This download contains two documents:

MAAWG Sender Best Communications Practices Executive Summary

starts on page 2

and

MAAWG Sender Best Communications Practices Version 2.0a-Updated

starts on page 12

Updated September 2011

MAAWG Sender Best Communications Practices
Executive Summary

Introduction

The first portion of this document serves as an Executive Summary of the MAAWG Sender Best Communications Practices (BCP). Please refer to the principal BCP Version 2.0 Update for more detail starting on page 12 of this document.

The MAAWG Sender SIG has set forth this Best Communications Practices (BCP) as part of the mission of MAAWG to reduce message abuse. This BCP creates a greater transparency between senders of bulk mail and the receiving operators. This transparency helps distinguish legitimate mailers from spammers and the BCP also advocate technologies and practices that help to make email a more secure and reliable communication channel.

While this document outlines industry Best Communications Practices, it is also understood that not all receiving networks and senders will implement all of these practices due to the complexity of the network infrastructures, public policy considerations and the scalability of network platforms.

BCP Overview

There are five primary topics and recommendations set forth in this BCP. These five topics are meant to cover everything from the habitual practices of mailing to more technical recommendations that deal with email sending architectures and the unsubscribe mechanisms as components of the email ecosphere. This Executive Summary is presented as a summary primarily of Sections III and IV of the BCP because of the technical discussions involved in these sections. There is also a list of definitions and an ESP Vetting Questionnaire at the end of this Executive Summary to assist readers. The remaining sections of the BCP should be understood as they are written.

Section III: Enhancing Sender Accountability and Messaging Reputation
Section IV: Managing Delivery Errors and List Maintenance

Enhancing Sender Accountability and Messaging Reputation

The communication between the sending and receiving servers is sometimes referred to as the "handshake." That handshake needs to happen on a foundation of trust based on the technological solutions that have been developed to establish identity and accountability.

Email authentication should be adopted by all mailers to help identify the originator of the email. These technologies take several forms, from path-based to cryptographic solutions that necessitate a public/private key pair. (For more information on email authentication, see the MAAWG white paper "Trust in Email Begins with Authentication.") Every aspect of the sending architecture, from the initial HELO to the

sending domains, should clearly identify the sender or the sender's clients. Authentication is one component of clearly identifying IP addresses. Dedicated IP ranges should be employed in the transmission of email where reverse lookups on those domains clearly identify the brand and Web site of the sender.

ISPs have put forth Acceptable Use Policies (AUPs) for anyone wishing to transmit mail into their networks. These should always be considered wherever possible and be referenced as part of the due diligence involved in establishing a reputable mailing campaign. One component of a reputable campaign is a well-coded message that delivers relevant and clearly identified content. This may include a tracking pixel and/or cookie that are clearly defined by the sender's Privacy and P3P (Platform for Privacy Preferences) policies. The email should also be free of attachments, large images, and forms or scripts that are commonly used by senders of malicious and fraudulent email.

A) ISPs have established Acceptable Use Policies (AUPs) with messaging rules to be read and implemented before attempting to deliver mail to their domains. Senders should take note of any and all AUPs for the domains to which they plan on delivering messages. In addition to the policies set forth by the receiving domains, mailers should be aware of any and all policies set forth by their ISPs and hosting companies.

B) Senders should incorporate as many authentication standards and technologies as their systems can support for each of their messaging streams: Transactional, Marketing and Corporate. These standards can range from mechanisms that help identify mailers by linking IPs to domains (Sender Policy Framework, known as SPF, and Sender ID) to more complicated cryptographic technologies like Domain Keys Identified Mail (DKIM). At the very least, senders should incorporate SPF records for their mailing domains. Senders should consider joining industry groups such as MAAWG, the ESPC (the Email Sender & Provider Coalition), EEC (Email Experience Council) and others to participate in the growth and adoption of best communications practices in the industry.

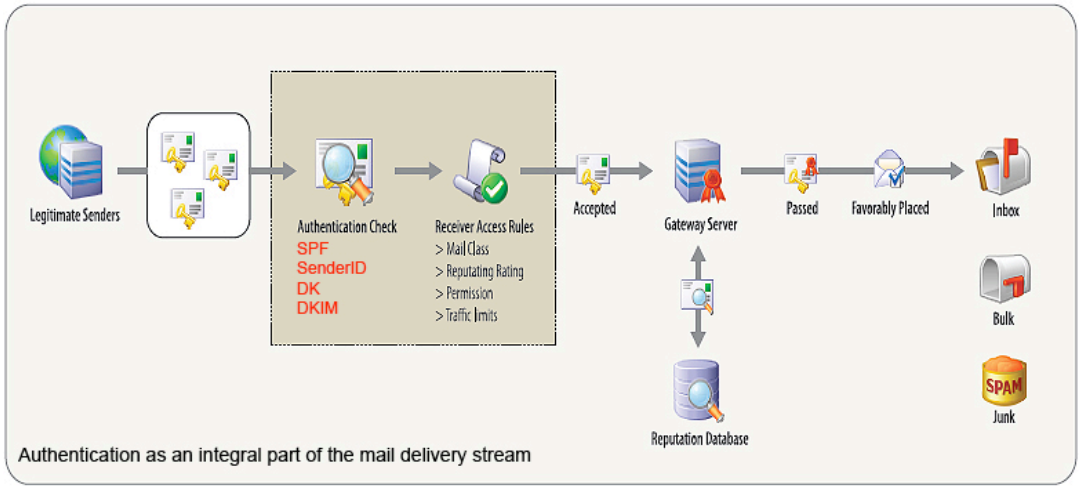

Diagram courtesy of StrongMail Systems, Inc.

