Communications and Information Technology Commission

ANTI-SPAM ENFORCEMENT GUIDELINES FOR SAUDI ARABIA

Final Version

23/02/2008

Submitted to:

Submitted By:

Acceptance of Deliverable

Name	
Title	
Role	
Project Name	
Document Title	
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 develop the necessary guidelines for the enforcement of the anti-SPAM policy framework in the Kingdom of Saudi Arabia. This will identify the agencies in charge of enforcing the anti-SPAM related regulations, the reporting mechanism, how the enforcement agencies will deal with these complaints at the national and international level, and the coordination means between these enforcement agencies.

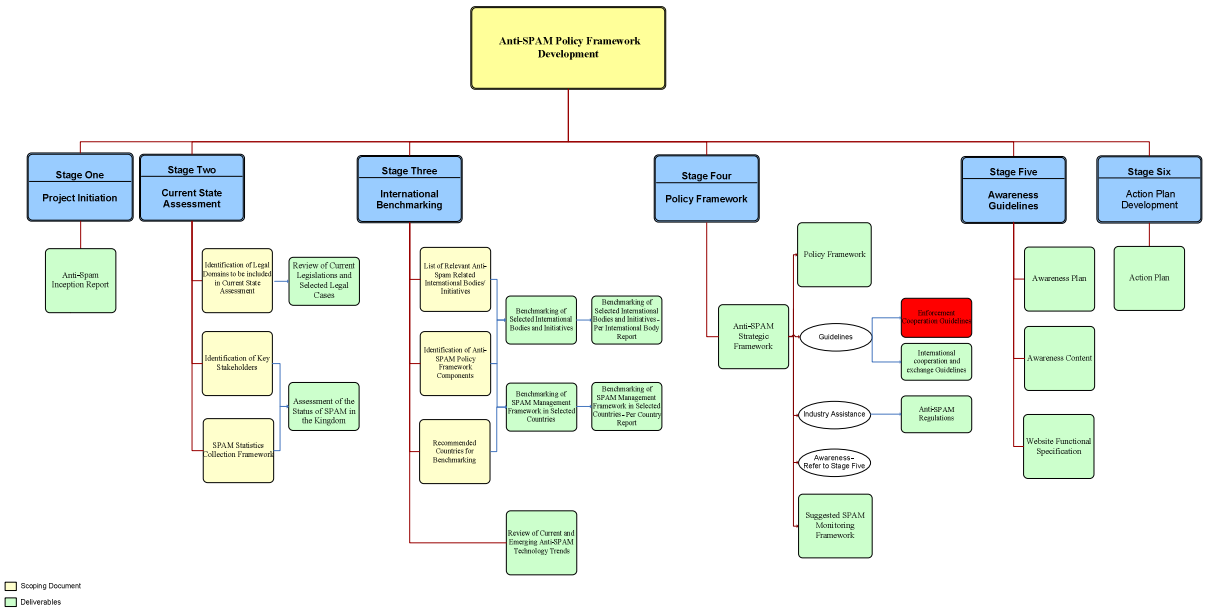
2. OUR APPROACH

The approach used to develop this document considers three main areas to develop the enforcement cooperation guidelines:

1. Identifying the agencies involved in the enforcement of the anti-SPAM policy framework;
2. Recommending a reporting and complaint handling mechanism; and
3. Defining the mechanisms of coordination between the involved enforcement agencies.

To address these points, we considered other countries' experiences, the international bodies' recommendations, and the existing relevant laws and enforcement procedures adapted currently in the Kingdom.

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



3. EXECUTIVE SUMMARY

While having the appropriate anti-SPAM rules and guidelines is necessary, the implementation and application of these rules is crucial and constitutes the second step towards a comprehensive anti-SPAM strategy. The timeliness and speed with which enforcement happens and sanctions are applied is critical, if SPAM is to be effectively curbed.

It was noticed that most anti-SPAM regimes have designated at least one enforcement agency to deal with SPAM related issues. Typically these agencies are: telecom regulators, consumer protection agencies, data protection authorities, and criminal prosecutors such as the police. Moreover, the international bodies, like Organization for Economic Co-operation and Development (OECD), recommend having a nodal agency and proper coordination between the various enforcement agencies at the national and international levels. In fact, OECD urges anti-SPAM regimes to ensure that SPAM enforcement authorities have the necessary authority to obtain evidence sufficient to investigate and take action against SPAMmers.

Based on the countries' experiences, international bodies' recommendations, and Saudi domestic laws, it was decided that the Telecommunication Act and the Anti e-Crime Act are the applicable SPAM-related laws in the Kingdom; accordingly, two enforcement agencies were designated in the Kingdom to enforce anti-SPAM policy framework. While the Ministry of interior (MOI) deals with SPAM associated with Anti e-crime Act violations, i.e. criminal and objectionable content, the telecom regulator, the Communication and Information Technology Commission (CITC) will be in charge of SPAM messages with unobjectionable content.

Although MOI and CITC will have joint responsibilities at the national level, for instance, ensuring the adherence by all parties to the Anti-SPAM policy framework, only CITC will be participating in recognised international bodies and sign agreements to cooperate on enforcement of laws relating to SPAM. Moreover, CITC will provide an international contact point to the outside world, to facilitate the international cooperation process.

On the national level, and to guarantee proper and sufficient coordination between the enforcement agencies, it was suggested to set up a Cross- Agency Program Steering Committee to monitor and track the progress of the SPAM-related initiatives.

Receiving and handling complaints is of great importance. It is recommended that four different channels to be available for SPAM victims to report SPAM. These are: email, fax, in person, and an online form. The SPAM messages' content will determine the enforcement agency to which the complaint should be routed.

4. AGENCIES INVOLVED IN THE ENFORCEMENT PROCESS

4.1 ENFORCEMENT AGENCIES AND NODAL AGENCY IN SAUDI ARABIA

Based on other countries' experiences, the international bodies' recommendations[1], and the existing SPAM-related laws in the Kingdom and the entities in charge of enforcing these laws, there will be two agencies involved in the enforcement of the anti-SPAM related laws in the Kingdom:

- Communication of Information Technology Commission (CITC); and
- Ministry of Interior (MOI).

