CMMC 2.0 Scoping Scenarios Analysis

Purpose of this analysis

Promote standardization of CMMC scoping

Identify areas where more clarification is needed

Encourage conversation about applicable practices

Intended audience

Cybersecurity Maturity Model Certification (CMMC) assessors, defense contractor cybersecurity staff, and Department of Defense

January 19, 2022

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Contents

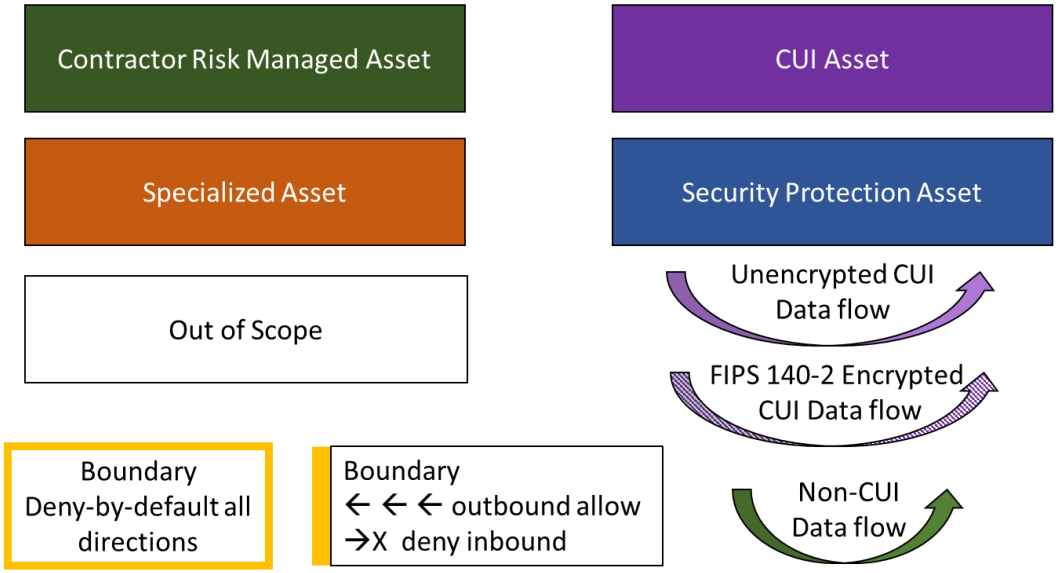
Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Background

This paper was inspired by 1) the questions posed by students while teaching Certified CMMC Professional classes, 2) over 200 conversations with defense contractors about their network design and readiness for CMMC.

In December 2021, I posted partial scenarios on LinkedIn for review by my fellow CMMC professionals. Several responded with their analysis and thoughts, which helped influence the final "Answer" section for each scenario. Thank you to those cybersecurity professionals who responded! - Amira Armond

Conventions used in this document



Abbreviations

CUI	Controlled Unclassified Information	OT	Operational Technology
CMMC	Cybersecurity Maturity Model Certification	DoD	Department of Defense
FIPS	Federal Information Processing Standard	SPA	Security Protection Asset
OSC	Organization Seeking Certification	CRMA	Contractor Risk Managed Asset
MDM	Mobile Device Management	VDI	Virtual Desktop Infrastructure
LAN	Local Area Network	VLAN	Virtual Local Area Network
SIEM	Security Information and Event Management	SSP	System Security Plan
C3PAO	Certified Third Party Assessment Organization	CIO	Chief Information Officer

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Source for CMMC Level 2 Scoping Guidance

This analysis builds on the CMMC Level 2 Scoping Guidance published by the Department of Defense.

The official guidance can be downloaded from the DoD Acquisition & Sustainment website at https://www.acq.osd.mil/cmmc/documentation.html

Please ensure that you are familiar with the CMMC Level 2 Scoping Guidance prior to reading this analysis.

Disclaimer

This document is not intended to contradict or replace official Department of Defense (DoD) guidance for CMMC. When in doubt, always follow DoD guidance and consult a paid cybersecurity or legal professional.

How to read each scenario

This analysis contains twelve assessment scenarios. The scenarios reflect common architecture designs used by defense contractors (for good or bad) and highlight topics which are not well discussed in current DoD guidance.

Each scenario starts with a network diagram which has assets partially identified. If an asset is identified as a certain asset type (such as a CUI Asset), you should use this identification during the scenario. Unidentified assets are typically colored gray or tan.

Following the scenario is a description of the contractor's architecture and (hopefully) enough information to categorize the unidentified assets. If something is not discussed, you should treat it as compliant and/or irrelevant to the scenario.

Next, a series of questions is asked, which is the interactive portion of this exercise. You will get the most benefit if you try to answer the questions for yourself.

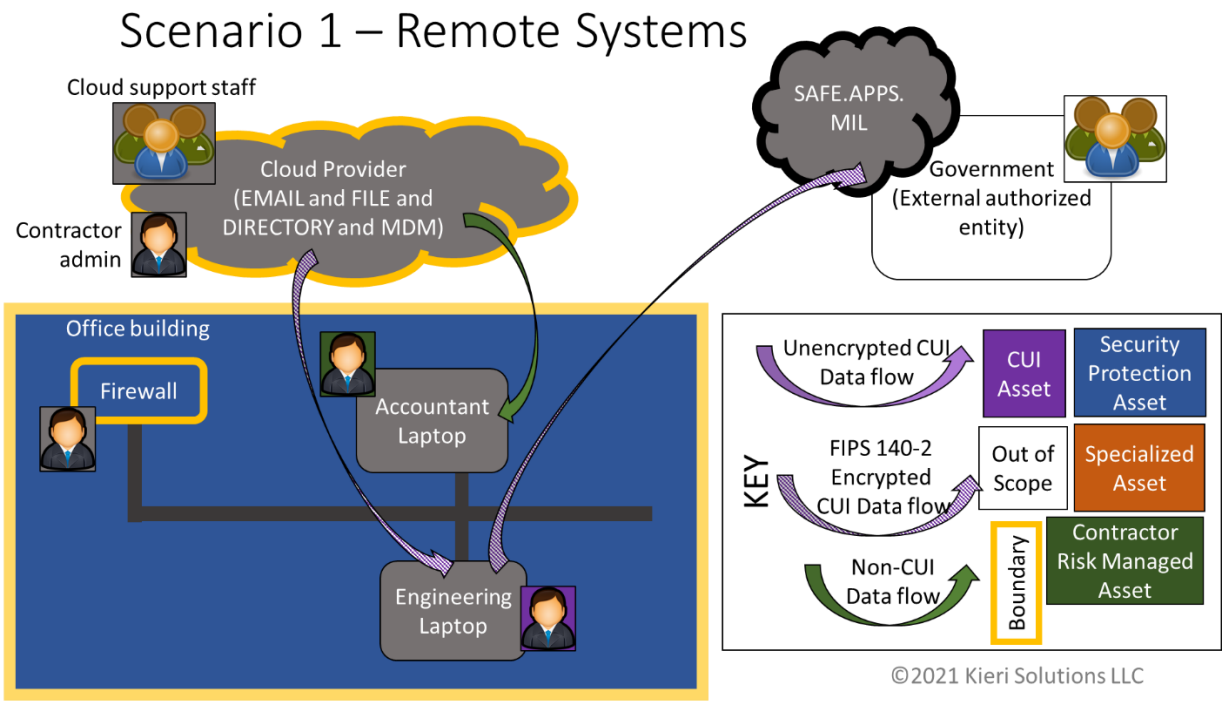
The second portion of the scenario is the Answers, where interpretation and analysis are listed. This is intended to give you insight into an assessor's thought process.

Finally, in most scenarios, we have a Key Concept box. These key concepts are the most valuable portion of the analysis and can be used as mental models for assessors.

Disclaimer: There is no guarantee that the answers in this document are correct. There is no guarantee that this is how the author or contributors would assess a future client. This analysis is submitted to the community to promote consistency and identify areas which need more clarification from the Department of Defense.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 1 – Remote Systems



The Organization Seeking Certification (OSC) is using the Government Community Cloud version (FedRAMP authorized) of Microsoft 365 for email, file, directory, and mobile device management.

Microsoft 365 is managed on the front-end by a company admin and managed on the back end by Microsoft. Controlled Unclassified Information (CUI) is held inside Microsoft 365 (SharePoint and Exchange). Other aspects of Microsoft 365 perform security for SharePoint, Exchange, and the company laptops.

The company transfers CUI between themselves and the government client using SAFE.APPS.MIL, which is a secure file sharing website provided by the US Government.

The company firewall is managed by company admin staff.

The Engineering Laptop is connected to Microsoft 365 for file, email, directory, and mobile device management. The Engineering Laptop has CUI stored inside it on the hard drive. The Engineering laptop user has access to file locations with CUI.

The Accountant Laptop is connected to Microsoft 365 for file, email, directory, and mobile device management. The Accountant laptop user account has no access to CUI file locations.

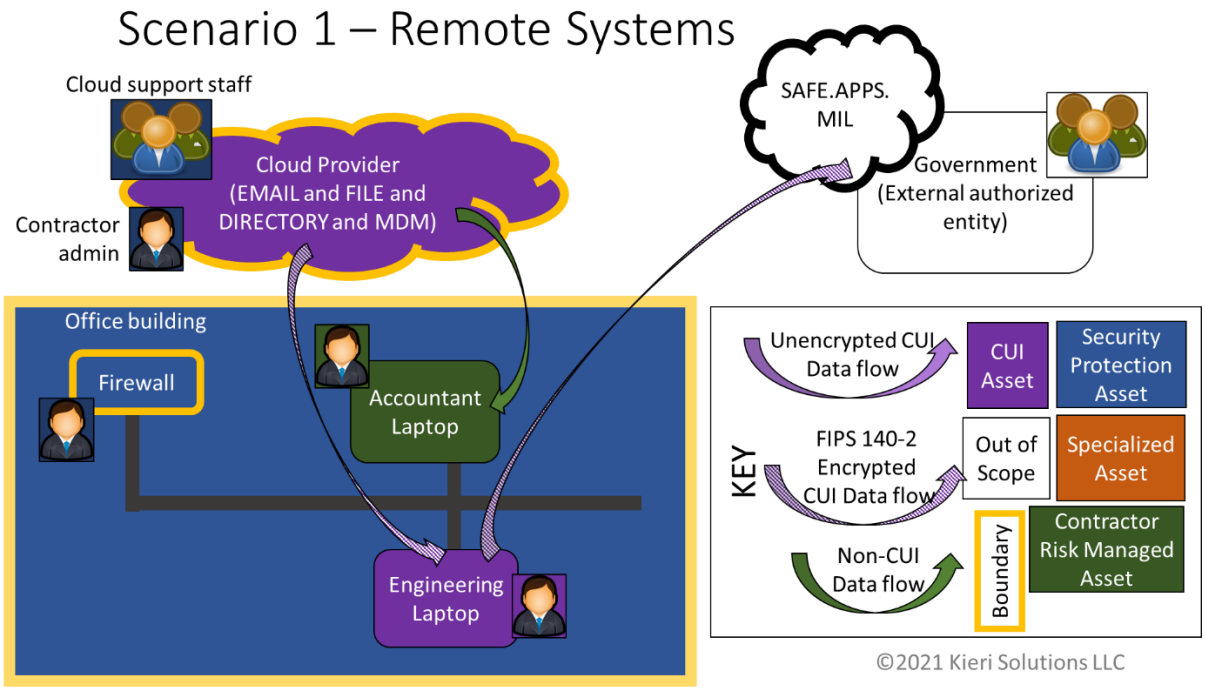
Questions

1) What type of asset is the Accountant Laptop?
2) What type of asset is the Engineering Laptop?
3) What type of asset is the Contractor Admin who manages the Firewall?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

4) What type of asset is the Cloud Provider?
5) What type of asset is the Contractor Admin who works on the cloud front-end?
6) What type of asset is the Cloud Support Staff that work on the cloud back-end?
7) What type of asset is SAFE.APPS.MIL?

Answer



1) What type of asset is the Accountant Laptop? **Contractor Risk Managed Asset (CRMA)**
2) What type of asset is the Engineering Laptop? **CUI Asset**
3) What type of asset is the Contractor Admin who manages the Firewall? **Security Protection Asset (SPA)**
4) What type of asset is the Cloud Provider? **CUI Asset**
5) What type of asset is the Contractor Admin who works on the cloud front-end? **SPA**
6) What type of asset is the Cloud Support Staff that work on the cloud back-end? **SPA**
7) What type of asset is SAFE.APPS.MIL? **Out-of-Scope**

Analysis

All administrator staff for the cloud and contractor perform security functions whether they are doing front-end, back-end, or on-premises admin work. When staff are both users of CUI and protectors of CUI, CUI Asset is more applicable. Cloud administrator staff will be Security Protection Assets if they do

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

not view customer data. Back-end security by the cloud provider (staff, processes, facility, systems) should be discussed in the contractor's System Security Plan (SSP) when they perform CMMC-required security protections for the contractor. This is especially true when CUI is put onto the cloud provider's systems (see **Thoughts on "Applicable practices"**).

The cloud provider could either be "in the room" during assessment or you could show proof that the cloud provider is doing their back-end responsibilities. This is exactly the same expectation for cloud providers as it is for other External Service Providers like Managed Service Providers. Even if those back-end staff cannot access the contractor's CUI directly (due to logical restrictions), they still perform required security for the systems that they manage. Note: It is very unlikely that cloud providers (especially the big ones) will participate in their client's CMMC assessments. Instead, they are more likely to provide third-party attestation (via a FedRAMP audit report and Shared Responsibility Matrix in this case) that their product complies with the security controls required by CMMC.

The Accountant Laptop is a CRMA because it is prevented from accessing CUI through administrative and technical means (permissions).

The Engineering laptop is a CUI Asset because it stores, processes, and transmits CUI.

SAFE.APPS.MIL and the Government entity are Out-of-Scope because they are covered by a different authorization boundary (the government's). Since the government has assessed SAFE.APPS.MIL and is in control of its security, it should not be part of the assessment scope for the contractor. The contractor should describe the data flows to SAFE.APPS.MIL within their System Security Plan (SSP) and/or procedures and/or user training since it is a key input-output method. Authorization boundaries are discussed in depth in **Scenario 12 – Authorization Boundary**.

The Cloud Provider should ideally be split into sub-systems which individually are identified as CUI Assets and Security Protection Assets. If we must look at it together as one category, CUI assets have a higher priority and more applicable practices than Security Protection Assets.

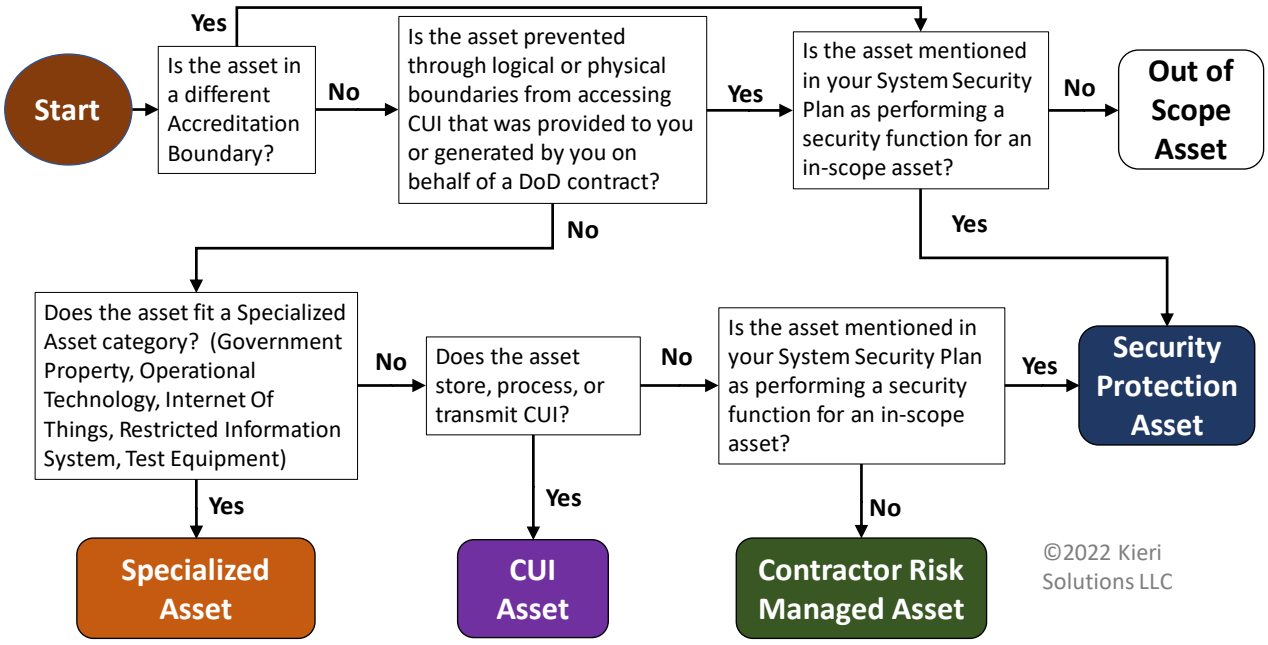
Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: Choosing between multiple correct asset categories.

There is no guidance from the DoD at this time regarding how to prioritize when an asset could fit into multiple categories.

Why prioritize one category instead of simultaneously applying multiple categories to an asset? The logic for multiple categories breaks down when we consider CUI Assets and Specialized Assets. If an asset were both a Specialized Asset and a CUI Asset simultaneously, it would be assessed. This is obviously not the intention of the scoping guide. Therefore, we need to pick the "best" category for each.

