CERT MANUAL AND POLICIES

Engr. Mikaela Rosebien A. Abitria

OBJECTIVES

- To familiarize the different CERT levels and role of NCERT
- To understand the general policies based on the CERT manual
- To know the different protocols and classification for CERT
- To familiarize the Traffic Light Protocol for information sharing

MORRIS WORM INCIDENT

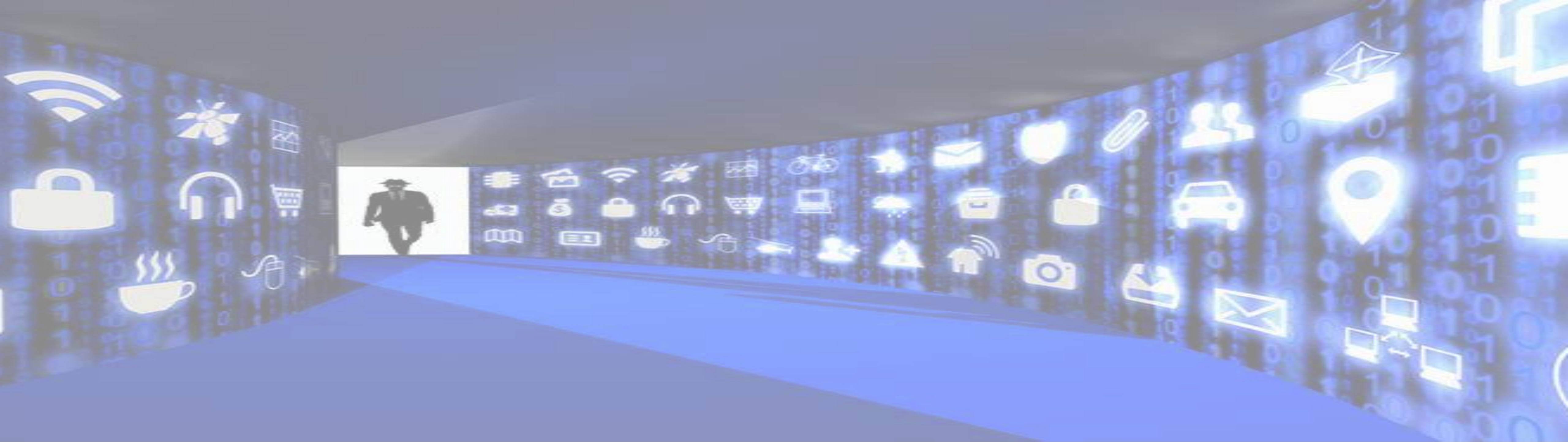
- Robert Morris, PhD student at Cornell University
- Launched the first ever internet worm on **November 2, 1998**
- Self-replicating worm which overloaded infected machines, just copied itself and didn't touch data
- Morris is the first one to be convicted in the US under 1986 Computer Fraud and Abuse Act

6000 Major UNIX machine infected

$10M-100M Estimated cost of damage

GENE SPAFFORD

- One of the foremost computer security experts
- First to analyze the famous Morris Worm which led to the conviction of Robert Morris
- Created a mailing list coordinating the **first incident response**.



FIRST CERT

DARPA formed the Computer Emergency Response Team (CERT) in Pittsburgh in November 1998

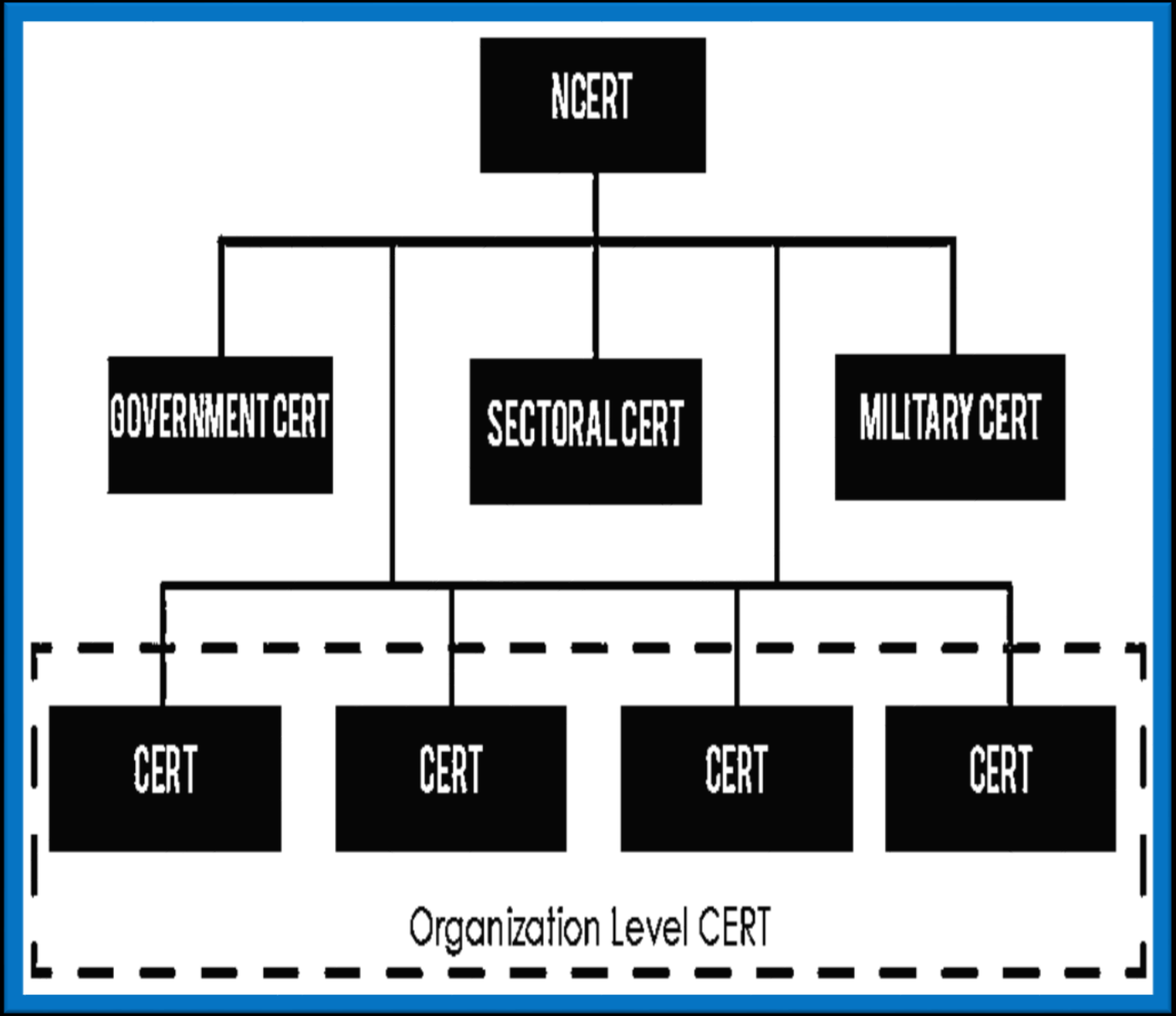
Today, it is part of the CERT Division of the Software Engineering Institute, which has more than 150 cybersecurity professionals

CERT is a registered trademark at Carnegie Mellon University

WHAT IS A CERT?

Computer Emergency Response Team (CERT) or Computer Security and Incident Response Team (CSIRT) refers to "an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security". At present, "both terms (CERT and CSIRT) are used in a synonymous manner.

- (ENISA, 2015 and ENISA, 2015a)



