AN OFFERING IN THE BLUE CYBER SERIES:

Where to begin with NIST SP 800-171 Implementation

Version 14 March 2022

#10 in the Blue Cyber Education Series

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.

- Sanitize or destroy information system media containing Federal contract information before disposal, release, or reuse.

2

FAR 52.204-21 fifteen basic cybersecurity requirements

- 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.

3

Preparation Process

- Describe your future business plan to ensure your business has cybersecurity

- Describe your Information System

- Describe your data and it's flow

- Describe your Information System Owner

- 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!

4

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
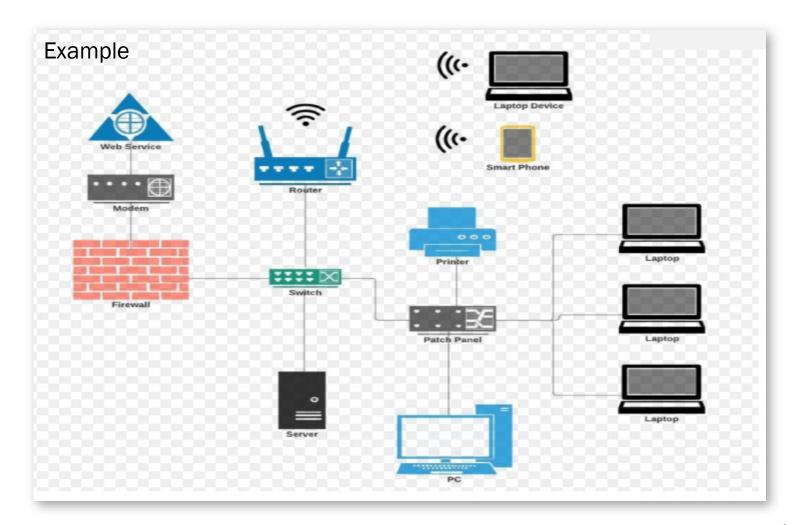
  - Facility

  - Specialized Assets

5

Draw your IS

Find some icons online and create a comprehensive drawing

Perhaps use a color on the components which handle CUI

Example

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

- Does your small business 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 you do not handle CUI you handle FCI. Your Intellectual Property (IP) protection will be enhanced by NIST SP 800-171 implementation

- If your firm handles HIPPA, or ITAR information – your requirements increase

Where is your 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
    - Portable devices
- Will you treat CUI and Proprietary Information the same?
- How will you handle Privacy information?

Who is your 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?
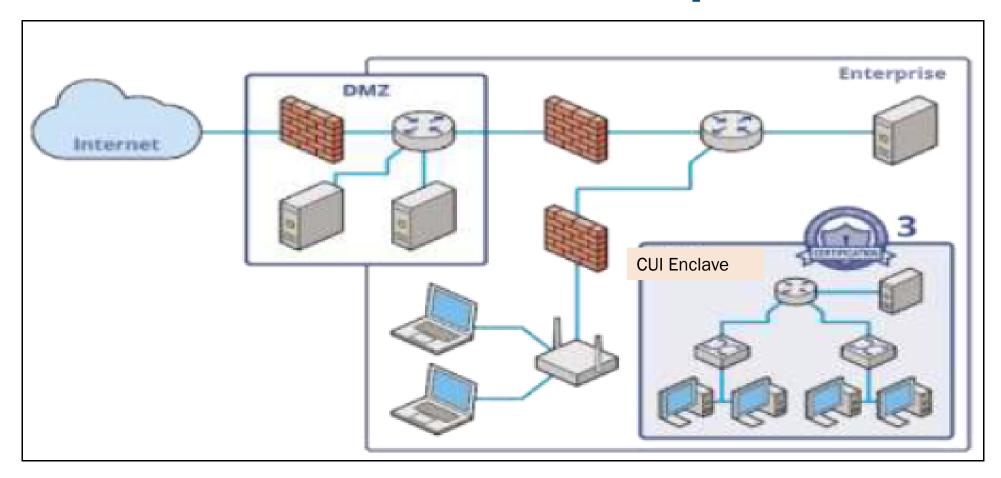
Isolated network for CUI

- 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.

