Cyber Security Operations in an Island State

TLP:CLEAR

CERTVU Operations

By: Dr. Jeff G Liu
OGCIO &
CERTVU Team

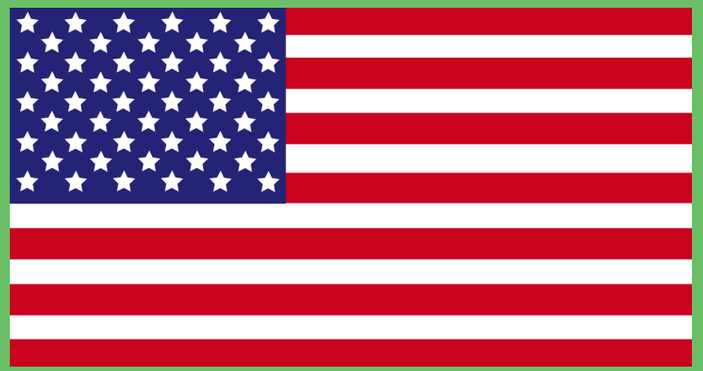
TLP:CLEAR

Outline

- Background
- The Problem
- The Strengths
- The Mandate
- The Incident Response Governance
- The Incident Response Structure
- Mechanism
- CERTVU Operations
- Setbacks
- Concluding Remarks

