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

Active Directory Federation Services (ADFS) Relying Party Trust (RPT) Request Form

User Manual

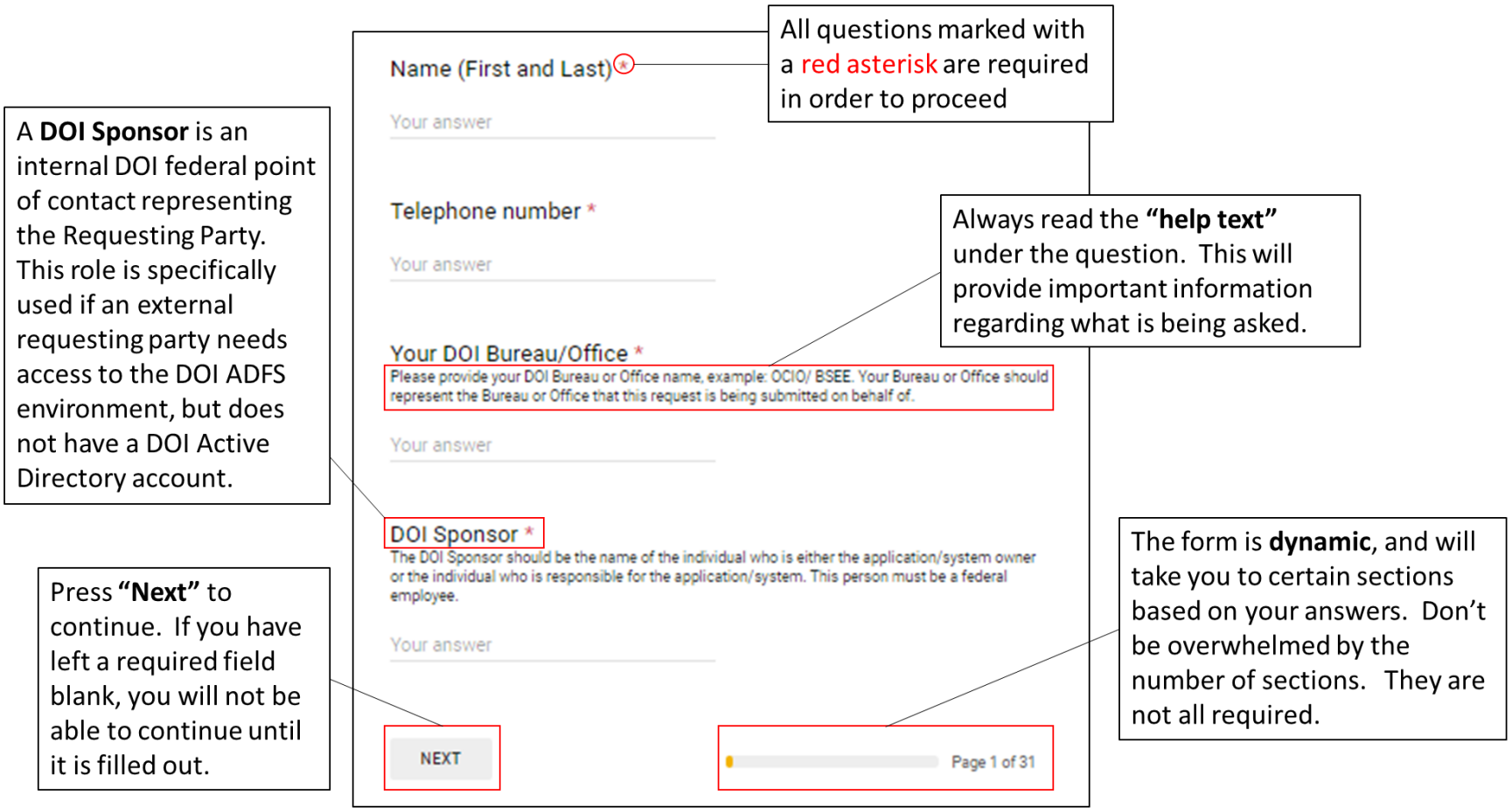
Contents

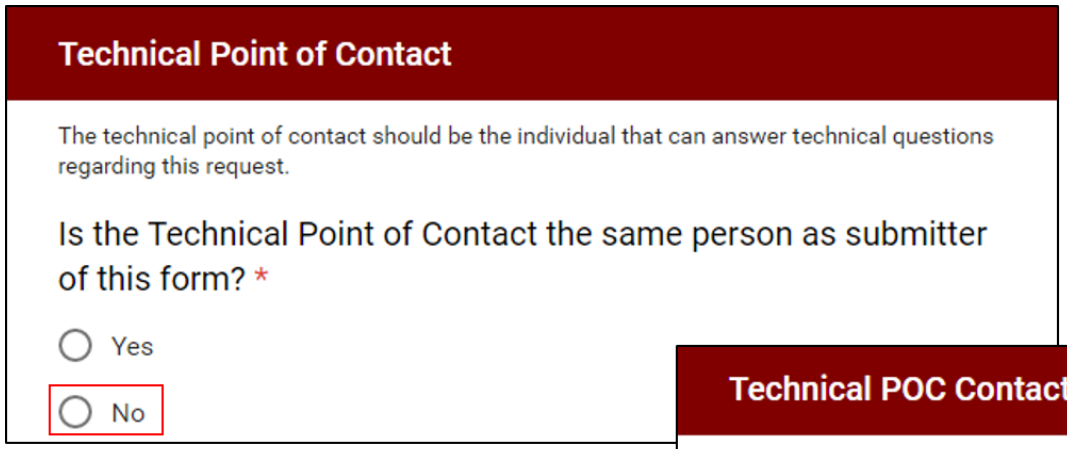
ADFS Request Form User Manual Description:

This user manual is designed to assist Requesting Parties/Federated Partners with understanding what information is requested and/or required to complete an Active Directory Federation Services (ADFS) Relying Party Trust (RPT) request via the intake request form. This document is broken into the following sections;

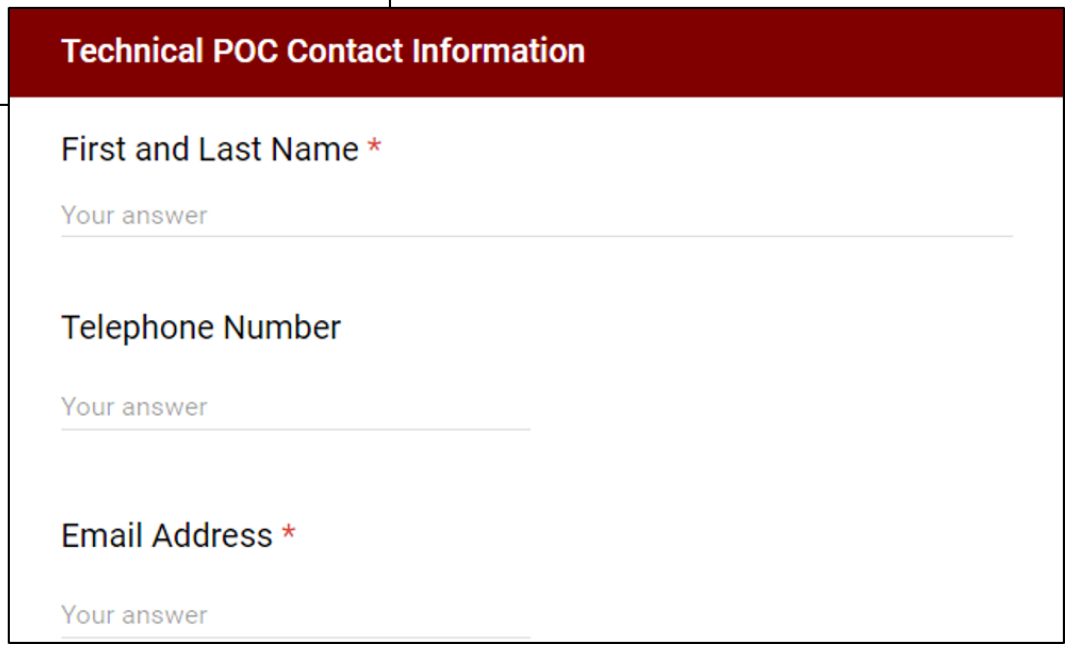
- **Section 1,** is required for all requests;
- **Section 2,** describes the difference between a "new" or "modification" of an existing relying party trust request
- **Section 3,** describes what's requested and/or required if you'll be submitting a new relying party trust request;
- **Section 4**, describes what's requested and/or required if you'll be submitting a modification to an existing relying party trust request;
- **Section 5,** provides helpful information if you're not sure who can provide the requested and/or required information being requested in the form.

Section 1: Requesting Party Information





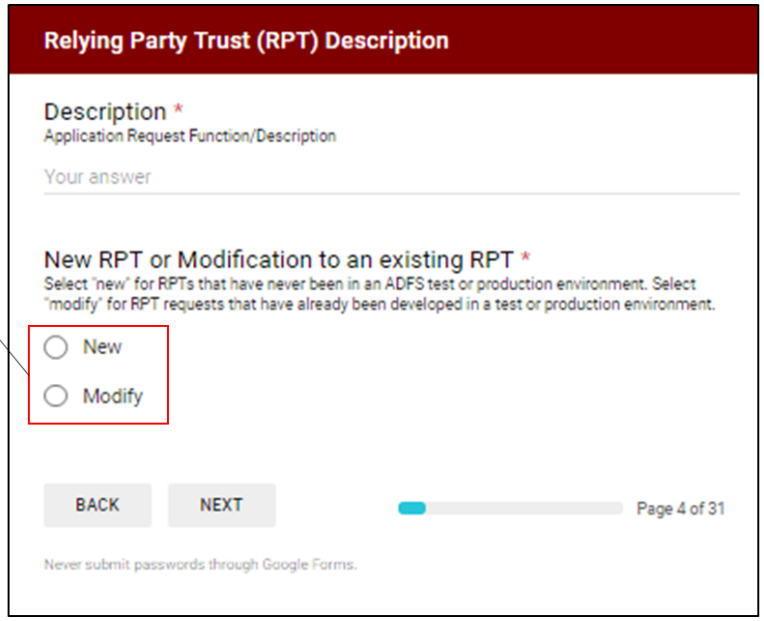
If there is a point of contact that has a more technical knowledge of the ADFS RPT requirement, please provide their contact information



Section 2: New Relying Party Trust vs. Modification to an Existing Relying Party Trust

A **new** Relying Party Trust refers to a request that has never been deployed into a production environment with the Department of the Interior by the Requesting Party organization

The types of questions received will vary greatly based on the selection made here



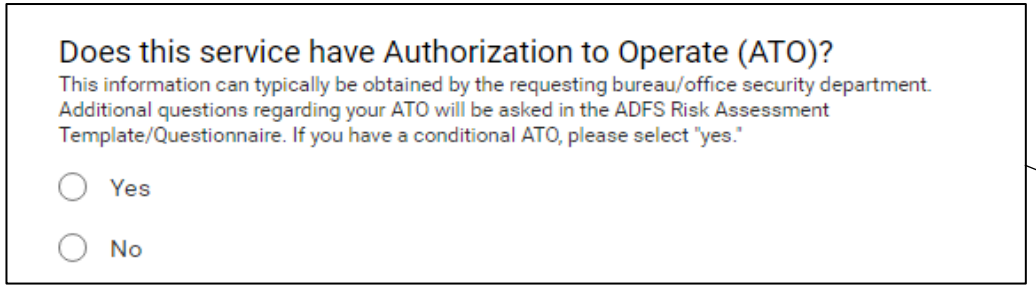
An existing RPT refers to a current Relying Party Trust that requires some **modification** (for example additional claims, a change in authentication rules, etc.).

Section 3: "New" Relying Party Trust (RPT) details what's necessary to complete a new RPT request.

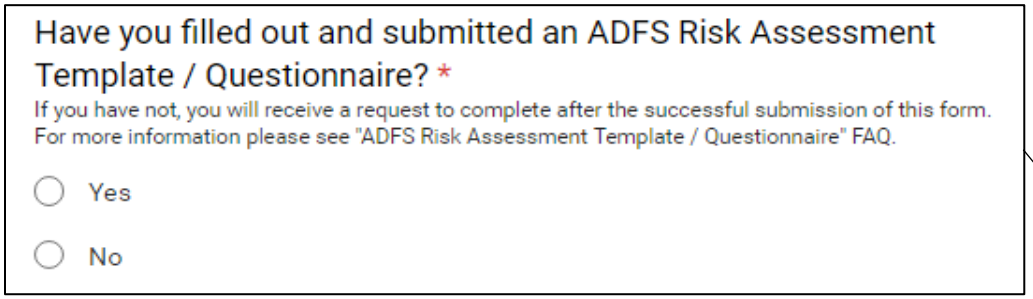
If you are interested in submitting a modification to an existing RPT, please go to:

Section 3: “New” Relying Party Trust (RPT)

Section 3a) Security Related Questions

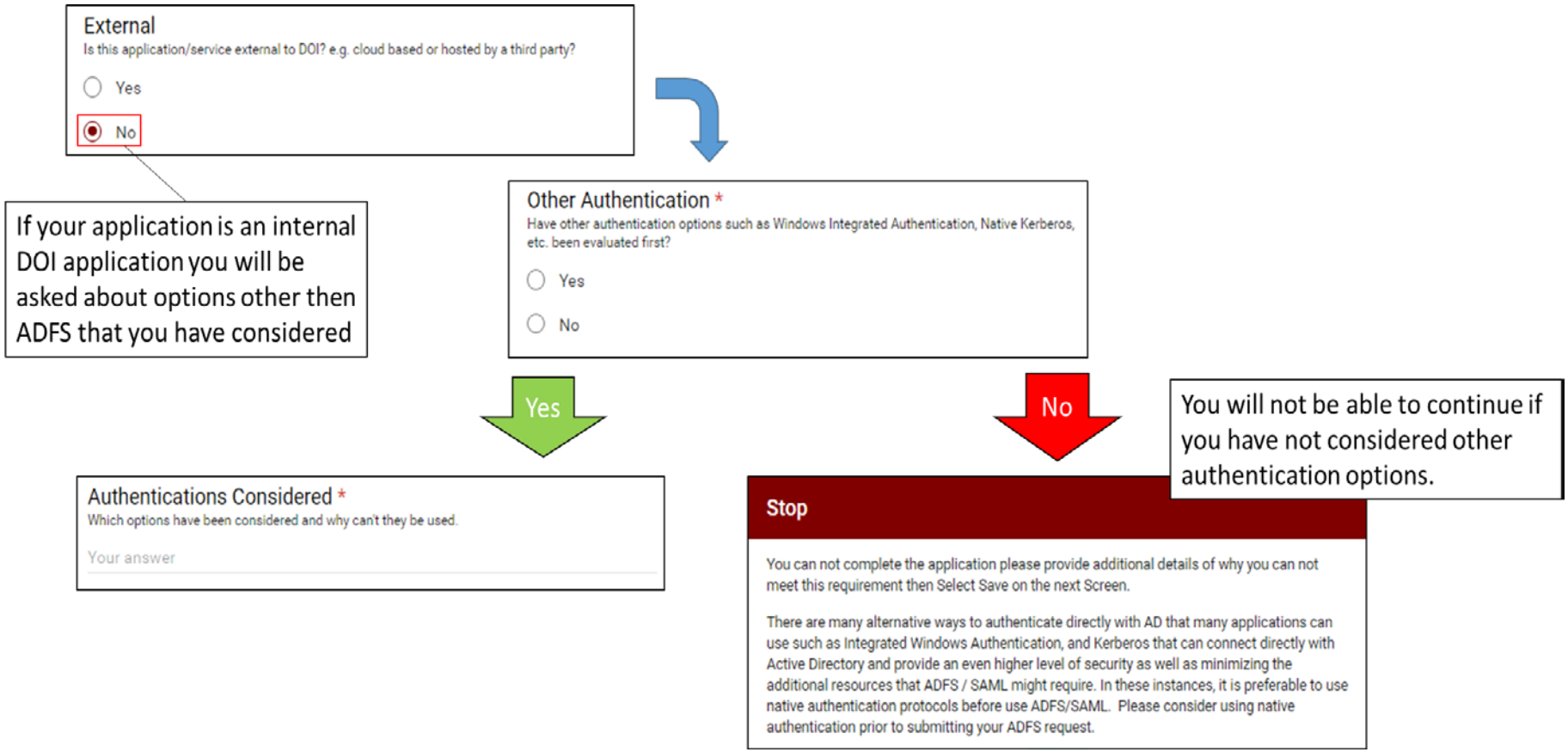


This is not a mandatory question, but an **Authorization to Operate (ATO)** is required before your application can go into Production.



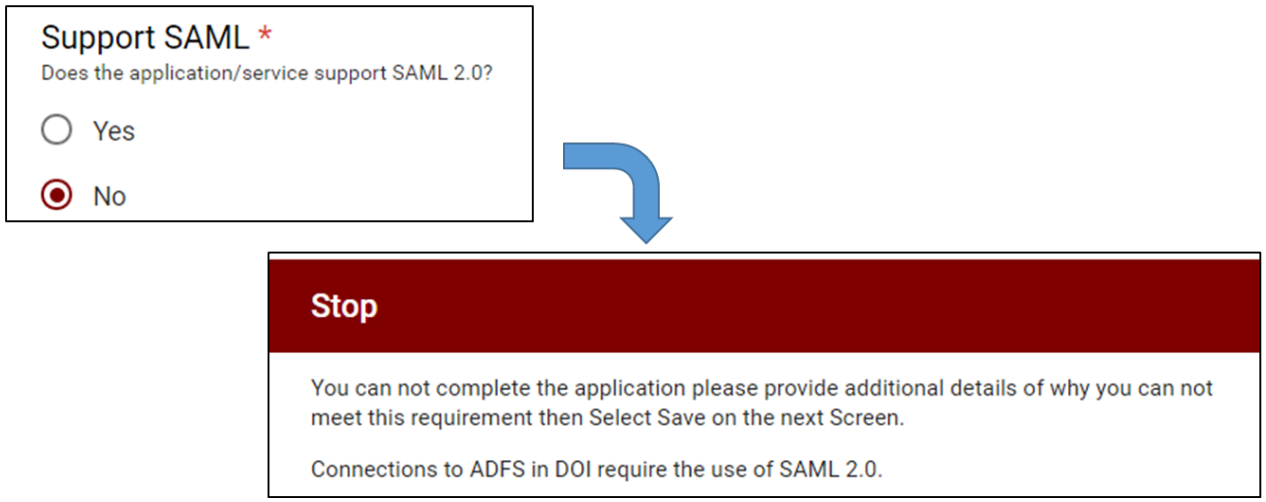
If you have not yet filled out an **ADFS Risk Assessment**, then one will be sent to you after completion of the ADFS request form is reviewed. If you are unsure, please select **No**.

Section 3b) Application/service external to the DOI

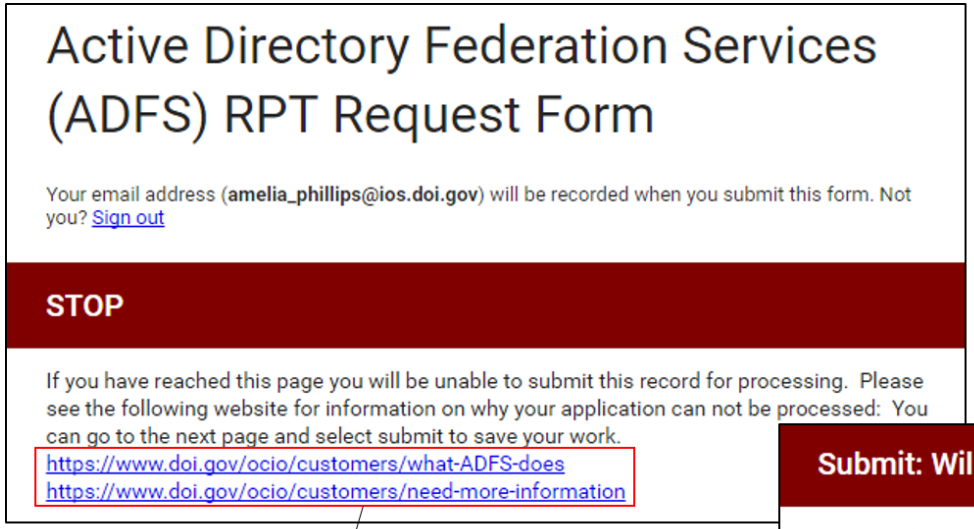


Section 3c) SAML 2.0 Requirement

An **application is required to support SAML 2.0** in order to obtain a Relying Party Trust with the DOI. SAML permits DOI to make assertions regarding the identity, attributes, and entitlements of user account to an external web service. Adoption of SAML is central to the agency's successful implementation of the Federal Identity, Credential, and Access Management (FICAM) strategy and corresponding two-factor PIV authentication requirements for cloud-based web applications and services. For more information regarding this requirement please see the memo "Mandatory use of Security Assertion Markup Language (SAML) 2.0 Standard for Cloud-Based, Web Application Authentication Information Exchange."

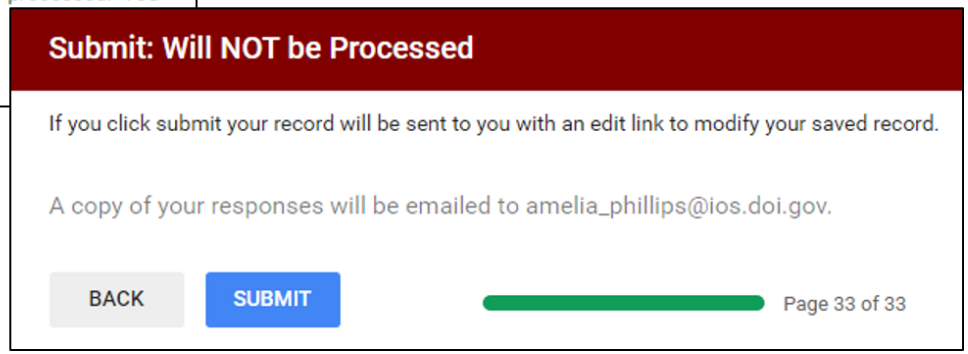


Section 3d) Hard Stops

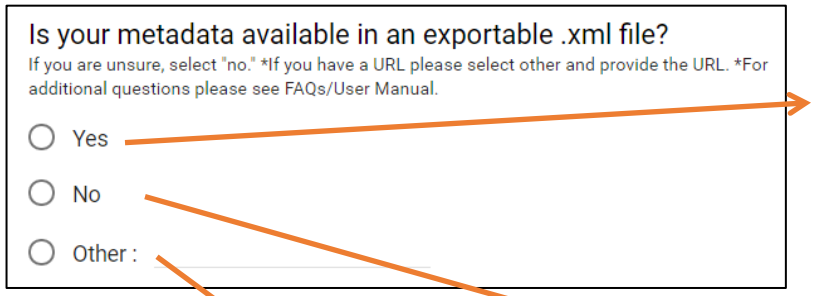


If you receive a hard stop, you will be able to save your responses to come back and finish it later if applicable.

You can follow these links for more information, or to submit a question.



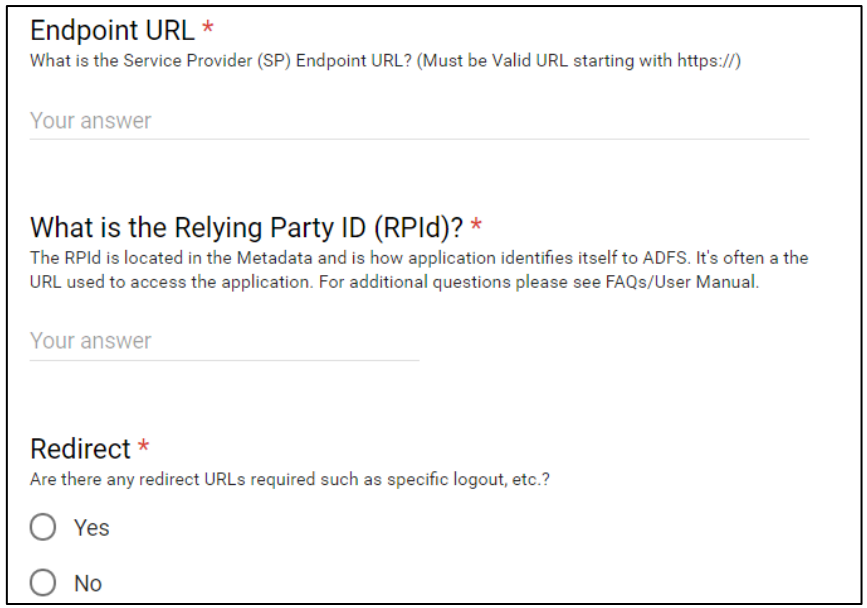
Section 3e) Metadata



If you select **Yes**, you will receive an email reminding you to attach the .xml file to an email and submit it to the Customer Support Center (CSC) helpdesk.

If you have the **url** for your metadata, please provide it in the "other" field.

