# Defining Boundaries: The Critical Role of External Service Providers (ESPs) in Securing the DIB

MSPs for the Protection of Critical Infrastructure

# Your Presenters

**George Perezdiaz**

Practice Leader, Cyber Risk & Compliance
SP6

**Joy Beland**
VP Partner Strategy
Summit 7

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


**PROCESS, STORE, OR TRANSMIT**

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


## OR PROVIDE SECURITY PROTECTION

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


## BASIC ASSUMPTION

*Nonfederal Organizations can implement a variety of potential security solutions…*

…to satisfy security requirements.

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


## BASIC ASSUMPTION

*Nonfederal Organizations can implement a variety of potential security solutions…*

- ❑ **(2015)** either directly or through the use of managed services

…to satisfy security requirements.

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


## BASIC ASSUMPTION

*Nonfederal Organizations can implement a variety of potential security solutions…*

- ❑ **(2015)** either directly or through the use of managed services
- ❑ **(2020)** directly or using external service providers (e.g., managed services)

…to satisfy security requirements.

# The Impact of ESPs in the Overall CMMC Program (or world of CUI)


## BASIC ASSUMPTION

*Nonfederal Organizations can implement a variety of potential security solutions…*

- ❑ **(2015)** either directly or through the use of managed services
- ❑ **(2020)** directly or using external service providers (e.g., managed services)
- ❑ **(2024)** or use external service providers

…to satisfy security requirements.

# The Impact of ESPs in the Overall CMMC Program (NIST 171rev3)


### 3.16.3. External System Services

**REQUIREMENT:** 03.16.03

a. Require the providers of external system services used for the processing, storage, or transmission of CUI, to comply with the following security requirements: [*Assignment: organization-defined security requirements*].

b. Define and document user roles and responsibilities with regard to external system services including shared responsibilities with external providers.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

**DISCUSSION**

External system services are provided by external service providers. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with the organization charged with protecting

# The Impact of ESPs in the Overall CMMC Program (and the DIB)

## The CMMC Guides (Scoping and Assessment)


- ❑ External Service Providers
- ❑ Security Protection Assets

# The Impact of ESPs in the Overall CMMC Program (or Federal Programs World)

## NIST 800-53

| | |
|---|---|
| External Information System Service Provider | A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. |

**Can you imagine a security and compliance world without External Service Providers?**

# The Impact of ESPs in the Overall CMMC Program (and the DIB)

- Percent of DIB organizations leveraging External Service Providers

**50% - 70%**

Estimates from

The Collective

# The Impact of ESPs in the Overall CMMC Program (and the DIB)

- **Percent of CMMC Level 2 Requirements Covered by External Service Providers**

**40% - 70%**

**Security Requirement Covered By ESPs**

**Estimates from The Collective**

# MSPs for the Protection of Critical Infrastructure

## Overview

MANAGED SERVICE PROVIDER COLLECTIVE

www.MSPCollective.org

# Who We Are

MSPs for the Protection of Critical Infrastructure (The MSP Collective) is a 501(c)6 Non-Profit Organization dedicated to helping the US Government and Federal Ecosystem understand the important role External Service Providers can play in protecting critical infrastructure

**Mission**:

To inform the US Government and Critical Infrastructure industries on topics related to Managed Service Providers and Managed Security Service Providers dedicated to the National Security mission of maintaining a secure, functioning, and resilient critical infrastructure

MSP COLLECTIVE

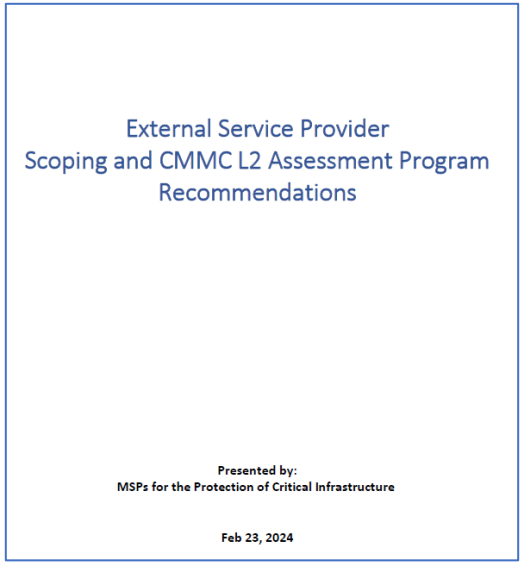
# Main Positions of MSP Collective

Standards – Is NIST 800-171 enough for Service Providers?

Congressional Appropriations for the SMBs

RPO Certification – Do the current requirements make sense?

ESP Program and Scoping Guidance Recommendations




MSP COLLECTIVE

# ESP Program Recommendations

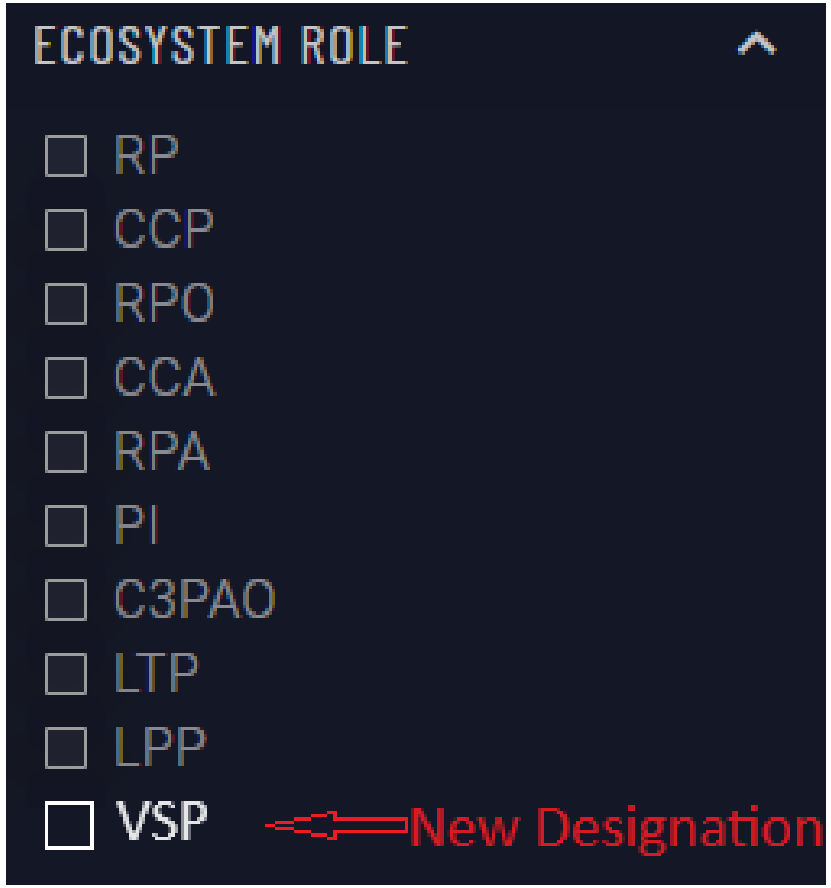
All Service Providers who perform or deliver security capabilities on behalf of the OCS must be validated for implementation of the same CMMC level requirements as the OSCs they support.

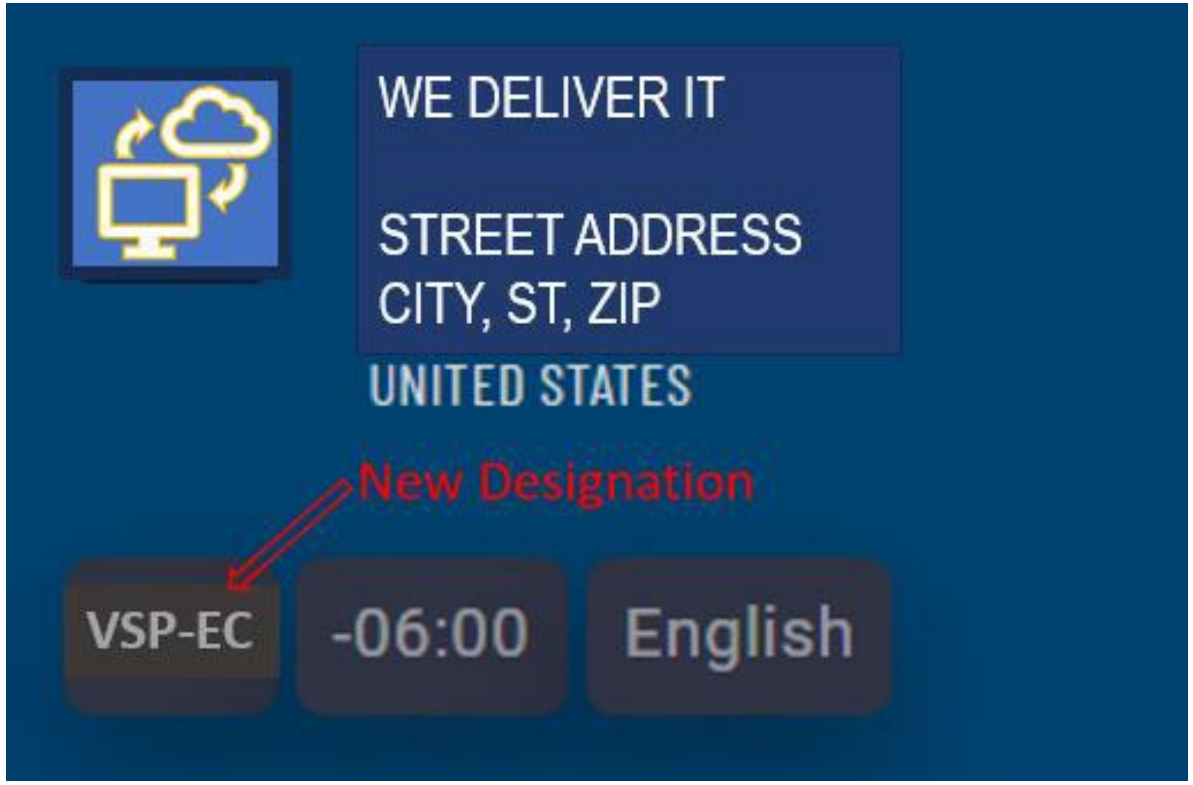
DIB contractors would receive the ***CMMC Level 2 Certification Assessment***, Service Providers would receive the ***CMMC Level 2 Validation Assessment***

