Council of the
European Union

Brussels, 15 July 2015
(OR. en)

10937/15

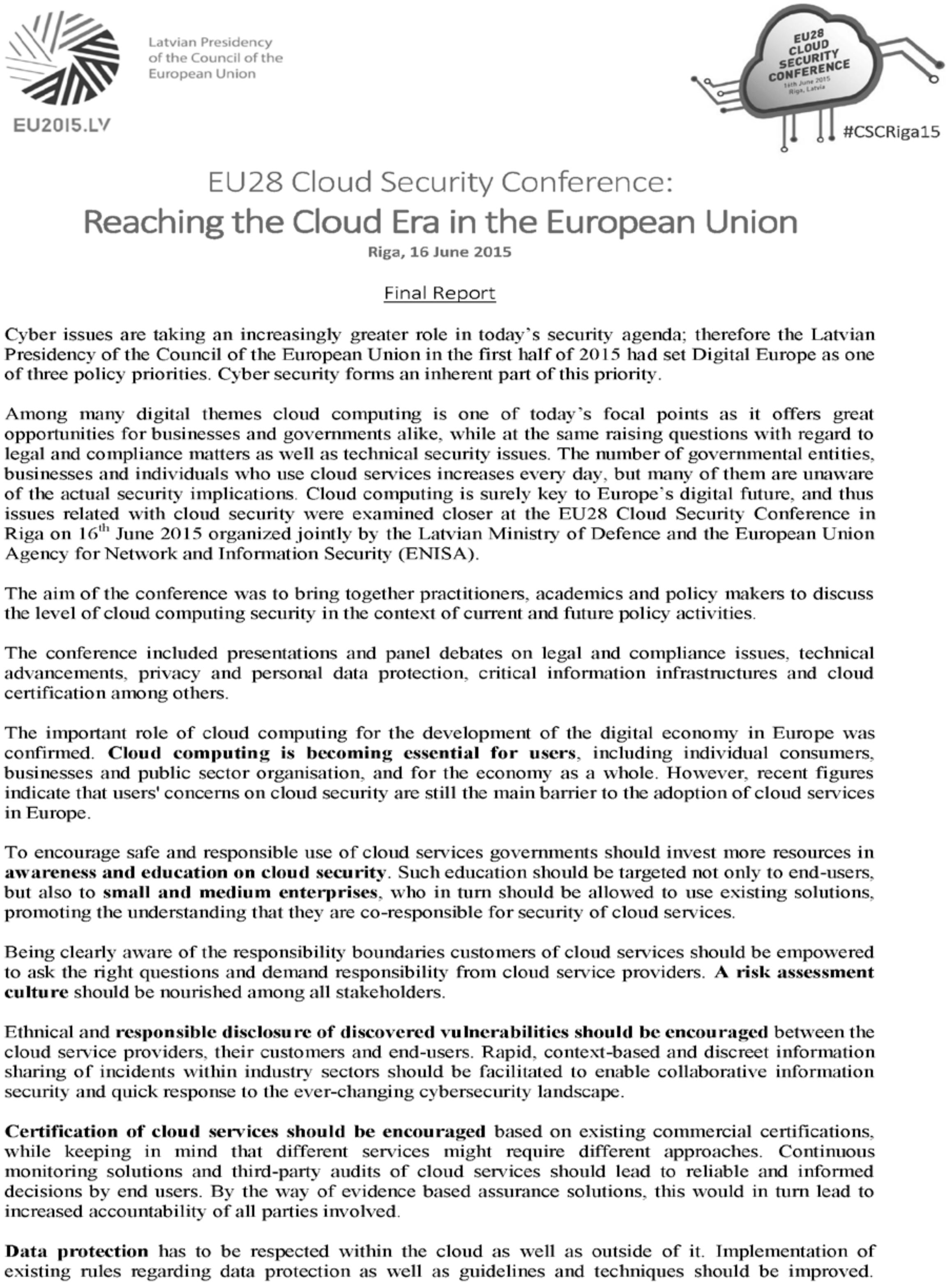
CYBER 71

NOTE

From:	LV delegation
To:	Delegations
Subject:	Final Report on the EU28 Cloud Security Conference: Reaching the Cloud Era in the European Union held in Riga on 16 June 2015

Delegations will find in Annex the Final Report on the EU28 Cloud Security Conference: Reaching the Cloud Era in the European Union held in Riga on 16 June 2015.

