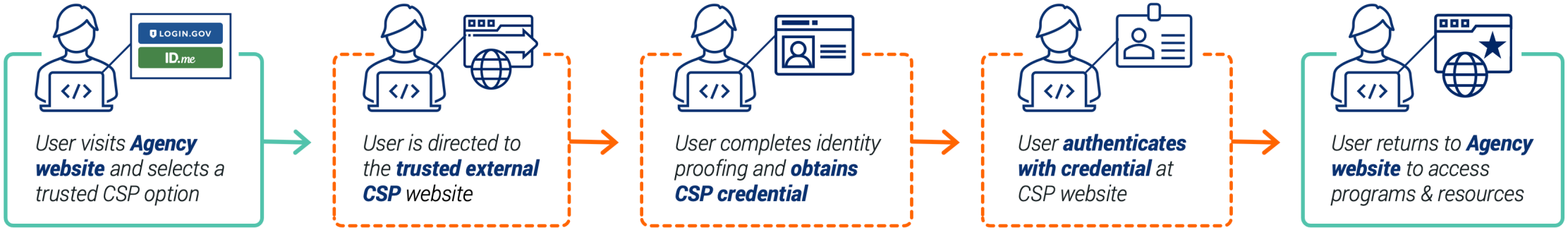
EASY DYNAMICS℠

CREDENTIAL SERVICE PROVIDER GO-LIVE

The ICAM Accelerator that Serves the American Public

Leveraging an external Credential Service Provider (CSP) allows organizations to **focus on their mission.**

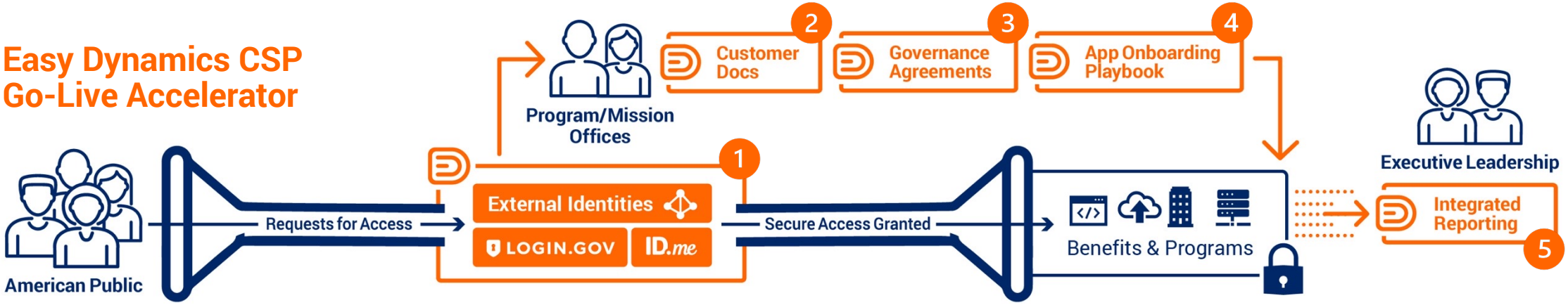


CSPs specialize in **identity proofing and credential management,** allowing agencies to dedicate their finite resources to **achieving mission goals.**

Internal Agency Website

External CSP Website

With our CSP Go-Live accelerator, agencies can start benefitting from an external CSP strategy **on day one.**



Our unique framework includes **five solution elements** that collectively reduce time to market **by up to 60%.**

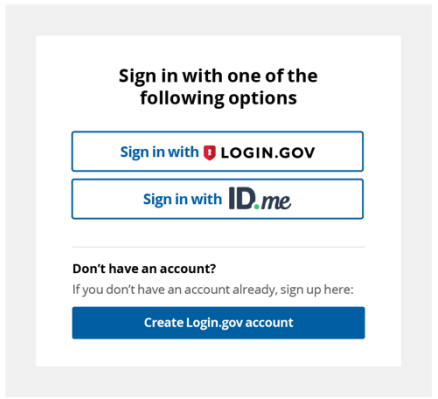
Identity Integration serves the public with trusted identities and authentication.

NIST-Aligned Governance Policies

+ Identity Assurance Level Enforcement
+ Authentication Assurance Level enforcement
+ Enforcement of geofencing, phishing-resistant and more

Differentiating Advantages

+ Alignment with Zero Trust central identity control plane
+ Policy-as-code enables strict governance reviews on policy changes
+ Enforces continuous compliance if CSP shifts configuration



USWDS-508 Compliant Authentication

NIST SP 800-63 Policies

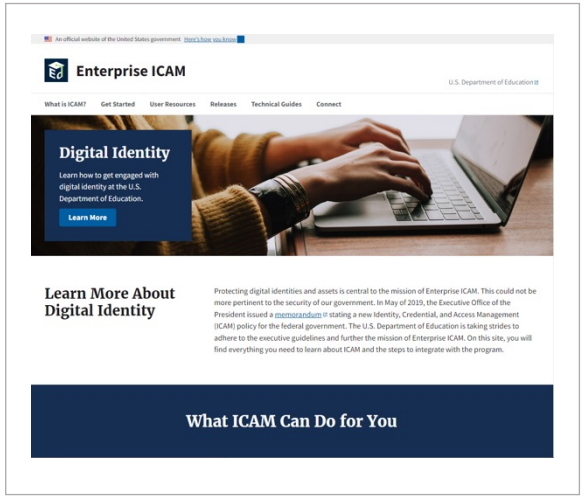
- *IAL1 / AAL2 OIDC*
- *IAL1 / AAL2 SAML*
- *IAL2 / AAL2 OIDC*
- *IAL2 / AAL2 SAML*
- *IAL2 / AAL3 PIV*
- *IAL2 / AAL2 Phishing-Resistant*

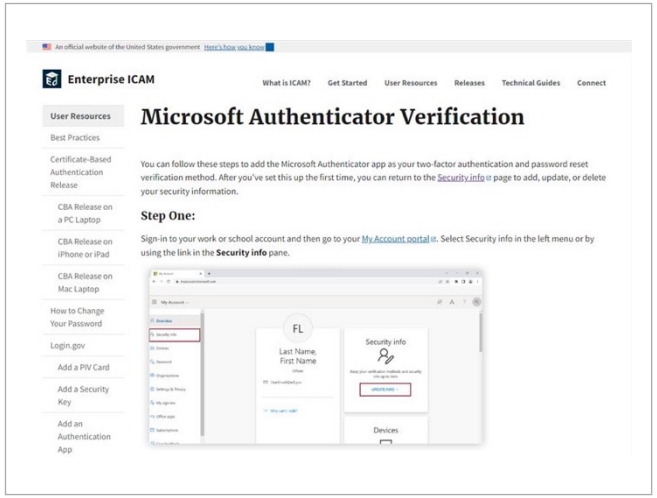
Azure AD Identity Policies

Customer Docs facilitate organizational change management and boost stakeholder buy-in.

2

Our ready-made document templates adhere to US Web Design System (USWDS) design principles and include **explainers and FAQs, starter content, and breakdowns of authenticator options.**

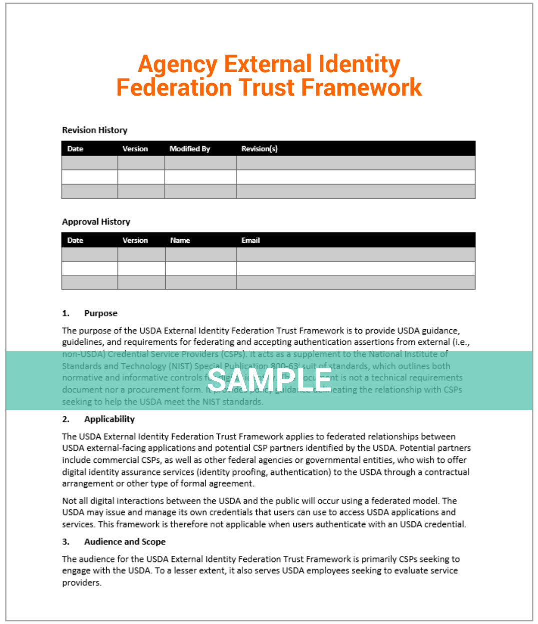




Our customizable **Governance Agreements** define how CSPs do business with agencies.

Example: Federation Trust Framework (FTF)

- ☑ Describes federation roles & responsibilities
- ☑ Provides key input for Interagency Agreements
- ☑ Defines CSP technical requirements
- ☑ Stipulates independent assessment & certification against NIST standards
- ☑ Details identity attribute bundles
- ☑ Features CSP incident response responsibilities



Agency External Identity Federation Trust Framework

Revision History

Date	Version	Modified By	Revision(s)

Approval History

Date	Version	Name	Email

1. Purpose

The purpose of the USDA External Identity Federation Trust Framework is to provide USDA guidance, guidelines, and requirements for federating and accepting authentication assertions from external (i.e., non-USDA) Credential Service Providers (CSPs). It acts as a supplement to the National Institute of Standards and Technology (NIST) Special Publication 800-63[i] suit of standards, which outlines both normative and informative controls f[illegible] [illegible]nt is not a technical requirements document nor a procurement form. It [illegible] [illegible]eating the relationship with CSPs seeking to help the USDA meet the NIST standards.

SAMPLE

2. Applicability

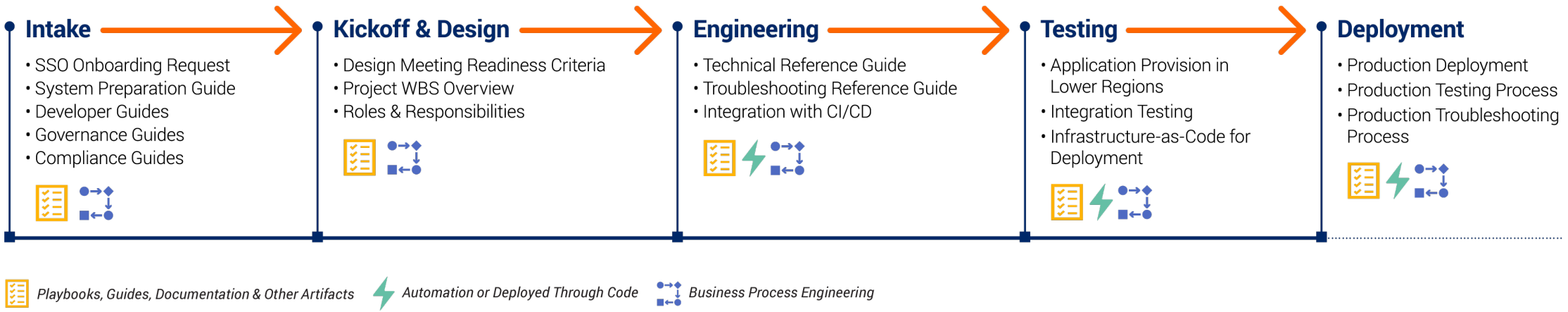
The USDA External Identity Federation Trust Framework applies to federated relationships between USDA external-facing applications and potential CSP partners identified by the USDA. Potential partners include commercial CSPs, as well as other federal agencies or governmental entities, who wish to offer digital identity assurance services (identity proofing, authentication) to the USDA through a contractual arrangement or other type of formal agreement.

Not all digital interactions between the USDA and the public will occur using a federated model. The USDA may issue and manage its own credentials that users can use to access USDA applications and services. This framework is therefore not applicable when users authenticate with an USDA credential.

3. Audience and Scope

The audience for the USDA External Identity Federation Trust Framework is primarily CSPs seeking to engage with the USDA. To a lesser extent, it also serves USDA employees seeking to evaluate service providers.

The **App Onboarding Playbook** enables rapid integration with enterprise ICAM solutions.

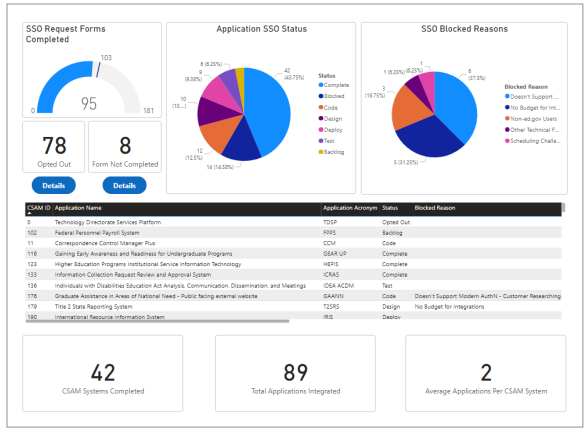


Integrated Reporting meets federal mandates and provides insights to agency leadership.

- ☑ **CY23 CIO Metrics Dashboard**
- ☑ **Application Onboarding Tracker**
- ☑ **Intelligence Insight**

Insights include:

+ Sign-ins from known malicious IP addresses
+ Impossible travel scenarios
+ Unusual resource/site access
+ Password cracking/brute force campaigns
+ Multi-stage attacks using correlated behavior



Quick Summary

Easy Dynamics has successfully managed external CSP go-live for **three federal enterprise-level ICAM programs.**

Based on these experiences, we've developed an accelerator with **five components that work in concert** with each other.

Deploying our accelerator **drastically reduces the time** between contracting with a CSP and reaping business value.

Contact Us

Pirooz Javan
Chief Technology Officer
+1 571.278.2454
pjavan@easydynamics.com

JJ Harkema
VP Solutions & Partnerships
+1 202.304.0769
jharkema@easydynamics.com

2000 Corporate Ridge, Suite 240
McLean, VA 22102

+1 202.558.7275

www.easydynamics.com