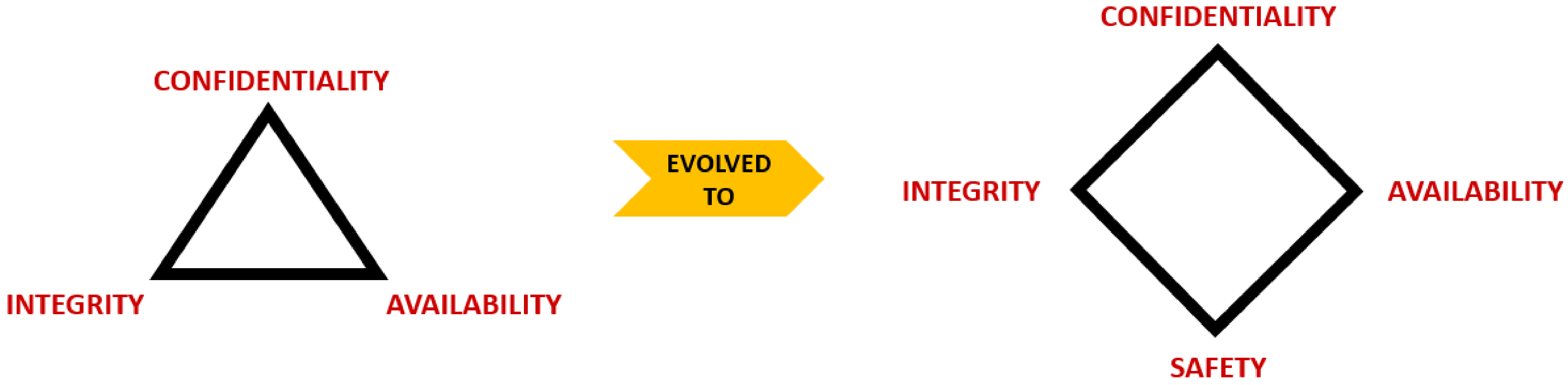
Complying With Requirements For Safeguarding Contractor Information Systems

TOPICS COVERED

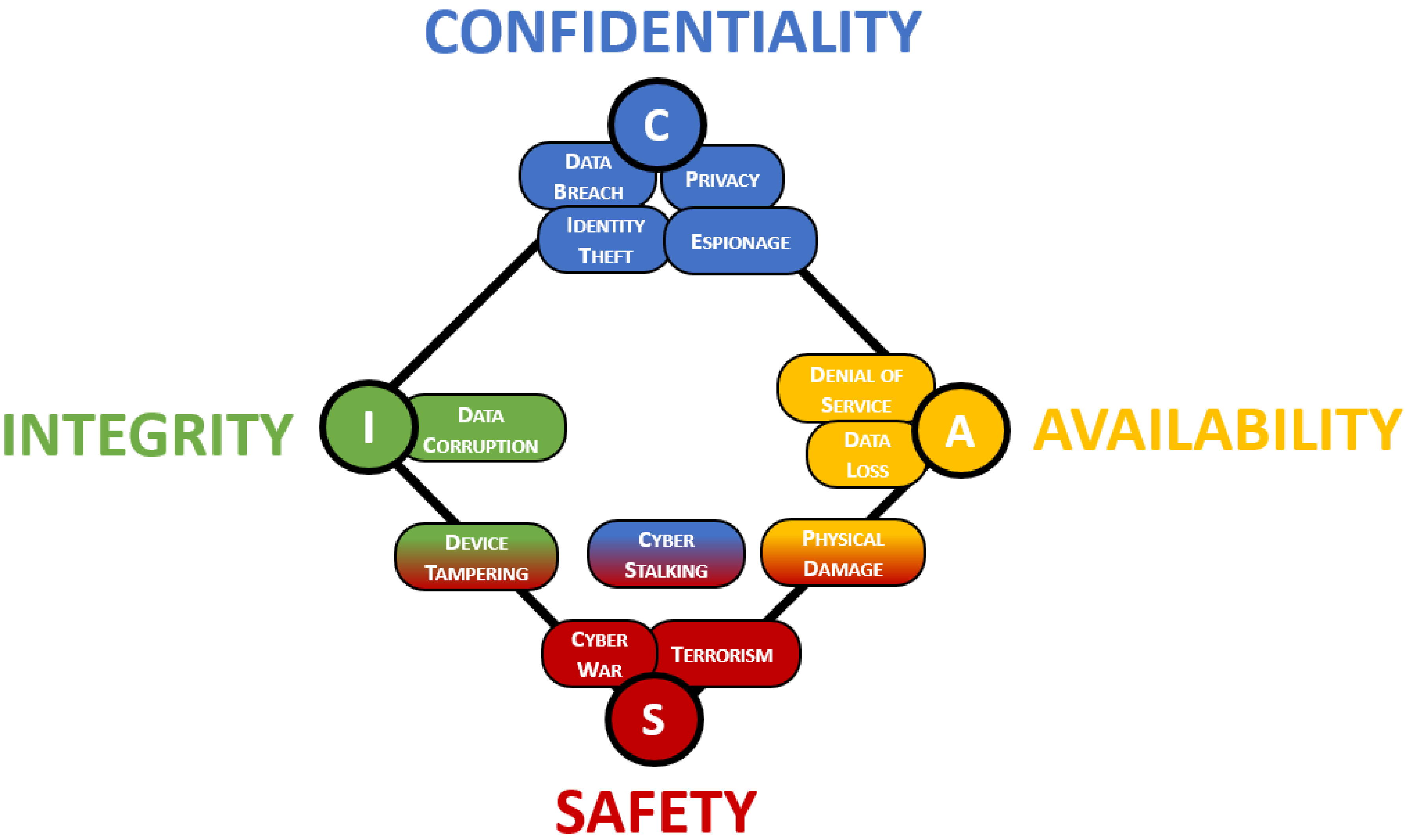
- Level-Setting On Security Concepts
- Review DFARS & FAR requirements
- Origin of NIST 800-171 Requirements
- NIST 800-53 Relationship To NIST 800-171
- Defining Due Care & Due Diligence
- Scoping Considerations For NIST 800-171
- Q&A