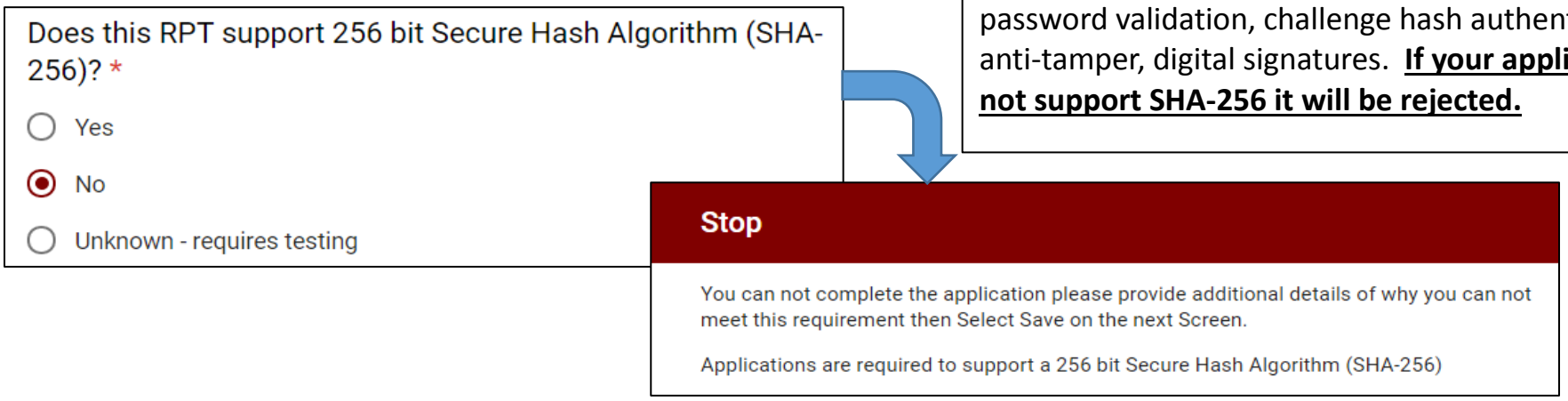
Select **No**, if you do not have metadata in an exportable .xml file or url, or if you do not know. It will take you to the following questions to obtain necessary



Section 3f) Certificate Signing and SHA-256 Requirement

If you select **Yes**, an email will be sent reminding you to attach the signing certificate and email it to the CSC helpdesk.

The **SHA (Secure Hash Algorithm)** is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. This makes it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. **<u>If your application does not support SHA-256 it will be rejected.</u>**



Section 3g) LDAP Attributes

You can use **Send LDAP Attributes as Claims Rules** when you want to issue outgoing claims that contain actual Lightweight Directory Access Protocol (LDAP) attribute values that exist in an attribute store and then associate a claim type with each of the LDAP attributes. For more detailed information see: https://technet.microsoft.com/en-us/library/ff678048(v=ws.11).aspx

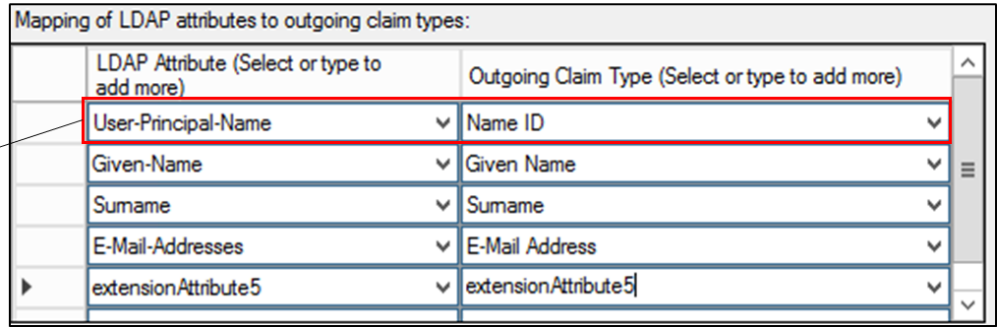
LDAP Attributes/Outgoing Claims *

What attributes are required as outgoing claims, please fill out the specifications as illustrated on a separate line for each attribute. LDAP Attributes ----> OUTGOING CLAIM

User-Principal-Name ----> Name ID

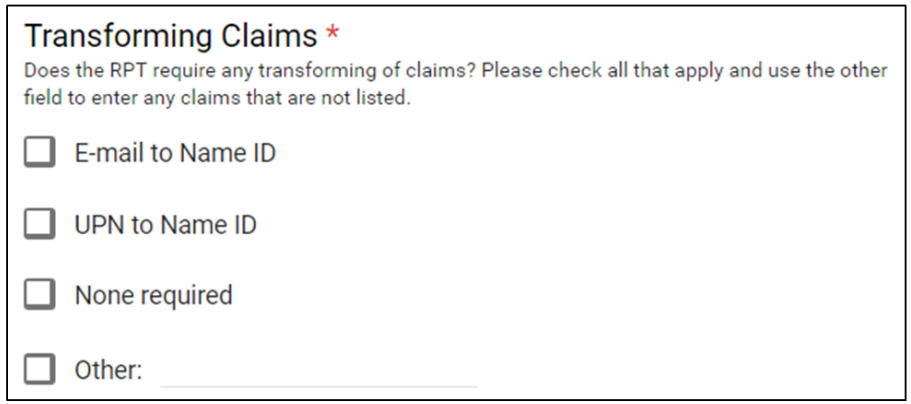
To answer this question note the example below:

Ex: User-Principal-Name ----> Name ID



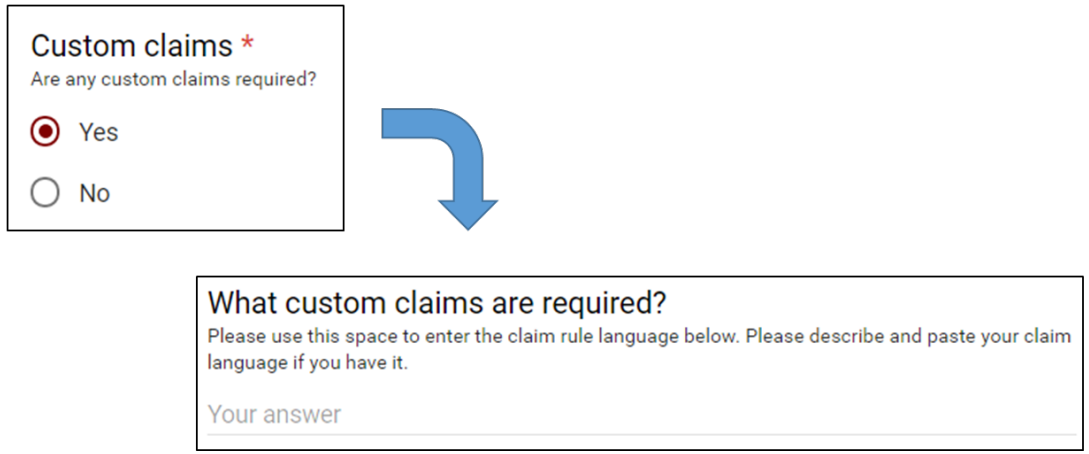
Section 3h) Transforming Claims

You can use **Transforming Claims** rules when you need to map an incoming claim type to an outgoing claim type and then apply an action that will determine what output should occur based on the values that originated in the incoming claim. When you use this rule, you pass through or transform claims that match the following rule logic, based on either of the options that you configure in the rule, as described in the following table. For more detailed information please see: https://technet.microsoft.com/en-us/library/ee913567(v=ws.11).aspx