Cyber AB Designation: **Validated Service Provider (VSP)**

MSP COLLECTIVE

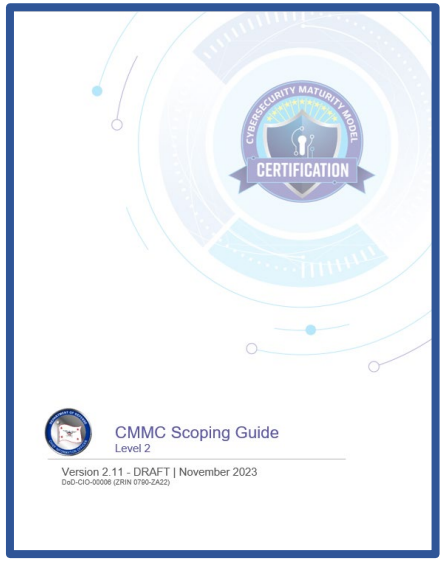
# ESP Program Recommendations

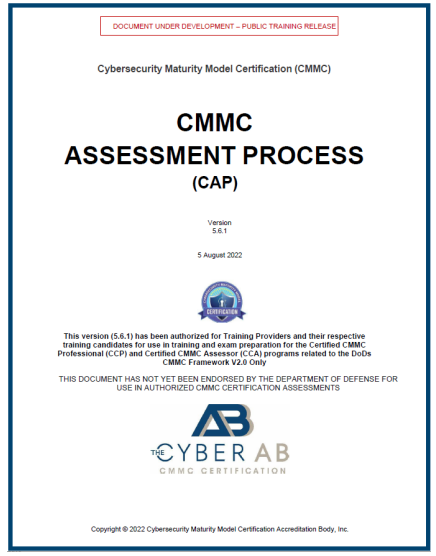



MSP COLLECTIVE

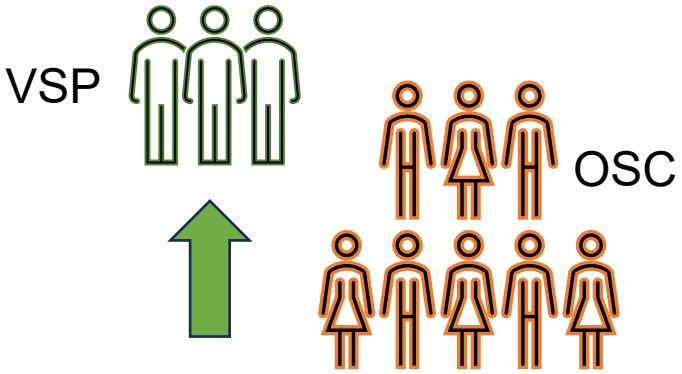
# ESP Program Recommendations




Include VSP Guidance in:

- The CMMC Level 2 Scoping Guide
- The CMMC Assessment Process




The Cyber AB will **prioritize** VSP Assessments by C3PAOs

High-Level Validated Shared Responsibility Matrix (SRM) included on the Cyber AB marketplace

| Category Name | CMMC 2.( | NIST Control Statement | AO | Assessment Objectives | [MSP] Responsibility |
|---|---|---|---|---|---|
| Access Control (AC) | AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | 3.1.3[a] | [a] information flow control policies are defined. | |
| | | | 3.1.3[b] | [b] methods and enforcement mechanisms for controlling the flow of CUI are defined. | S |
| | | | 3.1.3[c] | [c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. | |
| | | | 3.1.3[d] | [d] authorizations for controlling the flow of CUI are defined. | S |
| | | | 3.1.3[e] | [e] approved authorizations for controlling the flow of CUI are enforced. | F |

F = Full
S = Shared

MSP COLLECTIVE

# ESP Scoping Recommendations

The scope of services provided varies by ESP

MSPs and MSSPs unlikely to process, store, or transmit CUI for clients

**View of the Collective**:

- Services delivered that fully or partially address NIST 800-171 requirements for the OSC must be identified in a Shared Responsibility Matrix (SRM)
- The people, processes, and technology leveraged to deliver those services should be in scope for the MSP's or MSSP's own CMMC L2 assessment
- MSPs and MSSPs using Non-US Persons for clients with ITAR, EAR or NOFORN data must demonstrated that physical and logical access to the OSC environment has been removed



