MANUAL TRANSMITTAL

1.10.3

Department of the Treasury
Internal Revenue Service

NOVEMBER 17, 2016

EFFECTIVE DATE

(11-17-2016)

PURPOSE

(1) This transmits revised IRM 1.10.3, Office of the Commissioner of Internal Revenue, Standards for Using Email.

BACKGROUND

(1) This IRM provides guidelines for using email in the most effective and productive manner. It includes guidance on formatting messages in a way that will be easily accessible for all employees, including those using the Enterprise Remote Access System (ERAP). It also includes information on security guidelines, creation and use of distribution lists, and contacts for assistance with email issues.

MATERIAL CHANGES

(1) Text has been revised to clarify and update information including web site references.

EFFECT ON OTHER DOCUMENTS

IRM 1.10.3 dated November 12, 2015, is superseded.

AUDIENCE

All IRS employees

Terry Lemons
Director,
Office of Communications

1.10.3
Standards for Using Email

Table of Contents

1.10.3.1
(11-17-2016)
Introduction

(1) Email is now commonly used in business as an official form of communication, often replacing memorandums, meetings or phone conversations. This technology option is often the most efficient way to handle business communications and responsibilities. But its benefits can lead to burdens if we do not use this powerful tool judiciously. This section defines the standards for email use in Internal Revenue Service communications.

1.10.3.2
(11-17-2016)
Security/Privacy

(1) Email messages are official documents and should reflect this perspective. Email communications can be offered as evidence in court and can be legally binding. Before sending an email, you must consider how it reflects on the Service's image and take into account privacy, records management, and security factors.

(2) The privacy of email cannot be assured and is easily compromised. Messages can be forwarded to unintended recipients (sometimes outside the agency or even outside the government). The public we serve, or the Congress, who may have occasion to see an email message, do not differentiate between employees as individuals and our agency. We are the IRS.

(3) More information on the Service's email security policy is available at Cybersecurity's policy. Refer to the Electronic Mail (Email) Security section and the Privately Owned Email Accounts section of IRM 10.8.1

(4) No officer of employee of the IRS may use a personal email account to conduct any official business of the government. For details, see the interim guidance in PGLD-10-0616-0003. "Using IRS and Personal Email Accounts" (to be incorporated into the Email section of IRM IRM 10.5.1 *Privacy Policy*).

1.10.3.2.1
(11-17-2016)
Secure Messaging & Encryption

(1) The Internal Revenue Service processes Sensitive But Unclassified (SBU) information. The definition of SBU information is any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 United States Code (USC) Section 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction. See IRM 10.8.1, *Information Technology (It) Security, Policy and Guidance*, for guidance on Sensitive But Unclassified (SBU) information.

(2) Personally Identifiable Information (PII) is a specific type of sensitive information. PII includes the personal data of taxpayers, and also the personal information of employees, contractors, applicants and visitors to the IRS. Refer to the Personally Identifiable Information (PII) section of IRM 10.8.1 for additional PII guidance

(3) You should never consider email secure. Do not include taxpayer, SBU, or PII information in email messages or attachments unless you use IRS approved encryption technology.

(4) Use the Secure Enterprise Messaging System (SEMS, or "Secure Messaging") for sending Microsoft Outlook messages that contain SBU data. Secure Messaging enables you to digitally encrypt email messages and attachments for transmission among IRS email users including Criminal Investigation,, the Treasury Inspector General for Tax Administration (TIGTA), and Chief Counsel employees. In order for you to send a secure message through Outlook, both you and the recipient must have Secure Messaging installed. This allows au-

thorized employees to transmit SBU information to other authorized employees within the system once they have been enrolled and received training.

(5) Secure Messaging enrollment is an automated process for all LAN accounts with an Exchange mailbox in IRS. You can find the instructions for configuring the Outlook client to use the certificates at the Secure Enterprise Messaging Systems (SEMS) web site: *http://documentation.sems.enterprise.irs.gov/*.

(6) Alternatively, you may encrypt files to be e-mailed as attachments using the latest software provided by IT. Instructions are provided at *http://findit-mits.web.irs.gov/*.

(7) Do not send emails containing SBU data to taxpayers or their authorized representatives, even if requested, because of the risk of improper disclosure or exposure. Do not email SBU data to other external stakeholders, unless specifically authorized. For details, see the interim guidance on PGLD-10-0616-0003. “Using IRS and Personal Email Accounts” (to be incorporated into the Email section of IRM IRM 10.5.1 *Privacy Policy*).