TLP:CLEAR

Acknowledgement



APNIC FOUNDATION

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

TLP:CLEAR

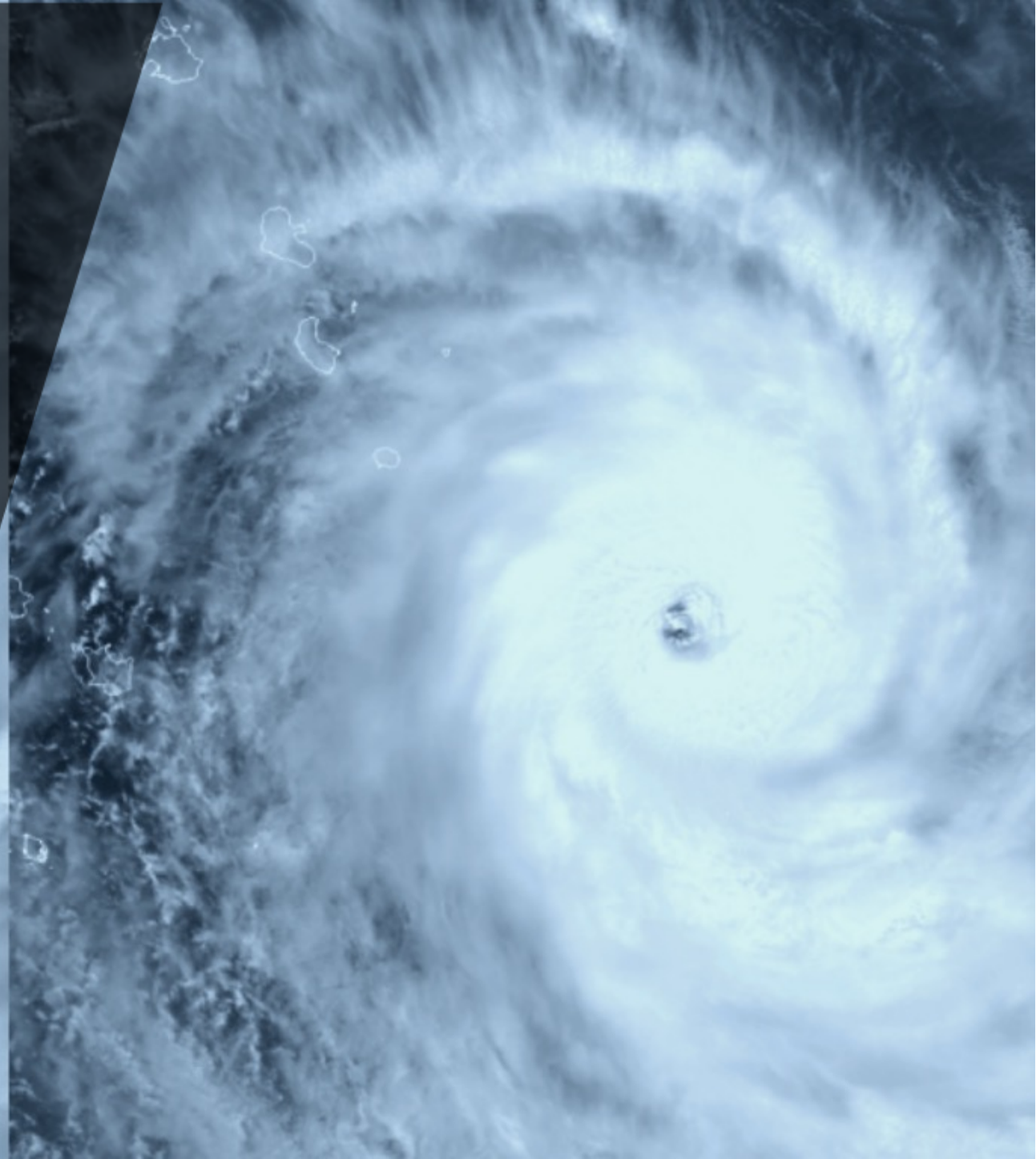
Background

- 2016 / 2017 - Cybersecurity Policy Mandate to establish a CERT
- Prior to CERTVU - Information Security Officer under OGCIO
- Systems & Network Security tasks
- SOC discussion
- CERTVU - 19th June 2018
- GBN Infrastracture spread across Vanuatu:
  - 6 Provinces
  - Submarine Cable & Towers
  - ISPs
  - 5000 + Users
- Services to all

TLP:CLEAR

The Problem

- Geographic Disadvantages
- Lack of Resources
- Financial Constraints
- Absence of Legislation
- Lack of Political Will or Buy-in
- Time
- Infrastructure
- Vulnerabilities
- Low Cyber-literacy



TLP:CLEAR

The Problem

- Bulleted
- Lack of Resources
- Financial Constraints
- Absence of Legislation
- Lack of Political Will or Buy-in
- Time
- Infrastructure
- Vulnerabilities
- Low Cyber-literacy

