Overview

The industry, state and IRS partners recognize that even though fraudulent filings will still occur, we all must be proactive and take steps to reduce or prevent the fraud. In 2014, a group of state and industry partners working together developed a set of minimum measures for tax software developers, especially in the online "do it yourself" ("DIY") market, to reduce the risk of account takeovers and other forms of cyber fraud. These measures were largely adapted from the National Institute of Standards & Technology ("NIST") publication 800-53, on which then-current IRS Safeguards standards were based. The minimum measures were also patterned after the "Know Your Customer" efforts then underway in online banking applications.

Since that first Trusted Customer effort, two key events have happened. First, the Security Summit, a cooperative effort of IRS, state tax and revenue agencies, and significant industry partners was convened by IRS. The Trusted Customer Requirements became a joint effort of the Authentication and STAR (Strategice Threat Analysis & Response) working groups of the Summit, guided by authentication and cybersecurity experts from the Summit members.

Secondly, as technology advanced and cyberattacks grew more sophisticated, NIST published document 800-63B, Digital Identity Guidelines, recommending more rigorous authentication standards. As a result, the Summit working groups have published a three-year roadmap to move Trusted Customer Requirements to the NIST Authenticator Assurance Level 2 (AAL2), which provides high confidence that the claimant controls authenticator(s) bound to the taxpayer's account. Summit industry partners are required to progress along this roadmap; all industry partners are encouraged to do so.

This current Trusted Customer document is therefore transitional. It restates the original minimum measures as an absolute baseline for DIY software security. However, it adds the current requirements for movement towards AAL2 that are required for all Summit partners and will at some point be required for all industry partners. These requirements will be incorporated into agency e-filing agreements for certification and will be verified by optional post-launch reviews.

Trusted customer is meant to serve as a baseline authentication standard and to continue to evolve as we progress along the NIST implementation timeline. In light of this consideration, any solution that meets or exceeds AAL2 will be exempt from the minimum requirements if the measure described is no longer utilized. To preserve innovation and creativity, Industry partners may choose to, and are encouraged to, exceed the standards established and conduct their own independent and unique analysis, based on patterns or trends they observe and identify. These requirements will be reviewed and strengthened as appropriate by July of each year, following the roadmap and/or new developments in authentication standards and best practices.

Do-It-Yourself (DIY) Audiences

Establishing a trusted customer requirement for the do-it-yourself audiences is an important step in building a robust tax filing system that:

- Follows nationally recognized standards for implementing identity authentication
- Ensures consistent minimum requirements are established for industry to efficiently support multiple tax agencies
- Mitigates the potential for account takeovers
- Reduces the opportunity for fraudulent return filing
- Establishes a process to verify identity in future interactions including account recovery
- Enhances security / protection measures for taxpayer confidential and sensitive information
- Increases the public confidence and trust in the tax filing system

It is understood that "DIY" includes off the shelf desktop software as well as online environments. The original Trusted Customer Requirements were designed especially for those environments:

- When the data is stored electronically online or
- When the customer establishes an online account.

Multi-Factor Authentication (MFA):

MFA is at the heart of both the minimum requirements and the AAL2 specifications. For the purpose of authentication, a "factor" is either:

a. Something you know (such as a password).
b. Something you have (such as a mobile device or a token), or
c. Something you are (such as a fingerprint or facial scan).

Requiring the use of multiple factors to authenticate the filer, especially if one or more factors must be in the actual taxpayer's possession, reduces the risk of an account takeover by a remote party. NIST 800-63B further categorizes specific factors into "restricted" factors and "unrestricted" factors which are more secure, and gives examples. Additionally, guidelines are provided below from NIST 800-53 or 63B to ensure that passwords, security questions, and other factors are deployed as securely as possible.

Out of Band (OOB) Verification:

The term "Out of Band," introduced in the original Trusted Customer minimum requirements, refers to a specific type of two-factor authentication where both of the factors are different communications channels. The online session between the filer and the tax software is considered the primary band for the efiling. The OOB requirement in the original Trusted Customer Requirements called for the software to authenticate the filer by contact through a separate channel outside of the efile band, such as a separate email service or a text to a mobile device. Out-of-band verification is accomplished by sending an email or text to the customer with a PIN or a link that includes a randomly generated PIN. The customer enters the PIN through a user interface or clicks on the link that provides a PIN back to the application. The

PIN is validated through the software before allowing the customer to continue with the efile process.

The new NIST 800-63B guidelines does not consider email to be an unrestricted factor. This current document strongly discourages the use of email as a primary authentication factor, and it cannot be used to meet the 2019-2020 Summit requirement to offer an unrestricted factor for authentication. Please see NIST publication 800-63B for guidelines and cautions for using SMS text over a public mobile telephone network for out-of-band verification.

NIST 800-63B STANDARD PROGRAMMING FOR PROCESSING YEAR 2020

The Objectives for incorporating NIST 800-63B Standards are to strengthen the current authentication procedures to provide a more secure login for customers. It will be critical to track and pass an indicator on the MeF and State Schemas to identify all customers who opted into the additional authentication factor and provide industry feedback based on an analysis of these fields.
Year two requires industry to offer at least **one** unrestricted authentication factor for MFA:

- **Account Creation**:
  - Leverage the existing authentication infrastructure and **include at least one unrestricted authentication factor** (e.g., PIN, secret grid, printed secret grid) for **client opt-in.**
- **Account Recovery:**
  - Reduce reliance on email account recovery and expand use of recovery through **unrestricted** and **restricted AAL options**.

See Appendix for NIST 800-63B AAL2 – Examples of Unrestricted Authentication Factors
The full NIST 800-63-B: https://csrc.nist.gov/publications/detail/sp/800-63b/final

New Customer Standard

Minimum Trusted Customer requirements for DIY efile software providers include the following measures for a first-time filer using the software:

I. Implement BOT detection technology and other security requirements in accordance with the IRS requirements in Pub 1345 to implement an effective challenge-response protocol (e.g. including requiring customers to pass Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to protect their Web site against malicious bots.

II. Username – no specific format requirement

1. Include helpful tips – such as do not use email address, SSN, First and Last Name, etc.
2. Disable the ability for the customer to automatically use the email address as a username.

III. Password

Through the use of strong passwords and locking out an account after multiple consecutive failed attempts, the goal is to mitigate password guessing and brute force attacks. These standards also meet the IRS Publication 1075: Safeguards for Protecting Federal Tax Returns and Return Information requirements. Note that these password restrictions no longer apply once AAL2 level authentication is implemented.

1. All customers are required to use a strong password (at least 8 characters, upper, lower case, digit and special char) as an important step for protecting their identity
2. Implement a 15 minute interval after lockout feature with no more than 10 unsuccessful login attempts
3. At least 8 characters
    - Including **all** of the following:
        - At least 1 uppercase letter (A-Z)
        - At least 1 lowercase letter (a-z)
        - At least 1 number (0-9)
        - At least 1 special character (punctuation)

IV. The original Trusted Customer minimum requirements state that if the out-of-band is unsuccessful, three security questions that must be answered within 1 minute per question (with the assumption that the website is ADA compliant). The following three sources of questions are available for industry to choose from.

1. Random third-party security questions
2. Question established by industry and answered by customer
    a. Do not use questions that have readily available answers
    b. Do not use questions that have answers that are shared with others or are available to others
3. Question and answer provided by the customer in a previous online session.

As part of the move to AAL2, the use of security questions is now discouraged and is being phased out, similar to the use of email.

V. Customer is requested to enter an email address to be used for future communication regarding the return, even if email was not utilized as an authentication factor.

VI. Customer is encouraged to enter a cell phone number, and it is required if the cell phone is used in out-of-band or other MFA.

VII. Identity Proofing protocol

1. The content of the Authentication Summary data element communicates the level of identity proofing and/or authenticaion completed as defined in the IRS and state schema. The requirements are available to all parties (industry, states and IRS).

2. Email Address Verification (see Filing Expectations) Note that NIST 800-63B discourages the use of email for authentication purposes.
   1. Out-of-band verification is required.
   2. If the customer does not complete the out-of-band, the industry partner must make their best effort to verify the email address.

   3. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.

Returning Customer Standard

For Processing Year 2020, Industry will:

- Require all returning customers to use a strong password (at least 8 characters, upper, lower case, digit and special char) and must be given the opportunity to change their password as an important step for protecting their identity;
- Implement a 15 minute interval after lockout feature with no more than 10 unsuccessful login attempts;
- Ensure that the customer has previously entered an email address;
- Ensure that the customer is encouraged to add a cell phone entry, required if the cell phone is utilized for out-of-band or other form of MFA.
- Implement BOT detection technology and other security requirements in accordance with the IRS requirements in Pub 1345 to implement an effective challenge-response protocol (e.g. including requiring customers to pass Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)) to protect their Web site against malicious bots.
- Establish three security questions with a requirement that the questions must be answered within 1 minute for each question, to be used if out-of-band is unsucessful.

- Random third-party security questions
- Question established by industry and answered by customer
  - Do not use questions that have readily available answers
  - Do not use questions that have answers that are shared with others or are available to others
- Question and answer provided by the customer during a previous authenticated session

- As part of the move to AAL2, the use of security questions is now discouraged and is being phased out, similar to the use of email.
- Note that password restrictions no longer apply once AAL2 level authentication is implemented.

I. Is the IP address from previous login?

- If yes, continue to next step.
- If no, is there a device tag match?
- If yes, continue to next step.
- If no, out-of-band will be initiated and successful completion of one of the following is required before proceeding:

1. Out-of-band verification or
2. If the customer does not complete out-of-band, the customer must answer randomly selected security question within 1 minute.
   a. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.

II. Is the device ID recognized from previous login?

- If yes, continue to next step.
- If no, is there a device tag match?
- If yes, continue to next step.
- If no, out-of-band will be initiated and successful completion of one of the following is required before proceeding:

1. Out-of-band verification or
2. If the customer does not complete out-of-band, the customer must answer randomly selected security question within 1 minute.

a. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.

III. Do the security questions on record meet the New Customer standards? (Not applicable if the company is choosing to use alternate authentication methods based on the below options, and such authentication is successful.)

- If yes, continue to next step
- If no,
  1. Customer must update security questions to meet the New Customer standard

IV. Is the customer indicating they have a new email address?

- To change an email address, customer must successfully complete one of the following:
  1. Out-of-band verification to email or cell phone with a notification sent to the old email address or cell with instructions on what to do if they didn't change their email address or
  2. Answer randomly selected security question within 1 minute

V. Is the customer indicating they have a new cell phone number?

- If the customer indicates that the cell phone number has been changed, an email must be sent including instructions on what to do if the taxpayer has not in fact changed the cell phone number.

VI. Has there been account activity within 90 days?

- If yes, continue to next step
- If no, AND the customer is NOT using a trusted/proven device or IP Address, out-of-band will be initiated and successful completion of one of the following is required before proceeding:
  1. Out-of-band verification or
  2. If the customer does not complete out-of-band, the customer must answer randomly selected security question within 1 minute.
     a. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.

VII. In cases of increased system risk based on identified facts and circumstances determined collaboratively by industry, agencies and IRS (needs to be flexible):

- Out-of-band will be initiated and customer is required to successfully complete one of the following before proceeding:
    1. Out-of-band verification or
    2. If the customer does not complete out-of-band, the customer must answer randomly selected security question within 1 minute.
        a. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.

VII. Prior to filing, Industry will complete Email Address Verification (see Filing Expectations)

1. The required method is for industry partners to initiate out-of-band verification.
2. If the customer does not complete out-of-band, the customer must answer randomly selected security question within 1 minute.
    a. Appropriate indicator that out-of-band was not successful must be included with the transmission of the return.
3. Note: this is another original requirement, only valid until email is, at some future point, ruled out for out-of band. Cell phone validation by similar method is desirable.

Filing Expectations

- No automatic prepopulation of banking information without taxpayer confirmation.
    - Routing number
    - Account number

- For Online DIY, if the primary and/or secondary SSN is being used in a new account in the current year that was used by a different account in the current year the following actions should be taken:
    - If the SSN is used in multiple accounts for the current year, the following actions must apply to all related accounts:
        1. Include the Authentication Review Code Indicator 6; SSN DUP, with the filing of the return that the primary and/or secondary SSN is used in another account, **AND**
        2. Notify account holder(s) that the Primary and/or Secondary SSN is used within another account **OR**
        3. Notify account holder(s) that the Primary and/or Secondary SSN is used within another account AND Implement Additional Authentication measures

prior to filing to validate the authenticity of one or more of the related accounts.
    - All account holders have the opportunity to report the situation to the right authorities if they suspect improper use of the SSN.

- For Online DIY, If the primary and/or secondary SSN is being used in a new account in the current year that was used by a different account in the **previous year, and you have the capability,i**nclude the Authentication Review Code Indicator 6; SSN DUP, with the filing of the return that the primary and/or secondary SSN is used in another account with the additional options to:
    1. Notify account holder(s) that the Primary and/or Secondary SSN is used within another account **OR**
    2. Notify account holder(s) that the Primary and/or Secondary SSN is used within another account AND Implement Additional Authentication measures prior to filing to validate the authenticity of one or more of the related accounts.
        - All account holders have the opportunity to report the situation to the right authorities if they suspect improper use of the SSN.

- The Authentication Working Group will be conducting an analysis of the new optional data elements being used this past filing season for consideration of making the data element required in a subsequent year. These elements may also become mandatory in state efiled returns.

- States are expected to ask for related information in their TY2019/2020 state LOIs

- For Online DIY software, a data element provided by the industry partner will be used to indicate the level of email or text verification performed for each filed return. Tax agencies may request acknowledgement of the use of out-of-band within the e-filing agreement and may use out-of-band capability and the indicators in the process of examining the internal analytics of the return.

- To reduce the occurences of multiple fraudulent returns, Industry will ensure that, at the point of filing, there are no more than two resident state returns filed with a single federal return.

Requirements Not Prescriptive:
This guidance, while prescriptive in nature, is to help organizations that may have either limited IT security budgets or limited IT security expertise to implement security requirements in a consistent, efficient and cost-effective manner. The document is formatted to provide clarity to the minimum requirements baseline recognized in current national standards as agreed upon by the working groups. Industry will meet the requirements set forth in this document based on their particular business models which may address identity authentication using

other features not identified in these minimum requirements. The IRS and state agencies will not dictate specifically how these standards are met and the industry partner ultimately must establish that the e-filing application meets or exceeds the minimum requirements. In order to encourage both innovation and the adoption of new and improved authentication technologies, the Trusted Customer Vetting Process provides a means for the industry partner to present an alternative proposed solution to a knowledgeable team of agency representatives. If the team can determine that the proposal meets or exceeds the baseline requirements, the Trusted Customer Vetting Team will recommend to IRS and the states that the industry partner be allowed to deploy the proposed solution. This process is intended to relieve the industry partner of the need to go through examination by each individual agency; of course any individual agency has the right to reject the proposed solution or require an approval process. Options to consider for tightening the identification process include authentication factors given below in the Appendix or in NIST 800-63B.

APPENDIX

NIST 800-63B AAL2 – Examples of Unrestricted Authentication Factors

Memorized Secrets (something you know)

- Passwords
- Passphrases
- PINs.

Look-up Secrets (something you have)

- Printed list of secrets
- Secret grid

Out-of-Band Devices (something you have)

- Secure communications apps, such as Signal, create a fingerprint that changes if the device on which the app is running ever changes.

Single-Factor OTP Device (something you have)

- Readily-available commercial OTP products
  - Hardware
  - Software

- Multi-Factor OTP Devices (something you know or something you are) – Require activation by input of a memorized secret or the successful presentation of a biometric in order to obtain a one-time password.

- Single-Factor Cryptographic Software (something you have)

- Client X.509 (TLS) certificate (Public & Private keys)

- Single-Factor Cryptographic Devices (something you have)

- "Smart cards" with an embedded processor in a credit card form factor are quite popular

- FIDO U2F authenticators

- Multi-Factor Cryptographic Software (something you know or something you are)

- Single-factor cryptographic software authenticators that they require the input of a memorized secret in order to access the private key for authentication.

- Factor Cryptographic Devices (something you have plus either something you know or something you are)

- Single-factor cryptographic device authenticators except that they require activation by the entry of a memorized secret or verification of a biometric.