2.1 for further details).

vii. **Establish an incident reporting mechanism**[59]

As suggested at section 1.1.1(b), it is important for the FSM to have a centralised entity to receive cyber reports (CERT). The CERT should also establish a plan to gather sufficient information to keep adjusting and improving the implementation of the Cyber Security Strategy.

viii. **Raising awareness**[60]

The FSM should set a program of awareness to build the general public's knowledge of the new cybercrime law and how to protect themselves online. The experiences of Vanuatu[61] and Myanmar may be relevant in this regard.

The awareness program should also work with platforms, community leaders and civil society organisations to raise awareness of misinformation and disinformation online, while respecting freedom of expression and other human rights online.

ix. **Strengthen training and educational programs**[62]

The FSM should include a plan to enhance cyber education, both to produce experts and train personnel.

[54] ENISA (n 8) 16–17.

[55] Ministry of Information Communication Transport & Tourism Development (n 32).

[56] ENISA (n 8) 24–25.

[57] International Telecommunication Union (ITU) et al (n 2) 36.

[58] International Telecommunication Union (ITU) et al (n 2) 42–50.

[59] ENISA (n 8) 20.

[60] Ibid 3-11.

[61] The Office of the Government Chief Information Officer (OGCIO) (n 33).

[62] ENISA (n 8) 23..

x. **Enact cybercrime legislation**[63]

The FSM should enact comprehensive legislation addressing substantial and procedural cybercrime laws. The FSM has a draft Cybercrime Bill to be passed by the FSM Congress. While the Cybercrime bill is intended to align with the international standard, i.e. the Budapest Convention, concerns on whether the bill is comprehensive enough, as well as the capacity to enforce these provisions, have been raised. Accordingly, the FSM should revisit these issues and revise and/or complement the Bill with other relevant legislation and support, adjusted to address the FSM's priorities, subject to the comments within section 1.3 of this report.

It is important for the FSM to take into consideration the need to complement its cybercrime legislation with other cyber-related laws regarding issues such as its governance structure, critical infrastructure, and Information Security Law. To that extent, the FSM may consider the Vanuatu experience, which also enacted several cyber-related laws. For instance, an 'ICT-related legal framework',[64] telecommunications related laws,[65] bills regarding e-commerce[66] and e-business,[67] encryption and data protection, and liability of intermediaries. However, we suggest this legislative agenda be done by the FSM in separate pieces of legislation. Experience shows that if several related but distinct topics are addressed in one piece of legislation, it can delay its enactment, preventing the FSM from achieving its cybersecurity goals.

xi. **Engage international cooperation**[68]

In order to strengthen cyber maturity, it is essential for the FSM to develop cooperative arrangements with the international community in order to enhance their capacity to respond to cyber threats. Therefore, we suggest that the FSM obtain the relevant internal approvals and develop a plan to insert itself into this community. Please see section 1.3 of this report for further details.

b. Strategy Implementation

The sections mentioned previously may be implemented progressively according to the FSM priorities and/or the route set in this Roadmap.[69]

[63] Ibid 25.

[64] Republic of Vanuatu, 'National Information and Communication Technology Policy' (December 2013) <ogcio.gov.vu/images/policies/Vanuatu-National-ICT-Policy-EN.pdf>.

[65] See Broadcasting and Television Act, Wireless Telegraph (Ships) Act, Telecommunications Act, Telecommunications and Radiocommunications Regulation Act No. 30.

[66] See Electronic Transactions Act No. 24.

[67] See E-Business Act No. 25 of 2000, amended by the Act No. 17 of 2007.

[68] ENISA (n 8) 26–27.

[69] Finally, it is important to mention that a plan to evaluate the Strategy and adjust it (if necessary) should be also considered.

1.2 Classified Information Protection

Following the priority recommendations from the CMM, it is recommended that the FSM prioritise the identification, classification and protection of its sensitive information. Government information is an asset that should be protected. Information can be discussed in conversations, recorded in hardcopy, or stored, processed and transmitted electronically. We agree with the Australian Government that *"all official information requires an appropriate degree of protection as information (and assets holding information) are subject to both intentional and accidental threats. In addition, related processes, systems, networks and people have inherent vulnerabilities."*[70] Identifying and classifying information will allow the FSM to choose appropriate protection, enable information sharing for both domestic and international cooperation and inform decision making.

