Poland wishes to thank the CWG Internet Chairman for opening this valuable public consultation on the Res. 1305. In response to that Poland reached out for the national sector and compiled this contribution with a view to share some of the finest examples of the Res. 1305 Annex 1 output.

We received a number of multistakeholder comments on that call, which all show that the openness of the Internet policy-making forums has intensively been looked for and that there are a lot of inputs that can enrich the discussion on the way forward for the Internet.

NOTE: Some of the contributions go beyond the Res. 1305 timespan i.e. before 2009 when the resolution and the Annex 1 Public Policy issues were adopted. Nevertheless a decision was taken not to crop them out so that the line of continuous commitment from some of the contributors was clearly seen.

Contributors: Ministry of Administration and Digitization (MAC), Office of Electronic Communications (UKE), Ministry of the Interior, Internal Security Agency (ABW), Research and Academy Computer Network (NASK), Poznań Supercomputing and Networking Centre (PCSS), Warsaw Technical University, Polish Chamber for Electronic Communication (PIKE).

Activities in Res. 1305 public policy issues broken into government agenda or other entity.

1. **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**
   a. **NASK[1] (Research and Academy Computer Network)**

Introduction of IDNs (2003) enabling the use of Polish language symbols in domain naming. Apart from substantial extension of naming register it provides facilities for ethnic minorities to register Internet domains using their mother tongue.

2. **International Internet Connectivity**
   a. **NASK**

NASK's international Internet connectivity is run mainly by means of purchasing services from international connectivity operators and through the DECIX (Internet exchange point based in Frankfurt).
Inter-operator cooperation is also carried out by way of offering services to companies based out of Poland.

   b. **PCSS[2] (Poznań Supercomputing and Networking Centre)**

Managing, developing and operating of the **Polish Optical Internet PIONIER[3]**, a nationwide broadband optical network that represents a base for research and development in the area of information technology and telecommunications, computing sciences (grids, etc.), applications and services for the Information Society.

3. **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**

   a. **Gdansk Technical University[4]**

[1] under the Ministry of Science and Higher Education, www.nask.pl
[2] www.man.poznan.pl
[3] www.pionier.net.pl
[4] www.pg.edu.pl

Active contribution to the global standardization process through participation in the Internet Engineering Task Force (IETF) and the International Federation for Information Processing (IFIP).

b. NASK

Committed, long-standing and active participation in the Council of European national Top Level Registries (CENTR, an association of Internet ccTLDs) and the ICANN. NASK is the sole funder, contributor and supporter of the Polish delegate to the GAC ICANN. It also delegated staff to the Management Board of ENISA. Since 2010 it has also been member of the Country Code Names Supporting Organization and is active in the RIPE Network Coordination Center.

c. PCSS

Launching of the K-root DNS server on the PIONIER network (2004) in Poznań. The server was the first one of this kind to have been set up in Poland and the Central and Eastern Europe.

4. The security, safety, continuity, sustainability, and robustness of the Internet

a. Warsaw Technical University[5]

Developing of the **NEWMAN** project. It aims at rolling out of infrastructure, staff training at regional level, supporting R&D of Polish research teams through exchange of information with facilities around the world by means of the backbone network of the Polish Optical Internet PIONIER.
The university is also running the projects PL-GRID and PL-GRID plus under which national data shops[6] are set up and developed.

b. NASK

- The main line around which NASK's Internet safety activities are structured is expanding and maintaining capacities for enhanced response on emerging network threats, which since 1996 has been channeled through the **CERT Polska**.
  CERT Poland was the first response team to have been established in Poland, tasked with taking measures to combat cyber-threats. Apart from that it also disseminates safety breach related information across end users and by constant cooperation with other CERTs it continuously develops in order to provide up-to-date and relevant service.