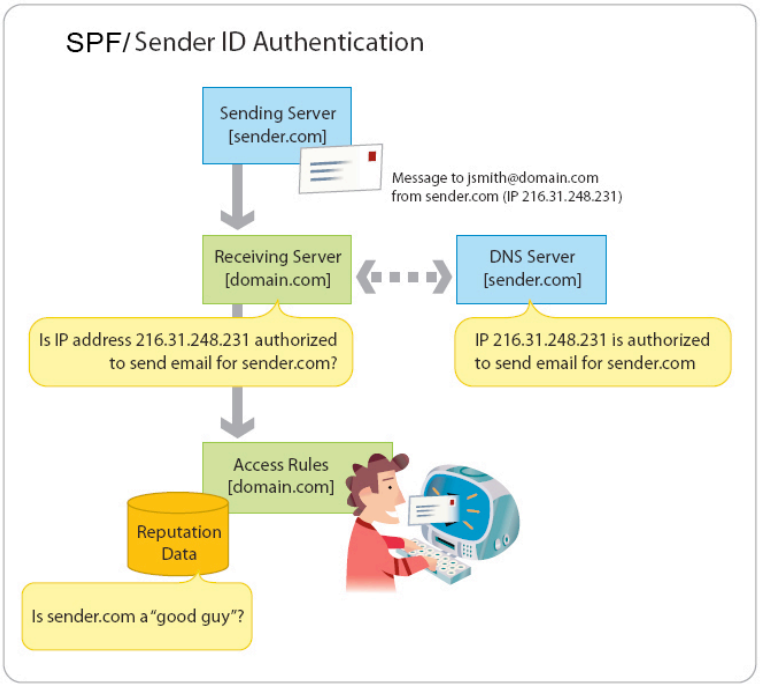

Diagram courtesy of StrongMail Systems, Inc.

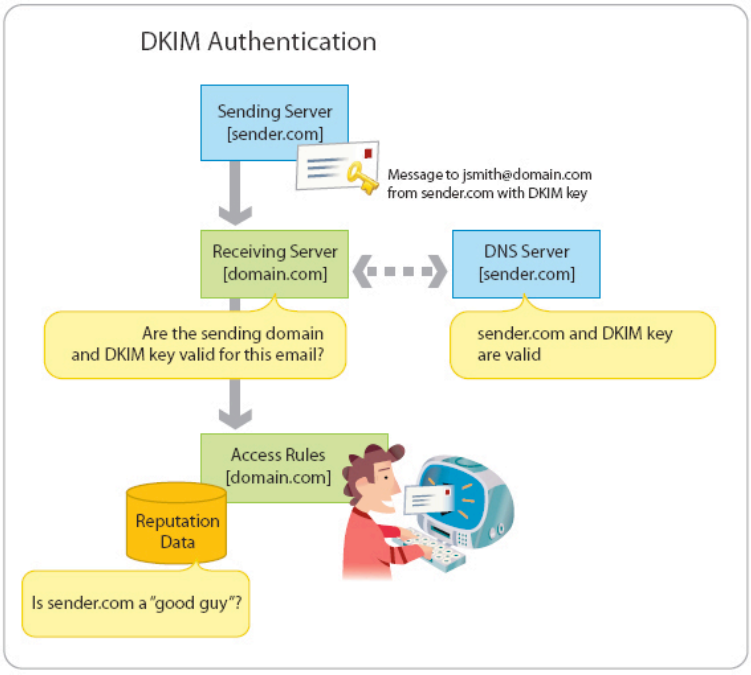

Diagram courtesy of StrongMail Systems, Inc.

- Different messages will have different requirements in terms of confidentiality and privacy. It is important to note that email authentication is not a means to secure confidential message content. Concerns of confidentiality should be addressed through secure messaging technologies.

C) One of the challenges that senders face is that of differentiation. From the perspective of ISPs, legitimate bulk mail may seem like UCE (unsolicited commercial email). In order to help identify themselves, legitimate senders should take steps to help maintain their identity as a means of

accountability through the proper configuration of their email headers and DNS records. These configurations should include the following considerations:

- Domain owners must ensure they include accurate information in the WHOIS database, which identifies owners of domains and how to contact them by entering the stable parent company, point of contact and name servers. Each registered domain must have an entry in WHOIS. WHOIS Proxy (anonymizing) services must not be used.

- All IPv4 and IPv6 addresses allocation must be accurately and completely documented. Documentation must take place via WHOIS or rWHOIS. Equivalent information via other formats in addition to WHOIS/rWHOIS is also acceptable.

  - Sub-allocations of IPs of net-blocks equivalent to or larger than /29 for IPv4 and /56 for IPv6 must be accurately and completely documented, in keeping with ARIN (and other RIR) policies, for example: https://www.arin.net/resources/request/reassignments.html.

- In addition to a matching and consistent reverse and forward DNS to help identify IPs, the HELO/EHLO and MAIL-FROM should remain consistent for a campaign (also for subsequent campaigns of the same nature) and be presented in the form of a domain name rather than an IP address. Changing names and/or identifiers midstream during a campaign can present significant delivery problems.