4.1.1 CITC

CITC is the commission regulating the telecommunications sector in the Kingdom. CITC is also charged with the responsibility of protecting the interests of users with respect to public telecommunications services and the Internet and propose regulations related to the telecommunications sectors. Further, CITC administratively manages the telecommunication spectrum in the whole Kingdom. All internet content viewed from the country is filtered for content that contradicts the national values or laws of the Kingdom of Saudi Arabia. Access to pornography, gambling, and drugs related sites is strictly prohibited and always filtered out by CITC.

According to the Telecom Act, any operator, individual or a juridical person misusing telecommunications services, such as causing damage to the public telecommunications networks or intentionally placing a message of an indecent or menacing nature or which causes panic or disturbance, will constitute a violation of the law.

The Telecom Act which is enforced under CITC stipulates that any usage of telecom media by a Telecom licensee to threaten or cause annoyance to the users is a breach of the Telecom Act and can cause the licensee to bear legal consequences. Clause 11 from Article 37 in the Telecom Act, also states that "Misuse of telecommunications services, such as causing damage to the public telecommunications networks or intentionally placing a message of an indecent or menacing nature or which causes panic or disturbance" by any operator, individual, or a juridical person constitutes a violation.

Based on the responsibilities assigned to CITC regarding the Telecommunication Act and licenses granted to service providers, and the possible violation of the Telecommunication Act provisions and the licenses in the context of SPAM, CITC will be the designated agency in charge of enforcing the anti-SPAM related laws falling under its jurisdiction.

4.1.2 MOI

The Ministry Of Interior (MOI) is the owner of the Anti e-Crime Act which aims at creating legal and regulatory standards to combat information, computer and internet crimes through specifying and determining the relevant crimes and punitive actions for each crime or violation in order to achieve the following:

1. Maintain information security;
2. Safeguard the rights associated with legitimate use of computers and networks;

[1] For detailed review of other countries' experiences and international bodies recommendations, please refer to Appendix A.

3. Safeguard public interests, morals, and communal values; and
4. Develop and safeguard the National Economy.

While the Anti e-Crime Act does not specifically or fully address SPAM, it does address certain aspects of SPAM, including aspects relating to using SPAM for Phishing purposes, spreading viruses, or publishing content that could be considered detrimental to the Kingdom's economy or security, offensive to its religious values and morals, or contrary to the privacy of resident individuals. Additionally, the MOI has recently begun planning for the establishment of a new division in charge of investigating e-crimes.

Accordingly, any SPAM messages violating the Anti e-Crime Act stipulations in terms of the content of the message, MOI will be directly involved in the enforcement process. Moreover, MOI will be in charge of receiving SPAM complaints, investigating, chasing and suing SPAMmers where appropriate.

4.1.3 THE NODAL AGENCY

Considering the distributed jurisdictions in the Kingdom and the different laws dealing with SPAM, there will be two designated nodal agencies in the Kingdom.

In the case of SPAM messages which violate the Anti e-Crime Act, i.e. a SPAM message of objectionable and illegal content, the MOI will be responsible of receiving, handling and processing the complaint.

On the other hand, messages of non-objectionable content will invoke CITC to intervene (i.e. annoying but non-criminal messages).

Further, CITC, as the telecom regulator, will have the ultimate responsibility of coordinating at the international level and will be participating with international bodies and signing agreements with other international agencies where appropriate.

The designated enforcement agencies in the Kingdom will have the following responsibilities:

- CITC and MOI will be enforcing the Anti-SPAM related laws where applicable;
- CITC and MOI will ensure effective communication, cooperation, and coordination between other enforcement national agencies;
- CITC will monitor the state of SPAM in the Kingdom, and ensure that the Anti-SPAM policy rules are being adhered to strictly by all parties;
- CITC will provide a means of measuring the effectiveness of the Anti-SPAM policy framework;
- CITC will participate in recognised international bodies and sign agreements, where applicable, to cooperate on enforcement of laws relating to SPAM;
- CITC will provide an international contact point to the outside world, to facilitate the international cooperation process.

5. COMPLAINT: NOTIFYING AND HANDLING PROCESS

5.1 SPAM REPORTING METHODS

Referring to other countries experiences, it was noticed that having many tools to report SPAM will grant the SPAM victims greater opportunity to notify the enforcement agency once they are SPAMmed. In fact, none of the countries provide one method to report SPAM as depicted in the table below.

	USA	Australia	Canada	Republic of Korea	UK	Belgium	Malaysia	Singapore
Email	✓	-	✓	✓	✓	✓	✓	✓
Online Form	✓	✓	-	✓	✓	✓	✓	-
Telephone	✓	✓	✓	-	✓	✓		✓
Teletypewriter	✓	-	-	-	-	-	-	-
Mail	-	✓	✓	-	-	-	✓	-
Fax	-	✓	✓	-	-	✓	✓	-
In Person	-	-	✓	-	-	-	✓	-
Software Tool	-	✓	-	✓	-	-	-	-

According to the OECD, agencies with a responsibility of enforcing SPAM-related laws should provide more than one means of notification for SPAM recipients, e.g. via e-mail, filling out a form on the agency Web site, telephone, fax or post. Most have also provided an online complaint form which has been proved to be an efficient mean to collect complaints and evidence.

Further, the ITU also has recommended establishing adequate complaint mechanisms that include dedicated e-mailboxes for the handling of user complaints.

Based on other countries' experiences, standard bodies' recommendations, the importance of reporting SPAM, and finally Saudi domestic environment, it is advised that the enforcement agencies in the Kingdom, i.e. the CITC and MOI, should provide for user complaints through four different channels:

1. An online form;
2. Fax;
3. In person; and
4. By email.

If any of the two enforcement agencies receives a SPAM complaint which falls under the other agency's jurisdiction, the complaint shall be forwarded accordingly.

5.1.1 ONLINE FORM

The online form should be the primary channel used to report SPAM since it is most widely used and recommended by the OECD. Nevertheless, it should be supported by giving users the ability to send their complaints through alternate channels including e-mail or fax, or by filing them directly through the agency offices.

