OECD Digital Economy Papers No. 210

Terms of Reference for the Review of the OECD Guidelines for the Security of Information Systems and Networks

OECD

Unclassified **DSTI/ICCP/REG(2012)6/FINAL**

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

16-Nov-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Information Security and Privacy

TERMS OF REFERENCE FOR THE REVIEW OF THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

JT03330864

Complete document available on OLIS in its original format
This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

DSTI/ICCP/REG(2012)6/FINAL
Unclassified

English - Or. English

TERMS OF REFERENCE FOR THE REVIEW OF THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

1. At the time of their adoption, the 2002 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security ("Security Guidelines") expressed an international consensus across participants from governments, businesses and civil society regarding security of information systems in a society characterised by network interconnectivity. They provided a framework of principles to protect and foster confidence in information systems and networks in a context where systems and networks played an increasingly significant role and where the stability and efficiency of national economies, international trade and social, cultural and political life increasingly depended on them.

2. Ten years later, there is a consensus among OECD members as well as non-governmental stakeholders to review, solicit input and perhaps, as a result, revise this instrument in light of continuing developments affecting the Internet economy at technical, economic, social and policy levels. These Terms of Reference[1] provide a brief description of the Guidelines and of the context, objectives, scope, and modalities for this process going forward.

The 2002 Security Guidelines[2]

3. In 1992, the OECD Council adopted the first Guidelines on the Security of Information Systems. They introduced nine principles for ensuring the security of information systems and high level recommendations regarding their implementation. An explanatory memorandum was also developed to accompany the Guidelines. Ten years later, the OECD reviewed the Guidelines to take into account the generalised adoption of Internet technologies which enabled the openness and interconnection of formerly closed and isolated information systems.

4. The revised Guidelines reflected a dramatic shift in the way security of information systems should be approached in an open digital world. Taking into account the increased reliance of all participants on information systems, networks and their related services, the 2002 Guidelines made a break with a time when secure design and use of networks and systems were too often afterthoughts. In order to respond to the ever-changing environment that results from the openness and interconnectivity of information systems based on Internet technologies, they called for a culture of security for information systems and networks where each participant is aware of the relevant security risks, assumes a degree of responsibility according to its role and where everyone takes steps to enhance security. They promoted a security approach that takes due account of the interests of all participants and the nature of the systems, networks and related services in order to provide effective security.

[1] These Terms of Reference were prepared by the Working Party on Information Security and Privacy (WPISP) and declassified by the Committee for Information, Computer and Communications Policy (ICCP) by the written procedure in November 2012.

[2] For more background about the history and role of the Security Guidelines, see OECD, 2012b.

5. To support this approach, the Guidelines were designed to include nine complementary high-level principles for all participants at all levels, including policy and operational levels. The principles create a framework for security in an open digital world where, instead of avoiding risk by limiting interconnectivity, participants determine the level of risk they can accept and manage security to reduce risk to that level. The principles can be used by decision makers in public and private sector organisations for the development of their security policies, as well as by government policy makers for the development of national public policies.

6. In contrast with the 1992 Guidelines, the 2002 revised Guidelines did not provide recommendations regarding the implementation of the principles and they were not accompanied by an explanatory memorandum. However, over the last ten years, the OECD has carried out in-depth analytical work in this area, monitoring technical and policy developments and developing policy recommendations in various areas. In particular, in 2008 the OECD Council adopted a Recommendation which provides policy and operational guidance for implementing the Security Guidelines in relation to the protection of Critical Information Infrastructures (CII) (OECD, 2008a).

7. Translated into ten additional languages including Chinese and Russian, the 2002 Security Guidelines have been widely disseminated and have had considerable impact. The United Nations Resolution Concerning the Creation of a Global Culture of Cybersecurity (United Nations, 2002) reflected the nine principles of the Guidelines and invited "Member States and all relevant international organisations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005". The Guidelines were also reflected in the European Council Resolution "on a European approach towards a culture of network and information security" (European Council, 2003) and in the Asia-Pacific "Strategy to Ensure a Trusted, Secure and Sustainable Online Environment" (APEC, 2005).

Context for the Review

8. The 2002 Security Guidelines anticipated the general adoption of broadband Internet which was at a very early stage in 2002 and is now a key feature of the Internet economy throughout the OECD and beyond. This review is undertaken in a context in which technology developments and ICT usage are characterised by a considerable increase in take-up and continued innovation. Ten years of innovation at all levels have marked the development of the Internet economy built upon an infrastructure offering faster speeds, greater bandwidth and wireless connectivity. Digital mobility is changing modes of consumption and business practices. It has created opportunities for unanticipated economic and social developments. Increased network, storage and processing capacity has enabled the emergence of "cloud computing" as a new IT operational model which in turn simplifies the technical implementation of new ideas by entrepreneurs and reduces cost for businesses and governments, among other benefits. Devices have considerably evolved with the spread of smartphones, tablets, e-readers, connected TV sets, RFID chips, sensors and smart appliances. Software innovation stimulated the emergence of new business models such as the "app economy" and "big data". The rapid and wide adoption of social media and Web 2.0, the spread of digital mobility, and of geolocation are good illustrations, among others, of the Internet economy as a vibrant technical, economic and social environment that benefits all sectors of the economy and the society.

