Virginia Information Technologies Agency

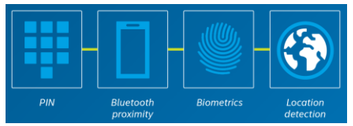
Enterprise Architecture
WCS MS SharePoint Online – VAR-719

COV Agency Staff

https://covgov.onmicrosoft.com

3rd Party Access

BR003 – Ability to allow external COV users access to specific site collections.



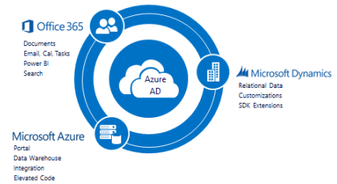
Multifactor Authentication

Secure Socket Layer — https:// SSL — **TCP 443 / TCP 80**

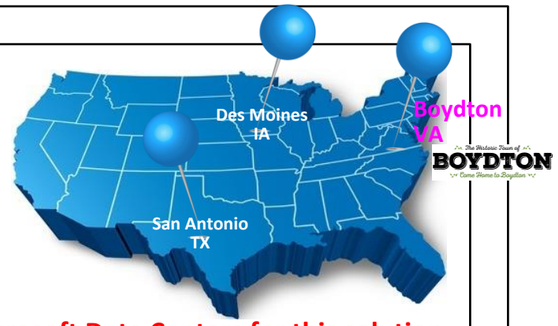
ECOS

ECOS Approved

SSO



Microsoft GOV Cloud



Microsoft Data Centers for this solution.

Boydton, VA is main data center. Data replicated only within the U.S.

COV Okta Integrated Windows Authentication (IWA) Web App

okta

Windows 2012 R2
...ADC44

Windows 2012 R2
...3935

Enterprise Identity Management Solution.
Federated users sign in with Okta.
Only Okta's Single Sign-on Solution is needed.
SSO integrates on-premise Active Directory (AD) with online MS Azure AD.
Uses java-based service (LDAP agent) that runs locally on any server.

TCP 443 / TCP 80

Cisco IronPort Security Appliance

TLS

Transport Layer Service 1.2

Data Protected in Transit by FIPS 140-2 level 2 validated.

TCP 443 / TCP 80

okta

Okta Cloud

Leveraging this solution because VITA has already purchased licenses for messaging.

covdsldap.cov.virginia.gov

LDAP Secure SSL 636

Active Directory

COV Active Directory (AD)

Already operational on premise.
Integration with MS Azure AD.
User identities managed on premise.
COV Directory Services LDAP Server

Virginia Information Technologies Agency
Central Enterprise Service Center (CESC)

Office 365 — SharePoint Online

SharePoint 2016 Online
Alternative Collaboration Solution

Enterprise SharePoint Environment

Storage, Access, and Collaboration Services

Cloud-based solution administered by VITA WCS personnel. SharePoint Online provides data isolation mechanisms at the storage level.

Data Protected at Rest

Windows 10 BitLocker

BitLocker Encryption

AES-256 ENCRYPTION

Office 365 Federated identity

Microsoft Azure Active Directory

Office 365 Federated Identity

Office 365 logical isolation of customer content is achieved through Azure Active Directory authorization and RBAC. Office 365 uses service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

Office 365 Microsoft customer lockbox

MS Customer Lockbox Service

Provides ability to explicitly allow/deny access to COV data.

Microsoft Cloud Services Leveraged for this Solution

Microsoft Office 365 is a cloud based service that can be configured to use a local Active Directory Federation Service (ADFS) to enable local users to sign on with their existing AD credential to gain access to various Microsoft online services such as Office, SharePoint and Lync.

VAR and Solution POC's: Raymond Waters and John Gordon

VITA Draft Discussion Document // REV – 103117

PURPOSE: To depict the solution VITA Security requires in order to approve VAR-719. SharePoint Online (Microsoft's Office 365 (O365) serves as an alternative collaboration solution. Will allow agencies to continue using the SharePoint platform for collaboration and intranet services instead of migrating to Google Sites should they choose. This solution can also be used to onboard new customers that currently maintain non-VITA provided SharePoint environments.

Robert Kowalke ~ Enterprise Architecture ~ robert.kowalke@vita.virginia.gov
Relationship Management & Governance (RM&G) @ Virginia Information Technologies Agency (VITA)
Commonwealth Enterprise Solutions Center (CESC)

Architectural Artifacts/Graphs/Views/Matrices/etc. reference page: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html