Guidance related to Competent Authority Obligations for Information Security Oversight

(Based on EASA Part-IS.AR, Reg. (EU) 2023/203 & 2022/1645)

A) Internal Responsibilities of the Competent Authority

Competent authorities must establish and maintain their own Information Security Management System (ISMS) to ensure resilience, credibility, and capability to oversee industry effectively. This includes:

1. **ISMS Establishment & Governance**
    - Define and document information security policies, roles, and responsibilities aligned with IS.AR.200 .
    - Implement risk assessment processes covering authority activities, facilities, services, IT systems, and interfaces with external organisations .
    - Maintain secure record-keeping, archiving, and personnel competence requirements .
2. **Compliance Monitoring & Continuous Improvement**
    - Conduct internal audits at planned intervals to verify conformity and effectiveness .
    - Apply continuous improvement processes (e.g. PDCA or DMAIC cycles) to enhance ISMS maturity and adapt to evolving risks .
3. **Confidentiality & Incident Response**
    - Protect sensitive oversight information, including reports from organisations .
    - Establish processes to detect, respond to, and recover from incidents with potential safety impacts .
4. **Contracted Activities Oversight**
    - When outsourcing security-related tasks, ensure suppliers are assessed, certified, and contractually bound to maintain EASA-level security standards

B) Communication to Industry

Competent authorities must provide clarity and transparency to industry stakeholders (operators, CAMOs, Part-145s) on their obligations and expectations. This includes:

1. **Regulatory Guidance & Expectations**
    - Publish national guidance referencing Part-IS obligations, highlighting industry's duty to establish ISMS, perform risk assessments, and ensure reporting of incidents/vulnerabilities .

- Define reporting formats, timelines (e.g. 72h reporting under IS.I.OR.230), and escalation criteria.

2. **Information Sharing & Awareness**
   - Share timely, relevant threat and vulnerability intelligence with organisations to support their risk assessments .
   - Coordinate with EASA and other Member States to promote harmonisation of practices.
3. **Oversight Findings Communication**
   - Notify organisations of findings, categorised according to severity and regulatory framework, requiring corrective action within agreed timeframes .
4. **Support & Engagement**
   - Promote awareness campaigns, workshops, and sector-specific briefings to ensure industry understands evolving threats and regulatory updates.

C) Assessment of Industry Compliance & Engagement

Competent authorities must apply a risk-based, performance-focused oversight approach to assess operators, CAMOs, and Part-145 organisations.

1. **Compliance Oversight Activities**
   - Evaluate whether organisations have implemented an ISMS that meets Part-IS obligations (scope, policies, resources, risk management) .
   - Review reporting systems for information security incidents and vulnerabilities .
2. **Audits & Inspections**
   - Conduct audits of information security processes, records, and incident management practices .
   - Validate training, competence, and staffing for ISMS responsibilities.
3. **Risk-Based Assessment**
   - Use structured risk classification methods to evaluate industry vulnerabilities, linked to safety consequences .
   - Benchmark maturity levels of organisational ISMS against continuous improvement models .
4. **Corrective & Enforcement Measures**

- Issue findings, require corrective action plans, and monitor implementation until closure .
- Escalate to enforcement actions where persistent or systemic non-compliance is identified.

Conclusion

EASA competent authorities carry a dual responsibility:

- To maintain their own secure, risk-managed ISMS and oversight capability.
- To ensure effective industry compliance by setting clear expectations, sharing information, and applying structured, risk-based oversight.

By fulfilling these internal, external, and oversight functions, competent authorities strengthen both regulatory credibility and the overall resilience of the aviation system against information security threats.