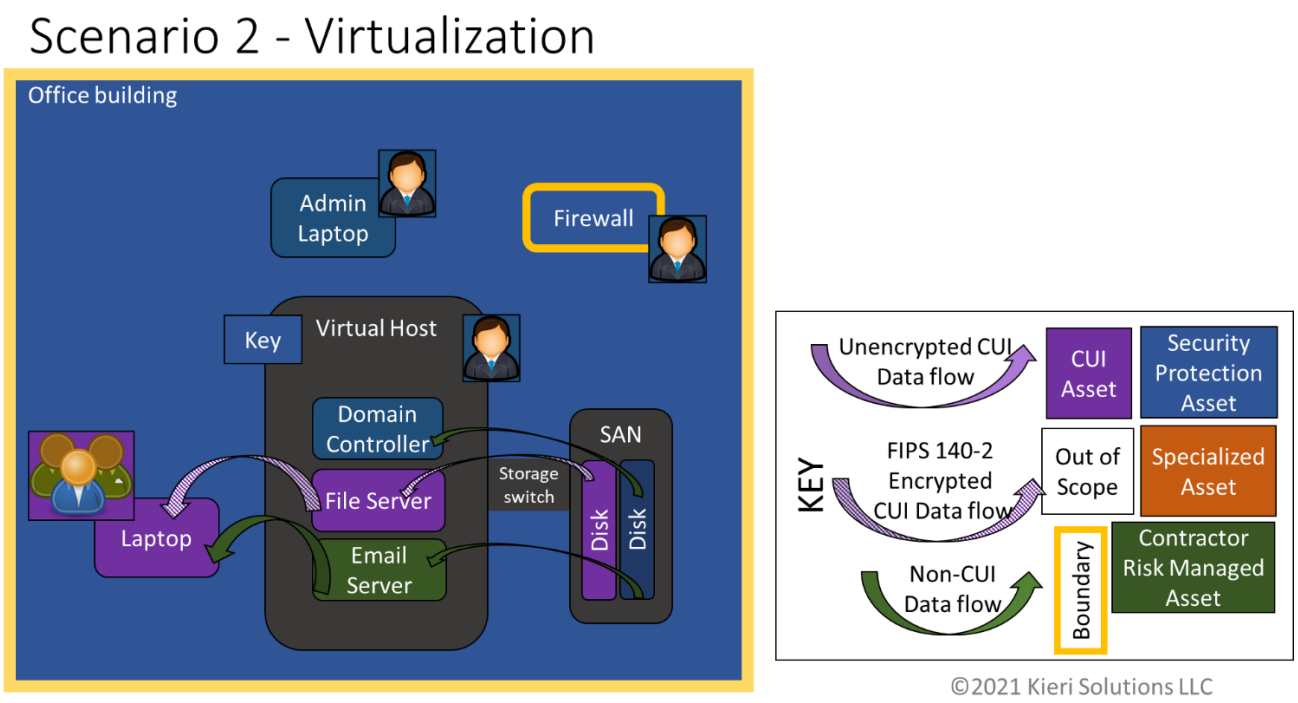
Below is a suggested decision flow[1] on how to make this determination until the DoD provides clarity. This flow purposefully restricts Security Protection Assets from having any CUI and aggressively defines Out-of-Scope to limit the amount of "SPA chaining". CUI Assets are assumed to be fully assessable for all applicable practices, including security functions that they perform on behalf of other assets. This results in the same security requirements as when CUI-containing assets are categorized as SPAs.



[1]Jeff Baldwin: An argument can be made that Security Protection Assets should be identified with the highest priority (compared to Specialized Asset or CUI Asset). This decision flow would require that Security Protection Assets be assessed against all compatible practices to prevent gaps in security and would require different sub-categories of SPA for internal versus external versus Commercial-Off-The-Shelf assets and sub-categories based on whether SPAs have CUI or not. This topic needs clarification from the DoD.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 2 – Virtualization



The defense contractor has their entire network on-premises.

Users access CUI on their laptops, which is stored centrally on a virtual file server. The virtual file server has a large quantity of CUI. The file server is configured to use Federal Information Processing Standard (FIPS) 140-2 validated cryptography for file transfers.

Users access email on their laptops, which is stored centrally on a virtual email server. There is no CUI in email.

The accounts, laptops, and servers are managed using a virtual Domain Controller.

The virtual servers are inside a physical Dell R630 server running VMware vSphere 7 (a virtual host operating system). Storage for the vSphere operating system (no CUI) is internal to the Dell R630.

Storage for the virtual servers is held in the Storage Area Network (SAN) in virtual disk files which are encrypted by VMware's BoringCrypto Module (FIPS 140-2 validated module cert #4028). The virtual files were encrypted by the VMware virtual host prior to being stored in the SAN. The VMware virtual host controls the decryption key.

The SAN is connected to the virtual host using a dedicated high speed storage switch. The files are transmitted using the iSCSI protocol, which limits its connection to only the virtual host using an Authorized Initiators list.

The file server has a virtual disk file as well as a virtual swap file in the SAN. The file server's virtual disk files are encrypted by VMware. The file server's virtual swap file is also encrypted by VMware.

The admin staff uses their admin laptops to manage the firewall, servers, user laptops, and SAN. The Admin Laptops do not access CUI by policy.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Everything inside the office building is physically connected to the Local Area Network (LAN) (not pictured).

Questions

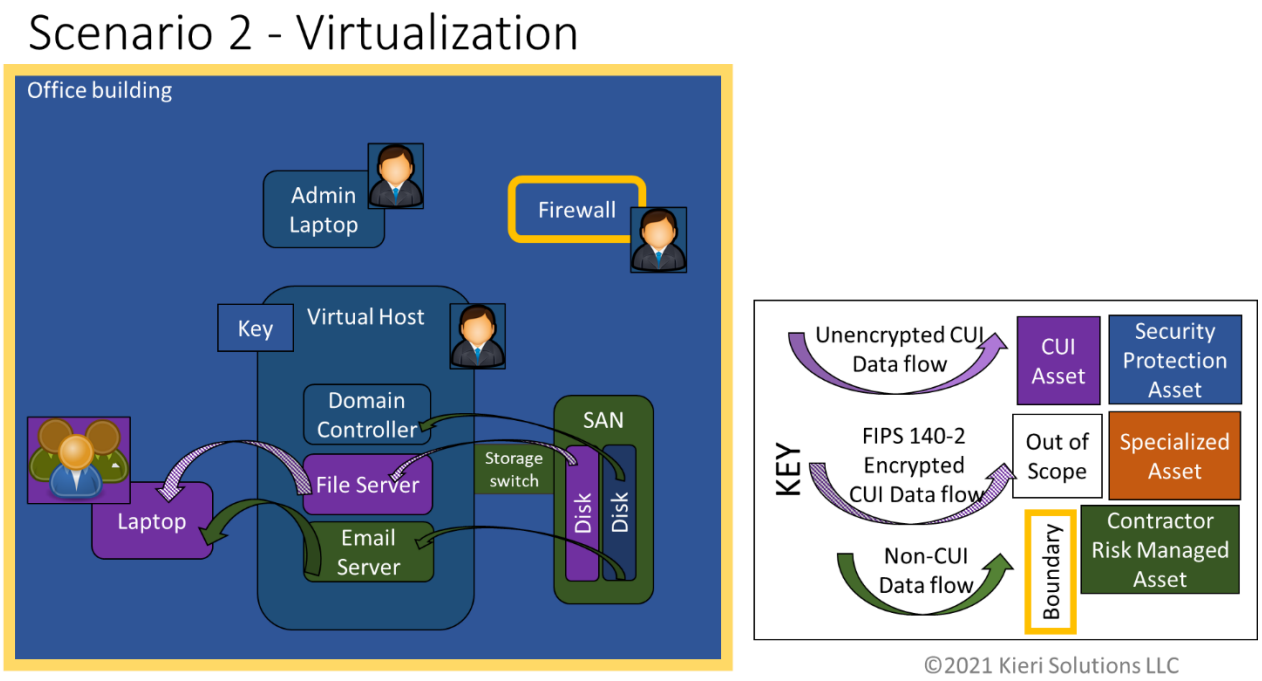
1) What type of asset is the Virtual Host?

2) Should the virtual servers be assessed against a different set of controls than the Virtual Host?

3) What type of asset is the SAN?

4) What type of asset is the storage switch (between the host and SAN)?

Answer



1) What type of asset is the Virtual Host? **SPA**

2) Should the virtual servers be assessed against a different set of controls than the Virtual Host? **Yes**

3) What type of asset is the SAN? **CRMA**

4) What type of asset is the storage switch (between the host and SAN)? **CRMA**

Analysis

The virtual servers include CUI Assets, CRMA, and SPA and should have different controls assessed based on their function. Virtualization should be considered an effective boundary between the systems

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

and between the virtual host and the systems, at a quasi-physical level. Logical separation (such as network) must be performed similarly to any device on the network.

The virtual host is a SPA because it doesn't touch CUI but provides security functions for CUI (due to logical segmentation of virtual machines from the host operating system).

The SAN should not be considered a CUI asset because the data is encrypted prior to being placed onto the SAN and the SAN has no ability to decrypt the ciphertext. This is discussed more in Scenario 8 "Is FIPS enough?"

The SAN also performs no security function that is being assessed under CMMC Level 2. The SAN is not a Security Protection Asset because it does not influence security of the CUI disk files (again, because they are encrypted with the key held in the Virtual Host). The SAN would affect failover and redundancy of the virtual servers, but we aren't assessing those functions.

Because the SAN is connected to CUI assets (because it is on the same network and there are no boundaries between them), it would be categorized as a CRMA.

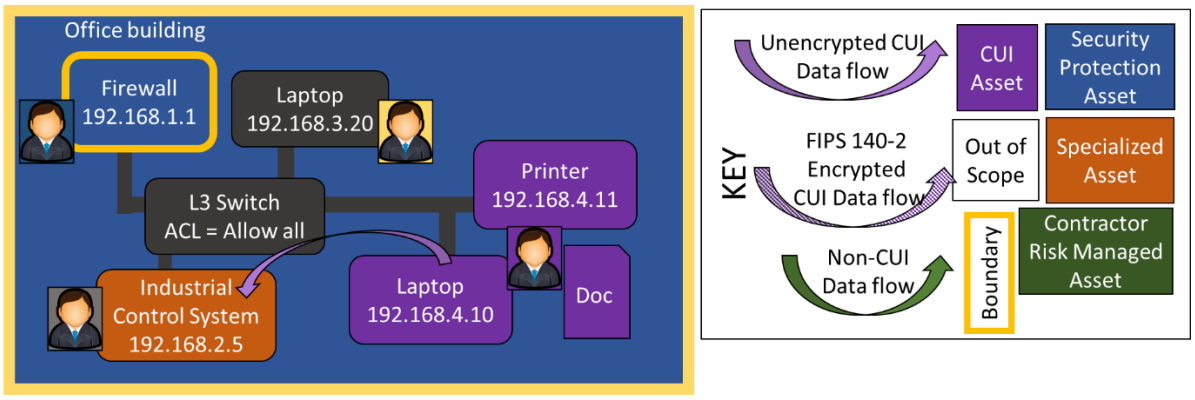
The high-speed storage switch would normally be a CUI asset because iSCSI traffic is a plaintext protocol, but because the virtual disks are encrypted using a FIPS 140-2 validated module at the host, the data would be encrypted in transit, even under iSCSI. Ciphertext should not be treated as CUI. The high-speed storage switch is a CRMA.

Key concept: Is an asset an SPA if it performs controls not required by CMMC?

Assets would only be categorized SPA if they perform controls required by CMMC under Level 2. So, a device that does not perform a CMMC required security requirement would not be considered an SPA, but more likely a CRMA.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 3 - VLANS



©2021 Kieri Solutions LLC

This is a defense contractor who specializes in manufacturing aircraft parts. The CUI category is Controlled Technical Information (CTI).

Inside their facility, they have a Local Area Network (LAN) which is split into multiple Virtual LANs (VLANs) using a Layer 3 switch. The Layer 3 switch performs routing between each VLAN (which are used for different Class C subnets). The access control list on the switch does not deny any type of traffic.

The Firewall functions as a boundary between the LAN and the Internet.

Computer Aided Design (CAD) diagrams are transmitted without encryption from the purple laptop to the Industrial Control System (ICS) across the network. The ICS cuts parts out of metal blanks. The ability for devices to "overhear" this transmission is limited to the Layer 3 Switch and devices on the 192.168.4.x and 192.168.2.x VLANs.

The tan user (near the gray laptop) performs bookkeeping and does not participate in manufacturing, but they have unrestricted access to the shop floor. The gray laptop (the bookkeeping laptop) can establish communications with any devices on the network, no matter what VLAN they are on, because the access control list on the switch does not deny traffic.

The gray user (near the Industrial Control System) maintains and programs the ICS and walks through the shop floor but does not touch any CUI laptops.

The printer is on the same subnet as the purple laptop. The printer is used to create physical diagrams which are posted on the shop floor for use during assembly.

Questions

1) What type of asset is the Layer 3 switch?

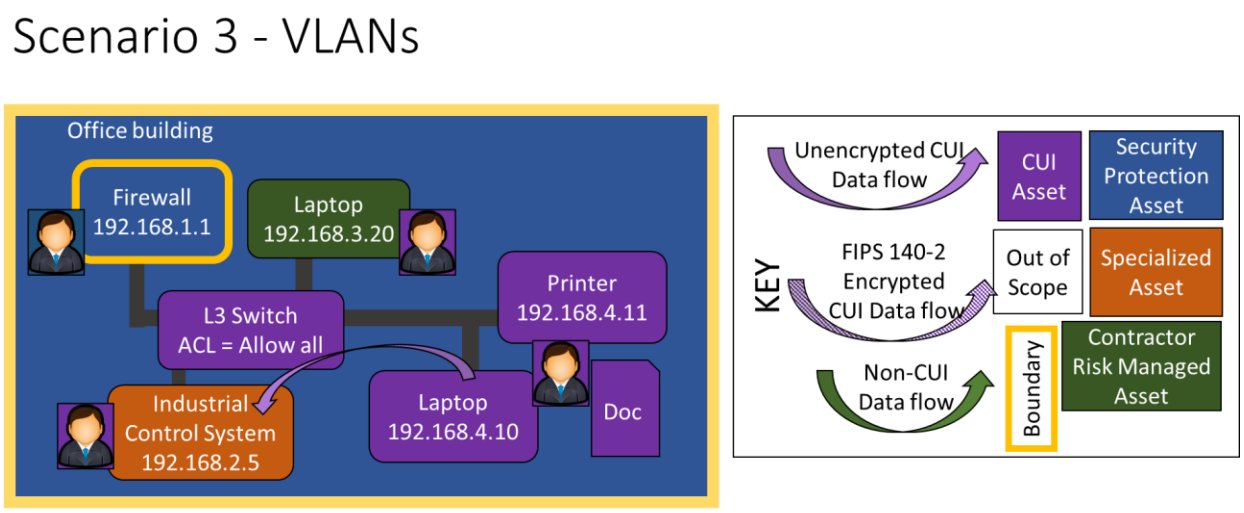
2) Since it is on a different VLAN, should the gray laptop be Out-of-Scope?

3) Should the tan user be in-scope because they are physically in the facility? What type of asset is the tan user?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

4) What type of asset is the gray Industrial Control System user?

Answer



©2021 Kieri Solutions LLC

1) What type of asset is the Layer 3 switch? **CUI Asset**

2) Since it is on a different VLAN, should the gray laptop be Out-of-Scope? **No. VLANs by themselves are not effective boundaries if traffic can route freely between them.**

3) Should the tan user be in-scope because they are physically in the facility? What type of asset is the tan user? **Yes. CUI Asset**

4) What type of asset is the gray Industrial Control System user? **CUI Asset**

Analysis

The VLAN by itself is not effective segmentation because there is no boundary which stops open communication between the VLANs. The Layer 3 switch is routing all traffic between the VLANs on demand, without any firewall rules set. VLANs in most companies are used as the diagram shows – to create separate subnets for IP address management, but they are not used as boundaries or segmentation. VLANs should only be considered effective boundaries if no routing is enabled between the VLANs or an Access Control List with deny-by-default rules effectively controls communications between VLANs.

The switch is a CUI asset because it is transmitting CUI between the laptop and the Industrial Control System (ICS). The switch would also transmit CUI between the laptop and the printer, assuming that the print protocol is not encrypted.

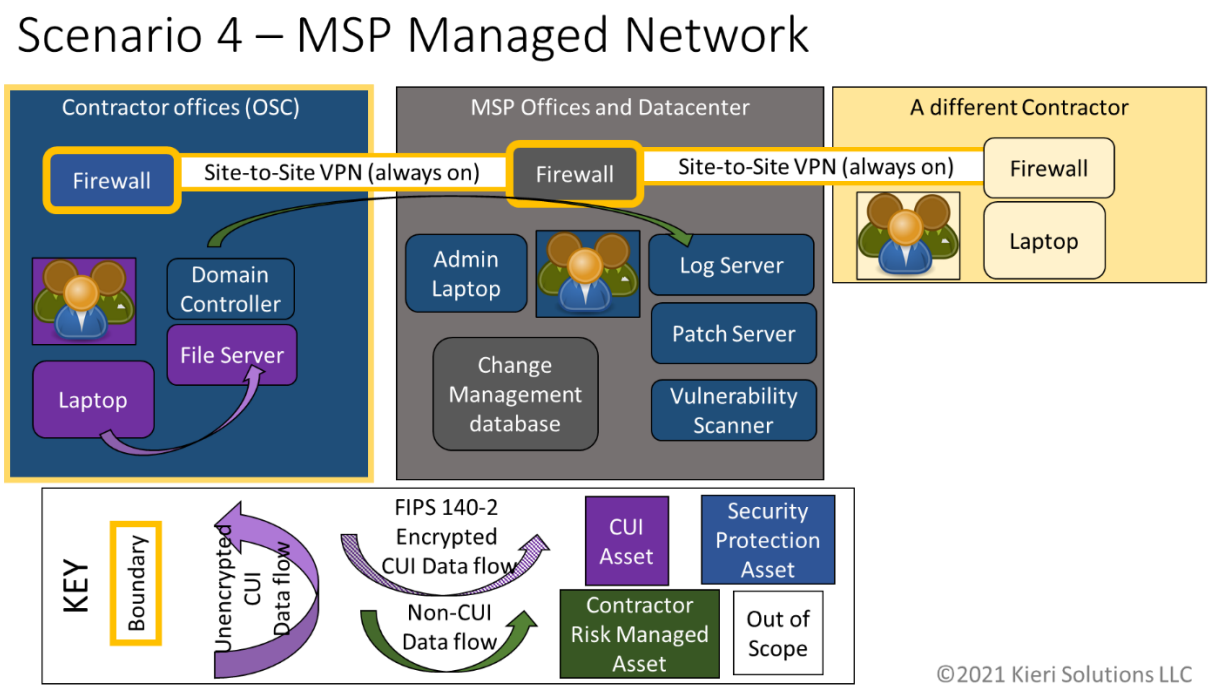
Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

The user of the Industrial Control System is a CUI asset because they interact with CUI on the Industrial Control System and access the shop floor.

