External Service Provider
Scoping and CMMC L2 Assessment Program
Recommendations

Presented by:
MSPs for the Protection of Critical Infrastructure

Feb 23, 2024

Purpose:

This paper outlines the program and scoping recommendations that would support the validation of a Service Provider as qualified to perform security capabilities on behalf of an OSA/OSC.

Definitions and Applicability:

Organizations Seeking Assessment (OSA) and Organizations Seeking Certification (OSC) often leverage an External Service Provider (ESP) entity in meeting NIST 800-171 requirements. People, tools and technology described in the CMMC Level 2 Scoping Guide (Nov 20, 2021) and the CMMC Assessment Process (Draft) v.5.6.1, where not qualifying as a CUI Asset by storing, processing or transmitting CUI but rather providing the Security Protection for the Assets that are storing, processing or transmitting CUI, fall into the category of a Security Protection Asset. This remains unchanged in the CMMC Proposed Rule, introduced in December 2023.

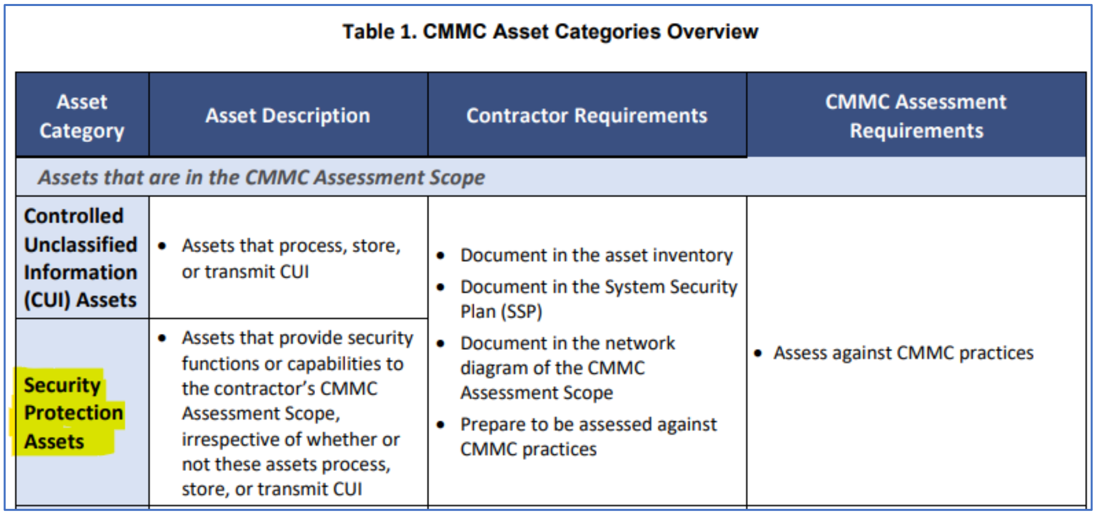


Table 1. CMMC Asset Categories Overview

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	• Assets that process, store, or transmit CUI	• Document in the asset inventory • Document in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC practices	• Assess against CMMC practices
Security Protection Assets	• Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI		

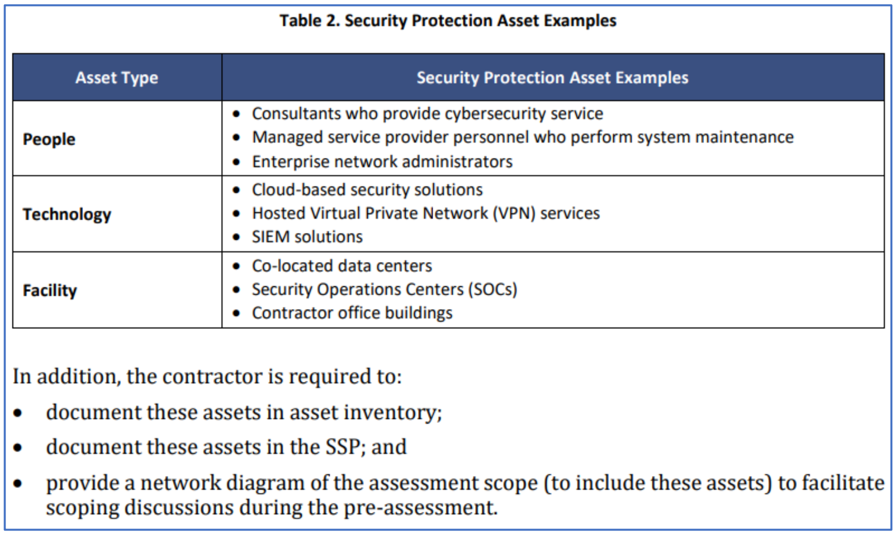


Table 2. Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings

In addition, the contractor is required to:

- document these assets in asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the assessment scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

Adding a layer of complexity, the External Service Provider organization whose assets are categorized as SPAs are also brought into the CMMC Assessment scope, as ESPs. In the December 2023 CMMC Proposed Rule, page 30, it is now stated "If an OSA utilizes an ESP, other than a Cloud Service Provider (CSP), the ESP must have a CMMC certification level equal to or greater than the certification level the OSA is seeking. For example, if an OSA is seeking a CMMC Level 2 Certification Assessment, the ESP must have either a CMMC Level 2 Certification Assessment or a CMMC Level 3 Certification Assessment."

Further, the Level 2 Scoping Guide | Version 2.11 document included with the December 2023 CMMC Proposed Rule provides additional guidance on ESPs (page 10), referenced here:

> **External Service Provider Considerations**
>
> An External Service Provider (ESP) can be within the scope CMMC requirements if it meets CUI Asset and/or Security Protection Asset criteria. **To be considered an ESP, data (specifically CUI or Security Protection Data, e.g., log data, configuration data) must reside on the ESP assets** as set forth in 32 CFR § 170.19(c)(2)**.** Special considerations in for an OSA using an ESP include the following:
>
> - Evaluate the ESP's shared responsibility matrix where the provider identifies security control objectives that are the provider's responsibility and security control objectives that are the OSA's responsibility.
> - Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the OSA's information security objectives.
> - As set forth 32 CFR § 170.16(c)(2) and 32 CFR § 170.17(c)(5) respectively, an OSA may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract, if the OSA ensures the Cloud Service Provider's offering either:
>   - is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace, **OR**
>   - is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline in accordance with DFARS 252.204-7012. This condition is met if the evidence includes a System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 requirements.
> - OSAs shall also be assessed at Level 2, as applicable, against their on-premise infrastructure connecting to the CSP. As part of the CMMC Assessment Scope, the security requirements from the CRM must be documented or referred to in the OSA's SSP, which will also be assessed.
> - If the OSA utilizes an ESP other than a CSP, the ESP must have a CMMC Level 2 Certification as set forth in 32 CFR § 170.19(c)(2). If the ESP is **internal** to the OSA, the CMMC requirements being assessed should be listed in the OSA's SSP to show connection to its in-scope environment.

In this context, we are herein referring to ESP's who do not process, store or transmit CUI as "Service Providers" and this paper is applicable to those commonly referred to as Managed Service Providers (MSP) or Managed Security Service Providers (MSSP).

Given the difference in scoping as it relates to CUI Data Flow at a DIB contractor vs. a Service Provider's external people, technology, or facilities utilized for provision and management of comprehensive IT and/or cybersecurity services on behalf of the DIB contractor, how does a Service Provider expect to scope the Security Protection Asset (SPA) or the Security Protection Information (SPI) to be assessed? Further, how would OSCs/OSAs know what component(s) of the service delivery "package" they purchase from a Service Provider were included in their Service Provider's CMMC Level 2 Assessment?

Program Recommendations:

- For clarification purposes, DIB contractors would receive the ***CMMC Level 2 Certification Assessment***, and it is suggested that Service Providers would receive the ***CMMC Level 2 Validation Assessment,*** with the associated designation of a Validated Service Provider (VSP) by the Cyber AB. We feel the difference in the name of the assessment will be helpful to serve as a distinction between an OSC who processes, stores or transmits CUI and has DFARS 7012 requirements versus a Service Provider who does not process, store or transmit CUI or work under DFARS 7012 requirements.

- The CMMC Level 2 Scoping Guide will incorporate the scoping guidance for asset categorization and scoping applicable to the Service Provider environment.

- The Cyber AB will incorporate guidance for the Service Providers' CMMC Level 2 Validation Assessment in the CMMC Assessment Process document.

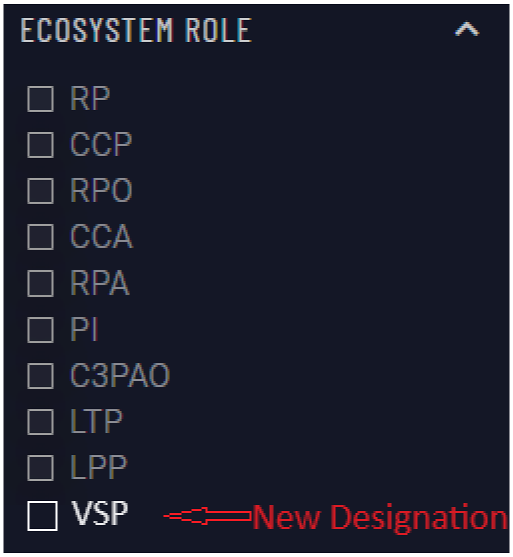
- The Cyber AB will prioritize the VSP program with associated CMMC Level 2 Validation Assessments by C3PAOs, understanding that a majority of "entities (small and other than small) pursuing CMMC Level 2 Assessment are likely to seek consulting or implementation assistance from an ESP to either help them prepare for the assessment technically or participate in the assessment with the C3PAO's" per page 135 of the CMMC Proposed Rule.

- The Cyber AB will add the ***VSP*** designation to the Marketplace with two types of designations;
  - VSP-EC for the VSP who demonstrates the ability to assist the OSA/OSC with export-controlled information[1] (ITAR, EAR, etc)
  - VSP for the VSP who demonstrates the capability to assist OSC/OSA with CUI **without** export-controlled information

- The Cyber AB will provide for a ***VSP*** badge for use on Service Provider website/emails.

- The Cyber AB marketplace site listing includes the date of validation and the high-level Shared Responsibility Matrix (SRM) presented for validation during the CMMC L2 Validation Assessment. For Example:

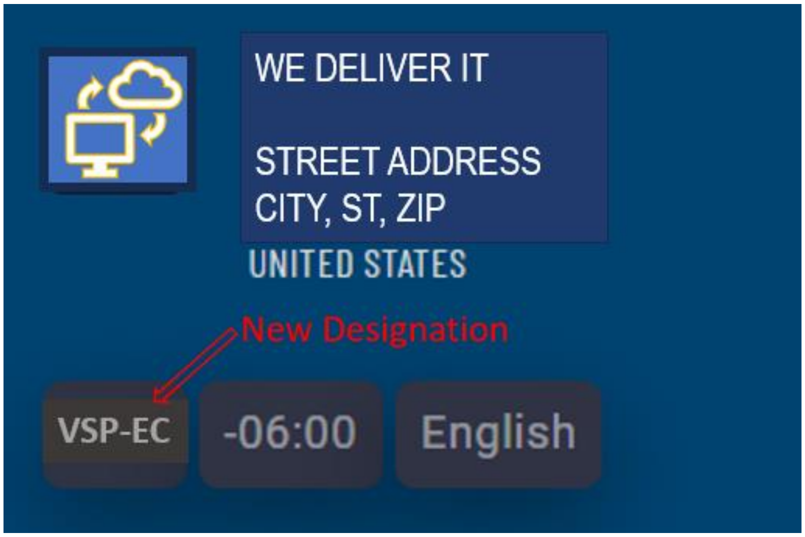
[1] The OSA/OSC is ultimately responsible for understanding the type of CUI they process, store or transmit and for validating the ability of the VSP-EC to provide security capabilities on their behalf. CUI Export control references are too vast to list in this paper, but a couple to start with would be https://www.archives.gov/cui/registry/limited-dissemination, https://www.dodcui.mil/Distribution-Statements/



ECOSYSTEM ROLE

- □ RP
- □ CCP
- □ RPO
- □ CCA
- □ RPA
- □ PI
- □ C3PAO
- □ LTP
- □ LPP
- □ VSP

New Designation



WE DELIVER IT

STREET ADDRESS
CITY, ST, ZIP
UNITED STATES

New Designation

VSP-EC -06:00 English

- The Service Provider SRM must reflect the NIST 800-171 r2 controls the Service Provider implements/performs on their clients' behalf in the manner of Full, Partial or No responsibility per control assessment objective, but no details of the control implementation will be included on the website version (see sample). Posting a high-level SRM with the Service Provider name and date of Validation Assessment will allow for OSAs to revise which of the NIST 800-171 r2 controls and assessment objectives were Validated by a C3PAO for that Service Provider. The Service Provider's SSP should detail and align with the scope of the C3PAO CMMC Level 2 Validation Assessment, and contain the control implementation details reflected in the high-level SRM posted on the Cyber AB website.

- Like a FedRAMP Moderate or High Authorization, the SLA, SSP and SRM provided by a Validated Service Provider should allow equivalency to be met as implemented for the OSA. In areas where the OSA and service provider have deviated from the service provider's Validated SSP and SRM, the OSA can remedy the variation prior to their formal CMMC Level 2 Certification Assessment, or the Service Provider will be required to participate in the OSA CMMC Level 2 Assessment with corresponding artifacts.

- Like a FedRAMP Moderate or High Authorization, the security requirements from the Validated Service Provider's SRM must be documented or referred to in the OSA's SSP.

