For Official Use **DSTI/CDEP/SPDE/M(2016)1**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

05-May-2017

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/CDEP/SPDE/M(2016)1
For Official Use

Cancels & replaces the same document of 05 May 2017

Working Party on Security and Privacy in the Digital Economy

DRAFT SUMMARY RECORD: 40TH MEETING OF THE WORKING PARTY ON SECURITY AND PRIVACY IN THE DIGITAL ECONOMY (WPSPDE)

15-16 November 2016

Elettra Ronchi: Tel: +33-1 45 24 18 28; e-mail: elettra.ronchi@oecd.org
Claire Hilton : +33-1 45 24 76 91; e-mail: claire.hilton@oecd.org
Christian Reimsbach-Kounatze: E-mail: christian.reimsbach-kounatze@oecd.org

JT03413757

English - Or. English

DRAFT SUMMARY RECORD: 40TH MEETING OF THE WORKING PARTY ON SECURITY AND PRIVACY IN THE DIGITAL ECONOMY (WPSPDE)

Joint SPDE/MADE expert meeting on "Improving the Evidence Base for Security and Privacy Policy Making"

DSTI/CDEP/SPDE/MADE(2016)1/REV1

1. SPDE and MADE held an expert meeting as part of their continuing collaboration on improving the evidence base for security and privacy policy making. The expert meeting consisted of two sessions:

Session 1. Improving digital security risk management in firms: measurement needs and challenges

2. Session 1 focussed on "Improving Digital Security Risk Management in Firms: measurement needs and challenge". Two presentations provided country specific perspectives:

3. Mr. Marc Uhrbach (Program Manager, Digital Economy Metrics, Statistics Canada) presented the Canadian efforts to improve the national evidence base of cyber security practices and incidents. Canada is developing a cybersecurity questionnaire for a survey to be carried out in 2018.

4. Ms. Heather Butler and Ms. Sabine Gerdon (Department for Culture Media and Sport, UK) provided an overview of the UK Cyber Security Breaches Survey aiming to monitor the effects of cybersecurity breaches on businesses, track awareness of government interventions and help businesses to better protect themselves.

5. Three speakers shared private sector perspectives and initiatives:

6. Mr. Eric Schuh (Head Casualty Center, Swiss Re, Switzerland) presented the Chief Risk Officer (CRO) Forum work on cyber risk. Mr Schuh presented a detailed categorization of cyber-risks and their costs to assist in the development of a common language, to make the industry safer. Delegates were encouraged to contact to CRO forum for further information.

7. Mr. Gilbert Canaméras (Secretary General, Federation of European Risk Managers Association) provided an overview of the (FERMA) European Risk and Insurance Survey carried out among its members since 2002. Mr Canameras suggested that FERMA could add value to the OECD Measurement Agenda by helping to define the most effective measures on digital security risk management;

8. Mr. Philippe Cotelle (Head of Risk Management and Insurance, Airbus Defence and Space) focused on the risk assessment methodology developed by Airbus in collaboration with a multidisciplinary experts group. The quantification of risk includes the valuation of tangible and intangible assets (i.e. data, processes, governance) under alternative scenarios (including catastrophic ones).

9. During the discussion, delegates noted the importance of a clear set of definitions needed to understand survey results. ***BIAC*** noted that clear definitions are essential to understand the survey results, e.g. businesses are unlikely to consider R&D costs as security costs.

10. Delegates also stressed the need to look beyond incidents and to include other measures . In particular, the ***MADE Chair***, Luis Magalhães commented on the tendency to focus on cybersecurity threats and to overlook business opportunities. He suggested that these surveys should be complemented by metrics about new technological developments to manage cyber threats, e.g. R&D related to cybersecurity. The ***Netherlands*** are trying to measure not only the number and cost of incidents but also the value of defensive measures to avoid attacks, threats and vulnerabilities.

11. Delegates also highlighted the need to better examine the concept of "costs" of security incidents for better quantification of impacts and to assist business in putting in place effective risk management practice. It was questioned for instance whether spending for addressing digital security threats and vulnerabilities should rather be considered as investments such as is the case for research and development (R&D). Furthermore, it was highlighted that the analysis of digital security risks would need to include the whole supply chain. ***Egypt*** pointed out that losses in confidence and reputation are harder to measure than financial losses. The delegation also called the attention to the costs arising from changes in production process in order to prevent cyber-attacks.

12. ***Slovenia*** reported on work by the European Statistical System and Eurostat, including two modules in the ICT Business Survey, one in 2010 on ICT security and the other in 2015 on ICT security policies. Eurostat is also testing a set of questions on ICT security, incidents and cost and the results show that questions on the value or the impact of incidents are difficult to answer.

13. Finally, delegates acknowledged that the digital security insurance industry was growing but still not fully mature. The lack of definitions of digital risk, the absence of relevant data series on past incidence and losses, the limited actuarial information available on the frequency and magnitude of actual and potential digital security and privacy incidents, and the ever-evolving nature of digital risks continue to be major challenges for the insurance sector. A common taxonomy was thus seen as key for its development as well as mechanisms for sharing data between all stakeholders, and it was highlighted that the OECD had a potential role in being one of the forums where cooperation and exchange could take place. Delegates also stressed the importance to focus on SMEs and the question was raised on what kind of information would be needed to better assess digital security risks faced by SMEs.

