# NATIONAL CYBER SECURITY INCIDENT REPORTING FORM

CII Owners should submit the details required under Part 1 by calling the specified telephone number for their respective sector within 2 hours of becoming aware of the occurrence of a relevant cybersecurity incident[[1]](#footnote-1) in accordance with **Regulation 5(1)(a) of the Cybersecurity (Critical Information Infrastructure) Regulations 2018** (“the Regulations”) read with Regulation 5(2)(a) of the same. If they are unable to do this within a reasonable time, they should text message these details to the specified telephone number, or fill in Part 1 and submit these to their respective Assistant Commissioners (ACs)[[2]](#footnote-2) under Regulation 5(1)(a) of the Regulations read with Regulation 5(2)(b)(i) or (ii) of the same.

CIIO Owners should also complete Part 2 *and* fill in/amend Part 1 as necessary, within 14 days after making the report mentioned in Regulation 5(1)(b) of the Regulations, in accordance with **Regulation 5(1)(b) of the Regulations**.

|  |
| --- |
| **PART 1** |
| **Section A: General Information** **CSA’s Reference Number (to be filled in by CSA NCSC):** Click here to enter text. |
| A1. AC or CII Owner that is reporting this incident (Choose only one option)

|  |  |
| --- | --- |
|[ ]  AC | Click here for a dropdown list of CII Sectors. |
|[ ]  CII Owner | Click here to enter the organisation’s name. |

 A2. Informer's Information  Name: Click here to enter text. Designation: Click here to enter text. Organisation: Click here to enter text. Email Address: Click here to enter text.  Telephone Number: Click here to enter text.A3. This is a/an[ ]  New incident[ ]  Update to a previously reported incident AC’s or CII Owner’s reference number for this incident (if any).  Click here to enter text.A4. This incident is classified under

|  |  |  |
| --- | --- | --- |
| [ ]  **Category 1** –*Section 14(1)(a) of the Act* | [ ]  **Category 2** –*Section 14(1)(b) of the Act* | [ ]  **Category 3** –*Section 14(1)(c) of the Act* |
| A prescribed cybersecurity incident in respect of the CII. | A prescribed cybersecurity incident in respect of anycomputer or computer system under the CII Owner’s control that is interconnected with or that communicates with the CII. | Any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the CII Owner. |

 |
| **Section B: Incident Details**  |
| B1. When did the CII Owner become aware of the incident?(Please specify in Singapore Local Time GMT+8)Date: Click here to enter the date.Time: Click here to enter the time. B2. When was the incident reported to the AC? (Please specify in Singapore Local Time GMT+8)Date: Click here to enter the date.Time: Click here to enter the time.B3. Types of Threats/Incidents (You may choose more than one option)[ ]  Denial of Service (DoS) [ ]  Distributed Denial of Service (DDoS)[ ]  Virus/Worm/Trojan [ ]  Intrusion/Hack/Unauthorised access[ ]  Website Defacement [ ]  Misuse of Systems/Inappropriate usage [ ]  Other: Click here to enter text.B4. Is this incident related to another incident previously reported to CSA? Choose an option. If “Yes”, please provide more details.Click here to enter text.B5. Please provide, to the best of your knowledge, the following details in respect of CII affected by the cybersecurity incident: The number of CII affected by the incident: Click here to enter text. Name(s) of the CII: Click here to enter text. Name(s) of CII Owner(s): Click here to enter text. Email Address: Click here to enter text.  Telephone Number: Click here to enter text.B6. Please provide further details of the CII that is/are affected by this incident. Details should minimally include:Location, purpose of the CII, hardware and software affected (please list details of hardware manufacturer, software developer, make/model, etc.).Click here to enter text.Where relevant, please indicate the Operating System (OS) of the affected CII: Choose an option.If “other”, please indicate the OS here: Click here to enter text.B7. Please provide the following details relating to the cybersecurity incident: To the best of your knowledge, when did the incident occur? (Please specify in Singapore Local Time GMT+8)Date: Click here to enter the date. Unknown: [ ] Time: Click here to enter the time.If “Unknown”, when was the incident first observed? (Please specify in Singapore Local Time GMT+8)Date: Click here to enter the date.Time: Click here to enter the time.To the best of your knowledge, how did the incident occur?Click here to enter text.How was the incident first observed/sighted/detected?Click here to enter text.B8. What are the effects that have been observed to result from the cybersecurity incident? This includes any effect on the CII and interconnected computers or computer systems, and any effect on the CII Owner(s), licensee(s) and/or users of the essential service supported by the affected CII (e.g. service performance degradation, disruption to service availability, loss of personal data, loss of business data, loss of log information, etc.).Click here to enter text.B9. Where the CII mentioned above has/have been adversely affected, is there any potential effect on other critical asset(s) owned or controlled by the CII Owner(s)/licensee(s)? (e.g., where a domain controller has been compromised, other systems using domain credentials from the domain controller may be affected)Choose an option. If “Yes”, please provide more details.Click here to enter text.B10. To the best of your knowledge, where the CII mentioned above has/have been adversely affected, is there any potential effect on asset(s) belonging to other CII Owner/licensee(s) (not necessarily from the same sector)? Choose an option. If “Yes”, please provide more details.Click here to enter text. |

