NextGen External User Management System (XMS) Overview

NextGen XMS – Capabilities

U.S. Department of Health and Human Services

NextGen XMS is a scalable, cloud-based solution that allows OpDivs to focus on their mission; and takes into consideration:

- Alignment with Digital Identity guidelines, ICAM and Cloud modernization efforts
- Security and compliance with federal standards (NIST, OMB, HHS EPLC requirements, etc.)
- Identity and Access Governance and delegated administration model
- Enterprise service that can secure access to external HHS applications
- Centralized platform that is flexible to integrate with third-party providers and services

Capabilities & Benefits

Secure Access:	***Allows external users to access protected applications using credentials issued by the General Services Administration's (GSA's) Login.gov or via other agency's PIV/CAC***
NIST 800-63-3 Compliance:	***IAL1, IAL2, and IAL3, and AAL2 and AAL3***
Identity Proofing/Delegated Proofing:	***Remote ID proofing using Login.gov; and delegated proofing for users that affiliate with an organization that's managed within NextGen XMS.***
Organization Affiliation:	***Ability to create organizations and manage affiliations to those organizations within NextGen XMS***
Access Requests/Approvals:	***Configurable access request framework for an application***
Organization Relationship Management:	***Ability to create organizations and manage affiliations to those organizations***
Accredited Platform and Helpdesk:	***NextGen ATO in place which includes Login.gov; no impact to integrated application's ATO, only ISA/MOU required***

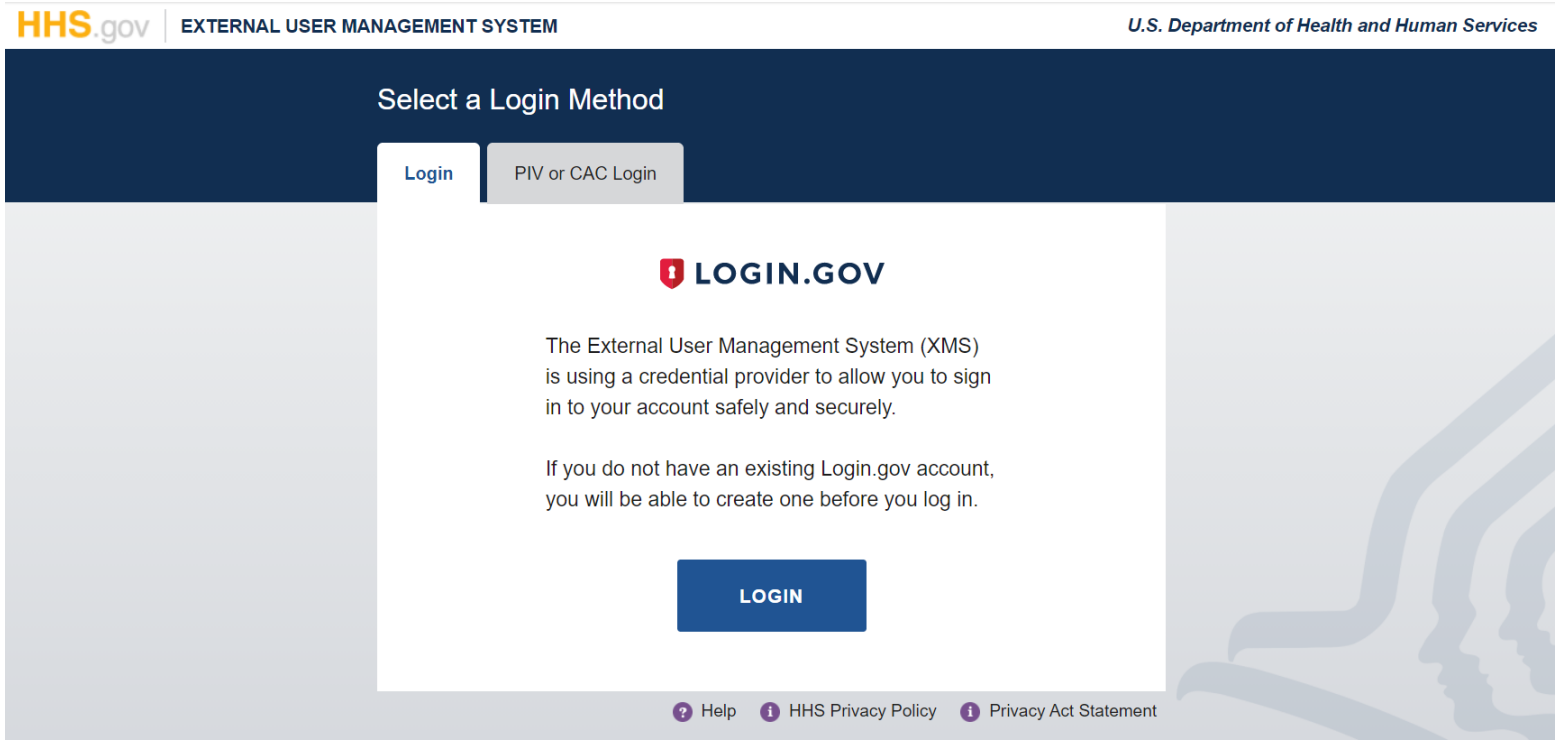
NextGen External User Management System (XMS) Overview

U.S. Department of Health and Human Services

The Authentication and Access Management services are supported via the NextGen External User Management System (XMS) across the external, non-HHS user community.

NextGen XMS Services:

- Authentication Services[1]
- Identity, Account, and Entity Management Services[2]
- Data Services[3]



[1] **Simplified Sign-On & Federation Capabilities**

[2] **Application Account and Entity Linking Capabilities**

[3] **Reporting and Auditing Capabilities**

NextGen XMS – Factors of Authentication

U.S. Department of Health and Human Services

In alignment with NIST 800-63-3 guidelines, NextGen XMS offers:

Identity Assurance Levels

IAL 1

Little or no confidence in asserted identity

No requirement to link the applicant to a specific real-life identity.

IAL 2

Some confidence in asserted identity

Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity.

IAL 3

High confidence in asserted identity

Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP

Authenticator Assurance Levels

AAL 2

High confidence in user ownership of credentials

Provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account.

AAL 3

Highest confidence in user ownership of credentials

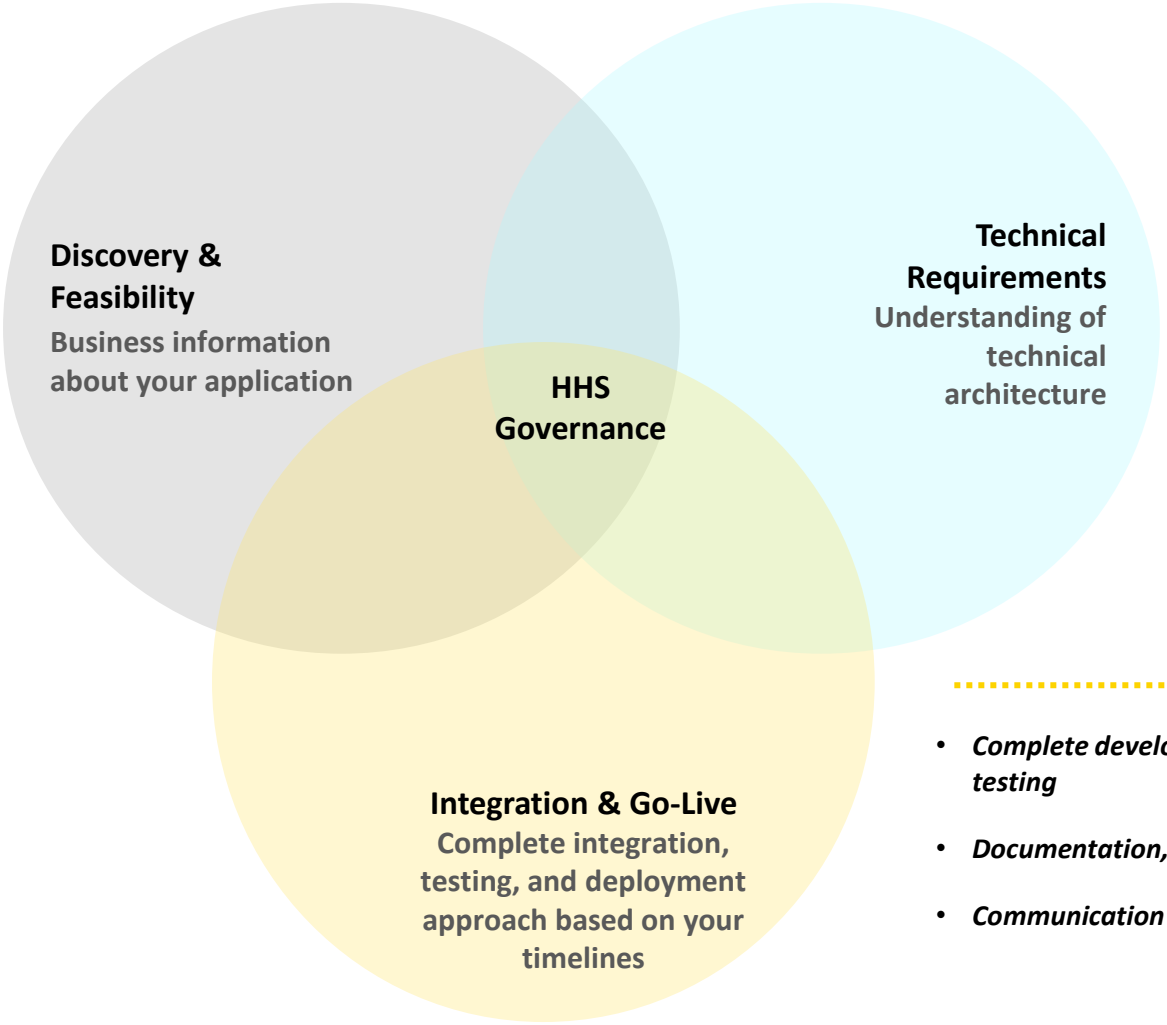
Provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account.

