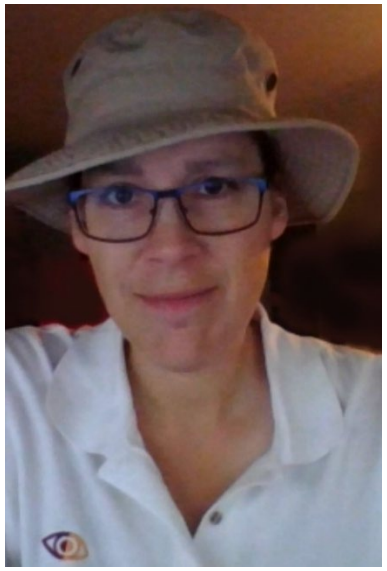
CMMC
What's In Scope for Assessment?

Current As Of: January 2023

Sponsored by:
COALFIRE FEDERAL

TODAY'S SPEAKERS



Amira Armond

President, Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO
Defense Cybersecurity Group
INFRAGARD National SME
Cyberwarfare

Stuart Itkin

Vice President CMMC & FEDRAMP Assurance, Coalfire

Sponsored by:
COALFIRE FEDERAL

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- NIST 800-171 Released Jun ‘15 / Updated Aug ‘16: 110 controls
  - Revision 3 draft planned for release in Spring of ’23
  - Expect 110 number to go up
- CMMC announced Jul ’19 to independently assess cyber implementation
  - CMMC 2.0 announced Nov ’21 / Interim rule expected ~~Mar~~ **summer** ‘23
  - 60 days after Interim Rule published, CMMC requirements could appear in DoD solicitations/contracts

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult
- "DoD may step up oversight and enforcement actions using its existing authorities. Delay in CMMC really is just a delay in mandatory assessments. The underlying contractual cyber requirements are binding now and will remain so."

Three Big Questions

- **What are we trying to protect? And why?**
  - We cannot protect information/data if we don't understand why something should be "Controlled"
  - We cannot protect CUI if it is not properly marked
- **From whom are we trying to protect it?**
  - Assume all US persons have access?
  - Is "Need to Know" a component of access?
  - What about friends, partners and Allies?
- **Can NDIA encourage the government to begin by:**
  - Focusing on most critical data/information
  - Providing some guidelines on releasability

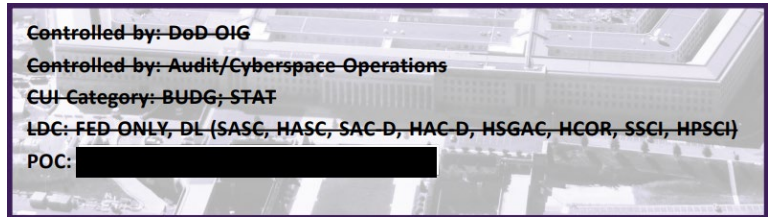
What needs to be secure?

Scope: It starts with business process

- **Business processes drive CUI "location"**
- **Technology enables business processes**
  - But technology may not always be the answer
- **In addition to IT, Assessment scope also includes:**
  - People
  - Facilities
  - 3rd Parties
  - Tooling / Capital Equipment / OT / IoT
- **Business and functional managers must understand and track business process support systems, applications, and services**

Follow the data

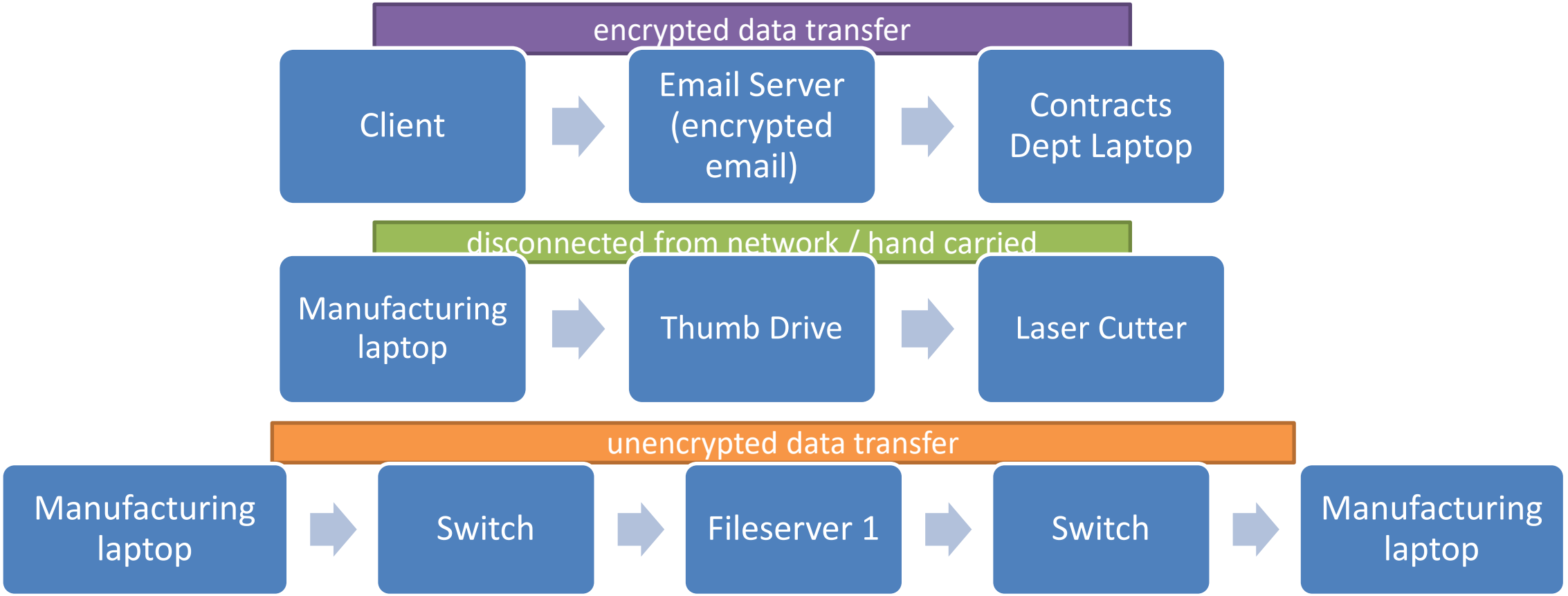
- **What is CUI in your environment?**
  - Properly labeled documents and digital files
  - Prototypes / manufacturing instructions
  - Incorrectly or not-labeled files, emails



CUI Location	CUI Type	Purpose	Data Owner / POC
Fileserver1	CTI	Project files for F-18 and HMMV	Greg Anderson
Laser Cutter	CTI	CAD files that give exact specifications to build F-18 parts	Greg Anderson
Engineer laptops	CTI	Project files for F-18 and HMMV that are in-use by the engineer	Individual laptop owners

Follow the data

- What does CUI move through?



CUI Assets

- **CUI Assets**: buildings, computers, network devices, information systems, clouds, people) that “Store, Process, or Transmit” CUI
- **All requirements apply at an overall level or at a granular level to protect the CUI:**
  - Must perform screening for people who work with CUI
  - Must have strong firewalls for networks with CUI
  - Must have secure buildings for facilities with CUI
  - Must be doing FedRAMP security for clouds with CUI
  - Must restrict software installation rights for laptops with CUI
  - Must strictly control permissions for networks with CUI

… when each requirement is implemented, CUI in digital or physical form is protected in a holistic manner

Risk-Managed Assets

- **Risk-Managed Assets**: buildings, computers, network devices, information systems, clouds that do not “Store, Process or Transmit” CUI but DO impact the security of CUI OR they “Store, Process or Transmit” CUI but are given an exception as “specialized assets”
- **Secure as much as possible, but allowed to skip some requirements (if you can justify it to the assessor)**
  - Operational Technology (manufacturing equipment)
  - Restricted Information System (configured a certain way because of contract requirements)
  - Computers and servers on the same network as CUI assets
  - People who work near, but not with, CUI

Commercial off the Shelf (COTS) Vendors

48 CFR § 4.1903 - Contract clause (applicable to small businesses, but not COTS items):

The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system..