The tan user of the gray laptop is a CUI asset because they have access to the shop floor.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 4 – Managed Service Provider



The OSC contractor office has a simple network design (single subnet) and has CUI assets and Security Protection Assets as described.

All administration and security is performed by the Managed Service Provider (MSP), which uses site-to-site Virtual Private Networks (VPNs) to manage their clients. Each client is on a separate address range and routing on the Managed Service Provider's firewall is used to send traffic to the correct client.

The VPN between the MSP and its clients allows the following protocols to any destination from the MSP network: HTTP, HTTPS, RDP, Telnet, SSH, SFTP, FTP. The MSP firewall allows inbound traffic from clients to the log server and patch server. The vulnerability scanner from the MSP is allowed outbound all ports and all destinations. Other ports and protocols are denied.

The OSC firewall accepts all traffic that passes over the VPN from the MSP network. The OSC firewall limits communication to-and-from the Internet. The OSC states in their system security plan that they do not consider the VPN between their network and the MSP to be a boundary.

The MSP has multiple clients that they administer in the same way, using shared Security Protection Assets and site-to-site VPNs.

Questions

1) Is the different contractor (tan) Out-of-Scope or a Contractor Risk Managed Asset?

2) What type of asset is the MSP firewall (grey)? Would it be expected to perform the same security practices as the contractor firewall, or a smaller set?

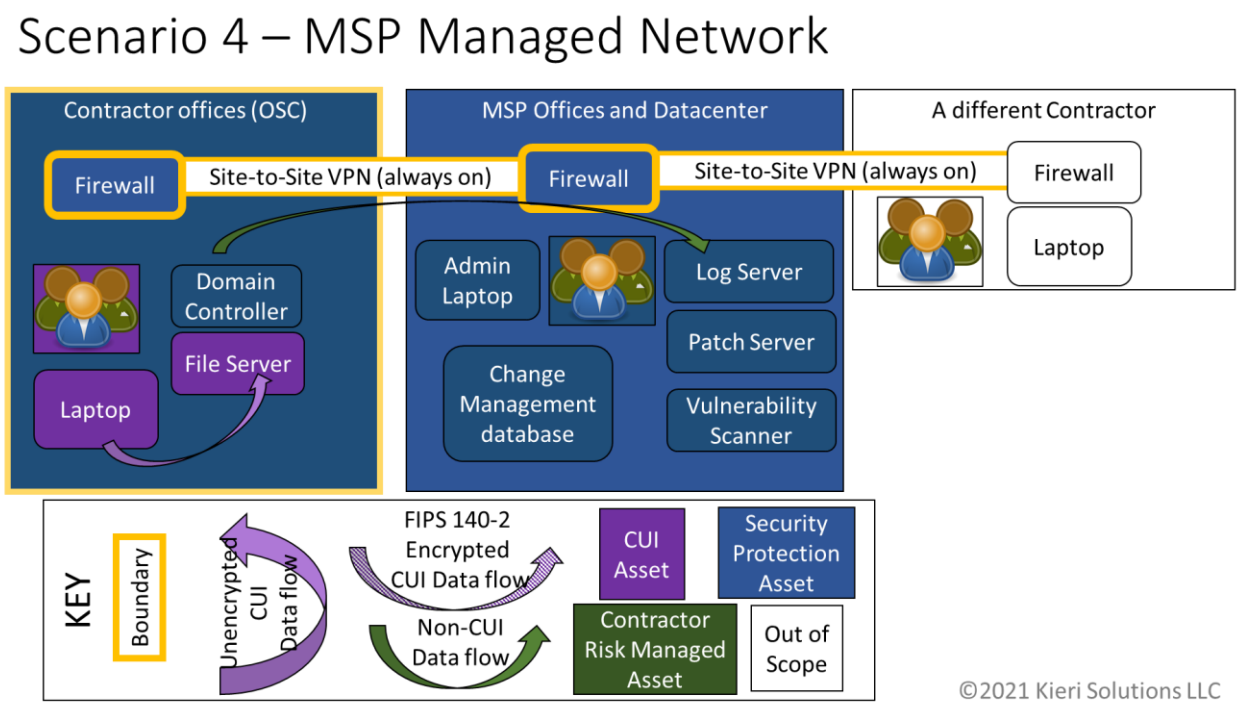
3) What practices would be applicable to the MSP's Change Management database? Would it be an assessable asset?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

4) What type of asset is the MSP's physical facility?

5) Given the interconnections between networks, is it possible for the contractor to pass their CMMC Level 2 audit assuming that everything in-scope for assessment passes their assessable practices? If not, what reason would you give?

Answer



1) Is the different contractor (tan) Out-of-Scope or a Contractor Risk Managed Asset? **Out-of-Scope**

2) What type of asset is the MSP firewall (grey)? Would it be expected to perform the same security practices as the contractor firewall, or a smaller set? **SPA. The same, or higher security practices.**

3) What practices would be applicable to the MSP's Change Management database? Would it be an assessable asset? **The Change Management Database is an SPA. It would be assessable, but under an extremely limited set of practices (mostly CM.L2-3.4.5).**

4) What type of asset is the MSP's physical facility? **SPA**

5) Given the interconnections between networks, is it possible for the contractor to pass their CMMC Level 2 audit assuming that everything in-scope for assessment passes their assessable practices? If not, what reason would you give? **Yes**

Analysis

The different contractor can be Out-of-Scope because there are effective boundaries and separation between the networks. The different contractor cannot go directly from their network to the OSC due to

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

deny by default firewall rules. The limited inbound ports (log traffic and patch server check-ins) are controlled and not at high risk of causing compromise of the MSP. This design makes me queasy due to risk of lateral movement but as assessors we are looking for the minimum bar and the MSP firewall meets it.

The MSP firewall is a SPA because it is used to protect the OSC from the MSP network as well as from other client networks. The MSP firewall should be equivalently-or-better managed than the OSC firewall due to risk of sideways attack.

The Change Management database is in scope. The database (as well as back-end server security for the database) is a Security Protection Asset (SPA). The data contents would be reviewed as part of several individual Configuration Management (CM) practices. Access to the database would be reviewed primarily during CM.L2-3.4.5. Most assessors would not expect a Change Management Database to be identified in an asset inventory or network diagram by the OSC.

The MSP's Office and Datacenter could initially be considered Out-of-Scope because there is no chance that CUI would be stored, processed, or transmitted by it. But it also fits into the category of SPA because it physically protects the Log Server, Vulnerability Scanner, Change Management Database, etc. According to the recommended prioritization / decision flow for assets, the facility would be an SPA.

I really hate MSPs having always-on connection to multiple clients. Worms (the malware kind) strike fear into my heart. However, as assessors, we need to limit arbitrariness. The requirements that I'm concerned with in this situation are:

1) Ensure that assessment scope includes all systems that are not "Out-of-Scope".
2) AC.L1-3.1.20 Control/limit connections to external systems.
3) AC.L2-3.1.3 Control the flow of CUI.
4) SC.L1-3.13.1 Control organizational communications at external boundaries.
5) SC.L2-3.13.2 Architectural designs that promote effective information security.
6) SC.L2-3.13.6 Deny network communications traffic by default.

Regarding whether this client is even eligible for assessment due to the connected networks, use this rule of thumb: if scoping is performed accurately and you can't find a violation of a requirement, then the client does not fail. Because everything that is assessed passes the assessment, the client would be able to pass their assessment.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: The definition of SPA is different in CMMC than in NIST SP 800-171.

The 800-171 definition is "components of nonfederal systems that process, store, or transmit CUI, **or that provide security protection for such components.**" If we used CMMC scoping guide terms, this would be stated as *only including assets which directly affect the security of CUI Assets*.

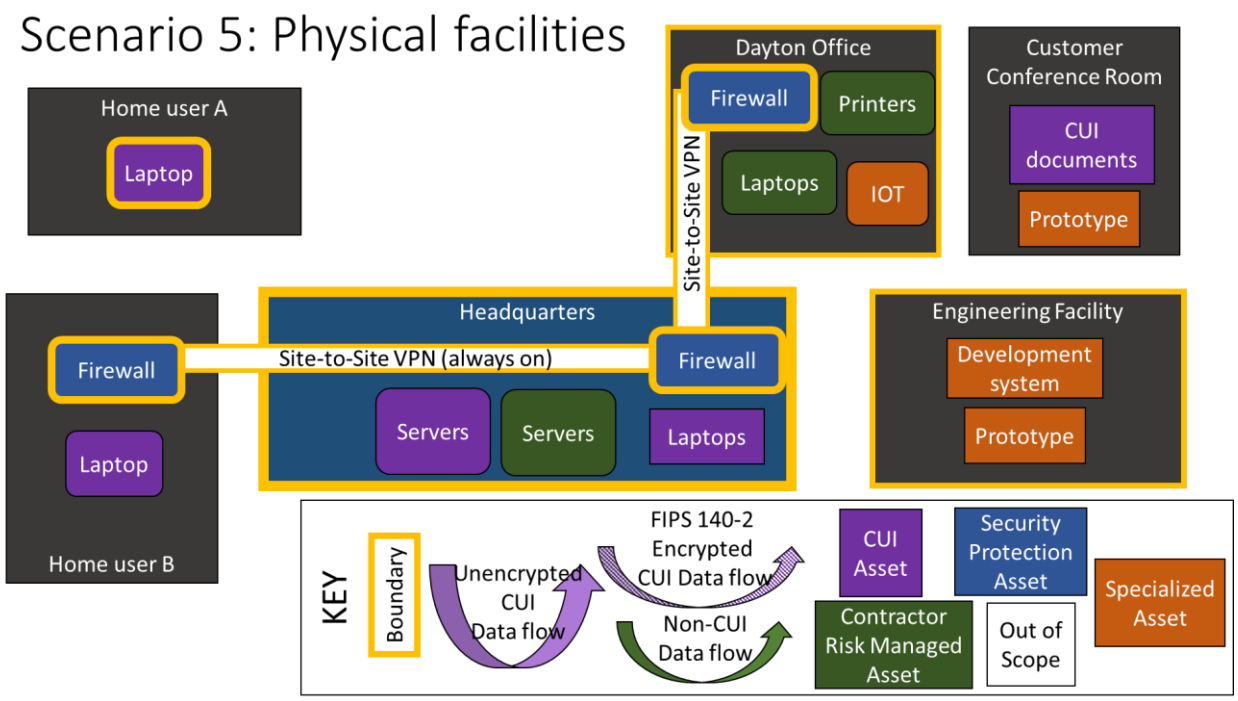
The CMMC definition is "Assets that provide security functions or capabilities to the contractor's **CMMC Assessment Scope**, irrespective of whether or not these assets process, store, or transmit CUI." The CMMC Scoping Guide indicates that the **CMMC Assessment Scope includes CUI Assets, SPA, CRMA, and Specialized Assets.**

The CMMC definition has hugely increased the number of components which are considered SPAs. As a result, we can have situations where SPAs perform security for other SPAs, creating a daisy chain effect reaching far beyond the contractor's information system. For example, your CUI asset could send logs to a SIEM that uses a different cloud antivirus which uses yet another SIEM, which uses yet another cloud antivirus. If SPAs of SPAs are not intended to be subject to inspection, this needs to be clarified before assessments start.

Even though the number of components considered SPAs has increased, it is unclear whether "applicable practices" has increased, or whether all SPAs are assessable. See sections **Thoughts on "Applicable practices"**, **Thoughts on "SPA Chaining"**, and **Thoughts on "Assessing SPAs for non-CUI Assets"** for additional discussion of this topic.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 5 – Physical Facilities



The Headquarters building hosts the datacenter as well as regular corporate staff. It has unencrypted CUI assets in it and the facility is considered a Security Protection Asset.

Sites connected with site-to-site VPN have the tunnel established 24x7. All ports and protocols are allowed freely for all sites that are connected to the VPN.

The Dayton office is connected to Headquarters using a site-to-site VPN which is always on. The Dayton office has no CUI assets within it, but the network provides unlimited connectivity to Headquarters.

The Engineering facility is completely disconnected. CUI is created there as part of development work. The Engineering facility has no "CUI Assets" within it, but it does have assets categorized as Specialized assets which contain CUI.

The Home user A just has a laptop. The OSC states that the laptop is fully secured and performs corporate-quality boundary functions for itself. The OSC says that the home network is Out-of-Scope due to their laptop security and requires the user to guard their laptop when it is unlocked.

The Home user B has a corporate-issued firewall which establishes a site-to-site VPN with Headquarters. Only the corporate laptop is connected to the downstream side of the firewall. The corporate-issued firewall is connected to the home network on the upstream side. A device plugged into the downstream side of the firewall has open communications to the corporate network.

The OSC gives quarterly demos to their customer at the Customer Conference Room. This is held inside the Customer facility and the OSC has no control over security there. CUI documents and prototypes are physically guarded by OSC staff the entire time they are in the conference room.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Questions

1) Would the Dayton office be considered an SPA, even though it has no "CUI assets"?

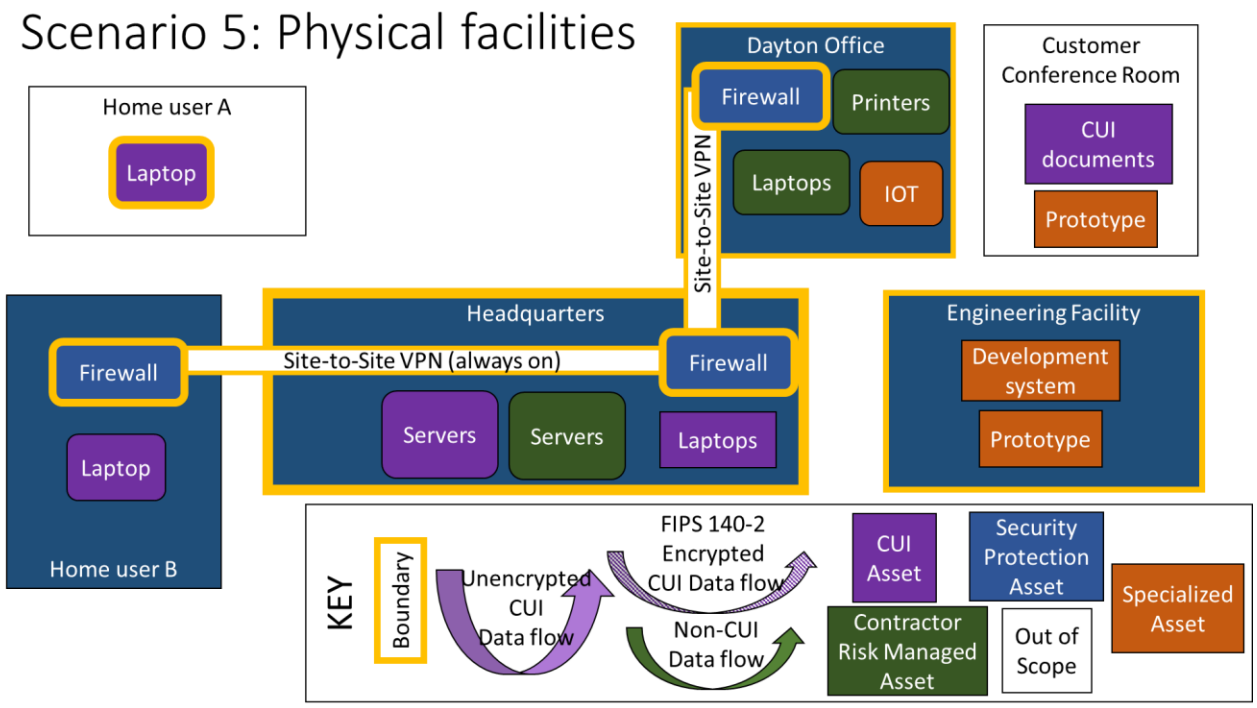
2) Would the Engineering Facility be considered an SPA, even though it has no "CUI assets"?

3) What type of asset is the Customer Conference Room?

4) Would the Home user A house be considered an SPA?

5) Would the Home user B house be considered an SPA?

Answer



1) Would the Dayton office be considered an SPA, even though it has no "CUI assets"? **Yes, because it provides security for SPA and CRMA.**

2) Would the Engineering Facility be considered an SPA, even though it has no "CUI assets"? **Yes, because it provides security for Specialized Assets.**

3) What type of asset is the Customer Conference Room? **Out-of-Scope**

4) Would the Home user A house be considered an SPA? **No – the home is not providing physical protection to the laptop. The laptop itself (Data-at-Rest encryption, passwords) and the user are providing the protection.**

5) Would the Home user B house be considered an SPA? **Yes, because the home is providing physical protection to the corporate firewall and network.**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Analysis

I went back and reviewed the definition for Security Protection Assets for this scenario because I had been treating SPAs as "components which provide security for CUI components" based on previous experience with National Institute of Science and Technology (NIST) Special Publication (SP) 800-171. This was not the right definition.

According to the scoping guide for CMMC Level 2, SPAs provide security for ANY in-scope assets.

"Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope…"

If you look at the summary table in the official Scoping Guide, it shows which assets are in the CMMC Assessment Scope: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, and Specialized Assets.

That is a BIG difference. That means that security assets for Contractor Risk Managed Assets are SPA. Security assets for Specialized Assets like Internet of Things (IOT) are SPA.

The Dayton facility should be considered an SPA because it provides security for any in-scope assets.

The Engineering facility should be considered an SPA because it provides security for any in-scope assets.