The comprehensiveness of information that victims provide is up to them. However, if the victims do not provide their names or other mandatory information, it may be impossible for the enforcement agency to refer, respond to, or investigate their complaint or request.

Recommended Fields in the online form:

- Victim's identification:
  1. Name;
  2. Age;
  3. Address; and
  4. Contact information.
- Complaint's attributes:
  1. Subject of Complaint;
  2. Name and Contact Information of the Company- the Sender/victim Complaining about if known;
  3. Name of Product that sender/victim are Complaining About;
  4. The mean used by the company to Contact the sender/victim;
  5. Copy of the offending SPAM message; and
  6. Date and time of message and technology utilized to transmit it.

5.1.2 FAX

A number of countries are using Fax as a media for processing complaints. Once the receiver receives a SPAM message, he can forward the SPAM message directly to a Fax number designated and published by the enforcement agency.

The criteria for accepting a 'Fax' complaint is as follows:

- Copy of the SPAM message.
- Victim's identification attached to the copy of the SPAM message:
  1. Name;
  2. Age;
  3. Address;
  4. Contact information; and
  5. Subject of Complaints.

5.1.3 IN PERSON

The 'In Person' channel for reporting SPAM was used in few countries. While the online form is an easy and quick tool to report SPAM, offering SPAM victims the chance to report SPAM via police offices is of great importance especially when people get Mobile SPAM while they have no access to the Internet. The criteria for accepting an 'In Person' complaint is as follows:

- Copy of the SPAM message.
- Filling all mandatory information in hand written complaint form that includes:
  - Victim's identification:
    1. Valid Personnel Identification Card.

2. Name;
3. Age;
4. Address; and
5. Contact information.

- Complaint's attributes:
  1. Subject of Complaint;
  2. Name and Contact information of the Company- the Sender/victim complaining about if known;
  3. Name of Product that sender/victim is Complaining About;
  4. The mean used by the company to Contact the sender/victim;
  5. Copy of the offending SPAM message; and
  6. Date and time of message and technology utilized to transmit it.

5.1.4 EMAIL

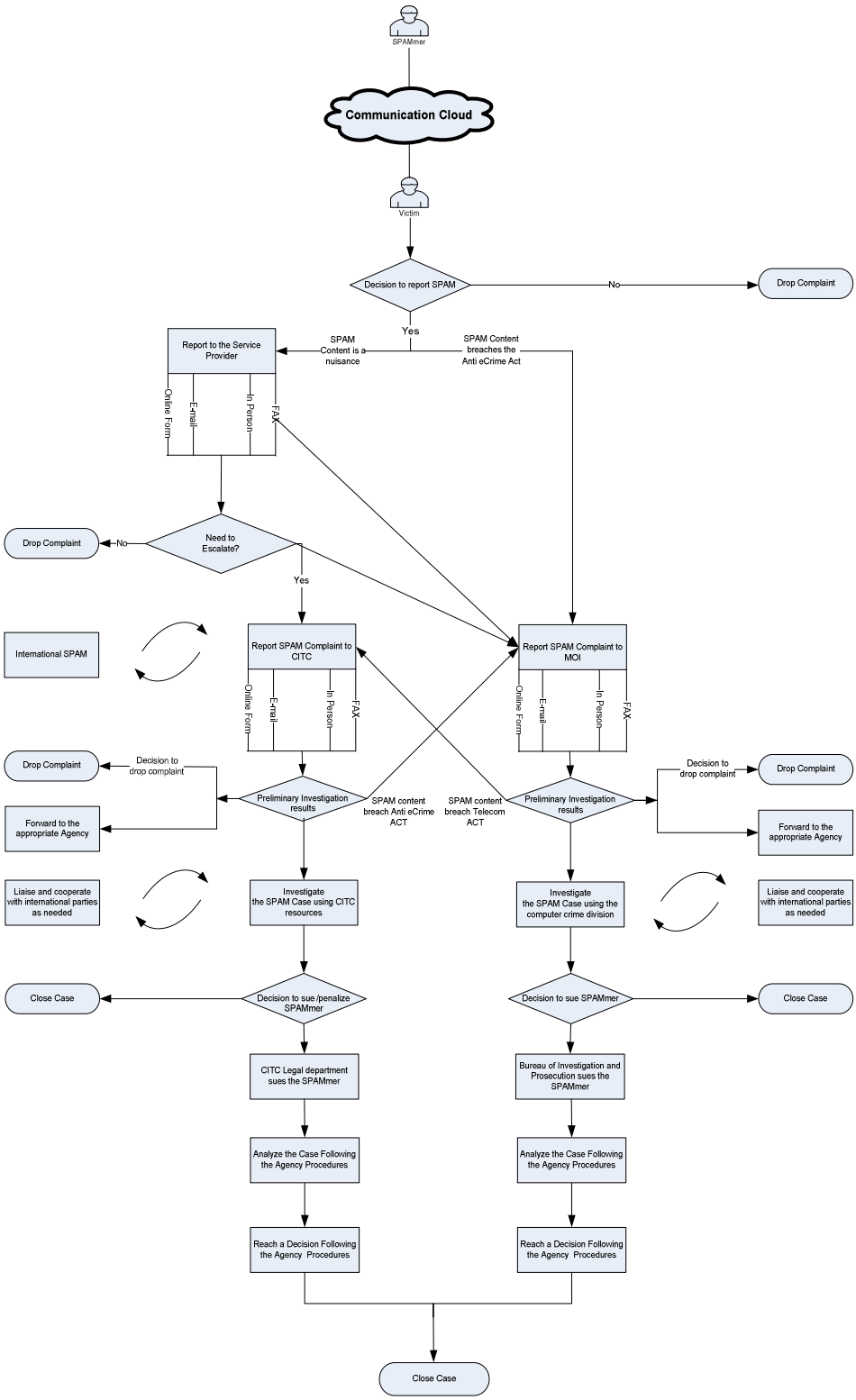
Once the receiver gets a SPAM message, he can forward the SPAM message directly to an email address designated and published by the enforcement agencies and ISPs.

