LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

E-Authentication Risk Assessment and Selection of E-Authentication Assurance Levels

This tool automates the instructions provided in the *HHS Guidance for Selection of E-Authentication Assurance Levels* to assist system owners (or designees) perform the E-Authentication Risk Assessment (ERA) and select the applicable E-Authentication (E-Auth) assurance levels for their system(s) in accordance with the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-63 Revision 3, *Digital Identity Guidelines*, June 2017. The *HHS Guidance,* which provides detailed instructions, can help clarify the significant changes from the previous E-Auth assurance process and new requirements in NIST SP 800-63-3.

For each HHS information system, the system owner (or designee) shall conduct an ERA and select the relevant E-Auth assurance levels in the early stages of the system development lifecycle (SDLC)/procurement process and periodically thereafter as mandated by the HHS Information Security and Privacy Policy (IS2P). When possible, the ERA and selection of the E-Auth assurance levels must be completed in the Security Governance Risk and Compliance (SGRC) tool.

The resulting E-Auth assurance levels in Part D are required for the implementation of the NIST SP 800-63A, NIST SP 800-63B, and NIST SP 800-63C system requirements for identification and authentication.

The following are the possible E-Auth Assurance Levels that may result from the ERA:

- **IAL – Identification Assurance Level** corresponds to the strength (aka robustness) of the identity proofing process.
- **AAL - Authentication Assurance Level** corresponds to the strength of the authentication process.
- **FAL – Federated Assurance Level** corresponds to the strength of the assertion protocol used in federated environments to communicate authentication and attribute information to a relying party (RP) (Note: This only applies when federated architectures are utilized).

Follow the process below to complete the system ERA Template and determine the applicable E-Auth assurance levels.

The system owner must approve the completed ERA Template regardless of whether or not E-Auth assurance levels are selected.

PART A – ENTER SYSTEM INFORMATION

System Name:	
System UUID:	
ISSO:	
System Owner:	
Date of Assessment:	

PART B – DETERMINE IF E-AUTHENTICATION RISK ASSESSMENT IS REQUIRED

Step 1: Is the system stand-alone, internal, with no network connections, and only performs business processes? If answer is “**Yes**”, no E-authentication is required. Proceed to **PART D** and obtain system owner’s approval. Retain approved ERA and note “no e-Authentication required” in the system security plan (SSP). If answer is “**No**”, go to **Step 2**.	Yes □ No □
Step 2: Does the system involve online transactions (editing, deleting, changing of information) with one or more users (e.g., employees, contractors, citizens, business partners, government entities, etc.)? **If answer is “Yes”,** then the selection of the assurance levels is required. Go to **PART C.** (See Section 2.2 in HHS Guidance for examples of systems that require E-Auth assurance levels). **If answer is “No”, no E-authentication RA is required. Go** to **PART D** and obtain system owner’s approval. Retain approved ERA and note “no e-Authentication required” in the system security plan (SSP).	Yes □ No □

PART C – SELECT ASSURANCE LEVELS

Note: To select the IAL, AAL, and FAL, follow the process described in Section 2.2 (2.2a 2.2g) in the HHS E-Authentication Guidance.

A risk-based approach is used to determine three (possibly different) assurance levels:

- IAL corresponding to the strength (aka robustness) of the identity proofing process,
- AAL corresponding to the strength of the authentication process, and
- FAL corresponding to the strength of the assertion protocol used in federated environments to communicate authentication and attribute information to a relying party (RP) (Note: This only applies when federated architectures are utilized).