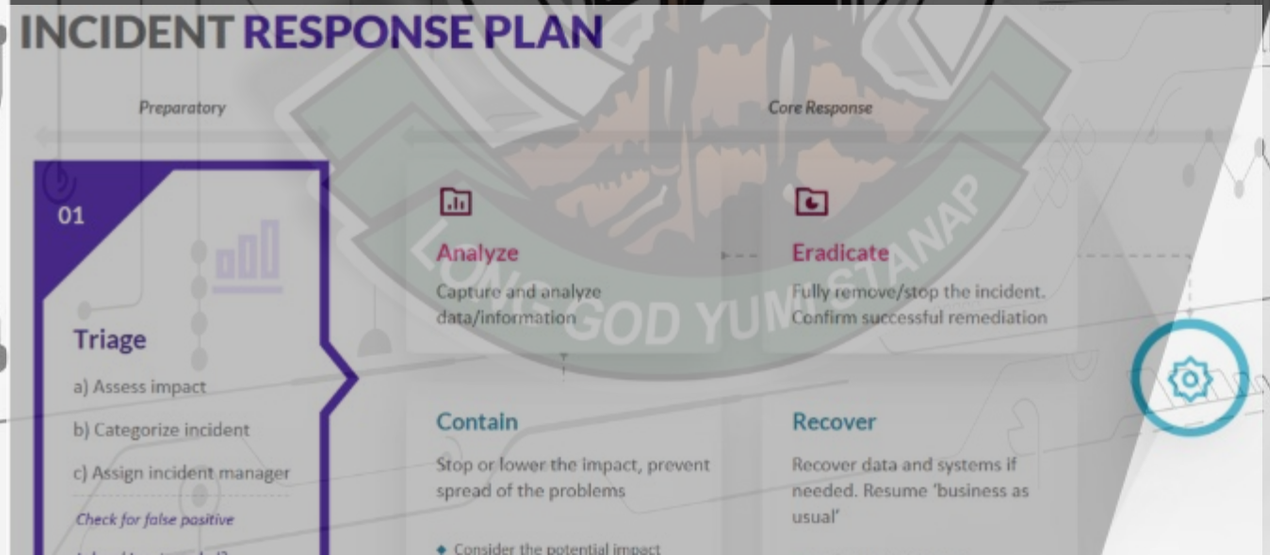
Strengths

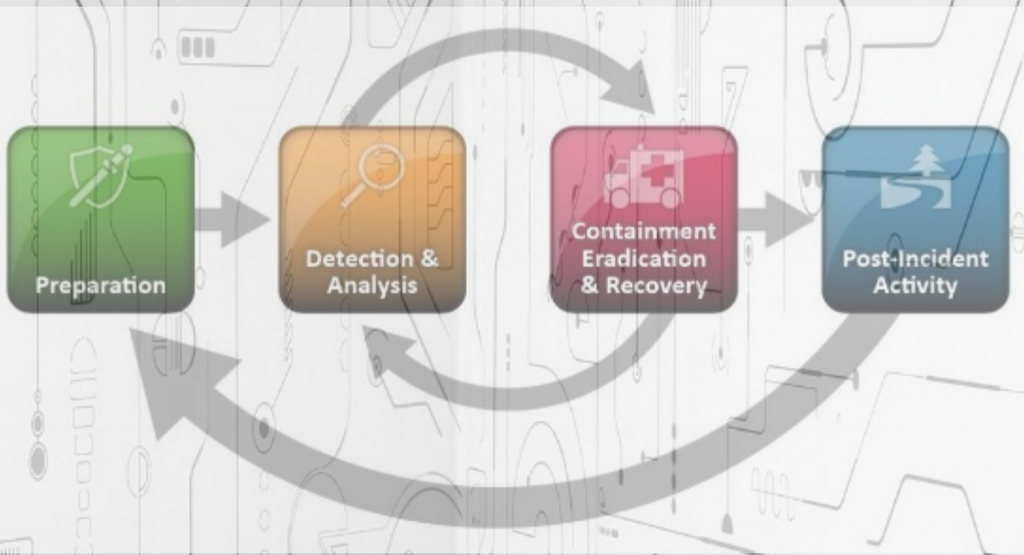
- Bulleted list
- Entity: CERTVU
- National ICT Policy 2013
- National Cyber Security Policy 2013
- Cybercrime Act No.22 of 2021
- National Cyber Security Strategy 2030
- Government Internal Security Policy Handbook
- GBN Infrastructure
- Political Will or Buy-in

TLP:CLEAR

The Mandate

- Incident Response





TLP:CLEAR

The Mandates

- Incident Response
- Provide Capacity Building and Awareness

TLP:CLEAR

Incident Response Governance Goals

VISION

- To create a secure, self-taught and security-aware capability environment for Vanuatu citizens, Government, business organizations by creating a better protected mindset for all citizens while being online; and
- To improve cyber security resilience, cyber hygiene and ensure cyber-threat preparedness of our borders and cyberspace are effectively active for a better National Security.

MISSION

We strive to create a proactive Cyber Security framework to secure and protect business operations by ensuring an improved two-way information sharing channel for a better Information Security management.

- Adjusting to other National Frameworks.
- Unify Awareness Campaigns.
- Build Cyber Capabilities and Talents.
- Increase International Cooperation.

Strategic Priorities

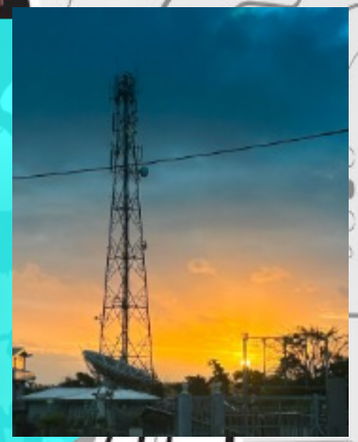
- Cyber Resilience
- Cyber Security Awareness
- Cyber Capabilities and Literacy
- Addressing Cybercrime
- International Engagement
- Cyber Security Standards and Legal Frameworks

The Incident Response Governance Mechanism

TLP:CLEAR

Critical infrastructure:

- What ?
- What is working, & What not working



Incident Response Team:

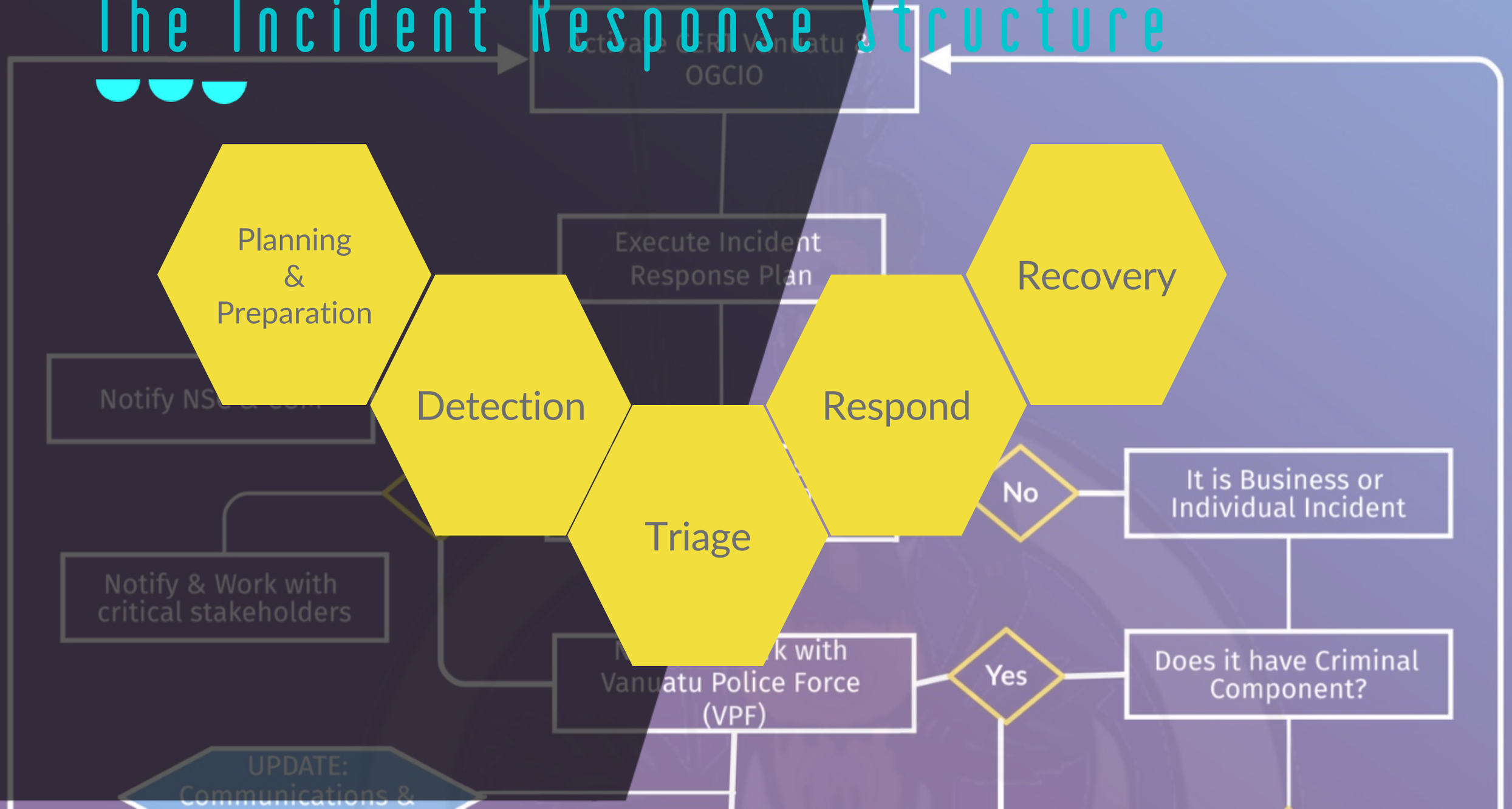
- Capabilities
- Willing to work
- Collaboration

Workflow:

- How tasks are done
- SOPs, Best Practices
- Communication

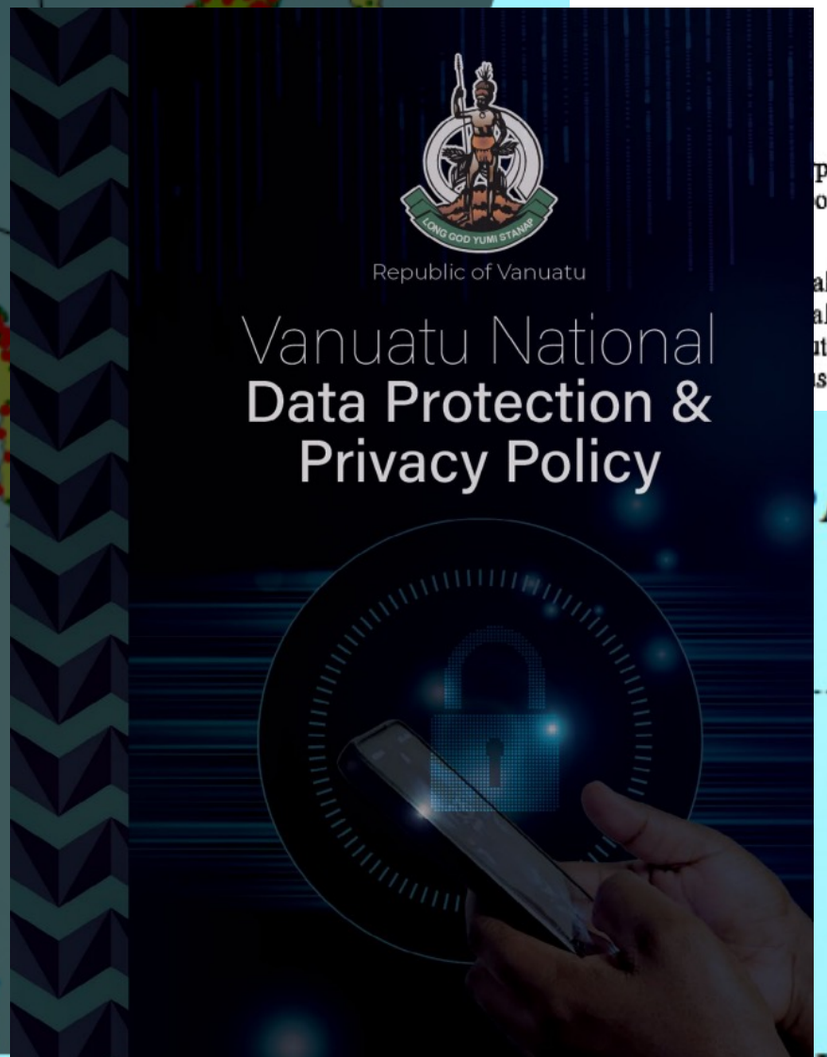
TLP:CLEAR

The Incident Response Structure



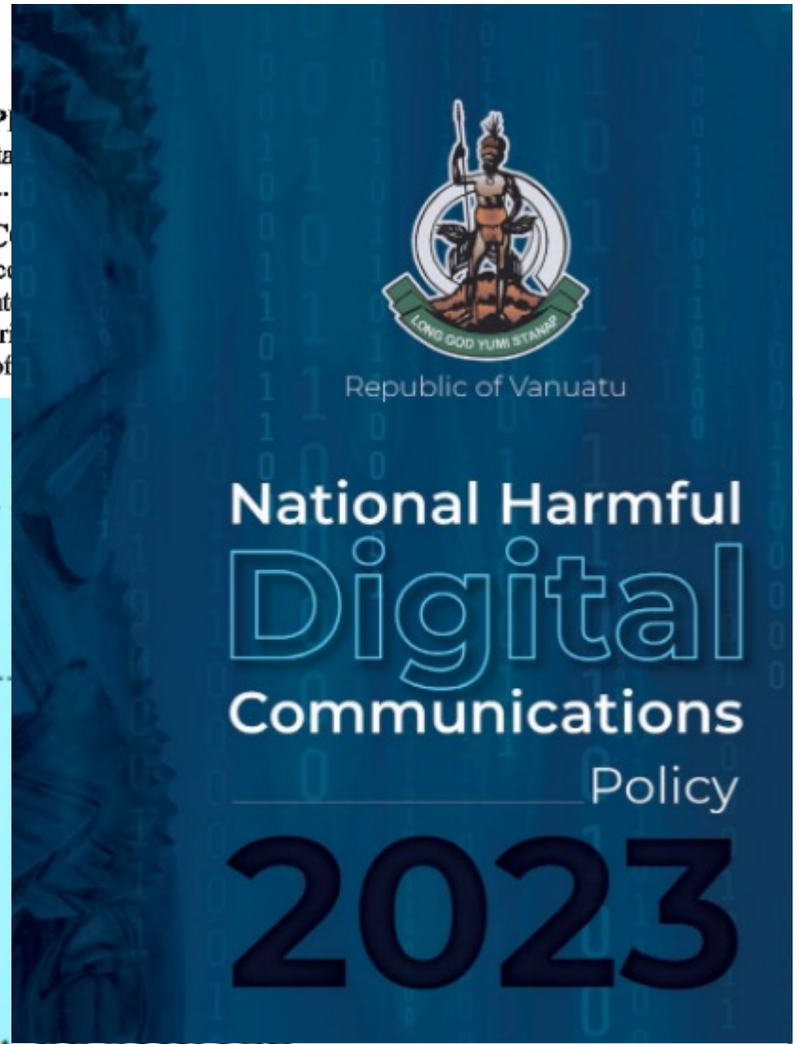