Fields required in the forwarded email are:

- Name of the sender/victim;
- Age;
- Valid return address;
- Accurate contact information;
- Subject of Complaints;
- In order to enable the enforcement agency to deal with complaints about SPAMming legitimately, the header of the suspect electronic message must be annexed to the message, as the information contained in these headers is essential for identifying and locating the SPAM sender.

5.2 COMPLAINT HANDLING PROCESS

How do enforcement agencies deal with SPAM complaint once they get notified? While the CITC and MOI do have their complaint handling process in place, the flowchart below clarifies the steps that should be taken by ISPs and the enforcement agencies starting with receiving a SPAM complaint, forwarding it and ending up prosecuting the SPAMmer.


SPAMmer
Communication Cloud
Victim
Decision to report SPAM
No
Drop Complaint
Yes
Report to the Service Provider
SPAM Content is a nuisance
SPAM Content breaches the Anti eCrime Act
Online Form
E-mail
In Person
FAX
Drop Complaint
No
Need to Escalate?
Yes
International SPAM
Report SPAM Complaint to CITC
Report SPAM Complaint to MOI
Online Form
E-mail
In Person
FAX
Drop Complaint
Decision to drop complaint
Forward to the appropriate Agency
Preliminary Investigation results
SPAM content breach Anti eCrime ACT
SPAM content breach Telecom ACT
Preliminary Investigation results
Decision to drop complaint
Drop Complaint
Forward to the appropriate Agency
Liaise and cooperate with international parties as needed
Investigate the SPAM Case using CITC resources
Investigate the SPAM Case using the computer crime division
Liaise and cooperate with international parties as needed
Close Case
Decision to sue /penalize SPAMmer
Decision to sue SPAMmer
Close Case
CITC Legal department sues the SPAMmer
Bureau of Investigation and Prosecution sues the SPAMmer
Analyze the Case Following the Agency Procedures
Analyze the Case Following the Agency Procedures
Reach a Decision Following the Agency Procedures
Reach a Decision Following the Agency Procedures
Close Case

Individuals who receive SPAM can contact the Service Provider / MOI to report the SPAM case based on the following categories of SPAM content:

1. Directly to CITC if the complaint is coming from outside the Kingdom.
2. To the Service Providers: SPAM content of nuisance nature, such as messages that include an unobjectionable content and the messages that cause damage to the public telecommunications networks or the messages which are indecent or menacing in nature or which cause panic or disturbance. These types of messages are prohibited in section 37 of the Telecom act.
3. To the MOI: SPAM content that breaches the Anti e-Crime Act, such as messages that contains criminal and objectionable content.

There are four ways to report SPAM to Service Provider / MOI. These are e-mail, or fax, or online form, or in person. Victims can use these means to lodge complaints regarding violations of the Anti-SPAM Regulatory Policy Framework of the Kingdom of Saudi Arabia.

Upon the recipient of SPAM complaint by Service Provider, it will be reviewed to determine whether the allegations could constitute a contravention to the Anti-SPAM Regulatory Policy Framework, and verify that the complaint meets the requirements and contains all the information needed to proceed to CITC / MOI by contacting them using E-mail, or fax, or online form, or in person. If not, the case will be dropped.

When the CITC / MOI staff receive the complaint, they review the matter to determine:

1. Whether to drop the allegations upon the decision of CITC / MOI;
2. Whether to forward the allegations to the appropriate agency;
3. Whether to redirect the allegations (CITC to MOI)/ (MOI to CITC) based on the SPAM content. This decision is taken based on whether the SPAM content breaches the Anti e-Crime ACT or Telecom ACT; and
4. Whether to investigate the case using CITC resources / MOI computer crime division.

Once the decision is made by CITC / MOI to investigate the SPAM case by using their internal procedures and cooperating with international bodies as needed, the process goes through the following steps:

1. Take the appropriate decision to sue, penalize, or drop the case based on the investigation results and case priority.
2. Close the case.

Complaint Priorities

Receiving a SPAM complaint does not lead the enforcement agency to automatically start the investigation process. Admittedly, some SPAM complaints might refer to 1 or 2 SPAM messages sent by mistake while other complaints might be associated with criminal and offensive content. Consequently, priorities will be set taking into consideration the flowing factors:

- Message contains false or deceptive claims (e.g. Phishing, scams, claims about health performance);
- Message contains a virus;
- Message contains offensive or criminal content (e.g. child pornography);
- Unsolicited Commercial E-mail;
- Degree of damage suffered (no specific example of damage provided);
- Volume of messages sent;
- Repeat offender;
- Mobile phone SPAM; and
- Message originates from outside KSA.

When MOI / CITC receive complaints, they should start analyzing and investigating the case by:

- Writing to the organization, outlining the substance of the complaint;
- Gathering facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentations.

The investigation division should be granted the authority to collect evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

A decision would be taken based on the evidence and investigation conducted.

Powers for Investigation

It is proposed that the MOI / CITC should be responsible for enforcing the Saudi Anti-SPAM policy framework. The MOI / CITC should have specific powers witch enable them to undertake investigations in an efficient manner. Moreover, MOI / CITC will forward SPAM cases which do not fall under their jurisdiction to the appropriate authority, for instance, SPAM messages violating the Anti-Commercial Fraud Law will be forwarded to the Ministry of Commerce (MOC). Therefore, it is proposed that the Anti-SPAM policy framework confers the following powers on the MOI / CITC:

- The power to obtain from any person information or documents relevant to the MOI's / CITC's investigation of a contravention or suspected contravention of the Anti-SPAM policy framework.
- The power to enter premises and to seize, remove or detain any computers, telecommunications device, documents or any other things upon obtaining a warrant from a magistrate.
- The obligation of the MOI / CITC not to disclose any information or document provided to them for investigation unless it is in the public interest to do so or the person providing any information or document has been given the opportunity to make representation on the proposed disclosure of the information or document.

