NCSI
national cyber security index

173. Marshall Islands 1.30

Population	**0.1** million	
Area (km²)	**0.2** thousand	
GDP per capita ($)	**0.0** thousand	

173rd National Cyber Security Index |||||||||||||||||| **1 %**
N/A Global Cybersecurity Index |||||||||||||||||| **0 %**
N/A **ICT Development Index** |||||||||||||||||| **0 %**
N/A **Networked Readiness Index** |||||||||||||||||| **0 %**

NCSI DEVELOPMENT TIMELINE

2024 2025 2026

100
80
60
40
20
0

RANKING TIMELINE

2022 2023 2024 2025 2026

1
36
71
106
141
176
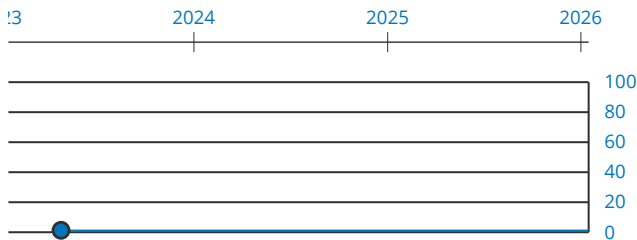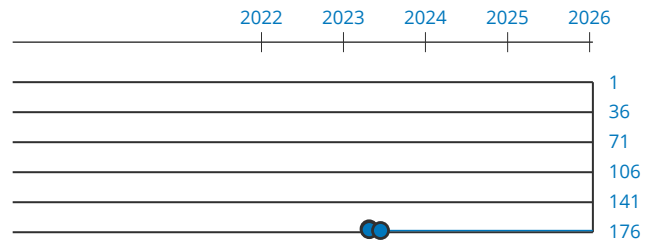
NCSI FULFILMENT PERCENTAGE

100
80
60
40
20
0

Policy Threats Education Global Digital Essential eID & TS Personal CIRC Crisis Police Military
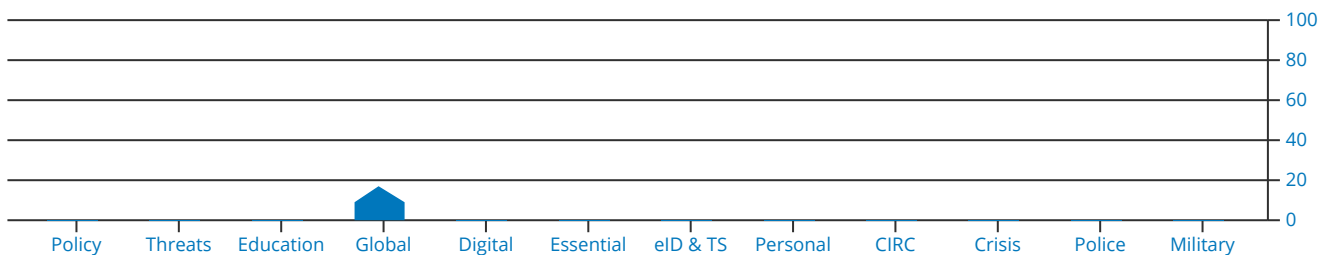
GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development — 0 / 7 **(0%)**

	0 /
1.1. Cyber security policy unit	0 / 3
1.2. Cyber security policy coordination format	0 / 2
1.3. Cyber security strategy	0 / 1
1.4. Cyber security strategy implementation plan	0 / 1

2. Cyber threat analysis and information — 0 / 5 **(0%)**

|	
2.1. Cyber threats analysis unit	0 / 3
2.2. Public cyber threat reports are published annually	0 / 1
2.3. Cyber safety and security website	0 / 1

3. Education and professional development — 0 / 9 **(0%)**

3.1. Cyber safety competencies in primary or secondary education	0 / 1
3.2. Bachelor's level cyber security programme	0 / 2
3.3. Master's level cyber security programme	0 / 2
3.4. PhD level cyber security programme	0 / 2
3.5. Cyber security professional association	0 / 2

4. Contribution to global cyber security — 1 / 6 **(17%)**

4.1. Convention on Cybercrime	0 / 1
4.2. Representation in international cooperation formats	1
4.3. International cyber security organisation hosted by the country	0 / 3
4.4. Cyber security capacity building for other countries	0 / 1
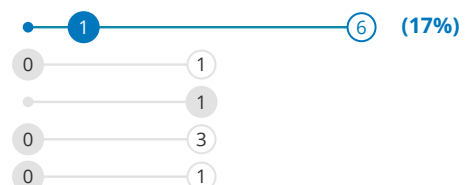
BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services
0 ——————— 5 **(0%)**

5.1. Cyber security responsibility for digital service providers 　0 ——— 1
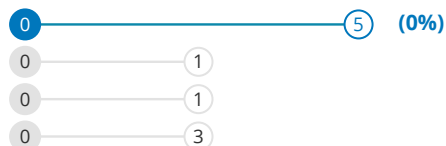
5.2. Cyber security standard for the public sector 　0 ——— 1

5.3. Competent supervisory authority 　0 ——— 3

6. Protection of essential services
0 ——————— 6 **(0%)**

6.1. Operators of essential services are identified 　0 ——— 1
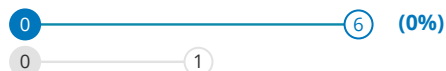
6.2. Cyber security requirements for operators of essential services 　0 ——— 1

6.3. Competent supervisory authority 　0 ——— 3

6.4. Regular monitoring of security measures 　0 ——— 1

7. E-identification and trust services
0 ——————— 9 **(0%)**

7.1. Unique persistent identifier 　0 ——— 1

7.2. Requirements for cryptosystems 　0 ——— 1

7.3. Electronic identification 　0 ——— 1

7.4. Electronic signature 　0 ——— 1

7.5. Timestamping 　0 ——— 1

7.6. Electronic registered delivery service 　0 ——— 1

7.7. Competent supervisory authority 　0 ——— 3

8. Protection of personal data
0 ——————— 4 **(0%)**

8.1. Personal data protection legislation 　0 ——— 1

8.2. Personal data protection authority 　0 ——— 3

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response
0 ——————— 6 **(0%)**

9.1. Cyber incidents response unit 　0 ——— 3
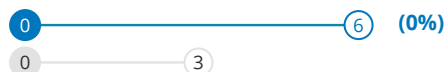
9.2. Reporting responsibility 　0 ——— 1

9.3. Single point of contact for international coordination 　0 ——— 2

10. Cyber crisis management
0 ——————— 5 **(0%)**

10.1. Cyber crisis management plan 　0 ——— 1
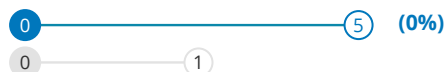
10.2. National-level cyber crisis management exercise 　0 ——— 2

10.3. Participation in international cyber crisis exercises 　0 ——— 1

10.4. Operational support of volunteers in cyber crises 　0 ——— 1

11. Fight against cybercrime
0 ——————— 9 **(0%)**

11.1. Cybercrimes are criminalised 　0 ——— 1

11.2. Cybercrime unit 　0 ——— 3

11.3. Digital forensics unit 　0 ——— 3

11.4. 24/7 contact point for international cybercrime 　0 ——— 2

12. Military cyber operations
0 ——————— 6 **(0%)**

12.1. Cyber operations unit 　0 ——— 3

12.2. Cyber operations exercise 　0 ——— 2

12.3. Participation in international cyber exercises 　0 ——— 1