Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity

The NIS Directive is the first EU-wide legislation on cybersecurity. The objective of the Directive is to achieve evenly high level of security of network and information systems across the EU, through:

1. Improved cybersecurity capabilities at national level;
2. Increased EU-level cooperation;
3. Risk management and incident reporting obligations for operators of essential services and digital service providers.

As part of the cybersecurity package adopted in September 2017, the Commission issued the Communication "Making the Most of the Directive on Security of Network and Information Systems" to assist Member States with guidance and best practice examples as well as to ensure a harmonised transposition of the new rules.

According to the Directive, all Member States need to adopt a **national strategy on the security of network and information systems** (NIS Strategy) defining the objectives and appropriate policy and regulatory measures. The strategy should include:

- Strategic objectives, priorities and governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Awareness raising, training and education
- Research and development plans related to NIS Strategy
- Risk assessment plan
- List of actors involved in the strategy implementation

Member States have to designate at least one **national competent authority** to monitor the application of the NIS Directive at national level and to nominate a **single point of contact** to liaise and ensure cross–border cooperation with other Member States. Additionally, the Member States need to appoint at least one **Computer Security Incident Response Team** (CSIRT). The CSIRTs role is to:

- monitor incidents at national level;
- provide early warning, alerts and information to relevant stakeholders about risks and incidents;
- respond to incidents;
- provide dynamic risk and incident analysis and increase situational awareness;
- participate in a network of the CSIRTs across Europe.

The European Commission supports Member States financially to increase their operational capabilities through the Connecting Europe Facility (CEF) – a key EU funding instrument for cross-border infrastructures in digital sectors. The CEF programme is providing €6.3 million in funding for the cooperation and information sharing platform for the Computer Security Incident Response Teams (CSIRTs), known as MeliCERTes. €18.7 million are allocated from the CEF programme for cybersecurity projects increasing capabilities of the CSIRTs between 2017 to 2020 (for example, for purchasing software tools, or covering the costs of trainings and exercises).

CEF funding is additionally being opened up to other stakeholders concerned by the NIS Directive – namely operators of essential services, digital service providers, single points of contact and national competent authorities with a further €13 million being available to those who apply under the next call for proposals from May to late November this year.

The NIS Directive established a **cooperation group that** is chaired by the Presidency of the Council of the European Union. The group gathers representatives of the Member States, the Commission (acting as secretariat) and the European Union Agency for Network and Information Security (ENISA). This cooperation group facilitates strategic cooperation and exchange of information among Member States and helps develop trust and confidence. The cooperation group has met six times to date starting from February 2017.

The Directive also established a **Network of the national Computer Security Incident Response Teams** (network of CSIRTs), to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

The group is chaired by a representative of the Member State holding the Presidency of the Council of the EU. It operates by consensus and can set up sub-groups to examine specific questions related to its work. The Commission provides the secretariat of the cooperation group.

The group works on the basis of **biennial work programmes**. Its main tasks are to steer the work of the Member States in the implementation of the Directive, by providing guidance to the Computer Security Incident Response Teams (CSIRTs) network and assisting Member States in capacity building, sharing information and best practices on key issues, such as risks, incidents and cyber awareness.

The Cooperation Group has so far produced, for example, non-binding guidelines on the security measures and the incident notification for operators of essential services.

Every one and a half years the group will provide a report assessing the benefits of the cooperation. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

How does the CSIRTs Network function?

The network is composed of representatives of the Member States' CSIRTs

(Computer Security Incident Response Teams) and CERT–EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). The Commission participates in the CSIRTs Network as an observer. The European Union Agency for Network and Information (ENISA) provides the secretariat, actively supporting the cooperation among the CSIRTs.

Two years after entry into force of the NIS Directive (by 9 August 2018), and every 18 months thereafter, the CSIRTs Network will produce a report assessing the benefits of operational cooperation, including conclusions and recommendations. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

More intense coordination in the netowork could be seen already mid-2017 during the Wannacry and Non-Petya ransonware attacks.

What are operators of essential services, and what will they be required to do?

Operators of essential services are private businesses or public entities with an important role to provide security in healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply.

Under the NIS Directive, identified operators of essential services will have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority.

The security measures include:

- Preventing risks
- Ensuring security of network and information systems
- Handling incidents

How will Member States identify operators of essential services?

Member States have until 9 November 2018 to identify the entities who have to take appropriate security measures and to notify significant incidents according to the following criteria criteria:

(1) The entity provides a service which is essential for the maintenance of critical societal and economic activities;

(2) The provision of that service depends on network and information systems; and

(3) A security incident would have significant disruptive effects on the essential service.

Which sectors does the Directive cover?

The Directive covers operators in the following sectors:

- Energy: electricity, oil and gas

- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare settings
- Water: drinking water supply and distribution
- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries

What kind of incidents should be notified by the operators of essential services?

The Directive does not define threshold of what is a significant incident requiring notification to the the relevant national authority. Three parameters that should be taken into account regarding the notifications are:

- the number of users affected;
- the duration of the incident;
- the geographic spread.

What are digital service providers and do they have to notify cyber incidents?

The NIS Directive covers:

- Online marketplaces (that allow businesses to make their products and services available online)
- Cloud computing services
- Search engines

All entities meeting the definitions will be automatically subject to the security and notification requirements under the NIS Directive. Micro and small enterprises (as defined in Commission Recommendation 2003/361/EC) do not fall under the scope of the Directive.

What are the obligations for digital service providers?

Digitial service providers covered by the NIS Directive are required to take appropriate security measures and to notify substantial incidents to the competent authority.

Security measures are similar to those undertaken by the operators of essential services and cover the following:

- Preventing risks
- Ensuring security of network and information systems
- Handling incidents

The security measures taken by digital service providers should also take into account some specific factors defined in the 2018 Commission implementing regulation:

- security of systems and facilities: a set of policies to manage the risk posed to the security of DSPs, which can be aimed at facilitating

technical IT security as well as physical and environmental security or the security of supply and access control;
- incident handling: measures taken to detect, report and respond to cybersecurity incidents and assess their root causes;
- business continuity management: the capacity to be adequately prepared with the ability of minimise impacts on services and to quickly recover from cyber incidents.
- monitoring, auditing and testing: regular checks to assess anomalies, verification that risk management measures are in place and that processes are being followed.
- compliance with international standards, for example, those adopted by international standardisation bodies (e.g. ISO standards).

What kind of incidents will be notifiable by the digital service providers?

The Directive defines five parameters that should be taken into consideraton, as specified by the Commission in its 2018 implementing regulation:

- Number of users affected: users with a contract in place (especially for online marketplaces and cloud computing service) or habitually using the service (based on previous traffic data);
- Duration of incident: the period of time starting when a digital service is disrupted until when it is recovered;
- Geographic spread: the area affected by the incident;
- The extent of the disruption of the service: characteristics of the service impaired by an incident;
- The impact on economic and societal activities: losses caused to users in relation to health, safety or damage to property.

The implementing regulation specifies four situations in which digital service providers are required to notify the relevant national competent authority or CSIRT, notably:

- If the digital service is unavailable for more than 5 million user-hours in the EU;
- If more than 100,000 users in the Union are impacted by a disruption;
- If the incident has created a risk to public safety, public security or of loss of life;
- If the incident has caused material damage of more than €1 million.

This list may be reviewed on the basis of guidance issued by the cooperation group, which will take into account the experience gained through the implementation of the NIS Directive.

What is the timeline for implementation of the Directive?

Member States have time until 9 November 2018 to identify businesses operating in their territory as “operators of essential services” – i.e. private businesses or public entities with an important role for the society and economy operating in critical sectors that will have to comply with security requirements and notify to national authorities significant incidents. The Commission will regularly update the overview on the state-of-

play of transposition in each Member State on its website.

For More Information

Joint statement by Vice-President Ansip and Commissioners Avramopoulos, King and Gabriel

---

Fatality notice: MOD confirms the death of Corporal Steven Wainwright

Corporal Steven Wainwright with his family.

Corporal Steven Wainwright died on Tuesday 1 May after being involved in a road traffic collision on the Akrotiri Sovereign Base Area in Cyprus. The incident is under investigation.

Cpl Wainwright enlisted into the RAF in 2006. Following successful completion of basic training at RAF Halton he went on to complete trade training at RAF Cosford (formally the Defence College of Aeronautical Engineering (DCAE)), graduating in October 2006. He then undertook his first posting to RAF Kinloss, working as part of the Nimrod Line Squadron until July 2008. Upon completion of his Trade Ability Tests, he was promoted to Senior Aircraftman in December 2006. Following his first tour, he returned to DCAE Cosford for

further training to qualify as a Technician, where he was subsequently assigned to RAF Marham to support Tornado operations. He remained there until December 2012 when he was posted to No. 6 Squadron, RAF Leuchars until June 2014. He then moved with the Squadron as part of a rebasing programme to RAF Lossiemouth where he has served ever since. He was successful on his trade promotion board for the rank of Cpl in October 2017.

Group Captain Andrew Dickens OBE, Commanding Officer 903 Expeditionary Air Wing said:

> Our deepest condolences go to Cpl Steven Wainwright's family and friends at what is a terrible, tragic time. He was a popular member of No. 6 Squadron, who are currently deployed as part of 903 Expeditionary Air Wing based at RAF Akrotiri in Cyprus. As a highly skilled aircraft technician, Cpl Wainwright was making a key contribution to Operation Shader in ensuring Typhoon aircraft could complete the challenging mission against Daesh. Cpl Wainwright was a dedicated professional who had served his country with distinction. All our thoughts are now with Cpl Wainwright's family, friends and colleagues as they come to terms with his tragic death.

Wing Commander William Cooper, Officer Commanding No. 6 Squadron said:

> Cpl Wainwright was an unfailingly professional technician who had an incredible passion for his family, his work and life in the Royal Air Force. He was a man who motivated and lifted everybody he interacted with at RAF Lossiemouth, especially on No. 6 Squadron. A fighter squadron is a very tight unit and Cpl Wainwright embodied all the qualities to make that possible. He was a mentor to those both more senior and more junior and by sheer force of personality produced results in people others could not.
>
> No task was too daunting or too challenging, he took adversity in his stride and, as a result, No. 6 Squadron is a far happier place and more effective fighting unit. Every job, every aircraft see-off, every mentoring role was conducted with the same cheery personality and calm professionalism. Unwavering dedication to operations was typical of Cpl Wainwright, be that at home on Quick Reaction Alert or overseas on Operation Shader. His shoes cannot be filled and he will be greatly missed by everybody on No. 6 Squadron, the thoughts of all of us on are with Cpl Wainwright's family at this incredibly difficult time.

Squadron Leader Chris Harris, Senior Engineering Officer No. 6 Squadron said:

> Always with a smile to share, even at the end of the hardest night shift, Steve was renowned for picking up morale with his infectiously positive approach to life. This unwaveringly positive

> determination transferred into his outstanding professional dedication, where he took justifiable pride in being one of the best engineers on the Squadron. Steve Wainwright was one of the first people I met on the Squadron, his characteristic good humour evident in our very first discussion where he introduced himself with his typical comedic style. Respected and admired across every trade on No. 6 Squadron and beyond, Steve will be sorely missed by all and our thoughts are with his family at this time.

Warrant Officer David Clegg, No. 6 Squadron Detachment Warrant Officer said:

> Full of charisma and highly respected by everyone, Stevie was an exceptionally friendly individual with a great sense of humour. As an aircraft engineer, he was one of the best and it was an absolute pleasure to work alongside him. His affectionate nature and loveable character shone through in everything he achieved and he will be sadly missed by all. Our thoughts are with his family at this sad time.

Group Captain, Jim Walls, Station Commander RAF Lossiemouth said:

> Cpl Wainwright was a member of our family here at RAF Lossiemouth, we all feel his loss deeply. He was a highly skilled individual who was a key part of our team. I always enjoyed the gift of his upbeat attitude. I particularly respected him for his values and approaches as a family man. We are all thinking of his loved ones at this tragic time.

Press release: Blitz on illegal fishing for Bank Holiday Weekend

The officers will work with the police and Angling Trust Voluntary Bailiffs to make sure anyone fishing is obeying the law including fishing in waters that are open to anglers, using the right tackle and equipment, and having a valid fishing licence.

Bank Holiday weekends are a great opportunity for families to get out and do some fishing on our waterways and the Environment Agency is keen to ensure everyone is enjoying themselves and doing the right thing.

Kevin Austin, Deputy Director Agriculture, Fisheries and the Natural Environment, Environment Agency said:

> The Environment Agency conducts enforcement operations throughout the year to protect fish stocks and improve fisheries.
>
> Our enforcement officers, Angling Trust Voluntary Bailiffs and police are out there to make sure everyone is fishing legally this weekend. Anyone caught can expect to face prosecution.
>
> Our work is intelligence-led, meaning we target known hotspots and act on reports of illegal fishing.

Is your local fishing spot open for fishing?

Anglers are reminded that it is currently the closed season for coarse fishing and fishing for coarse fish on rivers and streams is not permitted.

This is done to protect breeding fish, helping to safeguard stocks for the future. However, there are still plenty of places anglers can wet a line.

Anglers are encouraged to check which waterways are open to fishing. They can visit fishinginfo to find more information.

There are nearly 500 Angling Trust Voluntary Bailiffs doing a great job keeping watch on their local rivers and working alongside local police. However, the Environment agency is also asking the public to report any suspicious activity.

Money from rod licence sales is invested in England's fisheries, and is used to fund a wide range of projects to improve facilities for anglers including; protecting stocks, restoring fish stocks through restocking, eradicate invasive species, and fish habitat improvements. Fishing licence money is also used to fund the Angling Trust to provide information about fishing and to encourage participation in the sport.

You can check local fishing byelaws and get your fishing licence direct from GOV.UK

People are urged to report illegal fishing to the Environment Agency's incident hotline on 0800 807060, or Crimestoppers anonymously on 0800 555 111.

Press release: Dstl analysts support

Europe’s largest military exercise

A team of analytic specialists from Dstl are providing vital analysis to support military commanders in Europe’s largest military exercise, Exercise Joint Warrior. Lead by the UK’s Ministry of Defence (MOD), Exercise Joint Warrior is a multi-national military training exercise which takes place in the UK, predominately in the north-west of Scotland and on Salisbury Plain.

Dstl’s guidance is crucial for military leaders to understand the risks and benefits of the decisions they make when planning tactical activities and maneuvers during conflict.

Thousands of military personnel take part in the exercise from across the UK services, as well as those from NATO and other allied countries. It involves 38 naval vessels, 68 aircraft and a large number ground units. Operations include airborne assaults, amphibious landing and training in counter-insurgency, counter-piracy and interstate warfare.

Among the team of analysts from Dstl is Richard Hoyes, he said:

> Seeing your hard work and analysis influence a commander’s decisions is great; though, clearly there is a serious edge to all of the work involved; it is also good fun. At the start of the exercise I was in an airfield with hundreds of paratroopers who were prepping to deploy as per a real conflict. There were a lot of helicopters and fast jets; it all makes for a very meaningful and realistic experience.

The team is among more than 30 members of Dstl staff who are trained and ready to deploy anywhere in the world in support of military operations and exercises; all at a moment’s notice.

Richard added:

> On this joint operation, the Army, RAF and Navy work together as a team. You can gain great insight into a breadth of capabilities due to the fascinating mix of cultures with the likes of Danish, Lithuanian and Latvians among the nationalities working alongside UK personnel. This is the second exercise of this type that I have done and I have already developed working relations with other nations. It shows how seamlessly these nations can integrate together and fight side by side.

Dstl also has a 24-hour, 365-day ‘reachback’ capability, which provides rapid access to the breadth and depth of Dstl’s capabilities in support of military operations, not just with analysis but could include anything from computer modelling and highly detailed scientific advice to a review of previous

research studies for similar issues.

For more information contact the Dstl press office on 01980 956845 or at press@dstl.gov.uk

---

Press release: North East man fined for illegally burning waste

Mark Anthony Walsh, 57, of Maidstone Drive, Marton, Middlesbrough, appeared at Peterlee Magistrates' Court on Wednesday, 2 May, where he pleaded guilty to burning waste at Thorpe Larches in Sedgefield.

He was fined £5,800, ordered to pay £2,000 in costs and a victim surcharge of £80.

Prosecuting on behalf of the Environment Agency, Simon Crowder told the court that on 5 December 2016, the Environment Agency received information from Durham County Council about possible waste burning taking place on land at Beechgrove at Thorpe Larches in Sedgefield.

The following day two Environment Agency enforcement officers went to the property and spoke to Walsh, who said he had been burning waste packing which he had produced as a result of renovations on his own property. They left information with Walsh about the Environment Agency role and powers but did not see any evidence of burning.

In February 2017, the council contacted the Environment Agency to say they had received further complaints about burning waste at the land.

In March 2017, they received further information about fires at the address and attended the scene on two occasions. During one of the visits they saw no one was present with the fire. The waste pile was estimated to measure 5m by 2.5m and contained partially burnt household items along with a plastic wheelie bin, tin cans, garden waste, waste paper, metal springs and household electrical items.

During interview on 4 May that year Walsh said he only burnt bedding from the pig sty. Paul Whitehill, from the Environment Agency in the North East, said:

> The evidence, including images and visits by our enforcement officers, shows Walsh burning waste on his land illegally.
>
> Environmental laws are there to protect the environment and community and Walsh deliberately flouted those laws, putting the environment at risk. I'd encourage people to report waste crime to us so that we can investigate and take any necessary action.

Waste crime can be reported to the Environment Agency on 0800 807060, or Crimestoppers anonymously on 0800 555 111.