- Last year NASK took control over the government domain **.gov.pl.** with a view to provide enhanced protection on valuable resources.

c. ABW (Internal Security Agency)[7] (crosscutting activity covering section 5, 8 and 9)

- Development and adoption of cyberspace security policy
- Development of the **SBC.POL project** (Cyberspace Security System) in Poland.
- Cooperation at **pl. ID, CEPIK 2.0** projects on e-administration
- Creation of enabling environment on security through working out of recommendations and reports on cyber security.

d. MSW[8] (Ministry of the Interior)

[5] www.pw.edu.pl
[6] Facilities to manage geographically dispersed data with a view to making it available to research centers.
[7] www.abw.gov.pl

- Establishment of **CERT.GOV.PL** - the Governmental Computer Security Incident Response Team (2008) with the chief task in ensuring and developing the capability of public administration units to protect themselves against cyber-threats, in particular against attacks aimed at the infrastructure involving IT systems and networks.
- The **ARAKIS-GOV** system. An early warning system reporting threats arising on the Internet. The system has been developed by the IT Security Department of the Polish Internal Security Agency in cooperation with the CERT Polska. It was established in order to support the existing security measures protecting IT resources of public administration.

e. PCSS

- Establishment of the **PIONIER CERT** team (2001) tasked with security provision over the PIONIER network. One of the recent extensions of its terms of reference was launching research on DDoS (Distributed Denial of Service) type of cyber-threats.
- PCSS is also **active in cyber security R&D**. For example, in 2010-12 it developed the project "*High-security advanced architecture of the Integrated IT Platform*" meant for use by the Police. It produced a safe IT network and application environment allowing reliable, effective, calibration- and storage-friendly data processing, as well making available of applications. Other PCSS projects: "*Management of information and knowledge in services requiring higher level of protection*" with the outcome of a dispersed detection system targeting MetaIDS intruders or "*Sensory data correlation module for detecting unwarranted behavior and supporting decision-taking process (SECOR)*"
- **Running wide-reaching trainings** is another example of PCSS activity (many different target groups, various levels, technology-oriented studies), part of which, when recorded, is made available to the public free of charge.

5. Combating Cybercrime

a. NASK

- **Training.** In 2013 NASK trained ca. 500 enforcement agencies and justice affairs officers in combating cybercrime, with a focus on fighting sexual child abuse and child pornography.
- **CERT Polska.** Apart from standard assignment relating to incidents handling, coordination, collecting and sharing information on threats, CERT Polska specializes in analysis of malware and neutralization of botnets. Through CERT, NASK reaches out to cooperate with enforcement and government agencies in Poland and abroad.
- **Dyżurnet.pl.** NASK's response team tasked with receiving and reacting to notifications on illegal contents (especially child sexual abuse) on the Internet. All verified notifications are sent over to the Police or contact points at the International Association of Internet Hotlines (INHOPE).
- Full **implementation of the Domain Name Security Extension** (DNSSEC) on the .pl domain (2012).

b. MSW

- **"Razem bezpieczniej** (*Safer together*)**"** funding scheme. The programme mobilizes resources to co-finance regional level's and NGOs' projects aiming at limiting risks of threats including on the Internet.

[8] www. msw.gov.pl

- **Hotline 116111** (2008). The facility has enabled minors to report all threats on the Internet. Verified notifications are sent over to the Police or the dyżurnet.pl.
- Creation of **a cyber-security department** at the National Police Headquarters (2010)
- **Amended law –** adding new types of crime to the penal code (2009) enabling penalization of criminally approaching minors under 15 through means of telecommunications.

c. PCSS

- Active participation in the works of the PPBW (Polish Platform for Homeland Security). For one of the joint projects called "*Management of information and knowledge in services requiring higher level of protection*" the two agencies took up the issue of exchange of retention data between telecommunications operators and authorized information handlers (e.g. Police). The outcome was in working out a **standard format for exchange of information**, based on the XML and the ETSI technical specification TS 102 657.
- Based on that format, PCSS managed to develop a tentative prototype of the **SOPEL** system (Electronic crime exchange of information system). Plans for further development are in place.
- Further research is planned on combating cyber-crime, e.g.: development of systems detecting abnormalities of networks as well as sensory security systems.

6. Dealing effectively with spam

a. NASK

CERT Polska is active in fighting spam affecting Polish networks. The measures applied include deactivation of botnets and removing malware from computers used for spamming. That removal is basically carried by ISPs who are approached and notified through a special CERT Polska's IT platform - **n6**[9].

7. Issues pertaining to the use and misuse of the Internet

a. UKE[10] (Office of Electronic Communications)

- On 11 September 2013, the President of UKE published a **Manual on illegal practices of using telecommunications services and possible measures to protect safety, privacy and personal data when using publicly available telecommunications services[11].**
- In 2009, a certification programme of telecommunications services was launched by the Office of Electronic Communications. Between 2009 and 2013 telecommunications undertakings were awarded certificates, including in the **"Fair transfer" category**. The telecommunications undertakings who were awarded certificates in the "Fair transfer" category were obliged to provide transparent and reliable commercial information addressed to their customers as well as transparent procedures for the removal of failures and line verification, accompanied by information to the customer.

