

BIAC MAAWG BEST PRACTICES FOR INTERNET SERVICE PROVIDERS AND NETWORK OPERATORSⁱ

March 2006

Background

ISPs and network operators have an important role in the fight against spam.

Given this important role, ISPs, network operators, technical groups and alliances continue to share best practices for preventing/diminishing spam sent from or across their networks.

Although best practices will not, in and of themselves, constitute a comprehensive solution to spam, they are part of a multi-prong strategy for addressing the problem of spam. The larger the number of entities endorsing and applying common practices, the more effective they will be.

In the event that these voluntary Best Practices are taken up by ISPs and Network Operators, their positive impact will be increased if end-users also take necessary steps to protect the security of their computers, software and networks, including the protection of their personal identity on-line.

Intent

BIAC's Best Practices for ISPs and Network Operators are a set of voluntary principles developed by business aimed at enhancing the security of network infrastructures in the fight against Spam. Industry will continue to collaborate on additional technical and procedural measures to further implement these principles.

BIAC proposes the following Best Practices for ISPs and Network Operators as an important tool in combating Spam.

These Best Practices and any additional measures are voluntary, and in all cases precedence is given to applicable legal and regulatory frameworks.

Implementation of these Best Practices and any additional measures will vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges.

We note that flexibility in the implementation of these Best Practices and any additional measures is the key to achieving their broad and meaningful adoption by service providers of all sizes.

Given the rapid pace of technological change, the Best Practices will be reviewed and updated as necessary.

Best Practices

Context/Definitions

In any given national jurisdiction, each of the Best Practices is understood to be recommended only if it is not in contradiction with existing national legislation.

In the context of these Best Practices “ISPs and network operators” include any entity operating a SMTP server connected to the Internet.

BIAC Recommends to ISPs and Network Operators that:

- 1. Within the boundaries of the appropriate legal framework, ISPs and network operators address the problem of compromised end-user equipment by establishing timely processes to allow such end-user equipment and network elements to be managed and eliminated as sources of Spam;**
- 2. ISPs and network operators utilize industry standard technology to authenticate their email and/or their sources;**
- 3. ISPs and network operators block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be attained from the customer;**
- 4. ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately;**
- 5. ISPs and network operators establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints.**
- 6. ISPs, network operators and enterprise email providers communicate their security policies and procedures to their subscribers;**
- 7. ISPs and network operators attempt to send non-delivery notices (NDNs) only for messages originated by their own account holders;**
- 8. ISPs and network operators take measures to ensure that only their account holders use their e-mail submit servers;**
- 9. ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;**
- 10. ISPs and network operators ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries; that all local area network (LAN) operators are compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets," and**

that in particular, LANs do not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

ⁱ BIAC was created in March 1962 as an independent organisation recognised by the OECD as the official representative of the OECD business community (<http://www.biac.org>). BIAC's members are the major industrial and employers' organisations in the 30 OECD member countries, representing over 8 million companies. Via its 31 standing committees and policy groups, BIAC mirrors all economic policy issues the OECD covers and examines their potential impacts on business in both member and an increasing number of non-member countries like Russia, China and India.

The Messaging Anti-Abuse Working Group (<http://www.MAAWG.org>) 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. With a broad base of Internet Service Providers (ISPs) and network operators representing over 600 million mailboxes, key technology providers and senders, MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.