14. Participants noted how some areas were more appropriate for OECD actions than others. Digital security risk management practices and training and awareness activities by business do not seem to be currently surveyed in a systematic or comparable way and as a few delegates noted , although harder to measure, these are areas that policy-makers consider important. A priority for the OECD could be to compare national and international survey activities to date. Another priority could also be to address the difficulties associated with a lack of a common taxonomy, for example, articulating what is meant by a digital risk incident. Digital incidents are often still classified based on the nature of the event – for example, as data breaches, mishandling of information, or failures of technology. While such taxonomies provide a conceptual basis for describing technical failures, they are insufficient to deliver a business impact point of view, i.e. the economic risk.

15. The ***SPDE Chair***, Jane Hamilton, closed this session by informing participants about a workshop in May 2017 with policy makers and insurance professionals to look at emerging issues on this topic. She suggested that previous OECD work on CSIRT could help to develop clear definitions and made reference to the 2015 OECD Recommendation on Digital Risk Management for Economic and Social Prosperity as a framework for the measurement work. The ***WPMADE Chair***, Luis Magalhães supported Ms Hamilton's conclusions.

Session 2. Promoting comparability of personal data breach notification reporting.

16. Session 2 focussed on "Promoting comparability of personal data breach notification (DBN) reporting". Three speakers presented perspectives as Privacy Enforcement Authorities and OECD Country Experts.

17. Mr. David Smith (Privacy Expert, UK) provided an overview of the data breach notification (DBN) system in the United Kingdom at the Information Commissioner's Office (ICO) and the new rules which will come into force in May 2018 within the new EU General Data Protection (GDPR) system.

18. Mr. Matthieu Grall (Head of Technology Experts Department, CNIL, France) gave a presentation on the complexity of the current notification systems in Europe which is based on a number of regulations (General Data Protection regulation, ePrivacy, eIDAS- an EU regulation on electronic identification and trust services for electronic transactions in the internal market, the Network Information Service Directive, Telecom Package) and may involve various authorities, highlighting the need for a consolidated or common notification process ;

19. Mr. Beomsoo Kim (Executive Director, Barun ICT Research Center, Yonsei University, Korea) provided an overview of DBN regulation in Korea, which requires mandatory reporting, and presented some data to the delegates.

20. During the discussion, some countries took the opportunity to present their national DBN initiatives. Some were considering creating new indicators by better exploiting their existing national DBN databases while others questioned whether the current reporting systems did correspond to the needs expressed at the national and international level. In particular, ***Italy*** informed about the enlargement of the sectoral coverage for the mandatory DBN procedures; ***Japan*** explained the changes in the national DBN procedure as of next year; the ***Netherlands*** informed about their plans to exploit their national DBN database to produce new metrics. Several delegations stressed the need for "best practices" given current ambiguities on what to report, by when and how and some also expressed their interest in developing metrics to analyse the economic impact of DBN. The ***United Kingdom*** underlined the usefulness of accurate metrics to forecast DBNs. ***Portugal*** questioned if the current reporting systems correspond to the needs expressed at the national and international level and called the experts to develop metrics on the impact of DBN on production, trade, movement of capital and people. ***Norway*** underlined the need to come to a common agreement about what to measure in terms of DBN. ***Turkey*** suggested the compile a "best-practices" system especially from the perspective of SMEs on how do they cope with security breaches. ***BIAC*** called the OECD to analyse the economic damages from the noise caused by the breach reporting.

21. Delegates agreed that a useful priority action for the OECD could be to provide a focused review on how DBN metrics may add real value to policy making and what can be easily collected. It was further noted that this work would need to proceed in close collaboration with Privacy Enforcement Authorities (PEAs).

22. To conclude, the WPMADE and the WPSPDE Chairs reminded participants about the establishment of an informal taskforce to support work on the joint measurement agenda with a two year mandate and asked delegations to provide nominations to the Secretariat by end of 2016. The WPSPDE Chair Ms Hamilton closed the meeting with final comments, noting that the OECD's collaborative relationship with the International Conference on Data Protection and Privacy Commissioners (ICDPPC) as well as the Asia Pacific Privacy Authorities (APPA) would add significant value to this work. Summing up the two sessions, Ms Hamilton noted that the issues surrounding data breach notification are linked to improved security measures. The privacy and security communities must come together to effectively address these issues. The Secretariat was invited to further scope and carry out analytical work on the priority areas identified and report back at the next Working Party meeting.

Item 2. Adoption of the Draft Agenda

DSTI/CDEP/SPDE/A(2016)1/REV1

23. The Working Party adopted the draft agenda.

Item 3. Approval of the Summary Record of the 39th Session

DSTI/ICCP/REG/M(2015)2

24. The Chair (Jane Hamilton) noted that no comments had been received on the draft summary record of the 39th meeting of the Working Party.