Defense Acquisition Regulations System, DoD 252.204–7012 (applicable to small businesses, but not COTS subcontracts):

(g) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

- **COTS vendors, COTS items and COTS subcontracts are different**
- **Sales engineering, Service, and Support may create CUI**
- **Modifications to COTS items may be CUI:**
  - Superficial changes
  - Additions to a COTS product on behalf of or for the DoD
  - Engineering changes to a COTS product on behalf of or for the DoD

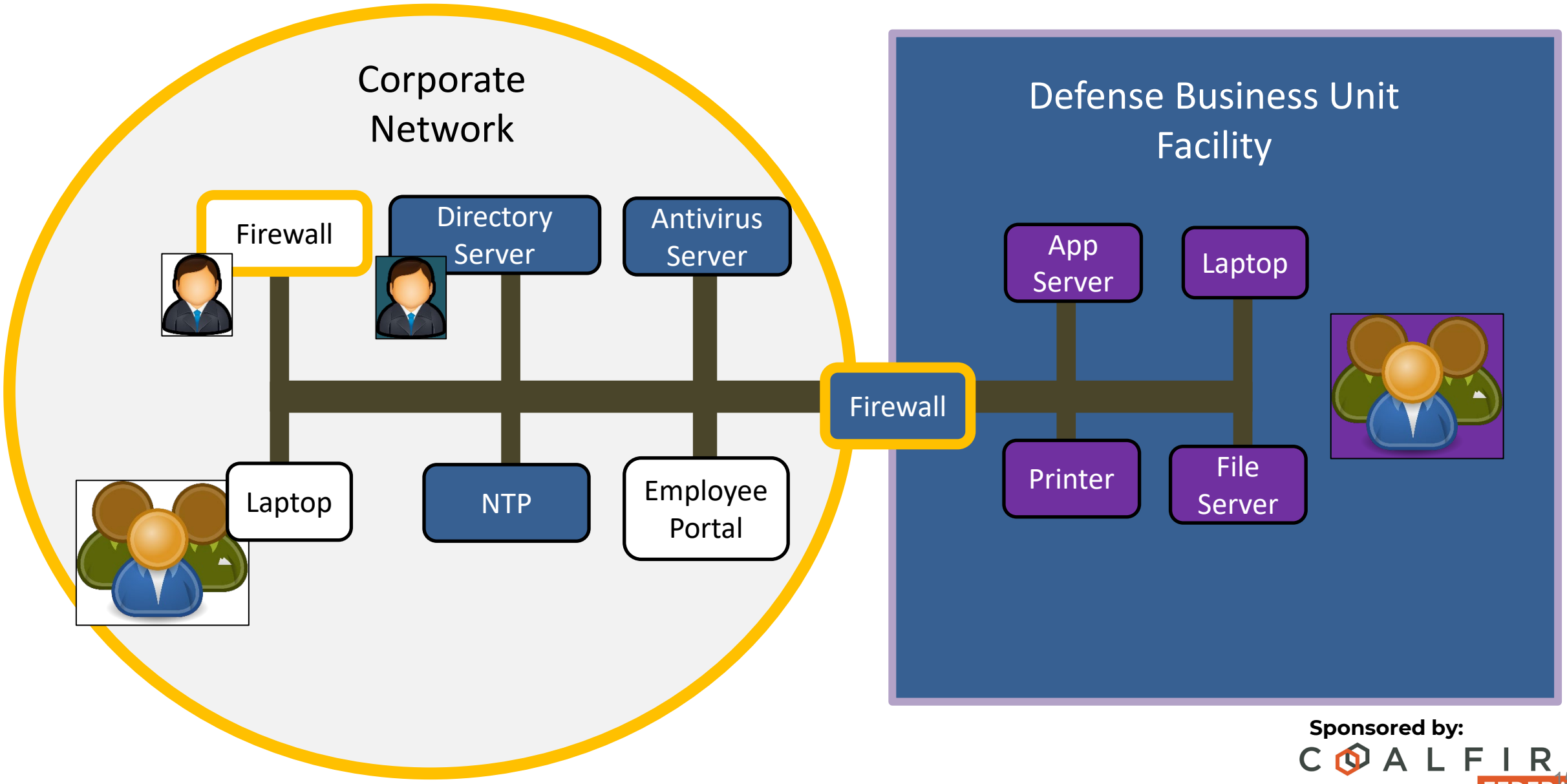
Cloud Services and Managed Services

- **Cloud Services that store, process, or transmit CUI are in scope…**
  - …And must meet the requirements of the FedRAMP Moderate baseline
  - …Relieve you of some responsibilities completely – FOR THAT SYSTEM
  - …Relieve you of some responsibilities partially – FOR THAT SYSTEM
- **Beware of claims: "We satisfy 85 of 110 CMMC controls"**
- **Managed Services and 3rd parties**
  - If they provide security services or have access to CUI, they are in scope
  - Ensure they can demonstrate they satisfy 800-171/CMMC

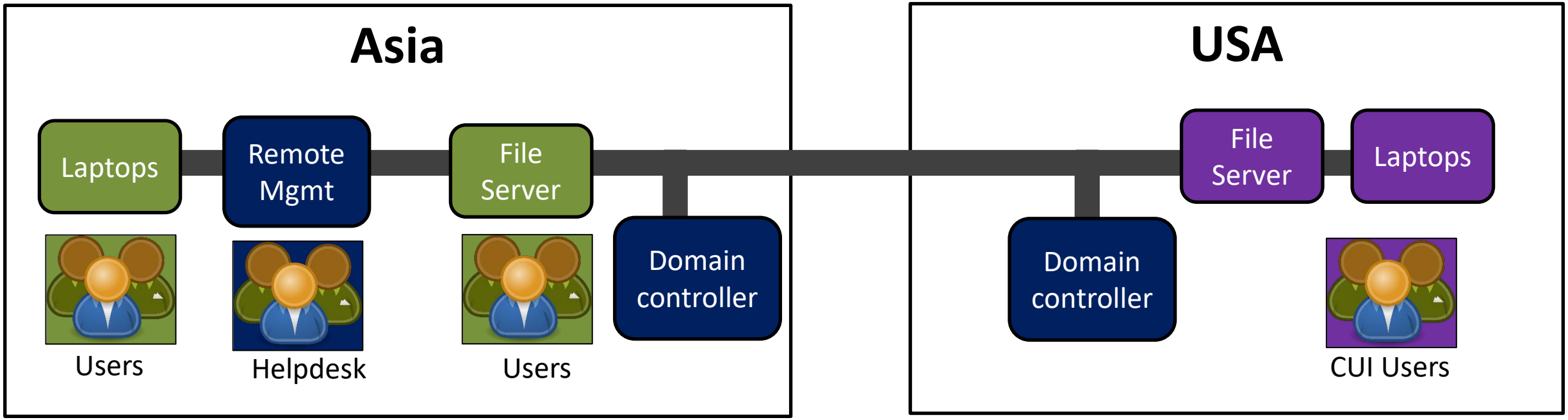
Common mistakes

- **Thinking “risk-managed” means “no security required”**
  - The workstation used to connect to virtual desktops is in-scope
- **Lack of effective boundaries to limit your scope**
  - Assessors expect deny-by-default firewalls between “in-scope” and “out-of-scope” networks
  - Expected to manage risks from connected networks and systems
- **Getting too complicated with data flows**
  - Make multiple small data flow diagrams. Limit the ways CUI moves.
- **CUI needs to be encrypted OR physically protected**
  - Unencrypted email is a huge no-no

Example: Larger company



Example: Multiple locations



NDIA Recommendations

- **Current plan as NDIA understands it will result in significant failure rates across the DIB (and government)**
- **3 Recommendations**

1. **DoD CIO include industry in their assessment plan**
   - Without correction, 1st year assessments could carry 75%+ failure rate
   - Likely to drive industry opt outs, anger & additional congressional oversight
2. **Assess MSPs as part of a cohesive strategy**
   - Verify providers meet standards on behalf of their clients
3. **Adjust implementation plan – Move away from cliff implementation**
   - Max 10% / 11 controls auto-fails
   - 80% of 110 controls = PASS
   - Consider further adjustments for small business

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult

Questions?

Sponsored by: