**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 take 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 miminum measures were also patterned after the "Know Your Customer" efforts then underway in online banking applications. This Trusted Customer concept was later expanded to include the Tax Professional environment, and a separate document was later developed for that audience.

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 tax professional 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.

Tax professionals are on the front lines of identity theft tax fraud prevention and detection. They see and interact with the filers in a way that surpasses what can be done in the DIY environment. However, IRS and the states still need for tax professionals to follow the necessary steps to provide agencies with the verification of taxpayer identity in a format that the agencies can utilize.

Additionally, the tax professionals themselves are becoming the target of hackers and fraudsters. We require that software ensure that the tax professionals authenticate themselves for each session with methodology that helps to detect and prevent remote takeover.

For these reasons, the measures described in this document apply to two different levels. First we have the requirements for the tax professional him/herself to authenticate to the tax software, in order to minimize remote takeover. Separately, we have the requirements for the tax professional to authenticate the front-end customer, and to relay that authentication to the tax agencies through the software, in a form that IRS and the state agencies can utilize.

The IRS and States working with Industry partners have established the following minimum set of standards and methodology that Industry will use to help deter potential identity theft tax refund fraud activity, which going forward will be based on increasingly stringent and effective national standards and protocols. To preserve innovation and creativity, Industry partners may choose to, and are encouraged to, exceed the minimum standards established and conduct their own independent and unique analysis, based on patterns or trends they observe and identify. These minimum requirements will be reviewed and strengthened by July of each year.

**Tax Professional Audiences**

Establishing a trusted customer requirement for the software packages labeled as Tax Professional with an Online presence 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 but not limited to password changes
- Enhances security / protection measures for taxpayer confidential and sensitive information
- Increases the public confidence and trust in the tax filing system

These steps will be accompanied by national and local messaging driving home these principles. Note that these requirements can and will change over time to respond to new technologies and new threats.

**Minimum Requirements for Identity Authentication**

The following minimum requirements for the Tax Professional Audience, includes:

- When data is stored electronically online,
- If the returns can be transmitted electronically, or
- Any other interactions completed online.

These requirements will be incorporated in agency e-filing agreements for certification and will be verified by optional post-launch reviews.

## REQUIREMENTS FOR AUTHENTICATION OF THE TAX PROFESSIONAL

The intent of the authentication requirements for the tax professional are to minimize the opportunity for remote takeover of the tax professional's identity, while minimizing the burden on the tax professional. As a workable compromise, it is reqired that the tax professional complete authentication at each sign-on to the professional software, at a minimum of once every 24 hours. It is not reasonable nor is it expected to authenticate for each filing.

### 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 in to "restricted" factors, and "unrestricted" factors which are more secure. Additionally, guidelines are provided from NIST 800-53 or 63B to ensure that familiar factors such as passwords 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 do not consider email to be an unrestricted factor. This current document strongly discourages the use of email as an 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 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 unrestricted authentication factor and provide industry feedback based on an analysis of these fields.

For the 2020 filing season, Trusted Customer for DIY software requires the software provider to implement at least **one** unrestricted authentication factor. For the 2020 filing season, the addition of at least one unrestricted factor is strongly recommended for tax professional software if the software provider has the capability:

- **User Login**:
  - 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

Software vendors providing software to Tax Professionals are required to establish validation that the individual signing on to the software is associated with the Tax Professional firm.

1. Strong password.
   a. Each user associated with the Tax Professional firm must use a username and strong password (at least 8 characters, upper, lower case, digit and special char).
   b. Through the use of strong passwords and locking out an account after many consecutive failed attempts, the goal is to mitigate password guessing and brute force attacks. These standards meet the IRS Publication 1075: Safeguards for Protecting Federal Tax Returns and Return Information requirements.
2. Passwords are required to expire periodically (such as every 90 days) per the tax professional Publication 4557.
3. Note that once AAL2 is achieved, password requirements are not required.
4. For web-based programs, 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.
   a. This requirement is upon entry into the software.
5. After *30 minutes* of inactivity, require mandatory log out and re-authorization with username and strong password.

6. Re-authorization is required every 24 hours regardless of activity.
7. **Optional**: Completing Out-Of-Band verification.
    i. Not a requirement for tax year 2019, but will be used for piloting and analytical purposes for 2020 consideration.
    ii. In the case of Tax Professional firms with more than one user access, the out-of-band / 2-Factor will use one of the following:
        - Business email – accessible by individuals in the office.
        - Office email - accessible by all members in the office.
        - Token
        - Finger print
        - Other equivalent technology
            a. If the user does not complete out-of-band, the user is not allowed access to the software unless the software offers another level of authentication.
8. **Optional:** Authentication prior to transmission:
    i. Not a requirement for tax year 2019, but will be used for piloting and analytical purposes for 2020 consideration.
    ii. As the last step prior to completing the transmission, industry can implement an authentication process that could include (and not limited to):
        1. Customer initiated pin
        2. Customer initiated strong password
        3. Finger print
        4. Token
        5. Implementing the use of Common Access Card (CAC) technology
        6. Other digital verification of identity technology.

**REQUIREMENTS FOR AUTHENTICATION OF THE CUSTOMER/TAXPAYER**

Authentication of the filer, to ensure that this is the genuine taxpayer, is a joint responsibility of the tax professional, the tax software, and the IRS and state agencies. The intent of this document is to recognize that the software does not control the actions of the tax professional. However, the software can, through the dialog with the tax professional, encourage best practices and improve the accuracy of the indicators submitted as part of the Authentication Header in the tax return. While personal knowledge of the customer is extremely strong authentication, agencies still need information to perform complementary authentication in case of tax professional system takeover.

For these reasons, the tax professional software should meet the following requirements:

1. Use plain language to determine the steps taken by the tax professional to authenticate the customer, and use the responses to accurately code the Identity Assurance Level Code in the Authentication Header. For example, it is understood that the majority of tax preparers do not have access to government systems to completely verify source documents. However, did the tax professional compare the name and address on the

drivers license to that of the return, and check that the photo and physical characteristics on the license reasonably match those of the customer?
2. Encourage the tax professional to provide additional data, such as driver's license information, by actions such as defaulting to setting the cursor for the tax professional to enter the data, not to the "no data available" option.

Professional tax software is expected to encourage these minimum requirements within the software dialog with the tax professional.

**Filing Expectations**

- For Tax Pro software, no automatic prepopulation of banking information without taxpayer confirmation.
  - Routing number
  - Account number

- 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.

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

- To reduce the occurences of multiple fraudulent returns, Industry partners 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:**

The following minimum requirements are established as a baseline and may incorporate guidance and samples from the STAR Group to aid organizations that may have either limited IT security budgets or limited IT security expertise. This guidance, while prescriptive in nature, is to help such organizations implement security requirements in a consistent, efficient and cost-effective manner. Also, it is based upon "Expected Results" from annual assessments. The document is formatted to provide clarity to the minimum requirements baseline recognized in current national standards as agreed upon by the working group. 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 government 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 his 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:

- Implementing the use of smart cards (ie. Personal Identification Verification (PIV), Common Access Card (CAC) technology or
- Other digital verification of identity technology.

**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.