Network and Information Systems Directive Update:
The Manufacturers’ Position
11 October 2021

1. Introduction
Where safety was the main challenge for aviation in the 20th Century, as it evolved from a new concept to a mature technology, one of the dominant challenges of the 21st Century is likely to be cybersecurity. Globally, cyber-attacks have continued to increase in frequency, sophistication and impact, and the aviation industry has felt effects both from coincidental infections and targeted attacks. To date, attacks have not had a safety impact and only affected business operations with attackers generally trying to target business interests – such as affecting operations for ransom or stealing intellectual property.

The aircraft manufacturing industry – represented by ASD – has experienced the effects of cyberattacks and has also recognised the potential for further damage to business operations and/or safety of flight and cabin crew, passengers and the public. The industry has already started to propose standards to increase the resilience of its members and suppliers. ASD members also fully support regulatory measures to ensure an acceptable level of security across aviation and to ensure a level playing field is established which would ultimately reward the good actors implementing security.

2. Problem Statement
The Network and Information Systems (NIS) Directive (EU 2016/1148), originally published in 2016, provides valuable direction in securing critical infrastructure in several defined sectors. Aircraft manufacturing is not listed as Operators of Essential Services (OES), thus is outside of scope. For the current NIS2 proposal (EC COM (2020) 823), aircraft manufacturing is proposed as an Important Entity (IE) that would be regulated similar to the OES. ASD does not believe it would be proportionate or effective to include aircraft manufacturing as an IE and would prefer that the proposed rules as defined in the European Union Aviation Safety Agency (EASA) Opinion 03/2021 on the Management of Information Security Risks (Part IS) is adopted as a lex specialis instead.

EASA’s proposed Part IS provides a holistic cybersecurity rule for the entire aviation sector with requirements for comprehensive information security management system to be implemented by all organisations covering Information Technology, Operational Technology and embedded systems such as the aircraft. The scope of Part IS extends across approvals for aviation organisations, including all Design Organisations, Production Organisations, and Maintenance, Repair and Overhaul Organisations involved in the design, production, maintenance and repair of aircraft.

About ASD
The AeroSpace and Defence Industries Association of Europe represents the aeronautics, space, defence and security industries in Europe in all matters of common interest with the objective of promoting and supporting the competitive development of the sector. Its membership comprises major European aerospace and defence companies as well as national associations.
with commercial aviation. Therefore, Part IS would include the aviation related organisations included in Annex II Important Entities, 5. Manufacturing, (f) Manufacture of other transport equipment.

The existence of two regulations applying to organisations with similar scope, intent and requirements but differing authorities for oversight, as is potentially the case for NIS2 and Part IS, will lead to significant economic friction and may be counterproductive to the intended goal of increasing cyber resilience. The regulators will interpret their respective rules differently leading to affected organisations diverting resources to create compliance material for each audit. There is also a high risk the regulators may have opposing views on compliance in some specific technical aspects, so the affected organisation would need to negotiate between the regulators to try to find a consensus opinion. Furthermore, the aviation industry has a high number of constraints on operations as a result of existing rules ensuring safety – these restrict options on some security measures that are typically utilised in other industries. With a regulator unfamiliar with the aviation ecosystem, its technologies and its constraints, organisations may be driven to take actions that contradict safe practices and rules.

3. Conclusion

The aviation industry represented by ASD has a vested interest in increasing cybersecurity resilience of aviation and is taking appropriate measures voluntarily as well as supporting applicable rulemaking tasks with EASA. The industry respectfully requests that the NIS2 Directive proposals are amended before adoption to consider future Part IS as a *lex specialis* to the NIS2 Directive. Such an amendment will increase cybersecurity resilience and effectiveness of aviation by strengthening the aviation specific oversight by EASA and the Member State National Aviation Authorities, generate clarity in rules for all stakeholders and reduce unnecessary costs and economic friction by removing duplication in rulemaking and oversight, and avoid inappropriate actions intended to increase cybersecurity.

****

*Signed by Jan Pie, Secretary General of ASD*

Brussels, 11 October 2021