CERTVU Operations

TLP:CLEAR



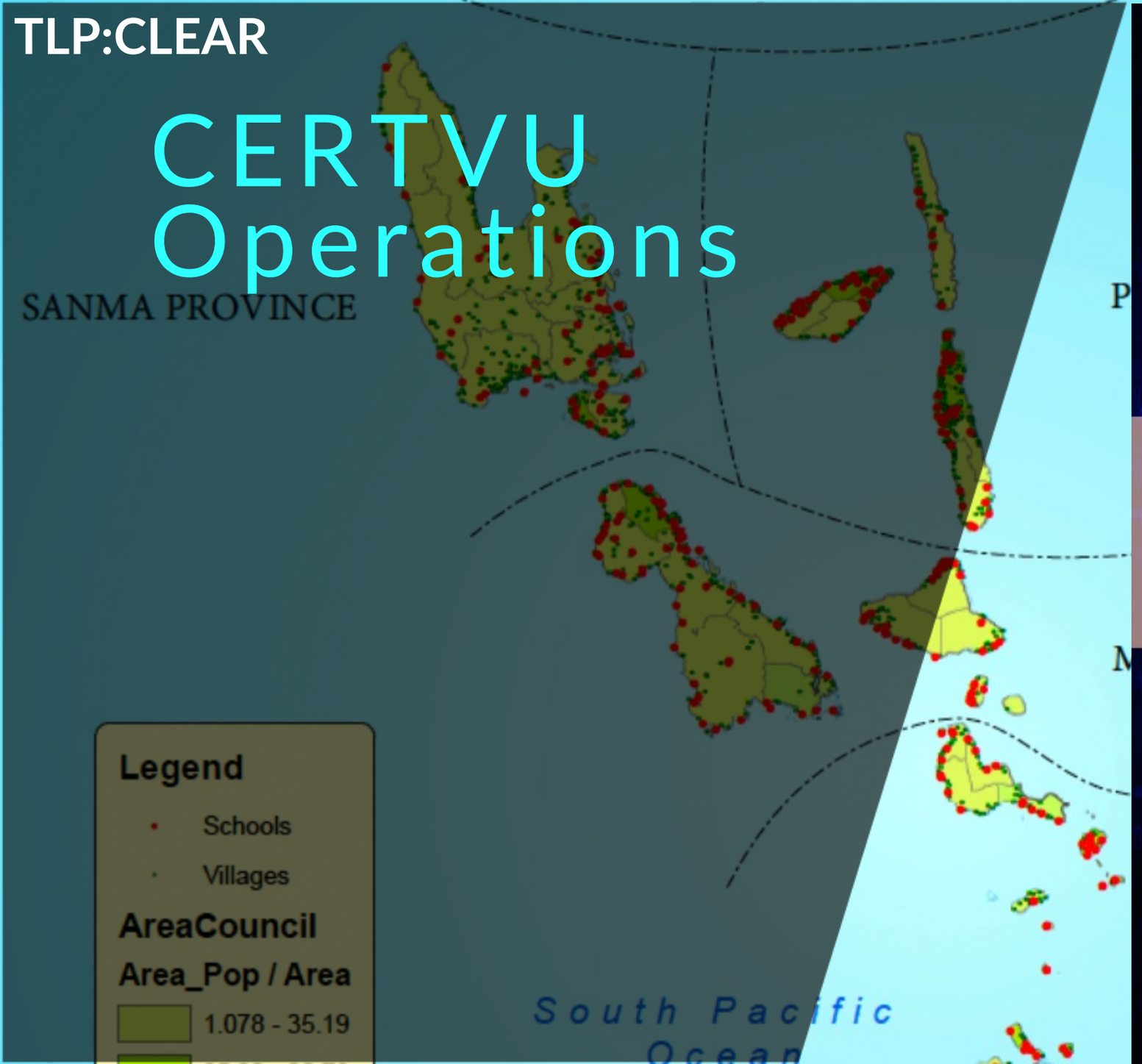
REPUBLIC OF VANUATU

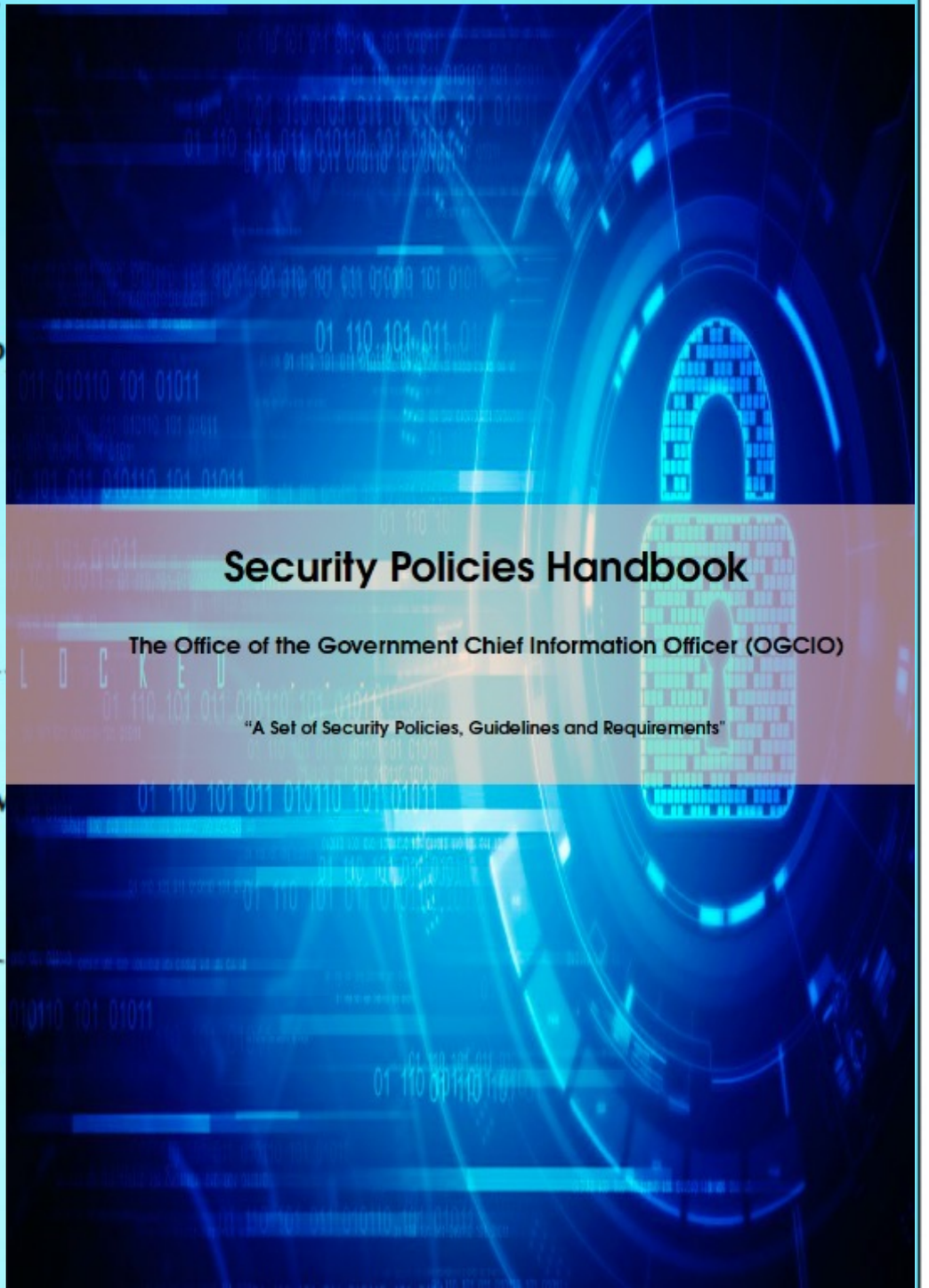
CYBERCRIME
ACT NO. 22 OF 2021



TLP:CLEAR

CERTVU Operations

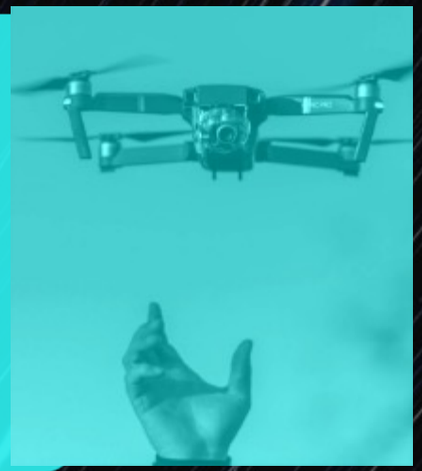




TLP:CLEAR

Setbacks

1 Time & Financial Constraints



2 Sophisticated Cyber-attacks

TLP:CLEAR

Concluding Remarks

"Logs are Gold"

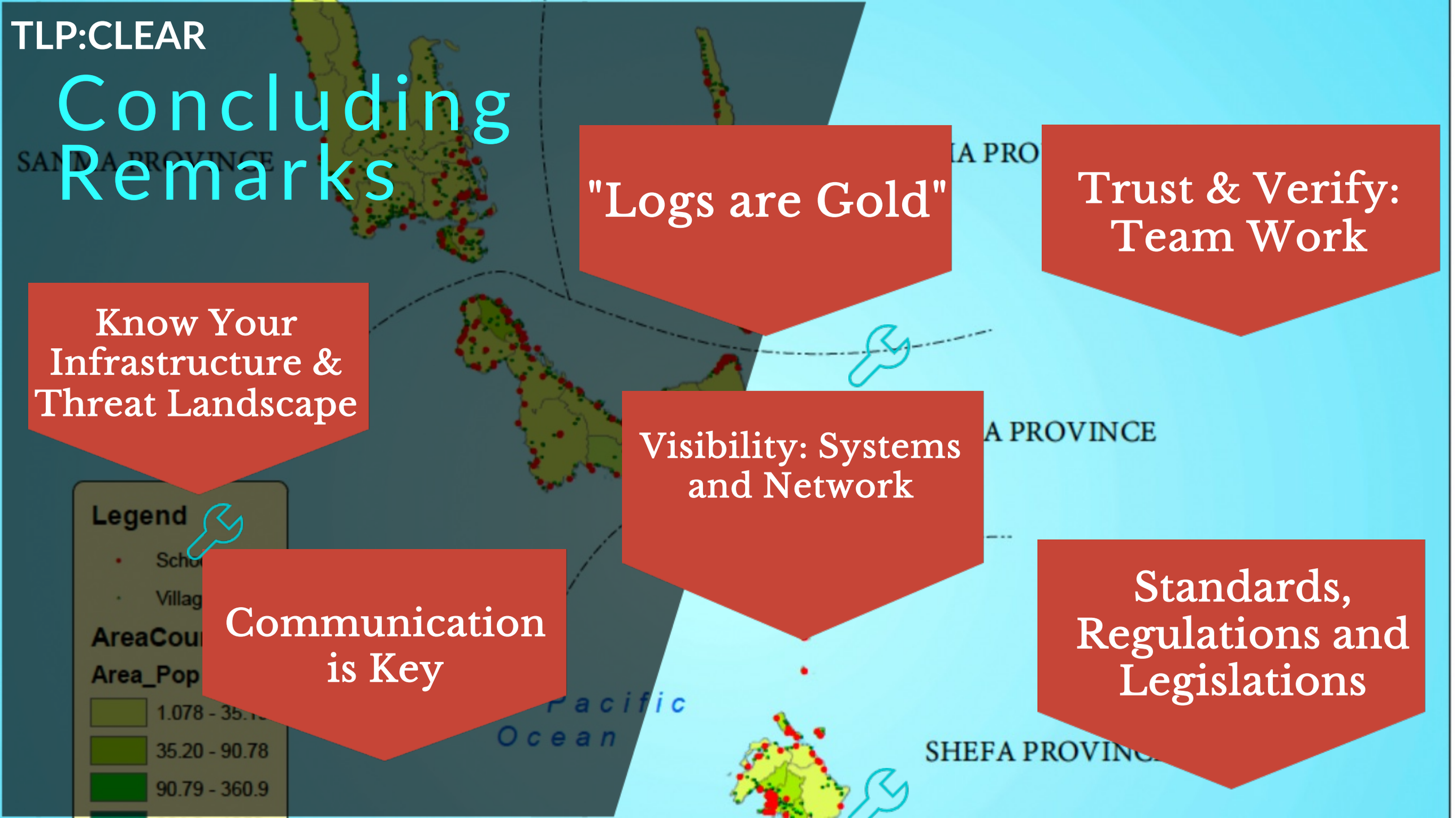
Trust & Verify: Team Work

Know Your Infrastructure & Threat Landscape

Visibility: Systems and Network

Communication is Key

Standards, Regulations and Legislations



Thank Yu Tumas!

CONTACT US

www.cert.gov.vu

info@cert.gov.vu

incident@cert.gov.vu

reports@cert.gov.vu

www.facebook.com/certvu