



U.S. Department of the Interior  
Office of the Chief Information Officer

# **ADFS Risk Assessment Template Questionnaire User Manual**

## 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  
Your answer

**Contact Email Address \***  
Your answer

**Contact Phone Number \***  
Your answer

**Department/Bureau \***  
Your answer

**NEXT**

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

|                                 |
|---------------------------------|
| <b>System Name *</b>            |
| <small>Long answer text</small> |
| <b>System Owner *</b>           |
| <small>Long answer text</small> |

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.

|   |
|---|
| <b>Authorizing Official *</b>   |
| <small>Long answer text</small>   |
| <b>Authority to Operate Date</b>  |
| <small>Month, day, year</small>  |

- 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.

Is the system/application included in a separate system boundary within CSAM? \*

☒ Yes

☐ No



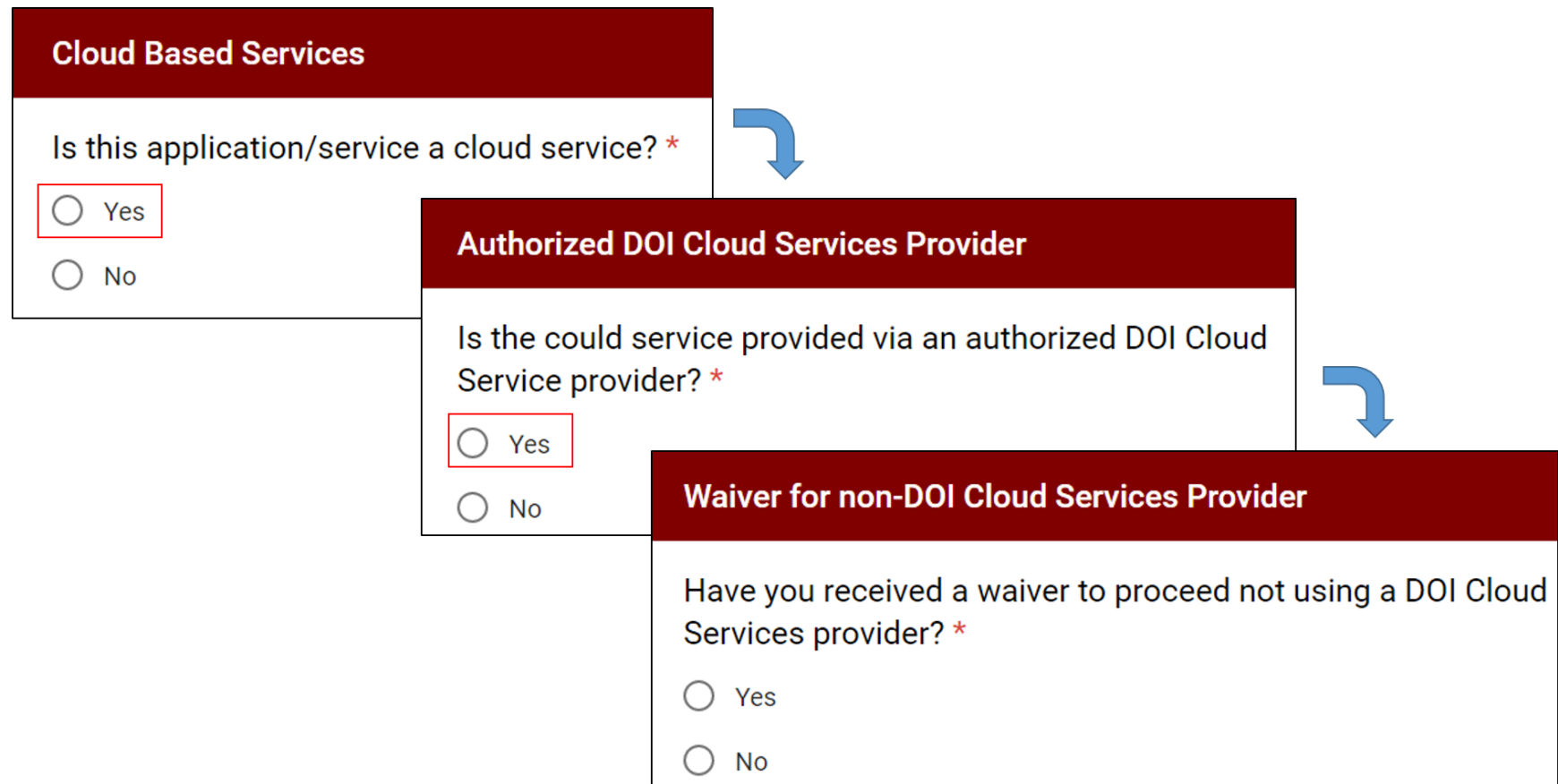
**Application is included in a separate system boundary for CSAM**

Provide Boundary Name \*

Your answer

### 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.



```
graph TD; A[Cloud Based Services] --> B[Authorized DOI Cloud Services Provider]; B --> C[Waiver for non-DOI Cloud Services Provider];
```

**Cloud Based Services**

Is this application/service a cloud service? \*

☒ Yes

☐ No

**Authorized DOI Cloud Services Provider**

Is the could service provided via an authorized DOI Cloud Service provider? \*

☒ Yes

☐ No

**Waiver for non-DOI Cloud Services Provider**

Have you received a waiver to proceed not using a DOI Cloud Services provider? \*

☐ Yes

☐ No

## 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 1 – Syntax Rules for AD Attributes Required for User Authentication

| Attribute CN               | LDAP Display Name        | Explanation   |
|----------------------------|--------------------------|---|
| <i>Given-Name</i>          | <i>givenName</i>         | <i>N/A – the attribute is not required for authentication</i>   |
| <i>Surname</i>             | <i>sn</i>                | <i>N/A – the attribute is not required for authentication</i>   |
| <i>User-Principal-Name</i> | <i>userPrincipalName</i> | <ol style="list-style-type: none"> <li>The <i>userPrincipalName</i> attribute must be in the Internet-style logon format where the user name is followed by the symbol @ and a domain name; for example, <a href="#">user@contoso.com</a>.</li> <li>All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards.</li> <li>The maximum number of characters for the <i>userPrincipalName</i> attribute is 113. A specific number of characters are permitted before and after the at sign (@), as follows: <ol style="list-style-type: none"> <li>Maximum number of characters for the user name that is in front of the at sign (@): 64</li> <li>Maximum number of characters for the domain name following the at sign (@): 48</li> </ol> </li> <li>Invalid characters: \ % &amp; * + = ? ' { }   &lt; &gt; ( ) , [ ] " .</li> <li>The @ character is required in each <i>userPrincipalName</i> value.</li> <li>The @ character cannot be the first character in each <i>userPrincipalName</i> value.</li> <li>The user name cannot end with a period (.), an ampersand (&amp;), a space, or an at sign (@).</li> <li>The user name cannot contain any spaces.</li> <li>Routeable domains must be used; for example, local or internal cannot be used.</li> <li>Unicode is converted to underscore characters.</li> <li><i>userPrincipalName</i> cannot contain any duplicate values in the directory.</li> </ol> |

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

### Explanation of PII risk per attribute

Exposure of Personally Identifiable Information (PII) or DOI/[Bureau/Office] sensitive information

Example of how to answer below questions: Attribute CN: LDAP  
Display Name: Explanation

Table 1 – AD Attributes Required for User Authentication

| Attribute CN           | LDAP Display Name | Explanation  |
|------------------------|-------------------|--|
| <i>I.e. Given-Name</i> | <i>givenName</i>  | <i>Contains the given name (first name) of the user.</i> |
|                        |                   |  |

### Explain PII Risk per attribute \*

Use this format to answer the question: Attribute CN: LDAP Display Name: Explanation. If you have multiple attributes, please hit enter after each one. (Please provide information for every attribute requested, even if the PII threat is low).

Your answer

Identify all PII risk mitigation activities which have been taken or are in place associated with sharing the information attributes above.

Your answer

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**

Has a Privacy Impact Assessment (PIA) been conducted? \*

☒ Yes

☐ No



**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

Click submit to finish.

☐ Send me a copy of my responses.

BACK

SUBMIT

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