25. The Working Party agreed to approve the draft summary record.

Item 4. Secretariat Statement

26. The Secretariat (Anne Carblanc) provided a brief update on developments since the Working Party meeting of December 2015, including main outcomes from the Ministerial Council Meeting, the Cancun Ministerial meeting on the Digital Economy and several high level G7 meetings in Japan. In particular, the G20 Hangzhou Summit in China on 4 -5 September 2016 where G20 leaders agree on a Digital Economy Initiative. Looking forward to 2017 and 2018, Ms Carblanc briefly outlined the CDEP Programme of Work and Budget (PWB) items, and the links with the horizontal Digitalisation Project. She noted that Ms Molly Lesher would provide greater details on the Digitalisation Project later in the afternoon.

27. The Working Party noted the Secretariat Statement.

Item 5. Report on the 2016 Ministerial Meeting

28. The Secretariat (Anne Carblanc) presented the outcomes of the Ministerial Meeting and highlighted its wide media coverage. The meeting had been attended by over 1 300 participants from 36 economies from a wide variety of backgrounds including Ministers, senior government officials, and representatives of business, the Internet technical community, officials, international organisation, and representatives of business, civil society and organised labour. The eight Panels had generated substantive discussion on the four main themes of the Ministerial; Internet openness and innovation, building global connectivity, trust in the digital economy, and jobs and skills in the digital economy. Outcomes of the Ministerial meeting included recognition of shared objectives and the impact of collective action as well as the adoption of the Cancun Ministerial Declaration to progress the OECD digital agenda. Ms Carblanc pointed out that the Cancun Declaration calls for the development of better data on the digital economy and noted the specific mentions to security and privacy work. She thanked the Working Party for its contributions to the Ministerial preparations.

29. The Working Party noted the overview of the Ministerial meeting.

Item 6. Working Party Mandates and Working Methods

DSTI/CDEP(2016)9

DSTI/CDEP(2016)10

30. The Secretariat (Anne Carblanc) presented the proposal by the CDEP Extended Bureau for revisions of the 2017-18 mandates and working methods of the CDEP Working Parties. Ms Carblanc highlighted the benefits of the regular review and renewal of the mandate as an effective means to enhance flexibility and innovation in the work carried out by the Working Parties. She noted that improving measurement and analysis of the digital economy was one key motivation for the CDEP Bureau proposal. She also highlighted the broadening of the SPDE mandate to include work on "the enhancement of access to data to foster digital innovation" as a follow-up to the Committee's work on data-driven innovation. Ms. Carblanc also presented the CDEP Bureau proposal to update and clarify the CISP mandate by including a reference to work on communication-related industries and platforms, and the need to address the implications of changing communication market structures and technological developments, from both supply and demand-side perspectives; and to refer to media in the context of convergence. Ms. Carblanc ended her presentation with a presentation on the reorientation of the mandate of MADE for 2017-2018 that would now include the analysis of "the contribution of digital economy policies to economic performances and social outcomes" and, in particular, "the evaluation of the impact of digital economy policies on economic performance, notably on growth, productivity and innovation, and on social well-being".

31. The Working Party welcomed the proposed changes to the SPDE mandate.

Item 7. Progress Report on PWB

32. The Secretariat (Elettra Ronchi) provided an update on progress in implementing the 2015-2016 Programme of Work and Budget (PWB). This included in particular the work on "Privacy in a data driven economy" (IOR 4.1), which was accomplished through the following reports: (i) Opportunities and Challenges in developing a risk-based approach to privacy [DSTI/ICCP/REG(2015)1/REV2]; (ii) Opportunity and Challenges relating to the management of digital security and privacy risk by SMEs [DSTI/ICCP/REG(2015)2/REV1 and (iii) the background report for Panel 3.2 of the 2016 Ministerial Meeting on the Digital Economy [DSTI/ICCP/REG(2016)1]. SPDE's contributions to the 2015-2016 PWB also included the work on "National strategies for managing digital security risks and Critical Information Infrastructures" (IOR 4.2), which was accomplished through (i) the 2015 Revision of the Security Guidelines – Recommendation on Digital Security Risk Management for Economic and Social Prosperity (from the 2013-14 PWB) and the questionnaire for the Review of the 2008 CIIP recommendation [DSTI/ICCP/REG(2016)2]. Ms. Ronchi also highlighted the work on "Privacy and security risk management in the health sector" (IOR 4.3), including in particular the development of the Council Recommendation on Health Data Governance [DSTI/ICCP/REG(2016)3/REV ; COM/DELSA/DSTI(2016)1/REV3] and the work on "Improving the Evidence Base for Policy Making in the Digital Economy" (IOR 3.5), the Digital Economy Outlook (IOR 5.2) to which the SPDE contributed significantly. The reports on "The Internet of Things: Seizing the Benefits and Addressing the Challenges" [DSTI/ICCP/CISP(2015)3/REV3] and "The Governance of globalized data-flows – Current trends and future challenges [DSTI/ICCP/REG(2015)3] were highlighted as two additional areas, where SPDE was also called to provide inputs.

33. Ms Ronchi then introduced the SPDE contributions to the 2017-18 CDEP PWB and the key output results (ORs) for the CDEP and its Working Parties on "Strengthening the foundations for the digital economy" as well as their contributions to the Horizontal Project "Seizing the Benefits of Digitalisation for Growth and Wellbeing", to which other OECD Committees are also contributing. Ms. Ronchi in particular highlighted the work on "Improving the evidence base for security and privacy policy making" (under IOR 1.2) and on Improving trust (IOR 1.3), which includes (i) Developing recommendations regarding the development of privacy and data protection strategies and (ii) Mainstreaming digital security and privacy risk management with a special focus on SMEs.

