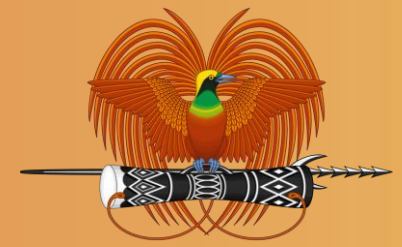
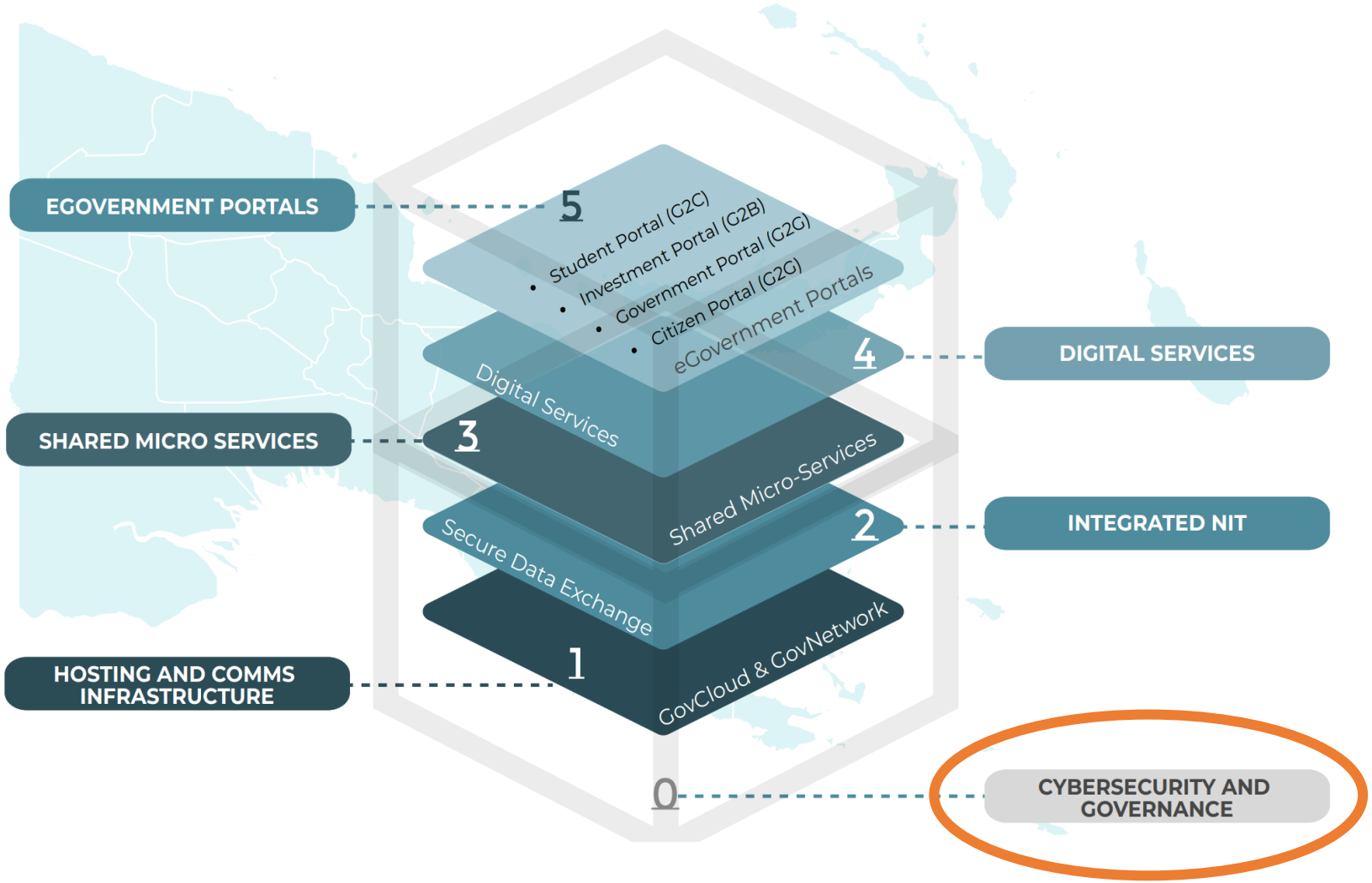
Department of Information And Communications Technology



