President of the National Assembly, Chair of the Committee, Minister(s), Members of Parliament,

I would like to thank you for this invitation to speak but also wish to thank you for organising a dedicated session on the resilience of critical infrastructure in the EU. I'm delighted to present to you today, it is a timely debate and given the Agency's key role in making Europe more cyber secure and in combatting cyber threats.

Landscape and challenges

2020 saw an alarming rise in cyber incidents globally. Within the EU, the percentage of reported incidents with a significant impact increased by 72% from 2019 to 2020. What we are seeing is that cyber incidents are becoming more sophisticated and complex.

The ransomware attack on the Irish Health Services in May of this year proved to be a real example of this increase and carries important lessons learnt, not only at the national but also at EU level. It was a national level incident that could happen in a similar manner in another Member State. It represents a good example of how to manage a crisis and illustrates the issues at stake in an incident of this scale.

Looking specifically at the critical sectors such as health we saw a rise in cyber incidents even before 2021. The reported 2020 incidents in the health sector increased by 47% from 2019.

The NIS Directive was the first European wide cybersecurity legislation, which Member States had to transpose into national legislation in 2018. Therefore the figures just mentioned for 2019 are from the first annual incidents report. It included big differences between number of reports between similar sized Member States (Found online in an interview with SLOV MB member: There are slightly more than 20 entities under NIS1 in Slovenia, while there are 10,000 in Finland). The differences in reporting across Member States poses a challenge to understanding the true number of cyber incidents and attacks in the EU.

Although the directive is bearing its first fruit; we have also noted gaps such as the incident reporting that have appeared since the directive was negotiated. Last December the Commission proposed to review the directive. From the point of view of the Agency, we welcome this proposal as it is necessary to amend a number of areas.

Opportunities

1. **scope**

It emphasises the need to review the **scope** of the NIS directive, which should be expanded in order to counter prevent and counter cyberattacks where they appear in our critical infrastructures The digitalisation of the economy and society means that many more entities provide key services but also that they are increasingly interconnected. By obliging more entities to fall under the scope, we can elevate the overall cybersecurity level across Europe.

It is crucial that we not only expand the scope of the directive in terms of the size of entities to also cover mid-sized players, but that we include new sectors (such as pharmaceutical, cloud computing service providers, data centres, food manufacturers, wastewater etc) into the definition of essential or important service providers.

There is also a need to harmonise the methodology used where possible to become more effective and attain better comparability. Streamlining entities' cybersecurity obligations would improve accountability and incentivise information sharing especially across borders.

Cooperation

Looking at the cyberattacks on the Irish health services, we saw that all layers were involved, the technical and operational layer but also the political and there are several lessons that could be translated into policies to build further resilience.

We need to ensure that also Member States with less capacities have the capabilities to tackle cyber incidents and crises. Increased **cooperation** including information exchange across borders and levels is necessary and beneficial to all Member States. The NISD2 envisions the institutionalisation of CyCLONe, which supports cyber crisis management authorities in increasing the level of preparedness to deal with large-scale incidents, develop a shared situational awareness, coordinate crisis management and support decision-making at political level.

2. **Investment**

The third opportunity the review of the directive brings is to raise of level of cybersecurity **investment**. Investment in cybersecurity remains low. EU organisations allocate on average 41% less to information security than their US counterparts. The EU Recovery plan offers a way out by investing in targeted

areas that will improve cybersecurity but also foster a robust cybersecurity market.

NIS directive 2 proposal introduces accountability for top management for non-compliance with cybersecurity measures. This is important to incentivise that especially operators of essential services like hospitals invest in cybersecurity. However, it is up for national budgetary authorities to demand more investment into cybersecurity within their national cybersecurity strategies.

Role of ENISA

The Cybersecurity Act sets the mission of ENISA, as EU Agency for Cybersecurity to achieve a high common level of cybersecurity across the Union.

We have a global shortage of cybersecurity professionals and this affects operators of essential services, the private as well as the public sector. ENISA's Cybersecurity Higher Education Database (CyberHEAD) is the largest validated cybersecurity higher education database in the EU. This along with the Cybersecurity Skills Framework and the cybersecurity competitions for young people aim to support Member States to enhance cybersecurity skills and competence across at all levels.

At the same time, we need to progress from strengthening resilience towards shaping the future and making sure that the technologies of tomorrow are secure. Research and innovation are key to be able to rely on a strong and leading European industry base in more areas of the digital economy – including cybersecurity. Alongside (pillar one, the NIS Directive and 2, the Cybersecurity Act) the EU Cybersecurity Competence Centre and the Network of National Coordination Centres will become the third pillar of European cybersecurity and one to which ENISA will contribute extensively.

Conclusion

Thank you to the Slovenian Presidency for this opportunity to speak to you today, I look forward to visiting your capital in September for the Cybersecurity Conference and hope to meet with all of you for this occasion.

I would also like to thank our Slovenian Management Board member, Uroš Svete and National Liaison Officer, Ivana Boštjančič Pulko for their dedication to strengthening cybersecurity in the EU.

I would like to thank again the chair for this opportunity to present the European Agency for Cybersecurity and put forward its views. It is a duty of the European administration to report to and assist the European legislators, and I welcome the opportunity to speak on these important matters to your respective national parliaments.