34. She highlighted how future work on risk management practices in firms and on data breach notification could build on progress made through recent analytical work such as the 2012 Proposals for improving the OECD model surveys with respect to information security and privacy (with WPIIS, now MADE) and the 2015 Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams (CSIRTs).

35. She noted that SPDE was expected to contribute also to work on "Unleashing the potential the Internet of Things and other emerging technologies" (IOR 1.4) and on "Measuring the effects of digital strategies and policies" (IOR 1.5), including in particular work on "Maximising the Economic and Social Value of Data (Understanding the Benefits and Challenges of Enhanced Access to Data)", and the contribution to the 2017 Digital Economy Outlook including the DEO Policy Questionnaire and the Chapter on Digital Risk and Trust. Work to review three OECD Council Recommendations was then highlighted: (i) the Recommendation on the Protection of Critical Information Infrastructure (2008), (ii) the Recommendation Concerning Guidelines for Cryptography Policy (1997), and the Recommendation on the Protection of Children Online (2012).

36. During the discussion, delegates highlighted the need to assure that needed resources would be made available for the SPDE Secretariat to contribute to both work streams and in particular the horizontal project "Seizing the Benefits of Digitalisation for Growth and Wellbeing".

Item 8. Data Governance

37. The chair proposed to change the order of the sub-items under the item on data governance and to start with the sub-item on "Enhanced Access to Data: Proposal for the Development of an Overarching Instrument on Enhanced Access to Data" before the sub-item on "Health Data Governance", which was then agreed by the SPDE.

8.a. OECD Council Recommendation on Health Data Governance

COM/DELSA/DSTI(2016)1/REV3

38. The Secretariat (Elettra Ronchi) presented the revised version of the draft OECD Recommendation on Health Data Governance, which was developed in close co-operation with the Health Committee and an informal expert Advisory Expert Group (including 65 members with expertise in privacy, law, statistics, research, IT and health policy from government, industry, academia and civil society). She recalled the rationale and the objectives of the work and presented the structure of the draft Recommendation, the list of the 12 recommended key measures to address major health data governance issues, and the timeline of consultations and work completed to date. The Health Committee (HC) and the Committee on Digital Economy Policy (CDEP) had reviewed the draft Recommendation during their respective June 2016 meetings and had provided written comments in July-August 2016.

39. On 7-8 November, following discussions at the HC, a REV3 that met the agreement of this Committee was posted on OLIS for any substantive comments by SPDE and CDEP delegates with a deadline of 14 November. The Secretariat presented the clarifying edits approved by the Health Committee and issued as the REV3 document under discussion.

40. During their discussion, delegates highlighted the need for further clarifying edits to the provided description of de-identification. In the interest of providing Delegates with additional time to consider the two amendments made to the draft Recommendation, the Chair recommended that delegates be given the opportunity to further discuss this item under agenda item 11 (after the coffee break on the following day). As a consequence, the Designation of the Bureau for 2017 (former agenda item 11) was moved to the end (as last item) of that day.

41. Delegates agreed to include the clarifying edits made to the REV3 version of the draft Recommendation (a shortened description of de-identification and implementation specific details added to the explanatory note to the Recommendation). A REV 4 version was issued for approval by CDEP and by written procedure by the Health Committee. The Secretariat noted that if there were no objections on the REV4 by 21 November COB, the draft Recommendation would be deemed approved by both Committees and transmitted to the OECD Council for adoption.

8.b. Enhanced Access to Data: Proposal for the Development of an Overarching Instrument on Enhanced Access to Data

COM/DSTI/CDEP/STP/GOV/PGC(2016)1

42. In view of the proposed revisions to the SPDE mandate which aim to include work on the enhancement of access to data to foster digital innovation, the Secretariat (Christian Reimsbach-Kounatze) presented a proposal submitted to the CDEP to develop an OECD instrument to promote coherence among OECD legal instruments that set out a framework to foster access, linkage and reuse of data. After summarising key conclusions from the horizontal project on Data-driven Innovation (DDI), in particular on the potential for enhanced access to data to maximise the value of data, Mr. Reimsbach-Kounatze presented the differences and similarities between existing related OECD Recommendations, most notably the Recommendation on Access to Research Data from Public Funding [C(2006)184], the Recommendation on Enhanced Access and More Effective Use of public sector information (PSI) [C(2008)36], and the International Open Data Charter. He highlighted that better coherence between existing instrument would help reduce uncertainties regarding key data governance issues such as data interoperability and portability, data ownership and control, data quality and curation, and data value and pricing. He then presented the proposal for the development of a new consolidated Council Recommendation based on general principles for enhancing access to data, and the proposed governance structure and timeline for this work.