The Customer Conference Room would be considered Out-of-Scope because the OSC has no control over it and because the introduction of materials is very temporary. The OSC is properly performing alternative physical safeguards for the CUI documents and prototypes.

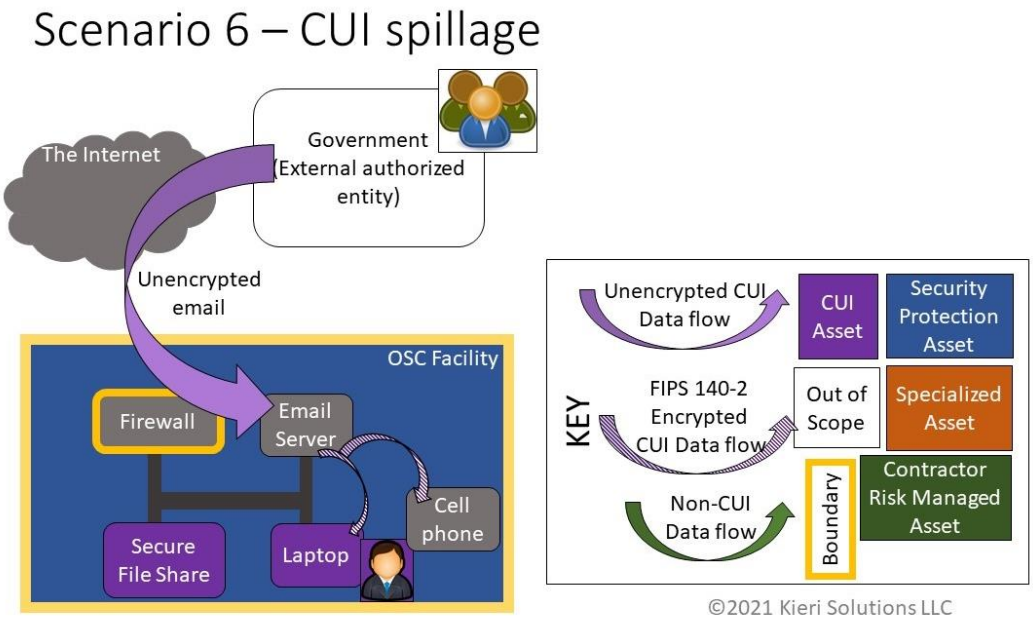
The Home user A house is Out-of-Scope because the laptop is secured logically to prevent access and tampering, even if a bad guy had physical access to it. The laptop is physically guarded by an authorized user while it is unlocked.

The Home user B house is a SPA because it provides security for the firewall, which allows unlimited access to the corporate network. A locked closet or cage could be used to protect the firewall so that a smaller space would require protecting. Logical security could be applied to the firewall (if capable) to prevent connection by unauthorized devices (Network Access Control and passwords). If local security was applied to the firewall to prevent access and tampering even if an attacker had physical access, then we could take Home user B's house Out-of-Scope.

At this point, you may be concerned because this scenario shows that many assets are considered SPAs, which are subject to inspection according to the scoping guidance from the DoD. This is indeed concerning, because if each of these SPAs is assessed, it will greatly increase the cost of assessment compared to the previous standard for NIST SP 800-171 assessments. The topic is discussed in more depth at the end of this document (see **Thoughts on "Applicable practices"**, **Thoughts on "SPA Chaining"**, and **Thoughts on "Assessing SPAs for non-CUI Assets").**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 6 – CUI Spillage



While interviewing the OSC for scoping, they mention that their customer at the US Government regularly sends CUI files to them via unencrypted email.

The CUI files are properly marked.

Because the user's cell phone is connected to email, the cell phone also receives a copy of the CUI files due to automatic synchronization. The cell phone has no special security enabled.

When CUI is received in this way, the OSC sends a polite email to the sender asking them to use the Secure File Share instead. The OSC saves the content of the email to their laptop and deletes the email message. Neither the email server nor the cellphone are sanitized according to NIST SP 800-88 each time this occurs. The OSC states this is because they would be extremely impacted due to regular poor practices by the customer.

The OSC would like the email server and the cell phone to be a Contractor Risk Managed Asset because they do not allow CUI on these assets by policy, and because they take action to delete the CUI when it comes in.

Questions

1) If unencrypted CUI emails are sent through the Internet, does that put the Internet in scope for the OSC?

2) If the Internet is in scope for the OSC (for any reason, not just this scenario), would you cancel the assessment before it starts? What justification would you use?

3) What type of asset is the OSC's email server?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

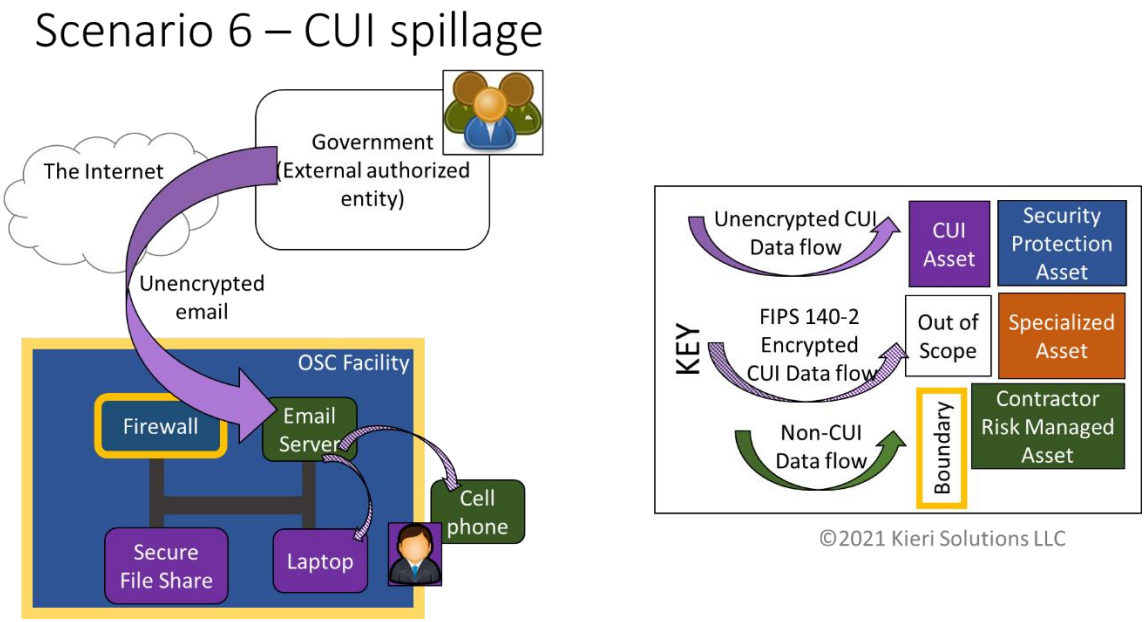
4) What type of asset is the OSC's firewall?

5) What type of asset is the OSC's cell phone?

6) As an assessor, do you feel it is required to perform a NIST 800-88 sanitization for CUI assets in order to move them from CUI Asset to CRMA or Out-of-Scope category?

7) Can you recommend a technical or administrative solution at the OSC that might help?

Answer



1) If unencrypted CUI emails are sent through the Internet, does that put the Internet in scope for the OSC? **No. The OSC did not choose to put CUI into the Internet and has no responsibility for the Internet.**

2) If the Internet is in scope for the OSC (for any reason, not just this scenario), would you cancel the assessment before it starts? What justification would you use? **Yes. Inability to assess practices against the Internet.**

3) What type of asset is the OSC's email server? **CRMA**

4) What type of asset is the OSC's firewall? **SPA**

5) What type of asset is the OSC's cell phone? **CRMA**

6) As an assessor, do you feel it is required to perform a NIST 800-88 sanitization for CUI Assets in order to move them from CUI Asset to CRMA or Out-of-Scope category? **Yes, in general (for CUI Assets). However, a spillage does not turn a CRMA or Out-of-Scope asset into a CUI Asset against the OSC's will. The OSC needs to take reasonable steps to remove the CUI data from these systems as part of**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

incident response. These steps should include reviewing guidance (some links below) on unauthorized disclosure, and possibly contacting federal authorities to report the incident and ask how to respond.

7) Can you recommend a technical or administrative solution at the OSC that might help? **Technical: Email filtering at the server could be used to reject any emails which contain CUI labels or specific categories of attachments. Administrative: The OSC could reply to the sender asking if they "meant to send CUI using an insecure method". This will normally result in the sender reviewing and decontrolling the document.**

Analysis

I have not been able to find a specific requirement for sanitization of equipment as a result of unauthorized CUI disclosure. The guidance lets the organization determine their own procedures for response. Best practice is to treat each CUI spillage as a cybersecurity incident, get an IT person involved to make sure it is deleted, and determine if the spillage is a reportable incident. If spillages are a re-occurring problem, I would personally also design security so that likely spillage objects (like the cell phone) are secured as much as possible.

So does the unencrypted email put the Internet, Firewall, email server, and cell phone into the "CUI Asset" category? I would say "barely no", because 1) the OSC is trying to keep the CUI out of them, 2) the OSC is controlling their own users to prevent CUI spillage from internal, 3) the OSC is communicating with the Government to try to fix the problem, and 4) the OSC is responding to delete the CUI off these systems. These assets would instead be CRMA assets (except for the Internet, which is completely out of the control of the OSC, and the Firewall which is still a SPA).

In regard to whether those assets are CUI Assets, to change my "barely no" to a "absolutely not", I'd want the OSC to forcefully tell the customer that they need to stop sending unencrypted CUI and escalate as needed. I'd also want the OSC to put technical measures into place, such as automatic rejection of emails that have CUI text strings or very large file sizes.

A friendly reminder from the manufacturing community to potential assessors: This is a much more common scenario than one may think. It is a business decision to continue to work with contracting officers that neglect to use secure file share services, and manufacturers/OSCs are often at the mercy of decisions made at the government or higher-level contractor tier. What an OSC does to respond to that CUI spillage is key.

References on unauthorized disclosure:

ARNG guidance for SECDEF OPSEC reinforcement - Unauthorized Disclosure student guide.pdf

Controlled Unclassified Information. Unauthorized Disclosures: Prevention and Reporting. ISOO

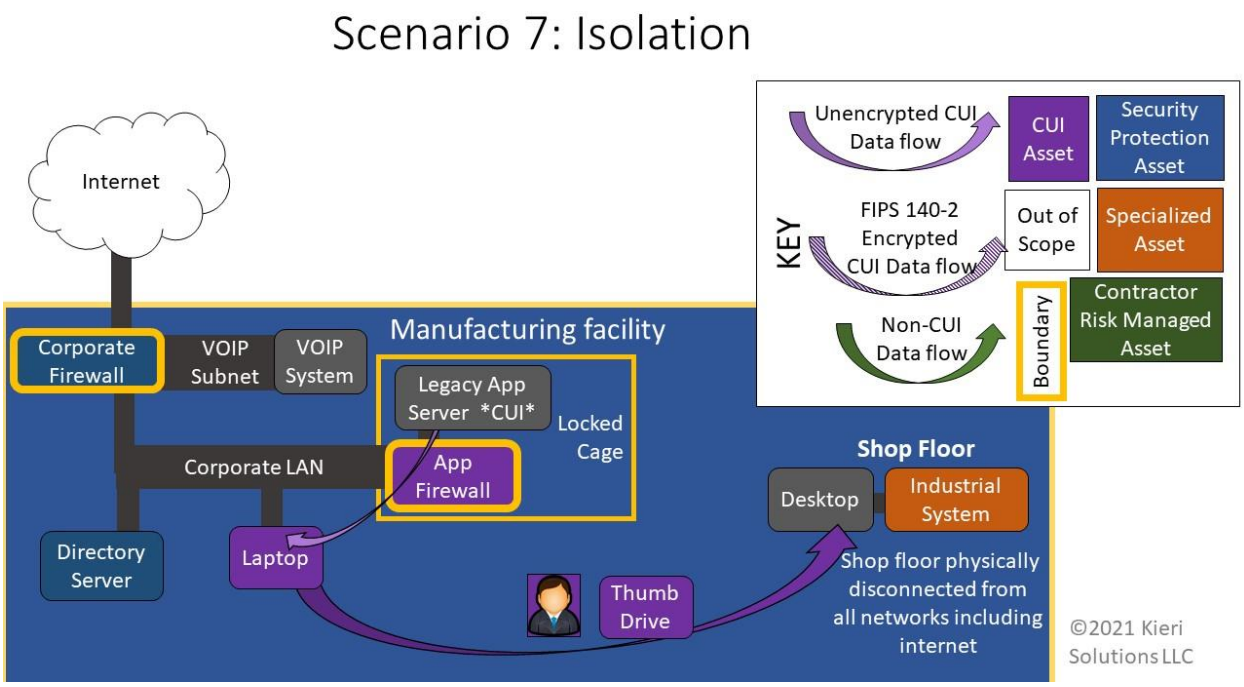
DoD Unauthorized Disclosure Desk Reference (DoD Insider Threat Management and Analysis Center)

32 CFR Sanctions for misuse of CUI

DoD Instruction 5200.48 Misuse or Unauthorized Disclosure of CUI

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 7 – Isolation



The OSC has decided to reduce risk by isolating their systems in various ways. Since they isolated the systems, can we skip assessing them?

The OSC has a simple Corporate LAN with a corporate firewall, directory server, and laptop.

The laptop is used to perform engineering which includes processing and storage of CUI diagrams and files. The laptop is a CUI asset.

The OSC has a Voice Over Internet Protocol (VOIP) system for phones which is isolated from the corporate LAN using a separate subnet. Logical isolation is effective - the firewall denies all traffic between the VOIP subnet and the Corporate LAN.

The OSC has a Legacy App Server which contains CUI. It runs on an old version of Linux and cannot be secured to meet CMMC standards. For example, the Legacy App Server has no password. The OSC has isolated it logically behind a separate firewall which only allows traffic to/from the laptop on port 1521. The OSC states that there are no known attack vectors across port 1521 and they can't restrict access more without stopping work. In addition, the OSC has put the Legacy App Server and the associated firewall inside a locked cage to prevent physical access.

The OSC has a disconnected shop floor network with a desktop (Windows 10) and a Specialized Asset (Operational Technology). They sneaker-net data between the laptop to the desktop using a thumb drive. All media protection controls are performed. The data is transmitted from the Windows 10 desktop to the Specialized Asset using electronic communications.

Questions

1) The OSC would like to categorize the VOIP system as Out-of-Scope. Do you agree?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

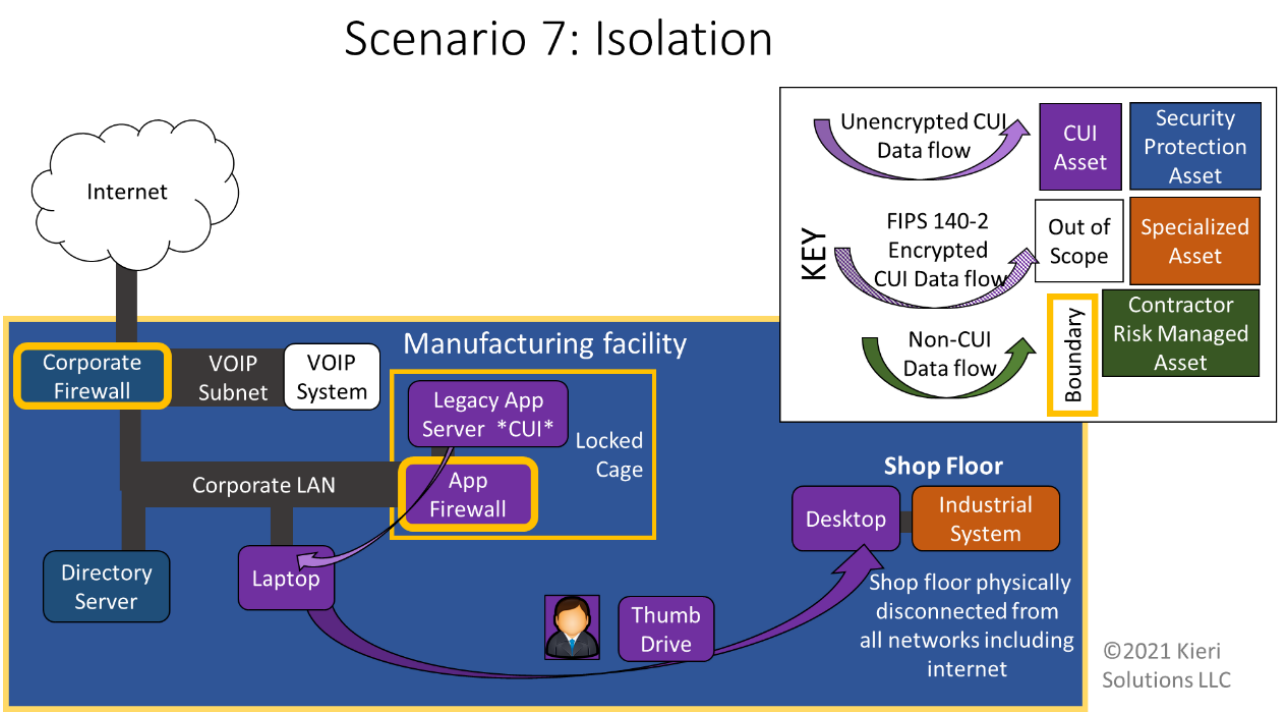
2) The OSC would like to categorize the Legacy App Server as Out-of-Scope. Do you agree?

3) The OSC would like to categorize the Shop Floor Desktop as Out-of-Scope. Do you agree?

4) If the Legacy App Server or the Shop Floor Desktop is categorized as a CUI Asset, would you review all controls against it? Would you review most controls? Would you review just a few controls? If just a few controls, which ones?

5) Would isolating the Legacy App Server and the Shop Floor in this way be considered an Alternative Implementation? As an assessor, can you accept this as stated by the OSC, or is there additional criteria to review?