1.10.3.2.2
(11-17-2016)
Suspicious Emails / “Phishing” /“Social Engineering”

(1) Individuals seeking to commit fraud or intending harm to the IRS or its employees often engage in a type of“social engineering,” called “phishing” wherein they use an alias and a seemingly innocuous cover story in order to gain the victim’s confidence and gather sensitive information. Such scammers may use email, and try to trick you into revealing your password, or personal information. If you receive a suspicious, bogus, or phishing email:

- Do not open any attachments
- Do not reply
- “Forward” the email to the electronic mailbox, (*phishing@irs.gov*)
- Delete the email after forwarding

For more information, see IRM 21.1.3 - Accounts Management and Compliance Services Operations.

1.10.3.2.3
(11-17-2016)
Emails as Possible Federal Records

(1) All federal employees and federal contractors are required by law to preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. Records must be properly stored and preserved, available for retrieval and subject to appropriate approved disposition schedules.

(2) The Federal Records Act applies to email records just as it does to records you create using other media. Emails are records when they are:

- Created or received in the transaction of agency business
- Appropriate for preservation as evidence of the government’s function and activities, or
- Valuable because of the information they contain

(3) If you create or receive email messages during the course of your daily work, you are responsible for ensuring that you manage them properly. The National Archives and Records Administration, in OMB M-12-18, notes that by December 31, 2016, federal agencies must manage all email records (both permanent and temporary) in an accessible electronic format. IRS offices must move or copy their record emails to a separate electronic recordkeeping system unless their system has the features specified in IRM IRM 1.15.6.6(2) that support records management and litigation requirements, including the

capability to identify, retrieve and retain the records for as long as they are needed. Some offices may need to print and file email records (along with related transmission and receipt data) if those offices still maintain paper recordkeeping systems (i.e. case files).

(4) An email determined to be a federal record may eventually be considered as having permanent, historical value by the National Archives. Therefore, ensure that all your communications are professional in tone.

1.10.3.2.4
(11-17-2016)
Emails are Subject to FOIA

(1) The public is aware of the role emails play in agency internal operations and emails are included in a growing number of Freedom of Information Act (FOIA) requests. Emails that are responsive to a FOIA request must be released unless the information contained in the email falls into one of nine very specific categories of exemptions. (See IRM 11.3.13 for more on FOIA processing). There is no category of exemption to protect the author or the Service from embarrassment.

(2) Emails provided in response to a FOIA must include the addressee, date and time. The address list, date and time are considered part of the record for both FOIA and record management purposes.

(3) Do not delete a message or attachment that is the subject of a congressional, Freedom of Information Act (FOIA), or discovery request or that is needed for litigation.

1.10.3.2.4.1
(11-17-2016)
Emails may be subject to electronic discovery

(1) Certain electronic records (like emails) may need to be identified and preserved when litigation is anticipated. In this case, you will be notified by your manager or Chief Counsel that relevant information must be preserved as part of the legal process. See IRM IRM 25.3.1.7 *Preserving Electronically Stored Information in Litigation Cases*, and Chief Counsel Directives Manual CCDM 34.7.1.1.4.

1.10.3.2.5
(11-17-2016)
Inappropriate Emails

(1) IRM IRM 10.8.27, *Information Technology (IT) Security, Internal Revenue Service Policy On Limited Personal Use Of Government Information Technology Resources*, defines the minimum standard for acceptable personal use of Government IT resources by IRS employees. The first exhibit, includes a summary of prohibited activities that includes creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings regardless of their subject matter.

(2) The Spam Protection section of IRM 10.8.1, states “Email spamming, sending or forwarding chain letters, other junk email, or inappropriate messages shall be prohibited.” In addition, the Electronic Mail (Email) Security section of IRM 10.8.1 states “Any use of IRS IT resources, including email, shall be made with the understanding that such use may not be secure, is not private, is not anonymous and may be subject to disclosure under FOIA.”

(3) If you receive an inappropriate email, please notify your immediate supervisor or your local Data Security Area. Do not forward it to your co-workers, friends or family, etc. You should delete the inappropriate email after notifying the proper authorities.