43. Delegates discussed the proposal. They confirmed the need for a better understanding of key concepts (e.g., on "openness" with regards to data and of data portability). Delegates also acknowledged current difficulties in addressing data governance issues and the need to discuss these issues internationally, in particular through the OECD. They stressed the importance of further analytical work on the economic benefits of enhanced access to data as well as on the opportunity costs or the potential benefits that are forfeited by not enhancing access to data. Delegates also highlighted the potential risks associated to data collection, which would not only include the risk of privacy violations but also the risk of reducing data quality (by adding noise to the data). Delegates recommended considering current initiatives by the European Commission such as the Digital Single Market - Free Flow of Data Initiative. They also recommended that the area of health and medical research be considered in the project. The SPDE Secretariat was asked to further consult with possible interested countries and submit tangible proposals on how to best move forward during the second quarter of 2017. In particular, delegates invited the Secretariat to further strengthen the evidence base with a workshop prior to engaging in the development of the new overarching Recommendation.

8.c. CCP's work on Consumer Data

44. The Secretariat (Michael Donohue) in charge of the Committee on Consumer Protection (CCP) provided an update on recent and upcoming work by the CCP on the governance of consumer data including a privacy or security dimension. This included in particular the presentation of the Revised E-commerce Recommendation and future work such as work on the Digital Economy Outlook, trust in the IoT, and on behavioural insights.

45. The Working Party **noted** the work of the CCP.

Item 9. Update on the Digitalisation Project

DSTI/IND/STP/CDEP/CP(2016)2

DSTI/CDEP(2016)7

46. The Secretariat (Molly Lesher) presented the proposed methodology, structure and governance for the 2017-18 horizontal project on "Seizing the Benefits of Digitalisation for Growth and Wellbeing". She highlighted in particular current trends in the use of digital technologies, the objective of the horizontal project, namely to "provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world", the proposed framework of the project, and possible cross-cutting modules.

47. Delegates discussed the proposal. They highlighted in particular the importance of the measurement framework, and the need to address major societal challenges including environmental challenges associated with digitalisation for example as possible cross-cutting modules. They also recommended looking at emerging issues such as the IoT and artificial intelligence (AI). The chair concluded highlighting possible SPDE-specific contributions such as the work on trust measurement, work on critical information infrastructure protection as well as work on enhanced access to data.

48. Delegates were invited to provide written comments by 9 December 2016.

Item 10. Future Work: Review of OECD Council Recommendations

10.a. 2012 OECD Council Recommendation on the Protection of Children Online

DSTI/CDEP/SPDE(2016)2

49. Prof Kristina Irion (University of Amsterdam) and the OECD Secretariat (Elettra Ronchi) introduced the item and provided an overview of policy developments on the Protection of Children Online since 2012. Delegates highlighted the changing risk landscape children are exposed to and the need to better measure and enhance the level of education and awareness of children but also of their parents. The collection of personal data of children by mobile applications (apps) and the role of parental consent were mentioned as examples of issues that needed to be further examined. Questions were raised to what extent anonymity could be considered as a risk factor and whether digital identity management should therefore be considered in the work.

50. Japan (Dr. Nagayuki Saito from Keio University) presented progress made on the implementation of the OECD Recommendation in Japan. After highlighting major trends related to children online, Dr. Saito highlighted recent initiatives in Japan to measure and address concerns related to children online. This included in particular the Internet Literacy Assessment indicator for Students (ILAS) survey, the results of which he then presented. Dr. Saito concluded his presentation with lessons learned and a number of suggestions for the review and possible revision of the OECD Council Recommendation on the Protection of Children Online, such as the need to revisit the typology of risks underlying the Recommendation. Delegates highlighted the need to differentiate between different children age subgroups when looking at the typology of risks.

51. The Secretariat (Elettra Ronchi) then briefly introduced the proposed process for the first review of the OECD Council Recommendation on the Protection of Children Online, which was adopted by the OECD Council in 2012. The Recommendation instructs CDEP to review the Recommendation and its

implementation, and report to Council within five years of its adoption and thereafter as appropriate. She highlighted in particular the outline of the proposed questionnaire to collect information on countries' initiatives and lessons learned.

52. Delegates agreed on timelines and proposed process and expressed support for the use of a questionnaire, the outcome of which would then be discussed at the SPDE meeting in May 2017, and inform the decision whether or not to revise the Recommendation. Italy, Japan, Korea and the United Kingdom expressed their support in promoting the exchange of best practices via a possible workshop, which would help inform the review process.

10.b. 2008 OECD Council Recommendation on the Protection of Critical Information Infrastructure

53. The Secretariat (Laurent Bernat and Nick Mansfield, consultant to the OECD) presented an overview of the responses from member countries received so far to the questionnaire circulated in May 2016. He highlighted that these responses were not sufficient to conduct a robust analysis on policy trends related to the Protection of Critical Information Infrastructure (CIIP), but still sufficient to conduct a preliminary high-level analysis with the objective to identify possible paradigm shifts that could suggest a need for the revision of the Recommendation. Responses suggest that the Recommendation has been relevant to date. However, most respondent agree that it needs to be revised if only to reflect the 2015 Recommendation on Digital Security Risk Management. Sectoral responsibility was still dominant across countries as well as the consensus to strengthen public/private cooperation. Survey responses confirmed that the interpretation of the concept of CII is becoming more consistent with the evolution reflected in the 2015 Recommendation on Digital Security Risk Management, in particular with the increased inclusion of services or functions as a basis for the definition of CII. Mr. Bernat introduced options for next steps in the review process. In particular, he stressed the need for more country responses to articulate in greater detail the current findings and develop possible high-level principles if appropriate. Furthermore, he highlighted the potential relationship with the horizontal project on the digital transformation to be finalised by 2018.

54. Delegates discussed the update and stressed the importance of the topic. The consistency with the Recommendation on Digital Security Risk Management was stressed as essential. Delegates welcomed the potential link to the horizontal project on the digital transformation of the economy and society. Current developments at EU and UN levels were highlighted. Delegates also expressed the need to better clarify and/or illustrate the distinction between the levels of escalations (incident, emergency and crisis) as well as between the impact on the infrastructure and that on organisations and the society. In this context delegates acknowledged the potential impact of incidents beyond national borders. The Secretariat was also encouraged to consider possible linkages with the project on enhanced access to data and to consider how regulatory objectives such as in the area of competition as well as sector specific regulatory objective such as in finance relates to CIIP. Balancing public and private interests was highlighted as important in this context.

55. Delegates agreed to 6 January 2017 as deadline for the second round of responses and to discuss this topic at the next SPDE meeting in May 2017. They noted the sensitivity of the topic and noted that responses should be kept confidential and unattributed in the reports.

10.c. 1997 OECD Council Recommendation concerning Guidelines for Cryptography Policy

DSTI/CDEP/SPDE(2016)3

56. The Secretariat (Laurent Bernat) introduced the procedural options for carrying out the fourth review of the 1997 OECD "Cryptography Guidelines". The Recommendation calls upon OECD member countries to review the Guidelines at least every five years, with a view to improving international co-

operation on issues related to cryptography policy. Mr. Bernat highlighted that all previous reviews (in 2002, 2007 and 2012) concluded that the Cryptography Guidelines continued to be "adequate to address the issues and purpose for which they were developed" and that there was no need to revise them during that respective year. He highlighted the process followed each time: brief report following a short questionnaire. Current developments making cryptography a more topical issue in some countries than at the time of previous reviews were highlighted. Mr. Bernat then presented options for the review process starting with a questionnaire to be circulated early 2017.

57. Delegates affirmed the importance and significant role of the Cryptography Guidelines in particular for trust in the Internet. They agreed with the Secretariat's assessment on current developments making cryptography a more topical issue today. Threats to privacy and the freedom of expression were stressed by Delegations as major reasons for the growing importance of cryptography. Delegates expressed their interest in further assessing the economic role of cryptography, and highlighted the need to emphasise that the use of cryptography to ensure confidentiality of data raises different types of issues from its use protect the integrity of data including through authentication and non-repudiation mechanisms. While noting that the subject of cryptography could be further explored in the future, delegates agreed with the proposed "light" review process based on a questionnaire and short report, with the understanding that the review could be started at any time in the near future. They agreed to provide their comments to the questionnaire by 6 January 2017.

Item 11. Designation of the Bureau for 2017

58. The Secretariat presented current nominations for the Chair and the Bureau: Chair: Ms. Katarina de Brisis, Deputy Director General, Department of National ICT Policy and Public Sector Modernisation, Ministry of Local Government and Modernisation (Norway): Bureau: Manuela Siano (Italy), Mr. Yoshikazu Okamoto (Japan), Beosoom Kim (Korea), Ali Rezaki (Turkey), Heather Butler (UK), Anne Tricaud (France), Jane Hamilton (Canada), Susan Ritchie (United States)

59. The Working Party agreed on the designation of the Bureau.

Item 12 Future Work

12.a. Workshop on Digital Risk Insurance

60. The Secretariat (Elettra Ronchi) provided an update (objectives, proposed draft agenda) on the workshop on digital risk insurance to be held in Switzerland, (the Swiss-Re Centre for Global Dialogue, Rüschlikon) on 12-13 May 2017.

61. The Working Party **agreed** on the plan for the proposed workshop.

12.b. Digital Economy Outlook

DSTI/CDEP(2016)5

62. The Secretariat (David Gierten and Cristina Serra-Vallejo) presented the outline of the Digital Economy Outlook (DEO) and the proposed timeline. Mr. Gierten presented in particular the outline of the DEO chapters to which the SPDE will contribute as well as briefly discuss the SPDE questionnaire received by SPDE delegates.

Item 13. Other Business

63. The Secretariat (Laurent Bernat) provided an update on the international partnership to develop a guide on national cybersecurity strategies (with ITU, OECD, World Bank, ENISA and others). This initiative, which was previously discussed in the SPDE Bureau, would bring together existing recommendations and guidance rather than create something entirely new. The Secretariat stressed that the scope of the work would not include national security and defence aspects and that the draft guide would be circulated to SPDE for informal comments when it would be sufficiently mature.

64. Delegates welcomed the Secretariat's engagement with other international organisations and underlined the opportunity to promote OECD work on a risk-based approach to digital security.

65. Mr. Nat Sakimura provided a brief update on the liaison with the ISO SC27 working groups including 53 participating national bodies and 20 observing national bodies. ISO SC27 working group 5 focus in particular on identity management and privacy technologies. Mr. Sakimura presented the list of major standards and publication released by the group. Delegates noted the presentation.

