Communications and Information Technology Commission

INTERNATIONAL COOPERATION AND EXCHANGE FOR SAUDI ARABIA

Final Version
23/02/2008

Submitted to:

Submitted By:

Acceptance of Deliverable

Name	
Title	
Role	
Signature	
Date	

Document Control Page

Document Amendment Record			
Change No.	Date	Prepared by	Brief Explanation

Table of Contents

1. PURPOSE OF THIS DOCUMENT

The purpose of this document is to propose a list of activities that Saudi Arabia can perform in order to effectively combat SPAM on the international level. These proposed activities are of three main types: being a signatory member of international agreements or bodies for sharing knowledge, developing bilateral agreements with different countries, and developing Anti-SPAM regional initiative to combat SPAM.

A list of international bodies that Saudi Arabia can collaborate with in combating SPAM is also mentioned. Moreover, a mechanism to foster collaboration with these parties is suggested.

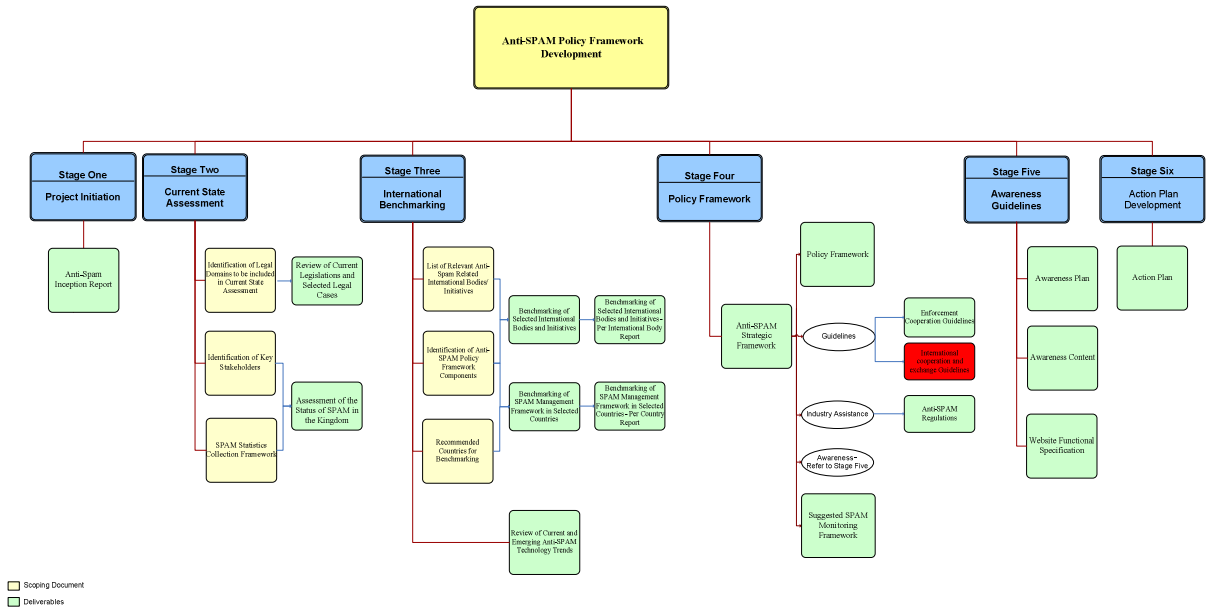
2. OUR APPROACH

The approach used to develop a list of recommended international bodies and agreements is based on the following:

- Identifying the international bodies that the Kingdom can be member of. This is based on the report ''Benchmarking of Selected International Bodies and Initiatives'' and the international trend and how most anti-SPAM regimes combat SPAM at the international level.
- Identifying the international enforcement agreements and international bodies where the Kingdom is already a signatory or member.
- Considering the specific characteristics and domestic legal, jurisdictional system and cultural values of the Kingdom of Saudi Arabia.

Based on the mentioned points, a list of international bodies and agreements were recommended for consideration taking into account the current Saudi international cooperation efforts in place, the Kingdom legal system, and the benefits where the participation will help the Kingdom in the fight against SPAM without impeding other existing agreements and laws.

The following diagram shows where this documents fits in the project:



3. EXECUTIVE SUMMARY

Global co-operation is fundamental to promote appropriate domestic frameworks to counter SPAM in all countries, and to encourage co-operation among governments, private sector, civil society and other stakeholders.