HIERARCHY OF COMPUTER EMERGENCY RESPONSE IN THE COUNTRY

GCERT

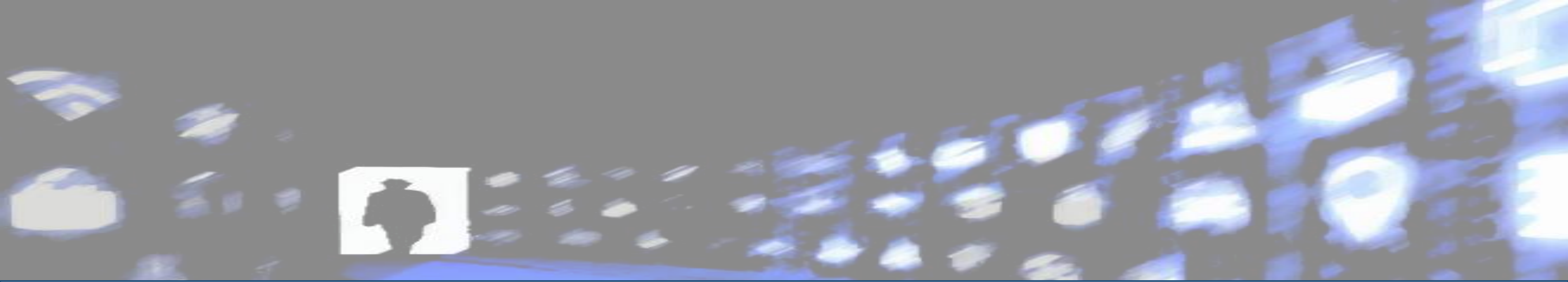
The Cybersecurity Officers (CYSO) shall create an organization headed by the chairman to be elected among member agencies. The chairman shall report to DICT on a regular basis.

DICT MEMORANDUM CIRCULAR 006

DICT MEMORANDUM CIRCULAR 005

All CIIs shall create a Sectoral CERT to be headed by the chairman elected among member organization within their respective sector. The chairman shall report to DICT on a regular basis.