Close of meeting

66. The Chair closed the meeting after recalling the date for the next SPDE meetings: 15-16 May 2017.

Participants list for Working Party on Security and Privacy in the Digital Economy (WPSPDE)/Liste des participants pour Groupe de travail sur la sécurité et la vie privée dans l'économie numérique (GTSVPEN)

15/11/2016 - 16/11/2016

Austria/Autriche

Mr. Martin FAZOKAS	*Austrian Federal Chancellary*

Canada

Ms. Krista CAMPBELL	*Director General* *Digital Policy Branch* *Innovation, Science and Economic Development Canada*
Ms. Jane HAMILTON	*Senior Policy Advisor and Chair of the WPSPDE* *Privacy and Data Protection Policy Directorate, Digital Policy Branch* *Innovation, Science and Economic Development Canada*

Estonia/Estonie

Ms. Liis REBANE	*Head of Estonian Cyber Security Policy* *Department of State Information Systems* *Ministry of Economic Affairs and Communication*

Finland/Finlande

Mr. Aku HILVE	*Director of Unit* *Public Sector ICT* *Ministry of Finance*
Mr. Juho KORTENIEMI	*Counsellor (Industry, Energy and Regional Development)* *Permanent Delegation of Finland to the OECD*

France

M. Hugues DE FRANCLIEU	*Adjoint au chef du Bureau Politique commerciale* *DG Trésor* *Ministère de l'Economie et des Finances*

M. Matthieu GRALL	*Commission nationale de l'informatique et des libertés (CNIL)*
Ms. Ismini RIGOPOULOU	*Legal and Policy Officer* *European and International Affairs Department* *Commission nationale de l'informatique et des libertés (CNIL)*
Ms. Anne TRICAUD	

Germany/Allemagne

Ms. Daniela FACKELMANN	*European and international IT and digitization* *Federal Ministry of the Interior (BMI)*

Hungary/Hongrie

Mr. András HLÁCS	*Counsellor* *Permanent Delegation of Hungary to the OECD*

Israel/Israël

Alon BACHAR	*Head of the Israeli law, Information and Technology Authority* *Israeli law, Information and Technology Authority*
Ms. Gili BASMAN REINGOLD	*Legal advisor* *Legal Department* *ILITA - The Israeli Law, Information and Technology Authority*

Italy/Italie

Ms. Manuela SIANO	*Italian Data Protection Agency*

Japan/Japon

Mr. Fumio SHIMPO	*Professor* *Faculty of Policy Management* *Keio University*
Mr. Yoshikazu OKAMOTO	*Planning Director* *Personal Information Protection Commission*
Mr. Tatsuya KUROSAKA	*Project Associate Professor* *Graduate School of Media and Governance* *Keio University*

Mr. Nagayuki SAITO — *Researcher*
Research Institute of Keio Media Design

Mr. Daisuke NAGASAKI — *Deputy Director, Office of International Affairs*
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry

Mr. Eiji UEHARA — *First Secretary*
Permanent Delegation of Japan to the OECD

Mr. Masanari YASHIRO — *First Secretary*
Permanent Delegation of Japan to the OECD

Korea/Corée

Mr. Kyeongman KIM — *First Secretary*
ICT, Science, and Nuclear Energy
Permanent Delegation of the Republic of Korea to the OECD

Bok Duk CHUNG — *Deputy Director*
Korea Communications Commission

Dr. Beomsoo KIM — *Professor, Associate Dean*
Graduate School of Information
Yonsei University

Kyonwoo SON — *Deputy Director*
Korea Communications Commission (KCC)

Mexico/Mexique

Mr. Guillermo GARCIA HERNANDEZ — *Minister-Counsellor for the Ministry of Economy*
Secretaria de Economia
Permanent Delegation of Mexico to the OECD

Mr. Carlos TENA — *Third Secretary*
Permanent Delegation

M. Philippe BETEMPS — *Executive Officer, Ministry of the Economy*
Représentation à Paris
Délégation Permanente du Mexique auprès de OCDE

Netherlands/Pays-Bas

Mr. Wim RULLENS	*Head International Organisations* *Directorate General Energy, Telecommunications and Markets* *Ministry of Economic Affairs*
Ms. Natalia CERRATO	*Economic Counsellor* *Permanent Representation of the Kingdom of the Netherlands to the OECD*

Norway/Norvège

Ms. Katarina DE BRISIS	*Deputy Director General* *Department of National IT-policy* *Ministry of Local Government and Modernisation*
Ms. Åste Marie SKULLERUD	*Department Director* *Department of Government Services* *Ministry of Local Government and Modernisation*
Mr. Cort Archer DREYER	*Senior Adviser* *Department of ICT Policy and public sector reform* *Ministry of Local Government and Modernisation*
Mr. Christian F. MATHIESSEN	*Senior Adviser* *Ministry of Justice and Public Security*

Portugal

Professor Luís MAGALHÃES	*IST, Instituto Superior Técnico, Universidade de Lisboa*
M. Manuel PEDROSA DE BARROS	*Director* *Communications Security Directorate* *ICP-ANACOM*
Mr. Pedro MATOS	*International Affairs* *Department of Information Society* *Fundação para a Ciência e a Tecnologia*

Ms. Maria OLIVEIRA FERNANDES — *Counsellor*
Permanent Delegation of Portugal to the OECD