The CIA Triad

For years, the focus of security controls was on the "CIA Triad" and now it has evolved to address real-world SAFETY concerns.

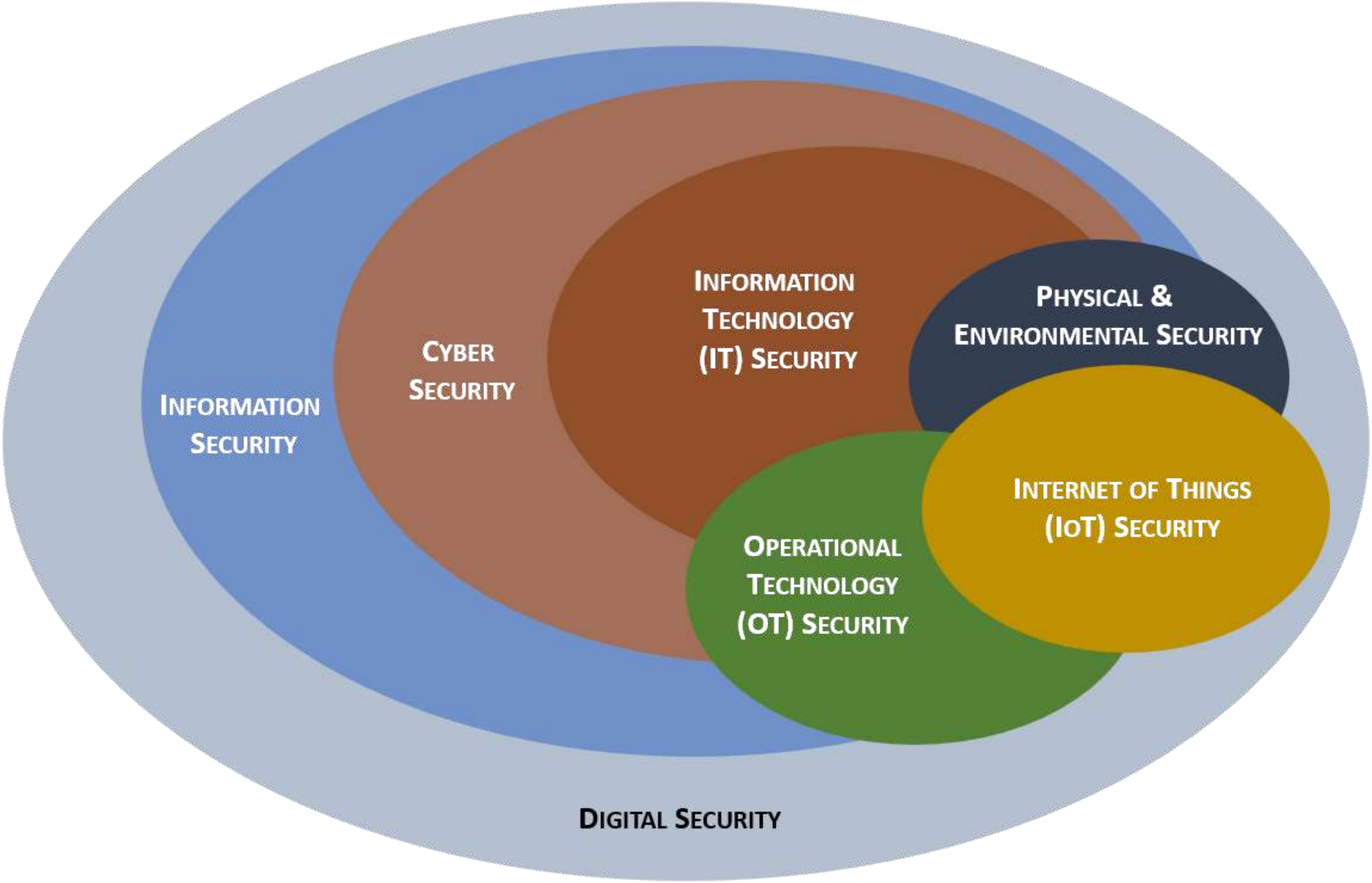


CIAS Security Model



Evolving Terminology

The scope of security concerns evolved over time


Information Technology (IT) Security
Physical & Environmental Security
Cyber Security
Information Security
Internet of Things (IoT) Security
Operational Technology (OT) Security
Digital Security

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) 252.204-7012

"Adequate Security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

- Defined by the security requirements in the contract for services or systems operated on behalf of the US Government.
- **Defined by NIST 800-171** for all other "Covered Contractor Information Systems."

"Covered Contractor Information System" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits "Covered Defense Information."

"Covered Defense Information (CDI)" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry.

Controlled Unclassified Information (CUI) Registry

"**Controlled Technical Information (CTI)**" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

