Electronic Authentication Risk Assessment (E-Auth)

Completing the E-Auth

E-Authentication risk assessments are used to define electronic assurance levels (EAL) needed to ensure authentication processes are appropriate for electronic transactions requiring authentication. The EALs also provide a basis for assessing credential service providers (CSP) on behalf of federal agencies. Either the system owner or the business owner of a system is required to complete the eAuth RA based on the criteria discussed below. The final workbook must be approved by the IT System Owner (usually the federal business sponsor). The completed workbook must be updated if changes are made to the system that result in changes to previous e-Authentication ratings.

The e-Authentication policy is found in the Office of Management and Budget Memo 04-04, E-Authentication Guidance for Federal Agencies. Technology recommendations and guidance are discussed in the National Institute of Standards and Technology (NIST) SP 800-63, Electronic Authentication Guideline

Step 1: Complete the E-Auth Threshold Analysis

1. On Step 1 (Tab 2) of the workbook, fill in the System Name, ISSO Name, System Owner Name (Federal business owner), Date of Assessment, and Date of Approval in the provided blanks. If you know your system's FISMA UUID you can provide it; otherwise leave blank and this can be assigned later if needed.
2. The Minimum Assurance Level box will be automatically filled in based on Step 2
3. Answer the three screening questions posed, which are:

- Does the system require users to login/authenticate to access its data/functionality?
- Is the system web browser based?
- Is the system publically accessible (i.e., to users connected ONLY to the public Internet)?

If you answer YES to all 3 of these questions, then you must proceed to Step 2 of the workbook and complete all required answers in Step 2. If you answered NO to any one of these 3 questions, then an eAuth rating is not required and you can skip to Step 3.

Step 2: Answer the E-Auth RA questions

1. On Step 2 (Tab 3) provide a response to each question by selecting the appropriate impact levels for each of the 6 Impact areas using the built-in dropdown menus (e.g, choosing between N/A, Low, Moderate, or High)
2. Once you have answered all 6 questions, proceed to Step 3 (Tab 4) of the Workbook to see your final eAuth rating and obtain owner approval.

Step 3: View and Approve the final ratings

1. Go to Step 3 (Tab 4) of the workbook to view the automatically assigned e-Auth Level noted as the Minimum Assurance Level. These will range from Level 1 to Level 4 based on the answers provided in Step 2. If you disagree with the final Level assigned by the tool, then you can re-evaluate your responses to Step 2 and adjust them as needed.
2. Obtain system owner approval by having the federal business owner approve on the provided signature line
3. Send a completed copy of the signed eAuth Workbook to the NCI ISSO at NCIIRM@nih.gov

Notes about e-Assurance levels (EALs) and tokens

The e-Authentication policy defines four assurance levels:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

Each EAL allows one or more token types. More details on the different tokens as well as various methods for proving identity are discussed in in NIST 800-63.

Token Type	Level 1	Level 2	Level 3	Level 4
Hard Crypto Token	X	X	X	X
One-time password device	X	X	X	
Soft Crypto Token	X	X	X	
Passwords and PINs	X	X		

It is important to note that the E-Authentication guidance does not apply to authorization. Authorization focuses on the actions permitted of an identity after authentication has taken place. Decisions concerning authorization are and should remain the purview of the business process owner.

Either form can be completed by the System Owner (contractor) or the Business Owner (Fed), but the appropriate completed form needs to be reviewed and approved in writing by the system's designated ISSO and the designated authorizing official (AO). The completed form is also maintained by the NCI ISSO and must be updated if changes are made to the system that impact the previous e-Auth ratings. Contact the NCI ISSO for help completing these forms (nciirm@mail.nih.gov).

e-Authentication resources

- Blank E-Auth form
- NIST 800-63 Electronic Authentication Guidance