Countries involved in the battle against SPAM consider international cooperation as one of the pillars of a comprehensive anti-SPAM framework. It contributes significantly in the fields of laws and regulations, enforcement, education and awareness, and industry cooperation.

The international cooperation could be achieved through cooperating with regional and international entities, signing agreements, singing Memorandum of Understanding (MoUs), and belonging to international bodies fighting against SPAM.

In fact, and due to its importance in the battle against SPAM, Organization for Economic Co-operation and Development (OECD) recommends that national co-ordination should be first priority.

Most anti-SPAM regimes have already participated in international bodies and initiatives such as the Organization for Economic Co-operation and Development (OECD), the International Telecommunication Union (ITU), the "Operation Secure Your Server", etc. Moreover, those anti-SPAM regimes have signed different forms of agreements such as bilateral and multilateral MoUs, or signing already existing networks of cooperation such as the London Action Plan (LAP) or the Seoul-Melbourne Anti-SPAM Agreement.

Based on the above international trend, the OECD recommendations, and the Saudi domestic laws and concerns, it was recommended that the CITC considers joining a number of international bodies for the purpose of sharing knowledge and experiences such as OECD, Messaging Anti-Abuse Working Group (MAAWG), Operation Secure Your Server, and Operation SPAM Zombies.

In addition, it was considered critical for the Kingdom of Saudi Arabia to sign the London Action Plan (LAP) and to consider signing bilateral and multilateral agreements with key countries that do not participate in the fight against SPAM at the international level and where SPAM originates. At the regional level, it was deemed substantial for the Kingdom to lead a coalition against SPAM consisting of the Gulf Cooperation Council (GCC) countries. However, other international initiatives and bodies were discarded due to their irrelevance to the anti-SPAM initiatives for the Kingdom. Examples are the followings:

SPAMHAUS
SPAMHaus is an informative site that tracks the Internet's SPAMmers. This site can be beneficial for ISPs to get an updated list of SPAMmers..

Asia-Pacific Economic Cooperation (APEC)
APEC is a forum for 21 countries in the Asia Pacific region to discuss the regional economy, cooperation, trade and investment. The activities, including year-round meetings of the members' ministers, are coordinated by the APEC Secretariat. Clearly, this forum is designed for Asia Pacific countries.

Internet Engineering Task Force (IETF)
It is an open, standards organization, with no formal membership or membership requirements. This task force is concerned with the internet as a whole and thus does not offer practical or particular implementations for SPAM related concepts, rules or frameworks.

4. SUGGESTED INTERNATIONAL AGREEMENTS AND BODIES TO JOIN

International SPAM-related agreements were signed by a significant number of anti-SPAM regimes, mainly, to cooperate on the international level in terms of enforcement, addressing SPAM related problems, propagate technical solutions and raising awareness.

Moreover, several anti-SPAM resources are released by selected international bodies[1] and initiatives such as ITU, OECD, MAAWG, etc. These resources include web sites, conferences, volunteer activities, white papers, Request for Comments and others.

Out of those agreements and international bodies, the LAP, OECD, MAAWG, and other initiatives were recommended for CITC to consider.

4.1 JOINING THE LONDON ACTION PLAN (LAP)

On October 11, 2004, government and public agencies from 27 countries responsible for enforcing laws concerning SPAM met in London to discuss international SPAM enforcement cooperation. At this meeting, a broad range of SPAM enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international SPAM enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting.

London Action Plan is an international plan designed to encourage communication and cooperation between countries in tackling SPAM and SPAM-related problems. LAP provides a set of best efforts that should be performed by its members in order to ensure effective communication and coordination among its members in the fight against SPAM. This includes designating a point of contact for further enforcement communications, encouraging the communication and coordination among different anti-SPAM authorities, and encouraging cooperation with the private sector in order to actively involve them in the fight against SPAM. It is also recommended that members complete the "OECD questionnaire on cross-border enforcement of anti-SPAM laws". This questionnaire is available in Appendix B.

4.1.1 BENEFITS OF JOINING

Benefits of joining the London Action Plan is to achieve efficient and effective enforcement of anti-SPAM regulations by taking part in periodic conference calls, at least quarterly, with other appropriate participants to:

- Discuss cases.
- Discuss legislative and law enforcement developments.
- Exchange effective investigative techniques and enforcement strategies.
- Discuss obstacles to effective enforcement and ways to overcome these obstacles.
- Discuss undertaking, as appropriate, joint consumer and business education projects addressing problems related to SPAM such as online fraud and deception, phishing, and dissemination of viruses. Such projects could include educational efforts addressing conditions facilitating the anonymous delivery of SPAM, such as the use of open relays, open proxies and zombie drones.
- Participate as appropriate in joint training sessions with private sector representatives to identify new ways of cooperating and to discuss SPAM investigation techniques.

[1] In fact, all the recommended international bodies and agreements were contacted and it was confirmed that the Kingdom can join all of them.

4.1.2 HOW TO JOIN

To join the London Action Plan (LAP) contact[2]:
admin@londonactionplan.org

4.2 THE INTERNATIONAL TELECOMMUNICATION UNION (ITU)

The International Telecommunication Union (ITU) is an international organization established to standardize and regulate international radio and telecommunications. ITU promotes the exchange of information and best practices and provides support to developing countries.

ITU is headquartered in Geneva, Switzerland. It is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. It is comprised of 191 state members from across the globe, and it has 3 sectors, namely the Radio communication sector, Standardization sector, and the Development sector.

Saudi Arabia is already a member of ITU as it is represented through the MCIT and CITC. Accordingly, the Kingdom is urged to benefit from the SPAM-related initiatives and, services offered by this organization through their Strategy and Policy Unit (SPU) and other activities related to Cybersecurity. Among other services, ITU offers its members reliable information, whitepapers and data related to SPAM. This information is focused on:

- Regularity approach,
- Enforcement cooperation,
- Industry driven activities, technical solution,
- Education and awareness, and
- International cooperation.

4.3 WORKING GROUP ON INTERNET GOVERNANCE (WGIG)

CITC is already a member of this group, represented by the Deputy Governor of Technical Affairs, Communications and Information technology Commission of Saudi Arabia, Riyadh.

The main activity of the WGIG was "to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005." It is suggested that the CITC coordinates with the WGIG with regard to SPAM-related issues; in particular, issues related to the use of the Internet, including spam, network security and cybercrime.

4.4 THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

The Organization for Economic Co-operation and Development (OECD) is an international organization of developed countries that accept the principles of representative democracy and a free market economy. OECD has a global reach with active relationships with some 70 other countries and economies, Non Government Organizations (NGOs) and civil society.

4.4.1 BENEFITS OF JOINING

OECD provides a variety of measures and initiatives to address SPAM. OECD also publishes periodic documents and works closely with member countries to help governments, regulators

[2] For joining instructions, an email has been sent and we are still waiting for answer. Email was sent to the email address provided in their web site: http://www.londonactionplan.com/

and industry players orient their policies relating to SPAM solution and provide them with effective ways to combat SPAM.
Considering the fact that the vast majority of countries selected for benchmarking are members of the OECD, such as, USA, Australia, Canada, UK, Belgium, etc, the various benefits mentioned earlier of becoming a member of such an organization, it is recommended for the CITC to consider joining the OECD.
Joining the OECD will assist the Kingdom in the fight against SPAM in the following areas:

- Support to develop a regulatory framework,
- Recommending policies and procedures for members to combat SPAM,
- Providing various initiatives to combat SPAM for industry players, service providers, and regulator.

4.4.2 HOW TO JOIN

Becoming a member of the OECD is not an automatic process. The Member countries of the Organization, meeting in its governing body (the Council), decide whether a country should be invited to join the OECD and on what conditions. This decision is made based on examining the countries policies and regulations to ensure that it is ready to assure the responsibilities of OECD.

4.5 THE INTERNATIONAL COALITION AGAINST UNSOLICITED COMMERCIAL EMAIL (ICAUCE)

iCAUCE, also known as CAUCE International, is the parent organization for the various national and supranational CAUCE groups. It is one of the world's largest volunteer anti-SPAM organizations, with chapters in the USA, Canada, the EU and over a dozen economies in the Asia Pacific region.