[9] http://n6.cert.pl
[10] National regulatory authority, www.uke.gov.pl
[11] www.uke.gov.pl/badz-swiadomy-zagrozen-w-sieci-12885

- In addition, the President of UKE takes numerous information and education measures - during direct meetings with consumers and by means of a Consumer Information Centre[12].

b. DSI MAC (Department of the information Society, Ministry of Administration and Digitization)

- Polish government supports all activities which aim to promote better understanding of a digital world among children, their parents and teachers. We encourage the safe use of the Internet and other digital media. In this context NGOs receive support from the government for their activities in the field of child protection on the Internet. Through open public competitions, announced by the Ministry of Administration and Digitalization in the second half of 2013, several projects, which aim at increasing of knowledge and skills in the use of the Internet, received substantial financial support. Various state-founded NGOs and public bodies are also tasked with combating child abuse and removing illegal online material, including child pornography. We are not, however, planning on introducing any sort of general filtering system, as these are expensive to set up and operate, have been proven to be ineffective and easy to circumvent, while often blocking legitimate content in the process. We encourage however the use of end-user solutions to protect minors from exposure to harmful content.

- The Polish government supports the development of Internet tools to increase capacity of the public authorities to improve transparency of the decision making process and dialogue with the citizens. We also support easy access to public sector information and we are planning to create user friendly tool for re-use of information that are stored by public authorities. We should work for the Internet to remain a free and unfettered media serving the free exchange of opinions in accordance with the initial assumption of its creators.

c. PCSS

- Cooperation was established with a number of secondary and post-secondary schools in the region. Its framework includes lectures for students, their parents, teaching staff, including on the occasions of the Safer Internet Day or school conferences grouping delegations from enforcement agencies, psychologists or those held at the request of teachers. Topics covered include: safe use of the Internet technologies, the issues of the use or yielding to cyberbullying, copyright infringement. Ways to get help are also being indicated.

- PCSS elaborated also on the use of modern IT technologies, in particular solutions available via the Internet, especially web pages and e-mail (training publication available free of charge).

8. Availability, affordability, reliability, and quality of service, especially in the developing world

a. UKE

- The President of UKE published its **Final Report on the outcome of work on identification of quality of service indicators** which was developed as part of the

[12] www.cik.uke.gov.pl

Memorandum for improving the quality of telecommunications services as a document drawn jointly and agreed between the Memorandum Leader (the President of UKE) and 44 Signatories to the Memorandum on Quality (telecommunications undertakings, service providers, measurement companies, scientific bodies and consumer organizations). All Signatories committed themselves to jointly strive for ensuring reliable and comparable information about quality of service (QoS) indicators for consumers[13].

- In order to launch measurement campaigns and further operations a **Steering Committee for Mobile Network Measurements** will be established in early 2014. It will be composed of telecommunications undertakings affected by the measurements (operators providing services in mobile networks) and the Office of Electronic Communications on equal footing. The first measurement campaign is planned for 1st half of 2014. Such measurement sessions are planned twice per year. UKE will have supervisory functions over these measurements. The measurements will be conducted by an independent entity (a measurement company). The choice of a measurement route should take account of population distribution patterns, traffic patterns and the area of service provision. The minimum duration of the measurement campaign is 800 hours. At least 80% of the measurements will be conducted in motion.
- UKE conducts **permanent quality tests for telephone calls** in PSTN, calls from PSTN to GSM networks and fax over PSTN, using the AWP-IŁ system (some 1000 probes).
- UKE has 4 ROMES (Rode&Schwarz) measurement sets for the assessment of quality of service indicators for voice and Internet access services over mobile networks. UKE conducts periodic measurements in large cities, on domestic highways and railway routes.
- UKE has an nGenius system for the measurement of availability and quality indicators in IP networks (measurement probes are installed at border routers of service providers).
- In 2014, UKE plans to implement a project aimed at developing a reliable IT tool for end-to-end measurement of broadband network parameters. UKE will make the System for Internet Quality Measurement (SMJI) available to Internet end users (clients) and the results of these measurements will be sent and stored in the SMJI in order to prepare reports and visualise measurement outcomes on a digital map of Poland.
- To ensure maximum benefits for users in terms of choice, price and quality of telecommunications services as well as effective and transparent enforcement of the obligation to publish information on the quality of publicly available telecommunications services (QoS), the **President of UKE published reports on the quality of service indicators for publicly available telecommunications services**. The purpose of quarterly publication of indicators for the networks of the tested undertakings is to compare the quality of services provided by individual operators for different types of such services (telephony, fax, data transmission) in fixed-line (PSTN) and mobile (GSM) networks. This information may be useful both for consumers when choosing their provider of telecommunications services and for