12

Cost Considerations

- 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. can easily follow S-cost curves (with additional incremental gains in capability coming at significant cost increases).
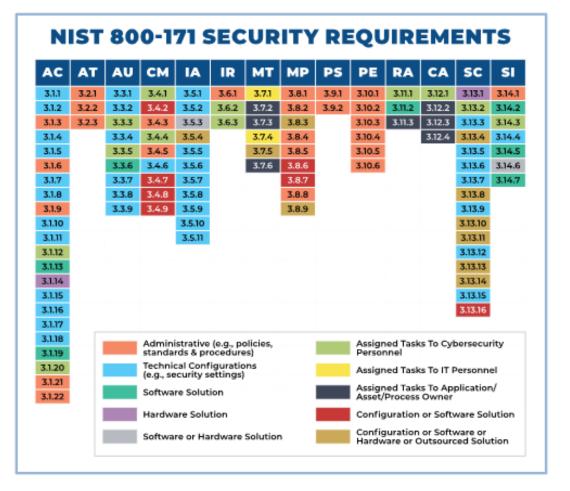
13

Industry Best Practices

- 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

- SBA Local Assistance: https://www.sbir.gov/local-assistance

- NIST Partners: https://www.nist.gov/itl/smallbusinesscyber/partners

- SANS: https://www.sans.org/information-security-policy/

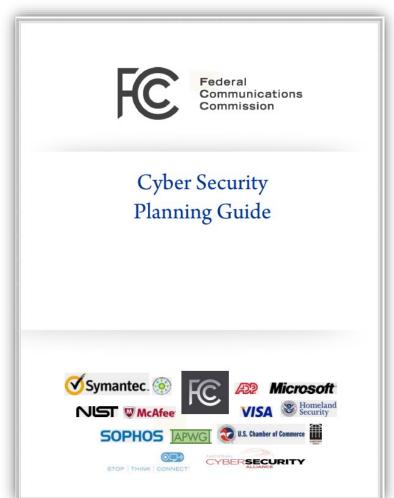- Project Spectrum IO: https://projectspectrum.io/#/

NISP SP 800-171 Requirements

FCC Cybersecurity Planning Guide

- Privacy and Data Security
- Scams and Fraud
- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Facility Security
- Operational Security
- Payment Cards
- Incident Response and Reporting
- Policy Development, Management

16

MANUFACTURING EXTENSION PARTNERSHIP (MEP)

MEP is a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers. Last year, MEP Centers interacted with 27,574 manufacturers, leading to $13.0 billion in sales, $2.7 billion in cost savings, $4.9 billion in new client investments, and helped create or retain 105,748 jobs.

MEP ● **MANUFACTURING EXTENSION PARTNERSHIP**®

Coronavirus: Resources, Updates, and What You Should Know

ABOUT NIST MEP +

MEP NATIONAL NETWORK +

EXECUTIVE ORDER 14005

SUPPLIER SCOUTING

CYBERSECURITY RESOURCES FOR MANUFACTURERS +

MATTR

MANUFACTURING INFOGRAPHICS +

MANUFACTURING REPORTS

MANUFACTURING DAY

MANUFACTURING INNOVATION BLOG

CONTACT US

HOW THE NETWORK HELPS MANUFACTURERS

CONNECT WITH YOUR LOCAL MEP CENTER

SUPPLIER SCOUTING

EXECUTIVE ORDER 14005 ON ENSURING THE FUTURE IS MADE IN ALL OF AMERICA BY ALL OF AMERICA'S WORKERS

ALL 51 MEP CENTERS HELPING U.S. MANUFACTURERS MAKE SUCH THINGS AS PPE FROM THE $50M APPROPRIATED BY CONGRESS

CONNECT WITH US

SANS Sites ∨   Search 🔍   Log In   Join

SANS

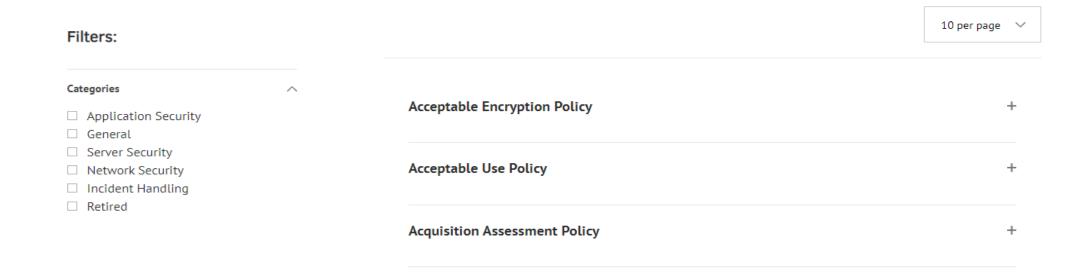Train and Certify   Manage Your Team   Resources   Focus Areas   Get Involved   About

Security Policy Templates

In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted here a set of security policy templates for your use. To contribute your expertise to this project, or to report any issues you find with these free templates, contact us at policies@sans.org.

Filters:

10 per page ∨

Categories ∧

- ☐ Application Security
- ☐ General
- ☐ Server Security
- ☐ Network Security
- ☐ Incident Handling
- ☐ Retired

Acceptable Encryption Policy   ＋

Acceptable Use Policy   ＋

Acquisition Assessment Policy   ＋

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.

- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions at https://www.safcn.af.mil/Contact-Us/

  - ➢ **Every Tuesday**, 1pm Eastern, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything.

19