6. COORDINATION BETWEEN THE ENFORCEMENT AGENCIES

6.1 NATIONAL COOPERATION- SUGGESTIONS

National cooperation is a must and the nodal agency must ensure that it has good ties with all companies, telecomm service providers, internet service providers, and other relevant entities that deal with SPAM in order to combat SPAM effectively within the country.

National cooperation must be formed in order to guarantee the reduction of SPAM and to have successful enforcement regime in place.

Based on other countries' experiences, and in order to ensure the progression of these initiatives in a smooth manner, it is suggested that a Cross- Agency Program Steering Committee will be formed between the MOI and the CITC to monitor and track the progress of these initiatives over the 18 month timeframe.

7. APPENDIX A: COUNTRIES' EXPERIENCES AND INTERNATIONAL BODIES GUIDELINES

7.1 COUNTRIES EXPERIENCES: ENFORCEMENT AGENCIES

According to the majority of the countries having anti-SPAM frameworks in place, either having a SPAM-specific law or multiple related laws, it is noticed that multiple agencies are in charge of enforcing the anti-SPAM related laws. The principal reason behind the plurality of enforcement agencies with responsibility for SPAM, however, is that the variety of abuse committed through electronic communications may violate protections provided for under various laws, each attributing responsibility to a different agency as follows:

- **Consumer protection law**: by deceptively inducing recipients into paying for worthless wares or tricking recipients into various kinds of scams and frauds.
- **Criminal law**: in case e-mails are used to send viruses or high volumes of electronic messages to the same e-mail account disabling or disrupting the recipient's ability to use it, or again in the case of fraudulent behaviour, when it is also a violation of criminal laws (such as the case of phishing).
- **Data protection law**: in case SPAMmers are sending unsolicited commercial e-mail for the purpose of marketing without the recipient's prior consent, i.e. using personal information (the e-mail addresses) without the permission of the owner.
- **Telecommunication law and data protection law:** when e-mails contain false return addresses and misleading subject lines or fail to offer an opt-out service or to respect opt-out requests.

The following table illustrates the designated nodal agencies in each of the selected countries as follows:

	USA	Australia	Republic of Korea	UK	Belgium	Malaysia	Peru	Singapore	Canada
Nodal Agency	X	X	X	X	X	X	X	X	-
Ministry/ Agency	Agency	Agency	Agency	Agency	Agency	Agency	Agency	Ministry	-
Type of Enforcement Agency	Consumer protection	Telecom	Data protection	Data protection	Consumer protection	Telecom	Consumer protection	Telecom	-

The following table summarizes the agencies involved in the enforcement process of the SPAM related law(s) in the selected countries:

	USA	Australia	Canada	Republic of Korea	UK	Belgium	Malaysia	Peru	Singapore
Consumer Protection Agency	X	X	X	X	X	X	-	X	-
Criminal Prosecutes	X	X	-	X	-	X	-	-	-
Data Protection Agency	-	-	X	X	X	X	-	-	-
Telecom Regulator	X	X	-	-	-	-	X	-	X

In addition to having multiple agencies enforcing the anti-SPAM applicable laws simultaneously, there is always one enforcement agency designated as the nodal one, regardless of having one specific SPAM law or multiple laws. The nodal agency plays an important role at both national and international levels, functioning as a point of contact, signing international agreements and participating in forums at the international level. Typically, the nodal agency has roles and responsibilities defined as follows:

- Monitor the state of SPAM at the national level, and ensure that the legislation is being adhered to strictly by all parties;
- Provide an international contact point to the outside world, to facilitate the international cooperation process;
- Provide for means of measuring the effectiveness of the anti-SPAM framework;
- Ensure effective communication, cooperation, and coordination between the involved agencies; and
- Sign agreements to cooperate on enforcement of laws relating to SPAM.

7.2 COUNTRIES EXPERIENCES: COORDINATION MECHANISMS

7.2.1 USA

The USA formed a domestic SPAM task force with representatives from the Department of Justice (DOJ), the Federal Trade Commission (FTC), and the state. They also conduct monthly conference calls to share the knowledge and information on SPAM trends, technologies, investigative techniques, targets and cases.

7.2.2 AUSTRALIA

Australia has addressed the challenges that might otherwise result from the lack of a single enforcement agency by seconding personnel from the Australian Communications and Media Authority (ACMA) to work in the Australian High Tech Crime Centre (AHTCC), which ensures effective communication between the two agencies. It also has agreements with three agencies to co-operate on enforcement of the Australian SPAM Act, and regularly refers SPAM e-mails with offensive/illegal content to the appropriate authority.

7.2.3 CANADA

Canada sets-up SPAM task force composed of experts, ISPs, consumer advocates, and marketing representatives established. The main purpose of the task force is to enhance consumer education, awareness, and promotion of an international framework.

7.2.4 KOREA

The nodal enforcement agency in Korea cooperates with criminal prosecutors if SPAMmers do not comply with administrative requests to cease their activity. Recently, Korea Information Security Agency (KISA) started blocking of SPAM mails sent by mobile IP through collaboration with 16 major domestic portals.

7.2.5 UNITED KINGDOM

The Office of Fair Trading (OFT) leads the national coordination strategy of national regulators with an interest in SPAM, it chaired two meetings where representatives from bodies such as the Information Commissioner's Office, Advertising Standards Authority, Department for Trade and Industry (DTI), Office of Telecommunications, Independent Committee for the Supervision of Telephone Information Services (ICSTIS), Local Authorities, Home Office and criminal authorities agreed to a matrix mapping out respective responsibilities as well as a workable referral system.

7.2.6 BELGIUM

In Belgium, cooperation among different authorities is informal. However, the Direction Générale du Contrôle et de la Médiation carries out the necessary investigations and coordinates for information sharing and participates in the process as a witness.

7.2.7 SINGAPORE

The Infocomm Development Authority (IDA) works closely with the three major Internet Service Providers, CASE, Direct Marketing Association of Singapore (DMAS), Singapore Business Federation (SBF) and Singapore infocomm Technology Federation (SiTF) to introduce a multi-pronged approach to tackle e-mail SPAM.

7.3 COUNTRIES EXPERIENCES: INTENATIONAL COOPERATION

This is a list of countries' experience in terms of International Cooperation initiatives:

7.3.1 US A[2]

The United States works with a multitude of international and regional entities on SPAM, including APEC, the OECD, ITU, and the European Commission.

The FTC is an enforcement agency that is designated as a primary point of contact to facilitate anti-SPAM enforcement co-operation with foreign enforcement agencies. Many initiatives were taken by the USA to facilitate international cooperation and cross-border enforcement; the USA:

- Has entered into memoranda of understanding on SPAM enforcement cooperation with agencies in the U.K., Australia and Spain.

[2] *Source: "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003"*

- Is a member in the London Action Plan, represented through the FTC to enhance cross border ant-SPAM law enforcement
- Works with a multitude of international and regional entities on SPAM, including APEC, the OECD, ITU, and the European Commission.
- Has taken a leading role in three areas of the OECD SPAM Task Force's anti-SPAM toolkit: global enforcement, technical solutions, and outreach efforts, in close collaboration among multiple US agencies and US private sector partners.
- Cooperated on individual SPAM enforcement actions with agencies in Canada, the U.K., Australia, New Zealand, and the Netherlands.
- Has participated in the Operation SPAM Zombies to educate ISPs and others about the problem of "zombie" computers being used to disguise the origin of SPAM.

Has undertaken an extensive program in the APEC-TEL on cybercrime and cybercrime legislation, assisting a number of APEC economies in strengthening laws against all threats to networks and critical infrastructure, including SPAM.

7.3.2 AUSTRALIA A[3]

The Australian Government has established a number of international anti-SPAM information sharing and enforcement arrangements with other governments and agencies:

- In October 2003, DCITA and ACMA signed an agreement with the Korea Information Security Agency (KISA) concerning cooperation in the regulation of SPAM.
- UK, US and Australia—tripartite MoU on SPAM, 2004: This MoU is designed to facilitate the sharing of enforcement information across borders.
- Australia and Thailand—joint statement on telecommunications and information technology—July 200: The statement includes an undertaking to exchange information about anti-SPAM policies and strategies.
- London Action Plan on SPAM—October 2004: Through its participation in the LAP, Australia also supported the US Federal Trade Commission's Operations Zombie Drone, SPAM Zombies, and Secure your Server.
- Signing the Seoul-Melbourne Multilateral MoU—Asia Pacific region—April 2005.
- The Australian Government is also responding to requests for information and assistance from nations wishing to establish their own strategic responses to SPAM.

Australia is also working with international organizations such as the International Telecommunication Union (ITU), the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), the Asia-Pacific Telecommunity (APT), the Pacific Islands Telecommunications Association (PITA) and the Organization for Economic Co-operation and Development (OECD) to develop a multilateral approach to reducing SPAM.

[3] Source:
- *SPAM ACT 2003*
- *SPAM (CONSEQUENTIAL AMENDMENTS) ACT 2003 No. 130, 2003*
- *SPAM REGULATIONS 2004 No. 56*

7.3.3 CANADA[4]

Task Force members and Industry Canada are taking a leadership role in the international organizations that combat SPAM, such as the OECD Task Force on SPAM, International Telecommunications Union, the Asia Pacific Economic Cooperation, and the world summit in the information society, including in the work of the United Nations working group on Internet Governance. The following are some of the forums and committees that in which Canada participated:

- London action plan (LAP), is international SPAM enforcement cooperation which is responsible for enforcing laws concerning SPAM. There board members range from data protection agencies, data protection plan, telecommunication agencies and consumer protection agencies. Industry Canada is a participating country in the London Action Plan, an initiative to facilitate international SPAM enforcement, spanning over 27 agencies in 15 countries worldwide.
- Operation secure your server, this cooperation helps individuals and organization to secure their servers and proxies from SPAM. Competition Bureau of Canada and E-Commerce Branch of industry Canada are partnered with operation secure your server to spread the word about how organizations can protect their servers.
- Operation SPAM Zombie, This cooperation helps consumers to secure their computers from sending SPAM from the PC's. Industry Canada, Electronic Commerce Branch and Office of the Privacy Commissioner of Canada are participating in this effort to encourage ISPs to implement anti-zombie measures.
- CAUCE, Is a consumer advocacy organization, campaigning against SPAM e-mail.

The Task Force also supported the anti-SPAM activities of the United Nations Conference on Trade and Development, the Internet Engineering Task Force, and the International Consumer Protection and Enforcement Network.

With the support of the Task Force, Industry Canada and the Department of Foreign Affairs have developed and are negotiating a series of bilateral agreements between Canada and the United Kingdom, Australia, the United States and the European Commission. Agreements with the United Kingdom and Australia will be ready for approval within the next two months. Further, a number of agreements are already in place to facilitate cross-border cooperation in enforcement of SPAM cases.

7.3.4 KOREA[5]

Twelve Asia-Pacific communications and Internet agencies have joined the Australian Communications Authority (ACA) and the Korean Information Security Agency (KISA) in signing the Seoul-Melbourne Anti-SPAM Agreement, a multilateral memorandum of understanding (MoU) on cooperation in countering SPAM. It said that the MoU is focused on sharing knowledge, information and intelligence about known sources of SPAM, network

[4] Sources:
- *Privacy Act. 1980-81-82-83, c. 111, Sch. II "1"*
- *The Personal Information Protection and Electronic Documents Act*
- *Competition Act of Canada*
- *Criminal Code of Canada*

[5] Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001

vulnerabilities, methods of SPAM propagation, and technical, education and policy solutions to the SPAM problem.

Within the terms of the MoU, the agencies of the two countries will work closely together, exchange information relating to SPAM and will try to develop cooperative mechanisms to combat the rapidly growing SPAM problem. This collaboration could be extended in the future to include joint enforcement actions.

With this MoU, Australia and Korea are leading the international effort to address SPAM, also encouraging other national communications regulators to work to develop a multilateral MoU in this field. A standard MoU could be used for a multilateral approach to agreements, simplifying the establishment of international cooperation principles for locating and dealing with SPAMers.

