Ministry of National Unity
National Archives of Malaysia

SARBICA
SOUTHEAST ASIAN REGIONAL BRANCH
BRANCHE RÉGIONALE POUR L'ASIE DU SUD-EST

International Seminar

DIGITAL RECORDS AND LEGAL ADMISSIBILITY 2024

Ir. Dr. Megat Zuhairy bin Megat Tajuddin
National Cyber Security Agency (NACSA)

Cyber Security – Enhancing the National Cyber Security in Malaysia

#IAW2024 #CyberArchives

MALAYSIA MADANI

#myarkibnegara
www.arkib.gov.my

CYBER SECURITY ACT 2024

Enhancing the National Cyber Security in Malaysia

10 June 2024

Ir. Dr. Megat Zuhairy bin Megat Tajuddin
Chief Executive of NACSA

Introduction

Competitiveness

In navigating the challenges posed by the current wave of technological advancement and digital transformation, it becomes imperative for Malaysia to position itself competitively on the global stage.

Technology and Progress

Embracing technology and digitization across all sectors is key to accelerating the nation's progress.

Digital Transformation

Consequently, concerted efforts from governmental bodies and stakeholders are underway to leverage digital tools and platforms, thereby enhancing service delivery and efficiency

COUNTRY DIRECTIONS

CATALYST OF DIGITAL ECONOMY

5G, IoT, AI

By embracing cutting-edge technologies

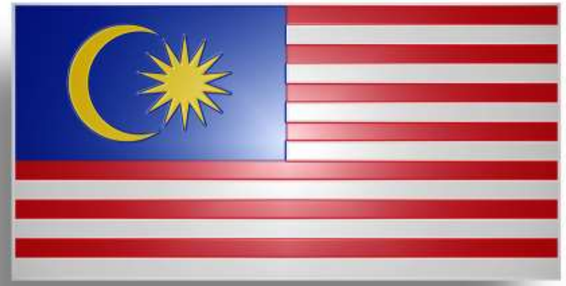
The Malaysian Government has made substantial commitments to ICT as a cornerstone for driving the nation towards a digital economy.