CYBERSECURITY AND GOVERNANCE

BY GEORGINA KIELE

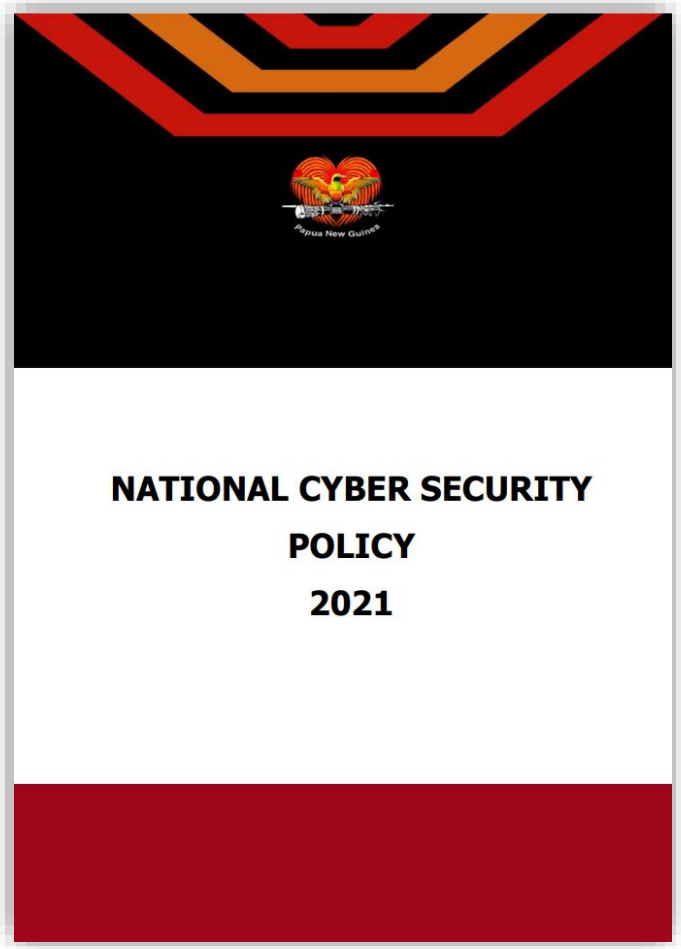
GOV STACK


EGOVERNMENT PORTALS
5
Student Portal (G2C)
Investment Portal (G2B)
Government Portal (G2G)
Citizen Portal (G2G)
eGovernment Portals
4
DIGITAL SERVICES
Digital Services
SHARED MICRO SERVICES
3
Shared Micro-Services
2
INTEGRATED NIT
Secure Data Exchange
1
GovCloud & GovNetwork
HOSTING AND COMMS INFRASTRUCTURE
0
CYBERSECURITY AND GOVERNANCE

National Cybersecurity Policy 2021

The National Cyber Security Policy of **aims to enhance the country's cybersecurity capabilities to protect its institutions, environment, resources, and people**. The policy is organized around several key goals:

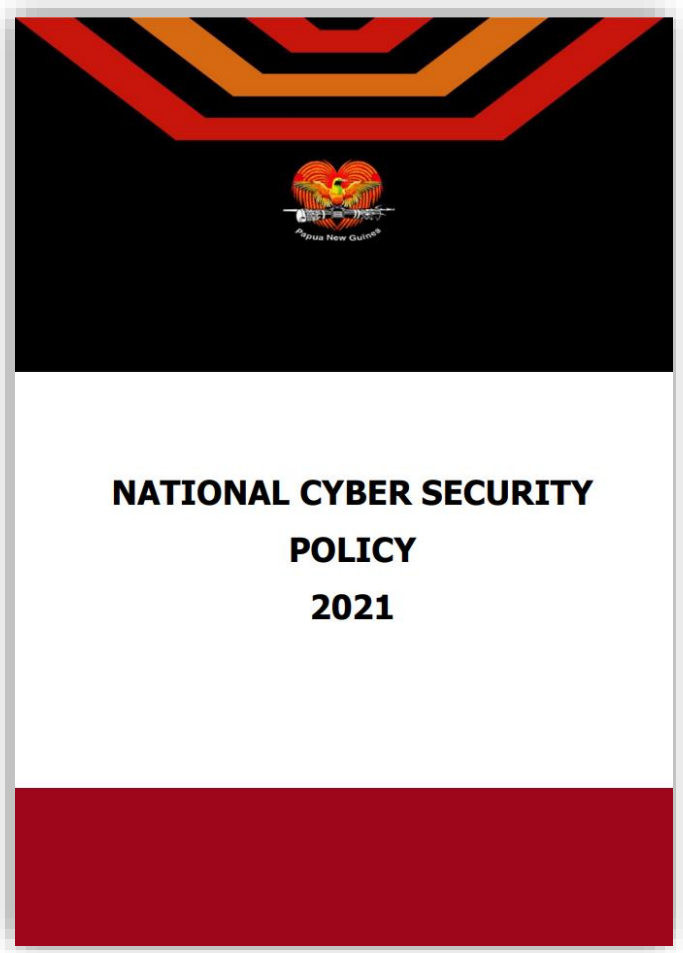
- Establishing a coordination mechanism and specialized institutions for cybersecurity.
- Developing national capability and capacity, improving cyber knowledge and skills, and raising awareness of cyber safety among stakeholders.



