IT Security of EU institutions
- eu-LISA model -

Brussels, 14 November 2013
Agenda

- Eu-LISA - Background
- Three Large Scale IT Systems in JFS area
- Security Model
- IT Security in the EU Institutions – Improvement-
eu-LISA - Background

EC Regulation 1077/2011 for the establishment of the Agency as Management Authority of Large Scale IT Systems in JFS areas:

SIS II, VIS and EURODAC

The Agency is responsible for the operational management and security of the Central Systems and of the

Communications Network
Three Large Scale IT Systems in JFS area

1. **SIS II** – 30 Schengen Area States (26MS+4NonMS) + EUROJUST and EUROPOL - Connected to several law enforcement national networks

2. **VIS** – 29 States (Schengen Area States + other) – Connected to Ministry of Foreign Affairs networks reaching several world regions (Africa, Middle East, soon South America and Russia)

3. **EURODAC** – 32 EU Countries - mainly connected to immigration services

…and the Communications Network: common secure transport vector
Security Model

eu-LISA and the three IT Systems are security governed by their own:

- **EC Establishing Regulation** (legal base)
- Series of adopted **Security Plans** and related **policies** and **procedures**
- eu-LISA is developing a **Risk Management Framework** to baseline common security measures to improve the controls of the Central Systems
Security Model

- The Central Systems are technically conceived to be **NOT connected to the Internet**, but only to authorised institutional networks through controlled national interfaces.
- Following the **self-protecting node** principle, a set of border protection controls "defend" the systems from typical interconnection risks (i.e. viruses) or other known attack vectors.
- **Strong monitoring** and **audit controls** are implemented at central level as preventive and detective measures.
IT Security in the EU Institutions - Improvements -

1. Set **IT Security standards** at EU level for an **end-to-end** approach. Need an **EU body to follow up and implement** such **standards**

2. IT Systems architectures based on **risk assessments** processes to assure cost effective security and privacy, **by design**

3. Security "**certification**" processes

4. Integrated **Identity Management and Information Labeling controls**, both as enabler for an effective assurance on information access
Thank you