PROJECTIONS OF MALAYSIA'S DIGITAL ECONOMY

25.5%

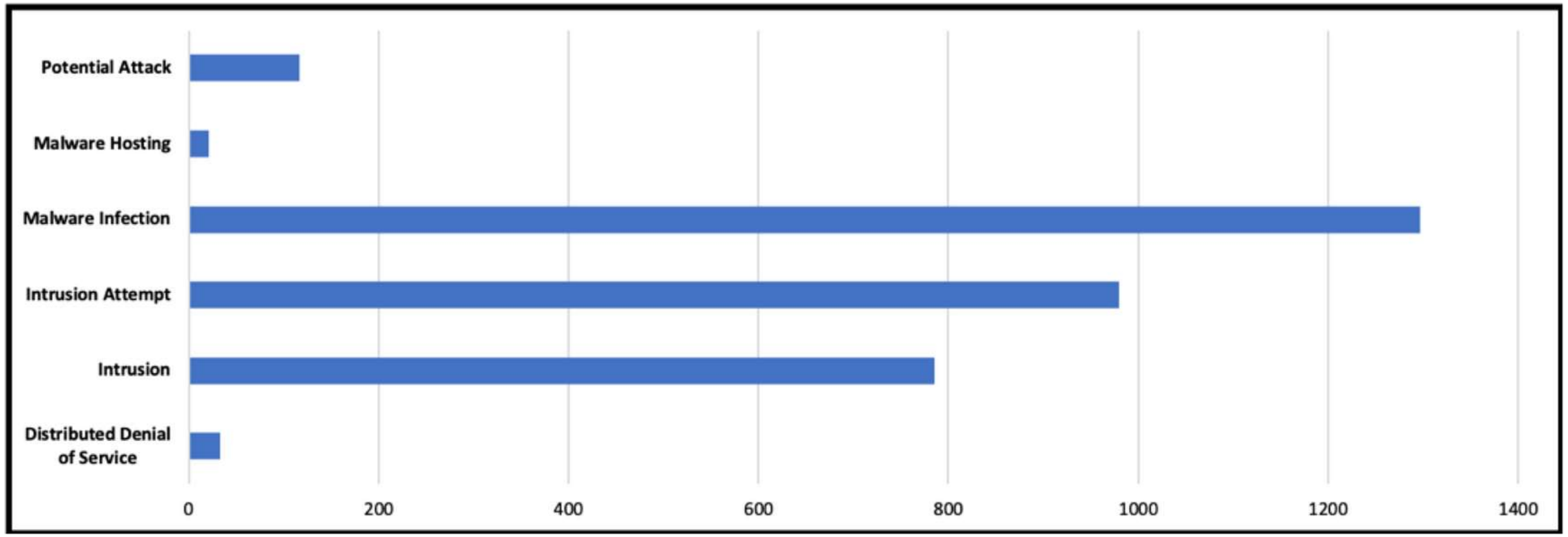
Gross Domestic Product (GDP) by 2025

This underscores the pivotal role played by the digital economy as a primary driver of Malaysia's economic growth and development.