National Cybersecurity Policy 2021

The policy involves the development of a **National Cyber Security Strategy** covering the:

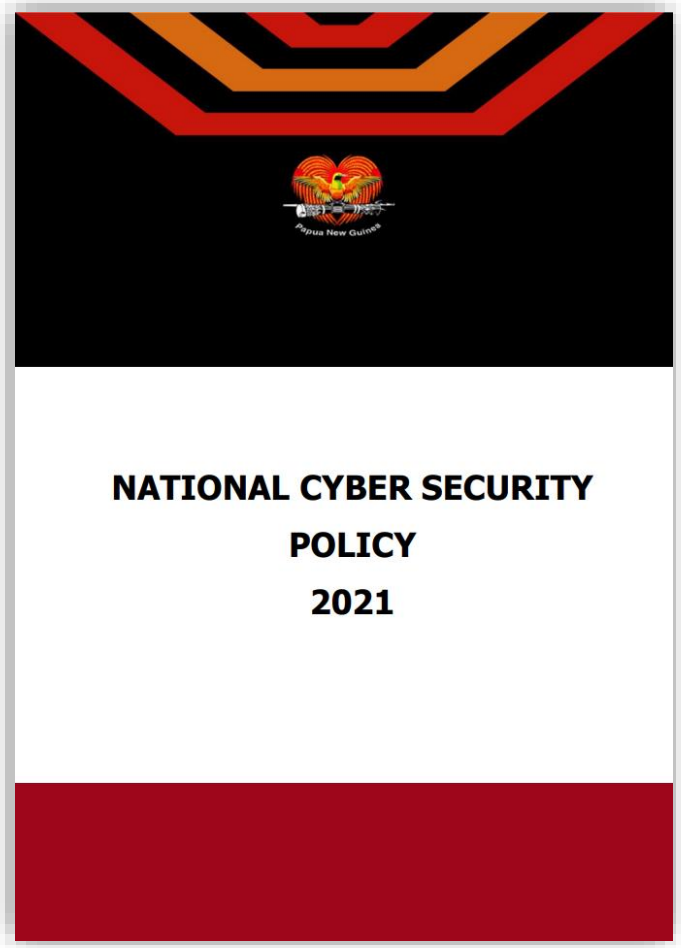
- protection of information systems
- fighting cybercrime
- legal and regulatory framework development
- promoting digital trust
- national and international coordination.



National Cybersecurity Policy 2021

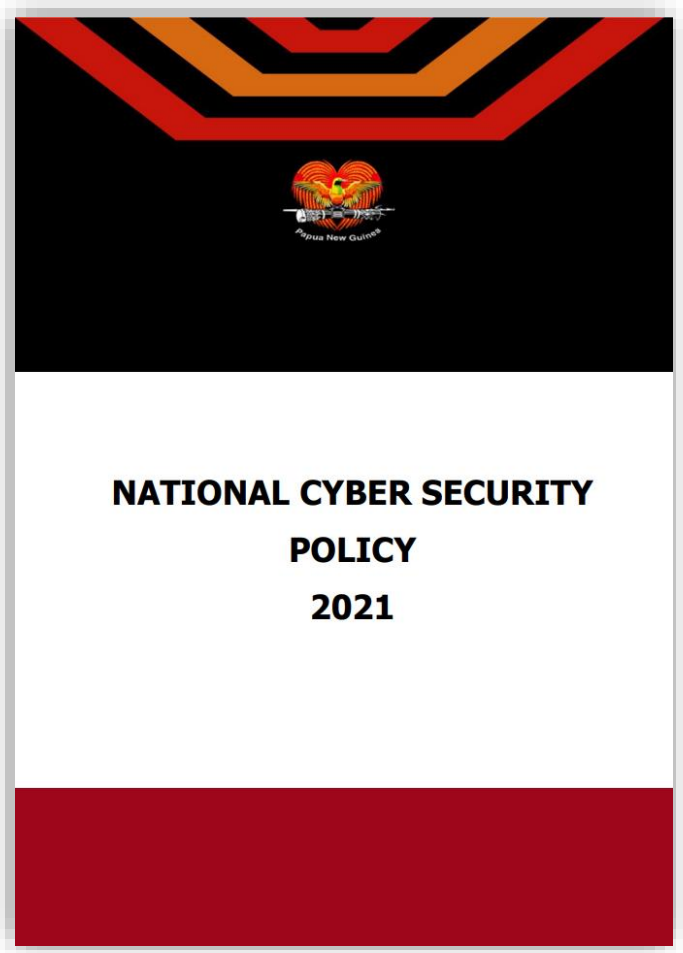
Other key points in the policy include:

- Establishment of a National Cyber Security Agency (NCSA) to coordinate government activities related to cybersecurity.
- Development of a National Cyber Security Legislation to implement the policy's goals.
- Recognition of the vulnerability of cyberspace to physical and cyber threats.
- The need to report cyber incidents, coordinate certification and accreditation of cybersecurity professionals, and improve cybersecurity laws and regulations.
- Protection of critical infrastructure from cyber threats.
- Collaborating with partners to identify and mitigate cyber risks effectively.