  The HELO/EHLO should be configured to match the reverse lookup of the mailing IP so that the domain remains the same across the various parts of the header and connection mechanism. If multiple servers are used to deliver mail through the same externally visible IP, their HELO/EHLO should be within the same domain and not identify themselves as different domains to remain consistent.

- The "From" name used in the mailing should be easily identifiable and relevant to the mailing. When considering how to identify the brand and campaign, consideration should be given to easily identifying the company and brand through the domain part and the friendly part of the From name.

- When maintaining separate and unique IP addresses is not possible, senders and/or messaging providers should take measures to create consistent means of identification at the domain level. The domain should remain the same across all of the senders and campaigns on the shared domain. A unique subdomain should be employed to separate and clearly identify the mailers on that domain.

  In addition, shared networks should try to be kept within the same range of IPs like a /24 (all 255 IP addresses in a class C network e.g. 255.255.255.[0-255]). The separation of senders on a shared network should not stop at the domain or the IP level. Effort should be made and measures taken to separate mail based on content (e.g. transactional vs. commercial).

- When deciding on a domain name, choose one that ultimately reflects and references the sender's Web site.

D) Senders should create transparent content for which they can be accountable.

- Verbiage requesting recipients to add the sender to their address book should clearly state that such action is not a guarantee of delivery.
- When constructing redirects in the body of the message, they should be similar and consistent, and not multiple and varied. (This is not to be confused with dynamic domain name-specific tracking links that are acceptable.)
- Refrain from sending large images, attachments or creating messages that are composed solely of an image(s).
- When employing tracking pixels (Web bugs or beacons), clearly state their presence in your public privacy or P3P policies.

E) Wherever possible, senders are advised to engage in a process of disclosure through whitelisting and establishing feedback loops with the ISPs that provide them. Senders should actively monitor abuse-related complaints from individuals and ISPs with an understanding that every ISP has the right to set their own abuse and complaint thresholds. As a monitoring mechanism of the domains, senders are advised to setup role accounts: abuse@[domain] and postmaster@[domain]. (For more information on role accounts refer to RFC 2821 and RFC 2142.)

F) Senders need to practice proactive due diligence before commencing a program of safe messaging by being aware of the age of their lists and refraining from sending to inactive accounts. ISPs are known to convert old accounts into traps to help them curb abuse by unscrupulous mailers. In addition to the age of a list, senders should be aware of their clients' list sources and differentiate between different qualities of lists by employing their own anti-spam techniques and/or contracting with a third party to help measure and characterize potentially abusive accounts and lists.

Managing Delivery Errors and List Maintenance

The other aspect of a good architecture is being able to interpret and respond accordingly to the machine responses referred to as bounces. Senders should become familiar with connecting limitations that ISPs impose on the delivery of email; too many connections may result in the blocking of the connecting IP and refusal of further connections. More is not better in this case and senders should be aware of these nuances.

The bounces that are sent back will include a codified message in the form of a numeric series and an expanded description sometimes called a DSN (Delivery Status Notification). In order to comply with established AUPs and to further distinguish one's self from the spammer community, senders should have mechanisms capable of reading and accurately interpreting these bounce messages. Actions taken in regard to bounces will range from unsubscription of invalid addresses on the first hard bounce, to limiting mailing to a domain where a block or some other form of service denial has been detected.

While it is true that certain receiving domains emit misleading error codes in violation of RFC 2821, it is best not to compound the error and completely ignore them either. Ignoring them will cause deliverability issues with sites that do not issue misleading codes, which are in the vast majority.

A) Senders should be aware and able to monitor the Delivery Status Notifications (DSNs) and should examine their SMTP logs for other errors. SMTP delivery errors are defined in RFC 2821 and RFC 3464. The examples given in the latter may not always exactly match the log[1]. Senders should carefully examine the text of the error to better understand the delivery problem.

B) In addition to describing errors, RFC 2821 sets forth guidelines for connection policies. Senders should familiarize themselves and take precautions to avoid making too many connections, as this can result in a temporary block. When connection timeouts occur, senders should be aware of this situation and limit the number of connections they are trying to establish, as this too can result in a block or complete denial of connections[2].

C) When experiencing transient failures (such as 4xx errors[3]), senders should vary their retry attempts. This variance may be partially determined by the content and nature of the message itself, as in the case of a timed offer or legal update. The retry process itself should not continue for more than (4) four days. The DSN should be examined as it may provide further guidance. If the failures continue, senders should evaluate if their sending infrastructure is in compliance with the published AUP at the domain in question.

D) Besides transient failures, senders may receive permanent failures[4]. Good mailing practice dictates that permanent failures should be removed from the mailable list and unsubscribed. It is advised that mailers assess the failures prior to removing the names and take into consideration that "out-of-office" and "mailbox full" errors may show up as permanent failures and are indicative of a correctable condition. Errors of the 55x_5.7.1[5] form are commonly indicative of a block or state of being that is in conflict with an ISP's AUP in addition to other error codes that convey a similar status.

   Investigation should be made and measures taken to resolve the situation prior to re-mailing or continuing to send mail to the domain. If no additional information is present that might point to another underlying cause for the permanent failure, senders should remove the email address and not attempt mailing it again.

---

[1] Log refers to a record of all the connection attempts, success and failures, that are kept by a mail server.

[2] It is important to remember that RFC2821 was written in 2001 – long before spam accounted for even 50% of all email – and as such, the examples given may seem quaint and outdated in comparison to today's systems.

[3] 4xx refers to temporary or not permanent failure messages, e.g. mailbox full.

[4] A permanent failure refers to an error message that informs the sender that the intended user does not exist at this domain, similar to calling a wrong number.

[5] One form of a permanent failure.

Mitigating and Resolving Messaging Disruption Issues

Disruptions to the communication stream are bound to happen; it is the sender's responsibility to keep logs of what they send and what is sent back to them in order to anticipate message disruptions based on a good analysis of hard bounce rates, and complaints through ISP feedback loops, where available. Senders should be able to distinguish between the various forms of feedback, including machine bounces and end user complaints. It is important to keep metrics on both as they will aid a sender in distinguishing different facets of list hygiene and ultimately help to keep the mailable population of their clients current and productive.

When appropriate, senders should be aware of established practices and modes by which ISPs perform contact resolution. Calling the CEO of an ISP company will not help you get the block lifted, although it might help change that dynamic block to something more permanent.

Keep in mind that a sender's domain is governed by their rules and the desires of their end users. Final authority based on what is allowed in and what is denied rests with the controller/operator of that domain. When attempting to remediate a problem, take into account that ISPs receive billions of messages and the technologies that help them identify and filter the good from the bad are not always perfect, but they are a necessary tool in helping curb spam and fraud from reaching a recipient's mailbox.

Appendix A: Notes on Permission and Subscription Management

i) Permission given by a subscriber can be revoked at any time.

ii) Subscriber permission, especially at the confirmed (double) opt-in level:

a. Avoids erroneous subscriptions due to typos and the accidental addition of spam traps to a mailing list.

b. Plays a part of the overall reputation of a given mail stream but other factors, including additional mail streams (i.e. the overall reputation of the sender), user complaints and IP history, may play a more important role in the decision-making process used by receivers to accept mail.

Appendix B: RFC Resources

Information on RFCs is publically available on the World Wide Web at a number of sites. The following links are to the IETF (Internet Engineering Task Force) Web site and archive of RFCs.

RFC	Title
2142	Mailbox names for common services, roles and functions. http://www.ietf.org/rfc/rfc2142.txt?number=2142
2821	Simple Mail Transfer Protocol (SMTP) http://www.ietf.org/rfc/rfc2821.txt?number=2821
2822	Internet Message Format http://www.ietf.org/rfc/rfc2822.txt?number=2822

Appendix C: ESP Vetting Questionnaire

The following questions are designed as a means to help marketers engage in a dialogue about best communications practices with a prospective ESP (Email Sender Provider) partner. By no means is this list complete; however, it is derivative of the principals put forth in this document and is provided here as a tool to check conformance with industry-stated best practices.

- Do you incorporate and comply with public AUPs?
- Do you provide dedicated IPs?
- Do you provide a dedicated IP for each type of message stream (marketing vs. transactional)?
- Do you match forward and reverse lookups for your IPs?
- Which methods of authentication do you support and provide?
- Which ISPs are you whitelisted with?
- Which ISPs have you established a feedback loop with?
- Do you distinguish between hard and soft bounces?
- What is your hard bounce policy?
- What is your soft bounce policy?
- What is your standard retry policy for soft bounces?
- How do you handle connection timeouts?

Appendix D: Definitions

Definition	Explanation
/24	Short hand notation commonly referred to as CIDR ranges. The /24 denotes all the IPs available in a class C network, or the IPs from 0-255.
Address Acquisition: Confirmed Opt-in or Double Opt-in	The subscriber enters an email address, a message is sent to that address, and the recipient must take affirmative action to confirm the subscription; for example, replying by email or clicking a URL.
Address Acquisition: Notified Single Opt-in	After entering an email address, that address receives a "welcome" message, possibly with further instructions.
Address acquisition: Single Opt-in	Single-step Web-form or other subscription address where the recipient enters an email address and messaging begins.
Dedicated IP Ranges	IPs dedicated to the sending of a certain kind of traffic, such as Corporate, Marketing or Transactional, with no other sole purpose and not shared between different brands, clients or domains.
Dictionary Attacks	A technique used by spammers where they guess parts of an address or use random word generators to make up the envelope portion of an email address; for example: a@domain, ab@domain, abc@domain. No permission is entailed.
Externally Visible IP	This is the public IP as opposed to the private IP that is used for identifying machines within a given network through Network Address Translation. Headers sometimes provide the routing information that may include private IPs. The internal IP schema is not at issue, only the IPs across multiple servers that are visible to the whole world.
Forward Lookup	Refers to an ordinary lookup of the host name to determine the underlying IP address.
From (Address)	The address that is seen by the end recipient and presumed to be the "sender" of the email.
Header	Email headers contain the routing, from, recipient, subject, date and other information given at the beginning of an email. (See RFC2822)
HELO/EHLO	The HELO (or EHLO) is the first command issued by an SMTP client (MTA or MUA) to identify the name of the sending machine. (See RFC2821)
List Purchase	A list of addresses is sold to a new owner(s). If the list is only sold one time to only one new owner, permissions may stay intact. If sold as multiple copies to various senders, permission is quickly diluted or totally lost.
List Rental	An advertiser hires a list owner to send the advertiser's message to the owner's address list. The list does not change hands.
Mail Transfer Agent (MTA)	An SMTP server or some other device used for the sending of email.
Mail User Agent (MUA)	An email client or some other commonly used program for the sending of email.
MAIL-FROM	Issued by the connecting MTA (mail server) via "Mail From" SMTP command indicating where the email originated from, and used by SMTP to indicate where mail transfer error messages (bounces) should be sent. This is normally not seen by the recipient and should not be confused with the Message From Address. (See RFC2821)