4.5.1 BENEFITS OF JOINING

Benefits of joining iCAUCE include the meetings held twice a year to share best practices and updated news of each region, to reconfirm their opposition to the threat of resources that Unsolicited Commercial Email (UCE) represents, and to form active agenda against UCE that best fit each region. iCAUCE approaches the growing problem of SPAM in each respective region with a three pronged strategy combining technical, policy and legislative solutions.
iCAUCE actively advocates on behalf of consumers to governments, legislators, law enforcement agencies and industry associations about matters related to the blended threat of spam, viruses and spyware.
iCAUCE includes both unsolicited commercial email (UCE) and unsolicited bulk email (UBE).
iCAUCE provides a support mechanism for volunteers who wish to undertake these activities in countries that do not have an independent lobbying organization.
Setting a national CAUCE and being a member of the iCAUCE will bring the following for the Kingdom in the fight against SPAM:

- Communication with other iCAUCE members and discussing best practices and updated news regarding SPAM,
- Discussing the threat of SPAM in the region,
- Discussing an active agenda against the unsolicited commercial emails.

4.5.2 HOW TO JOIN

First, the Kingdom of Saudi Arabia needs to set up a national CAUCE organization, which will then be eligible for associate membership in iCAUCE. The initial step would be to set up a national committee and in order to do so, the Kingdom is asked to identify the initial members and leaders of Saudi Arabia's national committee and whether the Kingdom will host its own

web site (and the URL) or need a site hosted by iCAUCE. Once the Kingdom's committee is active, the next procedural step is to create a CAUCE organizational web site, membership mailing list (or other forum) and organizational charter, and the Board of iCAUCE will review to ensure that the organization is aligned with iCAUCE's goals and purposes.

4.6 MESSAGING ANTI-ABUSE WORKING GROUP (MAAWG)

Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. The MAAWG is a group of telecommunications companies brought together by OpenWave in early 2004.

4.6.1 BENEFITS OF JOINING

Benefits of joining MAAWG include bringing the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging SPAM, virus attacks, denial-of-service attacks, and other forms of abuse by systematically engaging all aspects of the problem. This includes technology, industry collaboration and public policy.
Joining the MAWWG will assist the Kingdom in the fight against SPAM at the industry level in the following areas:

- Collaboration among members: in terms of developing and sharing industry best practices,
- Technology with regard to defining network standards for combating messaging abuse, including reduction of spoofing and prevention of identity forgery,
- Public policy to build effective interfaces to key standards and legislative bodies

4.6.2 HOW TO JOIN

To join the Messaging Anti-Abuse Working Group, contact: info@maawg.org.

4.7 ANTI-PHISHING WORKING GROUP (APWG)

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their PCs.

Further, the organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks. APWG provides a Report-Phishing service by building a repository of phishing scam emails and websites to help people identify and avoid being scammed in the future. Moreover, they provide technical whitepapers and briefings from APWG Sponsors, such as: McAfee, Symantec and RSA Security.

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, security solutions providers and research institutions. Note that because phishing attacks and email fraud are sensitive subjects for many organizations that do business online, the APWG has a policy of maintaining the confidentiality of member organizations.

4.7.1 BENEFITS OF JOINING

Joining the APWG will help the kingdom to get up-to-date information in their battle against SPAM. Information covers technical measures, awareness materials, and cooperation with other countries.
Joining the APWG will offer the Kingdom:

- SPAM-related awareness materials,

- Up-to-date Anti-SPAM technical solutions,
- Easy cooperation with other members.

4.7.2 HOW TO JOIN

To join the APWG, contact: Mmembership@antiphishing.org
The following information should be provided in the email:

- Name
- Company
- Phone
- Email address
- Membership type

For more information of Membership levels and benefits please check the following link: http://www.antiphishing.org/membership.html

4.8 OPERATION: SECURE YOUR SERVER

Operation Secure Your Server aims to stop SPAMmers from using "Open proxies" and "Open Relays" which allow unauthorized people to route their SPAM through servers.

It is suggested that the either CITC joins or nominates a Saudi agency to join the "Operation: Secure Your Server". Many countries have already joined the Operation: Secure Your Server such as: the USA, Australia, Canada, Republic of Korea, UK, Singapore, etc. In addition, the Operation: Secure Your Server will provide information about open relays, open proxies, including step-by step instructions on closing them.

4.8.1 BENEFITS OF JOINING

By joining the "Operation: Secure Your Server", Saudi Arabia will be assisted on how to secure servers and prevent SPAMmers from originating SPAM from within the Kingdom.

4.8.2 HOW TO JOIN

To join, the Operation: Secure Your Server, contact: secureyourserver@ftc.gov

4.9 OPERATION: SPAM ZOMBIES

Operation SPAM Zombies tries to counter SPAMmers using home computers to send bulk emails by the millions, obscuring its true origin. The Federal trade commission (FTC) announces "Operation Spam Zombies" in partnership with 20 members of the London Action Plan and 16 additional government agencies from around the world. The Commission communicates with service providers to help them take the appropriate measures to stop SPAM.

4.9.1 BENEFITS OF JOINING

By joining, the "Operation: SPAM Zombies", ISPs in the Kingdom will receive letters from the Federal Trade Commission and its international partners, urging them to employ protective measures to prevent their customers' computers from being misused by SPAMmers.
It is suggested that either CITC joins or nominates a Saudi agency to join the "Operation: SPAM Zombies". Most of the countries have joined the SPAM Zombies such as the USA, Australia, Canada, Republic of Korea, UK, Singapore, Malaysia, etc.
Moreover, FTC will work with its international partners to identify likely SPAM zombies around the world as well as the ISPs that operate the networks that are hosting them. The FTC will then notify those providers of the problem and urge them to implement corrective measures. In

addition, the "Operation: SPAM Zombies", contains a heavy dose of consumer education, including awareness programs and providing or directing consumers to zombie removing tools. Joining the "Operation: SPAM Zombies" will encourage the ISPs operating on the Kingdom to take preventive measures to reduce SPAM[3].

4.9.2 HOW TO JOIN

To join the Operation: SPAM Zombies, contact: uce@ftc.gov

[3] In fact, FTC will be sending letters to those ISPs urging them to:

- Block port 25 except for the outbound SMTP requirements of authenticated users of mail servers designed for client traffic. Explore implementing Authenticated SMTP on port 587 for clients who must operate outgoing mail servers.
- Apply rate-limiting controls for email relays.
- Identify computers that are sending atypical amounts of email, and take steps to determine if the computer is acting as a spam zombie. When necessary, quarantine the affected computer until the source of the problem is removed.
- Give your customers plain-language advice on how to prevent their computers from being infected by worms, trojans, or other malware that turn PCs into spam zombies, and provide the appropriate tools and assistance.
- Provide, or point your customers to, easy-to-use tools to remove zombie code if their computers have been infected, and provide the appropriate assistance.

5. DEVELOPING BILATERAL/MULTILATERAL AGREEMENTS:

While being a member of international bodies and agreements would address the international cooperation agreement requirements with a number of the key countries from where SPAM originates, it is recommended that Saudi Arabia also signs bilateral or multilateral agreements on a need basis with countries that don't actively participate in the fight against SPAM on the international level such Russia, Germany, France, and Italy, which are also considered to be a key source of SPAM. While there may not be many more such countries immediately, it is recommended that constant monitoring of the list of worst countries in terms of SPAM, provided by Symantec, Message Lab, and SPAMHAUS[4] is performed on regular basis. This will enable adding additional countries with which Saudi Arabia needs to sign such bilateral agreements over time.

[4] For instance, according to SPAMHAUS report as at the 26th November 2007, the first 10 worst SPAM origin countries were: USA, China, Russia, UK, Germany, South Korea, Japan, Canada, France and Italy.

6. DEVELOPING GCC COALITIONS AGAINST SPAM

It is recommended that the Kingdom of Saudi Arabia, represented by CITC, establishes and lead a coalition against SPAM consisting of the Gulf Cooperation Council (GCC) countries in order to fight against unsolicited commercial emails. Key activities of this coalition might include:

- Sharing knowledge, information and intelligence about known sources of SPAM, network vulnerabilities, methods of SPAM propagation, and technical, education and policy solutions to the SPAM problem,
- Facilitate sharing of information on SPAMmers and other related information among the members,
- Discuss legislative and law enforcement developments,
- Ensure effective enforcement and ways to overcome any obstacles,
- Prosecution of SPAMmers sending mail into other members' countries,
- Hosting meetings and conferences regarding SPAM,
- Ensuring GCC countries international cooperation against SPAM,

Longer term, the membership of this body could go beyond the GCC countries and include other Arab states also, thereby becoming more effective in controlling SPAM originating from the Arab countries

7. SUMMARY OF SUGGESTED AND DISCARDED INITIATIVES

The table below shows the suggested international initiatives the Kingdom should consider and the discarded ones as well:

	International Body / Initiative	Recommended Action
International Bodies and Agreements	Organization for Economic Co-operation and Development (OECD)	Join
	London Action Plan (LAP)	Join
	Bilateral and multilateral agreements	Signing with other countries on a need basis
	International Telecommunication Union (ITU)	KSA is already a member. More coordination is recommended.
	Working Group on Internet Governance (WGIG)	KSA is already a member. More coordination is recommended.
	The International Coalition Against Unsolicited Commercial Email (iCAUCE)	Join
	Operation Secure Your Server	Join
	Operation SPAM Zombies	Join
	Messaging Anti-Abuse Working Group (MAAWG)	Join
	GCC Coalitions	Set up
	SPAMHAUS	Discarded[5]
	Asia-Pacific Economic Cooperation Telecommunications & Information Working Group (APECTEL WG)	Discarded[6]
	Internet Engineering Task Force (IETF)	Discarded[7]

The table below maps the memberships of the selected countries in the Benchmarking exercise verses the international bodies:

[5] It is a volunteer effort based on Website. Many internet service providers and other Internet sites use free services offered by SPAMHAUS to reduce the amount of SPAM. In fact there are free and paid services in this regard. For instance, 'MAPS Relay Spam Stopper' available at http://work-rss.mail-abuse.org/rss/index.htmloffers paid services while 'Arbitrary black hole list' available at http://abl.v6net.org/ offer black lists for free.
[6] For the time being, joining APEC is suspended.
[7] Although the IETF has anti-SPAM activities, it is recommended that the CITC makes use of IETF's publications, relevant RFCs, conferences, etc.

International Body	USA	Australia	Canada	Republic of Korea	United Kingdom	Belgium	Malaysia	Singapore
ITU	✓	✓	✓	✓	✓	✓	✓	✓
OECD	✓	✓	✓	✓	✓	✓	✓	
SPAM-HAUS[8]								
LAP	✓	✓	✓		✓	✓	✓	
WGIG[9]								
APEC	✓	✓	✓	✓			✓	✓
iCAUCE		✓	✓	✓	✓	✓		
APWG[10]								
MAAWG[11]								
GSMA								
IETF								
Seoul-Melbourne Agreement		✓		✓			✓	

[8] A website for organizations to participate in to get the a database of SPAMmers
[9] Membership is represented by individuals from interested countries.
[10] APEC is an Anti-Phishing Working Group where organizations can participate
[11] MAAWG is a group of telecommunications companies from different countries

8. APPENDIX A: OECD RECOMMENDATIONS- INTERNATIONAL COOPERATION

- **Improving the ability to cooperate.**

Member countries should improve the ability of their SPAM Enforcement Authorities to cooperate with foreign SPAM Enforcement Authorities. Member countries should in this respect:

(i) Provide their SPAM Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to violations of their Laws Connected with SPAM upon request, in appropriate cases and subject to appropriate safeguards.
(ii) Enable their SPAM Enforcement Authorities to provide investigative assistance to foreign authorities relating to violations of their Laws Connected with SPAM upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things.
(iii) Designate a contact point for co-operation under this Recommendation and provide the OECD Secretariat with updated information regarding their Laws Connected with SPAM and the SPAM Enforcement Authority designated as the contact point. The OECD Secretariat will keep record of this information and make it available to interested parties.

- **Improving procedures for co-operation.**

Before making requests for assistance as foreseen in the previous paragraphs, SPAM Enforcement Authorities should:

(i) Proceed to some preliminary investigative work to determine whether a request for assistance is warranted, and is consistent with the scope and priorities set forth by this recommendation.
(ii) Attempt to prioritize requests for assistance and, to the extent possible, make use of common resources such as the OECD Website on SPAM, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.

- **Cooperating with relevant private sector entities.**

(i) SPAM Enforcement Authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of Laws Connected with SPAM. In particular, SPAM Enforcement Authorities should cooperate with these groups on user education, promote their referral of relevant complaint data, and encourage them to share with SPAM Enforcement Authorities investigation tools and techniques, analysis, data and trend information.
(ii) Member countries should encourage co-operation between SPAM Enforcement Authorities and the private sector to facilitate the location and identification of SPAMmers.
(iii) Member countries should also encourage participation by private sector and non-member economies in international enforcement co-operation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

9. APPENDIX B: OECD QUESTIONNAIRE ON CROSS-BORDER ENFORCEMENT

COUNTRY:
Section I: Description of national enforcement framework
A. Authority

- Do you have a specific anti-spam law in your country? (If yes, please provide the URL.)
- If so, what enforcement agencies are responsible for its enforcement? (Please provide the URL.)
- If not, which enforcement agencies have initiated proceedings against spammers under other laws, or have the power to do so? (e.g. enforcement agencies responsible for consumer protection, data protection or telecommunication laws).
- Please indicate whether each enforcement agency listed in responses to Questions 2 and 3 possesses civil, criminal or administrative powers or some combination of these powers.
- How do enforcement agencies receive complaints from spam recipients? (e.g. e-mail? online form? telephone?) Are enforcement agencies required to investigate every complaint they receive, and prosecute every case brought to their attention?
- If more than one agency possesses enforcement powers, are there established protocols or arrangements for referring complaints between the agencies?
- What are the primary investigative powers possessed by each enforcement agency? (e.g. can it request that evidence be provided voluntarily? issue compulsory process itself? request a court to obtain a warrant or issue a subpoena?)
- How does each enforcement agency initiate proceedings against a spammer? (e.g. can it bring its own action directly in a civil or criminal court? initiate administrative proceedings? refer cases to a public prosecutor?)

B. Sanctions, remedies and outcomes

- What legal remedies or sanctions are available to each enforcement agency? (e.g. injunctions or other conduct prohibitions? civil penalties? criminal fines? imprisonment? disgorgement of ill-gotten gains? monetary redress to spam recipients?)
- How many spam-related proceedings have been initiated by each enforcement agency? (If possible, indicate the number of administrative, civil and penal cases.) Please provide any readily accessible information about the outcomes of the proceedings that have already been concluded.
- Have any of these proceedings been settled without a hearing? If so, please indicate how many.
- If the sanction or remedy that is obtained is not complied with by the spammer, what further steps are available to the enforcement agency?

C. Private sector assistance

- How does the private sector provide assistance to enforcement agencies responsible for anti-spam laws? (e.g. assist in gathering evidence, testifying in court, providing affidavits?)
- What legal or practical restrictions are there on the ability of ISPs and others in the private sector regarding the provision of evidence about spam to enforcement agencies? Are there

laws or policies in place to act as incentives for the private sector to share information (e.g. providing indemnity to ISPs?)

- Under what circumstances is information that the private sector shares with the enforcement agency treated as confidential? If there is any such confidential treatment, how is it affected by the kind of information or material that the private sector has shared?

Section II: Cross-border aspects of anti-spam law enforcement
D. Cross-border challenges

- Can each enforcement agency take action against foreign spammers targeting domestic e-mail users? If yes, under what circumstances?
- Can each enforcement agency take action against a domestic spammer that is targeting foreign e-mail users? If yes, under what circumstances?
- Can each enforcement agency notify authorities in other countries about spam-related investigations that affect those countries?
- Can each enforcement agency share information with, or otherwise provide investigation assistance to a foreign enforcement agency? If yes, under what circumstances? (e.g. does the e-mail have to be illegal in both countries as a condition to sharing information?)
- What do you consider, or have you experienced, as being an obstacle to effective cross-border enforcement of laws related to spam?

E. Existing arrangements for international co-operation

- Does your country or its enforcement agencies have any bilateral or multilateral arrangements with other countries or agencies to co-operate in enforcing laws used against spammers? If so, please provide copies of any relevant arrangements. (e.g. laws, rules or policies)
- Does your country have any arrangements in place that could facilitate the recognition and enforcement of judgments obtained in spam cases in foreign courts? If so, please provide copies of any relevant arrangements.

F. National contact point for anti-spam enforcement

- Is there an enforcement agency in your country that could be designated as a primary point of contact to facilitate anti-spam enforcement co-operation with foreign enforcement agencies? If so, please provide the agency's name and contact information.

G. Cross-border policy

- What kinds of spam complaints would take highest priority or be most appropriate for cross-border enforcement co-operation? (e.g. deceptive, fraudulent or virus carrying spam, or unsolicited commercial e-mail?
- Is there an agency primarily responsible for spam policy issues? Please provide the agency's name and contact information.