Multi-Factor Authentication: Frequently Asked Questions

1. **What is Multi-Factor Authentication (MFA)?**

   Multi-Factor Authentication combines two or more independent credentials in order to gain access to a system. These credentials include something the user knows (e.g., password), something the user has (e.g., token device/smart card/smart phone) or something the user is (e.g., biometric verification).

2. **How does MFA work?**

   MFA provides an additional layer of security that you must clear after entering your user ID and password into the IIE SSO portal (Okta).

   Firstly, you will enter your user ID and password as usual. A screen will then appear asking you to choose an authentication method. The best option is a push notification to your phone. Your phone will display an alert, you will click accept, and you will be permitted to enter the system.

3. **Who is required to use MFA?**

   For your protection, anyone with an active IIE Okta account will be required to use MFA. This includes all IIE staff (domestic & international) offices plus external users like P/C, representatives, FPAs and Program Participants.

4. **What steps must I perform to enroll in Multi-Factor Authentication?**

   The following step-by-step instructions detail how to enroll in Multi-Factor Authentication (MFA). Using a web browser, visit http://portal.iie.org/

   - Log into the IIE portal using your Navigator credentials.
   - When enrolling in MFA, you must choose **at least two options** from the following authentication methods:
     - **Security Question:** the user chooses a security question to gain access.
     - **OKTA Verify App:** two options include a code that changes every 60 seconds, or a Push method, to approve authentication. The Okta Verify App is available both for iOS and Android devices within their respective app stores.
     - **SMS Authentication:** a text code will be sent to the user's configured mobile device.
     - **Voice Authentication:** an automated message that provides a 5-digit code will be delivered to the user's configured telephone (Home, mobile, or desk).

PLEASE NOTE: We strongly recommend the "security question" to be 1 of your MFA selections because it does not require the use of your mobile device in the

event that it becomes lost or stolen.

5. **How often will I need to use MFA?**

   MFA verification will not be prompted when you are connected to the IIE networks while physically present at any of the IIE Domestic offices. You can expect to receive a MFA verification prompt every time you login to the IIE Okta Portal If you are working remotely, off-site, within any IIE International Office or an external user.

6. **Should I register more than one authentication method?**

   Yes, the Technology Department strongly recommends that you enroll in at least 2 authentication methods (e.g. the Okta Verify App and the security question) to embrace a heightened security posture.

7. **I have received a MFA authentication request, but I wasn't attempting to login! What should I do?**

   This could mean that your IIE OKTA credentials have been compromised. Please complete the Single Sign-On (SSO) Support Request form located HERE