NextGen XMS – Integration Approach

U.S. Department of Health and Human Services

HHS Governance considerations include:
Enterprise Performance Lifecycle (EPLC), Interconnect Security Agreement (ISA)/Interagency Agreement (IAA), Security Reviews, Change Management, Customer Impact, and Enterprise Architecture Reviews

- ***Describe the user population that use your application? E.g.; citizens, state or local government, universities, private institutions***
- ***What is your current registration process and access requirements?***
- ***Do you require users to go through identity proofing?***
- ***What are typical user volumes?***

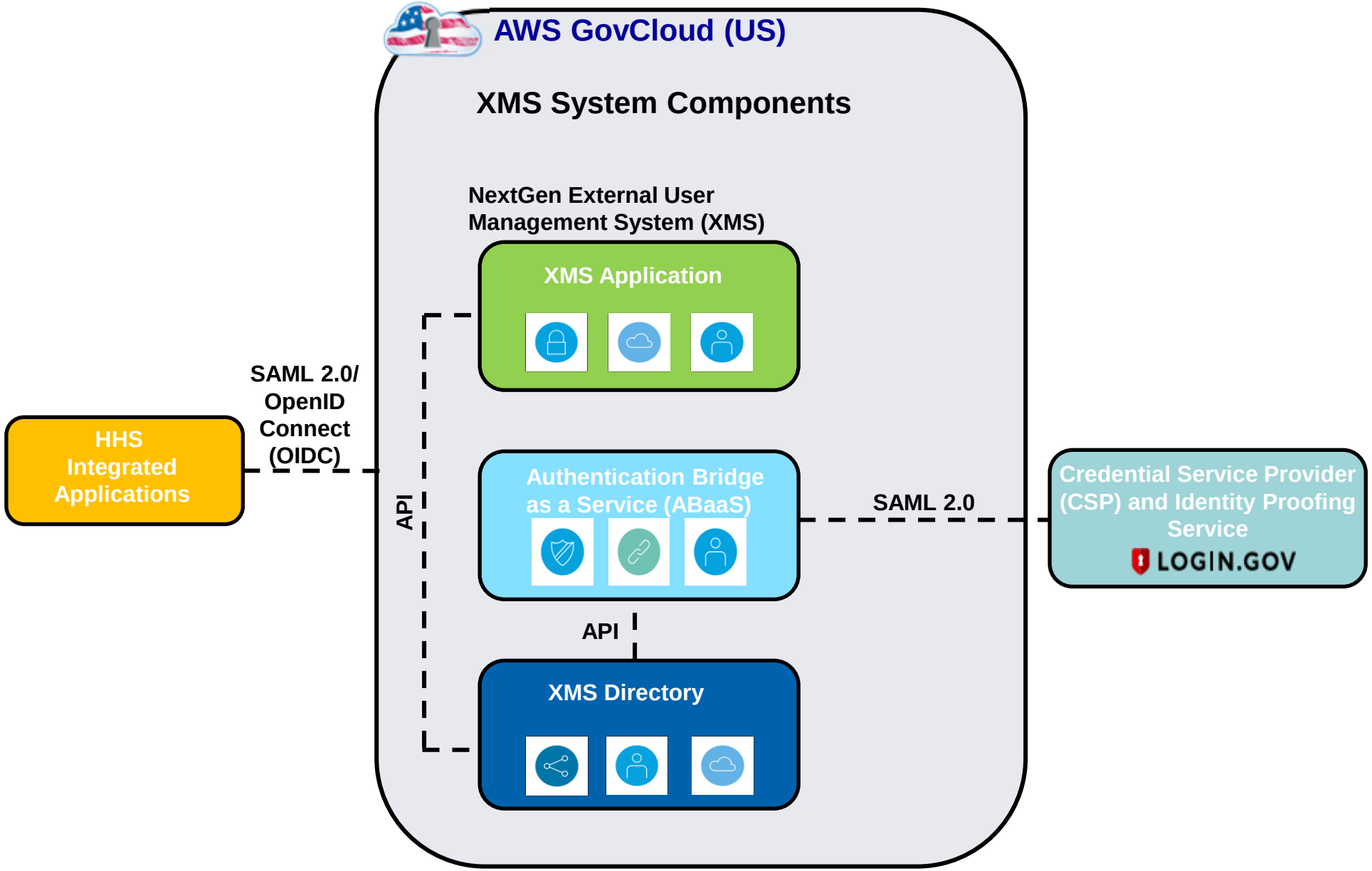


- ***Does you application support standard protocols like SAML 2.0 or OpenID Connect (OIDC)?***
- ***Is it a SaaS, Cloud Hosted, or on-Prem architecture?***

- ***Complete development and testing***
- ***Documentation, ISA, MOU***
- ***Communication planning***

NextGen XMS – High Level Architecture

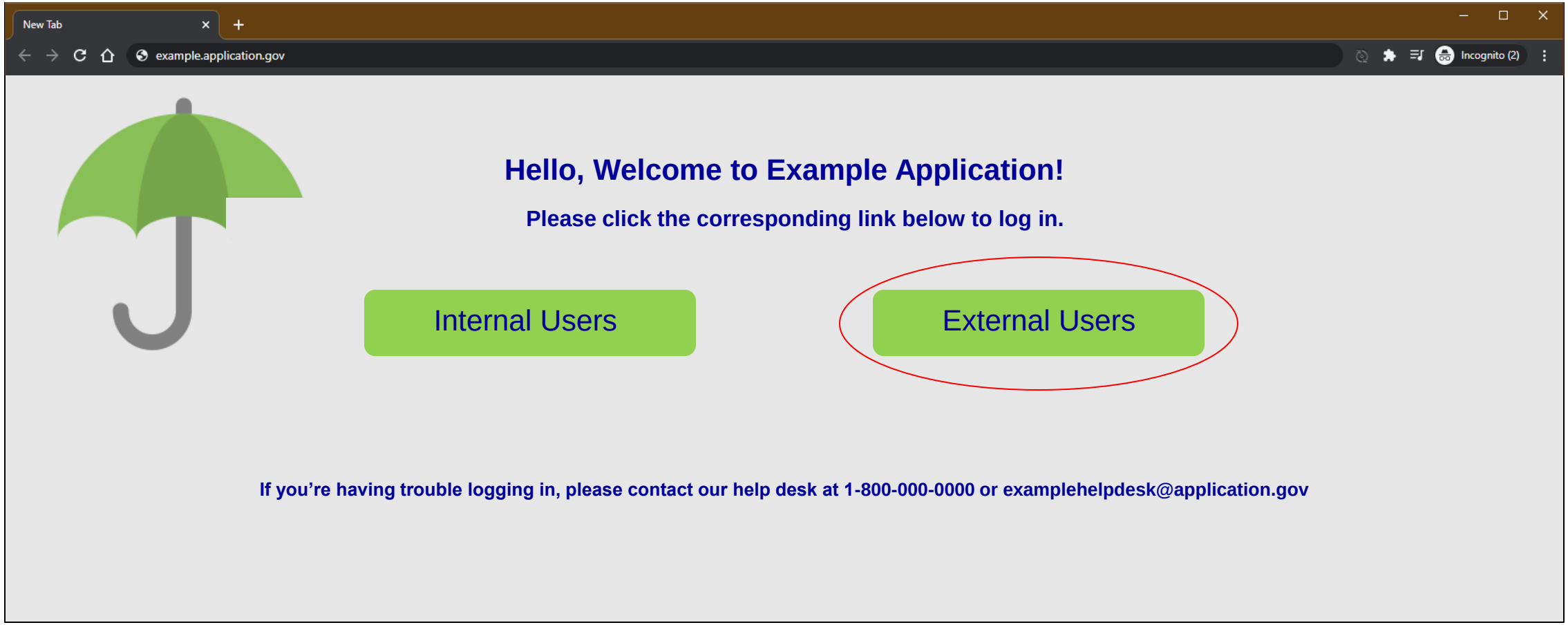
U.S. Department of Health and Human Services



NextGen XMS Walkthrough – Typical Login Flow

U.S. Department of Health and Human Services

When unauthenticated users arrive at the Target Application's URL, generally they are presented a "Login Page" showing options to login. For applications that have both internal and external users who authenticate at different levels through different systems, the login page may look something like this:

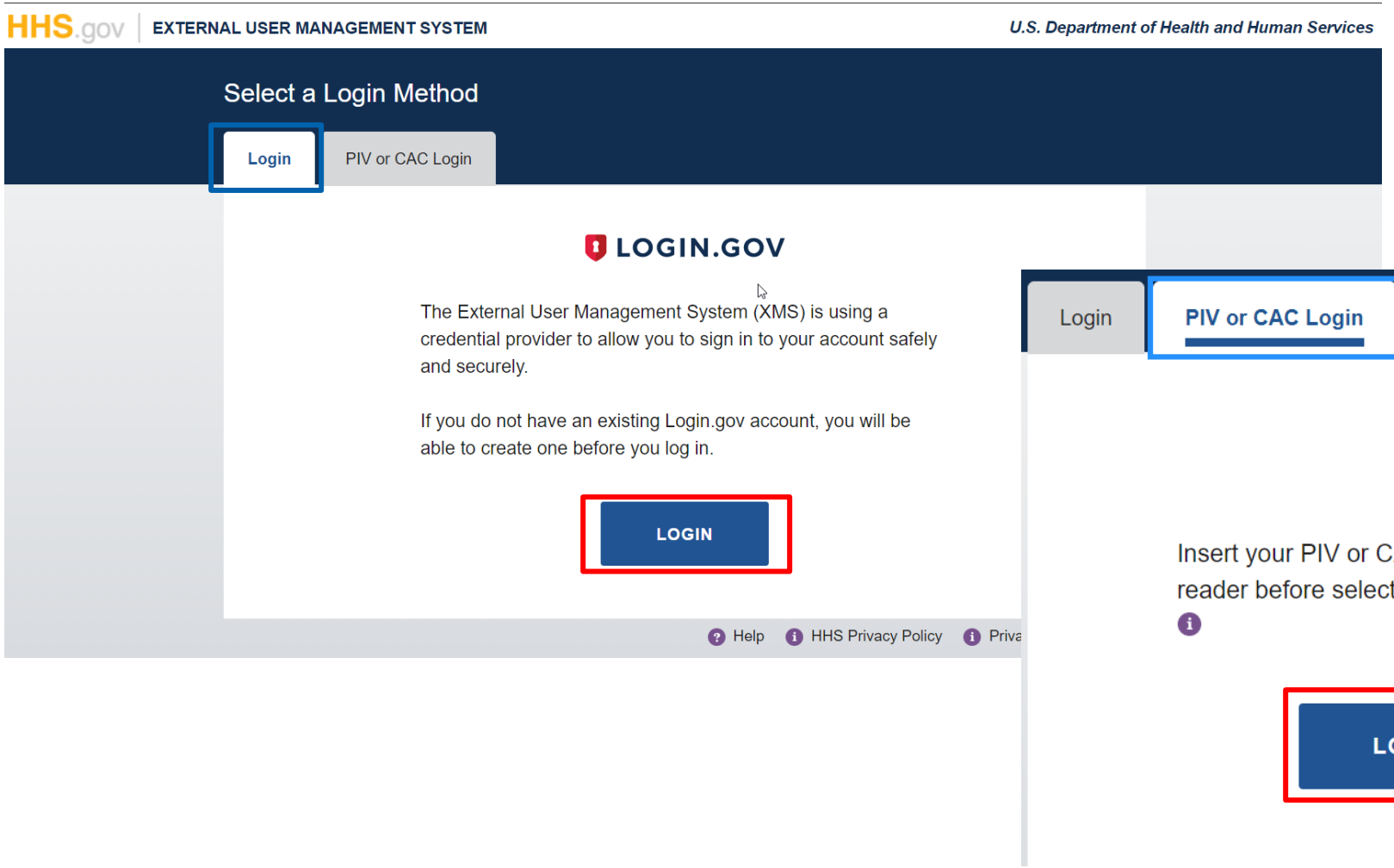


NextGen XMS Walkthrough – Typical Login Flow

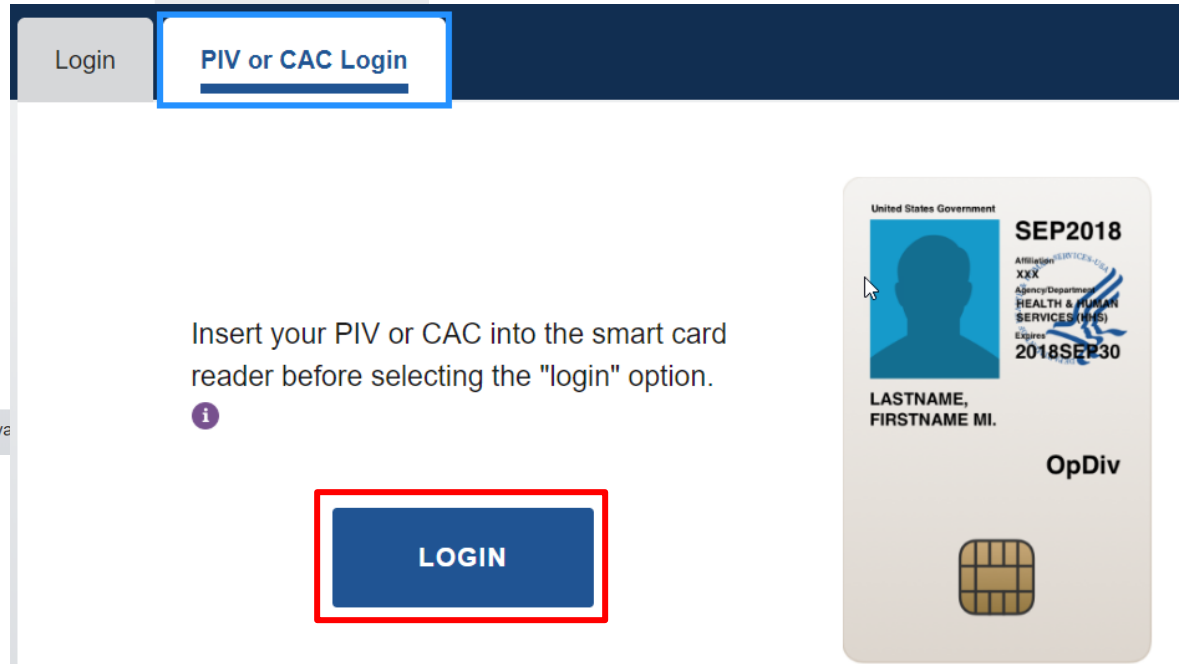
U.S. Department of Health and Human Services

The ‘External Users’ button on the previous page will kick off the authentication flow with XMS, and the user will be redirected to the XMS Login Page and asked to authenticate with one of the available options below.

Login.gov credentials:



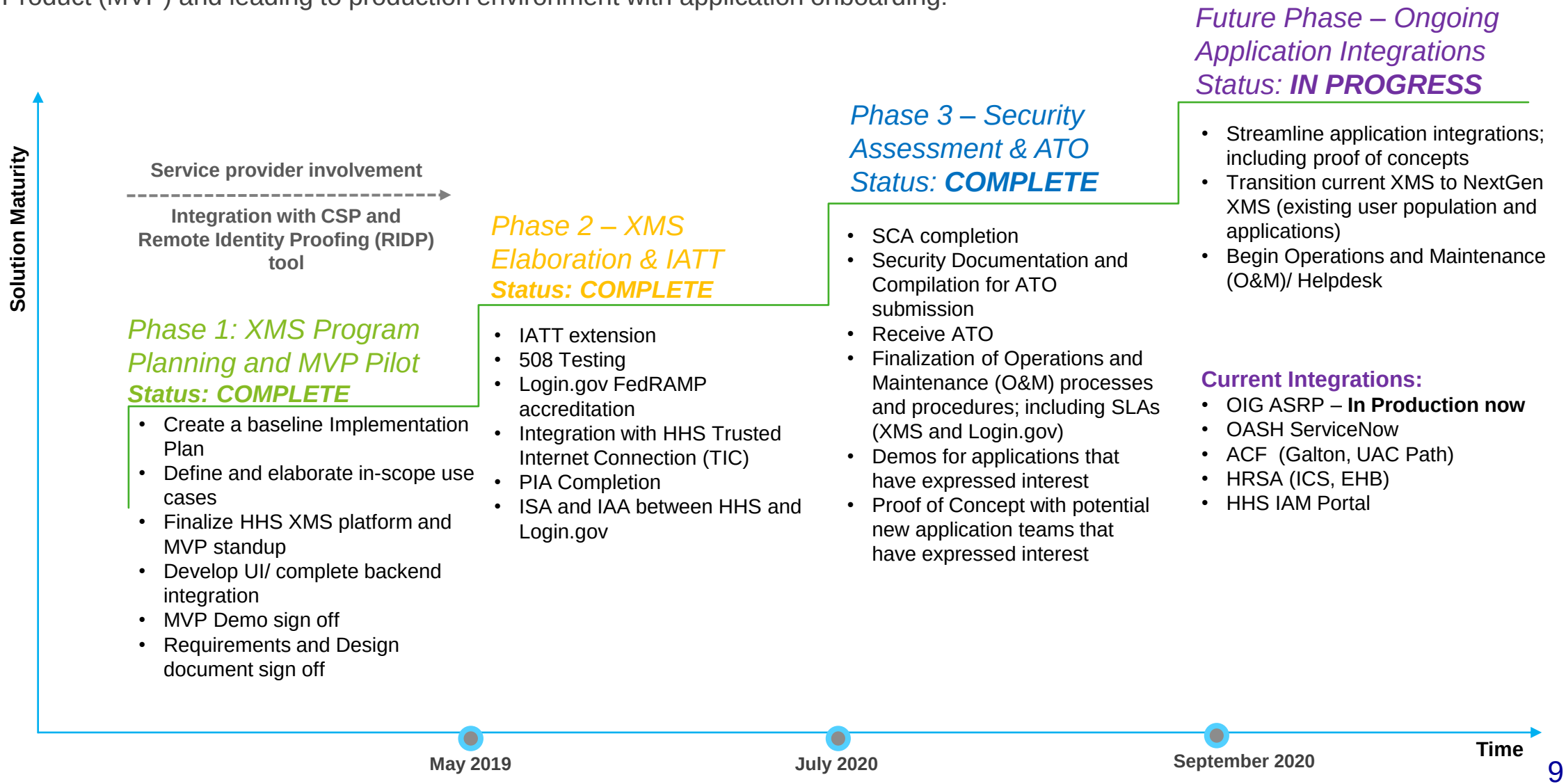
PIV/CAC credentials:



NextGen XMS Roadmap – Phased Approach

U.S. Department of Health and Human Services

This effort is broken into multiple phases which will continuously deliver incremental business value starting with the Minimally Viable Product (MVP) and leading to production environment with application onboarding:



Questions?

