Notised of Proposed Amendment, NPA 2019-07

Management of information security risks (Cyber security)

2019-11-07 POA-seminarium

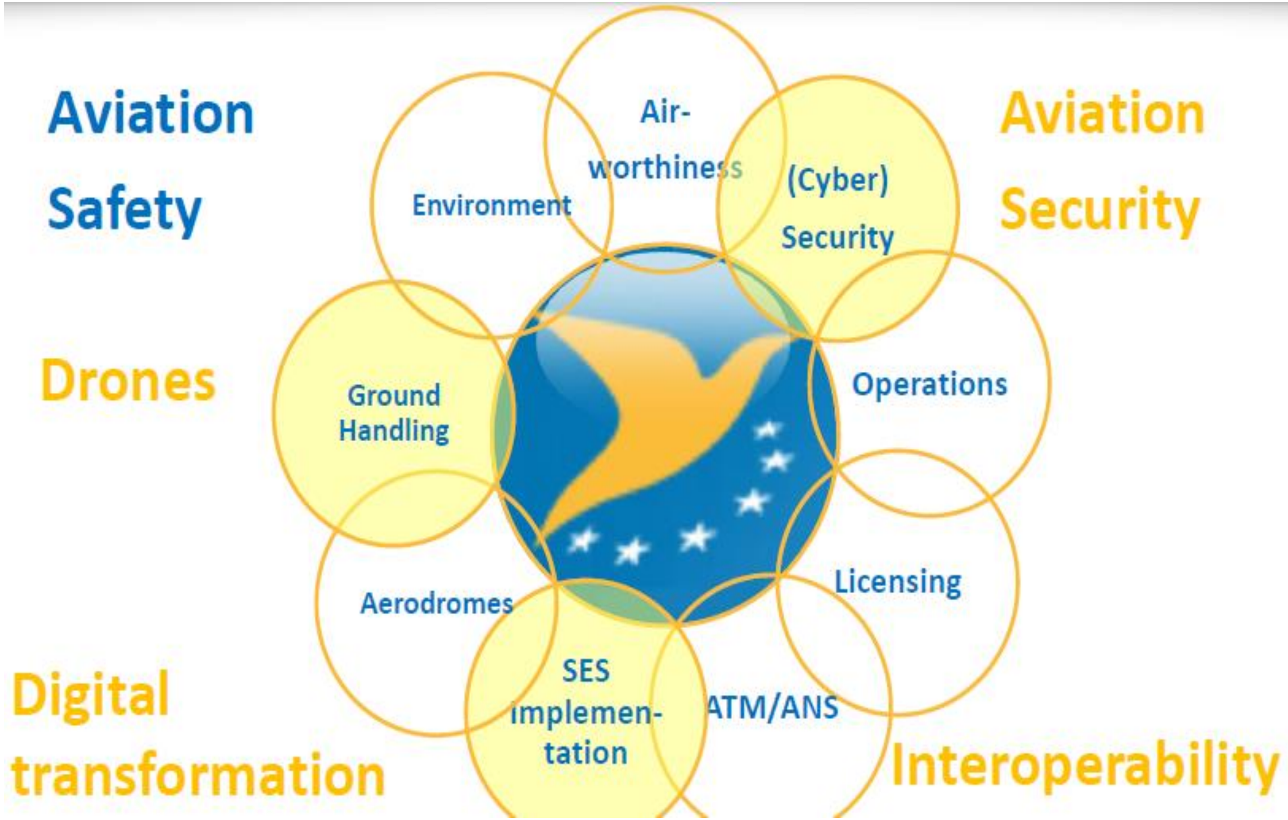
Gun Sunnerstam

TRANSPORT STYRELSEN

”Total system approach Aviation”

Bakgrunden för **NPA 2019-07** är ändringar i grundförordning

(EU) 2018/1139 för förberedande av krav på cybersäkerhet för att få ett helhetsperspektiv inom civil luftfart.



TRANSPORT STYRELSEN

NPA 2019-07 för (Cyber) säkerhet påverkar följande regelkrav med relaterade AMC och GM

(EU) no 748/2012,

No 1321/2014,

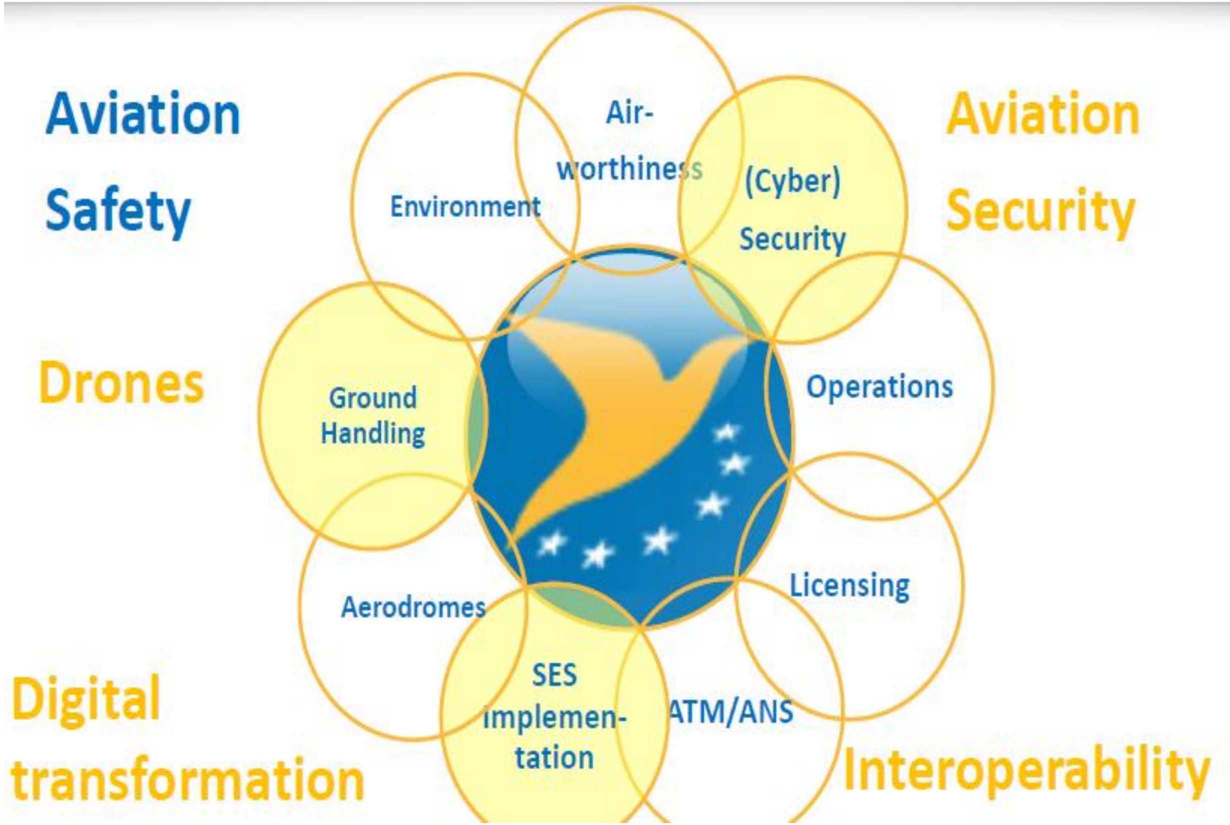
2017/373,

2015/340,

No139/2014,

No 1178/2011

No 965/2012



Vem omfattas av NPA 2019-07

- NPAn påverkar design, **tillverkning,** fortsatt luftvärdighet, underhåll, operativa, besättning, ATM/ANS och ska tillsynas av den behöriga myndigheten.
- NPA 2019-07 gäller inte för tillverkningsorganisationer enligt Del 21G vid tillverkning av ELA 2 luftfartyg (ELA2 =European Light Aircraft MTOM 2000kg, ej komplexa motoriserade luftfartyg (flygplan,segelflyg, ballonger VLR HKP)
- Det innebär att samtliga svenska POA org. berörs.

Förvaltning av information och säkerhetsrisker

Föreslår en introduktion för system för förvaltning av säkerhetsrisker relaterade till civila luftfartens informationssystem, med syfte att ta hand om riskerna angående informationssäkerhet som kan påverka sekretess, integritet och tillgänglighet av lagrad information samt skickad och processad information genom luftfartens civila system.

Artikel 1 i NPA 2019-07

Informationssäkerhet ingår under SMS men här väljer EASA att förtydliga kraven specifikt angående informationssäkerhet (Cybersäkerhet) för att skapa en förutseende organisationsledning med robusta system.

Kravet för POA är **att identifiera, skydda från, upptäcka, reagera och återhämta sig från incidenter som berör organisationens informationssäkerhet som kan påverka verksamheten och slutligen luftvärdigheten**.

TRANSPORT STYRELSEN

Subpart G- POA kommer att få en ny paragraf

21.A.146 Informations säkerhet

Produktionsorganisationen ska uppfylla regelkrav enligt (EU) 202X/XXXX

För Transportstyrelsen tillkommer krav i B-delen:

21.B.5

TRANSPORT STYRELSEN

NPA 2019-07 ska omhänderta i kommande regelkrav:

Beskrivning i AMC och GM på hur små organisationer ska implementera kravet samt ge exempel på;

- Hur man jämför förr och nu för att spåra förbättringar över tid.
- Hur det kan se ut i framtiden efter att förbättringar har införts.
- Jämföra olika organisationers tillämpning i syfte att dela goda tillämpningar.
- Bedöma mognaden hos underleverantörer.

Referens till ledningssystem för informationssäkerhet

4.1 Allmänt

4.2 Vad är LIS (Lednings InformationsSystem)

4.2.1 Översikt och principer

4.2.2 Information

4.2.3 Informationssäkerhet

4.2.4 Förvaltning av ledningssystem

4.2.5 Ledningssystem

4.3 Processorientering

4.4 Varför är LIS viktigt

4.5 Upprätta , övervaka, underhålla och förbättra LIS

4.5.1 Översikt

4.5.2 Fastställande av krav på informationssäkerhet

4.5.3 Riskbedömning inom informationssäkerhet

4.5.4 Riskbehandling inom informationssäkerhet

4.5.5 Välja och vidta säkerhetsåtgärder

4.5.6 Övervaka, underhålla och förbättra effektiviteten i LIS

4.6 Avgörande framgångsfaktorer

4.7 Nyttoeffekter med användningen av LIS-standarder

SS-ISO/IEC 27000: 2018

Ledningssystem för informationssäkerhet

TRANSPORT STYRELSEN

ISMS (Information Security Management System)

- Har man som POA-organisation förberett alternativt redan implementerat ett SMS-system då kan ISMS relativt lätt integreras i samma ledningssystem.

- Som vägledning vid implementering av SMS samt kommande krav på cybersäkerhet och som ett bra exempel hur man kan gå tillväga vid implementering av ett ledningssystem för kommande krav, kan delar är MSBs *Vägledning till ökad säkerhet i industriella informations- och styrsystem (Publ.nr: MSB718-juli 2014)*. Vägledningen kan återfinnas på: https://www.msb.se/RibData/Filer/pdf/27425.pdf

RIKTMÄRKEN FÖR SÄKERHETSARBETET
Det finns en ansvarig för den övergripande säkerheten i de industriella informations- och styrsystemen.
För varje verksamhetskritiskt system finns det en person som är utsedd till systemägare.
Systemägarnas arbetsuppgifter, ansvar, resurser och mandat är tydligt dokumenterade.
Alla systemägare är medvetna om sitt ansvar.
Det finns dokumenterade krav som ställs på en systemägare, såsom kompetens, utbildning, säkerhetsklassning, et cetera.


EASA rulemaking process milestones
Start
Terms of Reference
Consultation
Notice of Proposed Amendment
Proposal to Commission
Opinion
Adoption by Commission
Implementing Rules
Decision
Certification Specifications, Acceptable Means of Compliance, Guidance Material
1
2
3
4
5
Today
16.1.2019
27.5.2019
2020/Q2
2021/Q4
2021/Q4


WHERE?
WHAT?
WHO?
HOW?
WHY?
WHEN?

Cybersäkerhet –genomförande av cybersäkerhetsakten….Dir.2019:73

(Publicerad 1 november 2019, Regeringskansliet)

› **Så stärker vi cybersäkerheten i Sverige**

27 september 2019 · Debattartikel från Mikael Damberg, Per Bolund, Peter Hultqvist, Finansdepartementet, Försvarsdepartementet, Justitiedepartementet

---

› **Inrikesministern presenterar åtgärder för ökad cybersäkerhet**

27 september 2019 · Pressmeddelande, Webb-tv från Mikael Damberg, Justitiedepartementet

---

› **Nationell strategi för samhällets informations- och cybersäkerhet, skr. 2016/17:213, bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet**

16 juli 2018 · Rapport från Justitiedepartementet, Regeringen

---

› **Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019 –2022**

16 juli 2018 · Regeringsuppdrag från Justitiedepartementet, Regeringen