INDEPENDENT OFFICE
OF APPEALS

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 26, 2024

Control No. AP-08-0824-0017
Expiration Date: 8/26/2026
Affected IRMs: IRM 8.6.1, 8.24.1

MEMORANDUM FOR ALL IRS INDEPENDENT OFFICE OF APPEALS EMPLOYEES

FROM: Patrick E. McGuire */S/ Patrick E. McGuire*
Acting Director, Case and Operations Support

SUBJECT: Revised Procedures for Secure Messaging

This memorandum revises procedures for Secure Messaging in the IRS Independent Office of Appeals (Appeals) and supersedes interim guidance (IG) AP-08-0622-0008, Taxpayer Digital Communications – Mandatory Requirement to Offer Secure Messaging, dated June 29, 2022. Please ensure this information is distributed to all affected employees within your organization.

Purpose: This memorandum changes the terminology used for secure messaging in Appeals and provides updated secure messaging guidance to Appeals Employees.

Background: Previously, Appeals referred to its secure messaging platform as TDC Secure Messaging (TDC SM). Per guidance from the Office of Online Services, Appeals will now refer to its secure messaging platform as Secure Messaging. All future guidance, training materials, job aids and communications will refer to secure messaging used in Appeals as Secure Messaging and will no longer use the terms Taxpayer Digital Communications (TDC) or Taxpayer Digital Communications Secure Messaging (TDC SM) to describe Appeals' current secure messaging platform.

During the initial pilot for secure messaging, Feature Code DC was used to identify cases where secure messaging was offered to taxpayers. In June 2022, Appeals began offering Secure Messaging to all taxpayers so Feature Code DC is no longer necessary or required.

CARATS (Case Activity Record and Automated Timekeeping System) Action Code CO-TDC was previously required for each interaction through Secure Messaging. There is no longer a need to record each interaction using CO-TDC. Appeals Technical Employees (ATEs) will record the first communication through Secure

Messaging using CO-TDC and will record further communications using other applicable CARATS codes.

Prior guidance included instructions for ATEs to add Secure Messaging information to initial contact letters. In April 2023, we revised all initial contact letters used by Appeals to include an invitation to use Secure Messaging. It is no longer necessary to add this information to the contact letters.

Procedural Change: See attachment for updated Secure Messaging procedures.

Effect on Other Documents: This guidance will be incorporated into IRM 8.6.1, Conference and Issue Resolution, within two years from the date of this memo. IRM 8.24.1 will cross-reference IRM 8.6.1 regarding this guidance. This memorandum supersedes interim guidance (IG) AP-08-0622-0008, Taxpayer Digital Communications – Mandatory Requirement to Offer Secure Messaging, dated June 29, 2022.

Effective Date: This guidance is effective as of the date of this memorandum.

Contact: Appeals employees can visit the Secure Messaging page on the Appeals website, or follow existing procedures to elevate questions through their management chain and follow established procedures on How to Contact an Analyst.

Attachment:
Procedural Changes

Distribution:
cc: www.irs.gov

8.6.1.4.X (new)
Using Secure Messaging to Communicate

(1) Secure Messaging provides a secure platform where taxpayers or their representatives can digitally exchange messages and documents with Appeals.

(2) All Appeals managers and technical employees in IR and GS job series 0930, 0110, 1101, 0512, 0526 and 0801 who interact with taxpayers and their representatives must:

- request and maintain access to Secure Messaging
- complete the Secure Messaging User Training courses (supervisors will also complete the Supervisor Secure Messaging Training courses)
- provide their unique Secure Messaging identifier (eGain number) to taxpayers and representatives who wish to communicate about their open Appeals case through Secure Messaging
- timely respond to communications received through Secure Messaging

See the Secure Messaging page on the Appeals website for access instructions and training information.

(3) Taxpayers and representatives requesting to use secure messaging will visit www.irs.gov/connect to authenticate their identity, access secure messaging, and initiate communications with the Appeals employee. You may refer taxpayers to help.id.me for assistance with registration or login issues.

(4) Users will receive a notification email each time they receive a message through Secure Messaging.

8.6.1.4.X.1
ATE Case Actions for Secure Messaging

(1) ATEs must offer secure messaging to taxpayers in their initial contact with taxpayers in every case.

(a) If you make initial contact by correspondence, use one of the initial contact letters specified in IRM 8.6.1. Each of these letters includes an invitation to Secure Messaging.

(b) If you make initial contact by telephone, invite the taxpayer to use Secure Messaging during the call and document this in the case activity record (CAR). Review Publication 5437 with the taxpayer or representative, direct them to www.irs.gov/forms-instructions, or send the publication by fax or mail if necessary.

(c) If your initial telephone contact fully resolves the case and eliminates the need for any further contact, you do not need to offer Secure Messaging but must clearly document the reason in the Case Activity Record (CAR).

(2) If the taxpayer or representative requests to use Secure Messaging, provide your eGain number to them and direct them to www.irs.gov/connect to register.

(3) If the taxpayer or representative initiates communication with you through Secure Messaging, document the date of this initial communication in the CAR using CARATS code CO-TDC. Record further communications through Secure Messaging using other applicable CARATS codes.

(4) If the taxpayer or representative requests to discontinue communications with Appeals through Secure Messaging, document the date of this request in the CAR using CARATS code CO-TDW.

(5) When the taxpayer or representative requests access to the case file per the Taxpayer First Act (TFA), and you've all agreed that Secure Messaging is the best delivery method for the case file, follow IG Memorandum AP-08-0624-0011, Revised Guidance for Taxpayer First Act (TFA) Access to Case Files, and complete the following actions:

(a) Upload a signed, undated transmittal Letter 6271 to ACDS, addressed to the individual (taxpayer or representative) who requested access before submitting the STARS request. STARS will date this letter and update it to include the STARS Request ID number. Letter 6270 is not necessary because documents sent through Secure Messaging do not require password protection.

(b) Complete a Shared Team of Administrative and Redaction Support (STARS) request according to the TFA File Request instructions in the request guide. In the request, indicate the delivery method as "Secure Messaging (If chosen, requestor will send via Secure Messaging when request is completed)."

(c) Attach a completed TFA File Request to the STARS Service Request before submitting the request to STARS.

(d) Once the redactor uploads the redacted case file and Letter 6271 in ACDS, send Letter 6271, along with the redacted case file via Secure Messaging to the taxpayer or representative. If necessary, edit the date on Letter 6271 to the date you send it through Secure Messaging.

(6) If you're using Secure Messaging with a taxpayer's representative whose power of attorney is revoked or withdrawn, follow the POA Revocation Instructions to remove

the representative's access to messages related to the taxpayer. These instructions are found on the Secure Messaging page on the Appeals website.

(7) For certain BMF entities, whose case originated in LB&I, TEGE or Art Appraisal services, BSP can create a customer group mailbox in Secure Messaging, allowing access to multiple authorized individuals. See the Secure Messaging page on the Appeals website for information on this.

(8) Prior to submitting the case to your manager for closing, save a pdf copy of all communication that has taken place through Secure Messaging and attach it to the case in ACDS, then close the case in Secure Messaging. See the training materials or SHOTs videos on the Secure Messaging page for additional instructions.