Answer



1) The OSC would like to categorize the VOIP system as Out-of-Scope. Do you agree? **Yes, it is effectively separated from the in-scope network.**

2) The OSC would like to categorize the Legacy App Server as Out-of-Scope. Do you agree? **No. It has CUI on it.**

3) The OSC would like to categorize the Shop Floor Desktop as Out-of-Scope. Do you agree? **No.**

4) If the Legacy App Server or the Shop Floor Desktop is categorized as a CUI Asset, would you review all controls against it? Would you review most controls? Would you review just a few controls? If just a few controls, which ones? **If they were categorized as CUI Assets, I would review all controls against them (which apply to servers and desktops).**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

5) Would isolating the Legacy App Server and the Shop Floor in this way be considered an Alternative Implementation? As an assessor, can you accept this as stated by the OSC, or is there additional criteria to review? **Isolation is a common Alternative Implementation choice for systems that cannot be secured fully. Assessors need to verify that the OSC has gotten adjudication from DoD CIO or their prime contractor which confirms that the isolation is an acceptable alternative implementation for a set of specific practices.**

Analysis

The App Firewall is a CUI Asset because of the unencrypted CUI transiting through it. It performs security protection which limits the exposure of the Legacy App Server, but according to our recommended decision flow in **Scenario 1 – Remote Systems**, the CUI Asset category takes priority over the SPA category when the asset is a connected system and contains CUI.

Phone systems which could be used to discuss CUI verbally are only in-scope for CMMC if the system is physically or logically connected to your in-scope assets. For example, if your employees discussed CUI on their cell phones, the cell phone carrier would not be part of a CMMC assessment. Since the VOIP system is logically isolated using the firewall, it would generally not be in scope. Reference A104 in the Defense Federal Acquisition Regulation Supplement (DFARS) Cyber Frequently Asked Questions (FAQs).

As described in the scenario, while it is a little unclear, it sounds like the Shop Floor Desktop is not part of the OT system and does not fit the categories of Specialized Asset. Physically isolating the shop floor network is an excellent risk reduction measure but does not affect the asset category of any device. Physical isolation is an "alternative security measure" which could be established in lieu of other practices, but this would be determined on a per-practice level and may require permission from an authority.

The Legacy App Server as described does not easily fit into any of the categories of Specialized Asset. Since it does not, and since it has CUI on it, then it would be considered a CUI Asset. It is possible that the Legacy App Server could fit into one of the Specialized Asset categories (such as Restricted Information System) if it is critical for performance of the contract. If that was explained by the OSC to the satisfaction of the assessor, the Legacy App Server would change to a Specialized Asset.

Isolating the Legacy App Server behind a strict firewall and locked cage are excellent risk reduction measures and are probably the best thing the OSC can do to protect it when it does not have a password. However, if it is categorized as a CUI Asset, it is still expected to meet all applicable security practices. If these security practices cannot be performed, the assessor will need proof that the logical or physical isolation was accepted as an "alternative security measure".

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: Alternative, but equally effective, security measures.

Many contractors will use logical or physical isolation as an "alternative, but equally effective security measure" to reduce risk from assets that cannot meet some CMMC practices.

According to DFARS 252.204-7012(b)(2)(ii)(B) "The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

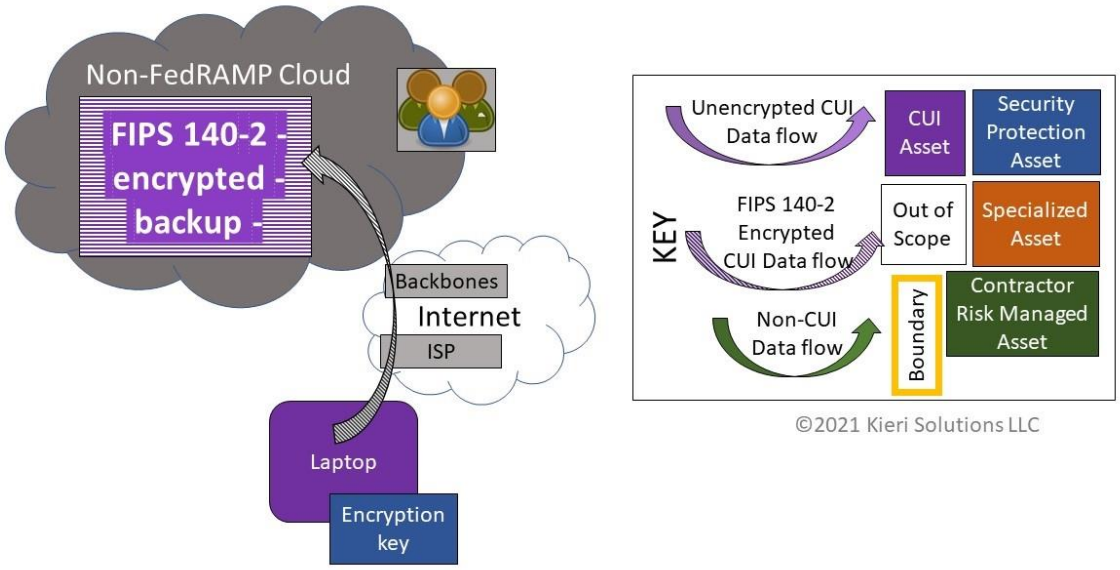
This means that **an assessor will expect to see an "adjudication by an authorized representative of the DoD CIO"** if the OSC wants to skip certain practices based on performing physical isolation of a network or system. This normally takes the form of an email from DoD CIO that approves a proposed solution.

There are circumstances where additional permission is not required. Reference A65 in the DFARS Cyber FAQs.

Subcontractors (non-primes) are expected to notify their prime contractor as part of contractual flow-down. Reference A69 in the DFARS Cyber FAQs.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 8 – Is FIPS enough?



The contractor's laptop is a CUI asset and is secured and managed to CMMC Level 2.

The contractor creates backups of their CUI files using their laptop. The backup is saved to the laptop as a large digital file.

This backup is encrypted with a FIPS 140-2 validated module while still on the laptop. The cryptographic key used to encrypt/decrypt is stored on the laptop.

Once the backup file is encrypted, it is transferred to a non-FedRAMP cloud provider for long-term storage. The transmission protocol between the laptop and the cloud cannot be proven to use FIPS 140-2 validated cryptography.

Questions

1) What type of asset is the cloud provider?

2) What type of asset is the Internet Service Provider which transmits encrypted CUI?

3) What type of asset are the Internet backbones which transmit encrypted CUI?

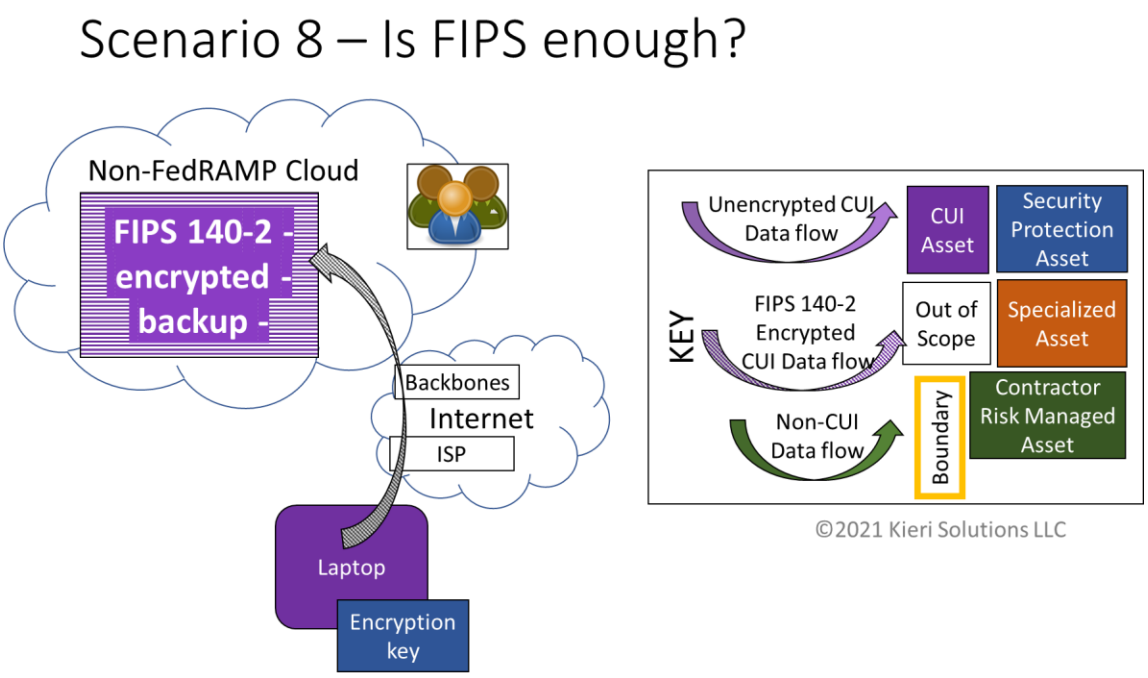
4) What type of asset are the cloud provider's support staff?

5) Is the data movement between the laptop and cloud considered to be "protected in transit" by a FIPS 140-2 validated module?

6) Does the cloud provider need FedRAMP moderate or equivalent, per DFARS 252.204-7012?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Answer



1) What type of asset is the cloud provider? **Out-of-Scope**

2) What type of asset is the Internet Service Provider which transmits encrypted CUI? **Out-of-Scope**

3) What type of asset are the Internet backbones which transmit encrypted CUI? **Out-of-Scope**

4) What type of asset are the cloud provider's support staff? **Out-of-Scope**

5) Is the data movement between the laptop and cloud considered to be "protected in transit" by a FIPS 140-2 validated module? **Yes**

6) Does the cloud provider need FedRAMP moderate or equivalent, per DFARS 252.204-7012? **No**

Analysis

Because the CUI data is encrypted using a FIPS 140-2 validated module on the laptop and the laptop has the only copy of the decryption key, the resulting ciphertext (the encrypted version of the data) is no longer considered CUI when it is away from the laptop.

Regarding data movement and protecting data in-transit: There are many different levels that data can be protected in. It could be protected at the file level through symmetric encryption. It could be protected using an encrypted application protocol. It could be protected through a secure channel provided by an HTTPS session. Or it could be protected through a secure channel provided by VPN. Only one needs to be FIPS-validated to consider the data protected in-transit. Because the data was encrypted at the file level before transmission, it doesn't matter whether secure protocols are used to move it.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: Ciphertext is not CUI

Many cybersecurity professionals feel that if CUI is encrypted with a FIPS 140-2 validated module, AND the decryption key is protected, the resulting ciphertext no longer needs to be treated as CUI. Another way to state this: Assets which store, process, or transmit only FIPS 140-validated ciphertext and have no access to the decryption key cannot be CUI Assets.

The problem is that there are no known official government documents that say that ciphertext can be treated as though it is not CUI or classified data. However, there seem to be several sources of acknowledgement that using cryptography (specifically FIPS-validated cryptography) to protect CUI changes the rules.

Sources of implied guidance:

NIST SP 800-88 guidelines for sanitization of data say that encrypted drives can be released for reuse or disposal as long as there is no chance that the decryption key could be released. "[Cryptographic Erase] should only be *used as a sanitization method* when the organization has confidence that the encryption keys used to encrypt the Target Data have been appropriately protected."

CMMC practice SC.L2-3.13.11 states "Employ FIPS-validated cryptography when used to *protect the confidentiality* of CUI."

CMMC practice SC.L2-3.13.8 states "Implement cryptographic mechanisms to *prevent unauthorized disclosure* of CUI during transmission…"

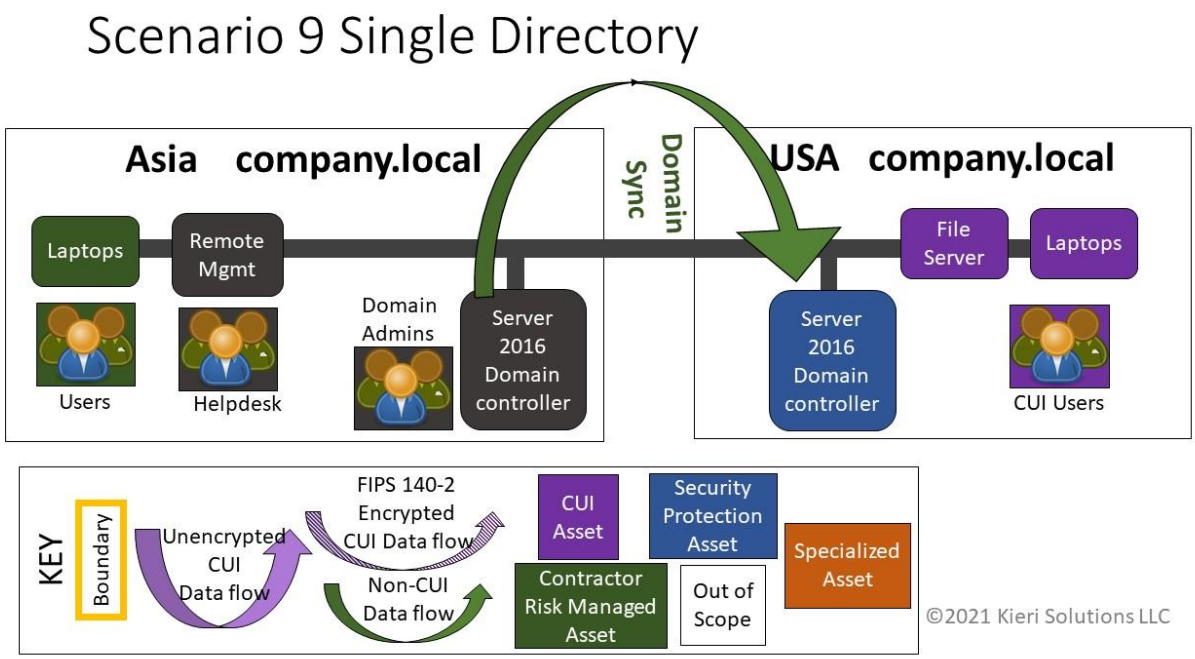
22 CFR Part 120 (ITAR regulation) "The ability to access technical data in encrypted form […] *does not constitute the release or export of such technical data*."

Nuclear Regulatory Commission Cryptographic Control Standard section 2.9.1 states "When clear text protocols […] are used for data transmission, the data traffic is "in clear text" and can be easily intercepted by someone using tools to access user emails, copy personal credentials, or copy sensitive files. Hence, to safeguard against unauthorized interception, data in transit is encrypted"

Because many cybersecurity practitioners consider encrypted CUI to still require protection and in-scope categorization like plaintext CUI, this is a topic that the DoD should clarify.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 9 – Single Directory



The defense contractor specializes in weapons systems and has offices in multiple countries because they sell their technology to multiple governments.

The defense contractor uses a flat network with a single Active Directory domain.

The type of CUI handled by the contractor is "Export Controlled", specifically International Traffic in Arms Regulations (ITAR) protected data. Because of ITAR regulations (weapons systems), their USA offices only employ or contract with U.S. Persons and their ITAR data is stored on a CUI File Server in the United States.

The United States users are in an Active Directory security group called USA_Only.

The CUI File Server is configured to only share files with accounts that are members of the USA_Only security group.

IT staff are primarily located in the Asia office and are not US Persons. The helpdesk performs helpdesk functions including remote management of all company laptops. The domain admins perform server administration, to include management of Active Directory using the Asia Domain Controller.

Questions

1) What type of asset is the Asia Domain Controller?

2) Is the USA_Only security group an effective boundary to keep CUI contained? If not, what could you change to make it an effective boundary?

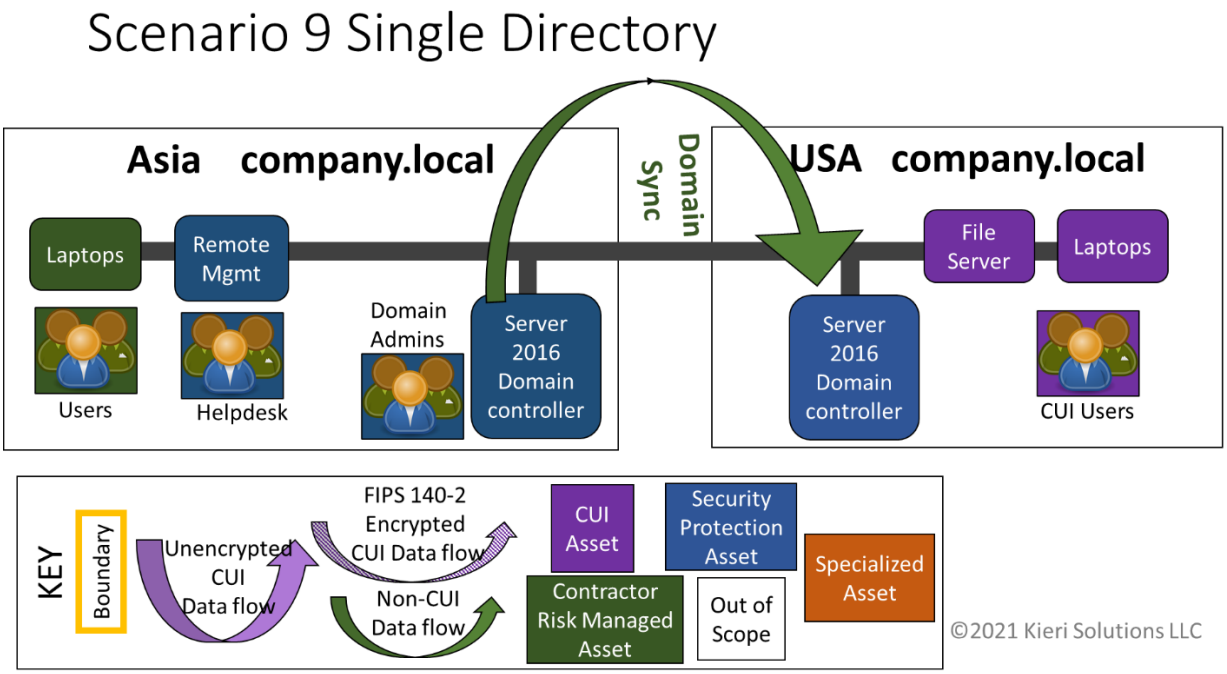
3) What type of asset is the Remote Mgmt server?

