Alliance for Internet of Things Innovation

Brussels, 11 March 2021

AIOTI Feedback to the Public Consultation on the revised draft NIS Directive (NIS2)[1]

I. INTRODUCTION

a. Security of and related to IoT ecosystems is one of the main trust components that AIOTI is and has been focussing on since it was founded. A substantial part of IoT ecosystems are already, or will become part of critical infrastructure, vital systems and essential services.

b. IoT is one of the main areas where physical and digital realities meet. Thus, the relationship between IoT and cybersecurity is crucial from the security point of view where a holistic perspective that includes a joint approach to physical, cyber-physical and digital security is required.

c. On 16 December 2020 the Commission adopted the proposal for a revised Directive on Security of Network and Information Systems (NIS2 Directive). The rationale behind the revision is to address deficiencies and limitations in its predecessor, the NIS Directive, both as per the dynamic pace of digital transformation which has broadened the take up of cloud, edge and IoT capabilities, the related expansion of the attack surface for adversaries and increasingly complex threat landscape, which requires more adaptive and innovative responses as well as without limitation that despite progress under EU rules, cybersecurity capabilities across the EU remain unequal and otherwise result in insufficient protection against cyber threats.

d. AIOTI therefor supports the intended objectives a revised draft NIS2 Directive, welcomes the possibility to provide feedback, and in the following paragraphs will expand on areas of the proposals that would require further clarification and that can otherwise further improve the current proposals in order to be able to achieve and continuously sustain the appropriate level of security in critical infrastructure, vital systems and essential services in general, and IoT security in particular.

e. Regarding IoT Security, in 2016 and 2017 AIOTI together with the Commission, ENISA and other relevant AIOTI members and other stakeholders has organised two workshops in which these and related topics has been extensively discussed and resulted in outcomes as published in two reports, which are encouraged to be taken good notice of and form the basis of the observations made below.[2]

II. MAIN OBSERVATIONS

Horizontal, Cross-cutting & cross-sectorial

1. There is a need for a horizontal, cross-cutting & cross-sector approach. Sectors are not isolated or otherwise silo-ed, and as per the ongoing and expediting convergence become more and more interconnected and hyperconnected, bringing greater opportunities, cross-fertilisation on best practices, data and intelligence sharing, but on the other end also augment known and unknown threats and vulnerabilities when they arise.

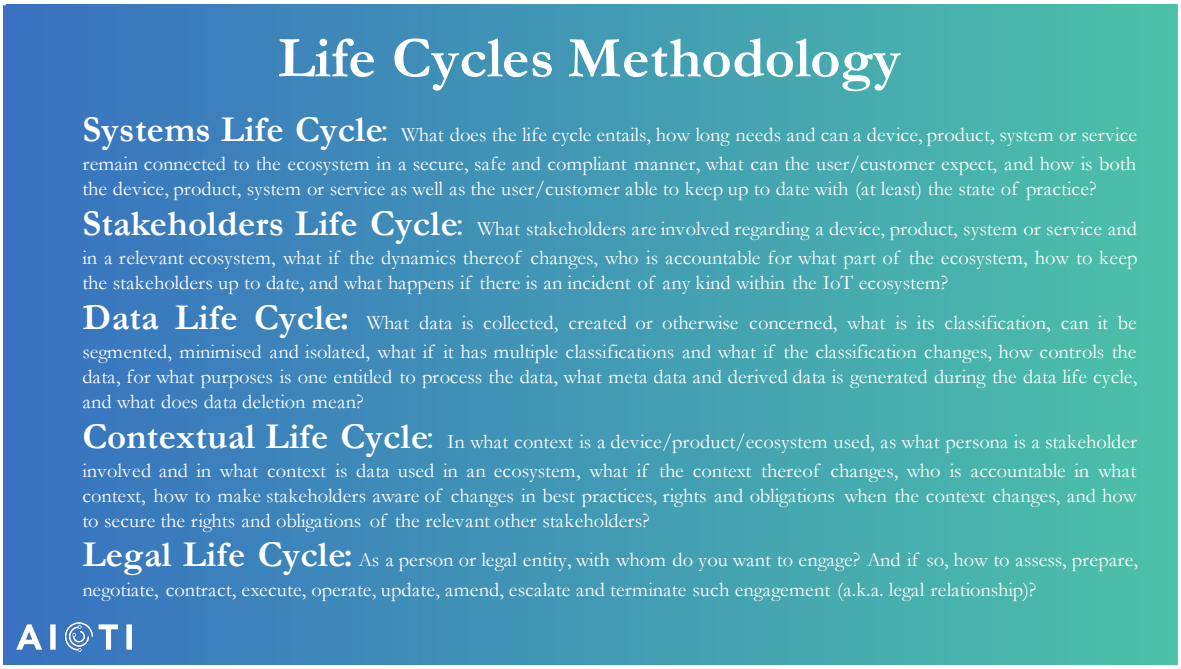
[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive

[2] AIOTI Workshop on Security and Privacy in IoT of 16 June 2016: https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week;
Final Report Workshop on Security and Privacy in IoT of 16 June 2016: https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf;
Final Report European Commission of 13 January 2017 Workshop on Internet of Things Privacy and Security: https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report

2. Ecosystem thinking, end-to-end, holistic and data-centric, is a prerequisite. For instance the harmonization of 'identification' in different critical, vital or essential IoT ecosystems is necessary. This is for instance particularly important in healthcare, (commercially of the shelf or other) wearables used in healthcare and other critical infrastructures and vital systems, and in mobility (vehicle-to-vehicle communication) and UAVs (whether transporting people or goods, proving incident support, or sensing or performing inspection tasks) within these critical, vital respectively essential physical, cyber, cyber-physical domains. In this context, possible uses of IoT devices in safety-critical and liability-critical systems need to be properly considered.
3. As NIS2 is devoted to networks and systems, it is essential to note that IoT is one of the links of the digital world with the physical one, being combination of the cyber-physical and physical worlds. Therefore, IoT is where cybersecurity meets security and safety - also within the context of the current NIS Directive as well as the NIS2 Directive - and both have to be addressed from an integral perspective. Cybersecurity threats can impact in the real world through IoT systems and physical actions over IoT can be part of cybersecurity attacks. Said otherwise, this creates or otherwise extends and augments the attack surface where AIOTI has been actively contributing already as mentioned in the introduction, and will further contribute.
4. The current NIS Directive requires Member States to identify operators of essential services as well as digital service providers within a certain timeframe. As was evidenced by the Impact Assessment Report published by the European Commission in June 2020, several Member States failed to do so which ultimately resulted in 'significant inconsistencies and fragmentation in the regulatory landscape, which undermines the level playing field for some operators and lead to further fragmentation of the single market.' Under the NIS2 Directive, additional sectors have been included which do not address the existing challenges mentioned above but rather exacerbates it.
5. Similar to the General Data Protection Regulation, the NIS2 Directive should also implement a horizontal methodology wherein it takes a risk-based, impact-based and principle-based approach to cybersecurity. By outlining basic principles as well as establishing a standard minimum threshold for security, the NIS Directive can enable organisations across different industries to implement resilient and future-proof processes and systems based on the dynamics of their organisation. Ultimately, doing so will also boost the overall level of cybersecurity in the EU (and its periphery) as envisioned by the NIS and NIS2 Directive.