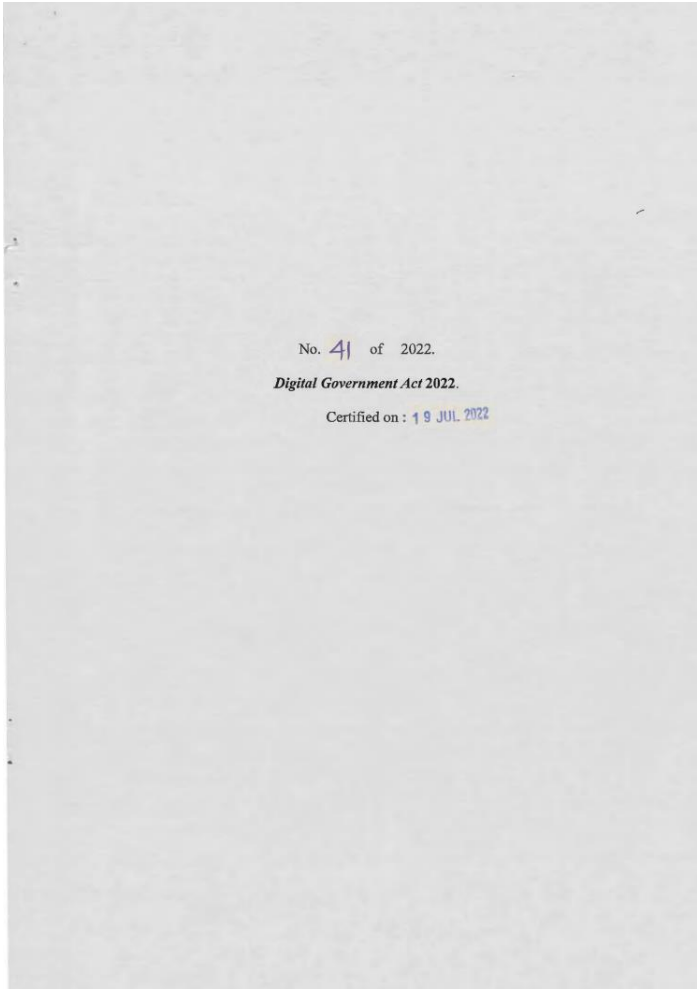
National Cybersecurity Policy 2021

Overall, the policy outlines a comprehensive approach to strengthen Papua New Guinea's cybersecurity posture and protect against a range of cyber threats to both its national security and critical infrastructure. Creating a more cybersecurity Resilient nation.



Digital Government Act 2022

- Section 18
  - The National Cyber Security Center (NCSC) is established
  - NCSC is jointly operated by DICT, Defense, Police, Justice, National Intelligence Organization and PMNEC
- Section 19
  - Functions of NCSC
- Section 21(2)(e)
  - NCSC is declared as a Critical Digital Infrastructure
- Section 55
  - NCSC approve technology cyber safety and security for Public body to an Internet Services Provider


No. 41 of 2022.

Digital Government Act 2022.

Certified on : 19 JUL 2022

CYBERSECURITY IN THE DIGITAL GOVERNMENT PLAN

2023
- National Cyber Security Center is Operational
- Cybersecurity standards establish

2026
- Cyber Resilience Matures
- PNG to be Cybersecurity Leader in the Pacific Region with the index rating with top 30 globally