Spain/Espagne

Mr. Jose Luis BARRON — *Chief of Area in Public Services and Contents*
Directorate for Information Technologies and Communications
Ministry of Finance and Public Fonctions

Ms. Maria DE MIGUEL — *Chief of Service*
SECRETARY OF STATE FOR TELECOMMUNICATIONS AND INFORMATION SOCIETY
Ministry of Energy, Tourism and Digital Agenda

Mr. Emilio GARCIA GARCIA — *Conseiller*
Departement des Relations Internationales
Ministry of Finances and Public Administration

Sweden/Suède

Mr. Ingolf BERG — *Head of Section*
Ministry of Enterprise and Innovation

Switzerland/Suisse

Mr. Peter PÜNTENER — *Conseiller d'ambassade*
Délégation suisse près l'OCDE

Turkey/Turquie

Mr. Mesut AYDIN — *Counsellor*
Permanent Delegation of Turkey to the OECD

Mr. Ali REZAKI — *Deputy Director*
BILGEM-SGE
The Scientific and Technical Research Council of Turkey (TÜBITAK)

United Kingdom/Royaume-Uni

Ms. Heather BUTLER — *Department for Culture Media and Sport*

Ms. Sabine GERDON	*Department for Culture Media and Sport*
Mr. David SMITH	

United States/États-Unis

Ms. Nasreen DJOUINI	*International Trade Specialist* *International Trade Administration* *Department of Commerce*
Ms. Susan RITCHIE	*Senior Advisor* *Economic Bureau* *Department of State*
Mr. Hugh STEVENSON	*Deputy Director for Int'l Consumer Protection* *US Federal Trade Commission*
Mr. Seth VAUGHN	*Environment, Science and Technology Advisor* *Permanent Delegation of the United States to the OECD*

Colombia/Colombie

Mr. Juan Manuel WILCHES	*Commissioner* *Communications Regulation Commission*

Russian Federation/Fédération de Russie

Mr. Nikolai Nikolayevich MURASHOV	*Federal Security Service*
Mr. Alexandr SAVELEV	*Senior Researcher* *Information law* *Higher School of Economics*

Ms. Elena TORBENKO	*Head of Division* *FSTEC*
Svetlana VOLKOVA	*Expert* *Federal Security Service (FSB) fo the Russian Federation*
Mr. Andrey ZHIVOV	*Department of International Copperation* *Ministry of Telecommunications and Mass Communications*

Brazil/Brésil

Mr. Pedro Lucas ARAUJO	*Project Manager* *Department of Broadband* *Ministry of Science, Technology, Innovations and Communications*
Mr. Carlos DA FONSECA	*Counsellor* *Head of the Information Society Division* *Ministry of Foreign Affairs*
Mr. Cesario Marcos LOPES DE ALEXANDRIA	*Counsellor* *Embassy of Brazil in France*
Mr. Pedro MENEZES	*Public Policy Specialist* *Secretariat for Information Technology Policy* *Ministry of Science and Technology*

Egypt/Égypte

Dr. Sherif HASHEM	*Vice President for CyberSecurity* *Egyptian National Telecom Authority (NTRA)*

Business and Industry Advisory Committee (BIAC)/Comité consultatif économique et industriel (BIAC)

Mr. Joseph ALHADEFF	*Chair of the BIAC Committee on Digital Policy* *Vice President for Global Public Policy and Chief Privacy Strategist* *Oracle Corporation*
Dr. Richard CLARKE	*Assistant Vice President, Global Public Policy* *AT&T*
Mr. Riccardo MASUCCI	*Intel Corporation*
Mr. Christopher Nicolas MÜLLER	*BIAC*

Civil Society Information Society Advisory Council

Mr. Suso BALEATO	*CSISAC*
Ms. Wafa BEN HASSINE	
Mr. Marc ROTENBERG	*Executive Director* *Electronic Privacy Information Center (EPIC)*

Internet Technical Advisory Committee

Mr. Gershon JANSSEN	*International Standards Policy Advisor* *OASIS*
Ms. Karen MCCABE	*Senior Director* *Technology Policy and International Affairs* *IEEE*
Mr. Natsuhiko SAKIMURA	*Kantara Initiative*
Mr. Benjamin DEAN	*Columbia University*

CloudFlare

Dr. Michael NELSON	*Public Policy* *CloudFlare*

FERMA

M. Gilbert CANAMERAS	*FERMA*

Swiss Reinsurance Company Ltd

Mr. Eric SCHUH	*Casualty Underwriting* *Swiss Reinsurance Company Ltd*

OECD/OCDE

M. Laurent BERNAT	*Policy Analyst - Cybersecurity, privacy, digital identity* *STI/DEP*
Ms. Claire HILTON	*Junior Research Assistant* *STI/DEP*
Mr. Christian REIMSBACH-KOUNATZE	*Economist/Policy Analyst - Economics of big data, employment/skills, green ICT* *STI/DEP*
Ms. Elettra RONCHI	*Senior Policy Analyst - Privacy, Security, Digital Economy* *STI/DEP*

Other/Autre

M. Philippe COTELLE	*Head of Insurance Risk Management* *Airbus Defence and Space*
Mr. Philippe LAURIER	
Ms. Bénédicte SUZAN	*Airbus Group*
M. Philippe WOLF	*IRT-SystemX*