Entire & Dynamic Life Cycles

6. While the NIS2 Directive has built on the gaps identified in the current NIS directive, it does not factor in the entire life cycle while dealing with cybersecurity but rather approaches it in a linear manner. In a broad sense, the security of network and information systems and its related attack surfaces and related persistent threats are dynamic and multi-dimensional. They will vary based on whether it is being tailored for conglomerates, SMEs, governmental agencies or any other organisation, and whether stand-alone, connected, interconnected or even hyperconnected. Hence, various factors need to be considered right from the design phase until - and including - the end-of-life phase.
7. Obviously, this does not imply that one sole party such as for instance an upstream manufacturer, midstream integrator or downstream customer is responsible for a whole life cycle, yet each will have its roles, (co)responsibilities and related (co)accountability with the whole life cycle in mind. The figure below (which is also further explained in the reports noted on the first page hereof) represents the different life cycles that an organisation must account for in order to take a holistic and overarching approach to cybersecurity, which have been discussed and established in various AIOTI workshops within internal and external stakeholders.



8. In addition, it is essential that the NIS2 Directive stresses the cyclical nature of designing and implementing security processes and systems given that they should not be viewed in a stand-alone manner but should be constantly re-assessed and re-aligned. It should consider functionality, performance, adaptability to emerging technologies, cost effectiveness and most importantly flexibility.
9. Cybersecurity incidents that have taken place worldwide in the last few years including the recent SolarWinds supply chain attacks[3] are a testament to how complacency can be catastrophic for a company's security processes and ultimately the company's reputation, market standing and similar for its affected customers in the public sector and private sector.
10. Hence, using approaches such as the Life Cycle Methodology given above, companies must strategically assess the efficiency of their existing processes, controls and systems in line with the different facets that impact them including technological innovation, evolving threat landscape, regulatory changes and the like.

Coherence

11. As both digital domains and dimensions have evolved since the current NIS Directive came into force, and since then multiple relevant regulations in these digital domains and dimensions have been proposed or already adopted, there should be an increased coherence between those. For instance, between the eIDAS Regulation (EUid) under development and the NIS2 Directive, vice versa.
12. The same goes for coherence with for instance the European Cybersecurity Act (CSA), Radio Equipment Directive (RED), General Data Protection Regulation (GDPR), General Product Safety Directive (GPSD), Machinery Directive, Medical Device Regulation (MDR), eIDAS Regulation (EUid), Sales of Goods Regulations (Art. 7(3)), proposed Digital Operational Resilience Act (DORA), proposed Regulation European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres or other current or upcoming or (to be revised or otherwise refitted) directives and regulations.
13. In this context, the policymakers should ensure seamless and clear application between horizontal legislative proposals and relevant lex specialis. In order to support Member States in strengthening their respective capabilities and competences, and improve (cyber)security and resilience, NIS2 should ensure that there are no overlaps or double reporting required amongst all cyber related legislative proposals, while at the same

[3] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

time acknowledging the attributes of different sectors. In this context, certain agreed parts of the NIS requirements might be extracted and put into a regulation to harmonize requirements throughout Member States as much as possible; this also to both address essential difference in implementation and operation of the current NIS Directive as well as to support Member States to strengthen their respective capabilities and competences in other to be able to implement appropriate measures, and otherwise improve (cyber)security, resilience and digital sovereignty. This would therefore not necessarily interfere with the wish of some Member States for the NIS2 Directive to remain a directive in general.