# ESP Scoping Recommendations

Examples of assets in scope

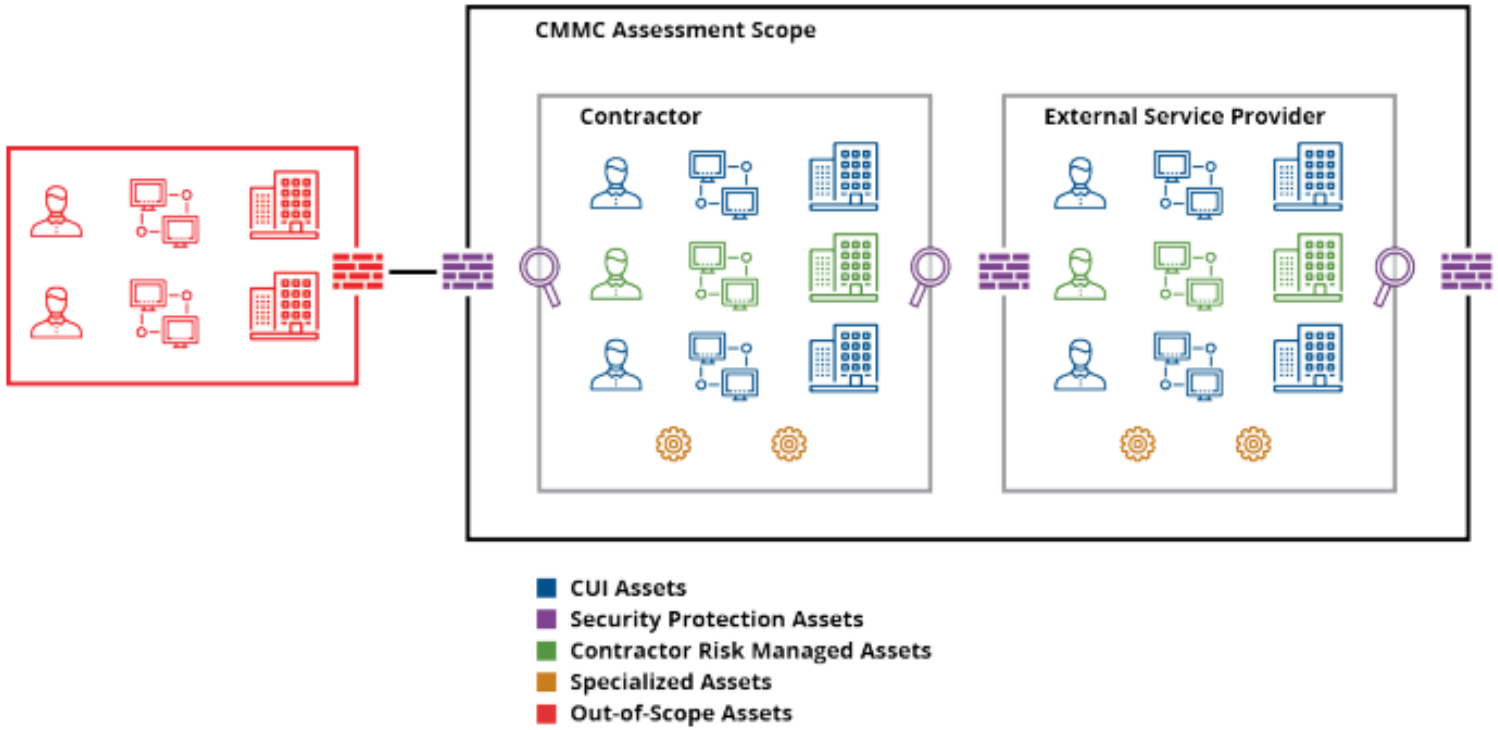
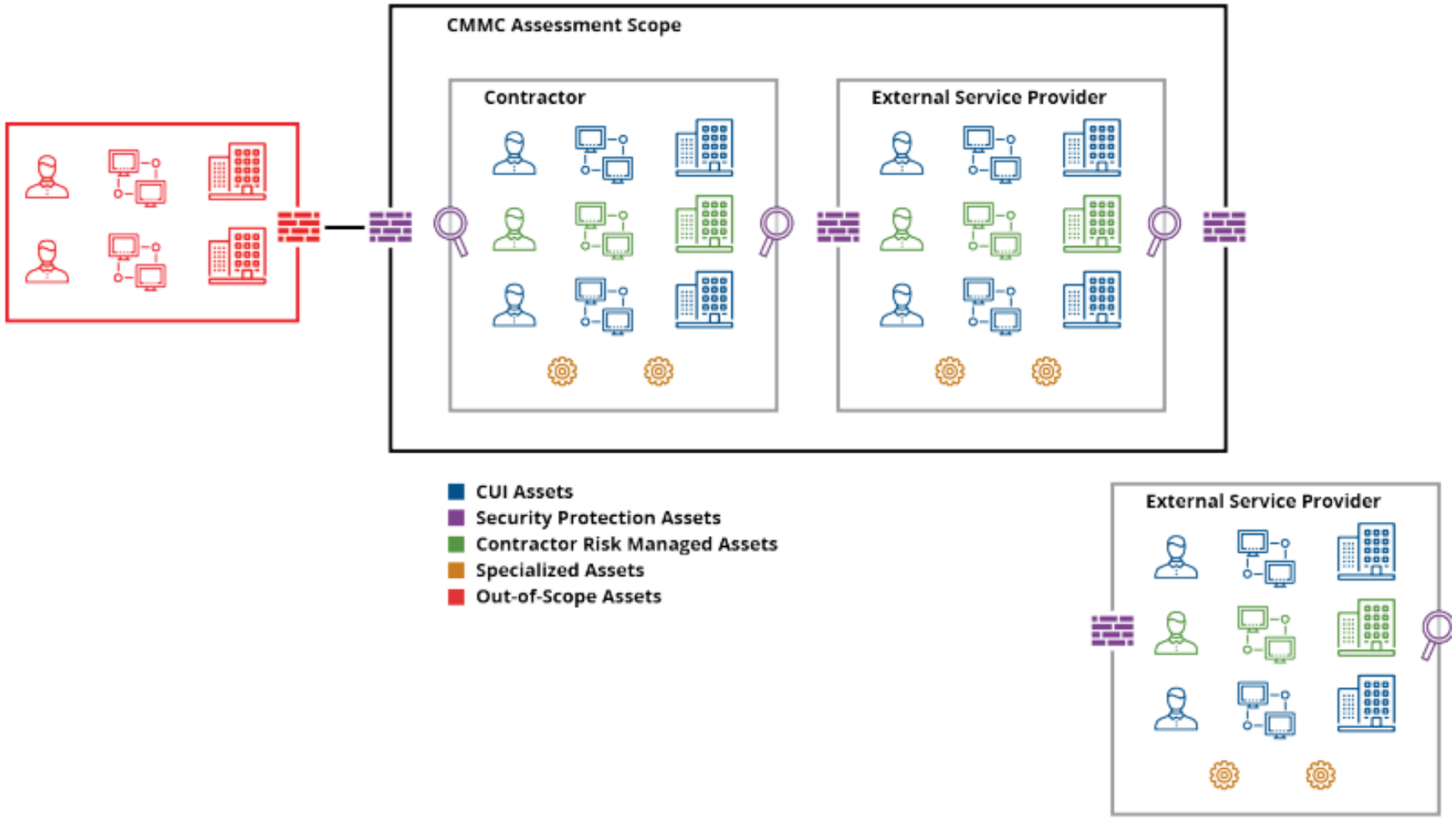