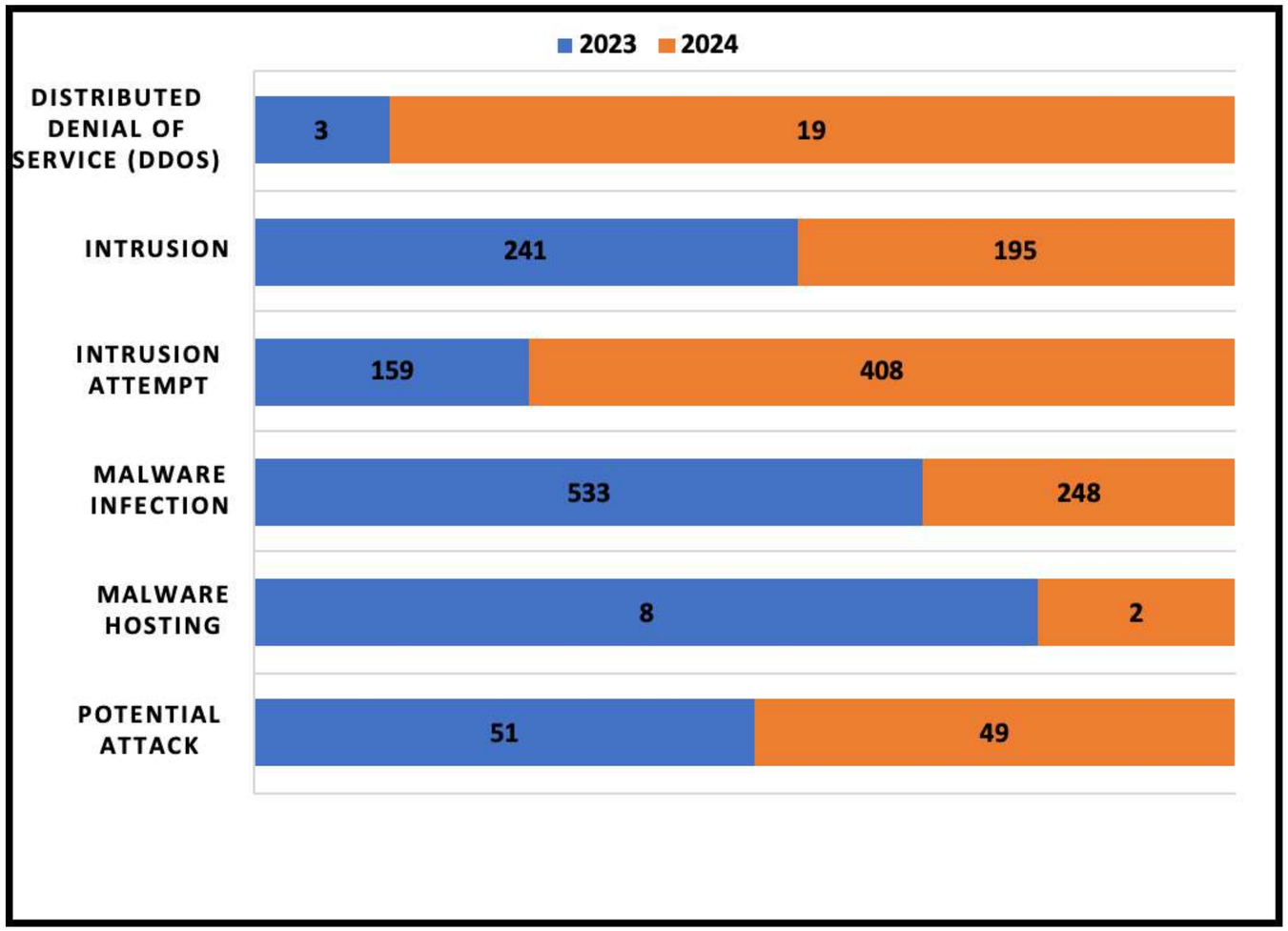


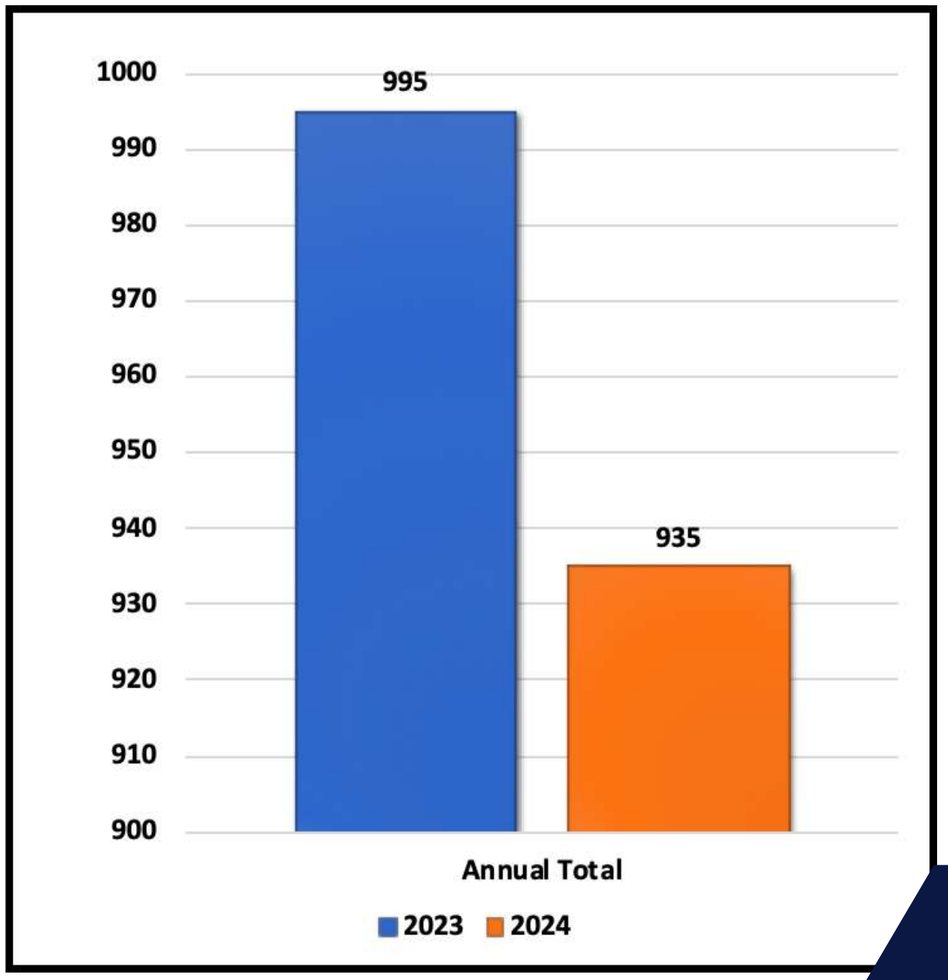
CYBER SECURITY INCIDENT STATISTICS

No.	Type of Incident	Total Incidents for The Year 2023 (January - December)
1	Distributed Denial of Service (DDOS)	33
2	Intrusion	785
3	Intrusion Attempt	980
4	Malware Infection	1297
5	Malware Hosting	21
6	Potential Attack	116
	Total	**3,232**



COMPARISON OF INCIDENTS BY TYPE OF INCIDENT FOR THE YEAR 2023-2024 (FIRST QUARTER)





CYBER THREAT TREND (Q1 2024)

HACKTIVISM

Increase in activity involving infostealer malware primarily driven by hacktivist groups who are exploiting leaked credentials