9. The Security Guidelines are to be reviewed every five years "so as to foster international co-operation on issues relating to the security of information systems and networks". The first review, in 2007, concluded that there was no need for revisions, although some delegations highlighted areas for possible future improvement. This second five-year review also takes inspiration from the 2008 Seoul Declaration on the Future of the Internet Economy, in which Ministers invited the OECD to assess their

application "in light of changing technologies, markets and user behaviour" (OECD, 2008b). The growing importance of the issues covered in this review was further highlighted in the OECD Recommendation on Principles for Internet Policy Making (OECD, 2011) which calls for Members to encourage co-operation to promote Internet security. The annex to the Recommendation explains that policies to enhance online security should not disrupt the framework conditions that enable the Internet to operate as a global open platform for innovation, growth and social progress.

10. Responses to a questionnaire circulated to delegations in June 2012 for the second review of the Guidelines, confirmed by discussions in the Working Party on Information Security and Privacy (WPISP), demonstrated a consensus among OECD delegations on the need to further review the Guidelines. This consensus results from the recognition of several main trends, such as:

- *The threat landscape has evolved in scale and in kind.* Since 2002, cybercriminality has considerably increased. Moreover, the exploitation of vulnerabilities in information systems provides an opportunity for economic, social and political disruptions of all kinds ("hacktivism"). Cybercriminals are increasingly sophisticated. Large scale cyber incidents affecting millions of users are becoming common. New and more sophisticated actors and attacks such as in relation to cyberespionage and "advanced persistent threats" are emerging, sometimes involving governments and threatening intellectual property or state secrets. Finally, there is a risk that information systems and networks become a new battleground for state rivalries, to the detriment of legitimate users and of the stability of this global digital ecosystem.

- *The perimeter of information systems is increasingly blurred.* In 2002, a key trend was the interconnection of previously isolated and clearly defined information systems. But interconnectivity has gone so fast and so far over the last ten years that the very concept of a discrete "information system" is being challenged. In this "hyper connected" world, information systems are becoming inextricably interwoven and mixed through the fast adoption of technologies such as cloud computing and practices such as the access by partners, contractors and customers to shared networked resources, and so-called "bring your own device" policies in organisations. In this hyper connected world - where every process, device and infrastructure is in some way interconnected - it is becoming difficult to define the perimeter of information systems or corporate networks. Today, networks transcend traditional boundaries to the point where they form a broader global ecosystem which cannot just be dealt with in its discrete parts.

- *IT and the Internet have evolved from being useful to individuals and organisations to being also essential to the society.* They have become a key source of growth and a driver for innovation and for economic and social development. But this success has also increased the dependence of our economy and society on these technologies. This dependence, which was one of the drivers of the adoption of the 2002 Security Guidelines, has evolved beyond the reliance of each economic and social actor on information systems and networks to carry out their daily activities. This hyper connected world has become essential to economic prosperity, to the functioning of critical infrastructures and to national security. Therefore security is no longer only a challenge for individual participants as contemplated in the 2002 Guidelines, it is also a collective priority for the society.

- *Cybersecurity policy making is at a turning point* (OECD, 2012a). Responding to cybersecurity challenges has become a national policy priority in many countries. Governments are developing comprehensive approaches integrating all facets of cybersecurity into holistic frameworks covering economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. New national strategies to strengthen cybersecurity are pursuing a double objective: *i)* to further drive economic and social prosperity and realise the full potential of the Internet as a new source of growth and platform for innovation, and *ii)* protecting cyberspace-reliant societies against cyber-threats. In so doing, policy makers face complex co-ordination and co-operation challenges, internally across governmental bodies, and with non-governmental stakeholders, both at the domestic and international levels. They also have to develop and implement action plans according to their strategies in a variety of areas such as critical information infrastructure protection, research and development, skills and jobs, economic incentives, cybersecurity exercises, etc.

11. The examination of the 2002 Guidelines in the light of these trends does not challenge the basic relevance of their principles. The recognition that only a flexible, holistic, risk-based approach can take into account the ever-changing nature of threats, vulnerabilities and impact in an open and interconnected environment is still valid. The seriousness of the threat landscape suggests that the effective application of the Guidelines is increasingly urgent.

12. The language of the Guidelines is based on the assumption that security should result from the protection of *information systems and networks*. It is recognised, however, that *the perimeter of information systems and networks is increasingly blurred* and that, as a consequence, the management of risks and the protection measures should extend to the more global ecosystem level.

13. In addition, the emergence of cybersecurity as a policy priority in governments and in organisations reveals a gap within the Security Guidelines. The overarching objective of new national cybersecurity strategies is to support economic and social development and to protect the functioning of society; and the objective of participants who adopt a security policy is to enable their organisation to achieve its goals and aspirations, rather than to protect its systems and networks. While this is consistent with the intention of the 2002 Security Guidelines, some of the terms they use such as the focus on the security of *information systems and networks*, can be perceived as though the main challenge were only of a technical nature.

Objectives, scope and approach to the review

14. The policy framework formed by the Guidelines' principles is still considered generally *valid* to address security in an open and interconnected technical environment. However, there is a general agreement that this framework is in need of review to assess whether it is *sufficient* to help participants reduce to an acceptable level the risk that security challenges pose to the further development of the Internet economy and to its contribution to economic and social prosperity. Over the last ten years, this level of acceptable risk has changed as the role of information systems and networks in the economy and society became essential and as threats and vulnerabilities have increased. Security issues are no longer perceived as just a technical challenge focusing on systems and networks. Today, security is considered as a means to address risks faced by participants and by the society as a whole in the realisation of their economic and social aspirations.

15. Therefore the review could aim to strengthen the Guidelines by realigning their perspective and language with the high-level economic and social objectives pursued by governments, businesses and individuals in the development of cybersecurity policies. The review could also facilitate the application of the Guidelines' principles by all participants. However, if revisions are forthcoming, the Guidelines as a whole should remain high level and technology neutral in order to remain relevant in a fast-evolving area.

16. In particular, the review of the Guidelines should aim to:

- Update, strengthen and complement the current Guidelines, including the principles, with a view to enhancing their impact in current and future contexts while preserving their internal coherence and overall logic.

- Facilitate the application of the principles through the development of guidance for government policy making and international co-operation in the area of cybersecurity for the Internet economy, based on the findings of the OECD comparative analysis of national cybersecurity strategies (OECD, 2012).

- Explore the value of integrating the 2008 Recommendation for the Protection of Critical Information Infrastructure into the Security Guidelines, with the objective of increasing the visibility of the former and the completeness of the latter, as they share the same objective of furthering the development of the Internet economy.

- Develop explanatory text to accompany the Guidelines' principles, facilitate their interpretation by all stakeholders and improve their impact.

Modalities

17. Consistent with the OECD Recommendation on Principles for Internet Policy Making (OECD, 2011) the first phase of the Security Guidelines' review will be conducted with the benefit of active participation of a wide variety of experts from governments, academics, business, civil society, the Internet technical community, as well as representatives of other international organisations. Expert input from member and non-member economies will be welcome. The experts will work primarily electronically. Teleconferences and/or occasional in-person meetings might be organised, as appropriate. To the extent possible such meetings would be held on the margins of already-planned events.

18. The purpose of these informal expert group discussions is to explore and prepare recommendations for consideration by OECD members at the Working Party on Information Security and Privacy (WPISP), within the scope outlined above, to ensure the continued effectiveness of the OECD framework for security of information systems and networks.

19. Building on suggestions already expressed in previous work (OECD, 2012a) and material provided in responses to the questionnaire circulated in the first part of 2012, the Secretariat will develop draft proposals in each of the areas identified for the review. Within one year, experts will be invited to discuss these proposals and make new ones to the Secretariat, with a view to informing the preparation of possible revisions by the WPISP. A progress report will be presented to the WPISP at its April 2013 meeting where delegates will have an opportunity to provide additional direction to the expert group. Further opportunities for consultation, including with non-members, can be considered as the process evolves. At the end of this first phase, the WPISP will decide if revisions are necessary and if so, begin the drafting process.

REFERENCES

APEC (2005), APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment. Available at: www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx

European Council (2003), Council Resolution on a European approach towards a culture of network and information security. Available at: www.oecd.org/dataoecd/53/59/37019852.pdf.

OECD (2002), Recommendation of the Council on Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Available at: http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=116&InstrumentPID=112&Lang=en&Book=False.

OECD (2008a), Recommendation of the Council on Protection of Critical Information Infrastructures. Available at: http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117&Lang=en&Book=False

OECD (2008b), Declaration for the Future of the Internet Economy (The Seoul Declaration). Available at: www.oecd.org/dataoecd/49/28/40839436.pdf.

OECD (2011), Recommendation of the Council on Principles for Internet Policy Making. Available at: www.oecd.org/internet/interneteconomy/49258588.pdf

OECD (2012a), Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy". [DSTI/ICCP/REG(2011)12/FINAL].

OECD (2012b), The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy. [DSTI/ICCP/REG(2012)8/FINAL]

United Nations (2002), Resolution Concerning the Creation of a Global Culture of Cybersecurity, A/RES/57/239. Available at www.oecd.org/dataoecd/53/60/37019786.pdf