Notifying to Fimea's NIS2 entity list

Use this form to notify an entity you represent to Fimea's NIS2 entity list.

Basic information of the entity

Name of entity *		Business ID *
Street name * Enter the official address of the entity reported to the Trade Register.		Street number *
City		Postal code *
PO Box	PO Box postal code	Country
Entity's email address * Enter the email address where the contact person responsible for cybersecurity can be contacted on weekdays between 8:00 and 16:15.		
Entity's phone number * Enter the phone number where the contact person responsible for cybersecurity can be contacted on weekdays between 8:00 and 16:15.		

Information about the entity's sector

Cybersecurity legislation (NIS2) applies to several sectors. Fimea supervises the implementation of the obligations laid down in cybersecurity legislation in certain sectors of health and manufacturing in Finland. Select the sector information describing the entity you represent. You can select several sectors, sub-sectors and entity types.

The health sector includes entities involved in manufacture of basic pharmaceutical products, entities involved in manufacture of pharmaceutical preparations, entities involved in research and development of medicinal products, pharmacies, blood establishments, entities supplying and providing medicinal products and medical devices in accordance with the EU Directive on the application of patients' rights in cross-border healthcare (2011/24/EU), and entities manufacturing medical devices considered critical during a serious public health threat.

The manufacturing sector includes manufacturers of medical devices and in vitro diagnostic medical devices.

Sector:

- ☐ Health: Entities involved in manufacture of basic pharmaceutical products
- ☐ Health: Entities involved in manufacture of pharmaceutical preparations
- ☐ Health: Entities involved in research and development of medicinal products
- ☐ Health: Pharmacies
- ☐ Health: Blood establishments
- ☐ Health: Entities supplying and providing medicinal products and medical devices in accordance with the EU Directive on the application of patients' rights in cross-border healthcare (2011/24/EU)
- ☐ Health: Entities manufacturing medical devices considered critical during a serious public health threat
- ☐ Manufacture: manufacturer of medical devices and in vitro diagnostic medical devices

Other operational information

The obligations of cybersecurity legislation (NIS2) apply to entities that meet the criteria of either an essential entity or an important entity.
Learn about the criteria for essential and important entities.

Essential or important entity? *

Select whether the entity you represent is an essential entity or an important entity. If the entity you represent is involved in several sectors supervised by Fimea and its activities are ones that partly match the definition of an essential entity and partly other activities, the entity you represent is considered an essential entity.

- [ ] Essential entity
- [ ] Important entity

Justification why an essential or important entity *

Select the option that you think best describes your activities.

- [ ] The entity I represent is a large entity in the health sector (Annex I)
- [ ] The entity I represent is a large entity in the manufacturing sector (Annex II)
- [ ] The entity I represent is a medium-sized entity in the health sector (Annex I)
- [ ] The entity I represent is a medium-sized entity in the manufacturing sector (Annex II)
- [ ] The entity I represent is the sole service provider in a Member State of a service that is essential for the maintenance of critical societal and economic activities
- [ ] Disruption of the service provided by the entity I represent could have a significant impact on public safety, public security or public health
- [ ] Disruption of the service provided by the entity I represent could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact
- [ ] The entity I represent is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State
- [ ] The entity I represent is an entity identified as a critical entity under the CER Directive

Does the entity you represent participate in a voluntary cybersecurity information-sharing arrangement? *

The NIS2 Directive requires supervised entities to notify their participation in voluntary cybersecurity information-sharing arrangements referred to in the Directive. Voluntary information-sharing arrangements referred to in section 23 of the Cybersecurity Act include cooperation with the CSIRT unit of Traficom's National Cyber Security Centre in information exchange groups involving the voluntary sharing of cybersecurity information. Voluntary information-sharing arrangements are also considered to include an entity joining a sector-specific mailing list maintained by the CSIRT unit of Traficom's National Cyber Security Centre. All entities subject to the Cybersecurity Act can join a list. Posts sent to these mailing lists include information security bulletins related to each specific sector.

- [ ] No
- [ ] Yes

The EU Member States where the entity you represent provides services falling within the scope of cybersecurity legislation *

Select the EU Member States where the entity you represent provides services in sectors supervised by Fimea. Fimea supervises the implementation of the obligations laid down in cybersecurity legislation in certain sectors of health and manufacturing in Finland. For companies belonging to a group, each entity in a relevant sector uses the mandate of its business ID to report itself to the NIS2 entity list for the scope of its activities in Finland.

☐ The Netherlands	☐ Cyprus	☐ Sweden
☐ Belgium	☐ Latvia	☐ Germany
☐ Bulgaria	☐ Lithuania	☐ Slovakia
☐ Spain	☐ Luxembourg	☐ Slovenia
☐ Ireland	☐ Malta	☐ Finland
☐ Italy	☐ Portugal	☐ Denmark
☐ Austria	☐ Poland	☐ Czech Republic
☐ Greece	☐ France	☐ Hungary
☐ Croatia	☐ Romania	☐ Estonia

Public IP ranges *

Report the public IP ranges of the entity you represent in one of the following formats: As an IP range (e.g. 198.51.100.0–198.51.100.255 or 93.190.96.0–93.190.103.255) or as CIDR (e.g. 198.51.100.0/24 or 93.190.96.0/21). You can also report the information as single IP addresses if the wider range is not known (e.g. 198.51.100.34) or as IPv6 (e.g. 2001:db8:3333:4444:5555:6666:7777:8888). NOTE! Do not enter any internal address ranges in this field. For example, the following networks are so-called private networks, which are internal address ranges: IPv4: 10.0.0.0-10.255.255.255 or 10.0.0.0/8 IPv6: fc00::/7.

Note! Send the PDF form as secure mail to: NIS2-CER@fimea.fi. Instructions for using Fimea's secure mail can be found on the website: https://fimea.fi/en/about_us/contact_information/secure-mail.

In the event of a change in the information submitted for the entity list, the entity must notify the change without delay, at the latest within two weeks. Entities also have to submit a notification if they no longer meet the criteria of an essential or important entity or if the entity has ceased its activities.

For support, contact NIS2-CER@fimea.fi.