[13] http://www.uke.gov.pl/nie-tylko-cena-przejrzyste-wskazniki-jakosci-uslug-13191

telecommunications undertakings in order to improve the quality of their network operation[14].

- As regards affordability of telecommunications services, the President of UKE published the **Position of the President of UKE of 19 July 2010 regarding the control of compliance with certain regulatory obligations, including assessment of price lists and rules and regulations of service provision, by the operator with significant market power in the retail market**. The purpose of this Position is to present the basic rules applied by the President of UKE in enforcement of regulatory obligations imposed on the undertaking with significant market power in retail markets, including price obligations[15].

- As regards availability and affordability, the President of UKE presented on 16 October 2012 a **Report on ensuring individual services comprising universal service by the market after expiration of the relevant obligation imposed on the designated operator** (i.e. after 8 May 2011). The document presented makes an assessment of the availability and affordability of services comprising universal service[16].

- As regards affordability of telecommunications services, the President of UKE in 2009 launched a certification programme of telecommunications services aimed at supporting equal and effective competition in the provision of telecommunications services - for the category "Offer comparison website." The certification programme of the President of UKE in the "Offer comparison website" category is addressed to entities operating in the telecommunications sector which provide price benchmarks for a wide range of telecommunications services.

b. PCSS

- There is a number of cutting-edge services to the PIONIER network that make it go beyond a standards level of commercial networks. These include applications allowing for advanced DVC sessions, dispersed calculations, universal hard drive, huge-scale calculations, etc. Those tools provide the academia with more access to and reliability of better quality networks.

- PCSS is closely cooperating with leading manufacturers of IT and measuring equipment. The joint efforts and solutions may have the potential for being implemented in final products making their way to the market.

c. NASK

Introduction of the Registry-Registrar system of partnership with entities representing domain subscribers, which allows them to be approached with the NASK's wholesale offer. That in turn works for the end user who enjoys more choice on the market both in terms of pricing and quality.

9. Contributing to capacity building for Internet governance in developing countries

No contributions received

[14] www.uke.gov.pl/files/?id_plik=10272 (sample report).
[15] www.uke.gov.pl/files/?id_plik=7350
[16] www.uke.gov.pl/files/?id_plik=10826

10. Developmental aspects of the Internet

a. NASK

- On 10th December 2013, all blocked regional names were finally made available for registration which soon had almost the whole pool registered or booked for registration.
- NASK is planning on the .PL Registry Lock to become a standard security measure along the Register still in 2014.
- There are plans also to implement modern, technologically advanced Registrar System allowing independent, self-reliant domain names management at end user level.

b. Warsaw Technological University

The Future Internet Engineering project in 2010-13. A joint effort of leading Polish technical universities. The project looked at ways to develop and evaluate next generation Internet infrastructure, including aspects of IPv6.

11. Respect for privacy and the protection of personal information and data

a. NASK

Information on domain names administered by NASK can be accessed using the WHOIS application which is a generally available database holding information on Internet domain subscribers. Information on subscribers and on domains subscribed is publicly available which respects rights of Internet users, trademarks owners, copy rights, etc.

b. PCSS

- Plans in place to launch the "TOR-box" research project, allowing end users, when in untrusted environment to request that a safe and anonymous communication channel be set-up (through e.g. a cell phone). PCSS is also looking forward to starting wide-reaching research on on-line privacy of end users using mobile devices, e.g. smartphones, palmtops, wearable electronics as well as the Internet of Things-related computer systems.
- Development and making operational of all-in-one systems of data storage, e.g. PLATON - Science Services Platform or the National Data Storage (both available at a national level, offering remote archiving and backup as added value to the PIONIER network).

c. DSI MAC

- In Poland the right to privacy and protection of personal data is a constitutional fundamental right – Poles, having experienced a totalitarian regime are especially sensitive on this subject. The Polish government is very much involved in the work on the new EU general data protection regulation, as we believe it is one of the most important pieces of legislation currently under discussion in Brussels. It will shape the area of personal data protection law in Europe for the next 20 years. The Polish government's objective during the work on the regulation is to develop the provisions that will ensure a high level of personal data protection without hindering the business activity of European enterprises.