Service Provider Validation Period:

- Service Provider's CMMC Level 2 Validation Assessment by a C3PAO must be renewed every 18 months to reflect changing Service Provider tools, services, etc. If no major changes have taken place during that time, a simple delta CMMC Level 2 Validation Assessment may suffice. See .Re-Validation Period and Requirement Recommendations.
- The OSAs CMMC Level 2 Certification Assessment which leverages the Service Provider's CMMC L2 Validation Assessment will last the OSA three years, to align with the OSA CMMC assessment cadence.

Service Provider Scoping Recommendations

Per the CMMC Proposed Rule page 172, "External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g. log data, configuration data) must be processed, stored or transmitted on the ESP assets to be considered an ESP."

Why is it important to identify the assets commonly leveraged by Service Providers for a CMMC Level 2 Assessment? Because a precedent has been set by C3PAOs who undergo a DIBCAC assessment of a secure CMMC L2 enclave that has been implemented for the specific purpose of the NIST 800-171A DIBCAC High Assessment, wherein the enclave is not used on a regular basis to perform CMMC-related consulting services (outside of the formal CMMC L2 Assessments). This is an appropriate use of an enclave for a C3PAO. In the Service Provider industry however, it is crucial that the scope of the CMMC Level 2 Validation Assessment includes the people, technology and facilities leveraged in delivery of security and IT services to the OSA, and having a secure enclave would likely not incorporate the applicable assets leveraged by a service provider in their day-to-day duties.

For example, in review of the NIST 800-171 control family **Incident Response (IR),** there are many individual roles representative of trained personnel required to fulfill the control capabilities. In smaller organizations, at the Service Provider staffing level, multiple roles may be performed by in-house and outsourced people, such as:

- Incident handling
- Contingency planning
- Incident response training and operations
- Incident response assistance and support
- Incident response monitoring and reporting
- Personnel (authorities) to whom incident information is to be reported

If the Service Provider performs some of these capabilities and outsources the rest to a Managed Security Service Provider (MSSP) or a 1099 entity that is not based in the US, and if the OSC/OSA they support has ITAR data included in their CUI, the assessment of the Service Provider must include those external personnel filling the IR roles and performing IR capabilities to allow for proper validation of qualified personnel.

As such, the following people, technology and facilities would qualify as assets that come into scope at a Service Provider, if the asset falls into the category of Security Protection Asset as described in the CMMC Level 2 Scoping Guide, or leverages Security Protection Data as described in the CMMC Proposed Rule, regardless of whether the asset directly stores, processes or transmits CUI on behalf of an OSC/OSA.

<u>Example Assets leveraged in Service Delivery:</u>

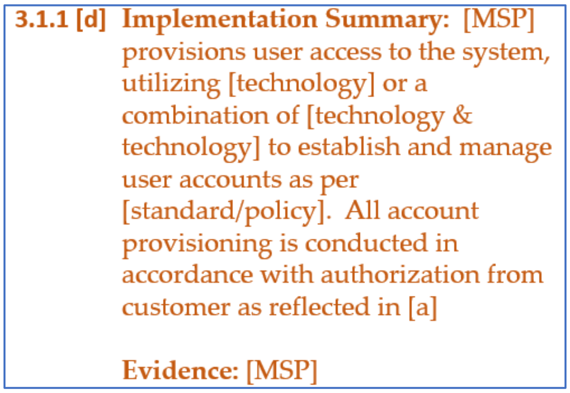
- Service Delivery personnel with physical or logical privileged access to the OSA in-scope environment, both W2 and outsourced (i.e. Helpdesk, SOC or NOC services)
- Authenticated access to the OSA in-scope environment such as Servers, Workstations, Mobile Devices used to provide service via chat, email, or remote support.
- Tools to manage the OSA environment (if provided by a CSP (i.e. SaaS, IaaS, PaaS) FedRAMP Moderate or High applies; if on-prem they must be secured according to NIST 800-171 r2)
  - Patching
  - Remote Helpdesk Assistance
  - Vulnerability Scanning
  - Deployment of Systems
  - Identification, Protection, Detection, Response, Recovery, or Remediation of OSA in-scope assets

    - SIEM, RMM, BDR, MDR, MXDR, Asset Management
    - Password Manager
- Security Related Functions and Programs (Ticket /ITSM, Change Management, Configuration Management, Vulnerability Management, Incident Response Management)
- Network Segmentation Technology used to protect assets in the boundary of the scope at the MSP (Firewall, Switch, etc.)
- MSP Corporate Policies & Procedures:
    - Training of personnel
        - CUI basic training
        - Insider Threat
        - Role Based SAT
        - SecOps Role Based Training
    - Onboarding
        - Screening of Personnel
        - US Citizen or US Person
    - Offboarding & Transfers
- Productivity Applications may be included depending on whether security protection information is processed or stored via the application. For example, if no security protection information is emailed or stored in the ticketing system due to company policy, those assets may be categorized as CRMA. Timesheet or resource management applications that would not be used to store or process security protection information may be categorized as out of scope.

Service Provider Documentation Recommendations

The Service Provider will include their own SSP in their Validation documentation, reflecting the same information required in Security Assessment control 3.12.4 to include the Service Provider’s in-scope infrastructure map and description, the scope components, the asset inventory and the detail of their control implementation (per assessment objective) as reflected in the SRM. Service Providers will include an example Service Level Agreement (SLA) with an OSA as part of their documentation package for Validation.

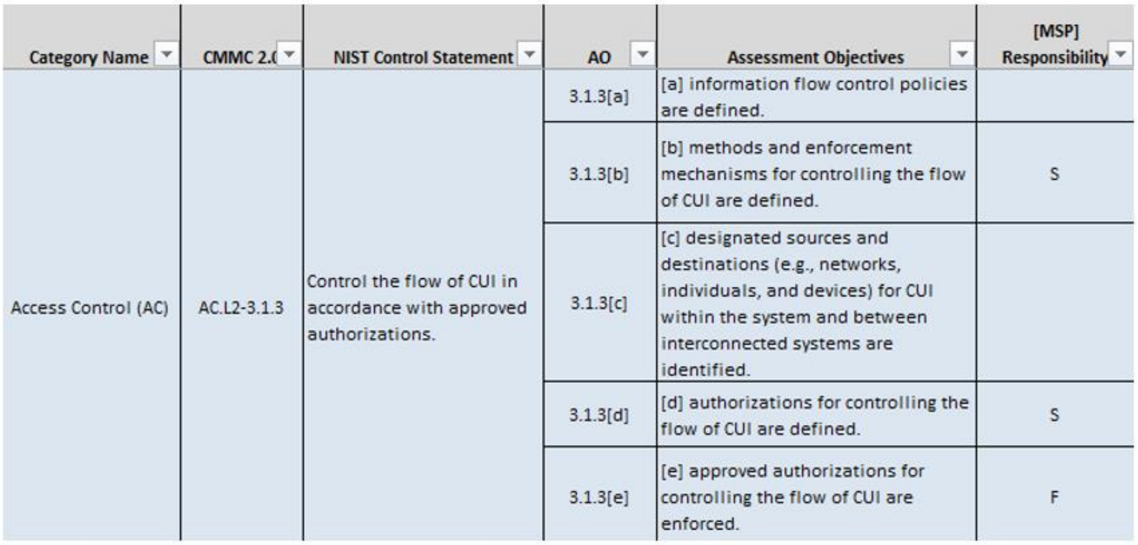
SSP Example:



3.1.1 [d] Implementation Summary: [MSP] provisions user access to the system, utilizing [technology] or a combination of [technology & technology] to establish and manage user accounts as per [standard/policy]. All account provisioning is conducted in accordance with authorization from customer as reflected in [a]

Evidence: [MSP]

SRM Example (high-level):



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

Re-Validation Period and Requirement Recommendations:

The nature of outsourced service delivery is to change the people, process and technology frequently enough to offer the most effective and affordable security technology and professional services to their customers. As such, a Re-Validation by an Authorized C3PAO is recommended every eighteen months, unless a major change is made in a previously assessed asset category that would impact all OSA clients supported by that service provider. An example of an asset category change would be:

- Outsourcing of personnel or responsibilities as a replacement of inhouse resources
- Remote Monitoring & Management (RMM) tool, SIEM tool or MXDR security platform replacement
- Merger or Acquisition of resources with another service provider

Service Provider Scenarios as Examples:

Two types of Service Provider scenarios are included herein, for the demonstration of people, technology and facilities that would come into scope for the CMMC Level 2 Validation Assessment of a Service Provider. **The Scenarios are not meant to infer that any given asset being included as a Security Protection Asset or a Customer Risk Managed Asset would qualify to pass an assessment as described, as the implementation of NIST 800-171 r2 security controls is not a part of this paper.**

Scenario One represents a Managed Service Provider (MSP) whose customer base includes both DIB contractors and commercial businesses such as healthcare and financial services firms. In Scenario One, we have provided two example DIB contractor environments:

Environment #1 that represents Hybrid on-premise CUI assets and cloud-based CUI assets
Environment #2 that represents a DIB contractor environment that is purely cloud-based.

Scenario One MSP does not work with DIB contractors who process, store or transmit the types of CUI that warrant export control restrictions.

Scenario Two represents a Managed Security Services Provider (MSSP) whose customer base is exclusively DIB contractors with the types of CUI that would warrant export control restrictions.

Questions and information:

The paper is presented by The MSPs for the Protection of Critical Infrastructure, an industry group whose mission is to inform the US Government and Critical Infrastructure industries on topics related to Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) dedicated to the National Security mission of maintaining a secure, functioning, and resilient critical infrastructure.
https://www.mspcollective.org
Info@mspcollective.org

Scoping Scenario #1- “We Deliver IT”

Description of MSP

We Deliver IT has half (six out of twelve) of their Tier 1, 2 and 3 Helpdesk technicians dedicated to DIB clients that process, store, or transmit **CUI** of the type that has no export restrictions (i.e. no ITAR/EAR, etc.). They also support the healthcare and financial services sectors. They provide on-prem and remote assistance via RMM tools and leverage an India-based Network Operations Center (NOC) to support customer servers for patching and overnight monitoring/maintenance.

We Deliver IT’s customers are encouraged to leverage a separate MSSP for the security services needed beyond the IT support they provide.

MSP Logical Environment Depiction (See Visio Diagram)

We Deliver IT leverages the following SaaS, IaaS or PaaS solutions:

1. Windows Server 2022 hosted in Azure Commercial, which contains the following:
    a. Folders: Client, Accounting, Sales and Operations
    b. Applications: Accounting, PSA (on-prem, hosted in Azure)
2. Office 365 Commercial including Email, One Drive and Teams
3. EDR/MDR/MXDR SaaS tool
4. SIEM tool
5. RMM tool
6. Vulnerability Scanning tool
7. Password Manager tool
8. Documentation & Configuration Management tool
9. MFA tool
10. Ticketing system

MSP Physical Environment and Personnel Depiction (See Visio Diagram)

We Deliver IT provides an office for employees and allows their staff to work remotely from their homes. The India-based NOC staff work only from their India HQ office.

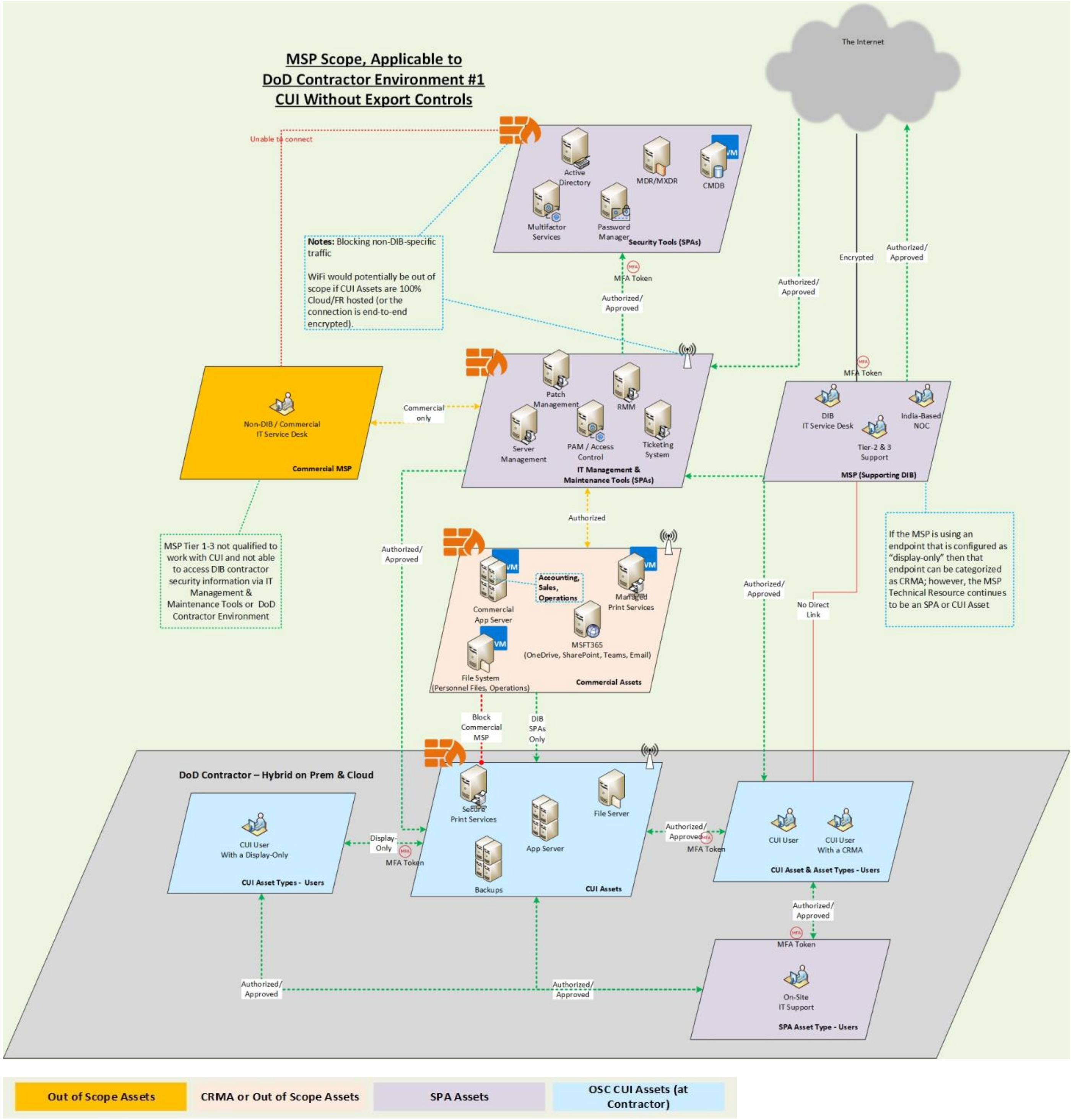
1. The USA MSP HQ has four internal offices
    a. CEO and Office Manager have access to the people, technology and software used in support of the DIB customer environments, but they do not do so via training and policy.
    b. HR and Service Delivery Manager have access to the people, technology and software used in support of the DIB customer environments with appropriate application of NIST 800-171 r2 controls. Their interior doors are controlled with key-card badges and signage for Sensitive Area.
    c. Tier I – Tier III DIB-supporting MSP helpdesk have access to the people, technology and software used in support of the DIB customer environments with appropriate application of NIST 800-171 r2 controls. Their interior doors are controlled with key-card badges and signage for Sensitive Area

d. Tier I – Tier III commercial MSP helpdesk, who do not have access to the technology, software or interior offices leveraged by the DIB-supporting personnel.

2. The India-based NOC has multiple offices with large call-center style cubicles spanning multiple floors of the office building for all service delivery personnel, whether they will interact with a CUI end-client environment or not. Their management works on a different floor from the service-delivery personnel.

DoD Contractor Environment #1:

1. CUI Ecosystem – Hybrid (Cloud and On-premises services) with two locations; Business Location (HQ) and Manufacturing / R&D Location
   i. MSFT GCC-High (License should be important to note)
   ii. SolidWorks
   iii. Product Lifecycle Management (PLM)
   iv. Document Control System
   v. ERP
   vi. 3D Printers



Notes: Blocking non-DIB-specific traffic

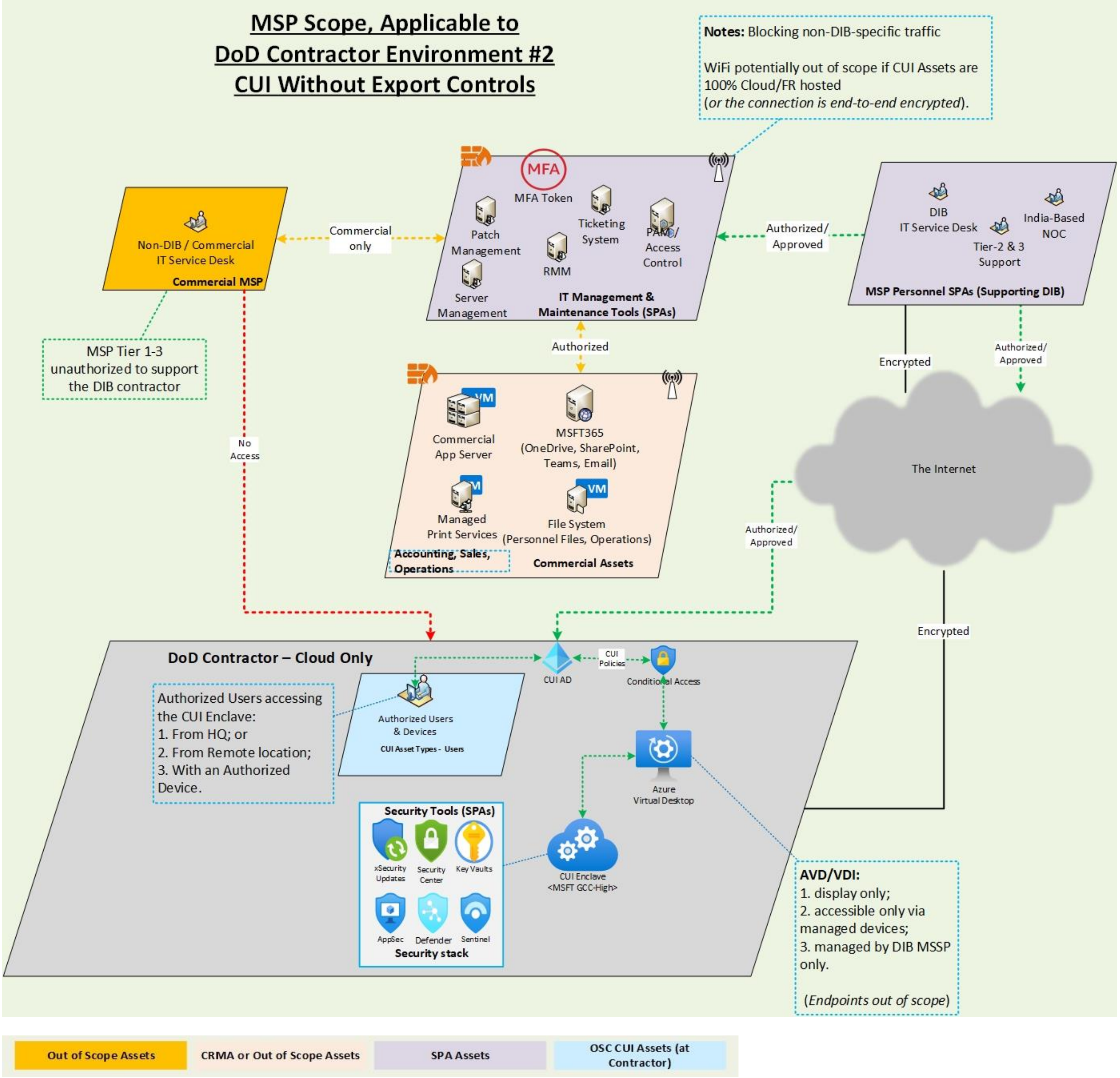
WiFi would potentially be out of scope if CUI Assets are 100% Cloud/FR hosted (or the connection is end-to-end encrypted).

MSP Tier 1-3 not qualified to work with CUI and not able to access DIB contractor security information via IT Management & Maintenance Tools or DoD Contractor Environment

If the MSP is using an endpoint that is configured as "display-only" then that endpoint can be categorized as CRMA; however, the MSP Technical Resource continues to be an SPA or CUI Asset

DoD Contractor Environment #2:

1. CUI Ecosystem – (Cloud Only); Locations: Business office, remote home offices. OSC is a Research Org with no tangible products.
    - vii. MSFT GCC-High (E3, E5)
    - viii. GCC-High Accessed via AVD only (Display Only)



MSP Scope, Applicable to DoD Contractor Environment #2 CUI Without Export Controls

Notes: Blocking non-DIB-specific traffic

WiFi potentially out of scope if CUI Assets are 100% Cloud/FR hosted (*or the connection is end-to-end encrypted*).

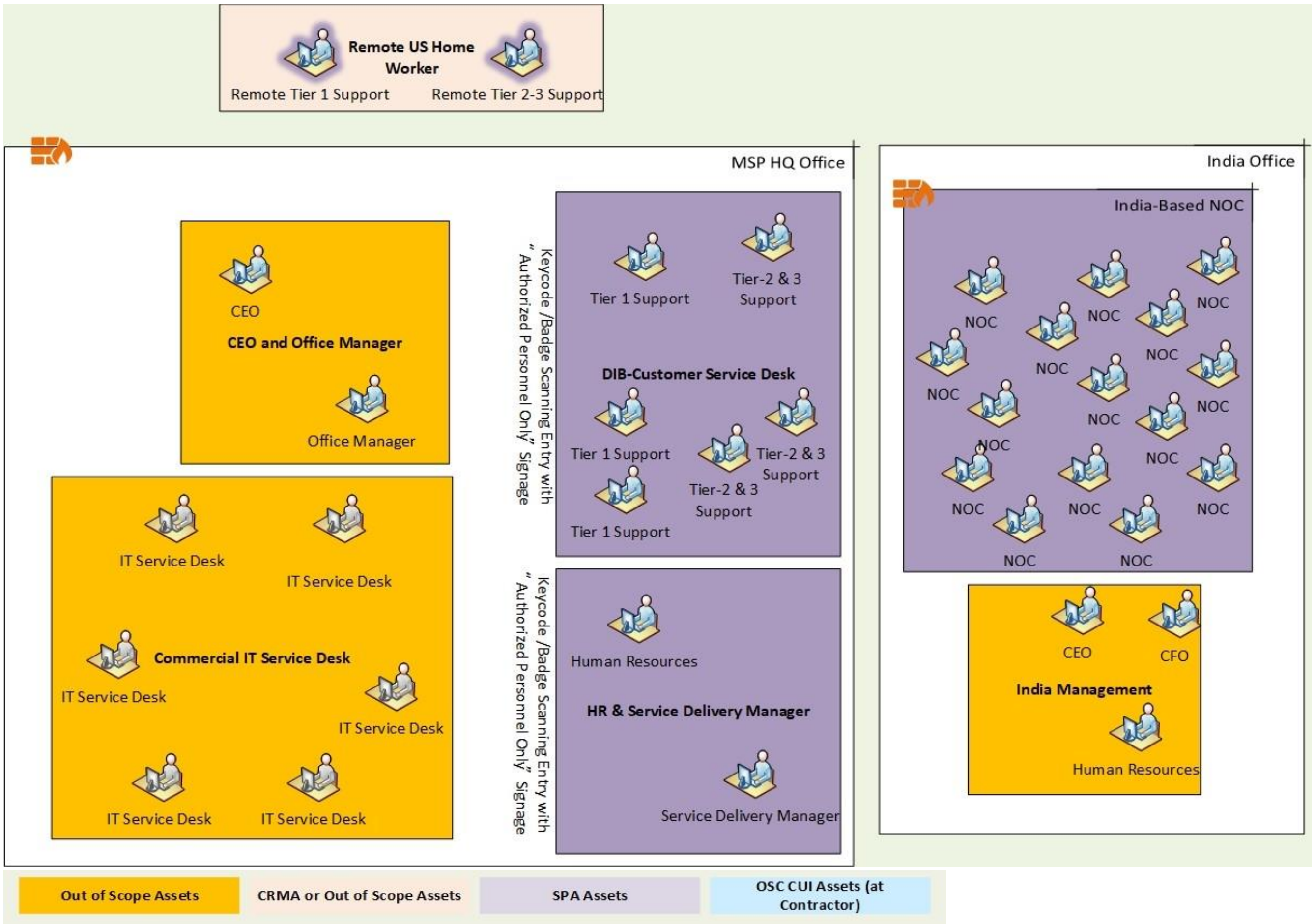
MSP Tier 1-3 unauthorized to support the DIB contractor

Authorized Users accessing the CUI Enclave:
1. From HQ; or
2. From Remote location;
3. With an Authorized Device.

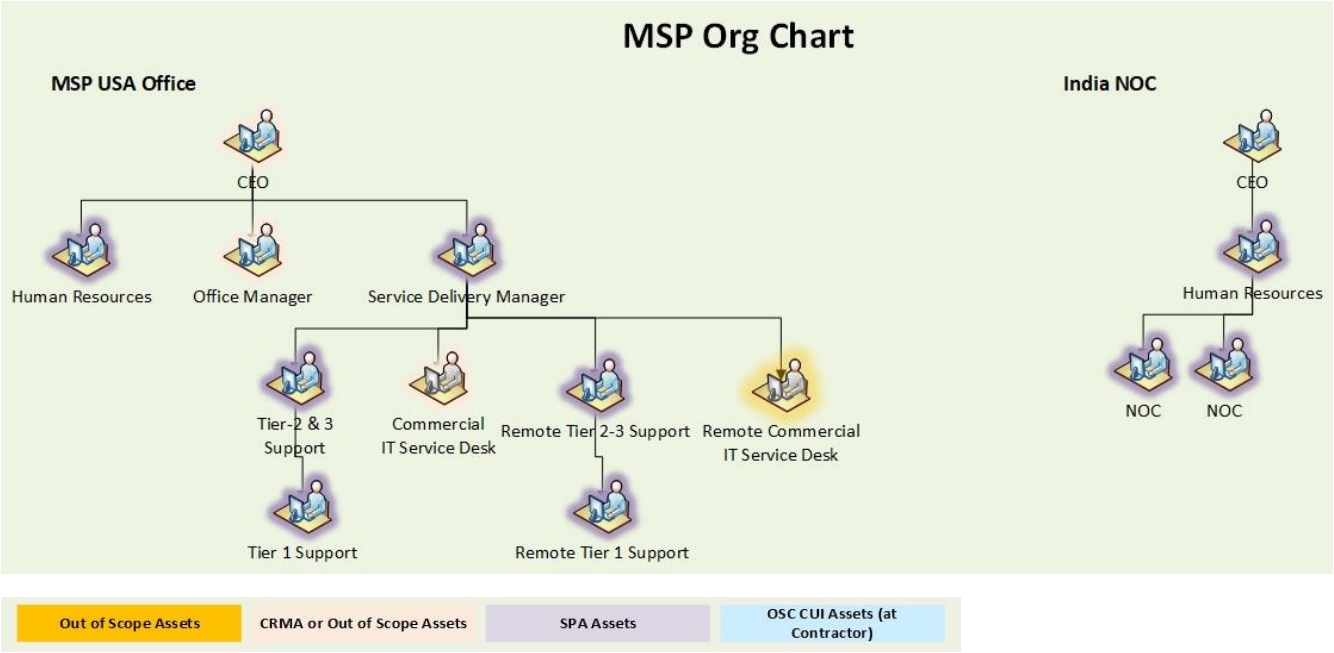
AVD/VDI:
1. display only;
2. accessible only via managed devices;
3. managed by DIB MSSP only.

(*Endpoints out of scope*)

MSP Physical Environment Scope



MSP Org Chart



Scoping Scenario #2 – “We Secure IT”

Description of MSSP

We Secure IT has 100% of their SOC Analyst I, II, & III team members dedicated to DIB clients. They only provide remote MSSP services via RMM tools; they have no on-prem support. The company is headquartered in the USA, where it has on-premises infrastructure that supports their client base.

We Secure IT's clients are encouraged to leverage a separate provider or in-house staff for IT services needed beyond the cybersecurity support they provide.

MSSP Logical Environment Depiction (See Visio Diagram)

We Secure IT leverages the following network and security solutions:

USA Only Location

- RMM (FedRAMP)
- Virtual Machine hosting security tooling
  - SIEM & SOAR - used in client environments
  - XDR - used in client environments
- Firewall/VPN
- Switch
- Google Workspace (Email, Drive, Meetings) with Endpoint Management integration
- Digital Voice
- Windows 10 Endpoints
- 1 Multifunction Printer
- Cable Modem
- Wireless Router

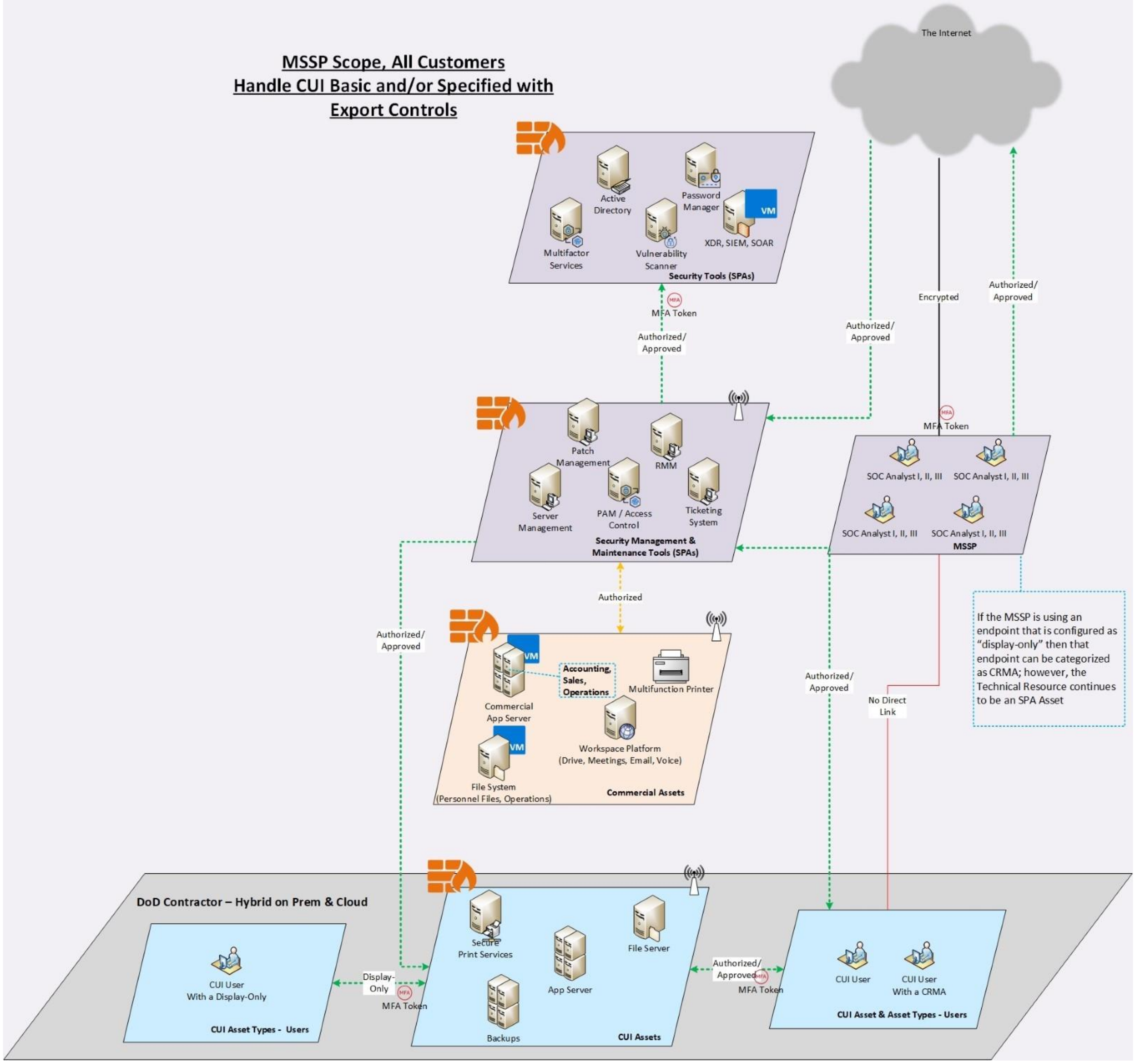
MSSP Physical Environment and Personnel Description (See Vizio Diagram)

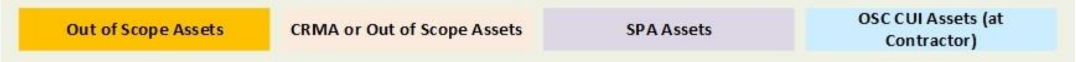
We Secure IT rents a large suite in a commercial office building. The front door to the main suite requires badge entry and all visitors must be signed in and escorted while on premises.

- Key fob access to office
- Server room is locked and requires
- Security Camera System monitoring all areas

We Secure IT only employs US citizens on their team, including maintenance and cleaning personnel. The CEO, Office Manager and Finance Manager have access to the people, technology and software used in support of the DIB customer environments with appropriate application of NIST 800-171 r2 controls, but they do not leverage those assets and work in their own office. The SOC Analysts, Human Resources and Service Delivery Manager have access to the people, technology and software used in support of the DIB customer environments with appropriate application of NIST 800-171 r2 controls. Their interior doors are monitored with 24/7 security cameras.

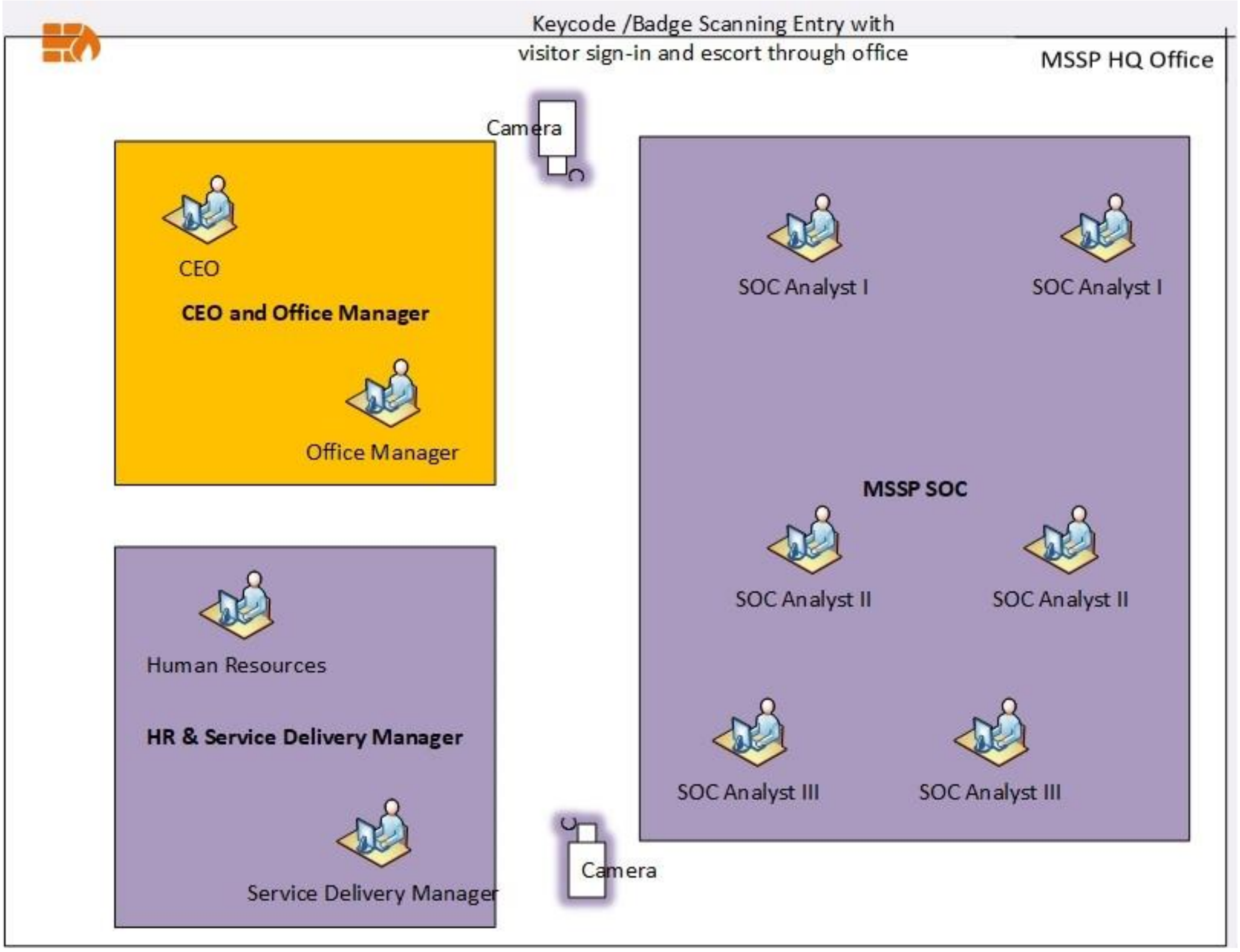
MSSP Logical Environment Scope



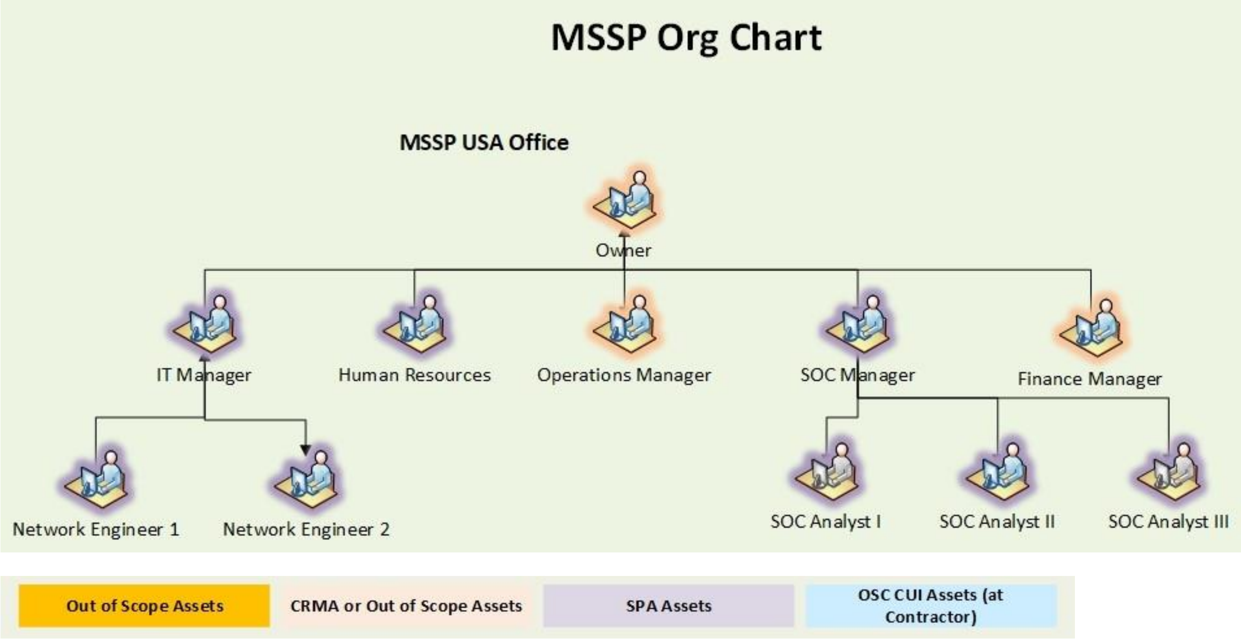


Out of Scope Assets	CRMA or Out of Scope Assets	SPA Assets	OSC CUI Assets (at Contractor)

MSSP Physical Environment Scope



MSSP Org Chart


MSSP Org Chart
MSSP USA Office
Owner
IT Manager
Human Resources
Operations Manager
SOC Manager
Finance Manager
Network Engineer 1
Network Engineer 2
SOC Analyst I
SOC Analyst II
SOC Analyst III
Out of Scope Assets
CRMA or Out of Scope Assets
SPA Assets
OSC CUI Assets (at Contractor)