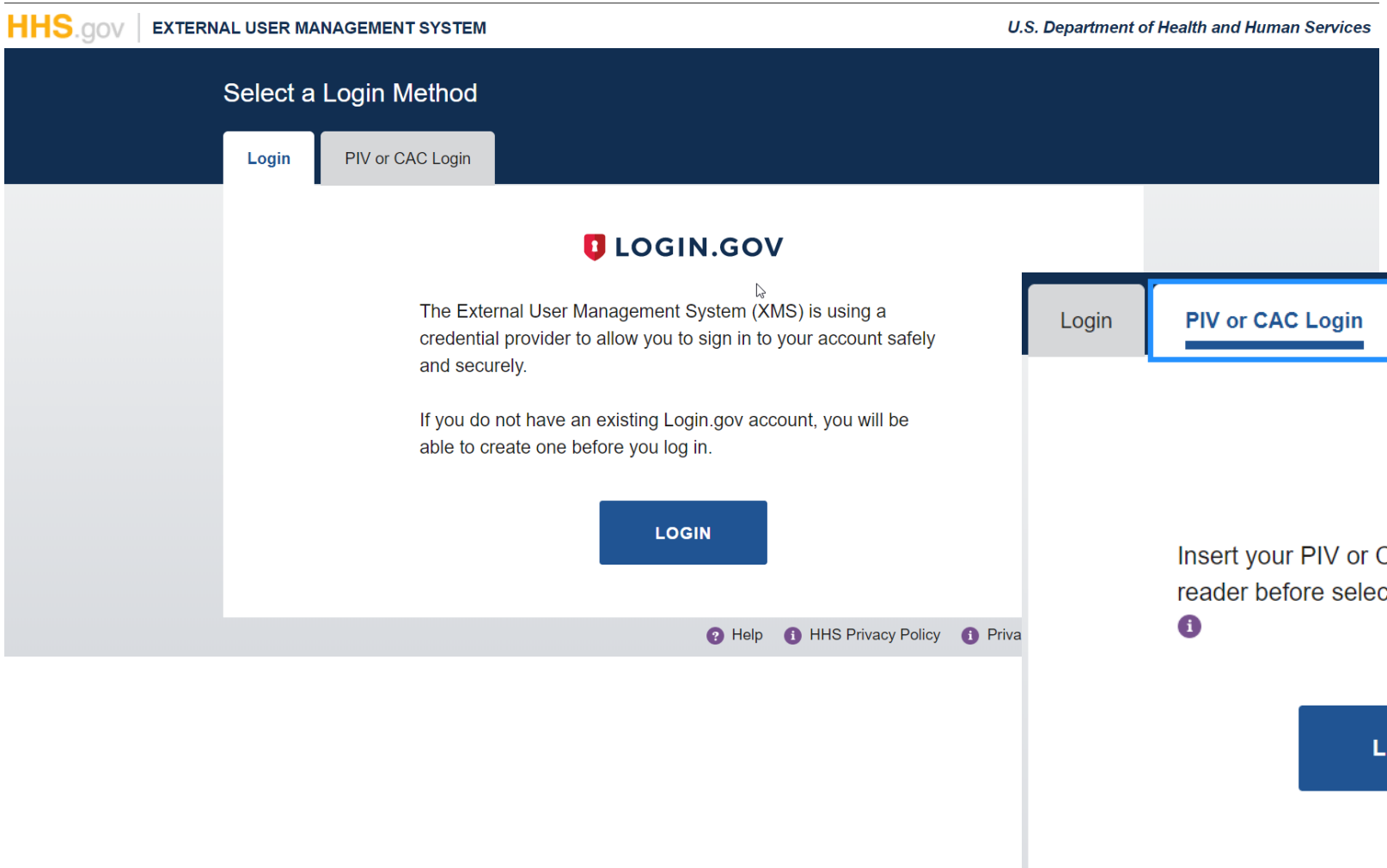
NextGen XMS Walkthrough

NextGen XMS Walkthrough – Login Page

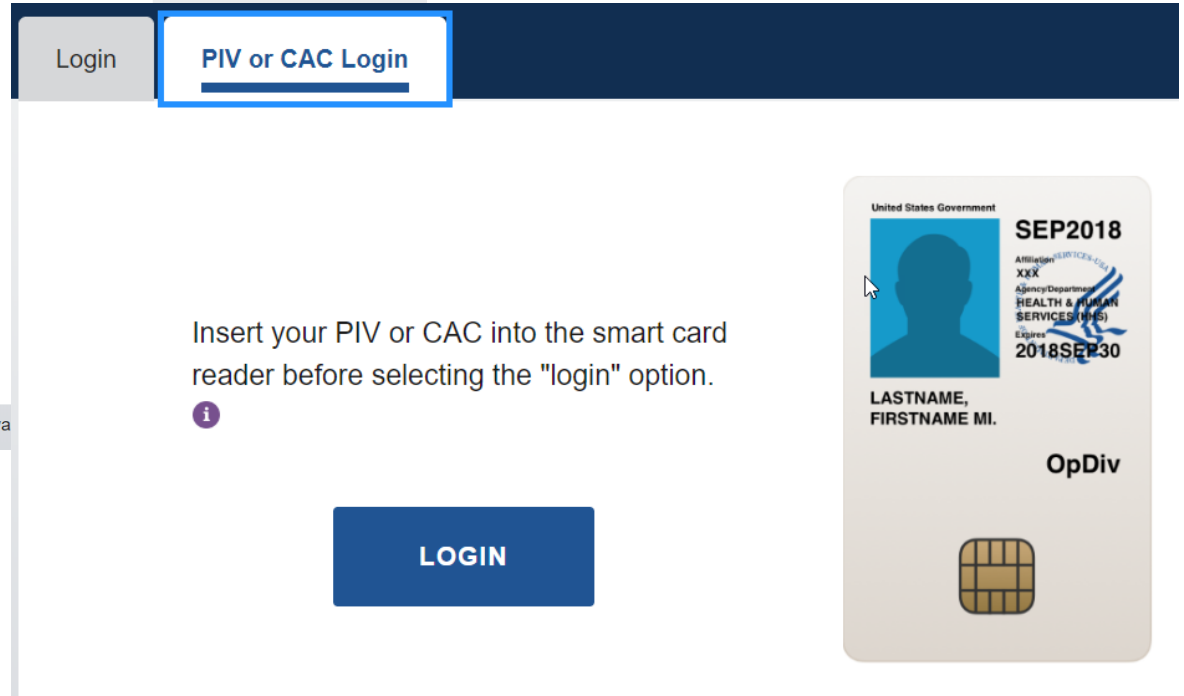
U.S. Department of Health and Human Services

Users have one of two options for authenticating into XMS:

Login.gov credentials:



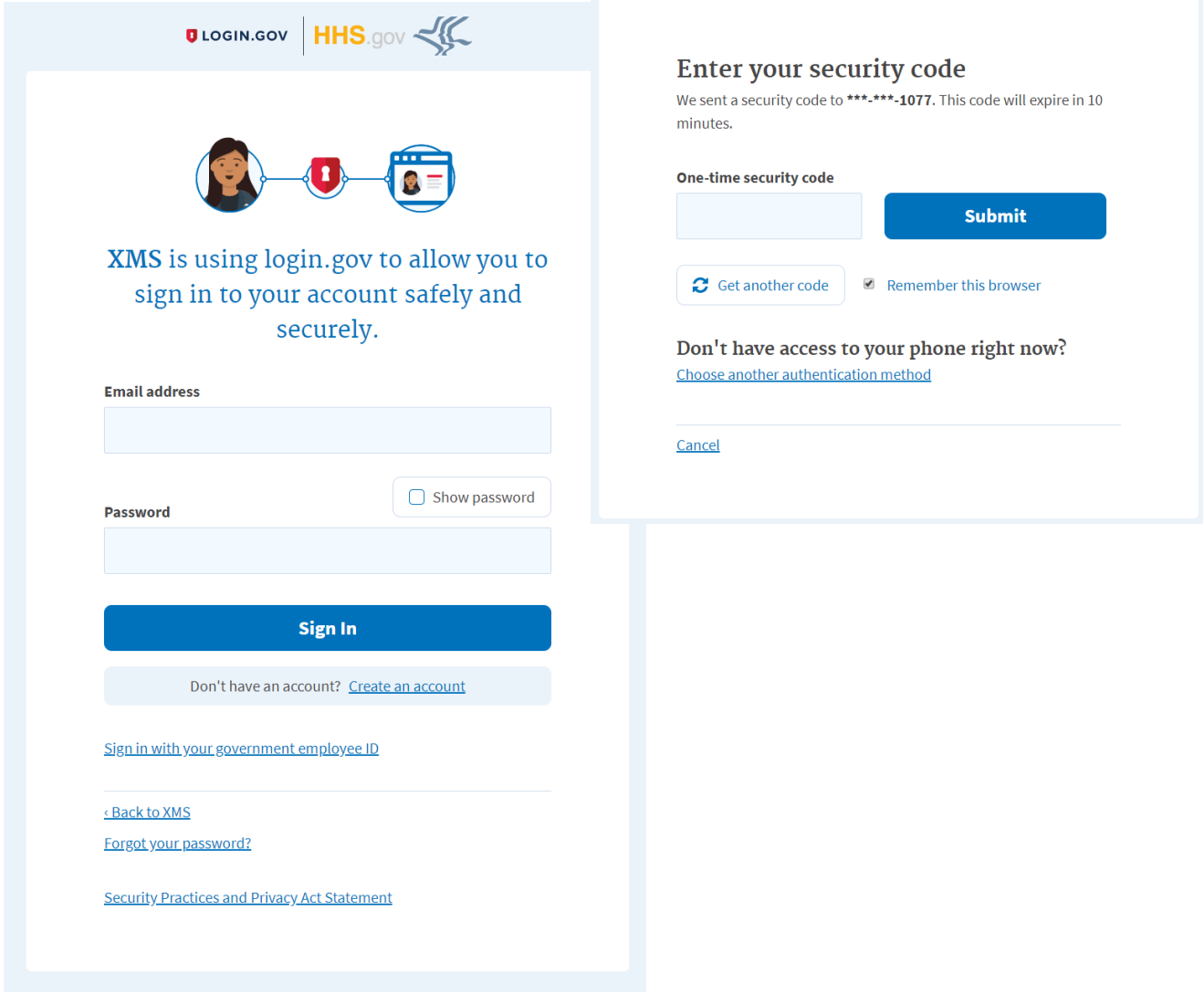
PIV/CAC credentials:



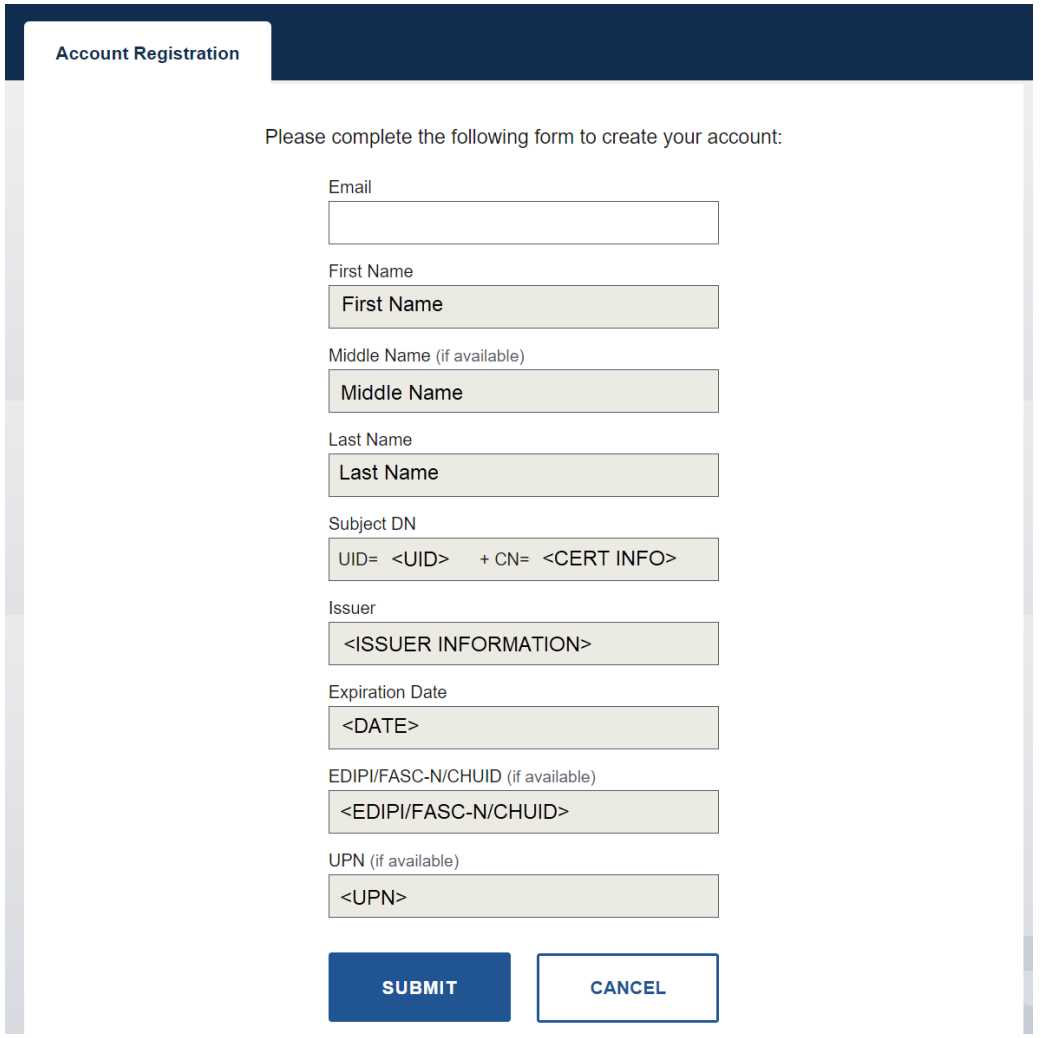
NextGen XMS Walkthrough – Logging In via Login.gov or PIV/CAC

U.S. Department of Health and Human Services

Users will be redirected to Login.gov's landing page to enter their credentials and second factor of authentication:



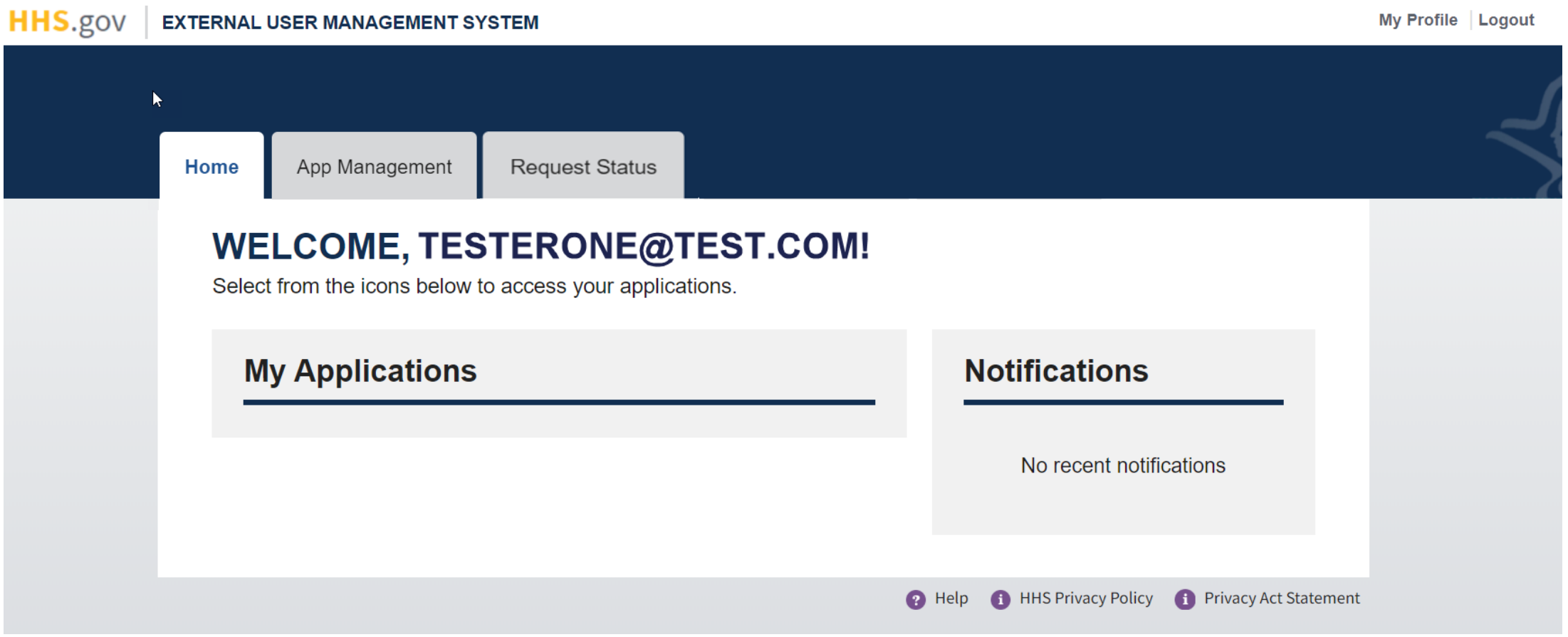
Users will be directed to register their PIV/CAC upon first-time log in to show ownership of account:



NextGen XMS Walkthrough – User Dashboard

U.S. Department of Health and Human Services

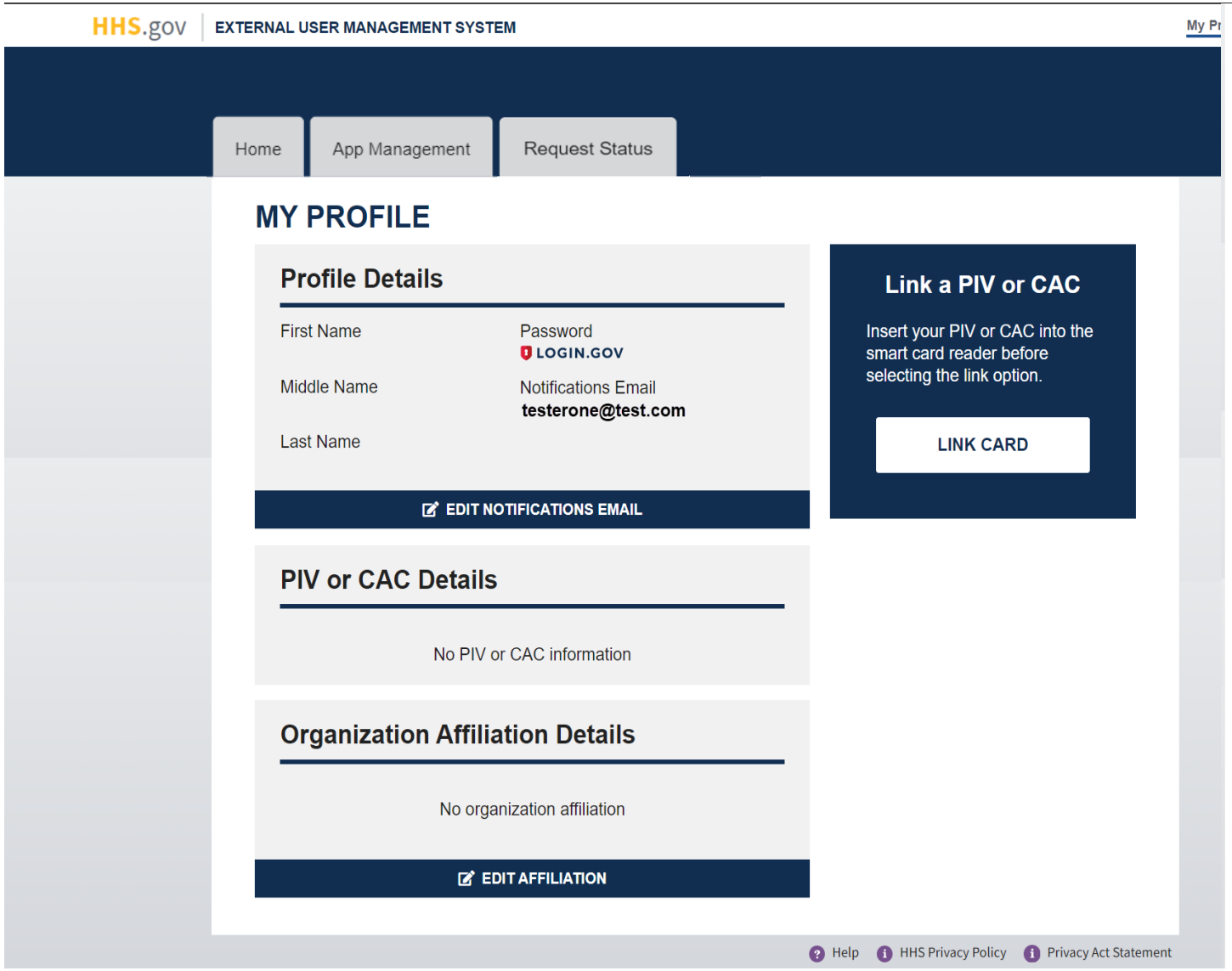
Upon successful authentication, users will be taken to their dashboard:

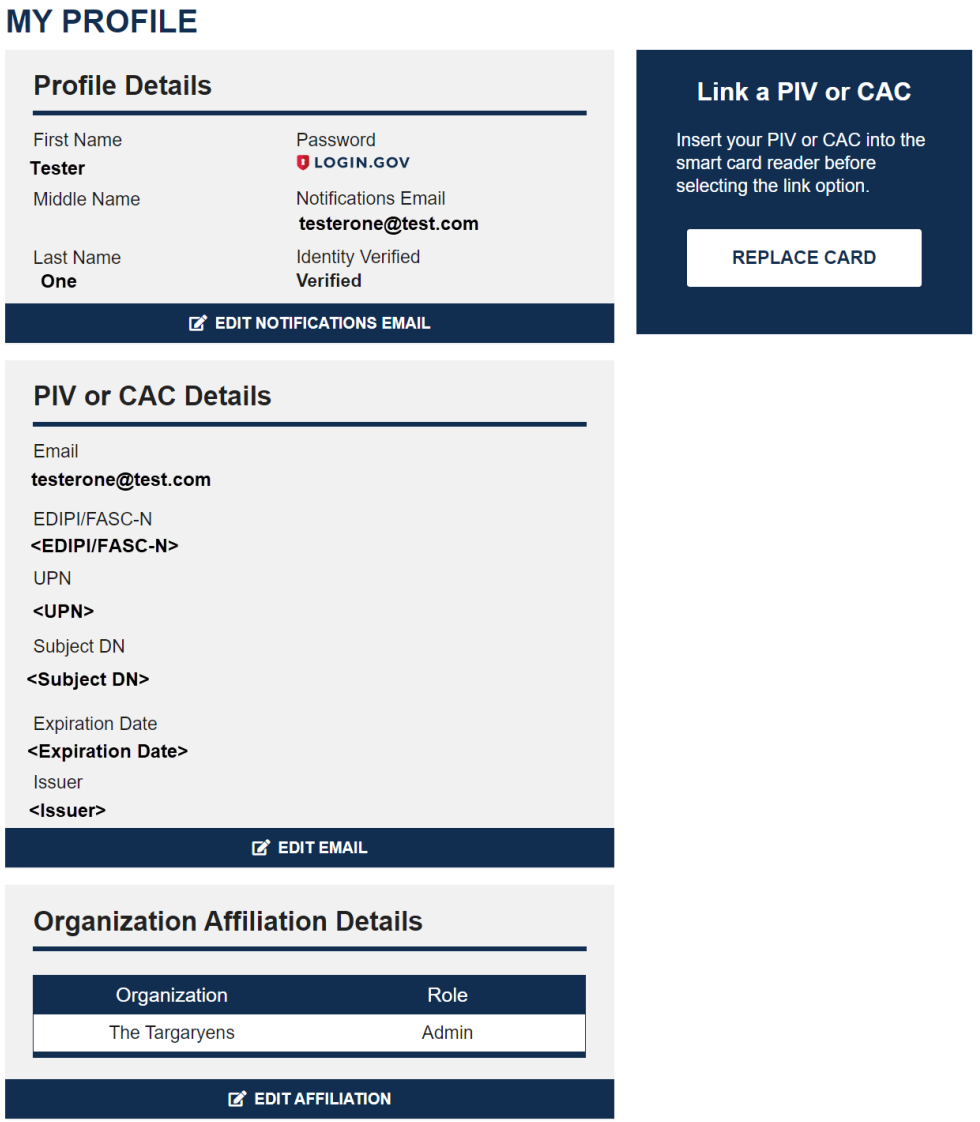


NextGen XMS Walkthrough – My Profile

U.S. Department of Health and Human Services

From the My Profile page, users will have the option to update their profile, or request affiliation with an organization:

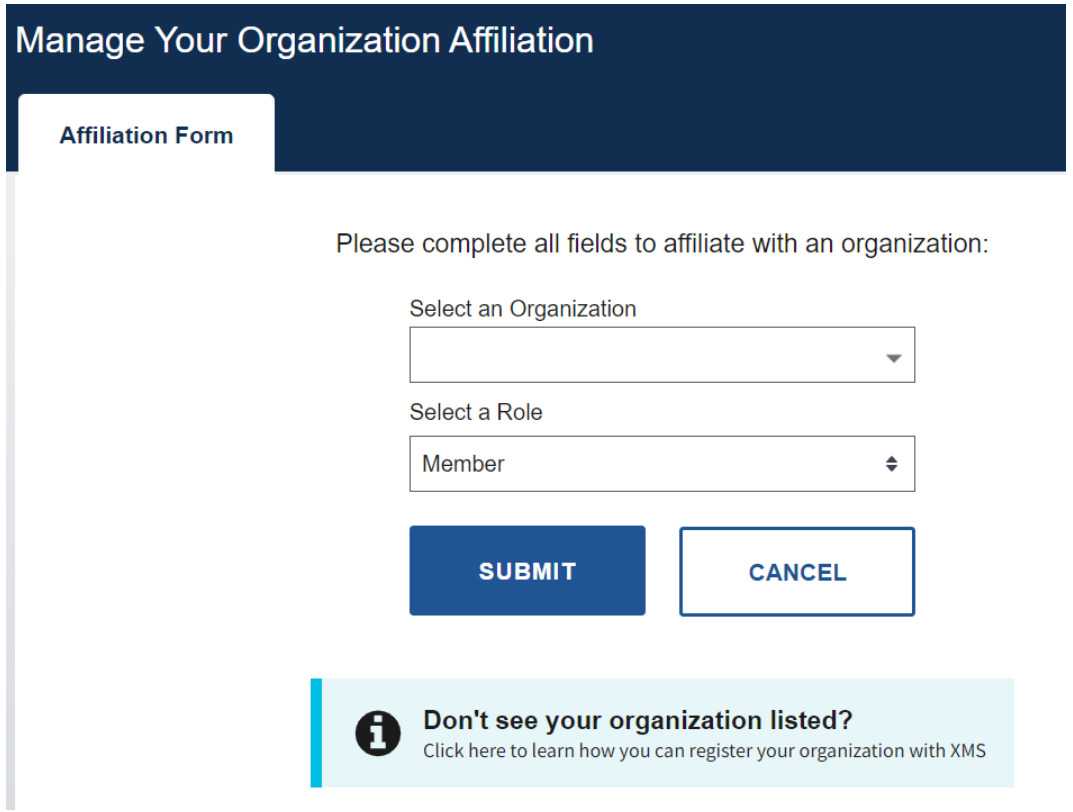


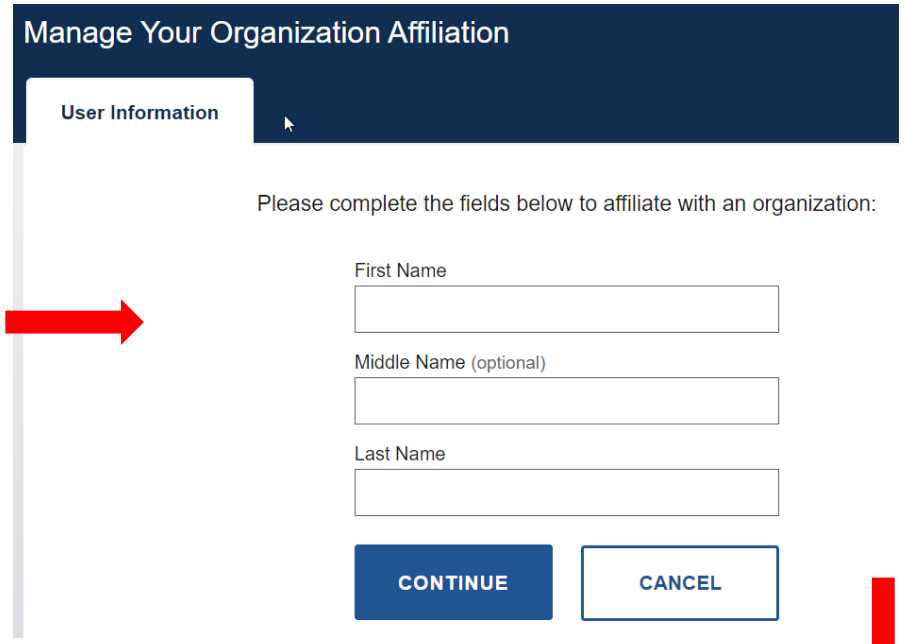


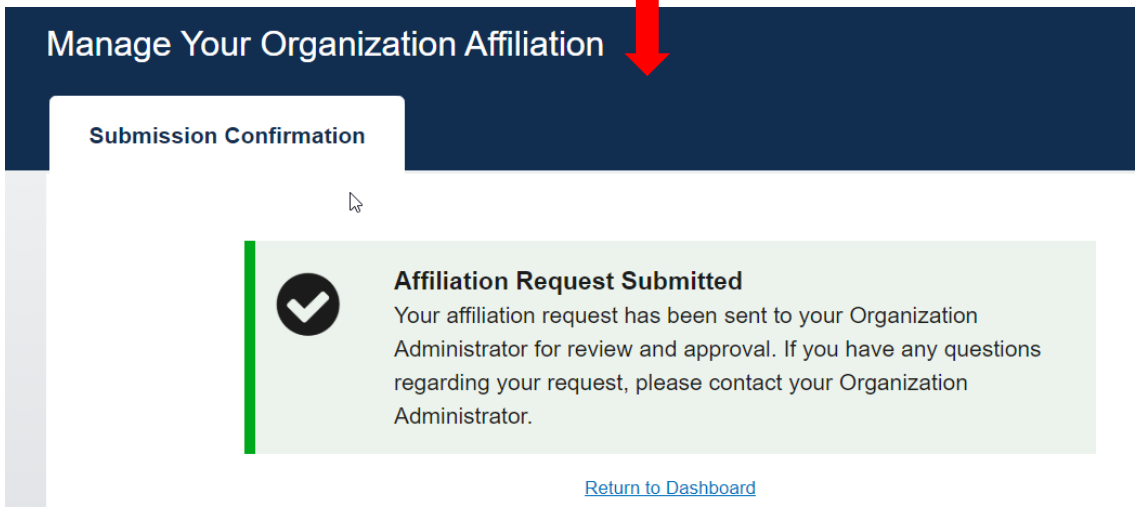
NextGen XMS Walkthrough – Affiliation Requests

U.S. Department of Health and Human Services

From the Organization Affiliation page, you may request to affiliate as a member or an administrator for an organization:







NextGen XMS Walkthrough – Organization Registration Request

U.S. Department of Health and Human Services

Users requesting to register an organization must perform identity proofing, understanding rules for submitting request:

Identity Proofing

As part of the Organization or Organization Administrator registration process, you are required to undergo identity proofing. For users that do not have a PIV or CAC, please follow the instructions on the following screens. **For users with a valid and active PIV or CAC, insert your card into a smart card reader before selecting the "Continue" button.**

Select a method of identity proofing from the options below:

- (●) I have a PIV or CAC
- ( ) I do NOT have a PIV or CAC

CONTINUE CANCEL

Registration Information

Organization Administrator FAQ

If your organization has not been registered with the External Management System (XMS), you or another employee of your organization will need to complete the registration process before being able to access organizational features. General information regarding the organization registration process is outlined below:

Who can complete the organization registration process?

Anyone who is an employee of the organization being requested and has a valid PIV or CAC is able to complete the process. The user completing the registration process will also be required to become the Organization Administrator, which involves successfully completing an identity proofing process (more information can be found by clicking the Organization Administrator FAQ link on this page).

What information is needed to complete the process?

A Federal Sponsor's first name, last name, and email address are required. If you do not have access to this information, you can either gather the required information from someone within your organization, or inform another employee who does know the information to complete the organization registration process from their XMS account.

CONTINUE CANCEL

Terms and Conditions

Please read the following terms and conditions carefully before continuing with the registration process.

All individuals that are creating an organization (or entity) with in the NextGen External User Management System (XMS) must comply with the following terms and conditions:

Ownership

XMS is the property of the U.S. Department of Health and Human Services (HHS), and is for authorized users only. The system is for official federal government business only. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative penalties.

Responsibilities

As the person creating or registering the organization with XMS, you are responsible for maintaining the integrity of, and are held accountable for, everything done within and on behalf of this organization.

Organization Registration

By registering this organization in XMS, you are attesting that the organization being created is a legal and real entity, subject to all federal and state laws. Information entered into XMS shall

☐ I acknowledge and understand my responsibilities and agree to comply with the Terms and Conditions Agreement for XMS

CONTINUE CANCEL

Complete Registration Request

Registration Form

Please complete the following form to continue the registration process:

Organization Name

Organization Classification

- Select -

Federal Sponsor Name

Federal Sponsor Email

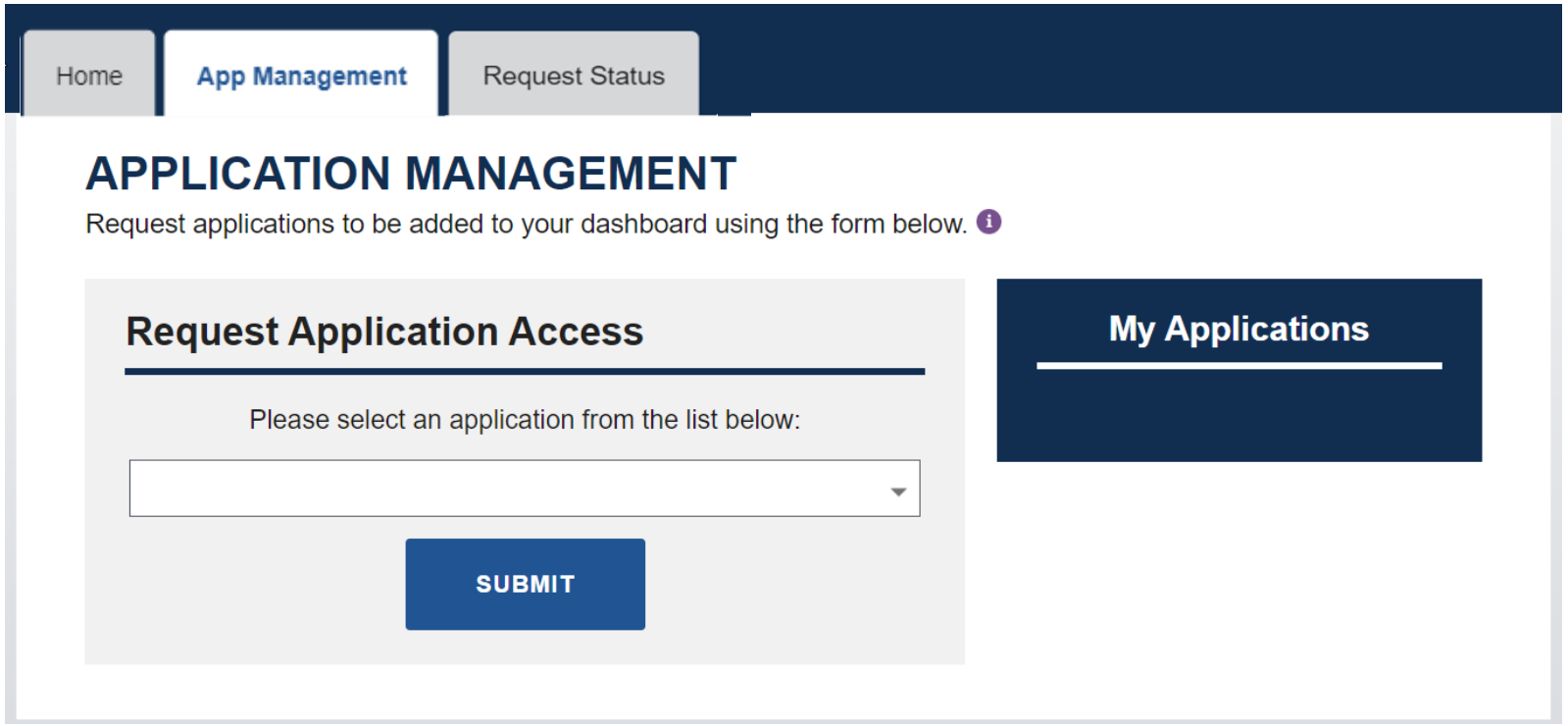
Business Justification (max. 2,000 characters)