Permission level: Opt-in	The recipient gives their permission before their address is collected and before any messaging begins.
Permission level: Opt-Out	Sender acquires addresses by means other than the recipient's prior permission, and the recipient can stop the mail upon request.
Request For Comment (RFC)	"Request for Comment" are documents produced under the aegis of the Internet Engineering Task Force (IETF) and are the technical standards for Internet protocols, formats and other mail technologies such as SMTP `(email), etc.`
Reverse Lookup	Reverse Lookups allow someone to determine the host name of an IP address. This provides a level of accountability and tracking. IP addresses enabled with a reverse lookup, are helpful in determining the identity of the IP.
Retry Attempts	Mail servers are configured to attempt and redeliver email that has bounced based on the specific type of bounce that the mail server receives. These attempts are often times configurable, as are the triggers for them. Retry attempts refers to the subsequent attempts of the mail server once it has received the initial bounce or refused connection.
Subdomain	A domain that is a second level domain of a larger domain but still within that larger domain, for example: foo.example.com, foo is a subdomain of example.com.
Traps	Traps or Spamtraps can be long closed accounts reactived by an administrator or brand new accounts setup and left to sit at a domain without being subscribed to any list in order to receive and track the email received as a means of identifying spammers. The idea is if the new account has never been subscribed to a list, every piece of email it receives is sent without permission and is then considered spam. In the case of an old account that is reactivated, user unknown or hard bounce messages would have been sent out for quite some time and legitimate senders should have removed the address from their lists. Once reactivated, those who send email to that account will be flagged for poor list maintenance or possibly even blocked in the future.

MAAWG Sender Best Communications Practices - Version 2.0

(Revised 02/06/08 and Updated September 2011)

Introduction

In an effort to facilitate the mission of the Messaging Anti-Abuse Working Group in reducing messaging abuse, the MAAWG Senders SIG offers these best communications practices for high volume SMTP-based email senders[6]. The goal of these practices is to enhance the transparency of legitimate messages and enable receiving operators to maximize their resources in the fight against messaging abuse.

In addition to the principles stated below, acceptable communications practices for email interchange must include regulatory compliance with the requirements inherent in the industry's Acceptable Use Polices (AUPs) and regional governments' regulations[7]. Senders must adhere to these requirements to avoid possible industry and law enforcement actions and risk inviting additional regulations. Senders also should consider joining and adhering to relevant self-regulatory initiatives, such as those prescribed by other industry trade associations and email accreditation providers.

While this document outlines industry Best Communications Practices, it is also understood that not all receiving networks and senders will implement all of these practices due to the complexity of the network infrastructures, public policy considerations and the scalability of network platforms.

I. Senders Must Obtain Clear and Conspicuous Consent

a. In establishing informed consent, senders must provide clear and conspicuous notice to users at the point of email address collection, and make that consent notice obvious and readily available for online reference at any time, by any party. The notice should allow reasonable users to easily and readily understand to what exactly they are consenting prior to providing their email address.

b. The notice should clearly state the specific type of list(s) to which users are subscribing and the sender should consider noting the potential frequency, type, and approximate interval of communications that will be received. If email addresses are to be used for secondary purposes, then that purpose should also be disclosed as part of the consent process.

---

[6] This does not refer to person-to-person traffic initiated by ISPs.
[7] See Appendix B: Email regulations by various regions.
[8] Validity can be determined by identifying email address syntax errors, domain errors, and message-attempt errors.

i. Whenever a sender collects an email address, it should follow up with a confirmation message sent to that address in order to determine the validity[8] of the supplied address. It should also indicate within the content of the message the recipient's granting of consent to receive messages from the sender.

1. Confirmation messages should be sent using a dedicated IP address.
2. Confirmation messages should be sent from the same 'From' address as other messages.

c. Senders are encouraged to work with industry partners to develop trusted subscription mechanisms that may more easily verify user consent.

II. Enable Clear, Conspicuous and Easy to Use Unsubscribe Options

a. Senders should make the unsubscribe process as clear and easy to use as reasonably possible.

b. Senders should process unsubscribe requests as quickly as reasonably possible and with the recipient in mind.

c. Senders are reminded that unsubscribe requests may be regulated and subject to the laws of varying jurisdictions.

d. Senders are encouraged to set expectations during the unsubscribe process detailing the specific timeframe in which the sender may process the unsubscribe request and from what list(s) or communication types the user has unsubscribed from.

e. Senders should adopt the List-Unsubscribe mechanism within the header of each message as described in RFC 2369.

f. Senders should use text descriptions, instead of images, to accompany hyperlinks to a one-click online unsubscribe web page.

i. Senders should have the capability to process email-based unsubscribe requests. Senders should also consider making offline unsubscribe mechanisms available. The sender's 'From' or 'Reply-to' email address should also be able to receive unsubscribe requests, unless otherwise indicated.

ii. When new subscribers are presented with hyperlinked online subscription preference centers with multiple subscription options, the specific list-unsubscribe option should be pre-checked by default for those lists in which users are subscribed. When a provider makes new subscription offers available, returning subscribers should be presented with these selections unsubscribed by default.

iii. The unsubscribe link must contain everything necessary to successfully unsubscribe from the list: Subscriber ID; which list to unsubscribe from, if there are multiple list options; and per-user-authentication-tokens, if necessary to prevent third parties maliciously unsubscribing someone else.

