Contents

ADFS Risk Assessment Template Questionnaire User Manual Description: ................................. 3
Section 1: Contact Information .................................................................................................... 4
Section 2: System Information .................................................................................................. 5
Section 3: Cloud Provider Information ...................................................................................... 7
Section 4: Active Directory Attributes and Risks Associated with Authentication ..................... 8
Section 5: PII Risks per Attribute ............................................................................................. 10
Section 6: PIA Information ......................................................................................................... 11
ADFS Risk Assessment Template Questionnaire User Manual Description:

This user manual is designed to assist Requesting Parties/Federated Partners with understanding what information is requested and/or required to complete the Risk Assessment Template Questionnaire via the google form provided after an Intake form is submitted. This document is broken into the following sections;

- **Section 1**, is required for all requests; Contact information
- **Section 2**, is required for all requests; System information
- **Section 3**, requests information regarding the cloud service if your application is a cloud-based application;
- **Section 4**, is required for all requests; Active Directory Attributes and Associated Risks
- **Section 5**, is required for all requests; PIA Information

**Where to find information to fill out form:** your Bureau’s Security Office.
Section 1: Contact Information

Contact Name
First and Last Name

Contact Email Address *

Contact Phone Number *

Department/Bureau *

All questions marked with a red asterisk are required in order to proceed.

Always read the “help text” under the question. This will provide important information regarding what is being asked.

Press “Next” to continue. If you have left a required field blank, you will not be able to continue until it is filled out.
Section 2: System Information

The **System Owner** is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented.

- The **Authorizing Official** (AO) is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
- An **Authority to Operate** (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of information security controls.
Section 3: Cloud Provider Information
If your application is a cloud service, you will receive additional questions. If you require a waiver, and have not yet received one, you will be contacted by DOI’s Cloud Hosting Services department to provide further information.
Section 4: Active Directory Attributes and Risks Associated with Authentication
When filling out this section, please provide the risk information for each individual attribute required.

Example of how to fill in the following questions: Attribute CN: LDAP Display Name: Explanation

<table>
<thead>
<tr>
<th>Attribute CN</th>
<th>LDAP Display Name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>In. Givem-Name</td>
<td>givenName</td>
<td>N/A – the attribute is not required for authentication</td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td>N/A – the attribute is not required for authentication</td>
</tr>
<tr>
<td>User-Principal-Name</td>
<td>userPrincipalName</td>
<td>1. The userPrincipalName attribute must be in the Internet-style login format where the user name is followed by the symbol @ and a domain name, for example, <a href="mailto:user@domain.com">user@domain.com</a> 2. All Simple Mail Transport Protocol (SMT) addresses should comply with email messaging standards. 3. The maximum number of characters for the userPrincipalName attribute is 113. A specific number of characters are permitted before and after the at sign (@), so please use maximum number of characters for the user name that is in front of the at sign (@) 4. Maximum number of characters for the domain name following the at sign (@): 48 5. Maximum number of characters for the domain name following the at sign (@): 8 6. Invalid characters: / @ * + &amp; ? { } [ ] &lt; &gt;</td>
</tr>
</tbody>
</table>

Please include all AD Attributes required for User Authentication

Use this format to answer the question: Attribute CN (Common Name): LDAP Display Name: Explanation: If you have multiple attributes, please hit enter after each one.

Your answer

Example based off of sample table:
Given-Name: givenName: N/A the attribute is not required for authentication
Identify any risks related to the improper use of attributes within AD which may cause the authentication to fail or be compromised. *
These are risks to your bureau application.

Your answer

Identify any mitigation steps, which have been taken to address the risks documented above.
These are steps that have been taken by your agency/bureau to mitigate risks to your application.

Your answer

Identify any remaining risk elements, which have not been covered above. Identify the risks and any mitigation steps that have been employed to lower the risk of occurrence

Your answer
Section 5: PII Risks per Attribute

Please provide risks for every attribute identified in Section 4.
Section 6: PIA Information
Not all requests require a PIA. If you have one, please provide the information for it. If you do not have one and one is required, you will be notified with the requirements later in the process.

![PIA](Image)

**PIA**

Has a Privacy Impact Assessemment (PIA) been conducted? *

- [ ] Yes
- [ ] No

![CSAM Location](Image)

**CSAM Location**

Please provide the CSAM boundary for PIA

If you don’t know the CSAM boundary, please contact your bureau privacy officer.

Your answer
Congratulations! You have reached the end of the form. You can request a copy of your answers to be emailed to you if you like. Press submit to submit form, or back to change your answers.