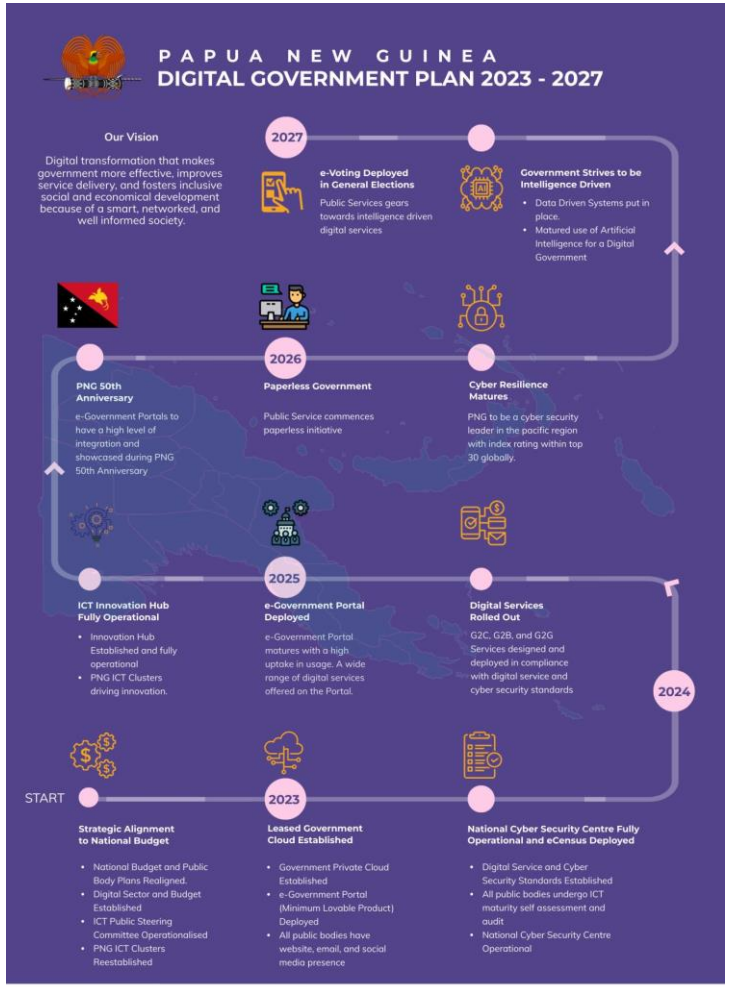


Figure 10: Delivery Timeline of the PNG Digital Government Plan 2023 - 2027

Approved by NEC

Other Frameworks

Digital Government Cyber Security Standards

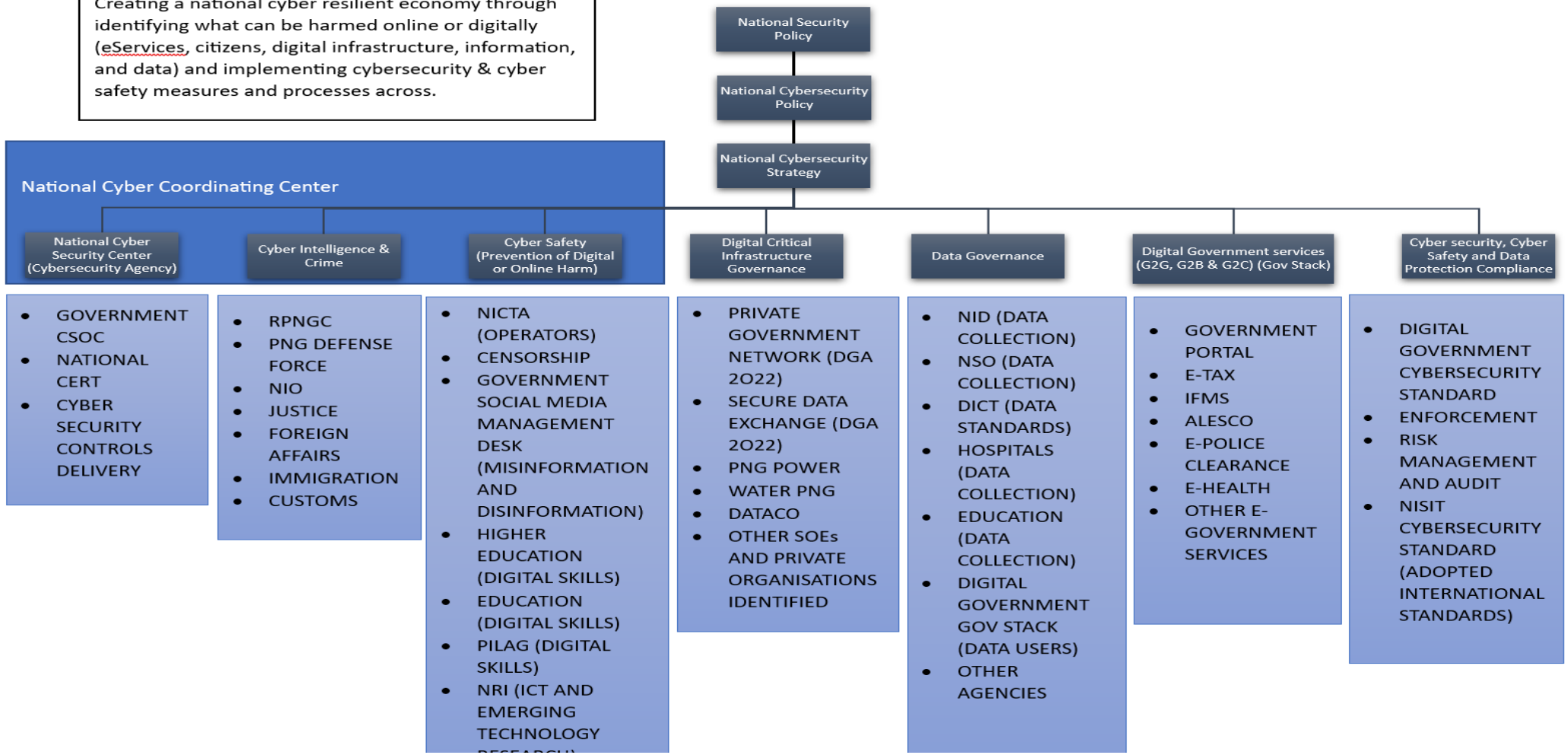
- Implementation of the Digital Government Act 2022 (section 19)

National Cybersecurity Strategy.

- Draft under internal Review
- The six goals are 1. Governance, 2. Risk Management, Preparedness & Resilience, 3. Critical Infrastructure & Essential Services 4. Capability & Capacity Building and Awareness raising 5. Legislation and Regulations 6. international Cooperation

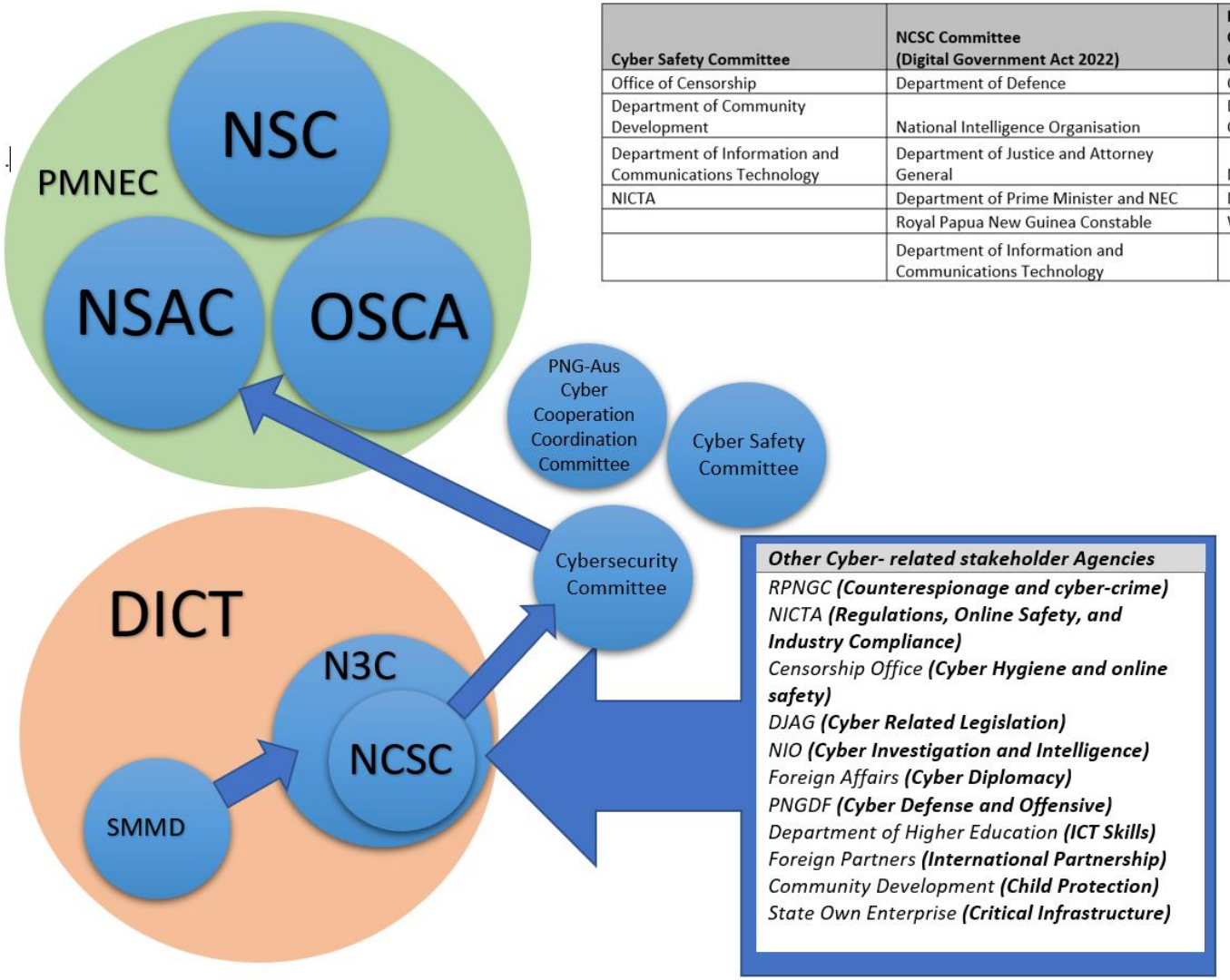
PROTECTING NATIONAL DIGITAL ECONOMY THROUGH NATIONAL CYBERSECURITY STRATEGY

Creating a national cyber resilient economy through identifying what can be harmed online or digitally (eServices, citizens, digital infrastructure, information, and data) and implementing cybersecurity & cyber safety measures and processes across.



