**Overview**

The industry, state and IRS partners recognize that even though fraud filings will still occur, we all must be proactive and take steps to reduce or prevent the fraud. Minimum requirements are established in cooperation with industry partners, states and the IRS to present a consistent standard for front-end customer identity authentication using recognized national standards from the National Institute of Standards and Technology (NIST) and the IRS Office of Safeguards. These standards also meet the requirements of the Security Summit Strategic Threat Assessment & Response (STAR) working group.

The Trusted Customer requirements are now defined by the IRS Security Summit to more closely adhere to NIST 800-63, for all online applications. Tax software providers must adhere to this new Trusted Customer Requirements beginning in processing year 2019.

Trusted customer is meant to serve as a baseline authentication standard 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 requirements below (ie: password requirements etc.).

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.

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.

**Passwords:**

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.

**Out-of-Band Verification:**

Tax agencies recognize that out-of-band verification is a national standard and allow for the optional identity verification protocol for Tax Professional software. Out-of-band verification is 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 process. The tax agencies will also include a question within their annual filing agreements to determine how the industry partner will implement out-of-band verification.

**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.

**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.

**NIST 800-63B STANDARD PROGRAMMING FOR PROCESSING YEAR 2019**

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 additional authentication factor and provide industry feedback based on an analysis of these fields.

Year one requires industry to implement the following::

* **User Login**:
	+ Leverage the existing authentication infrastructure and **add at least one optional** **unrestricted authentication factor** (e.g., PIN, secret grid, printed secret grid) for client opt-in.
* **Account Recovery:**
	+ Continue using email as a second factor for recovery or an **unrestricted authentication factor** the client opted into (e.g., shared secret, information from return, etc.)

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.
	1. 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). (Current IRS requirements are at 14-character password / pass phrase; however, 8 is sufficient for this year due to other security measures in place.)
2. Passwords are required to expire periodically (such as every 90 days) per the tax professional Publication 4557.
3. 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.
	1. This requirement is upon entry into the software.
4. After *30 minutes* of inactivity, require mandatory log out and re-authorization with username and strong password.
5. Re-authorization is required every 24 hours regardless of activity.
6. **Optional**: Completing Out-Of-Band verification.
	* 1. Not a requirement for 2018, but will be used for piloting and analytical purposes for 2019 consideration.
		2. 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
	+ - * 1. 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.
1. **Optional:** Authentication prior to transmission:
	* 1. Not a requirement for 2018, but will be used for piloting and analytical purposes for 2019 consideration.
		2. 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.

**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 TY17/2018 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.

**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.