- We are also involved in the process of modernization of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, a legal instrument of wider application that has recently transcended the borders of Europe. Poland believes it is time to begin work on a global scale convention on the protection of personal data. The ease with which data may be transferred across borders renders national legislation ineffective.

- The threats to personal privacy do not only originate in the commercial sector. The recent revelations concerning the scale of government suspicion less bulk data collection programs which should also be addressed.

- Poland plans to enact a law governing the use of CCTV monitoring systems in order to better protect the privacy, as well as modernize its privacy protection regulations before the new EU regulation is passed.

12. Protecting children and young people from abuse and exploitation

a. UKE

- On 2 July 2009, the President of UKE signed an Agreement on Safety of Children on the Internet. This agreement is a voluntary contribution of all signatories to ensuring children's safety on the Internet. Special emphasis was put on fighting illegal Internet content, such as illegal pornography and hate speech.

- On 23 December 2009, the Office of Electronic Communications concluded an Agreement on cooperation with F-Secure Sp. z o.o. under which an information and education website was established at **www.przyjaznynet.pl.** The website contains information on safety on the net, taking particular account of the children, as well as information on technological solutions, such as parental control, ensuring maximum protection of the user and of end user's terminal devices against cybercrime. In addition, www.przyjaznynet.pl promotes certification of telecommunications services in the "Safe Internet" category.

- Certification of telecommunications services is a programme managed by the Office of Electronic Communications from 2009 onwards. The ITU Council resolution 1305 of 2009 is implemented as part of the certification programme of telecommunications services for the "Safe Internet" category. The certification in this category aims at encouraging activities from telecommunications undertakings to ensure safety to network users, including primarily children and young people, and to improve the quality of services provided. The President of UKE in this way wants to stress the problem related to their safety on the net and to create the need for using tools available in the market that may ensure the highest possible protection against cybercrime.

- As part of implementation of the ITU Council resolution 1305 of 2009, the President of UKE joined on 23 September 2013 the Action Programme for protection of children against Internet pornography that is led by the Ministry of Administration and Digitization. The programme aims at increasing parental awareness of issues related to the Internet use and at improving their digital skills, which should result in more effective use of technical solutions that protect children against harmful content on the net.

- Moreover, there is a permanent section on safety on the net on the website of the Office of Electronic Communications – www.uke.gov.pl → Konsument → Bezpieczeństwo w sieci. This section contains up-to-date information on incidents related to Internet safety as well as advice to draw the attention of users, primarily children, their parents and guardians and Internet website creators, to the issues of children's safety on the net. Different contests promote also solutions which make the Internet use safe.
- In addition, in order to increase protection of telecommunications services (including the Internet) consumers' rights, the President of the Office of Electronic Communications operates a Consumer Information Centre (a hot line and a website at www.cik.uke.gov.pl) where subscribers may receive help and advice on safe use of the net or basic protection against specific risks.

b. NASK

- Resilient participant of European Commission's programmes Safer Internet and BIK Net
- Co-founder of the KURSOR educational project promoting use of new technologies at school, as well as student protection literacy on-line.
- Co-founder of other projects in that field: "*Adventures of File and Folder On-line*", "*Senior for senior*", "*Safe Internet Avenue*", "*Science Festival*", "*Science picnic*"
- Direct trainings targeting the young, teaching staff, parents and police officers
- The ABIT programme (*Safe Internet Academy*) – a series of free trainings (co-financed by European Union funds) for the 50+ and the visually impaired aiming at enhancing computer literacy.
- Co-organizer of Safer Internet Day
- Series of nation-wide conferences "Innovative Education" organized in all 16 voivodships;
- Expert seminars on cyberbullying, sexting, addictions
- Organizer of the international annual event "Safety of children and young people on-line"
- Carrying out of a joint research study on the use of video-chats by minors for explicit contents.