Where to begin with NIST SP 800-171

Kelley Kiernan
Professor, Cybersecurity
DAU
October 2024

What came first…
FAR 52.204-21
Basic Safeguarding of Covered Contractor Information Systems – Jun 2016

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls: Limit access to authorized users.

- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- Verify controls on connections to external information systems.
- Impose controls on information that is posted or processed on publicly accessible information systems.
- Identify information system users and processes acting on behalf of users or devices.
- Authenticate or verify the identities of users, processes, and devices before allowing access to an information system.

FAR 52.204-21 Security Controls continued

- Sanitize or destroy information system media containing Federal contract information before disposal, release, or reuse
- Limit physical access to information systems, equipment, and operating environments to authorized individuals.
- Escort visitors and monitor visitor activity, maintain audit logs of physical access, control and manage physical access devices.
- Implement sub networks for publicly accessible system components that are physically or logically separated from internal networks.
- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the information system and real-time scans of files from scans of files from external sources as files are downloaded, opened, or executed.
- *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

What data/information does your contract Information System (IS) handle?

- Does your small business contract handle Controlled Unclassified Information (CUI)?
  - Do you receive it from the government?
  - Do you create CUI? It's likely that you do for your Phase II SBIR/STTR contract.
    - Controlled Technical Information (CTI), which is a category of CUI, almost certainly describes your contract deliverables.
      - Training on www.dodcui.mil Then, You decide if it you are creating CTI.
- Even if your contract does not handle CUI you handle FCI. Your Intellectual Property (IP) protection will be enhanced by NIST SP 800-171 implementation
- If your contract handles HIPPA, or ITAR information – your requirements increase
- Learn more about CUI with DAU courses on the topic

Where is your contrct data? How does it flow?

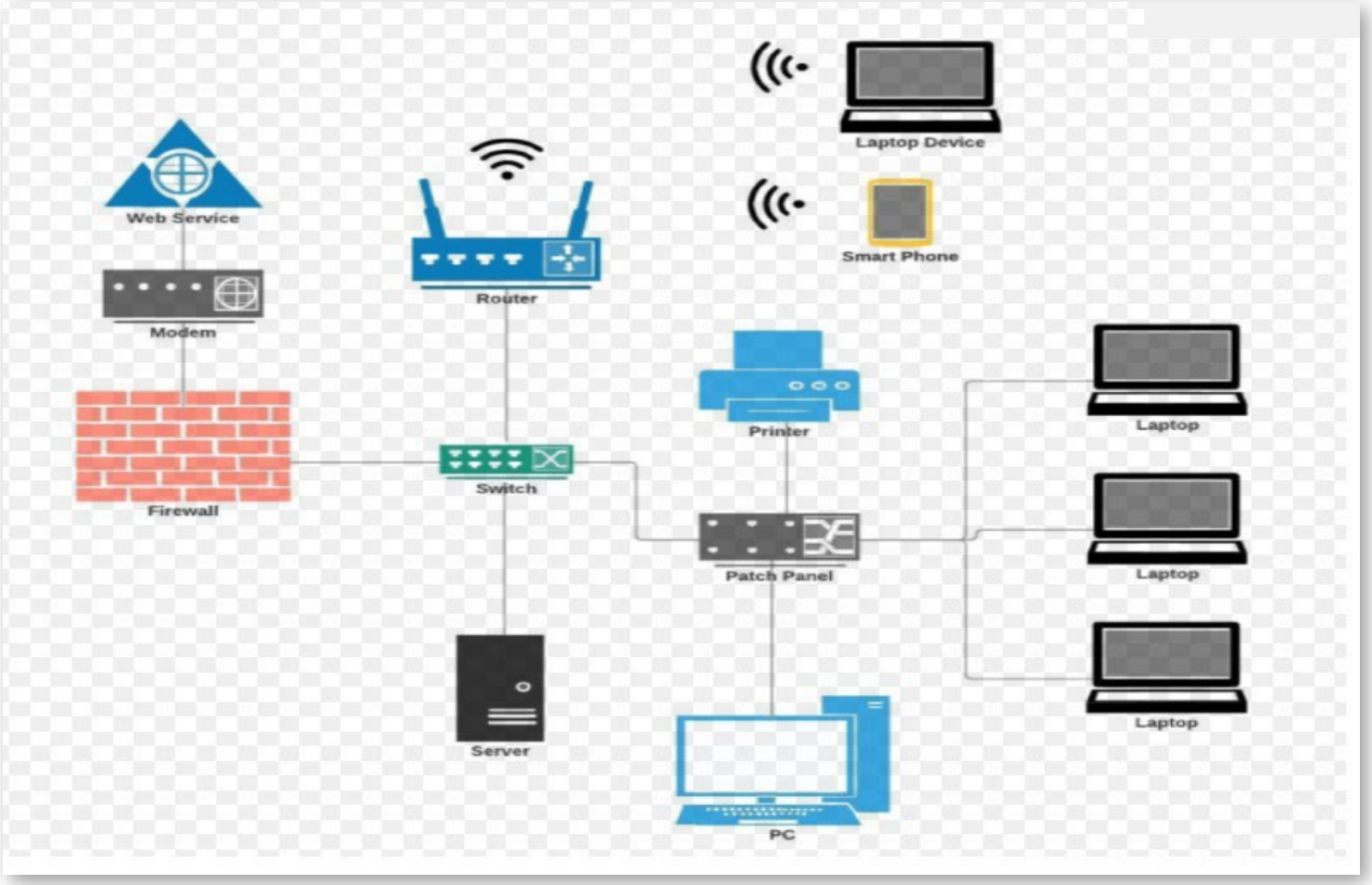
- Understand all the components of your IS?
  - Where is the CUI currently?
    - Local Storage
    - Cloud Storage
    - Printers, Servers, Workstations, IoT devices or other endpoints
    - Mobile/ Portable devices
- Will you treat contract CUI and Proprietary Information the same?
- How will you handle contract Privacy information?

Now that we understand the types of data on your contract Information System…

Draw your IS

Find some icons online and create a comprehensive drawing

Perhaps use a color on the components which handle CUI and another color for components which handle proprietary information.

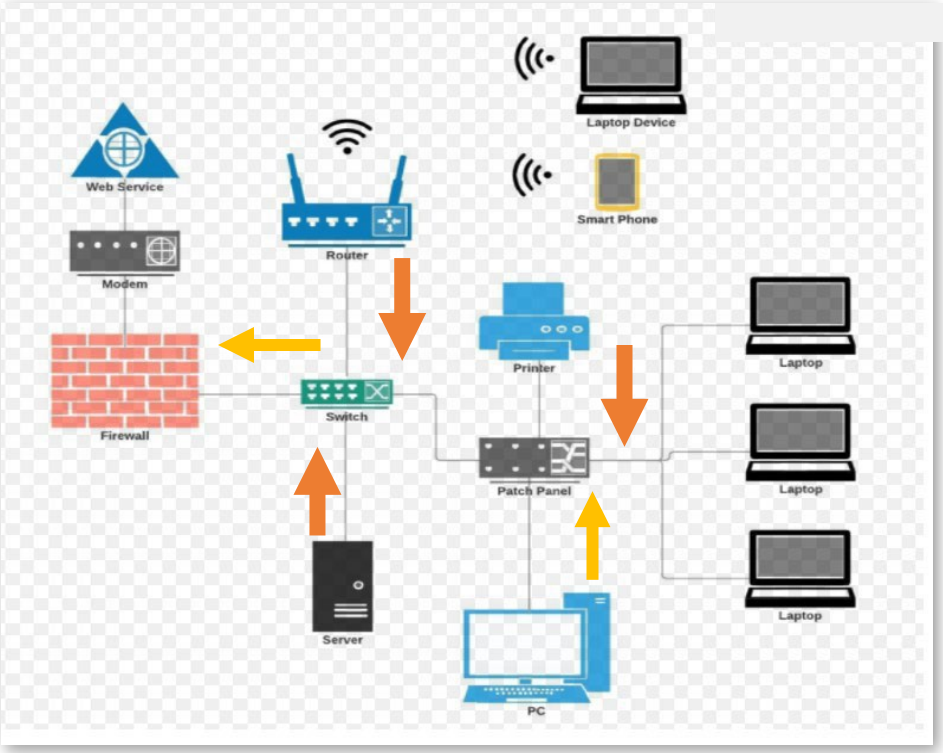


Now that we understand the types of data on your contract Information System…

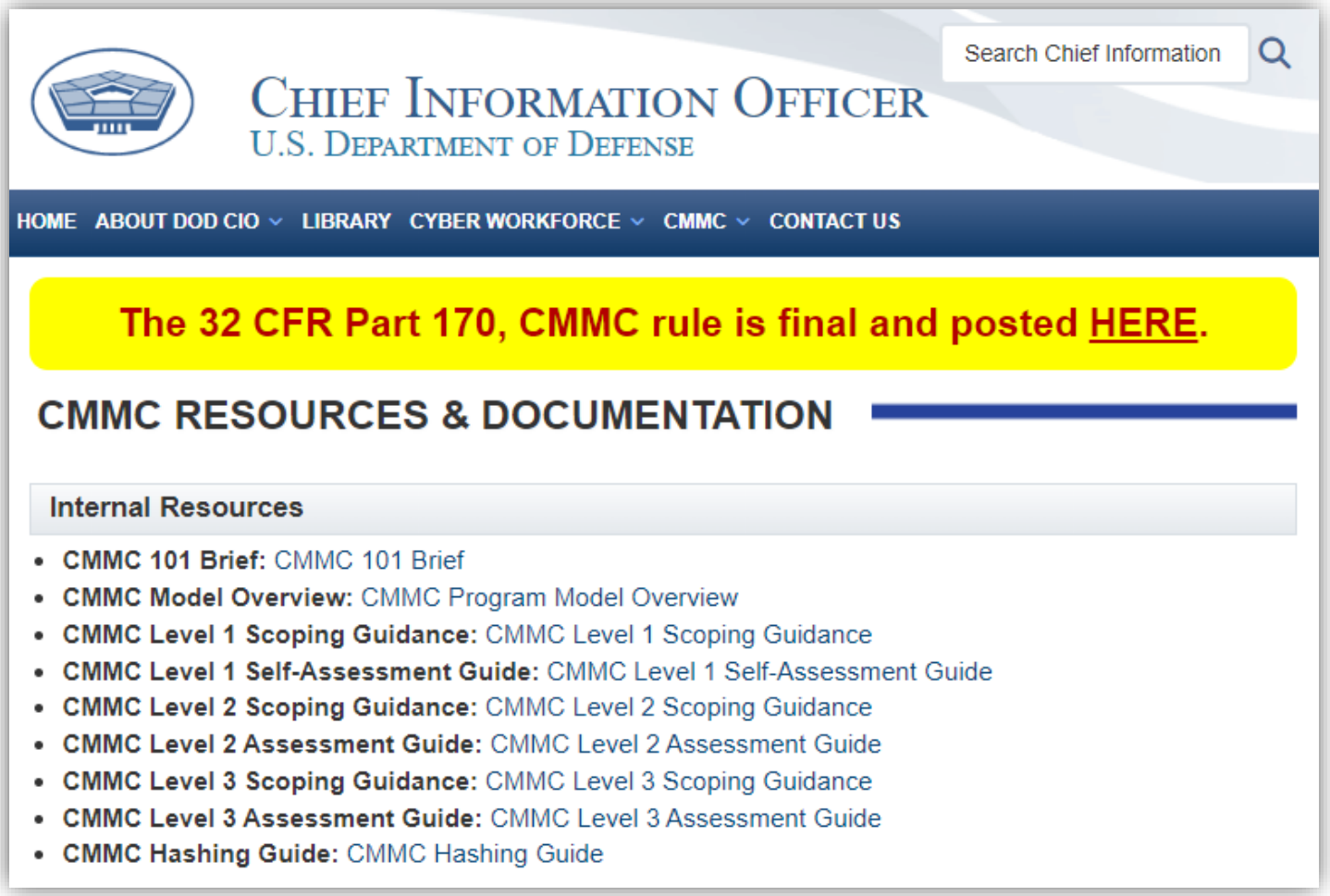
Go ahead and draw the path of both types of information through your information system, From the time they arrive to the time, you perhaps send them to another entity. Where is that data? And how does it flow? What are all the components of your information system? Where is the cui currently?

How will you treat cui and proprietary information? Will you treat them the same? And how will you handle privacy information?

These are questions, which need to be answered before we begin.



Scope your contract Information System's data with DoD Documents



https://dodcio.defense.gov/cmmc/Resources-Documentation/

Your Future Business Plan: Let's Scope It

- Assets process, store, or transmit CUI or FCI as follows:
  - Process – CUI/FCI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).
  - Store – CUI/FCI is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents).
  - Transmit – CUI/FCI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).
- Asset Type
  - People
  - Technology
  - Facility
  - Specialized Assets

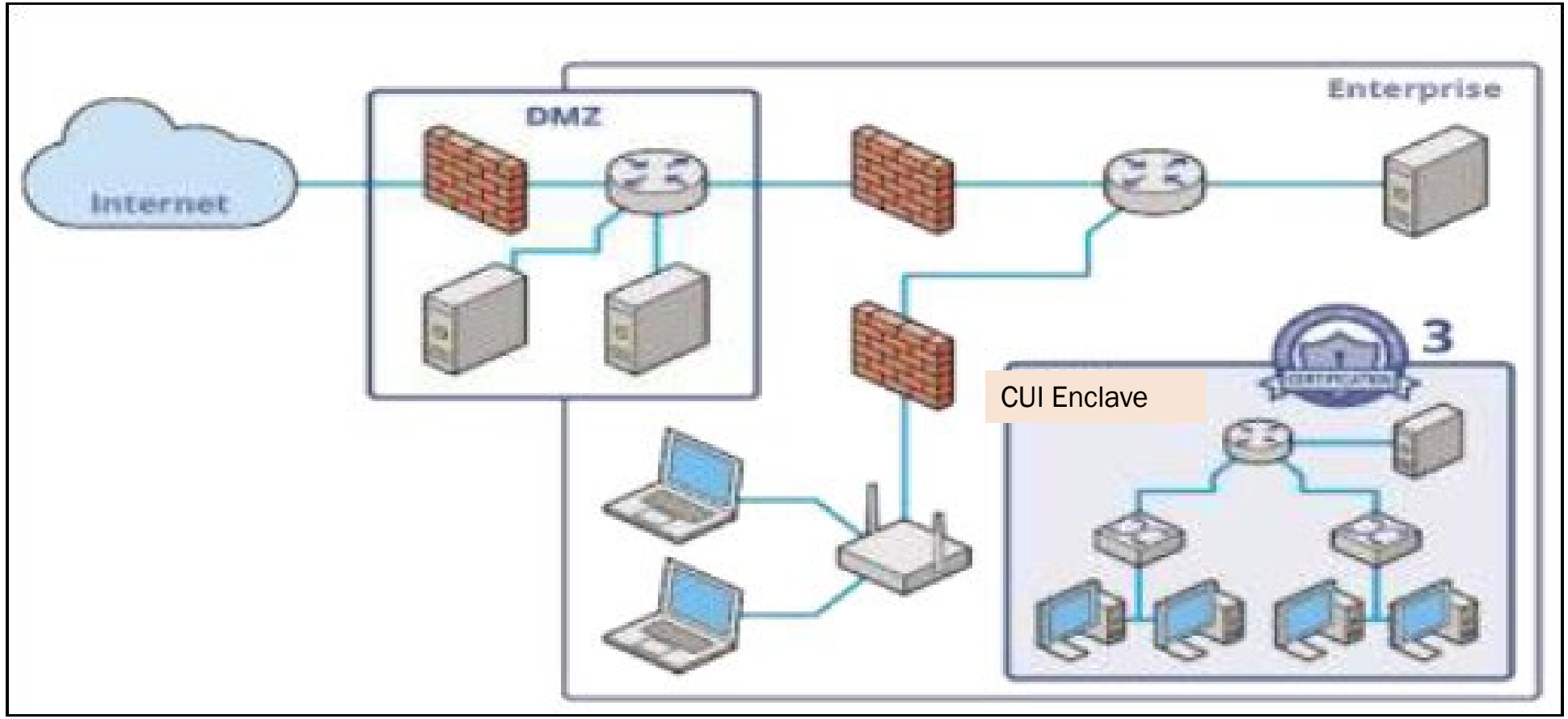
Who is your contract Information System Owner?

- Establish your Information System Owner
  - Is it an employee? Part time or Full Time?
  - It is a cyber professional who consults with your business?
  - Is it a Managed Service Provider
- Who will write your procedures and policies?
- What are your service-level agreement needs?
- Who will implement the technical changes?
- Who will train your employees?
- Who will monitor the logs, access, user-permissions and other records of your IS?
- Who will monitor adherence to procedures and policies?
- How will the firm's leadership gain a practical understanding of all the security requirements for your firm, so as to enable risk-informed decision-making?

Isolated network for CUI

- Advantages:
  - Lower Cost and faster to implement
  - Reduces your continuous monitoring and audit workload if the security requirements only cover 2-3 workstations and no phones
- Disadvantages
  - Susceptible to Insider Threat
  - Could restrict business operations
  - Air-Gap systems tend to create over-confidence

CUI Enclave Concept



Cloud Security

- If you don't own the infrastructure – it's a cloud
  - There are DISA-approved Clouds LINK https://marketplace.fedramp.gov/#!/products?sort=productName
  - There are hundreds of other clouds, including (probably) anything you pay a fee for and anything you can use to manage your system using the vendor's website.
    - Here is the security problem:
      - Many of these providers immediately open remote management links to your network (boundary control)
      - They install remote management software on your devices (admin rights not controlled by you)
      - They have passwords, network diagrams, and vulnerability info for your network (which could be stolen and used against you)
      - Since it isn't your company, their hiring practices, background checks, and internal controls are normally obvious (access management)
      - Since they connect to many networks, they could encounter malware on one client then bring it to your network.

Some of the Highest Cost Considerations

- Professional Advice
- Secure File Transfer – Acceptable means of secure transmission can be expensive. There is a monitoring requirement to ensure proper use of the solution your firm chooses.
- Secure File Storage – Encryptions is your friend. Once data/information is encrypted, it is cyphertext and not CUI; this can simplify your solutions. There is a monitoring requirement to ensure proper use of the solution your firm chooses.
- Secure IS Access – If you minimize the number of devices & people with access to the secure side of your IS and its endpoints (endpoints!), you can reduce your exposure and your monitoring costs.
- Monitoring – A person or an application will need to analyze your IS logs and potential threats. Changes in threat posture or percentage of the IS which handles CUI can be expensive.

Industry Best Practices

- DoD Cyber Crime Center: https://dibnet.dod.mil/dibnet/
- NSA DIB Cybersecurity Services: https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/
- FCC: https://www.fcc.gov/general/cybersecurity-small-business
- FCC Cyberplanner https://www.fcc.gov/cyberplanner
- NDISAC.org: https://ndisac.org/dibscc/cyberassist/
- CDSE Insider Threat Training: https://www.cdse.edu/catalog/insider-threat.html
- NIST Partners: https://www.nist.gov/itl/smallbusinesscyber/partners
- SANS: https://www.sans.org/information-security-policy/
- Project Spectrum IO: https://www.projectspectrum.io/#/

NIST SP 800-171 Preparation Process

- Understand the Importance of Scoping your contract implementation of NIST SP 800-171
- Describe your future business plan to ensure your business has cybersecurity
- Describe your contract Information System
- Describe your contract data and it's flow
- Describe your contract Information System Owner; It's important to have a professional on your team
- Could you make a sensitive data enclave work for your business?
- Are you in a DISA-approved Cloud?
- Take this information to your NIST MEP and ask for a Cybersecurity Gap Analysis – if your state NIST MEP Office can't offer you this service ask for an email referral to another state which can!

DAU

CYBER

CONTRACTS

SOLUTIONS

SECURITY

FAR 52.204-21 / Proposed CMMC Level 1

Basic Cyber Hygiene Walk-through

Nov 18, 2024
Dec 16, 2024

With Kelley Kiernan,
Professor of Cybersecurity at DAU

Register and learn more at
www.DAU.edu/events

www.DAU.edu

DAU

CYBER

CONTRACTS

SOLUTIONS

SECURITY

A Primer on Contract Requirements for Supply Chain Risk Management

With Kelley Kiernan,
Professor of Cybersecurity at DAU

Dec 12, 2024
1pm EST

www.DAU.edu

Register and learn more at https://www.dau.edu/events

Contact Information

Questions?

Kelley.Kiernan@dau.edu