PRIVACY, GOVERNMENTAL LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 05-16-2025

Control Number: PGLD-10-0525-0005
Expiration Date: 05-16-2027
Affected IRM(s): 10.5.1,1.10.3, 10.8.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: John K. Hardman */s/ John K. Hardman*
Director, Privacy Policy and Compliance

SUBJECT: Interim Guidance on SBU Data in Internal Email Subject Line

This memorandum issues interim guidance on including SBU (sensitive but unclassified) data in the subject line of internal email until the next publication of IRM 10.5.1 and is effective as of May 16, 2025. Please distribute this information to all affected personnel within your organization.

Purpose: This interim guidance clarifies privacy policy on the use of SBU data in the subject line of an internal email.

Background/Source(s) of Authority: This interim guidance falls under the authorities listed in IRM 10.5.1.1.6, Authority.

Procedural Change: The procedural changes in the attached interim guidance apply.

Effect on Other Documents: We will incorporate this interim guidance into IRM 10.5.1, Privacy Policy, by May 16, 2027. Authors of affected IRMs will incorporate likewise.

Effective Date: May 16, 2025
Contact: If you have any questions, please email the Associate Director, Privacy Policy, at *Privacy.

Distribution: FOIA Library (external) on IRS.gov

Attachment: PGLD-10-0515-0005
Attachment Interim Guidance: PGLD-10-0515-0005

The following changes take effect May 16, 2025**, for** IRM 10.5.1.

This memorandum uses ellipses (**…**) to show existing policy not changed and only shows the paragraphs with changes.

IRM 10.5.1.6.8
(05-08-2025)
Email and Other Electronic Communications

…

(6) When authorized to email SBU data, encrypt SBU data in emails using IRS IT-approved encryption referenced in paragraph (7) ~~technology~~. Review IRM 10.5.1.6.2, Encryption, and IRM 10.8.1.4.19.2.1, Electronic Mail (Email) Security. For external emails, do not include SBU data (including PII or tax information, such as the name control) in the email subject line, even if encrypted. ***For internal emails only***, you may include SBU data in the subject line, as the internal network protects the data on an encrypted platform.

Caution: For external emails, encryption methods do not encrypt the subject line or the header (email address information).

Note: Review IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives, for external email subject line and header requirements.

(7) Examples of IRS IT-approved encryption ~~technology~~ include:

Internal (within the IRS network)	External (outside the IRS network)
Secure email encryption using the Encrypt-Only option. ~~This encrypts the body of the email and attachments in transit.~~	• **Strongly recommended**: Use IRS secure alternatives to email. ~~For IRS secure alternatives to email, r~~ Review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. ~~For more information about when you can offer these alternatives, refer to your business unit procedures.~~ • **If alternatives are not available**: Secure email encryption using the Encrypt-Only option. This encrypts the body of the email and attachments in transit. **Reminder:** For external emails, this encryption protects only the body of the email and attachments in transit, not the subject line. Do not put SBU data in the subject line of external emails.

…

10.5.1.6.8.3
(05-08-2025)
Emails to IRS Accounts

(1) IRS personnel must use IRS email for email communications with other IRS personnel about official business matters. They must encrypt all internal email messages with SBU data (including PII and tax information) using IT-approved encryption.
Note: ***For internal emails only***, you may include SBU data in the subject line, as the internal network protects the data on an encrypted platform.
Caution: ~~Encryption methods do not encrypt the subject line or the header (email address information).~~

(2) For contractors, when provided with an IRS workstation as part of a contract, they must use their IRS workstation and account for all official communication (such as email or instant messaging). Refer to IRM 10.8.2.3.1.18, Contractor.

10.5.1.6.8.5
(05-08-2025)
Limited Exceptions to Email SBU Data Encryption

(1) **…**
(2) After evaluating business needs with potential risk, refer to the following limited exceptions for encryption in external emails. You must encrypt any SBU data with IT-approved encryption beyond these exceptions. Review IRM 10.5.1.6.2, Encryption.
Caution: Do not include SBU data ~~(including PII or tax information)~~, such as the name control, in the external email subject line. Encryption methods do not encrypt the subject line or the header (email address information) of external email.

Limited exception	Requirements
Subject line of case-related emails to the Department of Justice	a. … b. … c. If the body of an email or any attachment has other SBU data, you ~~IRS personnel~~ must encrypt ~~both~~ the email ~~and attachment using IT-approved technology~~.
…	**…**
IRS employees sending their personal SBU data via ~~IT-approved~~ encrypted email. …	a. You may choose to send your personal SBU data outside the IRS via encrypted email ~~or a password-protected encrypted attachment~~. b. … c. … d. …

…	…
Subject line of Taxpayer Advocate Service (TAS) case-related emails to Congress	a. This temporary limited exception allows the subject line to include the TAMIS (Taxpayer Advocate Management Information System) case or OAR (Operations Assistance Request(s)) number for TAS case-related emails with authorized, authenticated Congressional representatives who have an authorized need to know. This temporary exception will be valid for 12 months, or until TAS has implemented an alternative to external email communication, whichever comes first. b. If the body of an email or any attachment has other SBU data, you must encrypt the email.

10.5.1.6.8.6
(05-08-2025)
Other Secure Electronic Communication Methods

(1) For secure external communication, we strongly recommend using IRS secure alternatives to email to protect privacy and security. Review IRM 10.5.1.6.8, Email and Other Electronic Communications. These alternatives include: ~~The IRS offers some alternatives to email to protect taxpayer security and privacy:~~

Alternative	Description
Secure Messaging platform (formerly Taxpayer Digital Communication (TDC))	Taxpayers must register, so they can then send and receive messages on an encrypted platform. For the internal login page, refer to the internal Secure Messaging site.
Document Upload Tool (DUT)	The IRS initiates access to the tool by providing the link and, in some cases, a unique access code or ID, through a notice, phone conversation or in-person visit. This is a one-way (public to IRS) encrypted communication. Refer to the IRS Document Upload Tool (external) site.
Secure Large File Transfer (SLFT)	Hosted by Kiteworks, use this for large file transfer, with proper authentication and authorization. For more information, refer to the internal Secure Large File Transfer (SLFT) site.

Exception: Not everyone has access to these alternatives, but those who need to communicate with taxpayers do. They are available only for programs with approved business requirements and have deployed them.

(2) These examples of IRS-approved alternatives to email might not be your only options as technology evolves. Check with your business unit for other secure external communication methods.