Harmonisation & International Standards

14. Next to coherence as mentioned in the previous paragraph, the importance of harmonisation and (international) standards can not be overstressed. Fragmentation is one of the main challenges, also in the various IoT security dimensions in scope of the NIS2 Directive. While different sectors may have unique cybersecurity standards, there are a set of principle-based cybersecurity measures and controls that are common across sectors. Regarding such IoT security principles and the like, reference is made to the reports mentioned on the first page hereof. These can be found in various standards, such as for instance ISO/IEC 27000 Series, IEC 62443 and other information security and other security and safety open standards and other guidelines that either already exist or are under development by ESOs and other SDOs, including without limitation the recent guidelines by OECD on digital security of products[4].
15. Furthermore, to enable security and privacy functionality while facilitating integration and interoperability of key critical infrastructure industries, open standards should be preferred, where available, for security spending and solutions.
16. Harmonisation is not necessarily a matter of coming to one standard or the like, but also to find ways to co-exist and work to strengthening each other, such as between for instance a NLF-Approach and the current CSA. For an example, a NLF-Approach does address the lifecycle more from a go-to market day perspective, than a traditional certification approach because it does only look at the timeframe of the certification; a NLF-Approach using standards looks at the whole product life and takes the manufacturer accountable for it.
17. Collaboration as part of the harmonization approach may include sharing positions and ideas with international stakeholder also working on future cybersecurity requirements like the US Cyberspace Solarium Commission[5] (of which 27 of its recommendation have been put into law in January 2021[6]), Japanese METI or Indian TEC[7].
18. Also, guidance for harmonisation and implementation of crypto frameworks across the whole digital landscape is required, for instance regarding:
    a. Aligned cybersecurity and other standards for implementation of CSA, NIS2 Directive, NLF and other regulation for security, privacy & safety of IoT devices, mobile devices, edge computing, cloud services, data commons and data exchanges;
    b. Aligned standards for implementation of trusted crypto framework including trusted hardware and interfaces to bootstrap trustworthy implementation of the appropriate crypto protocols, key sizes and key management, lifecycle management across all architecture layers and verticals, and;
    c. Dynamic assurance to enforce the appropriate level of assurance; automation of risk-based Software Development Lifecycle (SDL)[8], Threat, Vulnerability, Risk Analysis (TVRA)[9] and continuous monitoring, including maintainability, functional suitability, performance efficiency, compatibility, usability, reliability, security, portability and trusted supply chain.

[4] http://www.oecd.org/digital/ieconomy/digital-security/
[5] Cyberspace Solatium Commission Legislative Proposals (July 2020): https://www.solarium.gov/report/legislative-proposals
[6] NDAA Update: https://www.solarium.gov/press-and-news/ndaa-override-press-release
[7] India TEC: https://www.tec.gov.in/inviting-comments-on-draft-guidelines-for-consumer-iot-security/
[8] As described In ENISA Good Practices for Security of IoT - Secure Software Development Lifecycle
[9] As described in ETSI TS 102 165-1 'CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)'

These, and the urgency to guidance, has increased as per the Covid-19 pandemic, such as for example in the healthcare sector and related sectors, including in mobility, at airports and harbours, across borders and industries.

As a result, it is encouraged the co-legislators to work towards a maximum harmonisation framework. This would contribute to legal certainty as well as to make implementation more efficient and related costs possibly lower. Such legal certainty is indispensable when covered organisation needs to respond to cyber threats effectively, quickly, and sometimes across several Member States (as per article 18 and article 20). In particular, national cybersecurity strategies preferably should be developed in a coordinated and coherent manner to avoid discrepancies and a fragmentation of the single market (as per article 5). Related hereto, the implementation as currently worded in article 21 may lead to fragmented approaches on mandating certification across EU Member States that would not strengthen the purpose of the EU Cybersecurity Act to establish a pan-EU framework for certification.

Linear is not necessarily enough

19. In line with the outcomes of the abovementioned workshops, standards or other policy instruments that have linear or otherwise process-based approach - such as for instance ISO 27001 - are good to have. However, these do not establish the dynamic and contextual appropriate levels of trust, trustworthiness, security and related end-to-end or ecosystem life cycle resilience that is required in real-life for and in critical infrastructures, vital systems and essential services. This for once as hackers and other malicious actors change their ways on a daily basis, and can easily manoeuvre around these instruments. Compliance to paper processes does not mean security in real time. The GDPR has these concepts already implemented, including in Article 32 GDPR about the requirement of state-of-the art security and related continuous dynamic accountability.
20. Therefore, also in context of the NIS2 Directive it is for once recommended to assess and refer to the European Cybersecurity Certification Framework and its certification schemes (such as the upcoming EUCS) to cover the risks from a products, services (including without limitation cloud services) and (edge, IoT and other) systems view and be able to adapt the assurance levels according to the risks. Certification to demonstrate conformity of highly critical products, services and systems shall be done on assurance level 'High' pursuant to the Cybersecurity Act to generate trust. In this context conformity assessment bodies should be taken into account to be able to leverage the European cybersecurity certification schemes also for critical infrastructures.