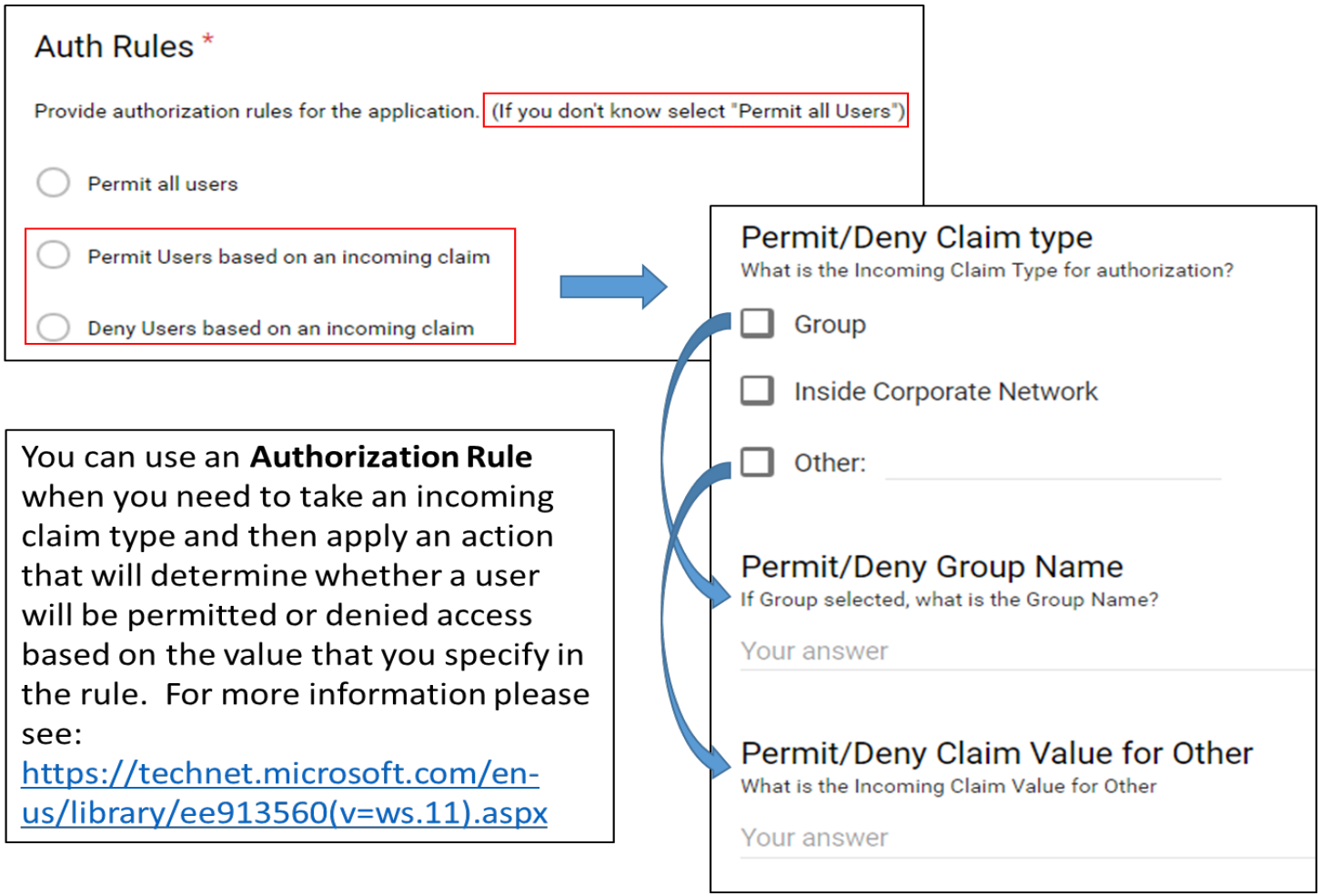


Section 3i) Custom Claims

You write a **custom claim** rule in Active Directory Federation Services (AD FS) using the claim rule language, which is the framework that the claims issuance engine uses to programmatically generate, transform, pass through, and filter claims. By using a custom rule, you can create rules with more complex logic than a standard rule template. For more detailed information please see: https://technet.microsoft.com/en-us/library/ee913558(v=ws.11).aspx



Section 3j) Authorization Rules



You can use an **Authorization Rule** when you need to take an incoming claim type and then apply an action that will determine whether a user will be permitted or denied access based on the value that you specify in the rule. For more information please see: https://technet.microsoft.com/en-us/library/ee913560(v=ws.11).aspx

Section 3k) Test URLs

Are Test URLs the same as Production? *
(If you don't know select yes)

- ○ Yes
- ◉ No

This question is asked in order to prevent you from having to enter information in twice.

The Test Environment is where all requirements are tested prior to going live to ensure that all requirements are met, there are no bugs in the code, etc. One all testing is complete the application can go live, by being placed in a Production Environment.

Endpoint URL *
What is the Service Provider (SP) Endpoint URL for test?

Your answer

Relying Party *
What is the Relying Party ID URLs for test?

Your answer

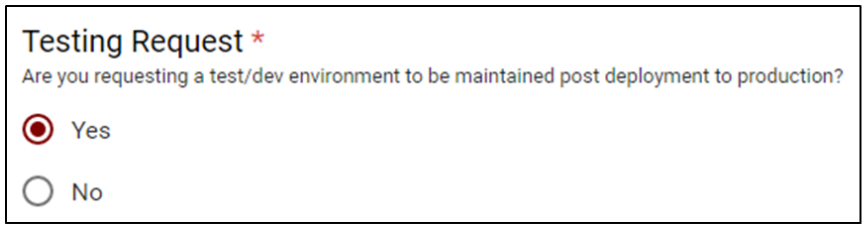
Redirect URL
Are there any redirect URLs required for test?