Step 1. Selecting IAL	
Step 1.a. To provide the service, do you need any personal information (Personally Identifiable Information [PII] or Protected Health Information [PHI])? If yes, go to **Step 1.b.** If no, IAL = 1. Verify that IAL1 is entered in **Step 1.k.** and proceed to **Step 2.**	Yes □ No □
Step 1.b. To complete the transaction, do you need the PII/PHI to be validated? If yes or unknown, go to **Step 1.c.** If no, IAL = 1. Verify that IAL1 in entered in **Step 1.k.** and proceed to **Step 2.**	Yes □ No □
Step 1.c. Specify the risks (to the organization or the subject) of providing the digital service by determining the risk impact categories:	
• Potential impact of inconvenience, distress, or damage to standing or reputation (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of financial loss (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of harm to agency programs or public interests (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of unauthorized release of sensitive information (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact to personal safety (select appropriate impact level):	Low □ Moderate □ High □
• The potential impact of civil or criminal violations (select appropriate impact level):	Low □ Moderate □ High □
Step 1.d. Are any of the above impact levels high? If yes, IAL = 3. Verify that IAL3 is entered in **Step 1.k.** and proceed to **Step 1.h**. If no, go to **Step 1.e.**	Yes □ No □
Step 1.e. Is personal safety assessed at moderate? If yes, IAL = 3. Verify that IAL3 is entered in S**tep 1.k.** and proceed to **Step 1.h.** If no, go to **Step 1.f.**	Yes □ No □
Step 1.f. Are any of the other categories assessed at moderate? If yes, IAL = 2. Verify that IAL2 is entered in **Step 1.k.** and proceed to **Step 1.h.** If no, go to **Step 1.g.**	Yes □ No □
Step 1.g. Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations? If yes, IAL = 1. Enter IAL1 in **Step 1.k.** and proceed to **Step 2.** If no, IAL = 2. Verify that IAL2 is entered in **Step 1.k.** and proceed to **Step 1.h.**	Yes □ No □

Step 1.h. Do you need to resolve an identity uniquely? If yes, proceed to **Step 2.** If no, go to **Step 1.i.**	Yes □ No □
Step 1.i. Can you accept references? If yes, use references if you can complete the transaction or offer the service without complete attribute values (consult NIST SP 800-63A for additional information). Then proceed to **Step 2**. If no, proceed to **Step 2**	Yes □ No □
Step 1.k. IAL selected in Step 1 above:	
Step 2. Selecting AAL	
Step 2.a. Specify the risks (to the organization or the subject) of providing the digital service by determining the risk impact categories:	
• Potential impact of inconvenience, distress, or damage to standing or reputation (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of financial loss (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of harm to agency programs or public interests (select appropriate impact level):	Low □ Moderate □ High □
• The potential impact of harm if information is publicly disclosed (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of unauthorized release of sensitive information (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact to personal safety (select appropriate impact level):	Low □ Moderate □ High □
Step 2.b. Are any of the above impact levels high? If yes, AAL = 3. Verify that AAL3 is entered in **Step 2.g.** and proceed to **Step 3.** If no, go to **Step 2.c.**	Yes □ No □
Step 2.c. Is personal safety assessed at moderate? If yes, AAL = 3. Verify that AAL3 is entered in **Step 2.g.** and proceed to **Step 3.** If no, go to **Step 2.d.**	Yes □ No □
Step 2.d. Are any of the other categories assessed at moderate? If yes, AAL = 2. Verify that AAL2 is entered in **Step 2.g.** and proceed to **Step 3.** If no, go to **Step 2.e.**	Yes □ No □
Step 2.e. Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations? If yes, go to **Step 2.f.** If no, AAL = 2. Verify that AAL2 is entered in **Step 2.g.** and proceed to **Step 3**.	Yes □ No □