Emerging Threats & Opportunities

21. The development of autonomous systems, artificial intelligence, quantum computing and other emerging technologies in the broad sense of the word should be taken into account in and through the NIS2 Directive, and national, regional and Union strategies (for instance AI used to attack and to defend). This for once as the related risk and impact may be affected, either positively or negatively. This in particular taking into account the expected amount of IoT devices in critical infrastructure, vital systems and essential services, whereby such IoT devices are or may not initially be designed for use in these domains.
22. It is important to be clear about the potential risk and impact of intended, expected respectively actual use, and how to both classify those and mitigate, monitor or even eliminate these. In this context, but also related to other existing or evolving technology, the duty of care and related accountability should be added as a main principle related to cybersecurity requirements, same as in the GDPR.

Other Observations

23. **Incident notification thresholds according to definition of end users:** Industry, such as for instance certain AIOTI business members that provide technology products and services to the public and private sectors, has an acute interest in achieving high security levels for our critical information infrastructure. By expanding the scope and number of service providers classified as essential entities, the current proposal however, does not address the B2B environment whereby one essential service provider might be the client of another essential service provider. The contractual obligations of service providers in these circumstances are not acknowledged,

which could lead to legal ambiguity and overlap in reporting obligations. What is more, a business client acting as an essential entity, and that uses third-party digital servicers or digital infrastructure to serve multiple end users, would be better positioned to assess the impact and gravity of an incident than the essential entity providing the digital services or infrastructure. Under the current proposal, a cloud provider or any other digital infrastructure provider deemed as essential, would have to report to the regulator without having the necessary information or overview of end users affected. We would thus recommend to include a clarification in NIS2 similar to the one in Art. 16(5) of the NIS Directive, '[w]here an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.' In addition, liability exemptions or safe harbours for notifying incidents should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Otherwise, in a mandated reporting obligation that would go against confidentiality and contractual obligations, there is a risk of reputational loss for both the client and the digital service provider.

24. **Reporting obligations timescales:** Recital 55, and Art. 20 propose to capture in reporting not only incidents but significant potential threats or so-called near misses. Where the intent is acknowledged, it is to be considered and balanced out that decreasing the threshold to near misses may result in an overflow of notifications and possible decreased net efficiency. In addition, Art. 30 suggests narrowing the timeframe for incident reporting to 24 hours for an initial report with information strictly necessary to make the competent authorities aware of the incident. Despite the minimum amount of information required and understanding that time of the essence in certain situation, the general timescale may be too ambitious - hence too short - in view of the priority for the particular organisation(s) to first address, recover and focus on the matter at hand. Furthermore, exposing information about an incident before a patch is applied or operations restored, may in some events make organisations more vulnerable to increased hacker attacks. Thus, it is to be considered to adopt the language and timeframe similar to Art. 33 of GDPR, whereas a breach should be reported without undue delay, but no later than 72 hours. This would also ensure harmonization between the Union's legislative instruments and clarity for service providers.

25. **Oversight regime and penalties:** In line with a larger scope which classifies more service providers as essential operators, a much more intrusive oversight regime for operators of essential services is envisaged in Art.29.2. Moreover, Art 31.4 introduces on site audits and other measures with potential severe penalties (up to 2% of global turnover) for non-compliance. This is a significantly more intrusive regime than under the current Directive and other lex-specialis in other sectors, such as DORA for Financial Services, and it is therefore suggested to consider a proportionate sanction and oversight regime that would allow service providers to operate seamlessly across different sectors. In addition, there is a risk that the same incident is sanctioned for its cause under NIS2 and for its effects under GDPR.

AIOTI, Brussels, March 2021