1.10.3.3
(11-17-2016)
Message Format

(1) Most IRS employees have access to email, but not everyone has the same email environment. Many employees work offsite and their email messages must go through the Enterprise Remote Access System (ERAP). A result is that these users often experience slower access and transmission. Email messages that IRS office workers download in fractions of seconds can often take longer for a field user. Additionally, graphics and stationery can't be read by adaptive equipment and can freeze the user's system.

(2) Unnecessary messages or excess volume of data within a message require time for the recipient to review and digest. Keep the reader's situation and need in mind at all times.

1.10.3.3.1
(11-17-2016)
Don't Slow Down the System

(1) To avoid slowing down transmission of information:

- Use Arial or another simple font on a plain background.
- Do not use animation, backgrounds, wallpapers, borders, graphics and photographs or any other graphic element as part of your stationery message format or signature. Exceptions will only be allowed for special IRS Commissioner initiatives.
- Refrain from sending large attachments to work groups or audiences. Remember every email message and any attachments, embedded graphics and photographs require a copy for each Exchange server store where each recipient's mailbox resides. Instead store the document on an IRS public web archive or SharePoint repository and insert a hyperlink into the message. Ensure the permissions allow access by all recipients prior to sending the message.

1.10.3.3.2
(11-17-2016)
Categorize Messages

(1) A meaningful subject line helps recipients prioritize their email. Categorize all email by type. Include only related information in a message. If there is another topic you wish to address, send it in a separate message. This makes it easier for the recipient to manage and respond to messages on different topics.

(2) Use the follow-up flag feature to identify items with required follow-up dates.

1.10.3.3.3
(11-17-2016)
Designate Priority

(1) Most email will be normal priority. Designate an email as high priority only if the receiver will need to act on the message immediately. If your message is truly urgent, consider trying to reach the recipient by phone or in person.

- "!" – High. Example – Computers will be down this weekend so overtime will not be scheduled and credit hours will not be approved. Example – We need volunteers for a task force in Washington that will convene in two weeks. Nominations are due this Friday.
- "blank" – Normal (the default)
- "down arrow"– Low. Example – The territory office of (another operating division) in another city has moved; its new address is…

1.10.3.3.4
(11-17-2016)
Designate Sensitivity

(1) Most email is of normal sensitivity. Messages designated as "private" or "confidential" should not be forwarded – but the system allows for this. Marking a message with one of these settings is advisory only. Recipients can take any actions on the message that they want to, such as forwarding the message to others.

(2) To designate sensitivity, from the "View" menu, select "Options" then select the appropriate designation.

- Private – Example: Communications with Labor Relations about an issue involving a particular employee.
- Confidential – Example: A proposal you are sharing with someone for their input, but which has not been shared with those who will approve or implement the procedures.
- Normal (default)

1.10.3.3.5
(11-17-2016)
Follow Guidelines of Email Common Sense and Etiquette

(1) To improve the effectiveness of email, follow these rules of etiquette and common sense guidelines:

a. Consider whether email is the best method for your communication. Sometimes, two-way dialogue by phone, Office Communicator or in person may be more effective. At other times, email may be best if you need written documentation.
b. Choose your recipients carefully. When selecting from the global address list, watch for duplicate names. If you frequently send messages to the same individuals, put them in your Personal Address Book. If two or more individuals have the same names, check the employees' properties in the Global Address List to ensure your intended recipient is the right person in the right location.
c. Do not use a distribution list (as a convenience to you) unless your message is appropriate for everyone on that list.
d. Use the subject line to categorize messages. Do not include any confidential or sensitive information in the subject line.
e. Forward messages only when necessary. Do not forward to people who have already received the message. Example: Do not resend Commissioner All-Employee messages.
f. Be concise.
g. Review your messages for accuracy in content, spelling, and punctuation. Hint: Set auto spell check to check all messages before sending and review any changes made .
h. If you say that a file is attached, attach it. Hint: attach the file before you compose the message.
i. Insert hypertext links to large documents stored on IRS document repositories.
j. Maintain your Inbox.
k. Respond promptly to messages.
l. Routinely purge your mailbox of purely personal messages and work-related non-record emails. Non-record messages include communications to all employees (i.e., IRS Headlines electronic newsletter), and information/reference email and word processing files received "for your information" or as a carbon copy (CC) in which you were not expected to and on which you did not take action.
m. Use the "To" address line for the primary recipient.
n. Use the carbon copy "cc" and blind carbon copy "bcc" features appropriately. Avoid copying people who do not need to see your message. In an internal office environment, it is rarely appropriate to use the "bcc" feature.
o. Use "Reply to all" only if all the original recipients ***need*** to know your response. Otherwise, reply only to the sender.
p. Never use "Reply to all" when you receive an email as a member of a large geographic or servicewide distribution list.

q. Use conversational grammar.
r. Do not use all caps or all lower case. Use punctuation.
s. Use the “out of office assistant” or “ auto forward” features when you will be out of the office for an extended time.
t. If you receive any messages with a known or suspected virus, delete them immediately and report the matter appropriately .
u. Avoid background, stationery or graphics.
v. Use a simple font and font size that is easily readable. For example, 12 point Arial is generally easy to read.
w. To accommodate those with visual impairments, select font and background colors that provide sufficient contrast and avoid unusual color combinations. For example, use the default font color (usually black or blue) rather than selecting red or green, use the default background color rather than selecting a background color and do not use the text highlighting feature.
x. Help prevent unnecessary email by telling recipients when your message does not require a reply.
y. Manage your email more effectively by using Outlook features such as voting buttons and invitation options. It will be easier for recipients to respond and easier to manage and track the results.

1.10.3.3.6 (11-17-2016) **Limit Size of Attachments**

(1) Large attachments can degrade overall system efficiency, so you should limit the transmission of large files as email attachments whenever possible.

(2) Consider alternatives for attachments larger than 10MB:

If ...	**Then ...**
“Attachment” has widespread impact and a shelf life	• Have it posted to your organization’s intranet site for retrieval, and • Include the hyperlink in the email message. • -or- • Save it to your shared directory or SharePoint site, and • Include file and path name in the email message.
“Attachment” does not have widespread impact and/or a shelf life	• Zip large files for faster transmission. • Eliminate official IRS seal from memos. • If possible, remove graphics, borders, pictures and non-standard fonts.

If ...	Then ...
"Attachment" is a large graphic presentation (i.e., PowerPoint, screen shots, scanned documents)	• Send it only to people who need to use or see the actual file. • Convert the information to a text file for those who only need the information. • Zip the file. • Have it posted to your organization's intranet site and email the hyperlink.

(3) If you are responding with an attachment, use "Forward " instead of "Reply" because attachments do not stay with replies.

(4) If you want to save the email message but do not need the attachment, follow these instructions:

- Open the message,
- Right click the attachment icon, and
- Select **remove** from the menu.
- Close file. Select "yes" at the "Do you want to Save changes?" prompt.

This will also save disk space.

1.10.3.3.7
(11-17-2016)
Malicious Attachments

(1) Ensure attachments are safe from viruses. Open attachments only if you trust the source and are expecting the attached file. Because of the impact the spreading of worms and viruses have on the IRS network, the Enterprise Messaging System is now configured to block all files with particular extension. If a file is sent via email with certain extensions (such as .exe, .vbs and .lnk), the message will be deleted without delivery.

(2) A number of virus variants try to bypass the IRS virus scanning software by including their damaging payload within a .zip file. Be cautious with any message you receive containing an attachment with a .zip file extension, and only unzip the file only if you trust the source.

(3) When you receive an email message with an attachment, save both the email and the attachment to a hard drive or network drive as soon as possible and remove the message and attachment from your mailbox. You free up space on your server by doing so.

1.10.3.4
(11-17-2016)
Using and Creating Distribution Lists

(1) Distribution groups/lists are a convenience when messages need to be sent to a large defined group. They allow users to send email messages to each individual on the list without selecting individual names. However, you should use them judiciously.

1.10.3.4.1
(11-17-2016)
Personal Distribution Lists

(1) Personal distribution lists are created by an individual user. Use your Outlook Help feature, keyword: personal distribution list, for instructions on creating and sharing personal lists.

1.10.3.4.2
(11-17-2016)
Global Distribution Lists

(1) IT and the SEMS staff can create global distribution lists for groups of practically any size and for any situation. These distribution lists are available for use from the global address list on Outlook. The list owner determines who will be authorized to use the list.

(2) There are several different types of global distribution lists.