Your answer

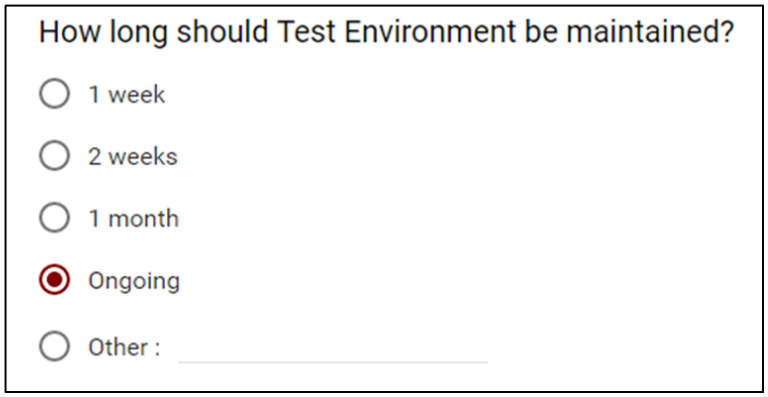
Testing Request *
Are you requesting a test/dev environment to be maintained post deployment to production?

- ○ Yes
- ○ No

Section 3l) Request to Maintain a Test Environment

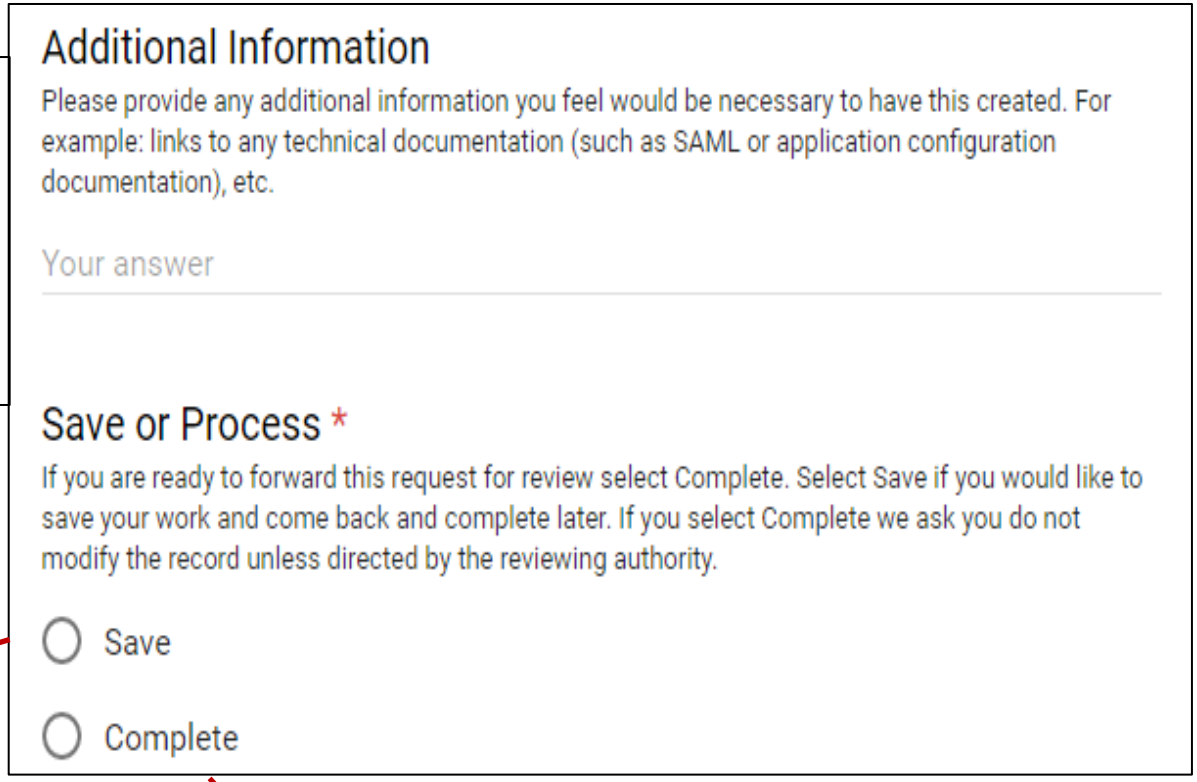


If you would like a Test Environment maintained after your application has gone into Production, you will give more information here.



Section 3m) Form End

This is the **end of the form**! Please provide any additional information you think would be helpful to the developers; e.g. links to technical documentation such as **SAML configuration documents.**

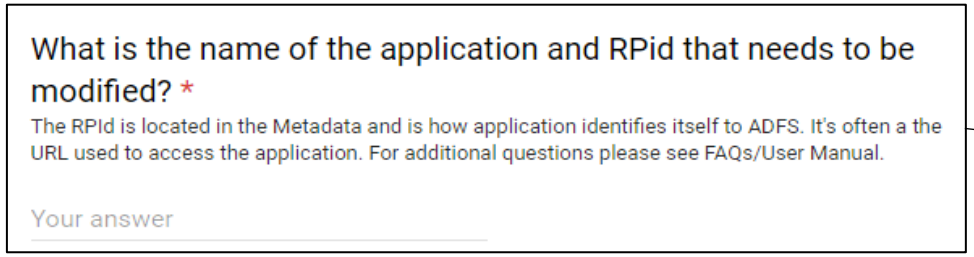


Select **Save** to save your work and come back to it later.

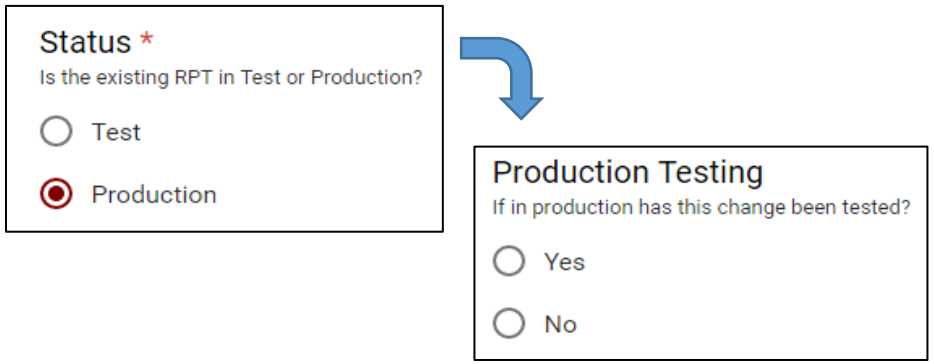
Select **Complete**, when you are ready to submit it for review to the ADFS team.
Note: Upon successful form submission, you'll receive an email with instructions on how to submit required attachments if you indicated you have exportable metadata or SHA256 certification.

Once you're ADFS RPT request has been reviewed **you'll receive a link to complete the ADFS Risk Assessment questionnaire** that must be completed prior to your application/service goes into production.

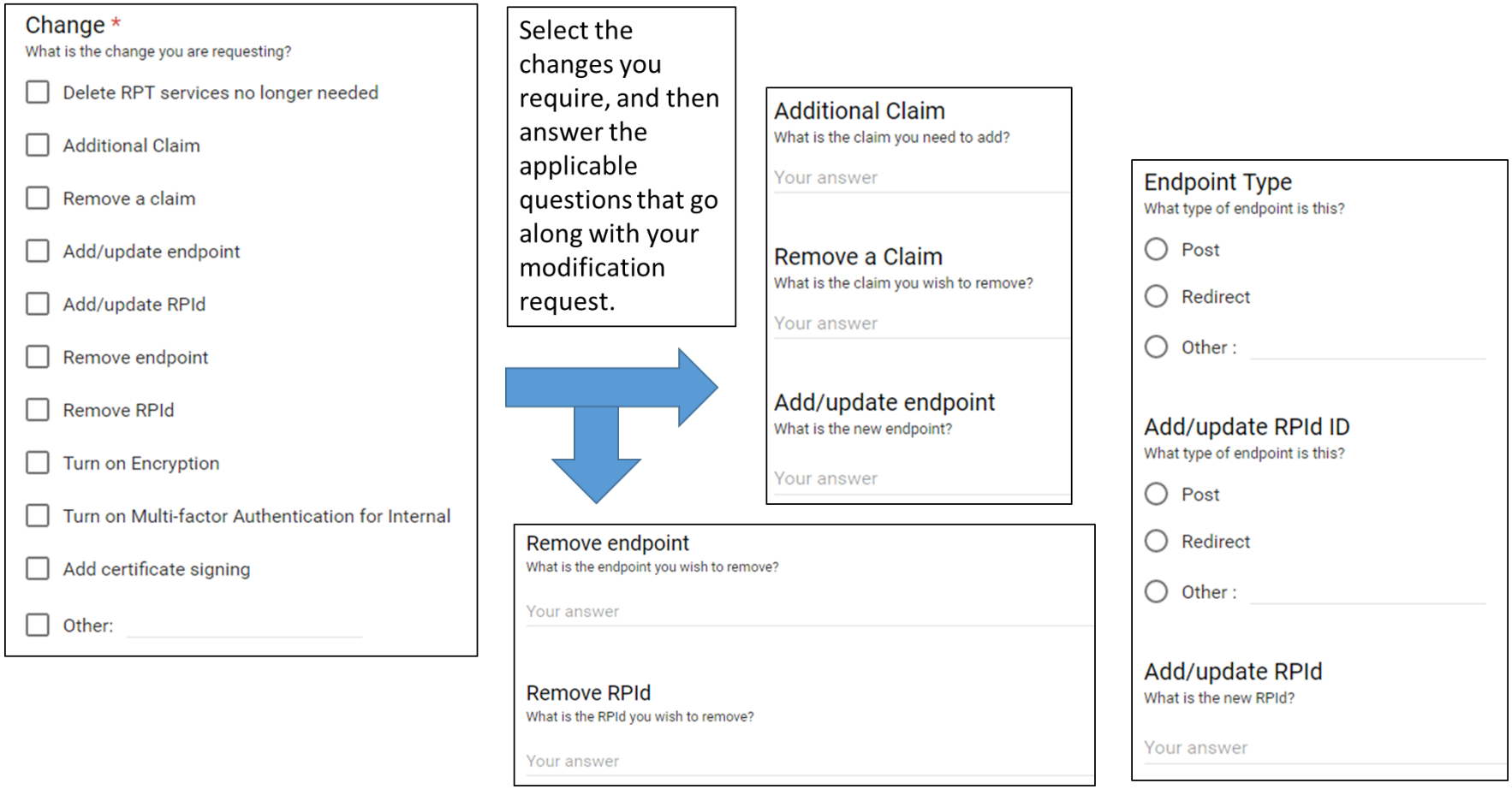
Section 4) Modification to an “Existing” Relying Party Trust (RPT)



The RPid is located in the Metadata, and is how the application identifies itself to ADFS. It is often the URL used to access the application.
The Rpid can be provided by whoever configured the application to SAML (this is often, but not always the vendor).



Section 4a) Modification Requirements



Section 5) Where to locate ADFS request form required information:

If you're not sure where to acquire the requested and/or required information to submit the ADFS RPT request form, please refer to the below table.

Information	Where to locate:
Authorization to Operate (ATO)	Your bureau's security office would have the application/system's ATO. The ATO refers to permission for a product to be used in an existing system.
Metadata	The vendor or application developer can provide this information. Metadata is defined as the data providing information about one or more aspects of the data; it is used to summarize basic information about data which can make tracking and working with specific data easier.
Does Application Support SAML?	The vendor or application developer can provide this information
Does Application Support SHA-256?	The vendor or application developer can provide this information
Test URLs same as Production URLs	The bureau/office point of contact or the vendor should have this information
The RPid	The RPid is located in the Metadata, and is how the application identifies itself to ADFS. It is often the URL used to access the application. The Rpid can be provided by whoever configured the application to SAML (this is often, but not always the vendor).
Custom claim rule	A claim rule that you author using the claim rule language to express a series of complex logic conditions. You can build custom rules by typing the claim rule language syntax in the Send Claims Using a Custom Rule template.
Where can I find help configuring ADFS 3.0 to communicate with SAML 2.0?	Please follow this link for detailed instructions: http://wiki.servicenow.com/index.php?title=Configuring_ADFS_3.0_to_Communicate_with_SAML_2.0
Where can I find help configuring ADFS 3.0 to communicate with Esri	Please follow this link for detailed instructions: https://doc.arcgis.com/en/arcgis-online/reference/configure-adfs.htm

ArcGIS Online?	
Where can I find help configuring SAML for WordPress?	Please follow this link for detailed instructions: https://support.onelogin.com/hc/en-us/articles/204353160-Configuring-SAML-for-WordPress