RANSOMWARE & APT

Notable rise in ransomware attacks with several companies falling victim through double extortion and intellectual property theft

TARGETED EXPLOITATION

Combination of outdated systems and misconfigurations have led to an increase in cybersecurity risks

FINDINGS

LACK OF MULTI-FACTOR AUTHENTICATION (MFA)

Neglecting to implement Multi-Factor Authentication (MFA) across digital services increases the risk of unauthorized access and exploitation

LOW CYBER HYGIENE AND AWARENESS

The absence of cybersecurity awareness programs leaves the workforce ill-equipped to recognize and mitigate cyber threats effectively

OBSOLETE ICT INFRASTRUCTURE

Modernizing cybersecurity infrastructure ensures that systems are equipped to withstand evolving threats, safeguarding sensitive information

REGIONAL CYBER CRISIS CASE

June 17 : Attempt to deactivate Windows Defender detected
June 20 : Ransomware attack on PDN, services disrupted
June 21 : Government confirms attack, $8 million ransom
June 22 : Migration of immigration data to AWS begins
June 24 : Normal operations resume for Immigration Services
June 26 : Brain Cipher establishes a new leak portal
June 27 : Gradual recovery of PDN
June 29 : Public apology by Communications Minister
July 1 : Forensic investigation reveals security weaknesses
July 2 : Brain Cipher announces free decryption keys