SUBMIT CANCEL

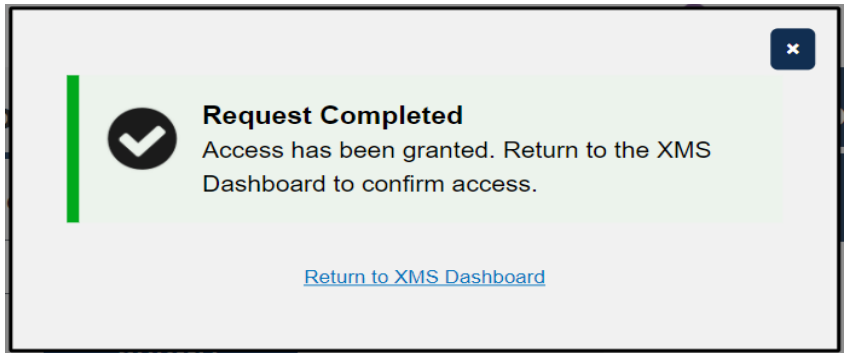
NextGen XMS Walkthrough – Application Access Request

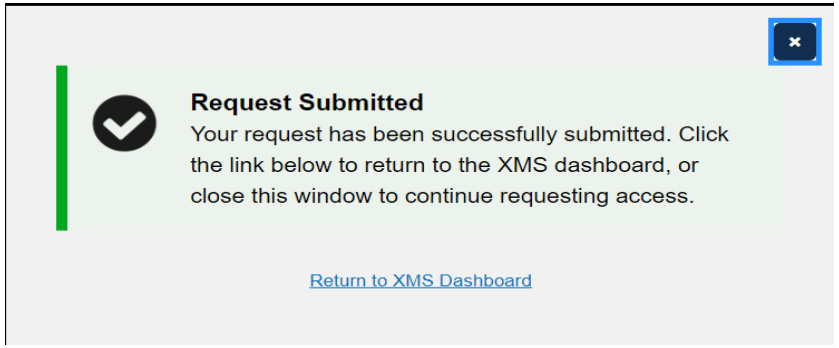
U.S. Department of Health and Human Services

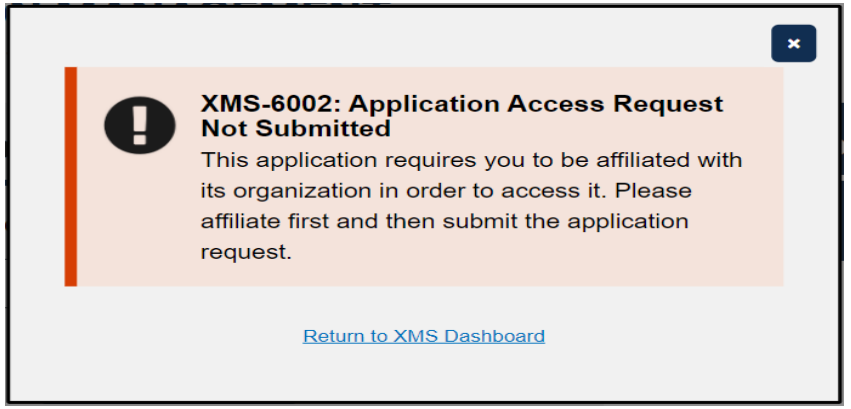
From the Application Management tab, you may request access to an application:



Sample configurations:



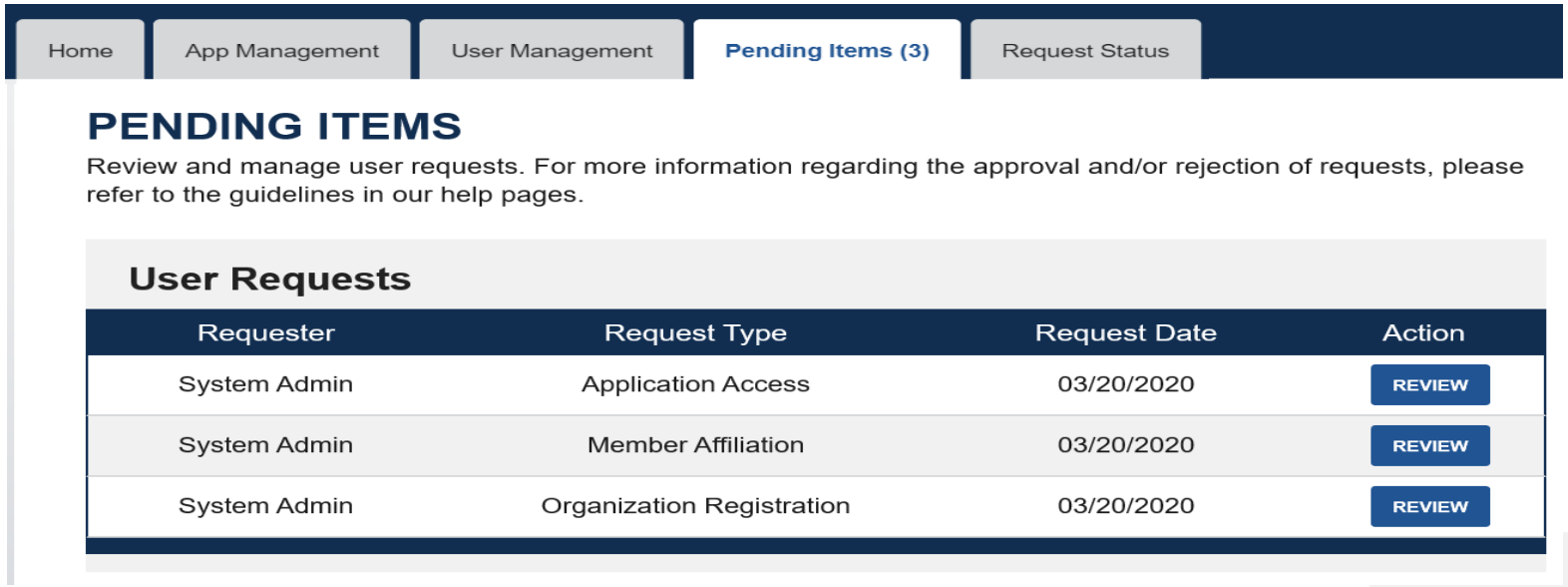




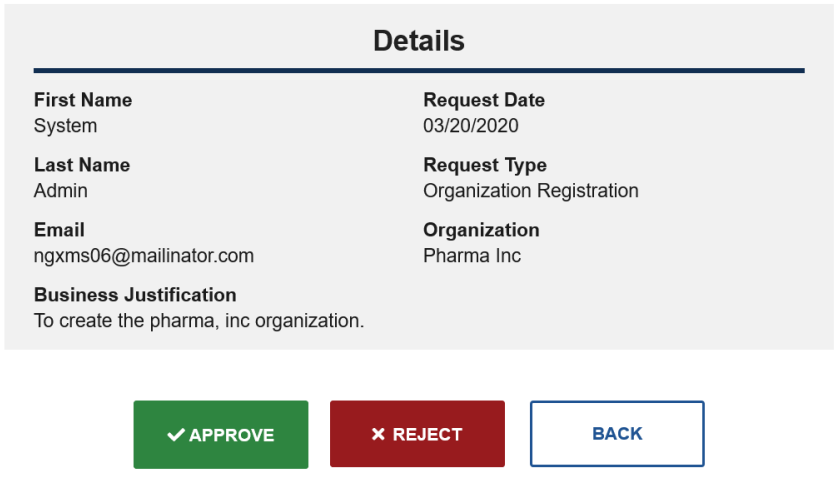
NextGen XMS Walkthrough – Approvals

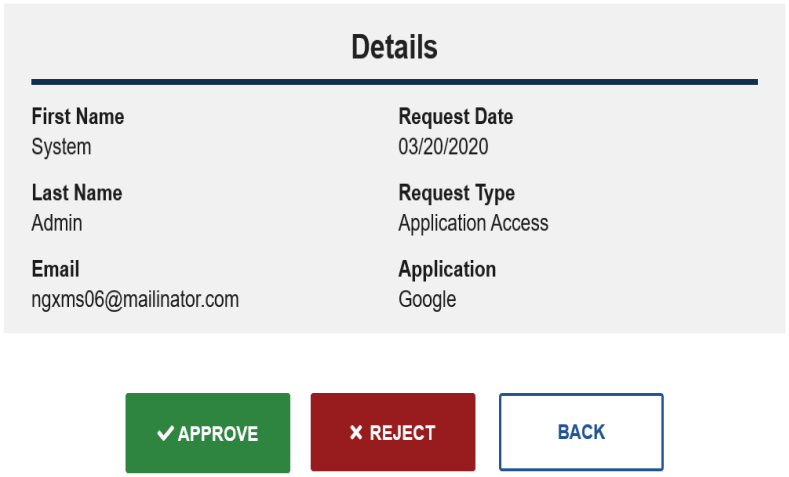
U.S. Department of Health and Human Services

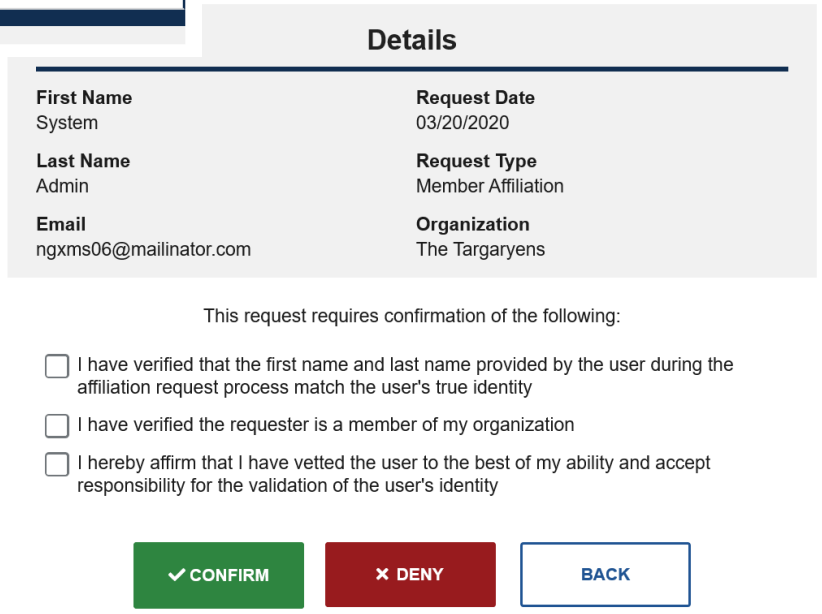
From the Pending Items tab, users can review and act upon requests submitted to them:



Sample Approval Requests:



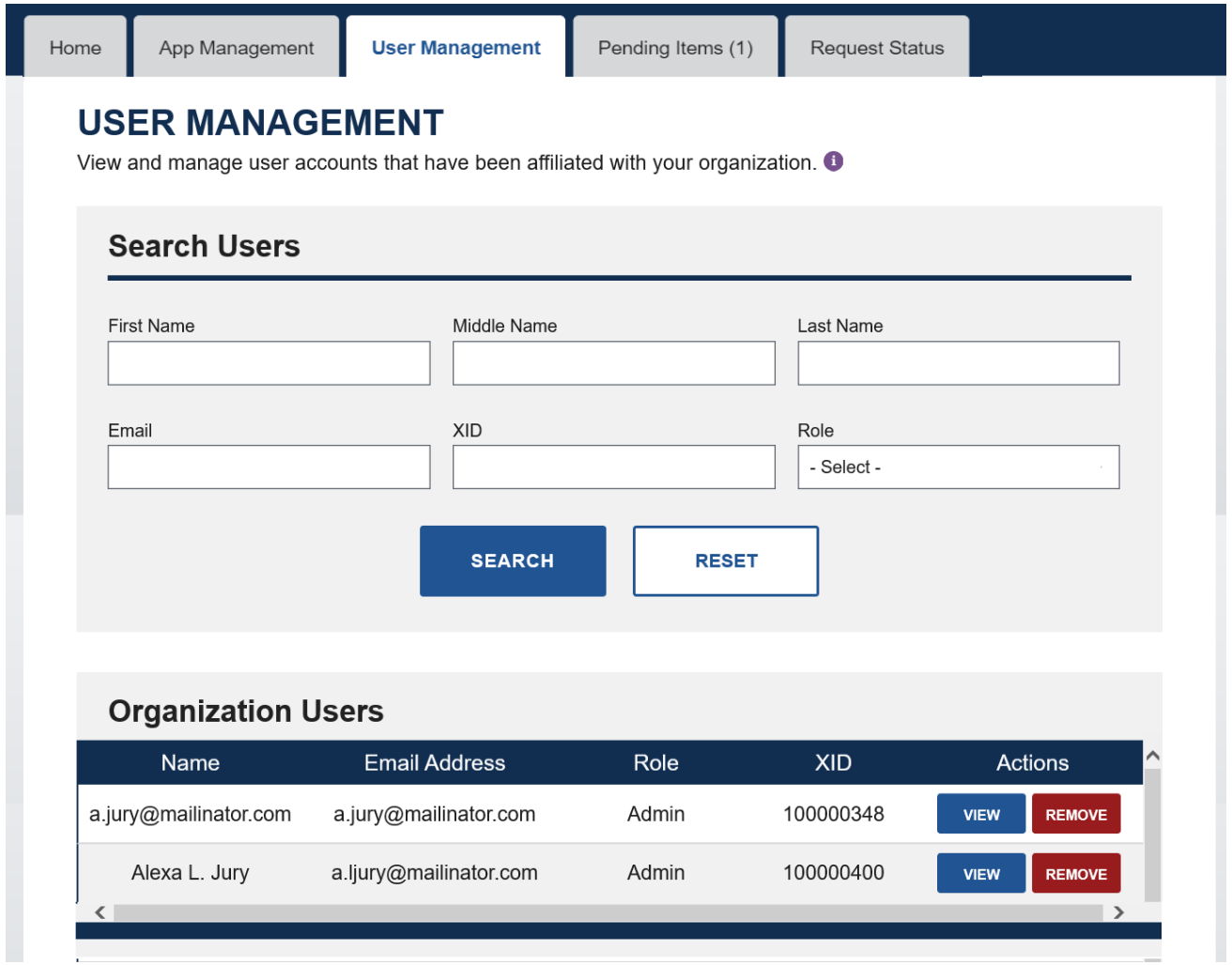


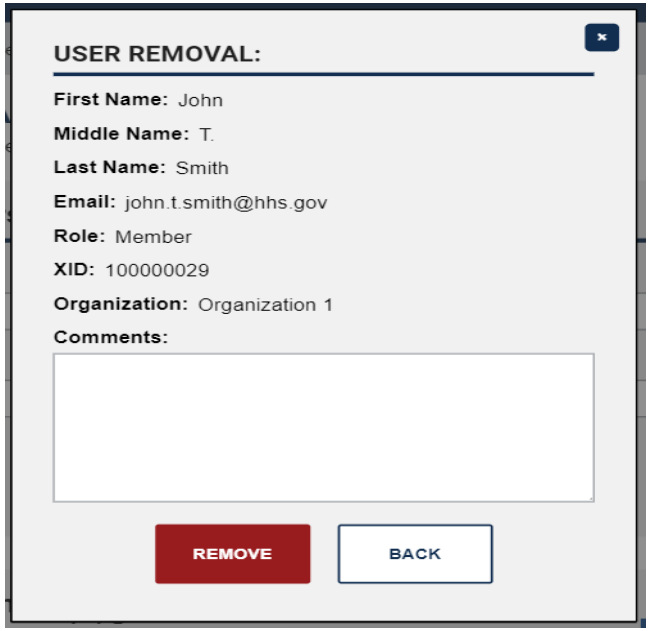


NextGen XMS Walkthrough – User Management

U.S. Department of Health and Human Services

From the User Management tab, Org Admins can manage users within their organization:

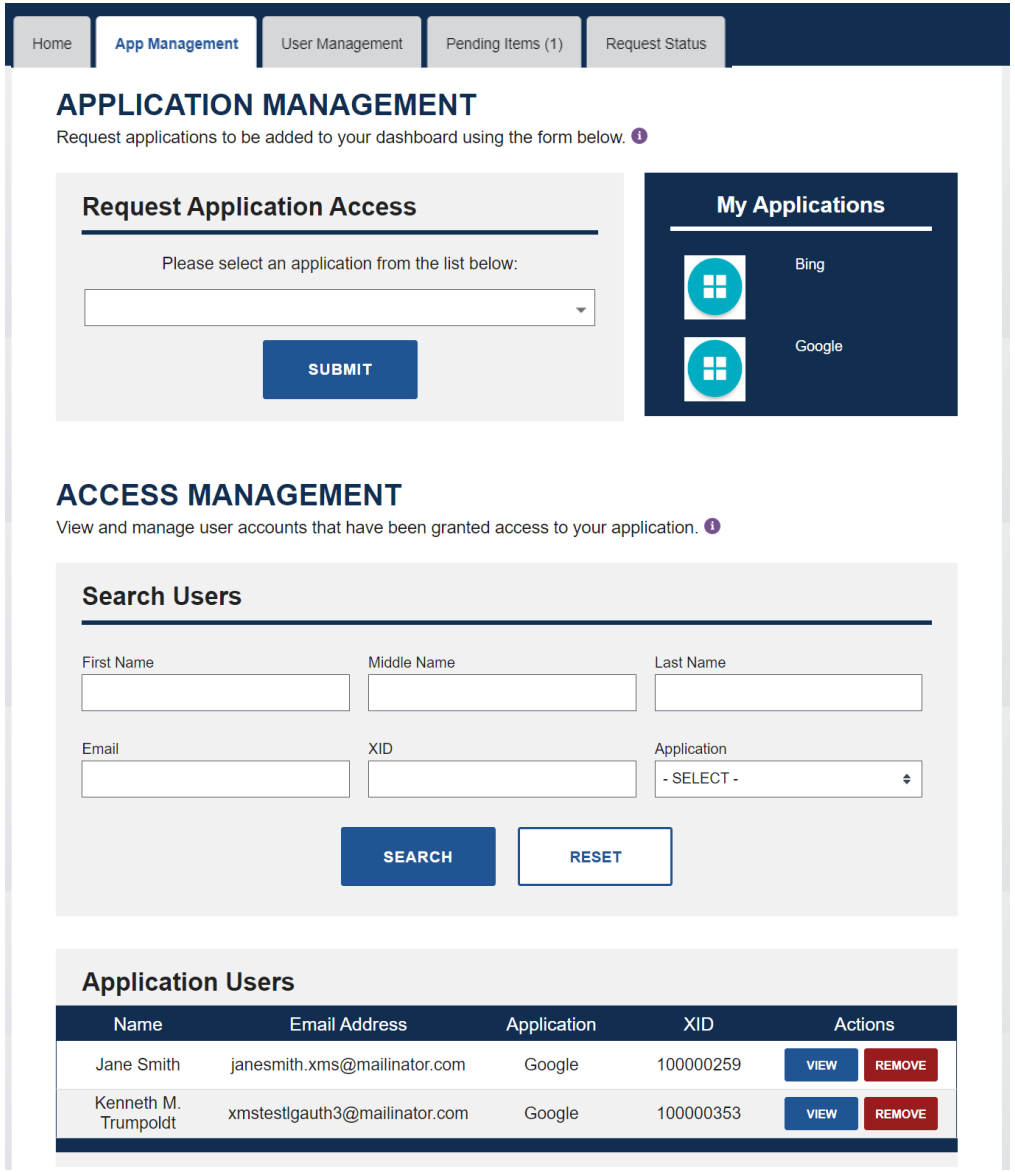


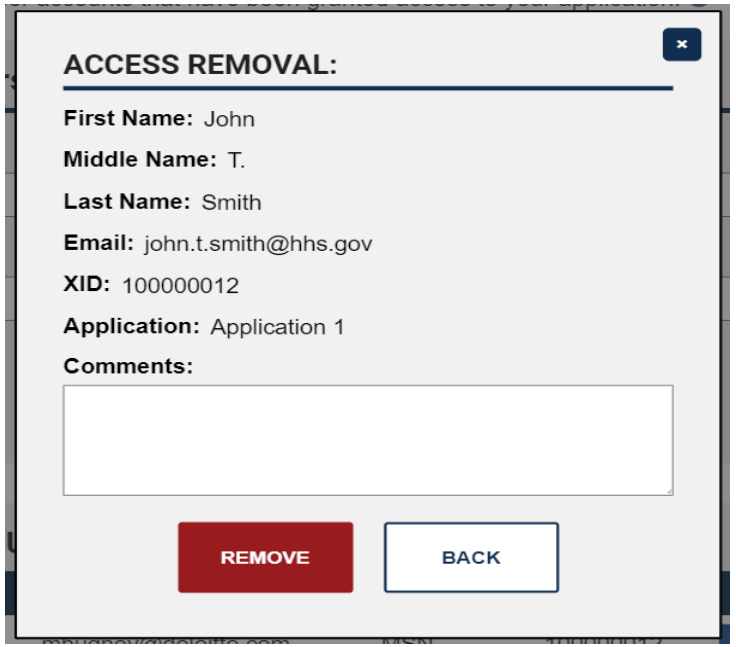


NextGen XMS Walkthrough – Application Management

U.S. Department of Health and Human Services

From the Application Management tab, App Admins can manage access for their applications:





NextGen XMS Walkthrough – Request Status

U.S. Department of Health and Human Services

From the Request Status tab, all users can view and manage their submitted requests: