

Unclassified

DSTI/CP/ICCP/SPAM(2004)1/FINAL



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

11-May-2005

English - Or. English

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

Task Force on Spam

**OUTLINE FOR THE OECD ANTI-SPAM TOOLKIT
(WORK PLAN)**

**DSTI/CP/ICCP/SPAM(2004)1/FINAL
Unclassified**

English - Or. English

JT00184012

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

The anti-spam toolkit was discussed by the OECD's Spam Task Force in March 2005 which agreed to recommend its declassification. The report was declassified through written procedure by the CCP and ICCP committees in May 2005.

The report is published under the responsibility of the Secretary-General of the OECD.

Copyright OECD, 2005.

Applications for permission to reproduce or translate all or part of this material should be made to:

Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

TABLE OF CONTENTS

INTRODUCTION	4
IMMEDIATE PRIORITY ELEMENTS, OPTIONS AND OUTLINES	5
ELEMENT 1 – ANTI-SPAM REGULATION	7
Deliverables under this item.....	7
Proposed development process	7
ELEMENT 2 – INTERNATIONAL ENFORCEMENT AND CO-OPERATION	8
Deliverables under this item.....	8
Proposed development process	9
ELEMENT 3 – INDUSTRY-DRIVEN SOLUTIONS AGAINST SPAM.....	10
Deliverables under this item.....	10
Proposed development process	10
ELEMENT 4 –ANTI-SPAM TECHNOLOGIES.....	11
Deliverables under this item.....	11
Proposed development process	12
ELEMENT 5 – EDUCATION AND AWARENESS RAISING	12
Deliverables under this item.....	12
Proposed development process	13
ELEMENT 6 – CO-OPERATIVE PARTNERSHIPS AGAINST SPAM	13
Proposed development process	14
ELEMENT 7 – SPAM METRICS.....	14
ELEMENT 8 - OUTREACH.....	16
Proposed development process	16
ANNEX I	17

INTRODUCTION

In the past few years spam has grown from a nuisance to a serious problem by filling users' mailboxes, clogging networks, facilitating the spread of viruses and becoming the vehicle for new fraudulent schemes worldwide. Spam activities, once limited to e-mail, are now spreading to a range of new communication services, including mobile phone multi-media messaging services, instant messaging services, and voice over IP. They are seriously threatening the reliability of e-mail as a communication medium and undermining trust and confidence in the Internet, therefore slowing the growth of the digital economy.

The problem of spam was firstly discussed by OECD members during the meeting of the Committee for Information, Computer and Communications Policy (ICCP) in March 2003. The Committee noted the need to increase attention to the proliferation of spam, and expressed support for further OECD involvement on this topic. In this regard, in February 2004 the OECD held a workshop on Spam, hosted by the European Commission in Brussels. Following the workshop, and considering the interest of OECD countries in the subject, the ICCP Committee, during its 2004 meeting, endorsed the creation of a horizontal Task Force on Spam, to assist in the further conduct and co-ordination of the work on spam at the OECD.

There is widespread agreement that there is not a single solution to the problem of spam. For this reason the Task Force has approached this issue in a broad way, to benefit from the multi-disciplinary expertise of OECD and its members, and to ensure effective co-ordination and supplement efforts to combat spam at national and international levels.

The main objective of the Task Force is to prepare an anti-spam Toolkit to foster the development and growth of anti-spam strategies and solutions across all sectors — including the technical, regulatory and enforcement fields — and to facilitate international co-operation. The toolkit is meant to become a policy instrument and a source of information and best practices for OECD as well as non-OECD economies. This document provides an outline description of the Toolkit and of the different elements which will be part of it.

IMMEDIATE PRIORITY ELEMENTS, OPTIONS AND OUTLINES

One of the agreed Terms of Reference of the OECD Task Force on Spam is to develop an “Anti-spam Toolkit” which aims “...to facilitate the development and growth of anti-spam strategies, arrangements and solutions, and to facilitate international co-operation against spam” (the Terms of Reference are in Annex I).

This paper is intended as a scoping document against which active participants can provide suggestions to ensure that the final scope of the toolkit has broad agreement across the stakeholders before proceeding with full development of the respective elements. Inputs and comments from countries which are not taking part in the project, or non-OECD member economies are also welcome. The document also aims to provide a preliminary stage management for the elaboration of the toolkit, without prejudice to the actual form that all or part of this toolkit will ultimately take. In considering “spam” it is not intended to utilise any one definition of spam, as it differs between countries, but to respect the choices each has made or will make.

In line with the objectives of outreach and of promotion of anti-spam strategies, the Task Force will aim as much as possible to identify and/or develop in the deliverables mentioned under each element below any educational materials and best practices that could be promoted under the various elements of the toolkit.

The elaboration of this toolkit will rely very much on the substantive input of stakeholders in the various areas covered. Such input may include taking responsibility for elaborating particular elements by providing first drafts of discussion documents, hosting meetings/workshops on specific issues related to spam, and providing timely and substantive comments on documents in progress.

The toolkit is proposed to be:

- A strategic information source - sufficiently detailed and structured, and supported by adequate analysis, that it informs stakeholders, identifies options and opportunities and facilitates future developments and co-operation.
- A source of practical information and tools for decision-, policy-, law-makers and enforcement agencies in this area.
- A state-of-play review of some aspects related to spam.

As currently proposed the toolkit has eight interrelated elements. When complete it will not form a single entity delivered at the one time, but will rather be a series of deliverables, delivered as they are completed, and which may take significantly different forms for different elements. The stakeholders and contributors will play a critical role in determining the final shape of the deliverables.

As mentioned above, although the toolkit will be developed primarily from the efforts of OECD members its potential use and benefits are directed at a much broader audience, which include non-OECD

economies, providing useful material and resources for those which may not already have legislation, arrangements and agreements in place to deal with spam at either the national or international levels.

The deadlines for the elements of the toolkit vary significantly from element to element, and many will require further development and review as they are partially or substantially dependant on volunteered resources. A number of elements, even when complete, may be “living” deliverables, which can be updated over time as new elements are created and added.

ELEMENT 1 – ANTI-SPAM REGULATION

The aim of this element is to provide a resource to support the development and review of anti-spam regulation strategies and arrangements and try to ensure that best practice is emphasised rather than advocating a particular approach. It will therefore have the greatest relevance to those economies which are developing or reviewing their spam regulation arrangements. It will also be an important tool for those economies that have existing regulatory arrangements and are looking for options to improve cross-border regulatory frameworks. It will not compare legislative frameworks in their entirety, but rather single out elements of particular frameworks as representative of the various possibilities.

Deliverables under this item

The deliverable(s) will provide a brief overview of spam regulation to date, some broad considerations for effective regulation and the key issues and decision points that will be encountered in developing a spam regulatory framework. For each decision point it will:

- Identify the likely reactions to any given decision.
- Provide (where available) examples of how such a choice has been legislated for elsewhere.
- Identify likely spamming strategies which may be used to attempt to circumvent this regulatory approach.

Cases which have potential cross-jurisdictional precedent or interpretive value will also be identified and cited where available.

This approach will ensure the audience has the benefit of the wide spectrum of regulatory approaches and has a broad decision-base from which to determine whether, and what type, of spam regulation is appropriate to their own legal and regulatory environment.

Proposed development process

An initial draft structure will be developed in consultation with Task Force members. The deliverable(s) will be progressively and sequentially developed as comments are received and an up-to-date version regularly posted to the EDG as the document develops.

ELEMENT 2 – INTERNATIONAL ENFORCEMENT AND CO-OPERATION

One of the elements of the current OECD work programme involves developing information “... on the different elements needed to support effective international law enforcement co-operation on spam, taking into account that the kinds of bodies charged with enforcing anti-spam laws vary from country to country. This will build on the existing framework for law enforcement co-operation ...Further, experience of ongoing bilateral initiatives, such as memoranda of understanding (MoUs) between countries to combat spam, will be studied.”

There is at present a patchwork of frameworks with commonalities and differences, within which some significant anti-spam enforcement actions have been undertaken. This element aims to comprehensively document the opportunities and challenges which surround one of the most problematic aspects of spam enforcement – that of international/cross-border enforcement and co-ordinated action against spammers. It also aims at exploring options for alleviating constraints. In this respect, exploring the experiences of operating across this patchwork, including the MoUs that have been developed between some nations will add value to the work.

Deliverables under this item

This element will include:

- National contact information and a snapshot of the anti-spam legal framework – for OECD countries and possibly also for non-OECD economies – including:
 - Web links to the relevant authorities and to the specific anti-spam law if the country has one.
 - Contact information for the agencies responsible for cross border enforcement.
 - Contact information for the authorities responsible for the formulation of spam policy.
 - Available sanctions.
 - Whether any other general law applies to the activity of spamming.
 - Whether particular agencies may take action against a foreign-based spammer.
 - Whether particular agencies may take action against domestic spammers who send spam outside the domestic territory.
 - Whether an enforcement agency may share information with a foreign counterpart.
- A report outlining:
 - The diversity of frameworks and agencies.
 - The challenges for effective cross-border enforcement.
 - Key issues and priorities for collaboration/co-operation.

- Existing efforts to address the challenges of cross-border enforcement such as the ICPEN arrangements, the existing Memoranda of Understanding on spam, Privacy and data protection arrangements, and the EU Contact Network of Spam Authorities (*e.g.* existing formal and informal agreements or arrangements to facilitate enforcement, including those with the private sector, and where possible an evaluation of their potential), the London Action Plan “On International Spam Enforcement Cooperation”.
- Options to facilitate future cross-border enforcement against spammers, including possible fora, forms and possible elements for future agreements on spam.
- A table of cases or actions already undertaken by enforcement authorities.

Proposed development process

This is a significant deliverable which will require a staged delivery. The process should be iterative, with investigations and discussions from the early stages of the project influencing the form of the later stages.

1. Obtain general information regarding enforcement and co-ordination issues and arrangements via a Questionnaire (complete).
2. Participate in activities on the workshop on spam enforcement in London co-sponsored by the UK OFT, the US FTC and the OECD and obtain feedback on follow-up activities.
3. Undertake discussions with agencies actively involved in spam regulation and enforcement.
4. Based on the information derived from the preceding points progressively develop the map and report outlined above including best practices and possible recommendations for specific OECD action.

ELEMENT 3 – INDUSTRY-DRIVEN SOLUTIONS AGAINST SPAM

The aim of this element is to explore the developing area of industry-led measures and strategies against spam at both the national and international levels.

This includes identifying the initiatives and achievements to date that industry groups and associations across a number of sectors have made through self-regulatory approaches to reduce the creation, transmission, or receipt of spam. It will also identify any further opportunities which seem to have potential, but are untested.

The approach will engage a number of key stakeholder groups in the development of this information including the ISP sector, the network operators sector, the direct marketing sector, and other sectors including civil society.

Deliverables under this item

- Inventory of industry-led solutions and partnerships against spam.

Proposed development process

Industry participation, especially through BIAC, is vital to developing a comprehensive overview. Some of the steps in the development process could include:

1. Literature search and a review of recent papers and documents.
2. Preliminary discussions with key industry associations/groups to identify any existing and contemplated initiatives.
3. Development of draft element structure and information base for consideration by Task Force members.
4. Development of draft element for elaboration/response by industry groups.
5. Sharing of draft through broader stakeholder groups/general EDG.
6. Identification/Development of best practices.

ELEMENT 4 –ANTI-SPAM TECHNOLOGIES

The goals of this element are to provide an understanding of the evolving technical environment so that effective anti-spam policies can be developed and to examine how certain technical measures can be used as tools and resources for enforcers.

Anti-spam technologies will be identified and examined. Commentary will also include any possible legal and societal ramifications which may arise from the use of such measures. No particular technology or approach will be advocated, but cross-government, cross-boundary, cross-industry international discussion will be facilitated and resulting recommendations will be made where appropriate. Since any technical approach at the Internet level requires widespread adoption to work, we will point out the distinctions between proposed Internet standards and certain company's proposed solutions.

Some of the aspects proposed for documentation are:

- Technical authentication frameworks.
- Reputation systems.
- Anti-virus tools.
- Anti-spy ware tools.
- Challenge/response systems (for example a test which requires human confirmation before continuing).
- Filtering (heuristic and Bayesian).
- Rate limiting.
- Blacklists/white lists.
- Spam-reporting systems.
- Relevant academic research.

Such a documentation exercise would also include as much as possible a discussion of the benefits, weaknesses (possibilities for spammers to circumvent the above mentioned technical solutions) and issues for lawmakers, enforcers, ISPs, ESPs and consumers.

Some of the elements here will overlap with Element 3 (Industry Best Practices and Education and Awareness), especially in terms of industrial and individual-level Information Technology security best practices.

Deliverables under this item

Industry participation, including through the BIAC, is vital to developing a comprehensive overview while avoiding undue focus on any one field of endeavour or commercial perspective. The proposed deliverables may address and/or include:

- Technical authentication frameworks.
- General comprehensive overview of anti-spam technologies.
- Periodic workshops as necessary.
- Identification/Development of best practices.

Proposed development process

It is proposed that this element be very substantially developed by industry associations and groups to ensure relevancy and an appropriate level of support by key industry players and sectors. Initial work on the element will involve:

1. Literature search and a review of recent papers and documents produced by relevant groups.
2. Preliminary discussions with key industry associations/groups to identify significant emerging initiatives.
3. Development of draft element structure and information base for consideration by Task Force members.
4. Development of draft paper(s) for elaboration/response by industry groups.
5. Conducting periodic workshops and re-evaluation.
6. Socialisation of updated draft through broader stakeholder groups/general EDG.

ELEMENT 5 – EDUCATION AND AWARENESS RAISING

This element aims to create an on line repository for the range of resources and education and awareness publications that have been or are being developed across a range of languages, targeted at education and awareness raising about spam and related topics. This will include information targeted at consumers, ISPs, government agencies, and business, covering such issues as:

- General information resources about the nature and extent of the spam problem including in individual countries.
- How to make sure you do not unintentionally send what could be considered spam.
- How to minimise exposure to spam.
- What it is and how to avoid falling for a “phishing” attack.
- What it is and how to avoid falling prey to “spyware”.
- What it is and how to protect against “zombie” and botnet problems.
- How to report spam or take action against spammers.
- The economic and social dangers of spam and the penalties spammers can incur.

Deliverables under this item

This approach will provide a consolidated reference point to facilitate organisations that are considering developing material, or similar guides in new languages, minimising duplication of effort and promoting the development of best-practice advice to stakeholders. By identifying future work while still at the proposal stage, this resource will facilitate agencies with similar requirements being able to work together to develop collaborative output and thereby reduce the cost of deliverables. This resource will be particularly useful to developing economies which have very limited resources to devote to spam.

As well as providing spam-specific publications it could also include publications about spam-related topics, for example “phishing” and “spyware”, where spam is a commonly used medium. There are numerous stakeholders in the private and civil society sectors who can contribute significantly to this deliverable, both in terms of identifying/providing resources, and also in terms of their effective delivery.

Proposed development process

Through the EDG a call has been made for links to copies of:

- Available resources and contact points where hard copies can be obtained (if available), and
- A list of resources currently proposed or under consideration, and relevant contact officers.

A number of countries have already contributed significant detail about resources available in their country. This information can be consolidated and crafted into a publicly available Web site. A number of possibilities exist for the best ongoing hosting and stewardship of the site. The Web site would need to be maintained over time. This is not expected to involve a significant workload, but must nonetheless be acknowledged.

Given the societal impact of the spam problem, the OECD intends to keep an open channel for public input and exchange with other non-governmental stakeholder communities. These could include electronic freedom of expression, privacy, consumer and anti-spam volunteer communities. Other forms of co-operation with these communities could include participation in workshops and informal discussions.

ELEMENT 6 – CO-OPERATIVE PARTNERSHIPS AGAINST SPAM

The aim of this element is to identify the range of co-operative arrangements in government and industry to attack the problem of spam, and identify effective models and/or methodologies that have emerged or are emerging.

A number of models have arisen where government works with industry or civil society to deal with online threats and issues, ranging from providing financial, material or regulatory support for activities, or by working in partnership with industry. Some examples of this include:

- The collaborative development and functioning of the Computer Emergency Response Team (CERT) arrangements which exist in many countries.
- Government-industry partnerships for the development/support of relevant non-government bodies such as, among others:
 - Internet Watch Foundation and NetAlert, which deal with online child protection.
 - ICSTIS, (the Independent Committee for the Supervision of Standards of Telephone Information Services), the industry-funded regulatory body for all premium rate charged telecommunications services in the United Kingdom, which regulates the content and promotion of services through their Code of Practice.

Possible areas of activity in relation to spam could include the development of industry-based clearing-houses for spam intelligence and complaints and spam metrics studies or monitoring arrangements. In the United Kingdom the government has already commenced development of a clearinghouse concept in partnership with industry.

Proposed development process

The process should be iterative, developing from feedback from industry meetings and consultations, with outcomes from the early stages of the project influencing the form of the later stages.

- Joint industry/government meetings to identify ideas, opportunities and possible pilot projects.
- Identify issues which may need to be overcome.
- Options circulated to broad stakeholder group (and possible public consultation) to obtain feedback, offers for assistance and facilitate prioritisation of options. (N.B. Some options/pilots may proceed without awaiting this feedback process if they already have enough support from industry/government/civil society sectors).
- Based on the information derived from this process, develop a priority list of projects and commence implementation subject to available resources.
- Undertake pilot programme evaluation and feed results into future work programme and priorities.
- Identify/Develop best practices.

ELEMENT 7 – SPAM METRICS

Progress on the proposal for significant OECD work on spam metrics has so far been difficult to achieve because there is no unified definition of spam.

Furthermore, different types of Internet users, individuals or business, do not have the same exposure to spam risks. Large well-known organisations and public administrations are more likely to be exposed to the spam phenomenon. However, indicators derived from automatic filters at such organisations can only give a partial view. Furthermore, depending on whether the Internet users are at home or at work, they are not affected by spam in the same way.

Beyond the different assessments of the nature of spam and methods to measure its intensity, one sees that there are currently two different types of spam grouped together: spam in “pipes” and spam in “mailboxes”.

- The first type of spam corresponds to messages burdening the network, which are filtered more or less automatically at the level of firewalls and various information security systems. At this stage, the damage created by the spam affects the security, reliability and effectiveness

of the internet mail system. In this case, anti-spam measures are mainly a professional management issue of internet traffic.

- The second type of spam corresponds to messages arriving in users mailboxes which have passed through various firewalls and criterion used by ISPs. According to the type of message received (and unfortunately opened) there could be multiple damages. In this case, spam is an Information Society issue which can affect the development of electronic commerce and Internet usage.

The two types of spam do not affect the same economic actors, nor call for the same anti-spam measures, nor can their intensities be measured with one unique statistical indicator.

Deliverables under this item

The aim of this element is to contribute to the development of a scoreboard consisting of many complementary indicators. This scoreboard could help to follow the evolution of spam, permitting a more complete analysis of multiple aspects of spam issues. It should contribute to identify action points and to follow their effectiveness over time. In this context, existing indicators (% of e-mail filtered which is classified as "spam") could be used, grouping them into a "basket" to provide a trend view over time, across a range of vendors. This could be undertaken while possibly also encouraging or sponsoring some research into spam databases to undertake *ex post facto* analysis of their data to provide information of either ongoing or transient interest.

Proposed development process

As regards the proposed "basket", it would include the existing indicator of the % of e-mail filtered which is classified as spam. This figure will vary significantly between sources due to the differing spam classification characteristics used by different organisations and the nature of their filtering model. The data would have to be anonymised and the different "lines" in the collection would not be tagged with specific source organisation names. Those organisations contributing the data could be cited collectively as data sources. There would also need to be an accompanying statement outlining the general reasons for the differences in trends between data sources (generically, not individually) to ensure no erroneous conclusions were drawn from these differences. This approach would, with the agreement of the participating organisations, leverage the existing data and preserve resources for those areas of most interest to the Task Force member organisations. It would provide a moderating effect on the factors which may produce artifacts in the data from one source, but importantly would allow cross-comparisons of trends.

The scoreboard could be developed along the following lines:

1. Identify the available sources, such as data published by anti-spam software providers, ISPs, advertising industry and sponsored links as well as regular studies by public agencies, universities or associations.
2. Research the details behind each data source.
3. Benefit from the experiences of National Statistical Institutions and similar organisations.

Development of the scoreboard could be proposed to the Working Party on Indicators for the Information Society (WPIIS).

ELEMENT 8 - OUTREACH

Due to the cross-border nature of spam, it will be critical that the scope of the Toolkit is extended as outreach to non-OECD economies.

Proposed development process

It is proposed that outreach activities include:

- Providing the toolkit as input into the WSIS-II process.
- Extending educational and best practices materials to other languages and countries.
- Expanding the OECD contact list to include also non-OECD economies.
- Sharing all toolkit outcomes with non-member economies, for example :
 - Conducting/participating in workshop(s) with the ITU, APEC, ASEM and others.
 - Posting publicly Toolkit elements and materials to receive comments and input from other interested non-OECD countries.
 - Reporting on spam issues in developing economies.
 - Creating mutual links to information on the ITU and OECD Web sites.
 - Producing informational CD ROMs.

For non-member economies, it is anticipated that the ITU will be a key interface for outreach activities.

ANNEX I

Terms of Reference of the Task Force on Spam

The Task Force on Spam is a joint subsidiary body of the Committee for Information, Computer and Communications Policy (ICCP) and the Committee on Consumer Policy (CCP). Its Terms of Reference are:

- To study, document and promote the range of existing and emerging anti-spam strategies, across all sectors, encompassing regulatory strategies, technologies, enforcement arrangements and strategies, and education and awareness-raising activities and materials.
- To develop and promote an anti-spam “tool-kit” to facilitate the development and growth of anti-spam strategies, arrangements and solutions, and to facilitate international co-operation against spam.
- To build upon work already done by OECD, the private sector, civil society, and other international organisations.
- To devise a public awareness strategy for OECD and a strategy for OECD outreach to share experiences with non-member economies in order to support global efforts to combat spam.

The Terms of Reference of the Task Force on Spam shall expire on 8 July 2006. The final deliverable will be a report to the ICCP and CP committees summarising the recommended package of policies and measures to combat the global problem of spam.