# CERT-PH CYBER INCIDENT DRILL 2021 (ON-LINE)

## I. BACKGROUND

### Rationale

The dynamic cybersecurity threat landscape demands for sustainable cybersecurity development. To ensure the protection of the Philippine's Critical Infrastructure, and Government and Public Networks, the cyber preparedness and response capabilities must continuously improve and mature to bolster the nation's cyber resilience.

In support of the on-going cybersecurity efforts and programs of the Philippine government, the National Computer Emergency Response Team (CERT-PH) under the DICT-Cybersecurity Bureau will be conducting a series of Cyber Incident Drills for the Critical Information Infrastructure (CII) sectors. This initiative shall help assess the capability and readiness of sectoral coordination for cyber incidents.

As the lead body mandated to formulate, coordinate and monitor cybersecurity plans and programs, the DICT endeavors to enhance the nation's cybersecurity readiness and incident response capabilities by holding cyber incident response exercises.

### Description

One of the strategies under the 1st Key Imperative of NCSP 2022 – the Protection of Critical Information Infrastructure (CII) is the establishment of a program for the National Cyber Drills and Exercise. The cyber incident drill event shall be a mandatory compliance for all government agencies and instrumentalities in order to sustain the development of our cybersecurity towards the desired maturity level. The Cyber Incident Drill and Exercise will use a set of scenarios to facilitate both participating Sectoral leads and sectoral organizations in carrying out incident handling, investigation, analysis, remediation, escalation and reporting.

The CERT-PH Cyber Incident Response Drill is a remote exercise which participants take part in real-time from each workplace remotely. The exercise will be facilitated by the National Computer Emergency Response Team (CERT-PH) with the aid of the CII sectoral leads. All the participants will be provided with a situation based on a scenario prepared in advance. The participants shall comprehend the situation according to the provided scenario and share information on an incident via platforms indicated in the Event Information Section Sub-section Platforms and Communication Channel.

**Objectives**

- To assess capability and readiness of sectoral coordination for cyber incidents
- To practice effective and adaptive incident handling and escalation procedures
- To train and examine participating agencies' incident response capabilities and communication
- To enhance collaboration between the Sectoral CERT Leads and their respective CII sectors in cybersecurity

**Target Venue and Participants:**

Participants shall be composed of CIIs from government agencies (their respective Computer Emergency Response Teams (CERTs), if applicable) and private organizations from the sectors of Healthcare, Media, Transportation and Logistics, and Water. Participating organizations shall form a team of at most three (3) participants preferably from, but not limited to, their IT department.

**Timeline:**

| Event | Date | Time |
|---|---|---|
| **Pre-Drill Communications Check (Technical Briefing)** | June 22, 2021 | 09:30:00 - 11:30:00 |
| **Cyber Incident Drill Proper** | June 24, 2021 | 09:00:00 - 12:00:00 |
| **Cyber Incident Drill Post-Drill Activity** | July 02, 2021 | To be announced (TBA) Zoom meeting per sector |

**How to join**:

Link to the CERT-PH Public Announcement: https://bit.ly/3fXdMAC

**II. Event Information**

**Registration:**

- Participants should submit their registration on or before June 11, 2021.
- Participating agencies should form a team composed of at most 3 personnel. It is highly recommended that the team be a combination of officers from Information Technology (IT), IT Security, Human Resource, and Legal.
    - Coordinate and assign a primary and secondary coordinator for each team that will serve as the focal personnel in the conduct of the event.

**Communication and Coordination:**

- Each organization shall designate a **PRIMARY** and **SECONDARY** coordinator in their respective CERTs.

- **PRIMARY -** All REPORTS, RESPONSES and INQUIRIES via email should only come from the primary coordinator. Primary coordinator is also tasked to acknowledge and respond to drill injects, and communicate with the Facilitators during the event.
- **SECONDARY -** In the case that the PRIMARY coordinator cannot participate during the drill, the said responsibility is transferred to the secondary coordinator. Secondary coordinator is also responsible for forwarding the drill injects to the other members of the team.

