NIS 2: Submission of IP range details

- Under the obligations of the NIS 2 Directive, entities governed by the regulatory framework must submit to the supervisory authority information on all of the entity's public IP ranges.

- Reporting IP addresses enables the proactive detection of vulnerabilities, cyber threats, and insecurely configured communication networks and information systems in organizations subject to the NIS2 Directive. These findings are reported to the organization, which improves the ability of the relevant parties to protect themselves against the exploitation of vulnerabilities and cyber threats. In Finland, the measures are handled by the CSIRT unit of the Finnish Transport and Communications Agency, which has the right to receive information from the supervisory authority about the list of entities (Cybersecurity Act, Section 41).

- The IP addresses to be reported include the organization's own public IP address ranges. The intention is therefore not to report the IP address ranges of any potential customer organizations. It is also not appropriate to report dynamic IP addresses that change frequently.

- To ensure that the support measures are as effective as possible, we encourage organizations to provide additional clarifying information about their IP address ranges in the form, if possible.

- If the entity's IP ranges are managed by another party, such as a telecommunications operator or some other service provider, the entity governed by the regulation must obtain the IP address information and submit it to the supervisory authority.

- IP address: A numerical code identifying a data processor, data transmission equipment or a network connection connected to the internet, e.g. 198.51.100.34.
- IP range: An IP range comprising a set of public network addresses (IP addresses).

- IP ranges must be submitted for the list of NIS2 entities in the following format:
    - e.g. 198.51.100.0–198.51.100.255 or 93.190.96.0-93.190.103.255 (IP range)

    or

    - e.g. 198.51.100.0/24 or 93.190.96.0/21 (CIDR format)
    - If necessary, the information may also be provided as individual IP addresses if a wider range is unknown: e.g., 198.51.100.34
    - The information may also be submitted in IPv6 format: e.g.
      2001:db8:3333:4444:5555:6666:7777:8888
      2001:0db8:3333:4444:0000:0000:0000:0000/64 (CIDR format)

- PLEASE NOTE: The following networks are private networks, i.e. internal address ranges, and should not be submitted to the list of entities:

    - IPv4:

    10.0.0.0-10.255.255.255 or 10.0.0.0/8
    172.16.0.0-172.31.255.254 or 172.16.0.0/12
    192.168.0.0-192.168.255.255 or 192.168.0.0/24

    - IPv6:

    fc00::/7
    fec0::/10

- To gather the information required, we recommend that you contact your own IT administration of service provider.

- Entities within the scope of the NIS 2 Directive must notify any changes to the IP address information submitted to the supervisory authority without delay, and, in any event, within two weeks of the date of the change.