NATIONAL CYBER COORDINATING CENTERN (N3C)

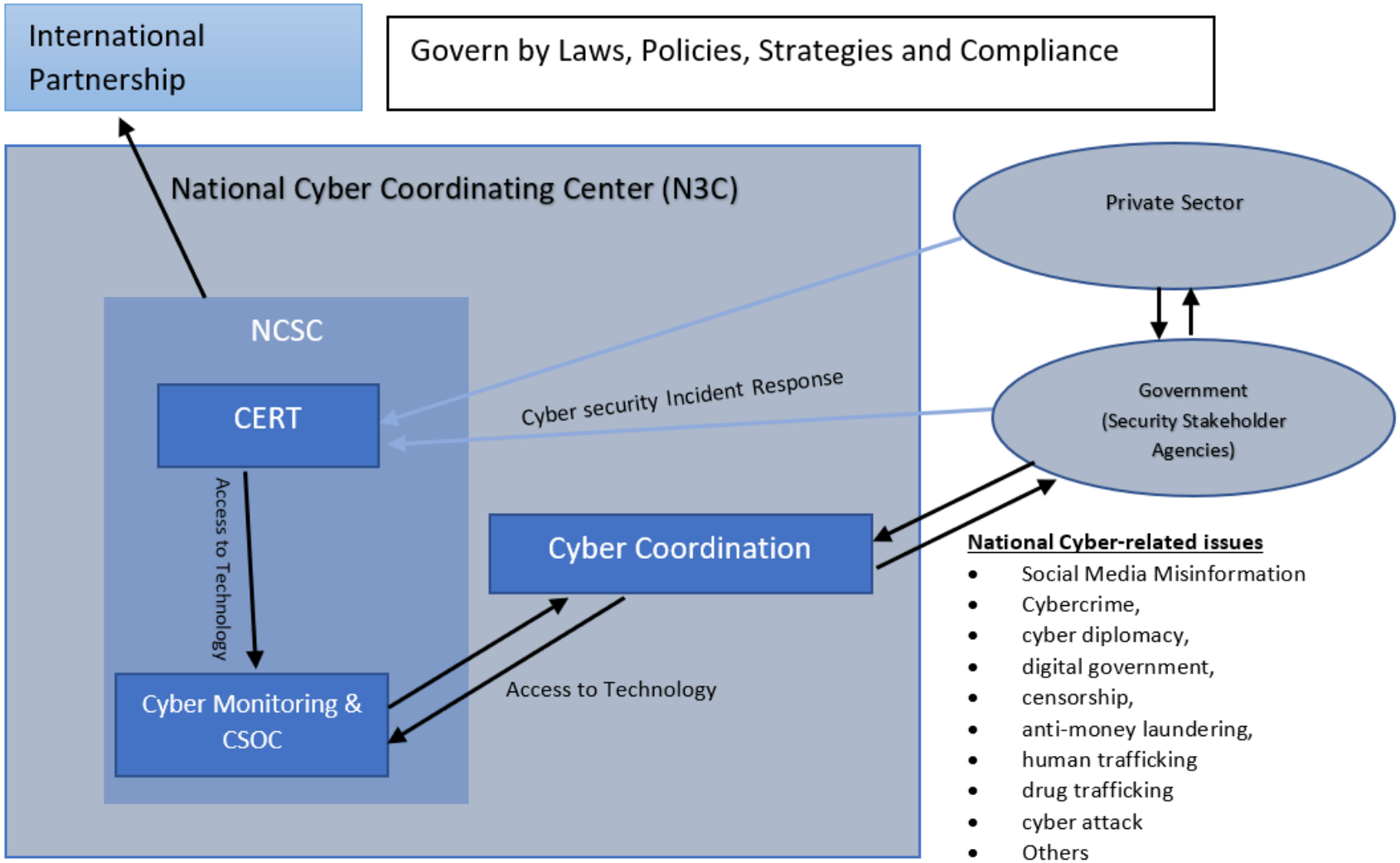
CYBER RESILIENCE FOR GOVERNMENT



Cyber Safety Committee	NCSC Committee (Digital Government Act 2022)	PNG-Australia Cyber Cooperation Coordination Committee (MOU)
Office of Censorship	Department of Defence	OSCA (Chair)
Department of Community Development	National Intelligence Organisation	Department of Information and Communications Technology
Department of Information and Communications Technology	Department of Justice and Attorney General	NICTA
NICTA	Department of Prime Minister and NEC	DFAT Australia
	Royal Papua New Guinea Constable	WYWY (DFAT Contractor)
	Department of Information and Communications Technology	

NATIONAL CYBER COORDINATING CENTERN (N3C)

N3C DESIGN



THE NATIONAL CYBERSECURITY CENTER OPERATION

OPERATIONS UPDATE

www.ict.gov.pg

NATIONAL CYBER SECURITY CENTER OPERATIONS

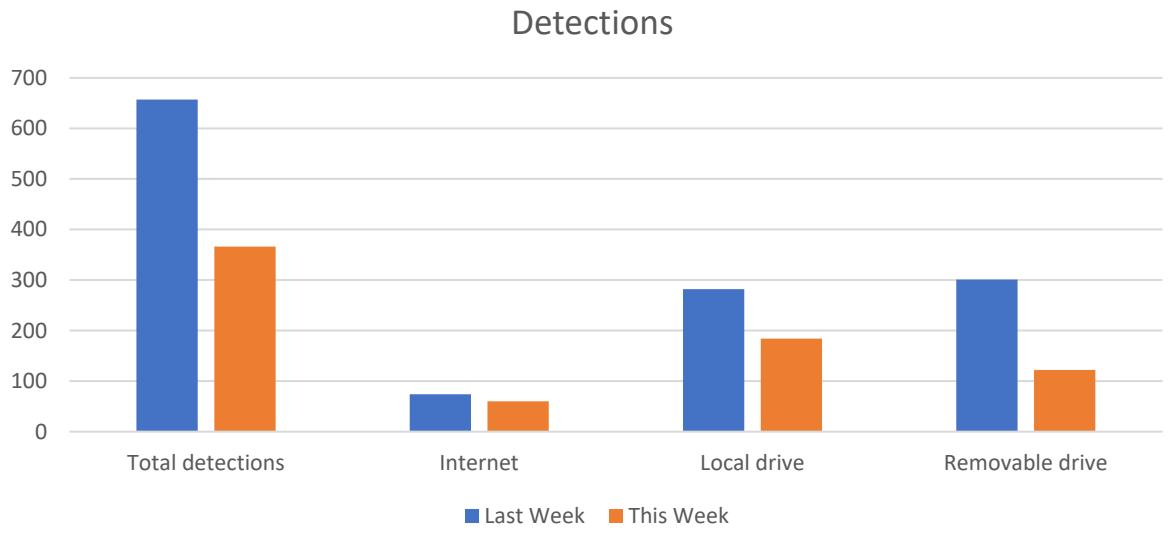
NCSC SERVICES

- Endpoint Protection for PC and Server (Available)
- Network Protection (Available)
- Cloud Security Monitoring (Available)
- Email Protection (coming soon)
- Online Training (Available)
- Cybersecurity Consultation (Available)
- SIEM and MDR (Available)
- Incident Handling Practices (Schedule by NCSC)

NATIONAL CYBER SECURITY CENTER OPERATIONS

ENDPOINT PROTECTION

Statistics shown in Security information and event management (SIEM)



Endpoint Protection:

	Department Name	New Endpoints	Total Endpoints
1	DAL		3
2	DFCDR		1
3	DICT		145
4	DIRD		82
5	DPE		39
6	DPLGA	1	103
7	ICAC	3	47
8	MSHQ		37
9	NCDPHA	4	16
10	NCOBA		24
11	NCSC		27
12	NEFC		3
13	NFA		1
14	NPS		3
15	PMNEC		139
16	PNGCS		1
17	SILAG		131
18	EHP-UBD		1
	*UNKNOWN		61
	Grand Total	**8**	**865**

** Departments are required to use a standard naming convention*

NATIONAL CYBER SECURITY CENTER OPERATIONS

// Threat Details

On July 19, 2023, the MDR team was alerted to 'EQL-WIN-CRD-PRC-NTDSUTIL-CREATE-FULL-1' activity on host [redacted]. After a thorough investigation, we determined that the alert triggered due to execution of command 'ntdsutil.exe "ac i ntds" "ifm" "create full c:\programdata\log" q q' which is a confirmed credential dump of the Active Directory database using the NTDSUTIL utility and saving it directory it to the "C:\ProgramData\Log" directory. Ntdsutil can be used to create an installation media that can then be used to extract credentials from NTDS. Upon reviewing running process, we observed an execution of a bat file 'c:\programdata\1.bat via cmd process having creation time of July 19, 2023 4:46:19 AM UTC. The bat file contains the commands for scheduled task 'DFATCHK ' to backup AD and then auto delete itself. We are continuing to investigate this active incident and will provide an Excel document that includes additional prioritized recommendations and a collection of findings in a subsequent email.
We have completed some additional analysis and have submitted some potentially malicious file samples from the host [redacted]' to our Sophos Labs Team for review. Labs has concluded that the file 'C:\Program Files\Common Files\microsoft shared\ink\DUI70.dll' is malicious, masquerading as a legitimate file, and side-loading malicious code. We noted process activity for the user [redacted]admin' on the host [redacted]server2' which resulted in the legitimate process 'C:\Program Files\Common Files\microsoft shared\ink\ShapeCollector.exe' reaching out to the remote domain 'gw[.]allstaffs[.]net', which appears to be unexpected activity. The initial execution of 'ShapeCollector.exe' was initiated remotely from an unprotected host at address [redacted], which resolves to the hostname [redacted]RINT-ICT'.

// Priority 1 Recommendations

1. Confirm if the activity described in our emails until date is expected.

2. Protect IPs [redacted]-PRINT-ICT').

3. Block the domain gw[.]allstaffs[.]net and remote IP address [redacted] at your network perimeter.

4. Perform domain-wide credential reset on administrator and service accounts, and all other accounts.

5. Reboot hosts [redacted]' and [redacted]gaserver2'.

6. Configure Fortinet Firewall to not be public-facing:

Fortinet:

Device: FortiGate-81F

Model: FGT81F

Serial Number: FGT81FTK21010034

THANKYOU