Korea is also part of the SPAM Zombies initiative, the Secure your server initiative the London action plan, and the Asia Pacific Coalition Against Unsolicited Commercial E-mail (APCAUCE), which includes member groups from Australia, Hong Kong-China, India, Malaysia and New Zealand. It also signed a Multilateral Anti-SPAM MOU with the Malaysian Communications and Multimedia Commission and the Australian Communications Authority.

Econsumer.gov, made up of the OECD and government agencies from 17 countries, provides a web form on which consumers of member countries can make cross-border complaints. “The information contained in your complaint will allow the government agencies to spot current fraudulent schemes and help us decide how we might take action”, reads the website. E-consumer’s site also includes links to governmental agencies, and information about how consumers may resolve their complaints, and is available in English, French, German, Korean and Spanish.

Korea has four enforcement entities. These are the Korea Information Security Agency (KISA), Korea Fair Trade Commission (KFTC), Korea Consumer Protection Board (KCPB), and Public Prosecutors. These entities usually take part in activities that try to counter SPAMming, including the following:

- Participated in Operation: Secure Your Server which aims to stop SPAMmers from using "Open proxies" and "open relays" which allow unauthorized people to route their SPAM through your server.
- Took part in Operation: SPAM Zombies which tries to counter SPAMmers using home computers to send bulk emails by the millions, obscuring its true origin.
- Is a member of APCAUCE, an all-volunteer, ad hoc coalition of European Internet users, network technology professionals, and Internet Service Provider administrators to promote legislation which would outlaw UCE. APCAUCE's is the Asia-Pacific branch of CAUCE.
- Signed an Anti-SPAM Multilateral MOU with the Malaysian Communications and Multimedia Commission and the Australian Communications Authority.

7.3.5 UNITED KINGDOM[6]

There are several initiatives in which the UK is cooperating with several other foreign entities, one of them being the London Action Plan, which was developed as a method of international

[6] Source:
- Statutory Instrument 2003 No. 2426, The Privacy and Electronic Communications (EC Directive) Regulations 2003

SPAM enforcement cooperation through encouraging communication and coordination between agencies to achieve efficient and effective enforcement and also by discussing cases, legislative developments, investigative techniques, ways to address obstacles to enforcement, and consumer and business education projects.

The second initiative, a memorandum of understanding on mutual enforcement assistance in commercial email matters where all participating bodies (US, UK, Australia) are required to share evidence. The purpose would be to facilitate effective enforcement against SPAM Violations; avoid unnecessary duplication; facilitate sequential, simultaneous or coordinated investigations of SPAM violations or suspected SPAM violations; facilitate research and consumer and business education; promote a better understanding by each of economic and legal conditions and theories relevant to enforcement against their respective SPAM violations and related activities; and keep each other informed of developments in their respective countries.

The third and fourth initiative which are being hosted by the US FTC, are codenamed Operation Secure your Server, and Operation SPAM Zombies.

The purpose of the secure your server initiative is to stop SPAMers from using "Open proxies" and "open relays" which allow unauthorized people to route their SPAM through servers. These unsecured servers are all over the globe. What Operation SPAM Zombies tries to counter is the fact that SPAMers use home computers to send bulk emails by the millions. They take advantage of security weaknesses to install hidden software that turns consumer computers into mail or proxy servers. They route bulk email through these "SPAM zombies," obscuring its true origin.

The OFT and ICO have taken parts in several initiatives aimed at fighting SPAM side by side with other enforcement agencies not in the kingdom. The UK has hosted and organized some of those, and simply taken part in others as well.

- The UK is a member of EuroCAUCE, an all-volunteer, ad hoc coalition of European Internet users, network technology professionals, and Internet Service Provider administrators to promote legislation which would outlaw UCE. EuroCAUCE's is the European branch of CAUCE.
- Established the London Action Plan (LAP) alongside 27 countries to promote international SPAM enforcement cooperation and address SPAM related problems, such as online fraud and deception, phishing, and dissemination of viruses. Today, the plan has expanded to include over 60 countries.

Has entered into memoranda of understanding on mutual enforcement assistance with agencies in Australia, and the U.S.A.

7.3.6 BELGIUM[7]

Thirty four countries including Belgium got together in April 2001 and launched econsumer.gov, a joint effort to gather cross-border e-commerce complaints, in which incoming complaints will be shared through the Web site with participating consumer protection law enforcers. Belgium also took part in Operation SPAM Zombies which tries to counter the fact that SPAMers use home computers to send bulk emails by the millions. They take advantage of security weaknesses to install hidden software that turns consumer computers into mail or proxy servers. They route bulk email through these "SPAM zombies," obscuring its true origin, in this case, mostly the US.

[7] Act of 11 March 2003 on certain legal aspects of information society services.

Belgium also is part of the "Contact Network of SPAM Enforcement Authorities" (CNSA) which facilitates the sharing of information and best practices in enforcing anti-SPAM laws between the national authorities of EU Member States. In addition, a voluntary agreement was drawn up in February 2005 to establish a common procedure for handling cross-border complaints on SPAM.

The Privacy Protection committee in Belgium has been leading the SPAM fight, with other national agencies, along side all the other nations combating UCE's. The country has participated in lots of beyond border activities and continues to play a vital role within the European community.

- Part of the "Contact Network of SPAM Enforcement Authorities" (CNSA) which facilitates the sharing of information and best practices in enforcing anti-SPAM laws.

Participated in the London Action Plan, an initiative to facilitate international SPAM enforcement, spanning over 27 agencies in 15 countries worldwide.

7.3.7 MALAYSIA[8].

The MCMC is member of the following international organizations:

- London Action Plan, LAP is international SPAM enforcement cooperation which is responsible for enforcing laws concerning SPAM. There board members range from data protection agencies, data protection plan, telecommunication agencies and consumer protection agencies.
- MCMC endorsed the London Action Plan on 18th May 2005. The London Action Plan (LAP) was initiated in London, United Kingdom on 11th October 2004 to combat SPAM problem at international level through cooperation between regulators and related industry bodies.
- Operation SPAM Zombie, This cooperation helps consumers to secure their computers from sending SPAM from the PC's. The Malaysian Communication and Multimedia Commission are participating in this effort to encourage ISPs to implement anti-zombie measures.

Also to encourage exchange of information on technical, educational and policy solutions to the SPAM problem, MCMC has signed a Multilateral Memorandum of Understanding on Cooperation in Countering SPAM (MOU) with Australian Communications Authority of Australia and Korea Information Security Agency of South Korea on 27th April 2005.

These include regional preparatory meetings for global conferences and other activities which focus on Malaysia's and the region's requirements.

Another aspect of the Malaysian Communications and Multimedia Commission's international activities is organizing and hosting attachments and similar working visits by its counterparts in other countries. In return, the Malaysian Communications and Multimedia Commission participate in bilateral meetings and negotiations, and initiates working visits to enhance relations with other regulators.

In the 3rd-5th May 2005 Malaysia has hosted the following conference: "ASEAN Telecommunications Regulator' Council (ATRC) Workshop on Anti-SPAM Strategies".

[8] Section 233 of the Communications and Multimedia Act 1998 (Act 588)

7.3.8 PERU[9].

Cross border cooperation in Peru takes place through their enforcement agency, Instituto Nacional de Defensa de la Competencia y de la Protección (Indecopi).

- The country's agency is also part of the International Telecommunications Union, but has only been a spectator till recently.
- Peru is also taking part in Operation secure your server, which aims to stop SPAMers from using "open proxies" and "open relays" which allow unauthorized people to route their SPAM through third-party servers, this cooperation helps individuals and organization to secure their servers and proxies from SPAM. Indecopi is partnered with operation secure your server to spread the word about how organizations can protect their servers.
- Operation SPAM Zombie helps consumers to secure their computers from SPAMers using who utilize home computers to send bulk emails by the millions, obscuring its true origin.

7.3.9 SINGAPORE[10]

To extend Singapore's anti-SPAM efforts to international shores, IDA participated in the US Federal Trade Commission's "Operation Secure Your Server" campaign, to encourage organizations worldwide to close open relays and proxies in January this year. IDA is also committed to partake in international initiatives, including participation in global and regional fora such as APEC, ITU, OECD and ASEAN.

The secure your server campaign is supported by 36 other agencies from 26 countries. Through this campaign, the US FTC sent business advisories to organizations worldwide with unsecured servers, explained the problems associated and provided instructions on how to protect computer systems from misuse.

7.4 INTERNATIONAL BODIES RECOMMENDATIONS[11]

The OECD states that cooperation at the national level would be particularly important to avoid duplication of activities, and allow the optimization of resources and the exploitation of synergies between the different players. Informal co-operation is a first step, but more clearly established channels of communications would simplify the process, increase transparency and increase the efficiency of the system.

This section describes the recommendations regarding the enforcement cooperation of the SPAM related laws by the following International Bodies:

- Organisation for Economic Co-operation and Development (OECD); and
- International Telecommunication Union (ITU).

[9] LEY QUE REGULA EL USO DEL CORREO ELECTRONICO COMERCIAL NO SOLICITADO (SPAM)

[10] SPAM CONTROL ACT 2007

[11] Please refer to **Error! Reference source not found.** for more information and contact details of the International Bodies

7.4.1 OECD[12]

Anti-SPAM regimes are recommended to work to develop frameworks for closer, faster, and more efficient co-operation among their SPAM enforcement authorities that includes, where appropriate:

- Establishing a domestic framework: Anti-SPAM regimes should in this respect:
  - Introduce and maintain an effective framework of laws, SPAM enforcement authorities, and practices for the enforcement of laws connected with SPAM,
  - Take steps to ensure that SPAM enforcement authorities have the necessary authority to obtain evidence sufficient to investigate and take action in a timely manner against violations of SPAM-related laws that are committed from their territory or cause effects in their territory. Such authority should include the ability to obtain necessary information and relevant documents,
  - Improve the ability of SPAM enforcement authorities to take appropriate action against (a) senders of electronic communications that violate laws connected with SPAM and (b) individuals or companies that profit from the sending of such communications,
  - Review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of laws connected with SPAM,
  - Consider ways to improve redress for financial injury caused by SPAM.
- Improving the ability to cooperate: Countries should improve the ability of their SPAM enforcement authorities to cooperate with other foreign SPAM enforcement authorities. Countries should in this respect:
  - 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,
  - 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,
  - Designate a contact point for co-operation at the international level.
- Improving procedures for co-operation: Before making requests for assistance as foreseen in the previous recommendations, SPAM enforcement authorities should:

[12] OECD contact information:

Website: http://www.oecd.org

Postal Address: OECD 2, rue André Pascal, F-75775 Paris Cedex 16, France

Telephone: +33 145248200

Fax: +33 145248500

- 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.
- Attempt to prioritise requests for assistance and, to the extent possible, make use of common resources such as Websites on SPAM, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.

- Cooperating with relevant private sector entities.
  - 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.
  - Countries should encourage co-operation between SPAM enforcement authorities and the private sector to facilitate the location and identification of SPAMmers.

7.4.2 ITU[13]

Besides the OECD, ITU has few recommendations in this regard.

According to ITU, international cooperation on enforcement is essential in order to ensure the effectiveness of anti-SPAM rules. In other words, it must be possible to trace back SPAMming activities and prosecute SPAMmers, regardless of national borders.

As a pre-requisite, national legislation could facilitate information sharing and mutual assistance between competent authorities in different countries. Appropriate bilateral and/or multilateral cooperation would enable appropriate information sharing and mutual assistance on specific SPAM cases.

The choice of the international instrument(s) to do this may depend on various factors. However, all organizations can in any event promote such cooperation on enforcement within the limits of their competence.

Certain countries, including some EU Member States, have concluded cooperation agreements (e.g. Memorandum of Understanding) to facilitate such cooperation. These documents generally call upon participating parties to produce their 'best efforts' to cooperate with each other on issues such as building evidence, user education, new SPAMming activities, training, etc.

---

[13] ITU contact information:

Website: http://www.itu.int

Postal Address:

ITU
Place des Nations

CH-1211 Geneva 20
Switzerland

Telephone: +41 22 730 51 11