LESSON LEARNED

Clear Crisis Communication Plan

Regular Backups and Testing

Regular Security Audits

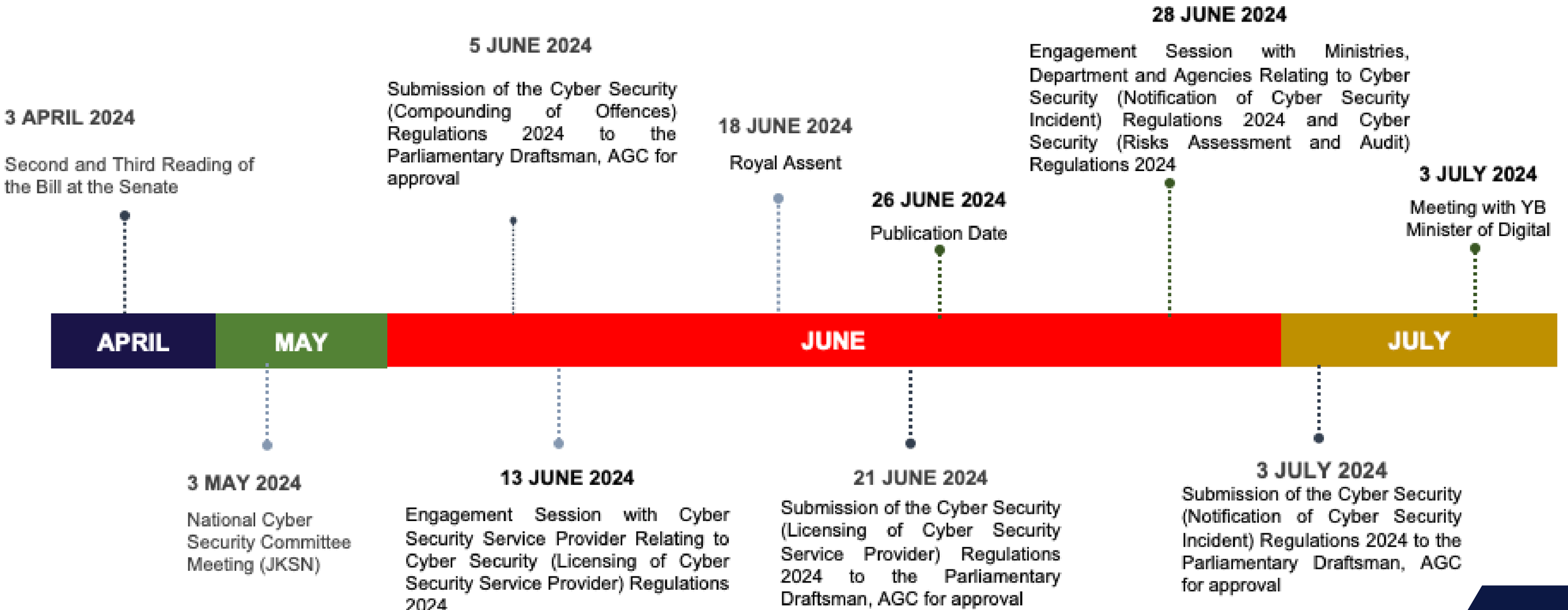
Strengthen Password Policies

INITIATIVE TO INCREASE NATIONAL CYBER SECURITY BASELINE

GOVERNANCE

Identify	Protect	Response	Detect	Recovery
Risk Management	**Effective & Ease of Use for Users**	**Anomaly & Unknown Threat Detection**	**Incident Management & SOP**	**Lesson Learnt**
• Identify Critical Asset and Dependencies • Prioritise Control	Access Control Hardening: • MFA • Least Privilege • Endpoint Protection • Remote Access	Response based on threat visibility The capability to response depended on the protection that has been implemented		Disaster Recovery Plan, testing and backup

CYBER SECURITY ACT 2024 [ACT 854] CRITICAL MILESTONE



CYBER SECURITY ACT 2024 [ACT 854]

- Published on 26 June 2024

  Royal assent by the YDPA on 18 June 2024 and proceed to be gazetted on 26 June 2024

- Not Yet in Force

  The four (4) regulations under the Act need to be gazetted too before it can be in force

THE 9 SECTIONS OF CYBER SECURITY ACT

SECTION I
PRELIMINARY

SECTION II
NATIONAL CYBER SECURITY COMMITTEE

SECTION III
DUTIES AND POWERS OF CHIEF EXECUTIVE

SECTION IV
NATIONAL CRITICAL INFORMATION INFRASTRUCTURE SECTOR LEAD AND NATIONAL CRITICAL INFORMATION INFRASTRUCTURE ENTITY

SECTION V
CODE OF PRACTICE

SECTION VI
CYBER SECURITY SERVICE PROVIDERS

SECTION VII
CYBER SECURITY INCIDENT

SECTION VIII
ENFORCEMENT

SECTION IX
GENERAL

IMPLEMENTATION OF THE CYBER SECURITY ACT 2024

3R

REGULATION

RESOURCE
(Manpower)

RESOURCE
(Budget)

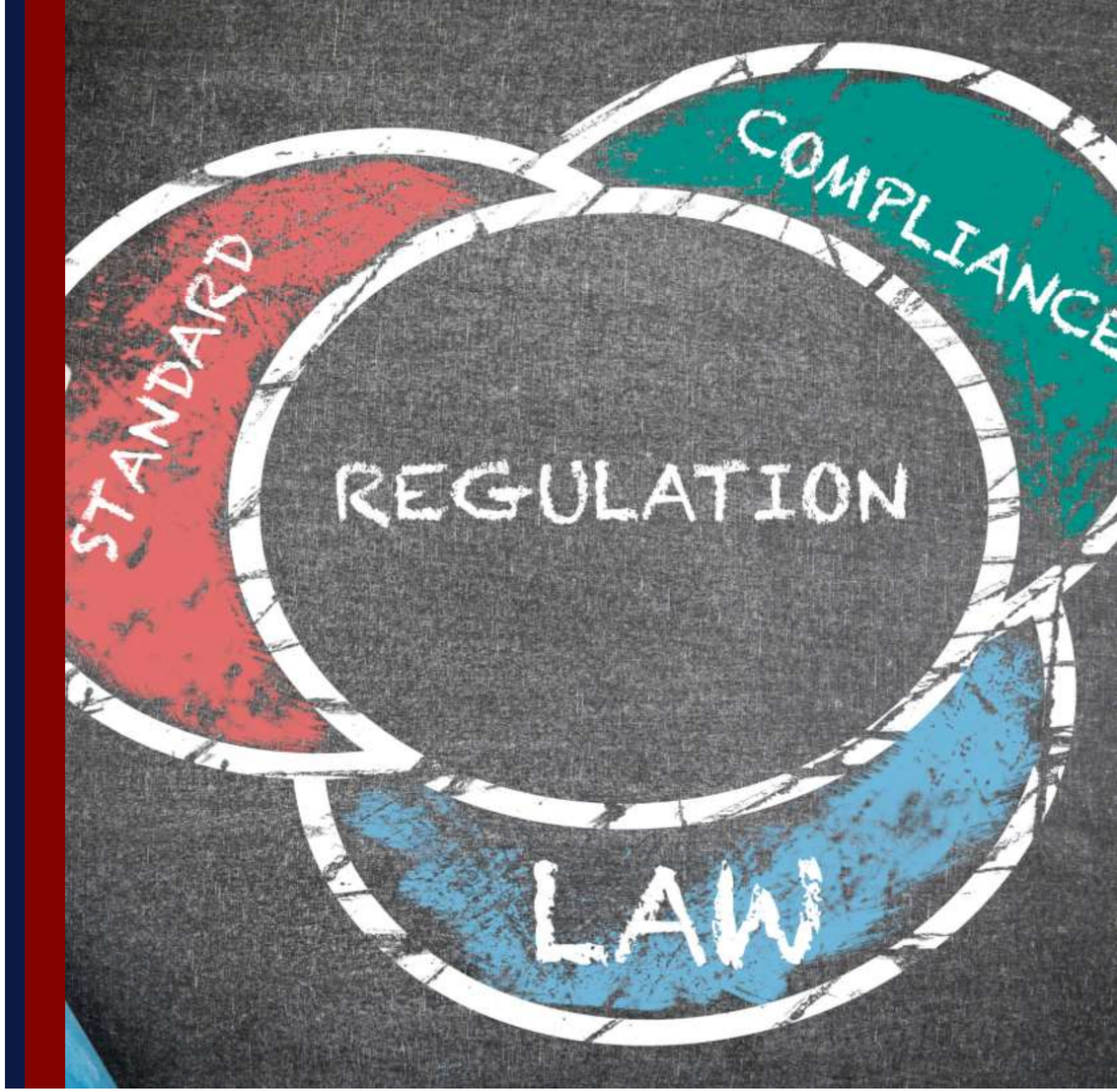
POWER TO MAKE REGULATIONS

CYBER SECURITY (LICENSING OF CYBER SECURITY SERVICE PROVIDER) REGULATIONS 2024

CYBER SECURITY (COMPOUNDING OF OFFENCES) REGULATIONS 2024

CYBER SECURITY (RISK ASSESSMENT AND TO CARRY OUT AUDIT) REGULATIONS 2024

CYBER SECURITY (NOTIFICATION OF CYBER SECURITY INCIDENT) REGULATIONS 2024



ACT 854

CYBER SECURITY (COMPOUNDING OF OFFENCES) REGULATIONS 2024

- ☑ 6 compounded offences
- ☑ 13 non-compounding offences

CYBER SECURITY (NOTIFICATION OF CYBER SECURITY INCIDENT) REGULATIONS 2024

Timeline of Reporting

- ☑ Within 6 hours of made known of an incident
- ☑ Full report within 14 days of incident

NOTIFICATION ON CYBER SECURITY INCIDENT

A cyber security incident in respect of the NCII comes to the knowledge of NCII Entity

6 HOURS

NCII Entity notify the cyber security incident to Chief Executive and NCII Sector Lead

The Chief Executive receive the notification on cyber security incident.

The Chief Executive shall instruct an authorized officer to investigate the cyber security incident

To ascertain:

1. whether a cyber security incident has occurred; or
2. in the case where a cyber security incident has occurred, determining the measures necessary to respond to or recover from the cyber security incident and preventing such cyber security incident from occurring in the future.

If the authorized officer finds that no cyber security incident has occurred

The Chief Executive shall notify the NCII Entity and dismiss the matter

If the authorized officer finds that a cyber security incident has occurred

The Chief Executive shall notify and may issue a directive to the NCII Entity

CYBER SECURITY (LICENSING OF CYBER SECURITY SERVICE PROVIDER) REGULATIONS 2024

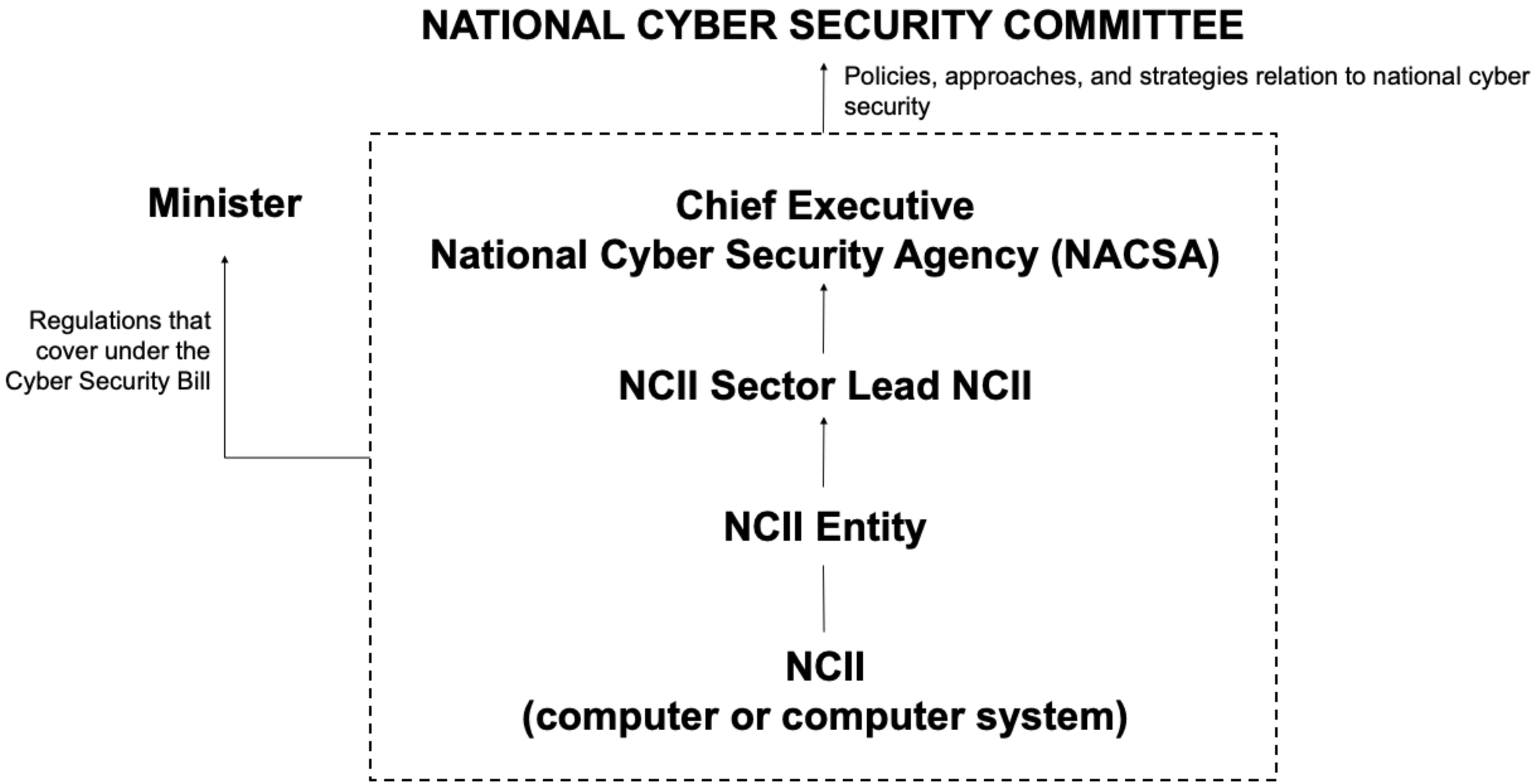
- Manage Security Operation Centre Monitoring Service
- Penetration Testing Service

CYBER SECURITY (Risk Assessment and AUdit) REGULATIONS 2024

Frequency of Activities

- Conduct a cyber security risk assessement at least once a year
- Carried out audit at least once in two years; or at such higher frequency

GOVERNANCE STRUCTURE



Conclusion

Ever-changing Landscape

The Cyber Security Act stands as a beacon of hope amid the growing complexities of the digital landscape.

Government Commitment

It symbolises our steadfast dedication to preserving the integrity, confidentiality, and accessibility of our digital ecosystems for future generations.

Secure, Safe and Trusted Cyber Space

In this era of digital advancement, let us unite in our commitment to leverage technology for the advancement of humanity, while remaining vigilant in safeguarding it from potential threats.

THANK YOU!

Contact Us

admin@nacsa.gov.my
www.nacsa.gov.my
NACSAmalaysia