4) What type of asset is the Asia Helpdesk?

5) If an Asia Domain Admin performed audit log reviews to ensure that only US Persons accessed the CUI File Server, would that be an adequate boundary?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Answer



1) What type of asset is the Asia Domain Controller? **SPA**

2) Is the USA_Only security group an effective boundary to keep CUI contained? If not, what could you change to make it an effective boundary? **No. We need to ensure that only US Persons can manage access to CUI. This is best done by using a separate directory for the USA assets. It could also be done by removing all non-US persons from the domain admins group. Encrypting the data with a password only known to US persons could work but would need to be reviewed closely as a solution, since it is easy to leave unencrypted data on the endpoint when working with encrypted files.**

3) What type of asset is the Remote Mgmt server? **SPA**

4) What type of asset is the Asia Helpdesk? **SPA**

5) If an Asia Domain Admin performed audit log reviews to ensure that only US Persons accessed the CUI File Server, would that be an adequate boundary? **No. We need to ensure that only US Persons can manage access to CUI. This also includes monitoring functions (because we can't trust others to raise an incident if they see malicious activity).**

Analysis

This scenario is ugly. There is a very high likelihood that the contractor will fail their assessment (and possibly get reported for International Traffic at Arms Regulation (ITAR) violations. But enforcement of CUI//SP-EXPT is beyond the scope of this article…

The answers assume that non-US Persons (people who live in Asia) would not pass CMMC's personnel screening requirements because of the Export Controlled CUI. This could be argued, however. CMMC allows the contractor to define their own personnel screening. I don't know what I would do if a

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

contractor handling ITAR data had internal policies saying that there is no nationality restriction. *To my knowledge, CMMC assessors are not expected to enforce federal law against their clients.* This is a topic that needs clarification from the DoD.

Luckily for us, the contractor in this example acknowledges that the data should be export controlled and limits access to just US Persons and US locations. Because of this, we can assume that the contractor has internally defined their personnel screening to be US Persons only.

A feature of Active Directory (used by the Server 2016 Domain Controllers) is that the entire directory is synchronized between all domain controllers. This means that if the Domain Controller in Asia is maliciously modified to add a non-US person to the USA_Only group, that change will be replicated to the USA Domain Controller. Anything which stops that automatic synchronization would also break the directory functionality.

Key concept: Access control must be managed by trusted systems

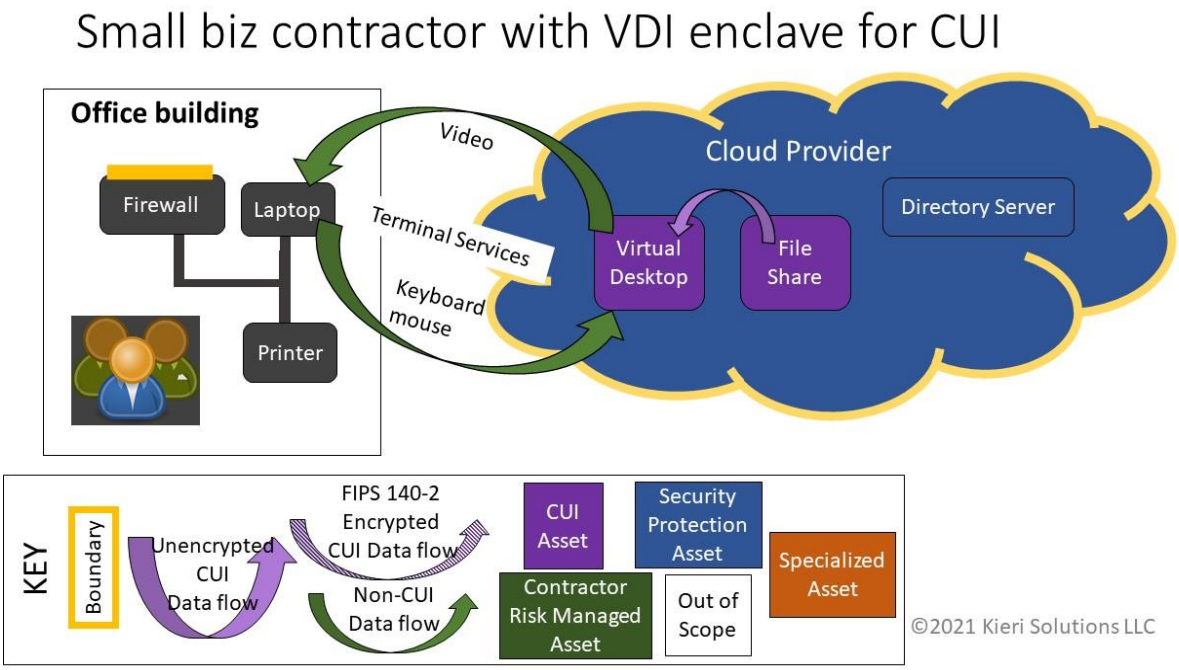
There are legitimate network designs where a single directory can be used for both trusted and untrusted environments. But the rule is that the directory needs to live in the trusted environment and be managed only by trusted people, or else you cannot expect the directory to limit access coming from untrusted people/systems.

For companies that are intent on a single directory (because they want their users to have a single set of credentials), this means that their CMMC-compliant enclave would need to host the directory for their entire corporate network.

This concept extends to all systems that control access to both highly secure systems and to lower security systems at the same time.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 10 – Virtual Desktop Infrastructure Enclave



The contractor has moved all of their CUI into a cloud enclave. The cloud is FedRAMP authorized. Virtual Desktop Infrastructure (VDI) is configured in the cloud which provides virtual user workstation functionality to work with CUI.

Only the ports required for Virtual Desktop are open on the Cloud Provider's gateway. The gateway allows access from *any* device on the Internet, but correct credentials, including Multi-Factor Authentication, must be provided. The OSC says that they have trained their users to only access the Virtual Desktop using corporate laptops. Other required boundary practices (such as monitoring, controlling, and protecting communications) are performed by the Cloud Provider's gateway. The assessor is concerned that the gateway may allow connection by unauthorized devices.

The Virtual Desktop session (server-side) is configured to block all communication except for Video, Keyboard, and Mouse signals. No copy-paste, no download of files, no printing, no hard drive or USB connections allowed.

The contractor performs the majority of their work using a simple corporate LAN inside their office building. The corporate LAN devices (firewall, laptop, printer) are secure to CMMC Level 1 (basic hygiene). The contractor performs training and oversight of their staff which effectively prevents attempts to print or scan CUI through the printer.

Questions

1) Would you consider the Cloud gateway to be an effective boundary if it permits connection without authenticating the user's device?

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

2) What type of asset is the Corporate Laptop?

3) What type of asset is the Corporate Firewall?

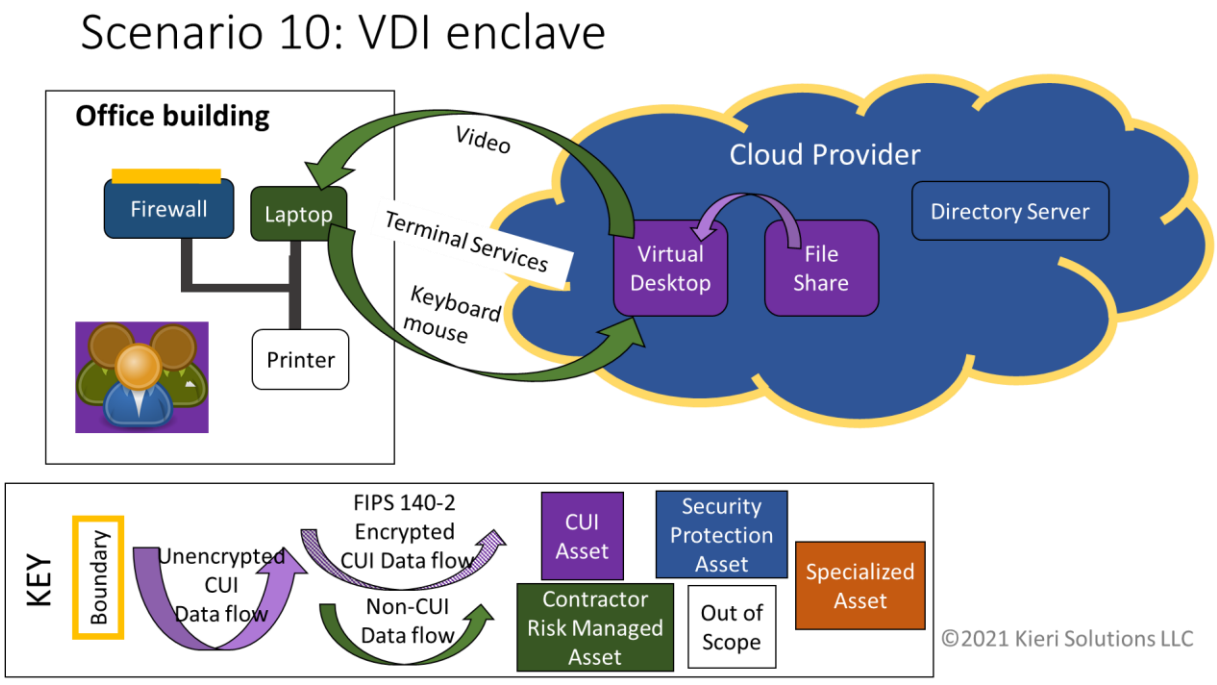
4) What type of asset is the Corporate Printer?

5) What type of asset is the Corporate User?

6) Is the assessor allowed to perform any tests against the Corporate Laptop to verify boundaries? Would the test be identified as a boundary test or a test against a specific practice?

7) If the VDI settings were configured client-side, would the asset types change?

Answer



1) Would you consider the Cloud gateway to be an effective boundary if it permits connection without authenticating the user's device? **Yes**

2) What type of asset is the Corporate Laptop? **CRMA is best answer. Out-of-Scope is arguable.**

3) What type of asset is the Corporate Firewall? **SPA**

4) What type of asset is the Corporate Printer? **Out-of-scope**

5) What type of asset is the Corporate User**? CUI Asset**

6) Is the assessor allowed to perform any tests against the Corporate Laptop to verify boundaries? Would the test be identified as a boundary test or a test against a specific practice? **If the asset is identified as CRMA, the assessor is allowed to perform a limited spot check in order to identify risks (such as ineffective boundaries). There is no defined practice or test category for these spot checks.**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Most likely, the spot checks would simply be identified as spot checks in an appendix of the test report.

7) If the VDI settings were configured client-side, would the asset types change? **Yes – the laptop would become an SPA, which is a higher priority than CRMA.**

Analysis

This paper is not attempting to consider CMMC Level 1 scope in any way. To the best of our knowledge, a CMMC assessment by a third party will never review Level 1 scope (focused on systems that handle Federal Contract Information). It is very likely that the corporate LAN would be included in a CMMC Level 1 scope, but this would only be self-assessed on behalf of the contractor.

The Cloud gateway is an appropriate boundary as long as there are effective controls to ensure that authorized users only access VDI with their corporate laptop. Because the OSC has trained their users to only access the VDI from corporate laptops, they can make a case that device control is performed at the user level. Assessors should trust the OSC but verify. There is a high risk that spot checks will discover a failure of this control if not technically locked down to IP range or registered devices.

The laptop could be either Out-of-Scope or CRMA. The laptop could potentially come into contact with CUI, but is prevented through technical measures, such as the configuration of the terminal services session. Normally technical measures preventing contact with CUI points us towards Out-of-Scope. However, many assessors will be concerned that malware or insider threat could record the screen because the asset is not fully separated from CUI. These threats should be risk managed. This is literally the definition and intent of CRMA.

When my company asked DoD Chief Information Officer (CIO) about Virtual Desktop as a solution, their response did not definitively say "Out-of-Scope". The response discussed a mixture of technical and administrative controls that would apply to the laptop. Based on this non-public feedback, it seems that CRMA will be the most acceptable category.

The firewall is an SPA, since it provides protection to a CRMA (the laptop). Since it is only discussed in the System Security Plan as relating to security for the CRMA laptop, it may not be assessable (because the CRMA is not assessable). See section **Thoughts on "Assessing SPAs for non-CUI Assets"**.

The printer's categorization is a little questionable. I am tending toward Out-of-Scope since there is no chance of CUI getting onto it if other controls are effective and it has no connection to in-scope systems.

Testing is allowed, but I'd go out of my way to relate each of them to a specific practice for the VDI, such as controlling connections to external systems.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: Is keyboard / mouse / video signal the same as CUI transfer?

Whenever we start talking about VDI, I always balance against this logic test: "If we are freaked out about a user possibly screenshotting their computer, why don't we confiscate the user's cell phone camera too?"

The user's likelihood to take pictures with their cell phone is assessable because the user is a CUI asset. That means we need to train the user, perform background screening, remove access quickly if there is a threat, PERFORM RISK ASSESSMENT, etc. So, we *are* treating that user as a risk. And if they thought the risk was high enough, the OSC *should* construct a system that prevents users from taking pictures. But it should be up to the OSC to determine that, as part of a good risk management process.

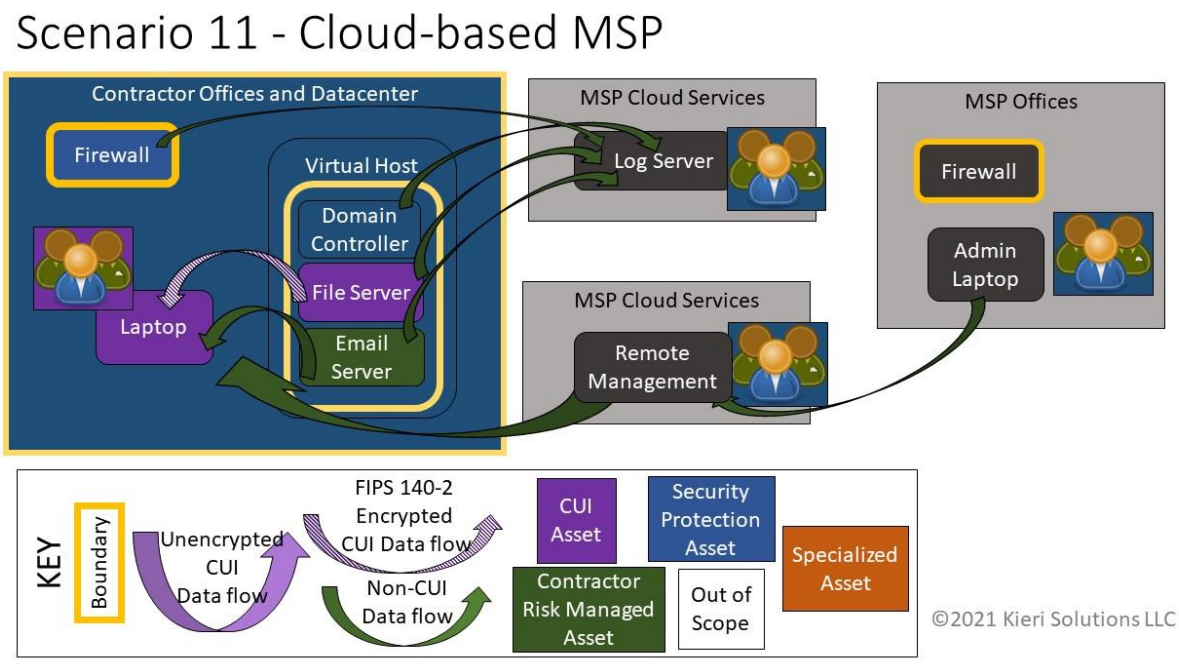
I keep thinking that the laptop fits perfectly into Contractor Risk Managed Asset because we literally are considering risks from the asset and are trying to prevent those risks from occurring. Precedent from previous assessments by the DoD is that they like to see the endpoint to be semi-managed based on risk. Antivirus, perhaps hard drive encryption, and preventing unauthorized access to the device.

Going back to the original question of whether a fleeting visual of CUI needs to be treated like CUI… most cybersecurity professionals say no if the viewer does not record it.

The concept of the properly configured VDI as a boundary is a critical technology for future CUI enclave enablement. DoD clarification of whether VDI is an acceptable boundary and expected risk management measures would be extremely beneficial to defense contractors.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 11 – Cloud based Managed Service Provider



The OSC is fairly typical. They have a virtual server on-premises which holds a Domain Controller, a File Server (which contains CUI), and an Email Server (no CUI). They have user laptops which process and store CUI. The OSC Firewall provides security protection for the network. The OSC has outsourced all IT functions to their MSP.

The MSP has licensed a suite of MSP-oriented tools which include agent-based remote management (pictured), logging (pictured), vulnerability scanner (not pictured), and antivirus server (not pictured).

The Remote Management cloud is accessed by the MSP administrator using web browser. Once authenticated, the administrator can connect to the desktop of any laptop or server with the agent installed and have video/keyboard/mouse access as though they are connected with Remote Desktop. Separate credentials have to be entered to unlock the operating system of the device.

The Log Server receives logs from each server and major network device. These logs do NOT contain CUI.

The MSP Firewall has no direct connection to the OSC's network.

The MSP Admin Laptop has no direct connection to the OSC's network. The Admin Laptop is used to access each MSP Cloud Service via web browser. The Admin Laptop does not directly connect to the OSC's network, but rather performs all management via cloud services.

The MSP has trained their admin staff to never view or move CUI using the MSP's systems. This appears effective – there is no sign that CUI has ever been, or will ever be, transmitted to the MSP's Office or Admin Laptop. The MSP has technically disabled all file transfer capabilities in the Remote Management cloud.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Questions

1) What type of asset is the MSP's Remote Management cloud?

2) What type of asset is the MSP's Log Server cloud?

3) Do the MSP clouds need FedRAMP moderate?

4) Should the MSP clouds be assessed to determine if Multi-Factor Authentication is enabled on MSP accounts?