**Figure 1. CMMC Assessment Scope**

MSP COLLECTIVE

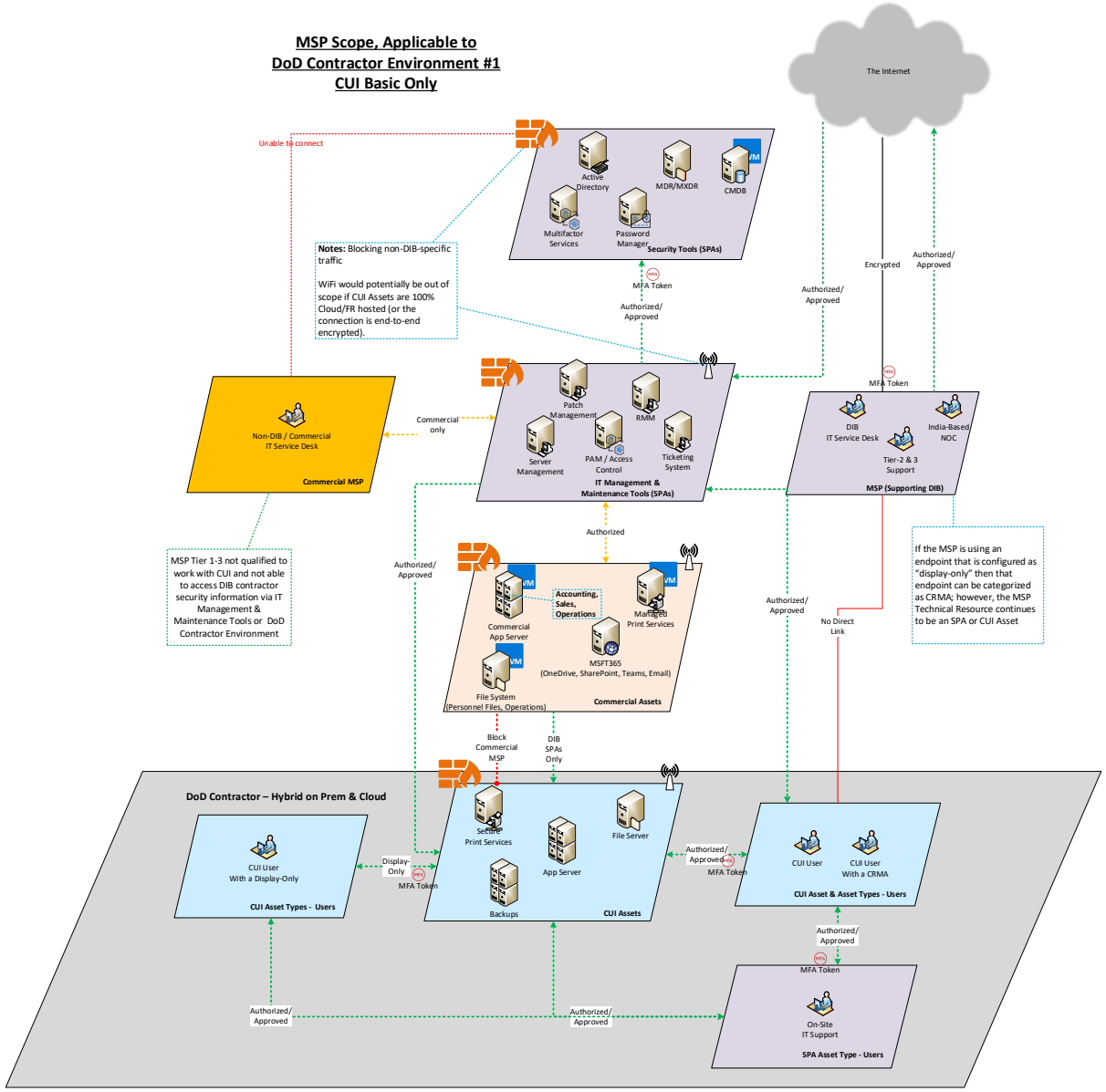
# ESP Scoping Recommendations

Examples of assets in scope

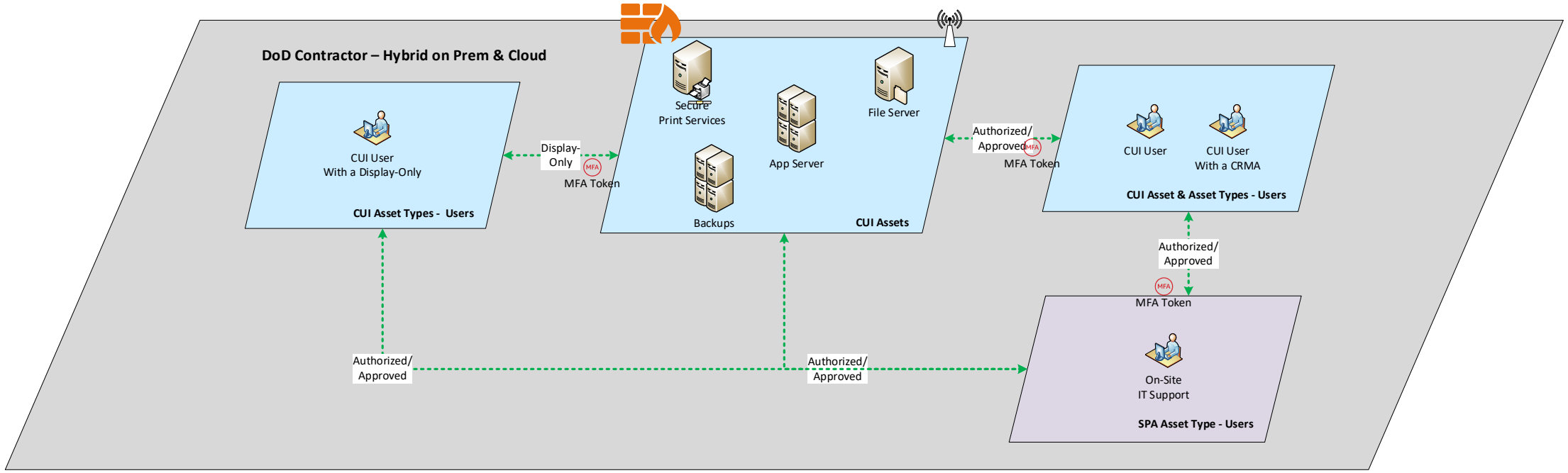



MSP COLLECTIVE

# ESP Scoping Recommendations

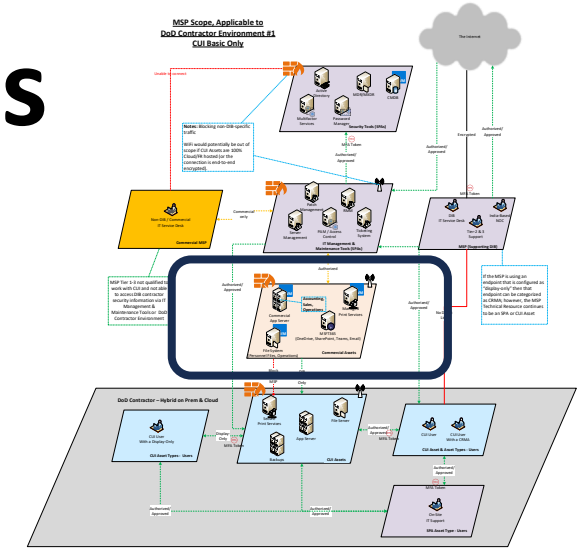


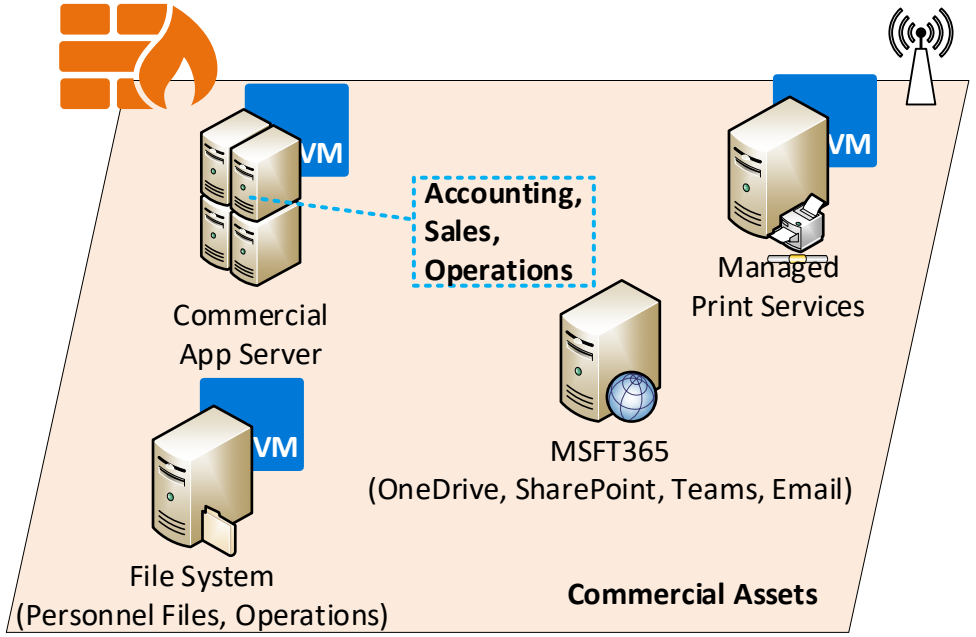
# ESP Scoping Recommendations
# The OSC




MSP COLLECTIVE

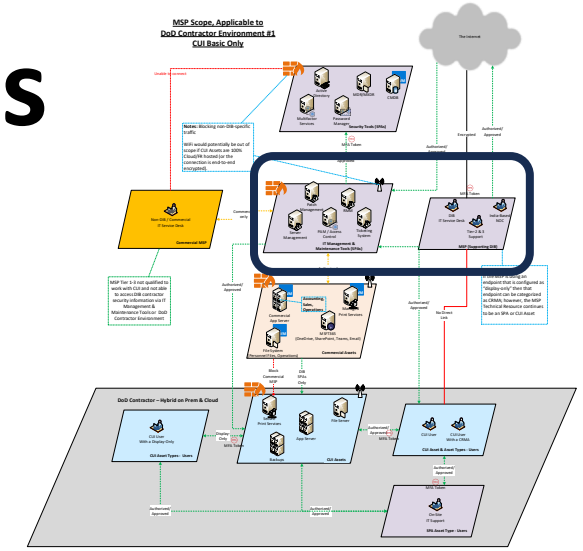
# ESP Scoping Recommendations
# The OSC's Commercial Assets

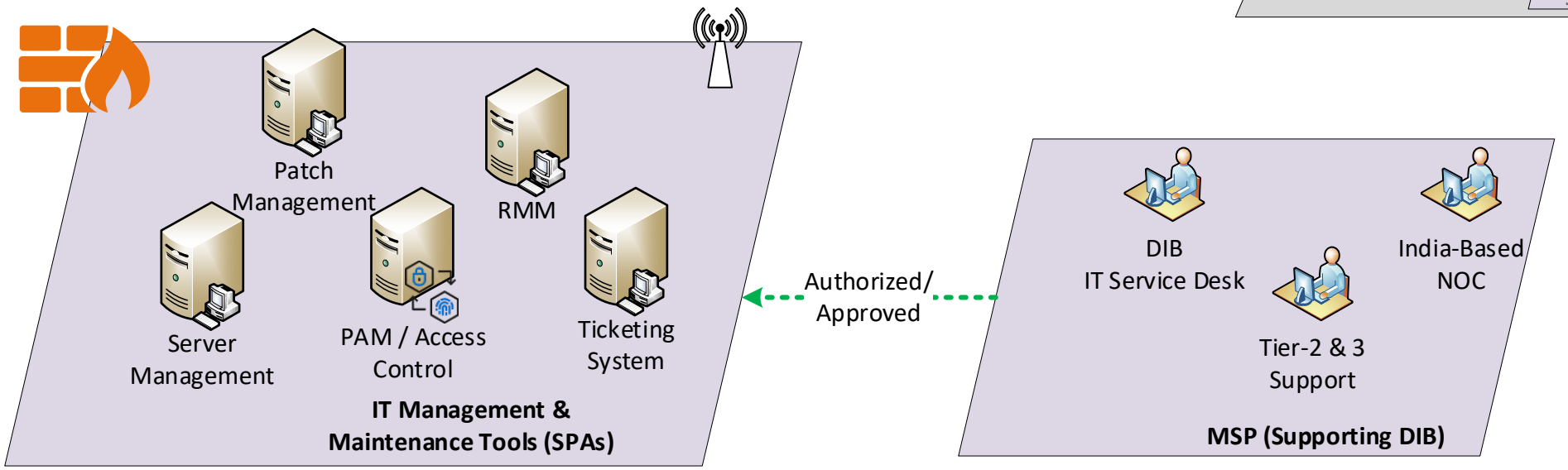



MSP COLLECTIVE

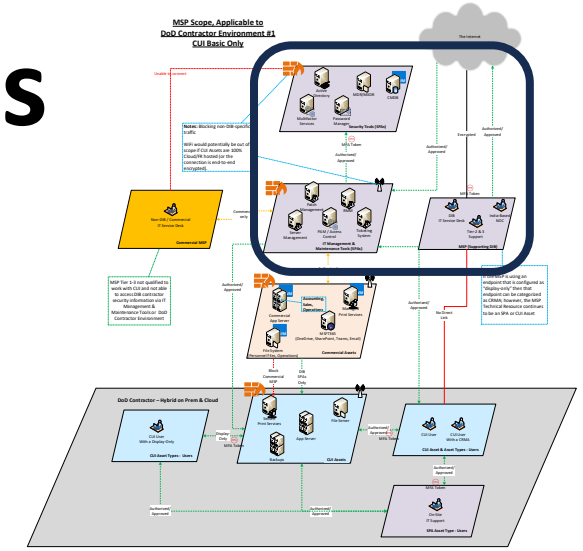
# ESP Scoping Recommendations
# The ESP Perspective

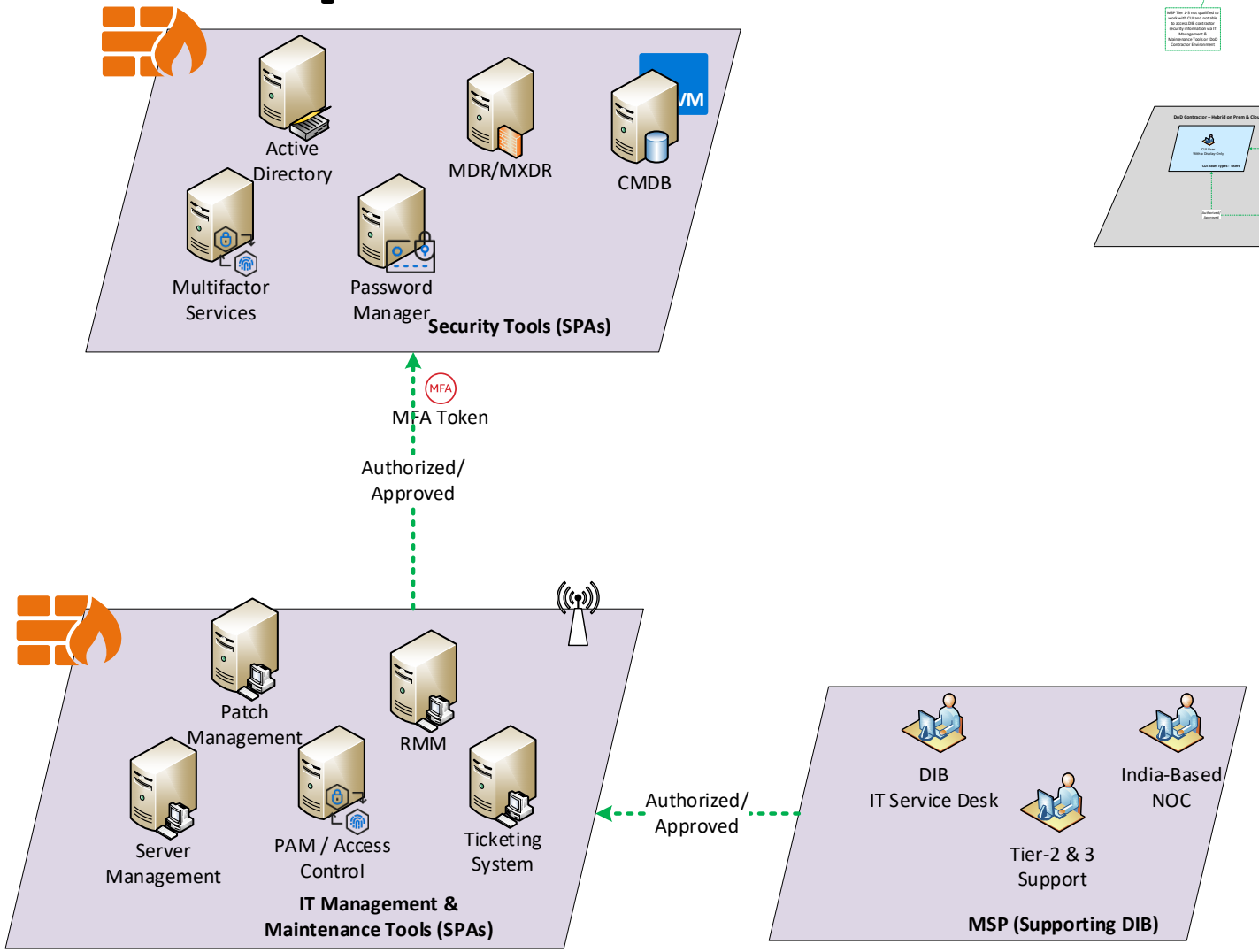





MSP COLLECTIVE

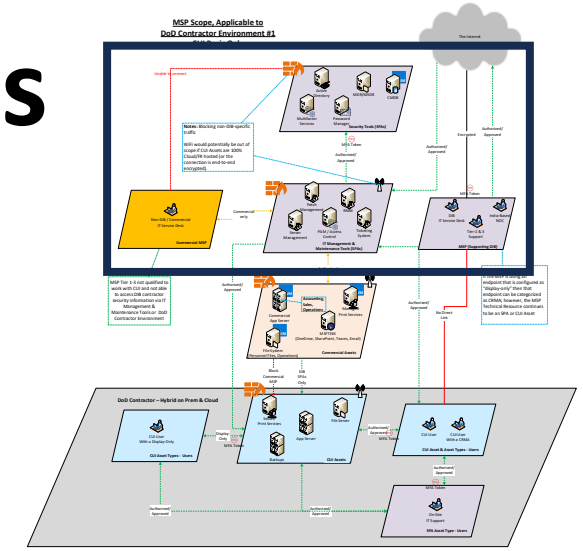
# ESP Scoping Recommendations
# The ESP Perspective




MSP COLLECTIVE

# ESP Scoping Recommendations
# The ESP Perspective



Unable to connect

Active Directory

MDR/MXDR

CMDB

Multifactor Services

Password Manager

**Security Tools (SPAs)**

MFA

MFA Token

Authorized/ Approved

Patch Management

RMM

Server Management

PAM / Access Control

Ticketing System

**IT Management & Maintenance Tools (SPAs)**

Commercial only

Non-DIB / Commercial IT Service Desk

**Commercial MSP**

Authorized/ Approved

DIB IT Service Desk

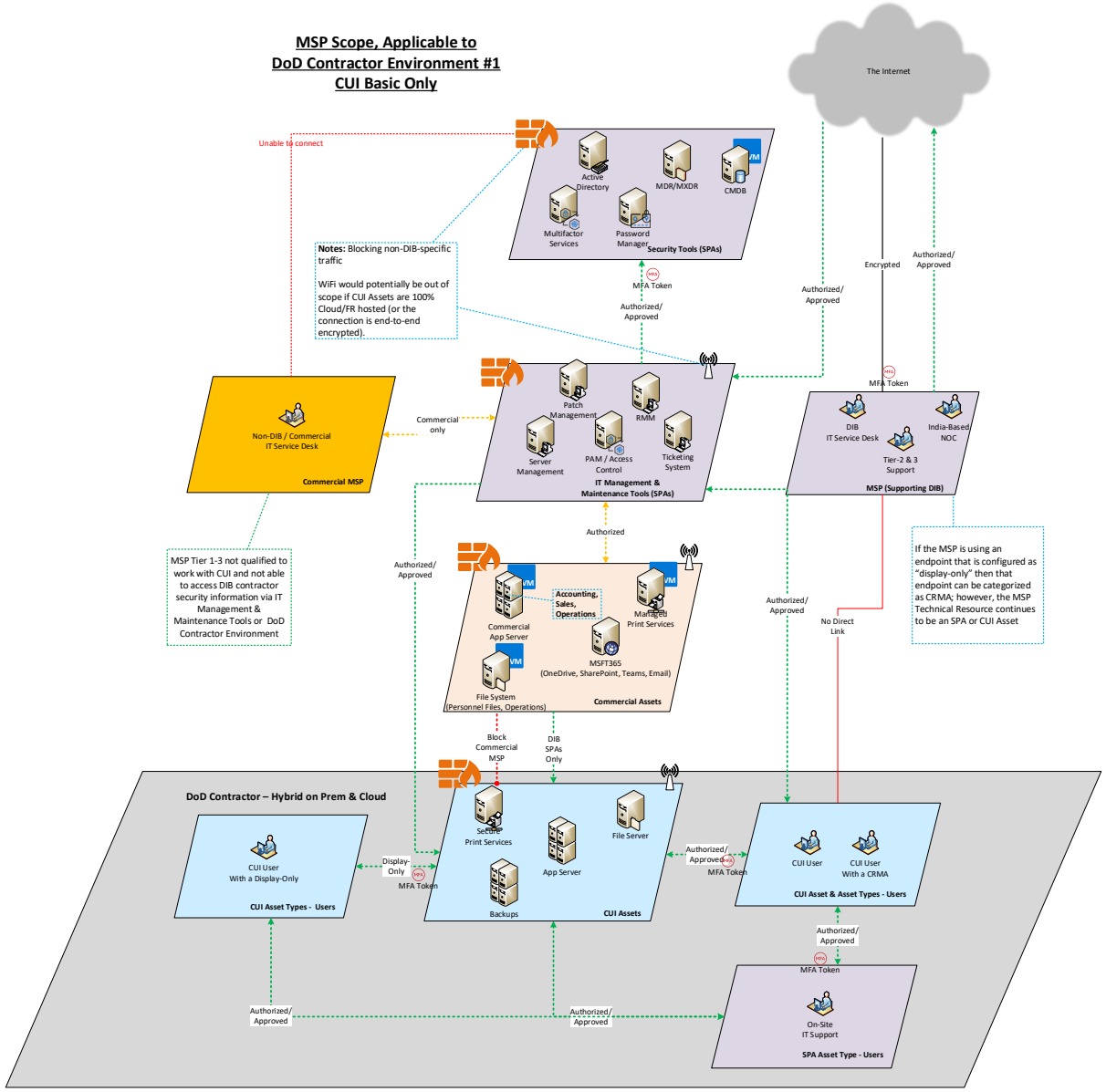
India-Based NOC

Tier-2 & 3 Support

**MSP (Supporting DIB)**

MSP COLLECTIVE

# ESP Scoping Recommendations



# Why the MSP Collective is Important

- Protecting Critical Infrastructure affects all of us
- If you are an ESP
  - It will create a level playing field when pursuing new opportunities
- If you are subject to DFARS 7012 or NIST 800-171
  - You can be confident your investments will yield the desired outcome
  - Your risk will be minimized
- If you are an SMB
  - Your interests will be represented
  - The cost barrier will be addressed
  - Your risks will be minimized
- If You are in Critical Infrastructure
  - Greater security and lower risk

MSP COLLECTIVE

# Join Us
## Become a Member of the Collective

MSP COLLECTIVE

MSPs for the Protection of Critical Infrastructure (MSP Collective)

www.mspcollective.org

info@mspcollective.org