Location specific	Considered local in scope, these lists contain members from a local site. For example, functional coordinators within a service center campus.
Special needs	Cross multiple organization boundaries and are often created for temporary groups, such as task forces.
Large lists	Contain more than 100 members and require specific set up and delivery restrictions. The AWSS all employee list (&AWSS Employees) is an example. ***Note:*** The use of large global lists should be confined to those who have a business need to communicate with the list. Examples include messages sent by IT to alert users of systems related issues or distribution of other approved servicewide communications tools such as *IRS headlines* or *Leaders' Alert.*
Lists created from a database	Membership for these lists is determined by specifying certain criteria within a database (such as TAPS or TIMIS) and populating the list with names meeting the criteria. Changes to membership cannot be made directly to the list, but must be made to information contained in the database. The SB/SE all-employee list (&SBSE All) is an example.

1.10.3.4.3
(11-17-2016)
Using Global Lists

(1) Before using a global distribution list to send an email message that requires follow-up actions or commitment of resources by recipients outside of your division, always discuss the requirement with the applicable Division Commissioner's office.

1.10.3.4.4
(11-17-2016)
Requesting a Global Distribution List

(1) Contact OSGetServices (1-866-743-5748) or TDD/TTY: 1-866-435-7486 to request creation of a new global distribution list (DL). You will need to provide the following information :

- Business need justification
- Scope – to whom it applies
- Anticipated "shelf life" of DL
- Name and number of the individual charged with maintaining the DL
- Proposed list of initial DL members
- If the list is automated, the conditional criteria of the members

Note: Distribution group/list names must be pre-approved by the designated business unit point of contact prior to opening the ITAMS ticket.

1.10.3.4.5
(11-17-2016)
Managing a List

(1) Distribution group/list managers can find information on modifying a list in the SEMS Documentation Library online at *http://documentation.sems.enterprise.irs.gov/*.

1.10.3.5
(11-17-2016)
Messages Intended for All Employees

(1) The IRS has the capability to send email messages to all employees; however this method of communication should be used sparingly. If you have a message you believe should be communicated servicewide, contact your business unit's communication office.

1.10.3.5.1
(11-17-2016)
IRS Headlines

(1) Generally, information requiring communication to all employees is distributed via the*IRS Headlines* electronic newsletter. The C&L Internal Communications (IC) branch distributes *IRS Headlines* every Monday using the all-employee global distribution list. Content for *IRS Headlines* should contain information relevant to a cross-section of IRS managers and employees. Examples of items found in IRS Headlines are those that include:

- Deadlines
- Action Items
- Strategic priorities and
- Employee accomplishments

(2) If you think you have information appropriate for *IRS Headlines*, you should take the following steps:

a. Originator discusses topic and schedule with the business unit's communication office. (If none, contact IC directly *http://irweb.irs.gov/AboutIRS/bu/cl/cldir/9296.aspx*.)
b. Business unit communicator discusses topic and schedule with the IC liaison for that business unit.
c. IC determines whether the topic is appropriate for *IRS Headlines*.
d. Originator and business unit communicator draft message and submit it to IC.
e. IC will provide editorial feedback on content, length, tone, and key messages.
f. IC will schedule article for publication in the *IRS Headlines* electronic newsletter.
g. IC will suggest ways to incorporate message into other internal communications products, when appropriate.

1.10.3.5.2
(11-17-2016)
Special All-Employee Emails

(1) On rare occasions, special circumstances may require the issuance of an all-employee email separate from *IRS Headlines … and more*. Any message submitted for distribution as an all-employee email will be subject to a stringent review process. The communications manager in your business unit is your initial point of contact when deciding whether to start the process of creating an all-employee email.

(2) When submitting a message for distribution to all employees, you must provide the following information:

- Significance to employees (Is there something they must know immediately to do their jobs correctly, to comply with the law, to prevent a systems failure, etc.?)
- Reason for extreme time sensitivity (Why is this information so critical to employees that it cannot wait for inclusion in the next edition of *Headlines*?)
- Necessity of email delivery instead of *Headlines* or other method (Why does this information have to be sent via a special email? Why wouldn't IRWeb (intranet) or *Headlines* be more appropriate ?)
- Desired outcome (What immediate action do you want employees to take?)
- Business objective

(3) The C&L Internal Communication Branch will determine the best method of communicating the message based on the information submitted.

1.10.3.6
(11-17-2016)
Assistance with Email Issues

(1) Use the following table to determine where to get assistance with email issues.

Topic	Resource
Security Concerns	Immediately contact the Computer Security Incident Response Center (CSIRC) at *http://www.csirc.web.irs.gov/* Email: csirc@csirc.irs.gov (866) 216-4809 (toll-free) (202) 283-4809 (local) (202) 283-0345 (FAX)
Technical problems w/Outlook	Submit OS GetServices ticket online at *http://getservices.web.irs.gov/*or by phone: 1-866-743-5748 or TDD/TTY: 1-866-435-7486.
Creating or changing criteria for an Automated Distribution Group/List (Requires an ITAMS ticket)	Contact OS GetServices online at *http://getservices.web.irs.gov/*or by phone: at 1-866-743-5748 or TDD/TTY: 1-866-435-7486.
SPAM issues	**DO NOT** open email; forward questionable email to **SPAM* with *"*Possible SPAM*"* in subject line. For additional information, take the Anti-SPAM Procedures link contained in the IT Navigation Guide.
Phishing/ Social Engineering issues	Do not open any attachments: do not reply: "forward" the email to the electronic mailbox, (phishing@irs.gov). Delete the email after forwarding. For more information, see IRM IRM 21.1.3, *Accounts Management and Compliance Services Operations*.

Topic	Resource
Email Maintenance and retention questions	Contact the Records and Information Management (RIM) Program Office at *Records Management

This Page Intentionally Left Blank

Exhibit 1.10.3-1 (11-17-2016)
Reducing the Size of Your Mailbox

The Secure Enterprise Messaging system (SEMS) establishes a standard size of 500 MB (500 megabytes) for individual mailboxes. The system mails you daily warning messages that the limit is being approached when your mailbox reaches a size of 475 MB. When it exceeds the 500 MB limit, you will receive the following warning each time you attempt to send a message:

- "You have exceeded your storage limit on your mailbox ".
- Inventory email to identify personal messages, work-related non-record messages and those email messages that meet the definition of a federal record (see IRM IRM 1.10.3.2.3 above). Delete personal and non-record messages no longer needed. Email messages identified as federal records must be handled in accordance with their NARA-approved disposition schedule and kept in an approved recordkeeping system (electronic or paper). To identify the appropriate disposition, consult the Records Control Schedules Documents 12829 and 12990 or contact the IRS Records Office at *Records Management.

It is not the practice of the SEMS staff to adjust any individual mailbox storage limits, but rather to provide guidance on reducing the size of the contents. The Outlook Help menu provides instructions for enabling and configuring both Auto-archiving and Rules to manage mail and mailbox folders to maintain proper storage limits.

Exhibit 1.10.3-2 (11-17-2016)
Postscript/Signature

Your email signature section should include only the identifying information that would otherwise be included in any official IRS communication (i.e. business card, memorandum, letter, etc.):

- Name
- Title
- Organization
- Street/email address
- Telephone/fax numbers

Refrain from including quotes or other personal messages as part of the signature section.

Follow these steps to create an automatic signature in Outlook:

- Select “Options” from the “Tools” menu. Choose the “mail format” tab. Use the “ Signatures” section at the bottom to create your personal signature line.

Please note: Consistent with IRM 10.8.26.3.4 , *Configuration Management*, if you’re using a mobile computing device with an email auto-signature capability, **configure it so that it does not disclose** that the email originated from a smartphone or mobile computing device (e.g., do not have it show “Sent From My Wireless Handheld”).

The following signature line is recommended using 12pt Arial or Helvetica for the PC and 14pt for the Mac, all flush left:

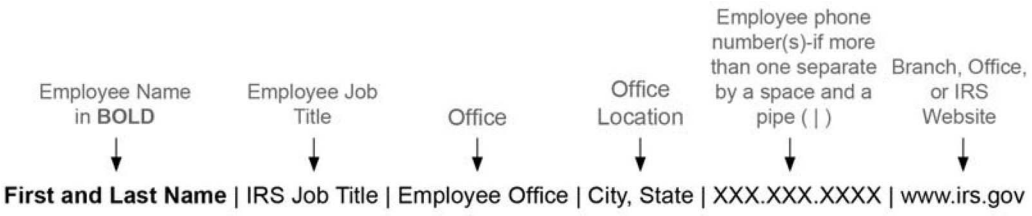

Figure 1.10.3-1

Examples of signature lines:

a. **John Doe** | Distribution Analyst | IRS Human Capital Office | 555.555.5555 | Atlanta, GA | hco.web.irs.gov/
b. **Jane Doe** | IRS Revenue Agent | Office of Examination | desk: 555.555.5555 | cell: 555.555.5555 | fax: 555.555.5555 | Boston, MA | AWS Friday | www.irs.gov