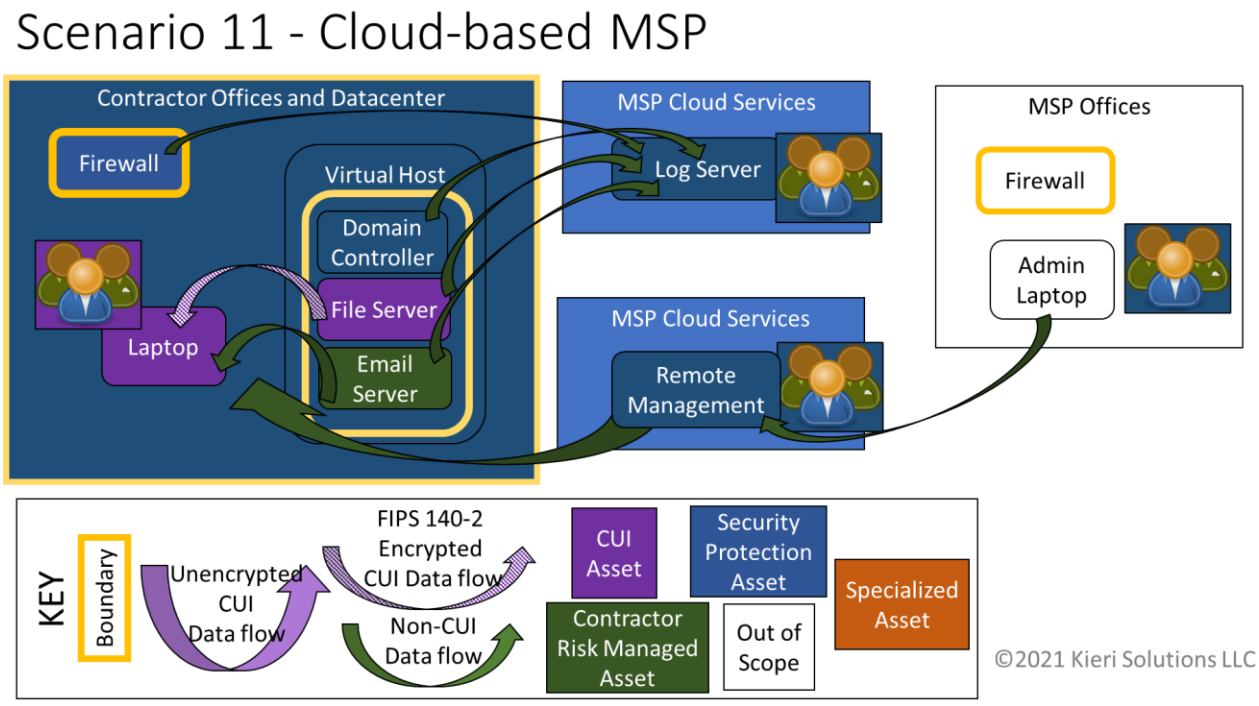
5) Should the MSP clouds be assessed to determine if "store and transmit only cryptographically-protected passwords" has been performed by the cloud provider?

6) What type of asset is the MSP's admin laptop?

7) What type of asset is the MSP's firewall?

8) What type of asset is the MSP's physical facility?

Answer



1) What type of asset is the MSP's Remote Management cloud? **SPA**

2) What type of asset is the MSP's Log Server cloud? **SPA**

3) Do the MSP clouds need FedRAMP moderate? **No, because they do not "Store, process, or transmit CUI"**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

4) Should the MSP clouds be assessed to determine if Multi-Factor Authentication is enabled on MSP accounts? **Yes, especially due to MA.L2-3.7.5**

5) Should the MSP clouds be assessed to determine if "store and transmit only cryptographically-protected passwords" has been performed by the cloud provider? **There is a strong split of opinion about this answer. Because they are SPAs, many assessors feel that this practice (and any other applicable practice) will be assessed based on their reading of the scoping guide. Historically, 800-171 and CMMC 1.0 assessments only reviewed that practice against CUI assets (not MSP clouds).**

6) What type of asset is the MSP's admin laptop? **Out-of-Scope**

7) What type of asset is the MSP's firewall? **Out-of-Scope**

8) What type of asset is the MSP's physical facility? **Out-of-Scope**

Analysis

Many people assume that all in-scope clouds are required to be FedRAMP equivalent – this is mostly incorrect. FedRAMP moderate (or verified equivalency) is only required by DFARS 252.204-7012 when a contractor "*intends to use an external cloud service provider to store, process, or transmit any covered defense information…"* This means that FedRAMP is only **required** for clouds that are categorized as CUI Assets.

Unfortunately, if you need to prove that a SPA provided by a cloud vendor performs the full suite of CMMC security requirements, there is virtually no source of proof other than a FedRAMP audit report. So de-facto, you are at risk if your SPA clouds are not FedRAMP authorized. For more analysis of which practices are applicable, review the section **Thoughts on "Applicable practices"**.

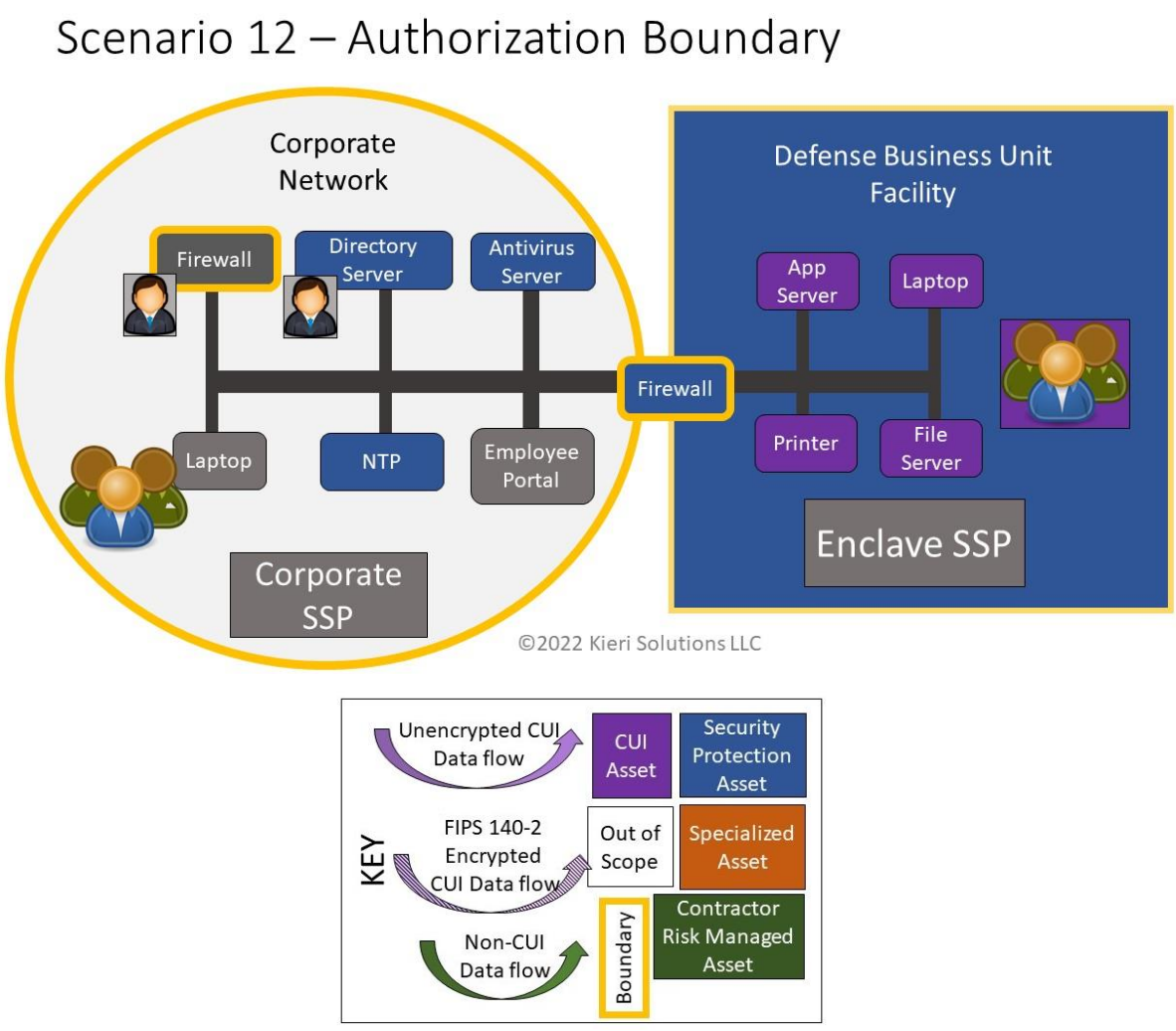
While the MSP's clouds do not require FedRAMP, they are subject to flow-down of paragraphs (c)-(g) in DFARS 252.204-7012 which requires incident reporting and cooperation with DoD forensic investigators.

The MSP's admin laptop, firewall, and physical facility are Out-of-Scope because they have no direct connection to CUI Assets (no way to access CUI) and because they aren't described in the System Security Plan as providing a required function for CMMC.

The MSP's Admin Laptop might be considered for CRMA because there is the possibility that CUI could be moved onto it through malicious action by the MSP staff. The reason it is not categorized as a CRMA is because there is effective separation and because the data flow controls are performed well before the admin laptop. The remote management software is technically restricted from moving data. The administrator staff are trained not to view CUI or transfer it. Unlike **Scenario 10 – Virtual Desktop Infrastructure Enclave**, the Admin Laptop should always be two steps away from CUI if the other controls are functioning properly. The administrative staff and the RMM are the SPAs that keep the Admin Laptop Out-of-Scope.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 12 – Authorization Boundary



The OSC is a large company with many business units that perform different types of US federal contracts.

The OSC has multiple System Security Plans (SSPs) in their environment. The OSC provides assessors with the SSP for the Defense Business Unit and the SSP for the Corporate network. The OSC states that other business units are described in other SSPs, which are not provided.

The OSC would like to do two assessments:

1) An assessment of their Defense Business Unit.

2) An assessment of the Corporate network, which only considers the in-scope assets that support the Defense Business Unit.

Corporate Network description:

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

The Corporate Network has no CUI in it and does not have any function which is designed to move CUI into it.

The Corporate Employee Portal website is used for timekeeping and training by all employees.

The Corporate Network Time Protocol (NTP) server, Antivirus Server, and Directory Server are used to provide security functionality for all the business units including the Defense Business Unit. The IT personnel that manage these servers are all screened, cleared, and authorized by Corporate in accordance with their CUI Protection Policy.

The Corporate Firewall is mentioned in the Corporate SSP as performing CMMC-required security functions for the Directory Server. However, it is not mentioned in the Enclave SSP as performing CMMC-required functions.

Defense Business Unit description:

The unit handles CUI and all assets should be considered CUI assets, except for the facility itself (SPA) and the firewall between the two networks (SPA). The firewall between the two networks denies traffic by default and restricts ports and protocols to the minimum for functionality.

Questions

1) During assessment of the Defense Business Unit, what type of asset is the Corporate Firewall (gray)?

2) During assessment of the Defense Business Unit, what type of asset is the Employee Portal (gray)?

3) During assessment of the Defense Business Unit, what type of asset is the admin for the Corporate Firewall?

4) During assessment of the Defense Business Unit, what type of asset is the admin for the Directory Server?

5) During assessment of the Defense Business Unit, what type of asset is the Corporate user laptop and users?

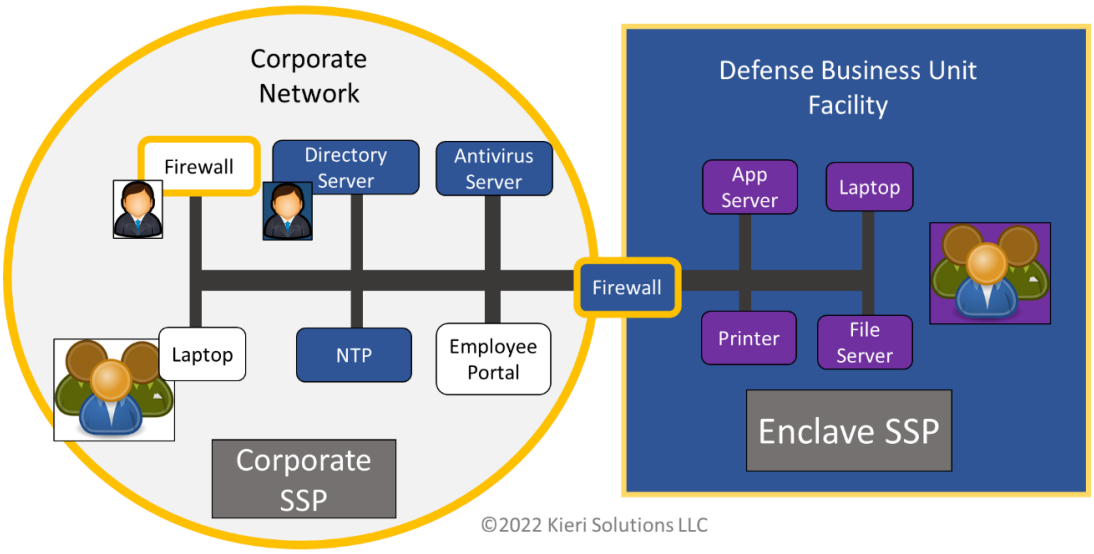
6) Which SSP should describe (and "own") the firewall between the networks?

7) As an assessor, would you be willing to do two assessments as requested? Does it matter which assessment goes first?

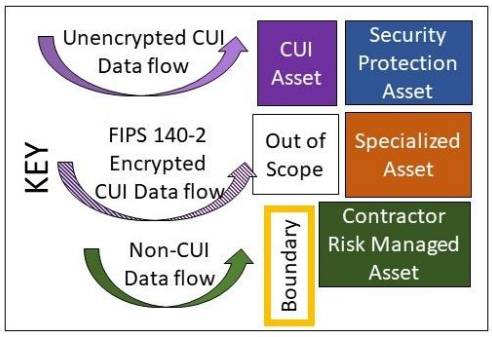
Answer

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Scenario 12 – Authorization Boundary



©2022 Kieri Solutions LLC



1) During assessment of the Defense Business Unit, what type of asset is the Corporate Firewall (gray)? **Out-of-Scope**

2) During assessment of the Defense Business Unit, what type of asset is the Employee Portal (gray)? **Out-of-Scope**

3) During assessment of the Defense Business Unit, what type of asset is the admin for the Corporate Firewall? **Out-of-Scope**

4) During assessment of the Defense Business Unit, what type of asset is the admin for the Directory Server? **SPA**

5) During assessment of the Defense Business Unit, what type of asset is the Corporate user laptop and users? **Out-of-Scope**

6) Which SSP should describe (and "own") the firewall between the networks? **The Enclave SSP makes more sense because the firewall is used as its gateway and primary logical boundary.**

7) As an assessor, would you be willing to do two assessments as requested? Does it matter which assessment goes first? **Yes. The Corporate network would need to go first (and pass their assessment) so that the Defense Business Unit can inherit security from Corporate.**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Analysis

Remember that an assessor does this work one small bite at a time. They will likely follow these steps:

1) Determine that it is logical to split the scope into two assessments with different boundaries.
2) Identify all in-scope assets related to CUI for the target contract. Also identify out-of-scope assets using the criteria "the asset cannot store, process, or transmit CUI."
3) Verify that all in-scope assets are in one of the two assessment scopes.
4) Perform the Corporate assessment (focusing on corporate).
5) Perform the Defense Business Unit assessment (inheriting protections from Corporate)

The regular users, user laptops, and Employee Portal in Corporate fit the definition of Out-of-Scope asset. With current separation and security controls, they cannot store, process, or transmit CUI. They also do not perform security functions for any in-scope asset. I believe it makes the most sense to review Out-of-Scope first and stop there if an asset meets the definition. This follows the recommended decision flow in **Scenario 1 – Remote Systems**.

From the perspective of the Defense Business Unit, the Corporate Firewall and the administrator of the Corporate Firewall are Out-of-Scope because they are part of a separate authorization boundary and because they directly perform no CMMC required security functions for the business unit.

From the perspective of the Corporate Network, the Corporate Firewall and the administrator of the Corporate Firewall are likely SPAs because they perform a required security function for the Directory Server (itself an SPA). An assessment of the Corporate Network would probably consider all SPAs for the "inheritable" systems to be in-scope, even though there is no CUI on the Corporate Network. It is not clear how to determine scope for CMMC assessments when there is no CUI within the assessment boundary. This may result in lack of consistency between CMMC assessors.

All administrators of the Directory Server are SPAs. They have a very important role in providing security for the Defense Business Unit.

The firewall between the two networks should ideally be described and "owned" by the Enclave SSP, since it provides security only for the Enclave. But it would be acceptable for Corporate to own that firewall too – it serves roughly the same role and risk as the Directory Server. In either case, the firewall between the two networks must be designed to protect the CUI Assets from the Corporate network.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Key concept: Authorization Boundary

Authorization boundaries are a concept used in the Risk Management Framework for government systems. Essentially, you can mark an information system "Out-of-Scope" if a different group is responsible for security, there is effective separation between your systems and the other system, the system supports a different mission or function, and you can trust that it meets compliance requirements. Reference NIST SP 800-37 r2, section 2.5 and Appendix G

Authorization Boundaries can be used to split assessments of information systems into different events, even within a single organization. An indication of this is when an organization manages multiple System Security Plans, with different groups responsible for different functions.

Splitting assessments into multiple Authorization Boundaries will be used in situations where an organization provides central security services for multiple clients. The central organization could be a Managed Service Provider, a Managed Security Service Provider, or it could simply be a corporate network servicing with multiple secure enclaves (this example). By assessing the central security services separately, each client can inherit protections from it.

Currently, there is no process for performing CMMC assessment of vendor networks (networks with no CUI). *Scoping is difficult because the logic for Out-of-Scope: "Cannot process, store, or transmit CUI" leads to the conclusion that the entire vendor network is Out-of-Scope unless a specific asset performs a required security function for the client, as we saw in this scenario.* Clarification and a standard process for performing "vendor assessments" is needed.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Thoughts on "Applicable practices"

As we worked through each scenario, it became more and more evident that we need to better understand what "applicable practices" means.

What is the historical precedent for applicable practices?

Based on word-of-mouth from assessed contractors, we have some historical precedent from DoD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). For NIST SP 800-171 and CMMC 1.0 assessments (pre scoping guide), only CUI Assets were assessed against every practice that could apply to them. Other systems were only subject to inspection if they provided a security function for CUI assets – and then they were only assessed to see if they were doing those identified security functions.

The precedent thus far has been that SPAs would be assessed only against practices that the System Security Plan says are performed by the SPAs. For a Security Information and Event Management (SIEM) server, this is normally only the following practices.

- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- Alert in the event of an audit logging process failure.
- Provide audit record reduction and report generation to support on-demand analysis and reporting.
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- Limit management of audit logging functionality to a subset of privileged users.

Historical precedent thus far would NOT assess the SIEM against other practices, even though other practices could be performed by that system type (or the back-end support team). The SIEM and related support team would not be assessed to see if they…

- Limit unsuccessful logon attempts.
- Terminate (automatically) a user session after a defined condition.
- Prohibit password reuse for a specified number of generations.
- Store and transmits only cryptographically-protected passwords.
- Remediate vulnerabilities in accordance with risk assessments.
- Employ architectural designs that promote effective information security.
- Assess security controls to determine if the controls are effective in their application.
- Perform AU practices relating to the SIEM's own logs

Cost of adding new practices to assessment

If *every* practice that can apply is assessed against Security Protection Assets, **the cost of compliance and assessment will skyrocket far beyond what we are seeing now.** I estimate this to be at least a 200-300% increase compared to current costs. In many cases, contractors will be forced to migrate their SPA functions internally because they will not be able to *prove* that outsourced SPAs perform the full suite of security practices compatible with that type of system.

If we choose an "in between path" by *selecting individual practices* that are applicable based on risk, then we create an issue with consistency. **The defense contractor is likely to select a different set of practices than the third-party assessor.** This would create a situation where the student prepared for test A but was given test B. This will cause a high degree of re-work, failed assessments, and bitterness among Organizations Seeking Certification.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Why are SPAs assessable when CRMA are not?

Why did the DoD decide that SPAs are assessed against CMMC practices while CRMAs and Specialized Assets are not? There are two possibilities that I see:

1. **Some** SPAs have privileged access to CUI assets and could cause a CUI compromise if misused, therefore **all** SPAs need to be fully assessed to ensure they are as secure as possible.
2. SPAs **need to be assessable** to verify they perform specific security controls that they contribute toward CMMC compliance.

If the DoD meant #1, wouldn't they have identified specific functions that are higher risk than others? Functions like the ability to change configurations, access protected areas of the operating system, or move files to-and-from the device? Those functions seem like they would warrant additional security measures.

Instead, the DoD called out SIEMs as their example of an SPA, which are extremely unlikely to be a source of direct compromise but serve a key role in performing Audit practices for the information system.

The more I review, the more it appears that DoD meant #2. From the scoping guide section on SPAs: "*For example, an External Service Provider (ESP) that provides a security information and event management (SIEM) service may be separated logically and may process no CUI, but the SIEM does contribute to meeting the CMMC practice requirements.*" **This tells us what the DoD is concerned about – how the SPA is contributing to meeting the practice requirements**.

How do government networks handle applicable practices?

When we discuss this topic with Risk Management Framework (RMF) experts who manage security for government networks, they reply that the precedent for RMF is to assess every possible practice against SPAs. But they will also say that they assess every possible practice against CRMAs and Specialized Assets too.

Under RMF, the US Government is allowed to accept risk, so when assets cannot meet security requirements, the network can still be authorized**. For CMMC, there is no functional risk acceptance mechanism**. The DoD also made the blanket decision that **CRMA and Specialized Assets are not subject to inspection** for CMMC at this time.

These two differences show that **DoD's expectation for defense contractors is dramatically different** than for their own networks under RMF. Not because the DoD wants contractors to be less secure, but because the danger of disrupting the Defense Industrial base is extreme if cybersecurity requirements are too strict. We cannot use RMF as our guide for what practices are assessable for SPAs.

Interpretation

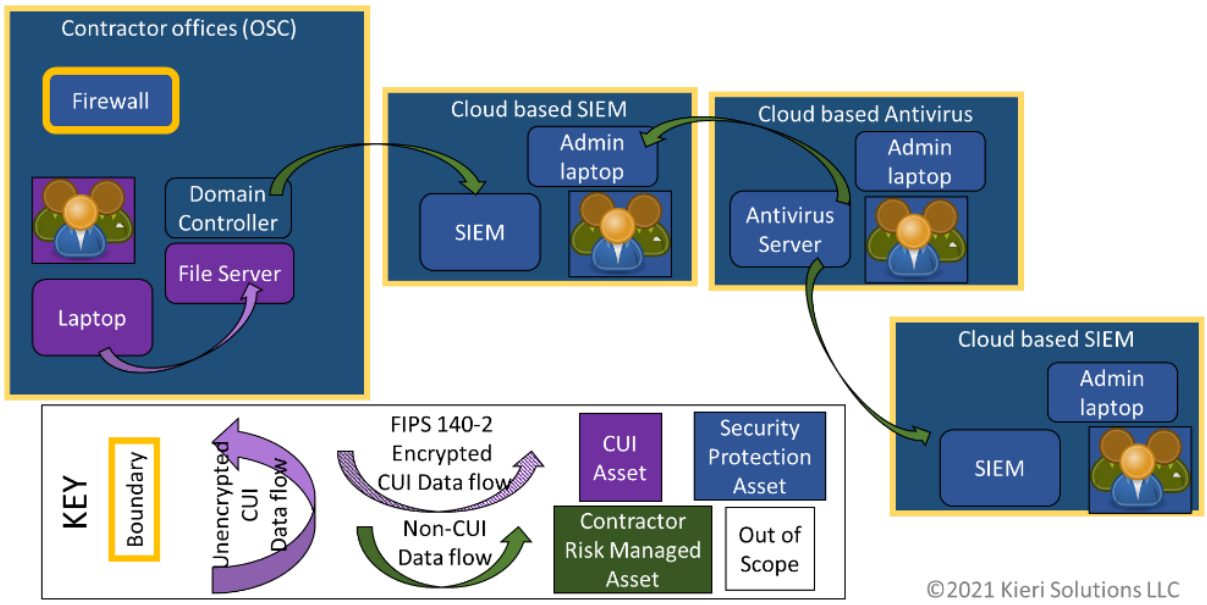
SPAs are assessable to validate their *contributions to meeting required CMMC practices* only.

This interpretation is highly controversial (though cybersecurity professionals agree on historical precedent as well as the cost of the alternative) because the Scoping Guide appears to treat CUI Assets and SPAs the same regarding "applicable practices". **This is the #1 topic that the DoD needs to clarify.**

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Thoughts on "SPA Chaining"

According to the scoping guide, assets that provide security for any other in-scope asset are also considered Security Protection Assets. Because of the way it is stated, an assessment scope could be interpreted as including multiple tiers of Security Protection Assets as shown in the diagram below.



In this diagram, the contractor states in their System Security Plan that they use a cloud-based SIEM to capture logs from their environment. That SIEM performs security and is in-scope as an SPA. But then the cloud vendor uses a Privileged Admin Workstation to manage their SIEM, which could also be identified as an SPA. And the antivirus on the Privileged Admin Workstation is managed by a cloud-based antivirus server, which could also be an SPA. And the cloud antivirus uses a second cloud-based SIEM for logging, which is also an SPA. And the second SIEM has its own Privileged Admin Workstation and privileged staff, which are also SPAs...

As this example hopefully makes clear, if SPA chaining is allowed to continue past the security function described in the System Security Plan, then we could have a never-ending line of SPAs to be assessed. Unfortunately, contractor supply chains are currently not mature enough to provide proof that these dependencies are compliant. If second and third tier SPAs are included in the assessment scope, it will be nearly impossible to pass an assessment due to lack of available evidence.

I doubt that the Department of Defense wanted this extreme interpretation (which allows infinite chaining) to be used. **More likely, the DoD expected that SPAs subject to inspection would be limited to the SPAs that were mentioned in the System Security Plan of the contractor.** These are the SPAs that **directly contribute to CMMC practice requirements** for CUI Assets or other first-tier Assets.

Interpretation

Past the first tier of SPAs, additional tiers of security assets would meet the definition of Out-of-Scope by having no access to CUI and by not contributing to meeting a practice requirement.

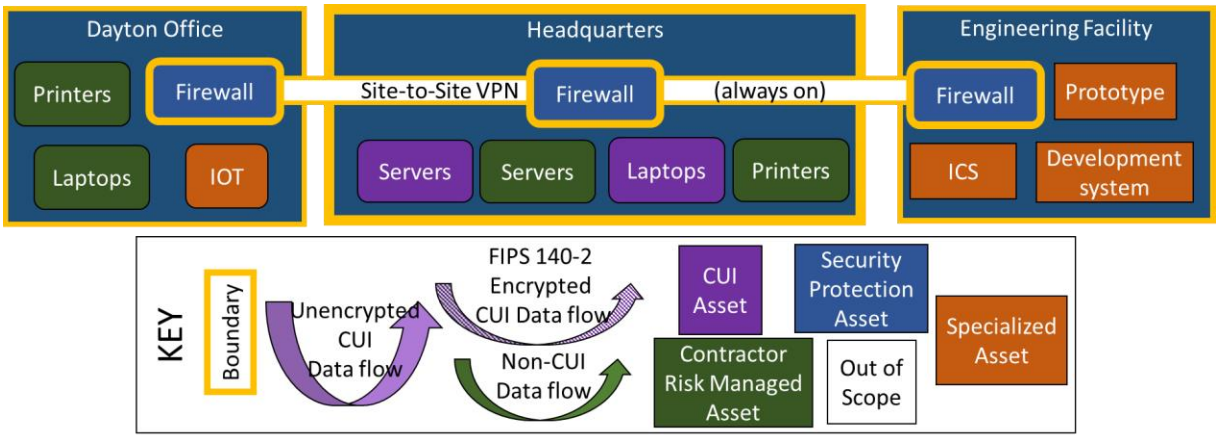
This topic needs clarification from the DoD.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Thoughts on "Assessing SPAs for non-CUI Assets"

According to the scoping guide, assets that provide security for any other in-scope asset are also considered Security Protection Assets. This could result in an interpretation where SPAs that only protect CRMA would be assessable while the CRMA they are protecting are not assessed.

An example of this would be a company that has physical facilities without CUI Assets, as shown in the diagram below. The Dayton Office and Engineering Facility do not directly protect CUI Assets.



For this example, let's assume that the corporate network is protected logically so that the network cannot be compromised through physical attack. But the non-CUI Assets (the printers, laptops, Internet of Things (IoT), and Specialized Assets) do need to be protected physically. The contractor's System Security Plan describes the Dayton Office and Engineering Facility's security to answer practice requirements for protecting these non-CUI Assets.

We could read the Scoping Guidance as requiring assessment of all SPAs even if they do nothing for CUI Assets. **But it doesn't make sense** – *why would we skip assessing security on a CRMA but then assess SPAs that only affect that CRMA?* I don't think this is what was intended by the Department of Defense.

Rather, it appears that the Department of Defense intended to limit **assessment** of SPAs to just those SPAs that perform **security requirements for CUI assets**. This interpretation is based on scoping guidance which says that **CRMA and Specialized Assets will not be assessed against CMMC practices** and identifying SPAs as assets that **contribute to meeting the CMMC practice requirements**."

How does this look during an assessment? The assessor would review the System Security Plan sections which address protection of CUI Assets. If the description for a CUI Asset says that an SPA is performing a required practice, then the assessor would review that SPA regarding that practice. But since the assessor is not assessing CRMAs or Specialized Assets, they would not consider the SPAs that are described only in the CRMA or Specialized Asset descriptions.

This interpretation is supported by historical assessments by the DoD for NIST SP 800-171 and CMMC v1.0. Historically, only SPAs that performed required security functions for CUI Assets were assessed.

Even if historical precedent is followed, this does not remove the CMMC 2.0 requirement to fully describe security for CRMA, Specialized Assets, and Security Protection Assets in the System Security Plan. It simply means that the contractor will not have their SPAs **assessed** unless the SPA protects CUI assets.

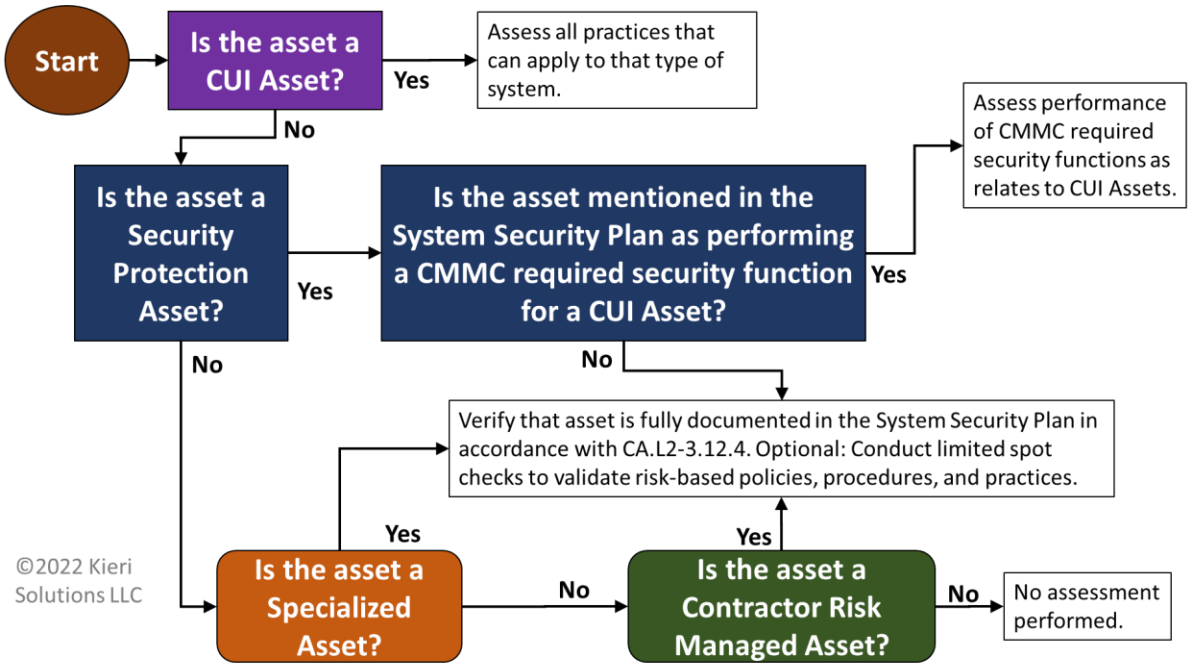
Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

It is worth mentioning that the scoping guidance provided by the DoD for CMMC Level 2 diverges significantly from the "adequate security" required in DFARS 252.204-7012 because scope is no longer directly related to CUI.

The example Engineering Facility highlights a scoping issue where Specialized Assets with CUI might not be assessed for physical protections. If we use the same rules for CRMA as we do for Specialized Assets, we will skip assessing security protections for Specialized Assets.

One possibility for resolving this gap is including information (e.g. CUI) as a type of asset. This aligns with existing asset classifications put forth by the Cybersecurity and Infrastructure Security Agency (CISA), NIST SP 800-160, Volume 2, Revision 1), and Carnegie Mellon's Software Engineering Institute (SEI)). At that point, we would consider the information to be a CUI Asset itself and facilities which protect CUI (such as the CUI inside Specialized Assets) would become SPAs. The definition of asset in the CMMC Assessment Guide for Level 2 leaves open the possibility of information being categorized as an asset (because it "has value to an organization") but does not list information as an example.

Below is a **suggested** high-level decision tree for practices that are subject to inspection if the interpretations of this paper are correct.



Interpretation

SPAs must be fully documented in the same way that CRMA and Specialized Assets are, but only SPAs which perform CMMC required security functions for CUI Assets are assessable against CMMC practices. This is a topic that the DoD needs to clarify.

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.

Conclusion

This analysis is a best attempt to understand the official guidance from the DoD and apply it to detailed scenarios and real-world situations while balancing it against historical precedent and assessment burden.

We hope that this analysis is useful to defense contractors and CMMC assessors from an educational standpoint. This is a work in progress which will change as clarification is provided by the Office of the DoD Chief Information Officer and as new CMMC assessments are conducted by the Defense Industrial Base Cybersecurity Assessment Center and CMMC Third Party Assessment Organizations.

We request that the DoD provide clarification if our analysis or interpretation veers from what was intended by the official scoping guide.

Thank you for your consideration.

Amira Armond

Credits

Primary author

Amira Armond, President of Kieri Solutions LLC. CMMC Provisional Instructor. CISA, CISSP.

Amira Armond is the Vice Chair of the C3PAO Stakeholder Forum, the president of Kieri Solutions LLC, and the chief editor for CMMCaudit.org. She is a CMMC Provisional Instructor and is an active speaker and blogger for cybersecurity and compliance. Amira Armond provides consulting and training on NIST SP 800-171, CMMC, and secure systems architecture to clients ranging from Fortune 50 companies to small defense contractors.

Contributors

Allison Giddens, President (Operations), Win-Tech, Inc.

Jeff Baldwin, CISSP-ISSAP-ISSEP, CCSP, CISM, CISA, PMP, AWS CSAA, CySA+, CMMC Provisional Instructor

Joy Beland, Edwards Performance Solutions. CISM, SSAP, CMMC-AB Provisional Assessor, Provisional Instructor

Vince Scott, CEO Defense Cybersecurity Group, Inc. CMMC Provisional Assessor, Provisional Instructor

Nathan Regola, Ph.D., President of Regola Cyber. Contributor only for scenarios, not opinion essays.

Brian Hubbard, Director of Commercial and Cybersecurity, Edwards Performance Solutions. CMMC Provisional Instructor, Provisional Assessor. CISM, PMP

Copyright ©2022 Kieri Solutions LLC. All Rights Reserved. All trademarks, service marks, and tradenames referenced in this material are the property of their respective owners. This document is for educational and informational purposes only. It is not intended to provide direction to contractors.