The FSM can follow the guidance for classifying information in the Protective Security Policy Framework released by the Australian Government.[71] As part of this assessment process, the FSM may adopt the following two criteria: i) consider the potential damage that the information under analysis may cause to the Government, organisations, or individuals, and ii) set the classification at the lowest reasonable level needed to provide protection. The chosen classification markings should include classifications for information that international partners cannot share.

The main categories of the Australian Government information are the following:

- **Official:** Routine government information related to business, service delivery, commercial activity, and policy development.[72] The 'Official' category can be further subdivided into two sub-categories: Official and Official-sensitive. The collection of this information and the requirements to disclose it should be regulated.[73]
- **Protected:** This type of information can cause damage (e.g. degradation of organisational capability).
- **Secret:** This type of information can cause severe damage (e.g. threatening the internal stability of the FSM).
- **Top secret:** This last type of information can cause exceptionally grave damage such as threats to national security, undermining people's dignity, widespread loss of life, among others.

In the classification scheme presented, the last three categories are the ones that require additional protection. It is recommended that the FSM enact legislation to detail the requirements for protecting the different chosen classifications of information, including information that can be shared with international partners or allies and what must remain secret to the FSM. Other measures may include requirements for screening personnel (government and contactors) prior to granting access to different classifications of information; requirements for physical security to protect information stored, processed, transported, or discussed; and technical controls for electronic communications and information in the digital environment.

[70] Attorney-General´s Department, Australian Government, 'Protective and Classified Information' <www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information>.

[71] Ibid 6–8.

[72] Ibid 10.

[73] See Privacy Act 1988 (Cth).

1.3 Cybercrime Law and Training

Based on the critical threats and the information gathered in Phase One, it may be necessary to enact legislation urgently to address any specific critical threat identified within Stage 1 of the Roadmap but not currently addressed (e.g. online child protection).[74]

Noting the FSM has a draft Cybercrime Bill to be passed by the FSM Congress, the FSM Government should enact this legislation to regulate cybercrime, including both substantive and procedural laws. The Cybercrime Bill is an important first step in this legislative agenda, addressing a range of substantive and procedural issues related to cybercrime.

The OCSC considers it crucial for the FSM to adhere to the Budapest Convention even if the FSM is not a party to the Convention. Alignment with the provisions of the Budapest Convention will enhance its position within the international community and facilitate cooperation with other countries when it comes to any crime involving electronic means. Indeed, two key benefits from adhering to the Convention are: *"the ability to directly request preservation from US providers (or to have US government officials rapidly send preservation requests on their behalf) and the ability to request subscriber information directly from US providers."*[75]

In addition, the Budapest Convention provides minimum standards. The challenges of cybercrime have continued to evolve, and the FSM may consider additional provisions based on the experience of other jurisdictions in responding to these challenges. For example, the FSM may benefit from the experience of Vanuatu in drafting its Cybercrime Bill as part of its Cybersecurity Strategy 2020.[76] Assistance may also be gained by looking to the legislation of countries which have progressed further in their responses to cybercrime. The United Nations Conference on Trade and Development (UNODC) has prepared a document with all the references to every piece of legislation (and draft, when applicable) related to cybercrime.[77] The United Nations Conference on Trade and Development (UNODC), the Council of Europe and Interpol provide extensive materials to assist countries in developing cybercrime laws.

Finally, it is highly important for the FSM to create and put in place some training and awareness programs to build knowledge of the new laws and how citizens can protect themselves online. The Digital Education Action Plan 2021-2027 released by the European Commission may be helpful in this regard[78]. Websites such as Cyber Baykin[79] and Get Safe Online can be useful to raise awareness and provide guidance to vulnerable groups and the general public.[80]

[74] Federated States of Micronesia Environment Data Portal, 'FSM National ICT and Telecommunications Policy 2012' (2021) <fsm-data.sprep.org/dataset/fsm-national-ict-and-telecommunications-policy-2012>.

[75] Cybercrime Convention Committee, 'The Budapest Convention on Cybercrime: Benefits and Impact in Practice' (2020) 22 <rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.

[76] See Bill for the Cybercrime for the Cybercrime Act No. of 2020 released by the Republic of Vanuatu. <parliament.gov.vu/images/Bills/2020/2nd_Ordinary/English/Bill_for_the_Cybercrime_Act_No_of_2020.pdf>

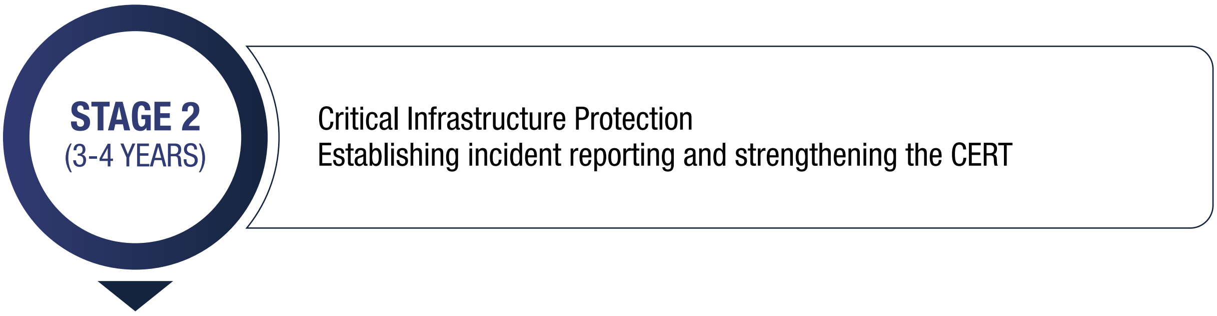
[77] United Nations Conference on Trade and Development (UNCTAD), 'Cybercrime Legislation Worldwide' (2020) <unctad.org/page/cybercrime-legislation-worldwide>.

[78] European Commission, 'Digital Education Action Plan (2021-2027)' <ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en>.

[79] 'Cyber Baykin' <www.cyberbaykin.org/?fbclid=IwAR30wPbGWZ-kYZTcxabQf5vUxM-ZerfK78jXTAUWd-vdu17cq0378XQJRwo>.

[80] 'Get Safe Online Kiribati' <www.getsafeonline.org.ki/>.

2. STAGE 2 (2-4 YEARS)



STAGE 2
(3-4 YEARS)

Critical Infrastructure Protection
Establishing incident reporting and strengthening the CERT

Figure 3: Stage 2 of the Cybersecurity Roadmap for the FSM

2.1 Critical Infrastructure Protection

Following the definition of critical infrastructure and the development of the agreed process for identifying organisations and assets in Stage 1 of the Roadmap, it is now necessary for the FSM to start the process of identification. It is highly important that the analysis made by the FSM in this regard involves effective collaboration between the public and private sector, as the latter usually control many of the critical infrastructure assets.

It is crucial for the FSM to then create a security scheme to protect the identified critical infrastructure.[81] This may include: development and implementation of safety principles, enhancement of information sharing systems, reinforcement of incident response capacity, risk management and preparation of incident readiness.[82]

Finally, it is vital to assign a responsible authority(ies),[83] including contributions from the private sector. Indeed, the critical infrastructure owners and/or operators have a major role in this regard, and responsibility should be assigned to them where appropriate.[84]

[81] National Institute of Standards and Technology (NIST) (n 30).

[82] National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 'Critical Infrastructure' <www.nisc.go.jp/eng/>.

[83] For example, the Japanese government assigned critical infrastructure organisations to 5 different ministries: Financial (FSA), Information and Communication (MIC), Medical, water (MHLW), Electric power supply, gas, chemical, credit card, petroleum (METI), Aviation Airport, Railway, Logistics (MLTI). Ibid.

[84] For example, in this regard Kiribati defined the following: The providers of critical infrastructure are required to take technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems. To coordinate the activities the provider of critical infrastructure shall appoint a member of senior management as Chief Information Security Officer and ensure that it earmarks a specific budget for implementing Cybersecurity measures. Furthermore the provider of critical infrastructure is obliged to carry out a risk and exposure self-assessment at least once a year and document this process. Ministry of Information Communication Transport & Tourism Development (n 32).

2.2 Establishing Incident Reporting and Strengthening the CERT

Now that the FSM CERT has been established in Stage 1 of the Roadmap, there are two additional steps required regarding the FSM CERT. The first is to develop and implement an incident reporting process, supported by a process and policy for the protection of information received and shared with others. The second, is to ensure ongoing strengthening of the CERT in response to the changing threat landscape.

2.2.1 Incident Reporting

The FSM CERT should establish an incident reporting process and specific standards that every relevant agency should comply with when sharing information within the FSM. For instance, a guideline that the FSM might follow is the Information Exchange Policy (IEP 2.0) released by The Forum of Incident Response and Security Team (FIRST).[85] The objective of the regulation within this document is to *"tell (information) recipients how they need to store the information they receive, what they can do with that information, who they can share that information with, and what licensing restrictions there are attached to the information."*[86]

The Traffic Light Protocol,[87] which is also developed by FIRST, is a method the FSM may implement to facilitate labelling its information and identify which one, how, and with whom that information can be redistributed. (e.g. information marked as 'red' should not be disclosed and is restricted to participants only).[88]

Besides identifying the type of information and the rules for its distribution, identifying the participants in this dynamic is highly important. Determining who is the policy authority, the providers, recipients and their roles or responsibilities are crucial.[89] It is also important to decide whether this reporting should be voluntary or compulsory.[90]

Further, the United States (throughout the National Institute of Standards and Technology) also releases[91] standards to provide minimum information security requirements (both functional and assurance[92]) that enhance the operativity of its cybersecurity systems that may be relevant for the FSM to consider. For instance, the ISO/IEC JTC 1/SC 27 is good guidance that the FSM may consider as addresses methods, techniques and guidelines to protect security and privacy aspects.[93]

[85] Forum of Incident Response and Security Team (FIRST), 'Information Exchange Policy 2.0 Framework Definition' (2019) <www.first.org/iep/FIRST_IEP_Framework_v2.0.pdf>.

[86] Ibid.

[87] Forum of Incident Response and Security Team (FIRST), 'Traffic Light Protocol (TPL)' <www.first.org/tlp/>.

[88] Ibid.

[89] Ibid.

[90] see Lennon Y.C. Chang, ´Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait'. Cheltenham, Edward Elgar (2012).

[91] '40 U.S. Code S. 11331' <www.law.cornell.edu/uscode/text/40/11331>.

[92] Karen Scarfone, Dan Beigni and Tim Grance, 'Cyber Security Standards' <tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153>.

[93] DIN, 'ISO/IEC JTC 1/SC 27' 'Information Security, Cybersecurity and Privacy Protection' <www.din.de/en/meta/jtc1sc27>.

2.2.2 Strengthening the CERT

In order to support the protection of critical infrastructure, it will be important for the FSM government to ensure that sufficient budget and resources (people and tools) are allocated for the ongoing operation of the FSM CERT. When determining the budget and resources required, the FSM should consider the vulnerabilities, risks and controls identified during the critical infrastructure identification process, vulnerability and threat intelligence provided by partners, types of incidents reported by constituents and the ability to provide proactive services such as vulnerability scanning and penetration testing. Staff should have dedicated roles to allow them to focus solely on CERT activities and the budget should also include provision for the ongoing professional development of staff, ensuring that skills are kept up-to-date and that staff have sufficient time to engage in the international CERT community.