|  |
| --- |
| **PART 2**  |
| **Section C: Incident Handling Status**  |
| C1. What is/are the type(s) of follow-up action(s) that has/have been taken at this time? Click here to enter text.C2. What is the current status or resolution of this incident? Choose an option. C3. If it has not been resolved, what is the next course of action? Click here to enter text.C4. What is the earliest known date of attack or compromise? If earliest known date is unknown, please indicate accordingly. (Please specify in Singapore Local Time GMT+8)Date: Click here to enter the date. Unknown: [ ] Time: Click here to enter the time.C5. What is the source/cause of the incident? (Indicate ‘NIL’ if unknown)Click here to enter text.C6. Has the incident been reported to any law enforcement agency? Choose an option. If “Yes”, please specify which agency has the incident been reported to.Click here to enter text. |
| **Section D: Other Information**  |
| D1. IP Addresses(Required if surfaced from the incident)Please provide the list of IP addresses surfaced from the incident. Please state the involvement of the IP addresses in the incident (e.g. Victim, Malware Command & Control Servers, etc.). If IP addresses were resolved from domain names, please specify the domain names and the date/time of resolution of IP addresses from the domain names.

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **Involvement** | **Domain name from which IP address was resolved**  | **Date/Time of Resolution of IP address from Domain name**  |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

D2. Domain Names (Required if surfaced from the incident)Please provide the list of domains surfaced from the incident. Please state the involvement of the domain names in the incident. (e.g. Drive-by-download Servers, Malware Control & Command Servers, defaced website)

|  |  |
| --- | --- |
| **Domain Name**  | **Involvement of Domain name** |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

D3. Email Addresses (Required if surfaced from the incident)Please provide the list of email addresses surfaced from the incident. Please state the involvement of the email addresses in the incident. For example, an email address from which a phishing email appears to have be sent from, etc.

|  |  |
| --- | --- |
| **Email Address**  | **Involvement of Email Address** |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

D4. Malicious Files (Required if surfaced from the incident)Please provide information on the malicious files surfaced from the incident in the box below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Filename** | **Size** | **MD5 hash** | **Technical Analysis (Yes/No)** |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Choose an option. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Choose an option. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Choose an option. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Choose an option. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Choose an option. |

D5. Please provide an assessment of the sectoral situational awareness. (This section is applicable to AC(s) only)Click here to enter text. |

1. See Section A4 below. [↑](#footnote-ref-1)
2. Sector Leads would have been appointed Assistant Commissioners of their respective sectors. [↑](#footnote-ref-2)