Protecting Controlled Unclassified Information using Secure Microsoft Cloud Technology

David George

Information Security, MRIGlobal, Kansas City

Introduction

Federal agencies routinely generate, use, store, and share information that, while not classified, still requires some level of protection from unauthorized access and release. CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies. CUI is not classified information.

Safeguarding Controlled Unclassified Information (CUI) is a Department of Defense (DOD) requirement and a key tool for the protection of sensitive, unclassified information. MRIGlobal has configured and deployed a 100% cloud-based secure enclave for protecting CUI to satisfy this requirement. However, securing CUI shouldn't limit the tools and productive applications required to handle and consume CUI data. By implementing and securely configuring an enclave in the Microsoft Government Community Cloud, employees will be able to facilitate the security requirements of handling CUI while using key business applications they are used to (SharePoint, Outlook, PowerPoint, OneDrive, Teams, etc.). The Microsoft Cloud infrastructure that this enclave is built on is only available to Government Contractors and meets all information security requirements necessary to use and store Controlled Unclassified Information (CUI).

"**ARCUS**" will be the official MRIGlobal name used when referring to this secure cloud enclave.

Cloud Architecture

The Office 365 Government Community Cloud High (GCCH) Information System is built on the Microsoft Azure Government platform housed within 8 dedicated government data centers in the US and supports the Federal Risk and Authorization Management Program (FedRAMP) accreditation at a high impact level. This FedRAMP High program provides rules for how the physical IT hardware (servers, routers, switches, etc.) that make up the GCCH cloud are secured. Access is restricted to the infrastructure and rules for all Microsoft GCCH employees include:

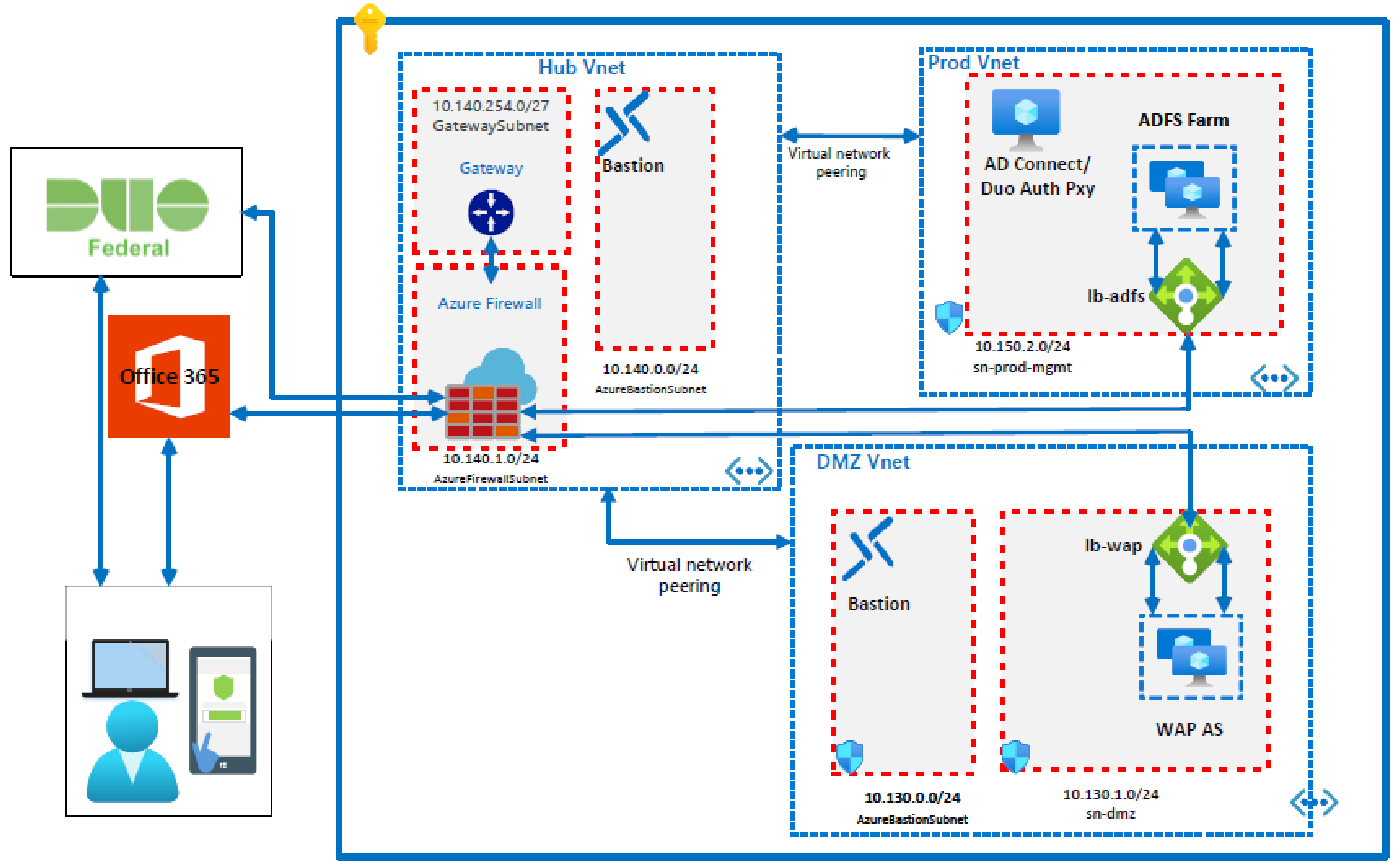
- Screenings and FBI background checks
- US citizenship
- Criminal history checks
- Fingerprinting check against FBI databases

Unique features and capabilities of the GCCH environment include logically segregated data silos for each instance (contractor), all data is stored within the United States,

This design fully isolates ARCUS from the MRIGlobal corporate network and protects against any attacks that might originate from internal systems as well as internet-based attacks.

Key Design Features	
New Email Address @mriglobalusa.org	- Protects email containing CUI within Outlook - Separates email containing CUI from corporate email
Data Loss Prevention	Allows you to tag outbound attachments and emails as CUI preventing them from being forwarded to unknown recipients
Dedicated SharePoint Site	Each project will have a dedicated site for storing CUI data keeping it secure and easily accessible
Dedicated OneDrive	Secure OneDrive for storing CUI and PII within ARCUS
Personal Virtual Machine	Each user will have access to a dedicated VM for logging into and using ARCUS

ARCUS System Design

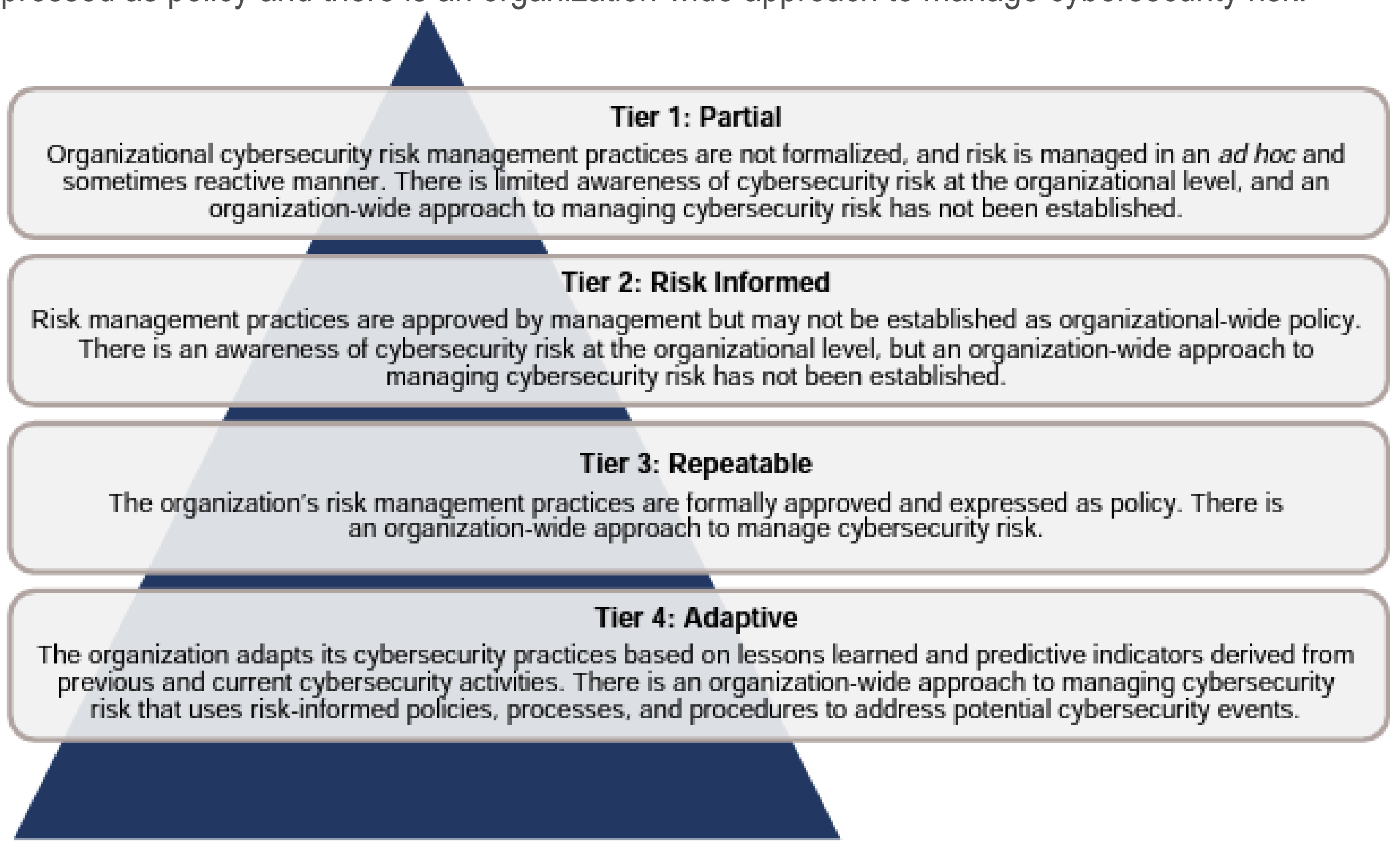


CISA Cybersecurity Framework

The CISA Framework focuses on three main components: Core, Implementation Tiers, and Profiles. These components enable an organization to identify its cybersecurity practices, provide context for its cybersecurity approach, and describe its current and target (or goal) cybersecurity posture. These three components also help an organization examine its cybersecurity activities in terms of its specific priorities.

The CISA framework models the NIST 800-171 requirements in a way that allows organizations to gauge risk, set priorities, and develop policies and procedures for securing CUI Information.

The Framework presents "Implementation Tiers" to outline how an organization views and handles cybersecurity risk and the processes in place to handle that risk. An objective target for the DIB should be at least Tier 3 in which the organization's risk management practices are formally approved and expressed as policy and there is an organization-wide approach to manage cybersecurity risk.



Tier 1: Partial

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk Informed

Risk management practices are approved by management but may not be established as organizational-wide policy. There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.

Tier 3: Repeatable

The organization's risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.

Tier 4: Adaptive

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

NIST 800-171 Compliance

The cybersecurity requirements within NIST 800-171 are designed to safeguard CUI in the IT networks of government contractors and subcontractors. It defines the practices and procedures that government contractors must adhere to when their networks process or store CUI.

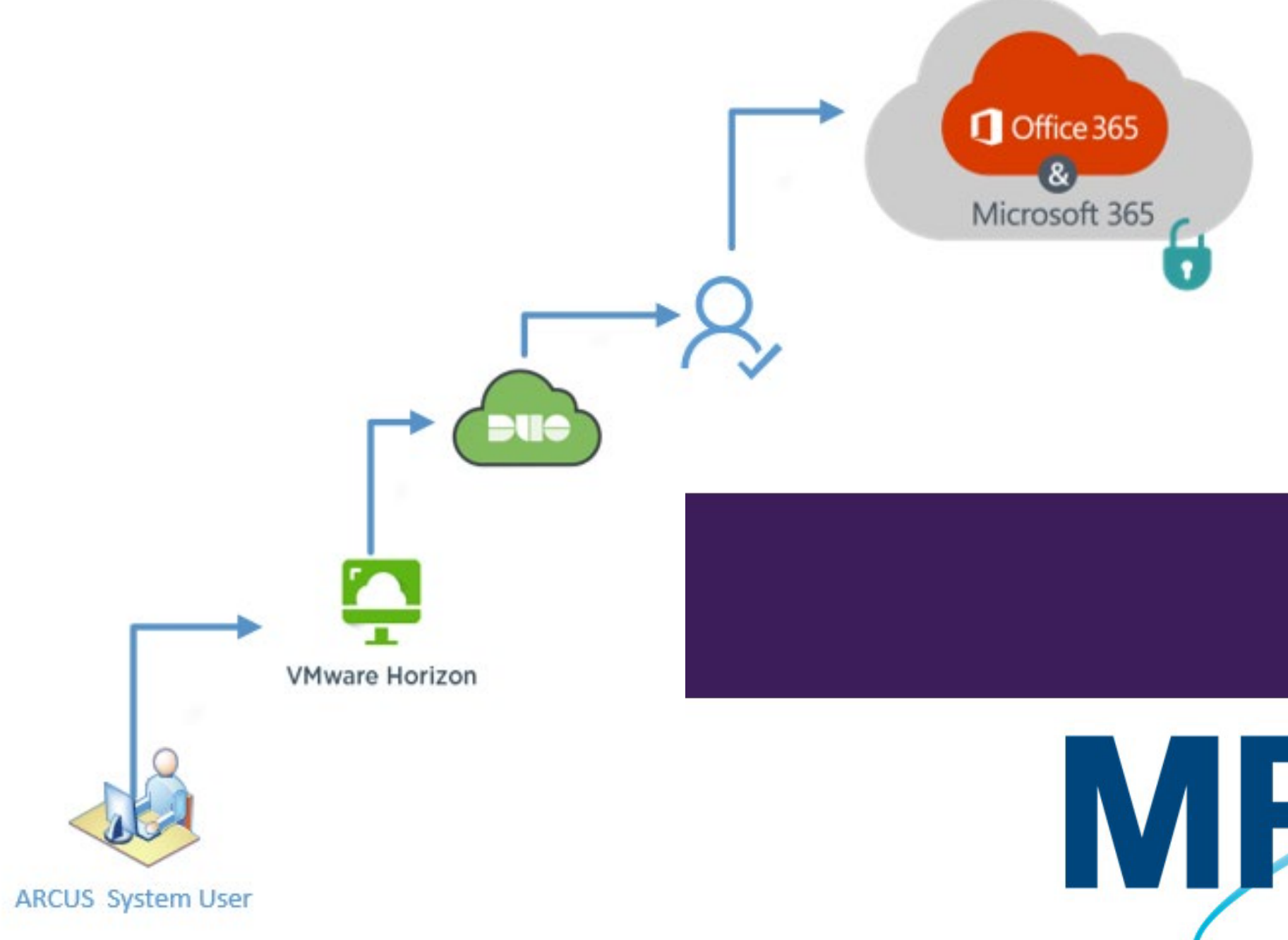
Any organization that processes or stores CUI on behalf of the US government is required to be compliant with the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) cybersecurity standards.

NIST 800-171 consists of **110 requirements**, each covering different areas of an organization's IT technology, policies, and practices. Requirements cover aspects like access control, systems configuration, and authentication procedures. They also set out the requirements for cybersecurity procedures and incident response plans.

The 110 security requirements of NIST 800-171 are organized into **14 families**. Each family contains the requirements related to the general security topic of the family. These groupings are intended to ensure it is straightforward for an organization to employ and self-assess the application of the requirements. Within the 110 security requirements, **320 security controls** must be fully implemented in order to achieve accreditation for processing CUI.

Implementation

All projects requiring the use of CUI will be transitioned to ARCUS and employees will receive training and credentials for using the system. This diagram outlines the authentication and logon process.



ARCUS Virtual Machines are accessible through the MRIGlobal VDI System at vdi.mriglobal.org

CUI

ATTENTION

Need Assistance?

MRIGlobal Service Desk
Service Desk (x2800)
Hours: 7 a.m. - 6 p.m. Central

For after-hours support:
(816) 753-7600 ext. 2800 (follow the prompts to reach the on-call technician)

CUI SharePoint Repository
https://mriglobalusa.sharepoint.us

Contact Information

David George
T: (816) 326-5500
E: david.george@mriglobalusa.org

MRIGlobal
425 Dr. Martin Luther King Jr Blvd
Kansas City, MO 64110

The science you expect. **The people** you know.