g. Senders that receive an abuse-related complaint from a recipient should:

---

[8] Validity can be determined by identifying email address syntax errors, domain errors, and message-attempt errors.

i. Immediately honor any and all abuse-related complaints regarding an email list subscription as if they were an unsubscribe request.

ii. Accept abuse-related complaints at "role" account email addresses, including abuse@sender-domain and postmaster@sender-domain, as well as monitor complaints sent to the WHOIS or other domain directory service contact email address for that particular sending domain name.

iii. Monitor and work to minimize the amount of abuse-related complaints received as they could result in a violation of a senders' outbound or receivers inbound Internet or Email Access Provider acceptable use policy.

h. Senders are encouraged to work in conjunction with industry participants to develop trusted unsubscribe mechanisms that may more easily facilitate subscriber choice.

i. Senders should identify the recipient email address in the message body to remind recipients which email address they are subscribed for a particular list.

III. Enhancing Sender Accountability and Messaging Reputation

a. Senders should be aware of and adhere to inbound messaging acceptable use policies (AUPs) of each Internet or Email Access Provider, where available, to which messages are sent. Senders should also be aware of, and comply with, the usage policies of their own sending Internet access providers, IP services partner, and domain name registrars.

b. Senders should adopt email authentication for all types of messaging, such as through path-based and cryptographic methodologies.[9]

i. Senders should consider using varying authentication mechanisms and identifiers based on various types of messaging.

ii. Senders should also recognize that email authentication does not secure the content of a message during transport, so senders with private content are encouraged to adopt secure messaging technologies in conjunction with email authentication methodologies to ensure the protection and integrity of messaging content.

iii. Senders should ensure authentication records are current and regularly inventory all domains to ensure full coverage of all domains and IPs and to verify that no errors exist.

[9] Path-based methodologies include the Sender Policy Framework (SPF) and Sender-ID, and cryptographic methodologies include DomainKeys Identified Mail (DKIM).

c. Senders should adopt these messaging identification practices:

   i. Ensure accuracy and accountability for outbound messaging domain name record identification within the WHOIS database.

   ii. Ensure that reverse domain name system (rDNS) records are established for outbound and inbound messaging domains.

   iii. Dedicate and maintain consistency with outbound Internet Protocol (IP) address(es) per sender and with their corresponding domain names, i.e.: forward and reverse DNS should match.

   iv. Senders should use consistent domain names in (but not necessarily across) HELO/EHLO, rDNS, MAIL-FROM and body 'From' for each campaign or list, and not use different domain names for the same campaign.

   v. Ensure the HELO/EHLO presented by the SMTP client is the valid fully-qualified domain name (FQDN) of the sending host, rather than a literal IP address.

      1. This host name should also resolve to a DNS address resource-record-set used by the host.

      2. The HELO/EHLO should match the reverse DNS of the sending IP even if it is from an IP address shared between multiple campaigns and/or domains. In environments where multiple email servers are behind a router, the HELO/EHLOs of each server should be in the same domain.

      3. Corollary: the HELO/EHLO should be the same for all email emitted from a given IP, except as noted under 2 above.

   vi. The three components of the RFC 822/RFC 2822 'From' mailbox address(es) (display-name, local part, and domain) should all be equally identifiable and accountable and should be consonant with each other. That is, a human reader of all three values should be able to interpret these as referring to the same organization or entity, and the addresses should be appropriate to the content of the message.

   vii. In cases of multiple senders on a shared IP network, messaging administrators should ensure:

      1. Common identification of shared email server-level domain names identifying the messaging provider with an option to include identification of the sender in conjunction with the messaging provider.

      2. If the messaging provider uses its own domain name for visible and/or envelope identification, then it is also encouraged to allocate a sender-level subdomain in conjunction with that messaging provider's domain, such as news@sender-domain.messaging-provider.com or provide a sub-domain for the HELO/EHLO and rDNS which will identify the sender.

      3. Maintain consistency and similarity of outbound IP addresses for senders, such as being within a small number of stable IP ranges.

      4. Maintain dedicated IP ranges for certain types of senders or content, such as differentiating transactional messaging from commercial messaging or other content that is highly likely to fall under corporate policy restrictions.

   viii. Messaging domains should reference the sender's Web site.

d. Sender content should be transparent and accountable by following these principles:

   i. When requesting users to add a sender's 'From' address to their recipients' address book, senders should point out to recipients that this entry does not ensure message receipt, but rather, is requested because it may improve the likelihood of delivery to the recipients' inboxes or the delivery of images and URL enablement.

   ii. Refrain from use of multiple and various domain name redirect links within the body of a message. (This is not to be confused with dynamic domain name-specific tracking links that are acceptable.)

   iii. Minimize the use of large image files and messages composed of a single image.

   iv. Refrain from the use of special coding scripts and embedded forms.

   v. Refrain from attaching files to messages.

   vi. Senders should use anti-spam filter tools to evaluate potential content delivery issues and distinguish their content from that of commonly used text and content-structures used by non-permission based emailers.

   vii. Use of cookies and tracking pixels (i.e.; Web bugs or beacons) should be clearly and conspicuously disclosed in a sender's privacy and P3P policies.

   viii. Senders should refrain from using only images to present the substance of the message, unsubscribe instructions or identifying whom the sender is or whom the message is being sent on behalf of. In other words, the substance of the message, unsubscribe instructions and sender identification should be displayed as regular text or text with HTML markup in the message rather than an image or Web-linked image.