- The CERT-PH personnel should be informed of any changes between the PRIMARY and SECONDARY coordinators.
- During the actual Cyber Incident Drill:
    - The cyber incident drills are composed of multiple incident scenarios that will be sent to participating organizations.
    - CERT-PH will be the one who will send the **first and last injects** for the drill exercise.
    - The remaining injects will be communicated and coordinated with the assigned **Primary Coordinator** per organization and their respective **Sectoral Lead**.

**Platforms and Communication Channels:**

- **Email Communication**:
    - Sending of drill scenarios and injects will only be facilitated through the email addresses of the coordinators provided IN THE REGISTRATION FORM.
    - Acknowledgement receipts and responses from coordinators shall also be sent via email.

- **Discord Application**:
    - Discord will be used as the communication medium in the conduct of the Pre-Drill Communications Check (Technical Briefing) and Drill Event Proper, wherein facilitators will accommodate questions and inquiries, and provide technical assistance to participants.
    - Invitation links to the dedicated Discord Server will be sent to verified participants on **June 17, 2021** via email.

- **CTFd Platform**:
    - The CTFd is a capture the flag platform that will be used to submit the organizational CERTs' incident drill findings.

- Each drill scenario has questions that must be answered via the platform to gain points.
- The scoreboard will only be visible to CERT-PH.
- Credentials and the link to the CTFd platform will be sent to verified participants on **June 17, 2021** via email.
- The CTFd platform will only be accessible during the communications check and cyber drill proper.

## III. Cyber Drill Methodology

- Participants are expected to carry out investigations on the scenarios and evidence given during the drill. This will require the participants to exercise skills necessary when responding to a cyber incident. This includes response time, confirmation, gathering of evidence, investigation, analysis, and reporting.
- Participating agencies will be scored according to the correctness of the findings. Other team's scores will not be available to other participant teams.
- CERT-PH will use the drill scores as key indicators in assessing the capability and readiness of sectoral coordination for cyber incidents
- All instructions, guidelines, report templates, and additional materials shall all come from the Rules of Engagement to be discussed by the CERT-PH during the Pre-Drill Communications Check (Technical Briefing).

## IV. Evaluation:

All participating agencies and organizations are expected to fill out the Cyber Incident Drill Feedback Form that will be used to improve future cyber incident drills. The form will be sent out by CERT-PH during the last scenario.

## V. Certificate of Participation

Certificate of Participation will be provided.

**FAQs:**

q1. **Who should attend the National Cyber Incident Drill?**

a1. Anyone can be part of the event, even without prior knowledge on cyberthreats and attacks. However, it is recommended for Information Technology (IT) and IT Security professionals to participate in the Drill.

q2. **What is the minimum system requirement to accomplish the drill scenarios?**

a2. The drill scenarios and questions will be available in the CTFd platform. However, the drill artifacts must be investigated and analyzed via the participant's machine. So it is recommended to have at least a windows operating system. Also having a linux or unix based system is an advantage for the participants in answering some of the drill questions.

q3. **Do we need 3 participants to participate in the Drill?**

a3. No, at least one (1) dedicated participant can join and complete the drill. We do not limit the number of members per organization who can assist the team in solving the drill scenarios and injects. However, only three (3) officially designated members will have access to the drill platform.

q4. **Do we need to use Virtual Machine and/or VPN to analyze the artifacts?**

a4. VM and VPN are not required for this event, but it is recommended to use Virtual Machine that has security tools and applications to analyze and investigate the artifacts.

q5. **Who can we contact if there are problems and/or issues encountered during the drill?**

a5. Private Discord channels will be used for CERT-PH to accommodate the participants in their questions and inquiries.

q6. **Is it mandatory to install Discord in our Desktop/Laptop?**

a6. No, participants may also use the Discord mobile application as an alternative.

q7. **Can we allow non-registered participants to join the pre-drill and actual drill event?**

a7. No, we will not accommodate additional participants past the registration deadline as this may disrupt the event flow. Participants are required to attend the pre-drill (technical briefing) as necessary technical details about the conduct of the actual drill will be discussed by the facilitators.

q8. **What if I cannot join the Pre-Drill (Technical Briefing) activity?**

a8. Your team must have at least one (1) dedicated member to participate in the pre-drill who can relay the information discussed during the pre-drill activity to the entire team. The attendance form must still be accomplished either by you or your teammate.