SECTORAL CERT



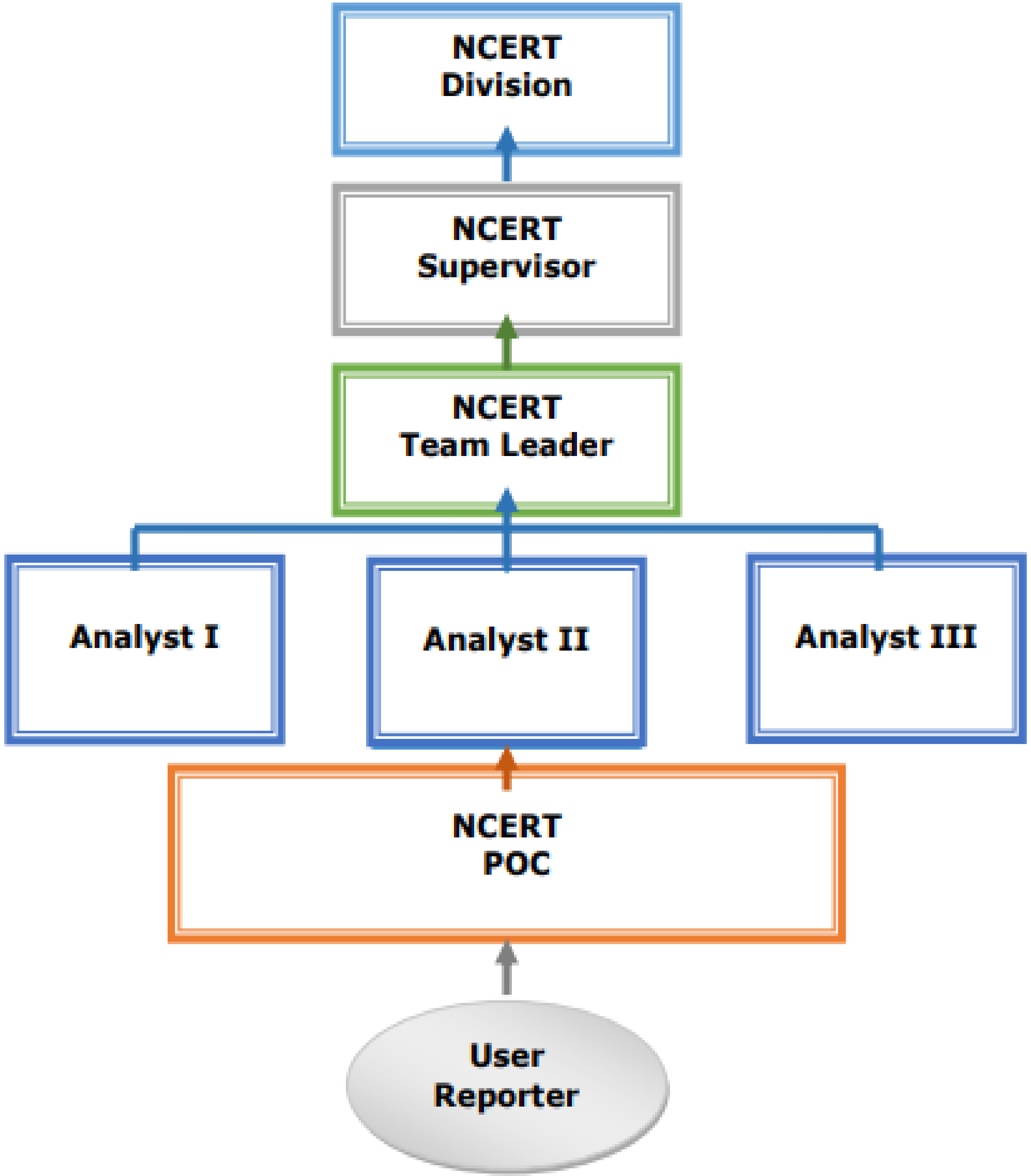
NCERT

NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

CERT-PH

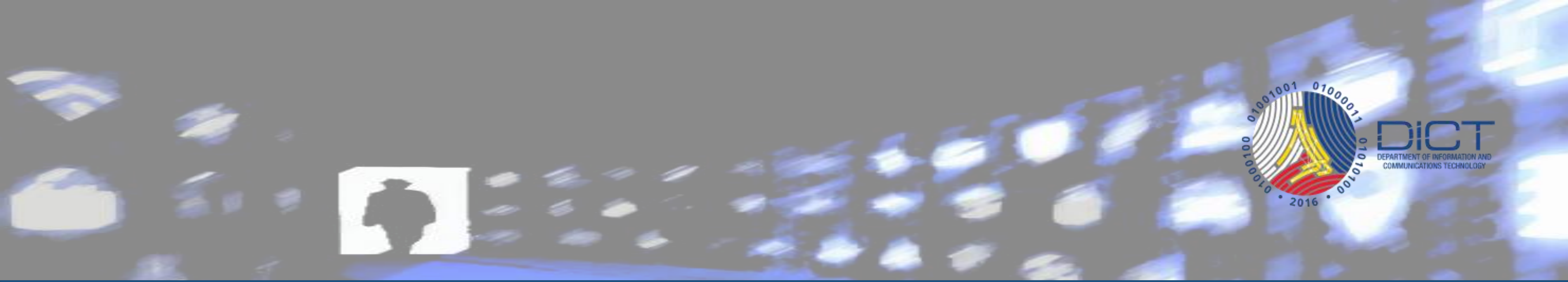
Responsible in **receiving, reviewing**, and **responding** to computer security incident reports and activities nationwide.

NCERT STRUCTURE



ROLES AND RESPONSIBILITIES

ROLE	FUNCTIONS
POC	provides 24/7 frontline service in the implementation of the Computer Emergency Response which establishes the first POC with users or reporters of any detected incident or event
ANALYST	Perform analysis and evaluation of information to determine the relevance which will prompt immediate response and initiate series of actions to respond to the incident or event.
TEAM LEADER	Supervise and evaluate reported incidents before assigning caseloads to Analyst with appropriate set skills
SUPERVISOR	Supervise the team and external groups assigned to perform support services in responding to information security incidents or events



CERT MANUAL

Framework for the incident response plan which will become the basis for creating the CERT of each organization

GENERAL POLICIES

DOCUMENTATION

- Information whether written, spoken or recorded electronically or printed, shall be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle.
- Retention period of 6 years

ACCOUNTABILITY

- Ensure the integrity and reliability of the government's digital presence and corporate identity as part of its commitment to good governance
- Establish control in reporting all computer emergency incidents and events through appropriate channels

ESTABLISHING CERT

- Computer emergency incidents and events shall be classified for information systems based on the potential impact on an organization
- All reported incidents must be identified to initiate immediate response actions to deal with the information security incident

1. ACTIVATION OF NCERT PROTOCOL

- Activate within **24 hours** after confirmation of the validity of the incident
- Proper coordination between relevant NCERT personnel

2. ASSESSMENT PROTOCOL

- Upon assembling the NCERT Team, the assessment is executed and reviewed to ensure all pertinent facts are established
- Designated persons will take action to notify appropriate internal and external groups, as necessary:
  - Internal Communication
  - External Communication
  - Report Originator
  - Status

PROTOCOLS AND CLASSIFICATIONS

3. CONTAINMENT PROTOCOL

- Counteract the immediate threat;
- Prevent propagation or expansion of the incident to other system of the organization;
- Minimize actual and potential damage;
- Restrict knowledge of incident to authorized personnel only; and
- Preserve information relevant to the incident.

4. CORRECTIVE MEASURES PROTOCOL

- Secure processing environment; and
- Restore processing environment into its acceptable and secure state. Status

PROTOCOLS AND CLASSIFICATIONS

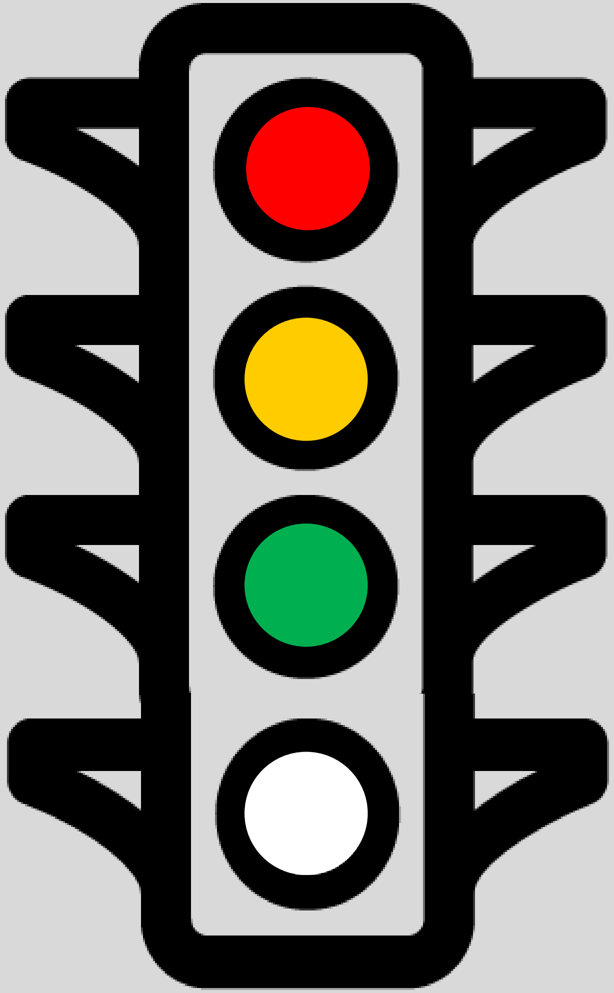
5. CLOSURE PROTOCOL

- Actively engaged throughout the life cycle of the information security incident
- Continuously assess the progress/status of all containment and corrective measures; and
- Determine at what point the incident is considered closed or resolved.

6. POST INCIDENT REVIEW PROTOCOL

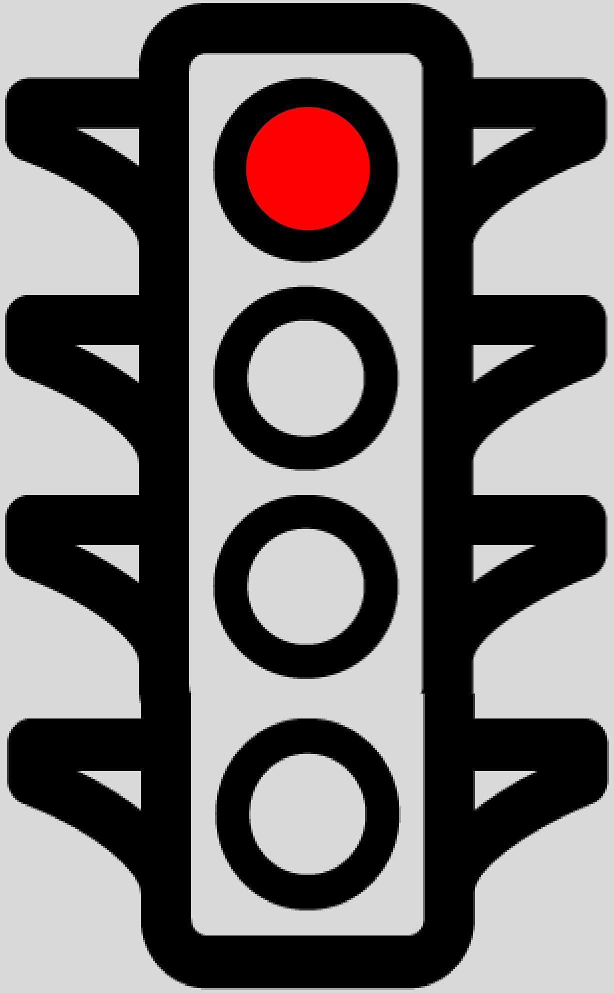
- Improving and polishing the over-all incident response process; and
- Conduct the follow up with the report originator, third parties or other relevant stakeholders, as required or as appropriate environment

PROTOCOLS AND CLASSIFICATIONS



TRAFFIC LIGHT PROTOCOL

A set of designations developed by the Forum of Incident Response and Security Team (FIRST) used to ensure that sensitive information is shared with the appropriate audience.



TRAFFIC LIGHT PROTOCOL

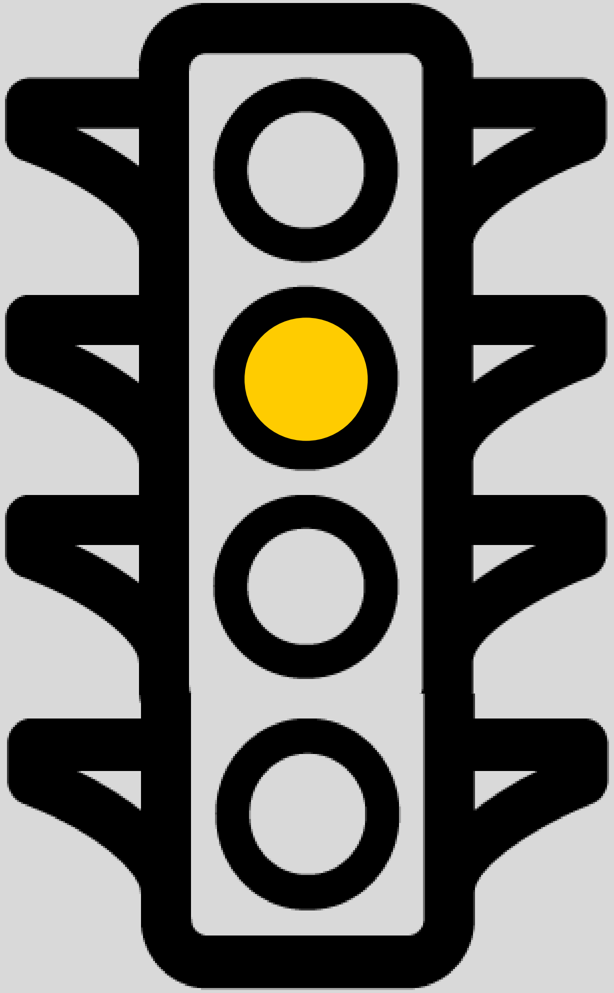
NOT FOR DISCLOSURE, RESTRICTED TO PARTICIPANTS ONLY

When should it be used?

When information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.

How it may be shared?

Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.



TRAFFIC LIGHT PROTOCOL

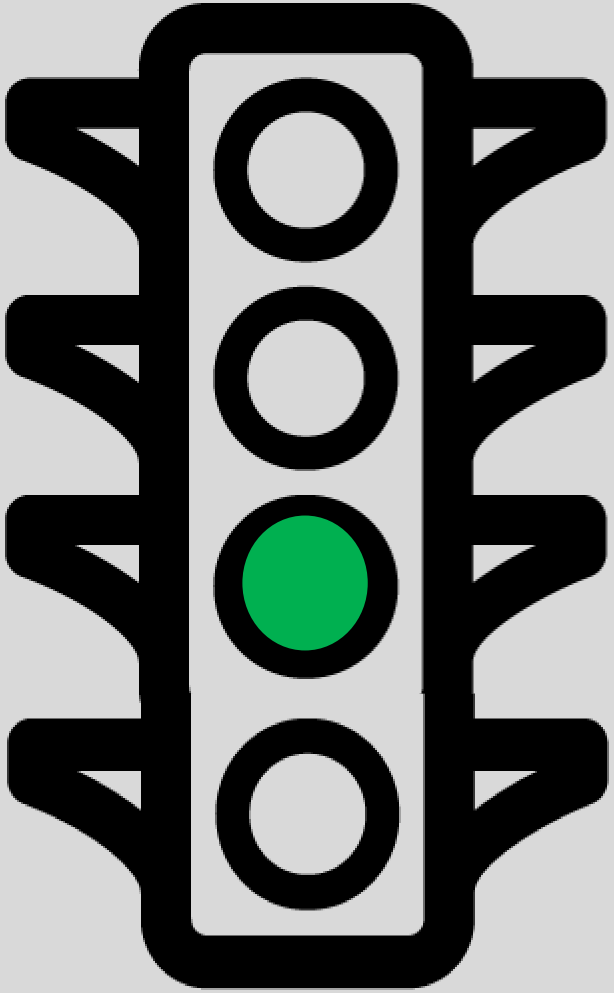
LIMITED DISCLOSURE, RESTRICTED TO PARTICIPANTS' ORGANIZATIONS

When should it be used?

When information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

How it may be shared?

Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.



TRAFFIC LIGHT PROTOCOL

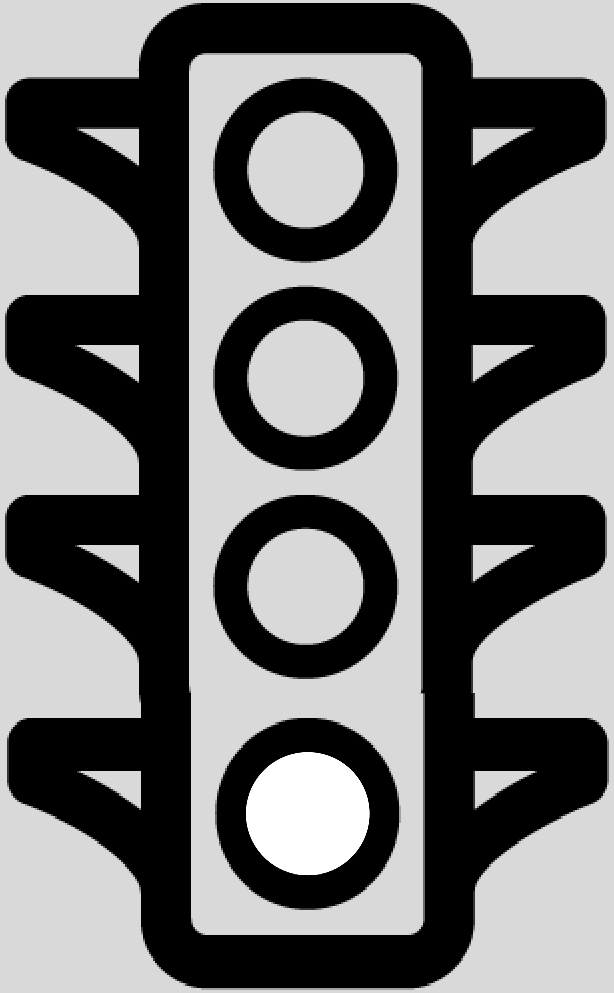
LIMITED DISCLOSURE, RESTRICTED TO THE COMMUNITY

When should it be used?

When information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.

How it may be shared?

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels



TRAFFIC LIGHT PROTOCOL

DISCLOSURE IS NOT LIMITED

When should it be used?

When information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

How it may be shared?

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

REVIEW

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

- Philippines National CERT (CERT-PH) shall be the central authority for all the CERTs in the country.

- CERT is composed of different personnel with respective responsibilities

- Document everything!!!

- CERT must be activated within 24 hours from the validity of the incident.

- The Traffic Light Protocol is a standard for information sharing and is composed of 4 colors: Red, Amber, Green, and White.

QUESTIONS?