e. Senders should identify themselves and enable accountability through designated Internet or Email Access Provider whitelist and/or abuse feedback loop request web pages or other postmaster-specific communications.

   i. Messaging from Internet or Email Access Providers to abuse or related role accounts should be scalable to the proportion of mail sent by that sender or messaging provider.

   ii. Senders should actively monitor and work to minimize abuse-related complaints received from an individual or network provider. Senders should also recognize that there is no parity in the percentage of abuse-related complaints sent from one Internet or Email Access Provider to another, and that each provider sets their own thresholds for acceptable numbers of complaints.

f. Senders should adopt their own anti-spam techniques or obtain services by third-parties that employ their own techniques to characterize lists of potentially abusive accounts. For example, when a sender identifies an account or data segment that appears to have triggered a decoy-based anti-spam filter, use of that account or data segment should be suspended and investigated.

g. Senders should actively attempt to identify and account for any addresses that have not received email for a lengthy period of time. When identified, senders are encouraged to ensure the maintained accuracy and behavioral response interest-level with these legacy addresses as some Internet Access or Email Providers may re-use these addresses for other customers or with their anti-spam recognition efforts.

IV. Managing Delivery Errors and List Maintenance

a. In addition to monitoring Delivery Status Notifications (DSNs), senders should ensure relevant SMTP session logs are also reported and examined. SMTP delivery errors are defined in RFC 2821 and in RFC 3463. RFC 3464 defines DSN message format extensions to aid with the parsing for error codes. Senders should note that error code examples given in the RFC documents may not accurately reflect the actual cause of an error, and the text accompanying the error describing the cause may need to be examined.

b. Senders should strategically incorporate RFC 2821 section 4.5.4.1 into their sending retry attempts.

   i. Too many connections to the same host may result in the host rejecting subsequent connections from the same client for a period of time.

   ii. When connection timeouts occur or temporary errors are received, the number of simultaneous connections being attempted should be reduced.

c. Senders should vary retry attempts in conjunction with network operator response codes indicating a temporary status failure such as a 4xx error code. The duration or the number of a sender's overall retries may vary depending upon the nature of the message content.

   i. A sender's retry process should not continue beyond four (4) days, which allows server recovery following a weekend outage. On occasion, the DSN will offer information on how to retry transient failures.

   ii. If senders encounter multiple sequential temporary status failures, they should investigate whether their SMTP infrastructure is in conflict with a receiving network policy.

d. When senders encounter permanent delivery failure error codes, which may include text or other descriptive elements, they should assess some of the following conditions prior to extraction of the failed addresses:

   i. Errors indicative of resource-related delivery failure codes might require an extended assessment period to accommodate the message; for example, the problem might be a vacation-related overflow condition.

   ii. Errors including a 55x_5.7.1 (Delivery not authorized, message refused) error code are violations of ISP Acceptable Use Policies and should be investigated prior to engaging in subsequent messaging.

e. Senders should not attempt to send subsequent email messages to addresses found to be non-deliverable as a result of one or more persistent permanent DSN failures (hard bounces). Senders should remove such addresses unless subsequent additional information indicates there has been a change in its status.

Editorial Note: *MAAWG is committed to increasing accountability and transparency for SMTP error messaging. Please see the MAAWG document Configuring Human Readable Delivery Status Notifications (DSN) for more details.*

V. Mitigating and Resolving Messaging Disruption Issues

a. Senders should be aware of, and recognize all relevant Internet access or email providers' inbound messaging Acceptable Use Policies (AUPs). In most cases, the provider's Web site will contain links or other navigation to their respective AUPs.

   i. Another such method may be to access a SMTP HELP transmission, which may refer to the provider's AUP.

   ii. In the event that the website or SMTP does not disclose the AUP, then the sender is encouraged to contact the provider directly.

b. Senders should track accountability metrics for the individual IP addresses and domain/subdomain names for all outbound messaging, including:

   i. Recipient complaints through ISP feedback loops, directly from recipients, or through third-party services.

   ii. Permanent DSN failure percentages (i.e., hard bounces)

   iii. Spamtrap addresses (when available, typically through third parties[10])

c. Senders should access and track metrics through Internet or Email Access Provider postmaster data repositories, where available[11.]

d. Senders should use reasonable means to establish delivery-test accounts at relevant Internet or Email Access Providers to provide increased accountability for network-wide deliverability issues as opposed to investigating potentially isolated incidents reported by recipients. Senders are encouraged to use delivery-test accounts as evidence in the event that further investigation is warranted with the provider. Senders should be able to provide an actual email message sent to that domain rather than forward a message sent to another provider.

e. When messaging disruption issues are identified, senders should:

   i. Investigate and identify the full extent of the disruption to IP addresses or domain names and potential content-specific causes.

   ii. Investigate the SMTP error logs to identify the specific return code associated with that disruption. According to RFC 3463, the error code in the text portion of the message for an Acceptable Use Policy violation is designated as 5.7.1.

   iii. Identify the most applicable email address or Web page for contacting the messaged-to entity in question.

      1. In many cases this is the postmaster@ISP or abuse@ISP email address (or) postmaster.ISP.com.

---

[10] For example, services such as Spamcop offer senders metrics on deliveries to spamtraps per day.

[11] For example, Microsoft offers senders access to its Smart Network Data Services portal detailing messaging metrics sent to MSN/Hotmail.

2. Senders are encouraged not to contact non-abuse or postmaster-related entities, such as the advertising, customer service or other corporate communications representatives, unless all other options are exhausted.

iv. Include the most specific IP addresses and domains in use and indicate the applicable recipient-specific SMTP error identification in the correspondence.

v. Be prepared to identify the specific source and date/time of subscription consent with recipient addresses in question.

f. Senders should be proactive and participate in relevant industry groups as well as list their own abuse-related contact information in any publicly accessible forum in the event that a provider or end-user wishes to contact them.

g. Senders should apply and use reporting services that track ISP abuse, feedback loops and junk email to proactively monitor and manage user complaint reports.

For technical or policy reasons, senders should recognize that Internet and Email Access Providers may provide little or no explanation for the reason why sender messaging is disrupted or how senders can mitigate future instances of this disruption from occurring. For more details on Internet and Email Access Provider policies, refer to the MAAWG Code of Conduct.

Appendix A: Commonly Used Definitions

IP Address
An IP address (Internet Protocol address) is a unique address that devices use in order to identify and communicate with each other on a computer network using the Internet Protocol standard (IP)—in simpler terms, a computer address. Any participating network device—including routers, computers, time-servers, printers, Internet fax machines, and some telephones—can have their own unique address. Also, many people can find personal information through IP addresses.

/24 Network
A 24 bit IP network with space for 254 hosts. A typical IP allocation set used by broadcast mailers.

Domain Name System (DNS)
The Domain Name System (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer host names) to IP addresses. It also lists mail exchange servers accepting email for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use.

RDNS
Reverse DNS lookup (rDNS) is a process to determine the host name associated with a given IP address. Typically, the DNS is used to determine what IP address is associated with a given host name; so to reverse resolve a known IP address is to lookup what the associated host name for it. A reverse lookup is often referred to simply as reverse resolving, or more specifically reverse DNS lookups. RFC 1912 says that all hosts on the Internet should have a valid rDNS entry.

RFC

In internetworking and computer network engineering, Request for Comments (RFC) documents are a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies. Through the Internet Society (ISOC), engineers and computer scientists may publish discourse in the form of an RFC memorandum, either for peer review or simply to convey new concepts, information, or (occasionally) engineering humor. The Internet Engineering Task Force (IETF) adopts some of the proposals published in RFCs as Internet standards.

WHOIS

WHOIS is a TCP-based query/response protocol which is widely used for querying a database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet. WHOIS lookups were traditionally made using a command line interface, but a number of simplified Web-based tools now exist for looking up domain ownership details from different databases. Web-based WHOIS clients still rely on the WHOIS protocol to connect to a WHOIS server and do lookups, and command-line WHOIS clients are still quite widely used by system administrators.

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is the *de facto* standard for email transmissions across the Internet. Formally SMTP is defined in RFC 821 (STD 10) as amended by RFC 1123 (STD 3) Chapter 5. The protocol used today is also known as ESMTP and defined in RFC 2821.

- EHLO: A client SMTP supporting SMTP service extensions should start an SMTP session by issuing the EHLO command instead of the HELO command. If the SMTP server supports the SMTP service extensions it will give a successful response, a failure response, or an error response.

- HELO: In the HELO command the host sending the command identifies itself; the command may be interpreted as saying "Hello, I am<domain>."

Fully Qualified Domain Name (FQDN)

A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: *somehost.example.com.* An FQDN differs from a regular domain name by its absoluteness; a suffix will not be added.

MX Record

An MX record or Mail exchanger record is a resource record in the Domain Name System (DNS) specifying how Internet email should be routed. MX records point to the servers to send an email to, and which ones it should be sent to first, by priority.

Delivery Status Notifcation/DSN (aka: Bounce)

An automated electronic mail message from the receiver's mail system, the message tells the sender that the message could not be delivered. The original message is said to have "bounced."

Appendix B: Email regulations by various regions

Australian Spam Act
http://www.comlaw.gov.au/Details/C2005C00382
Among other provisions, this act requires a subscription removal within five business days.

Canada's Anti-spam Law (CASL) / C-28
http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/page-1.html
Among other provisions, this act requires express or implied consent and that a subscription be removed within 10 days.

Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

CAUCE-Cornell Spam Law Inbox Project
http://www.inboxproject.org
A collection of materials related to anti-spam law

Europa

http://europa.eu/legislation_summaries/internal_market/single_market_services/l24120_en.htm
Summary of EU data protection legislation in the electronic communications sector

Europa Eur-Lex
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72002L0058:EN:NOT
EU national execution measures and provisions of member states concerning Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
http://uscode.house.gov/download/pls/15C103.txt
Among other provisions, this act requires subscription removal within ten business days.
The act also has provisions for express authorization when collecting wireless email addresses or suppression of wireless email domains: http://transition.fcc.gov/cgb/policy/canspam.html

Appendix C: Email Associations or Services with Sender Initiatives

Anti Phishing Working Group (APWG)
http://www.antiphishing.org

Canadian Marketing Association (CMA)
http://www.the-cma.org/

Direct Marketing Association (U.S.)
http://www.the-dma.org/index.php
http://www.emailexperience.org/

Federation of European Direct and Interactive Marketing (FEDMA)
http://www.fedma.org

Interactive Advertising Bureau (IAB)
http://www.iab.net/

Network Abuse Clearinghouse
http://www.abuse.net/

Online Trust Alliance (OTA)
https://otalliance.org/

TRUSTe
http://www.truste.org/

U.K. Direct Marketing Association
http://www.dma.org.uk/