3. STAGE 3 (4-6 YEARS)

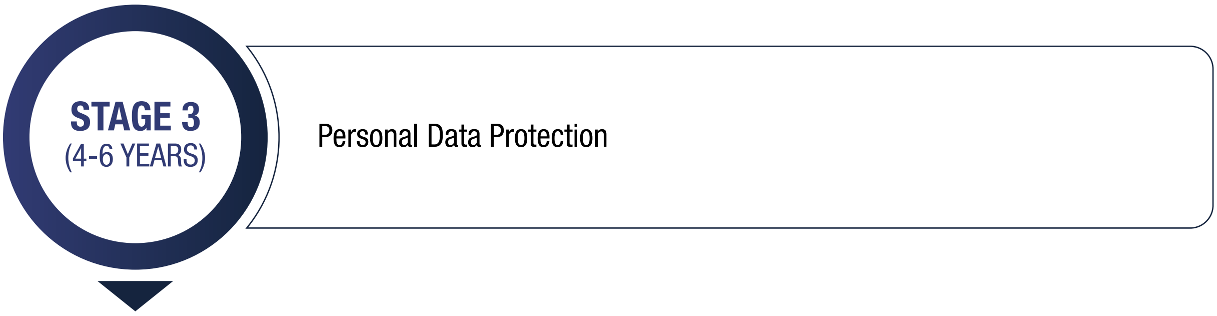

STAGE 3
(4-6 YEARS)
Personal Data Protection

Figure 3: Stage 2 of the Cybersecurity Roadmap for the FSM

3.1 Personal Data Protection

Although the FSM is making substantial progress in developing a Cybercrime Bill, the FSM should consider complementing its effort by enacting a legal framework to protect its citizens' personal data and privacy, contributing to the safe flow of information. This aligns well with the FSM plans to move forward with an E-Government and E-Commerce system.

It is crucial for the FSM to enact a regulatory framework and put in place the technology to i) protect individuals against abuses and violations to their privacy and personal data when storing and processing their data, ii) assure the quality of the stored information, which must be *'adequate, relevant and not excessive'*,[94] and iii) ensure the lawful collection and exchange of information and to prevent its use for unlawful purposes.

A relevant example is the harmonized binding international instrument in the data protection field developed by the European Council.[95] The EU Agency for Fundamental Rights and the Council of Europe released a modernized edition of the Handbook on European Data Protection Law, which provides a comprehensive understanding of aspects related to data protection, which the FSM may consider.[96]

[94] European Union Agency for Fundamental Rights et al, 'Handbook on European Data Protection Law' (2018) 24 <www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>.

[95] Council of Europe, 'Council of Europe Data Protection Website' <www.coe.int/en/web/data-protection/home>.

[96] European Union Agency for Fundamental Rights et al (n 94).

Further, the Council of Europe released some regulations that can guide the FSM. Some of the most relevant are:

- Regulation (EU) 2016/679:[97] We agree that "effective protection of personal data (…) requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data".[98] Therefore, this regulation provides a general and comprehensive framework to ensure the free movement of personal Data within the Union, that the FSM may take into consideration.
- Directive (EU) 2016/680:[99] This document establishes more specific rules related to processing *"of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences"*[100] by competent authorities within the criminal justice sector.
- Regulation (EU) 2018/1725:[101] This document was drafted to guarantee the protection of citizens from the processing of personal data by institutions and bodies. The framework provided is intended to be coherent and align with the Regulation (EU) 2016/679

These documents can provide the FSM with a model regarding the specific rules that need to be enacted to protect personal data. We believe it may also be relevant to set the applicable definitions, principles,[102] and relevant actors to further develop an effective legal framework that responds to the FSM's specific requirements. The United Nations Conference on Trade and Development has prepared a document with all the references to every piece of legislation (and draft, when applicable) related to data protection that the FSM may consult.[103]

4. CONCLUSION

This roadmap has been developed in collaboration with key stakeholders from the FSM following the acceptance of the final CMM review report. The roadmap provides a pathway beyond the CMM recommendations, detailing a national program with specific actions to be taken over the next six years. To achieve sustainable change from within the FSM and provide protection to the country's critical functions and most vulnerable citizens, this program must be led and implemented by a senior government official who has sufficient authority, budget and resources.

[97] Official Journal of the European Union, 'Regulation (EU) 2016/679' (April 2019) <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

[98] Ibid.

[99] Official Journal of the European Union, 'Directive (EU) 2016/680' (April 2016) <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN>.

[100] European Union Agency for Fundamental Rights et al (n 94) 32.

[101] Official Journal of the European Union, 'Regulation (EU) 2018/1725' (October 2018) <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN>.

[102] A relevant example may be the Schedule 1 of the Australian Privacy Act (Privacy Act 1988).

[103] United Nations Conference on Trade and Development (UNCTAD) (n 77).

GOVERNMENT OF THE FEDERATED STATES OF MICRONESIA

PEACE UNITY LIBERTY

OCSC
Oceania Cyber Security Centre

MONASH University

APT