Panel 1: Challenges for an integrated approach to cybersecurity risks
Different perspectives (safety, security, essential services)
S Schwindt, GE Aviation

AeroSpace and Defence Industries
Association of Europe

ASD
rue Montoyer 10 I 1000 Brussels, Belgium
info@asd-europe.org I www.asd-europe.org

Membership

17 Companies

AIRBUS
BAE SYSTEMS
DASSAULT AVIATION
FINCANTIERI
HENSOLDT
indra
KONGSBERG
LEONARDO
LIEBHERR
MBDA
NAVAL GROUP
Navantia
Rolls-Royce
SAAB
SAFRAN
THALES

23 National Associations

NIDV DEFENSIE & VEILIGHEID
ADS
BDI
AGORIA
GIFAS
AED PORTUGAL
tedae
IAD
ASSOCIATION OF FINNISH DEFENCE AND AEROSPACE INDUSTRIES
SOFF
FSi
FAD
APAI
BDLI
BDSV
AILV CZECH REPUBLIC
AOBP
WKO WIRTSCHAFTSKAMMER ÖSTERREICH ARGE Sicherheit & Wirtschaft
BDIA
SaSaD
HASDIG

Representing approximately >561 000 employees and >€126.7 bn in civil aviation

“Manufacturing” Sector

- ASD members are referred to as the manufacturing sector (approximately 5000 companies)
- Design and manufacturing of aircraft (airplanes and helicopters) and the associated equipment installed within plus ground systems for Air Traffic Management
- NIS Directive does not apply to members although some customers are subject to NIS
- Only Aviation specific regulations plus general regulations such as GDPR
- All very simple for regulatory purposes?

Organisational Approvals

- OEMs typically have minimum 3 organizational approvals:
  - Design Organizational Approval (DOA, Part 21)
  - Production Organizational Approval (POA, Part 21)
  - Maintenance, Overhaul and Repair Approval (MRO, Part 145)
- Some OEMs have additional approvals for their own airports and other services (under thresholds for OES under NIS Directive!)

Organizational Oversight

- Approvals for organizations within company granted by separate authorities:
  - POA and MRO granted by NAA (except pan-European companies such as Airbus)
  - DOA granted by EASA
- Companies and organisations are global – different sites may fall in different jurisdictions
- OEMs have oversight responsibility for their lower tier supply chain

Industry Preparedness and Response

- Historically, manufacturing industry has been very engaged
  - Developing standards both for Acceptable Means of Compliance and industry improvement
  - Discussions with regulators on promoting increased safety and better design practices
- Safety Management Systems have been existing in principle in industry before regulations
- Security auditing of supply chain is already in practce

Industry Desires

- Harmonisation and level playing field for cybersecurity in Europe and globally
  - Industry led proposals for Aviation ISMS
- Simple, economic rules
  - Acceptable Means of Compliance that are performance driven

✓ Performance based regulation that scales with size and complexity of organisation and product/service

Industry Desires

- Oversight appropriate for global companies
  - Address Accountable Manager structure w.r.t. cybersecurity and allow company-wide cybersecurity organization to account for current global company structures

✓ Option for delegating accountability to a central corporate cybersecurity office