Step 2.f. Are you making PII or PHI accessible? If yes, AAL = 2. Verify that AAL2 in **Step 2.g.** and proceed to **Step 3.** If no, AAL = 1. Enter AAL1 in **Step 2.g.** and proceed to **Step 3.**	Yes □ No □
Step 2.g. AAL selected in Step 2 above:	
Step 3. Selecting FAL	
Step 3.a. Are you federating? If no, proceed to **Step 4.** If yes, go to **Step 3.b.**	Yes □ No □
Step 3.b. Specify the risks (to the organization or the subject) of providing the digital service by determining the risk impact categories:	
• Potential impact of inconvenience, distress, or damage to standing or reputation (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of financial loss (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of harm to agency programs or public interests (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact of unauthorized release of sensitive information (select appropriate impact level):	Low □ Moderate □ High □
• Potential impact to personal safety (select appropriate impact level):	Low □ Moderate □ High □
• The potential impact of civil or criminal violations (select appropriate impact level):	Low □ Moderate □ High □
Step 3.c. Are any of the above impact levels high? If yes, FAL = 3. Verify that FAL3 is entered in **Step 3.i.** and proceed to **Step 4.** If no, go to **Step 3.d.**	Yes □ No □
Step 3.d. Is personal safety assessed at moderate? If yes, FAL = 3. Verify that FAL3 is entered in **Step 3.i.** and proceed to **Step 4**. If no, go to **Step 3.e.**	Yes □ No □
Step 3.e. Are any of the other categories assessed at moderate? If yes, FAL = 2. Verify that FAL2 is entered in **Step 3.i.** and proceed to **Step 4.** If no, go to **Step 3.f.**	Yes □ No □
Step 3.f. Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations? If yes, go to **Step 3.g.** If no, FAL = 2. Verify that FAL2 is entered in **Step 3.i.** and proceed to **Step 4.**	Yes □ No □

Step 3.g. Are you making PII or PHI accessible? If yes, FAL = 2. Verify that FAL2 is entered in **Step 3.i.** and proceed to **Step 4.** If no, go to **Step 3.h.**	Yes □ No □
Step 3.h. Are you using front channel assertion presentation? If yes, FAL = 2. Verify that FAL2 is entered in **Step 3.i.** and proceed to **Step 4.** If no, FAL = 1. Verify that FAL1 is entered in **Step 3.i.** and go to **Step 4.**	Yes □ No □
Step 3.i. FAL selected in Step 3 above:	
Step 4. Overriding Restriction on the Selections of the Assurance Levels (Executive Order 13681 requires that personal information (Personally Identifiable Information [PII] or Protected Health Information [PHI]) be protected by multi-factor authentication.)	
Step 4.a. Was AAL1 selected in **Step 2** above? If no, enter AAL value from **Step 2.g.** into **Step 4.e.** and proceed to **PART D.** If yes, go to **Step 4.b**.	Yes □ No □
Step 4.b. Is IAL2 or IAL3 Selected? If yes, then AAL1 is not allowed. The minimum allowed assurance level is AAL2. Go to **Step 4.d**. If no, go to **Step 4.c.**	Yes □ No □
Step 4.c. For IAL1, does the system process, collect, or store PII or PHI? If no, then AAL1 is permitted. Verify that AAL1 is entered in **Step 4.e.** and proceed to **PART D.** If yes, go to **Step 4.d**.	Yes □ No □
Step 4.d. AAL1 is not allowed. The minimum allowed assurance level is AAL2. Enter either AAL2 or AAL3 in **Step 4.e.** and go to **PART D.**	AAL2 □ AAL3 □
Step 4.e. Final AAL Selection from Step 4 above:	

PART D – APPROVAL

System Name:	
System UUID:	
ISSO:	
System Owner:	
Date of Assessment:	
ASSURANCE LEVELS:	
System Identity Assurance Level (IAL)	
System Authentication Assurance Level (AAL)	
System Federated Assurance Level (FAL) – applies only for federated systems	
If the selected IAL, AAL, or FAL deviate(s) from the process presented in this template, enter the values:	IAL: AAL: FAL:
If the assurance levels deviate from the process, provide a summary justification for the deviation and the process used to specify the values.	
SIGNATURE:	
System Owner Signature (or Designee):	
System Owner Contact Information:	
Date Signed:	