ANNEX



Latvian Presidency
of the Council of the
European Union

EU2015.LV

#CSCRiga15

EU28 Cloud Security Conference:
Reaching the Cloud Era in the European Union

Riga, 16 June 2015

Final Report

Cyber issues are taking an increasingly greater role in today's security agenda; therefore the Latvian Presidency of the Council of the European Union in the first half of 2015 had set Digital Europe as one of three policy priorities. Cyber security forms an inherent part of this priority.

Among many digital themes cloud computing is one of today's focal points as it offers great opportunities for businesses and governments alike, while at the same raising questions with regard to legal and compliance matters as well as technical security issues. The number of governmental entities, businesses and individuals who use cloud services increases every day, but many of them are unaware of the actual security implications. Cloud computing is surely key to Europe's digital future, and thus issues related with cloud security were examined closer at the EU28 Cloud Security Conference in Riga on 16th June 2015 organized jointly by the Latvian Ministry of Defence and the European Union Agency for Network and Information Security (ENISA).

The aim of the conference was to bring together practitioners, academics and policy makers to discuss the level of cloud computing security in the context of current and future policy activities.

The conference included presentations and panel debates on legal and compliance issues, technical advancements, privacy and personal data protection, critical information infrastructures and cloud certification among others.

The important role of cloud computing for the development of the digital economy in Europe was confirmed. **Cloud computing is becoming essential for users**, including individual consumers, businesses and public sector organisation, and for the economy as a whole. However, recent figures indicate that users' concerns on cloud security are still the main barrier to the adoption of cloud services in Europe.

To encourage safe and responsible use of cloud services governments should invest more resources in **awareness and education on cloud security**. Such education should be targeted not only to end-users, but also to **small and medium enterprises**, who in turn should be allowed to use existing solutions, promoting the understanding that they are co-responsible for security of cloud services.

Being clearly aware of the responsibility boundaries customers of cloud services should be empowered to ask the right questions and demand responsibility from cloud service providers. **A risk assessment culture** should be nourished among all stakeholders.

Ethnical and **responsible disclosure of discovered vulnerabilities should be encouraged** between the cloud service providers, their customers and end-users. Rapid, context-based and discreet information sharing of incidents within industry sectors should be facilitated to enable collaborative information security and quick response to the ever-changing cybersecurity landscape.

Certification of cloud services should be encouraged based on existing commercial certifications, while keeping in mind that different services might require different approaches. Continuous monitoring solutions and third-party audits of cloud services should lead to reliable and informed decisions by end users. By the way of evidence based assurance solutions, this would in turn lead to increased accountability of all parties involved.

Data protection has to be respected within the cloud as well as outside of it. Implementation of existing rules regarding data protection as well as guidelines and techniques should be improved.

Knowledge on data protection mechanisms should be shared for the benefit of all stakeholders. Security is a priority not only because of user privacy being at stake, but also because of the emerging threat vectors. It is additionally noted that big data and end-user profiling process requires further analysis.

Governmental clouds based on the customised needs of each country can positively strengthen cross-border cooperation between governments and the industry provided that governments create clear procurement guidelines in collaboration with the industry. Stakeholders should enhance information sharing of implemented solutions and good practices.

Cloud services benefit from an **open market**, therefore closing borders to promote security is not a solution and would be detrimental to the use and development of cloud computing. To make positive use of the open market and promote economic growth, **Cloud providers within the European Union should become more innovative and competitive.**

Critical infrastructure sector sees increase in cloud usage and voices the need for elaborate security measures and specific risk assessment techniques.

Furthermore, cloud security was **discussed in relation to the recent regulatory and policy initiatives**, such as the ongoing data protection reform, the proposal for a Network and Information Security directive, cloud computing communication and the Digital Single Market strategy. It was agreed that further policy actions on cloud security could support trust and confidence in cloud services by addressing outstanding issues in the following ways.

Future Policy actions regarding cloud services should be flexible and adaptive as to allow further technological advancements of cloud security. Such policy must use technology-neutral language and only consider legal obligations based on general principles to allow for flexible solutions. It cannot be created in such a way to endanger the existence of the small cloud providers. Compliance fatigue must be avoided while **co-regulatory and self-regulatory initiatives** are to be supported.

Security related topics that require further discussion and guidance include requirement for data geolocation, foreign jurisdictions, and access to data of Europeans.

The findings of the EU28 Cloud Security Conference were discussed and presented to the wider audience of the Digital Assembly 2015 – a high-level event taking place in Riga on the 17th and 18th June, 2015.