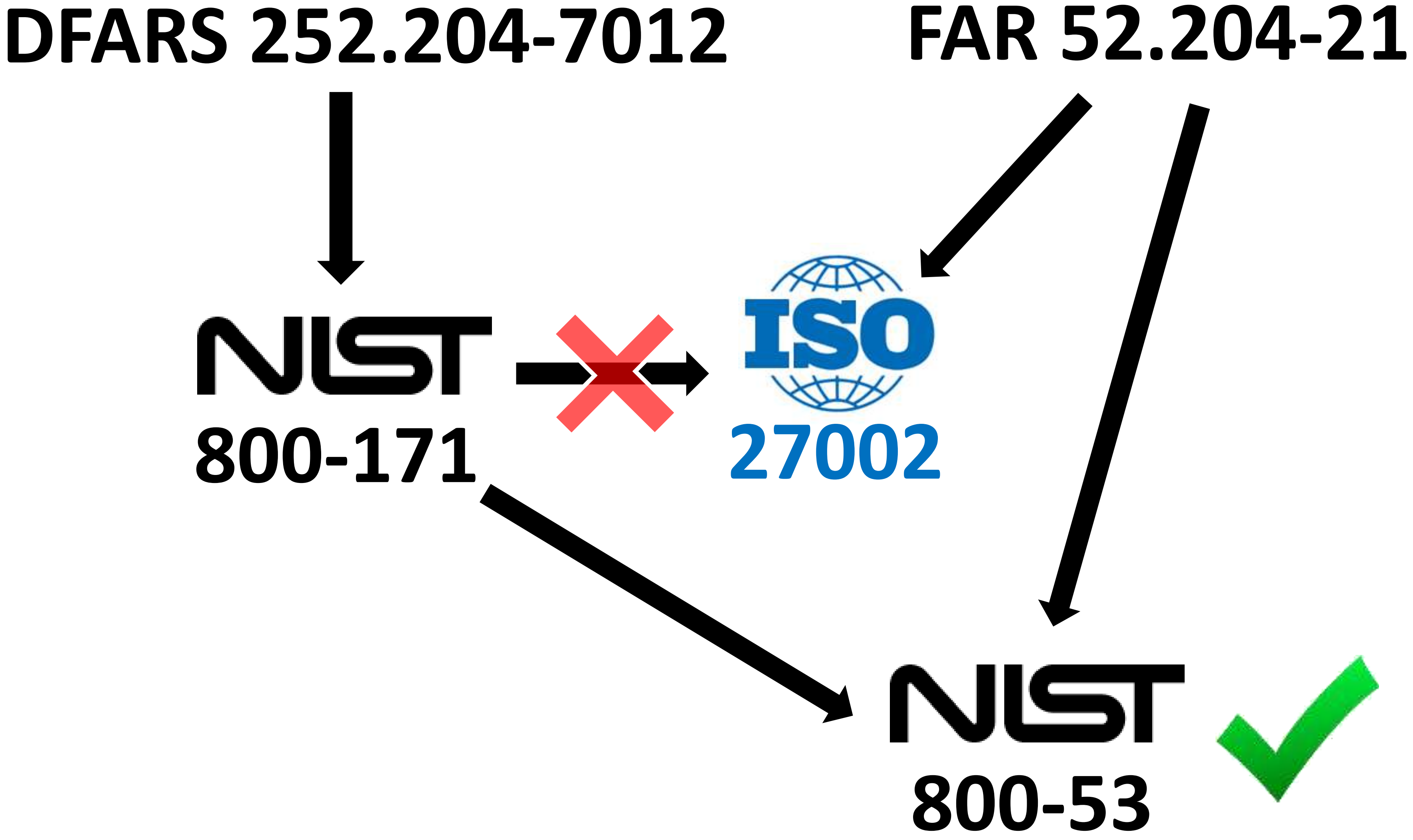
- Controlled technical information is to be marked in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents."
- The term does not include information that is lawfully publicly available without restrictions.
- "Technical Information" means technical data or computer software. Examples of technical information include:
  - Research and engineering data
  - Engineering drawings
  - Associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and
  - Computer software executable code and source code.

Federal Acquisition Regulation (FAR) 52.204-21

“Safeguarding” means measures or controls that are prescribed to protect information systems.

- Defined by fifteen (15) non-prescriptive, generic security controls

Picking A Framework



DFARS 252.204-7012

FAR 52.204-21

NIST 800-171

ISO 27002

NIST 800-53 ✓

NIST 800-171

NIST 800-171 is made up of fourteen (14) families of controls.

- These families of controls consist of a basic security requirements section and a derived security requirements section.
- Both basic and derived are required.
- Controls start with a 3.X.X because it is covered in Chapter 3.

Basic Security Requirements

The basic security requirements are obtained from **FIPS Publication 200**, which provide the high-level and fundamental security requirements for federal information and systems.

Derived Security Requirements

The derived security requirements, which supplement the basic security requirements, are taken from the security controls in **NIST 800-53**.

NIST 800-171

Appendix D

Provides informal mapping of the security requirements related to:

- NIST 800-53
- ISO 27002

Appendix E

Complete listing of applicable security controls that support CUI-derived security requirements.

- Equates to the NIST 800-53 MODERATE baseline security controls

Due Care vs Due Diligence

Due Care

Degree of care that an ordinary and reasonable person would normally exercise under circumstances.

- Establishing security policies, standards & procedure documentation
- Conducting Business Impact Analysis (BIA)
- Establishing documented roles & responsibilities

Due Diligence

Refers to the ongoing effort made by a reasonable individual to avoid harm to another party.

- Conducting technical compliance audits
- Conducting periodic risk assessments
- Performing periodic performance reviews

Where To Start?

#1. Document your business processes and data workflows to identify known and potential instances where CUI is stored, processed or transmitted. [due care]

#2. For each instance identified, evaluate the business need to handle CUI:

- If CUI is not needed, stop collecting it and securely dispose of what has been collected.
- If CUI is required, consider migrating the data/process and consolidate it elsewhere in the CUI environment to reduce scope, improve controls, and reduce risk. [due diligence]

#3. Determine the extent of NIST 800-171 compliance through a scoping exercise. [due diligence]

NIST 800-171 Scoping

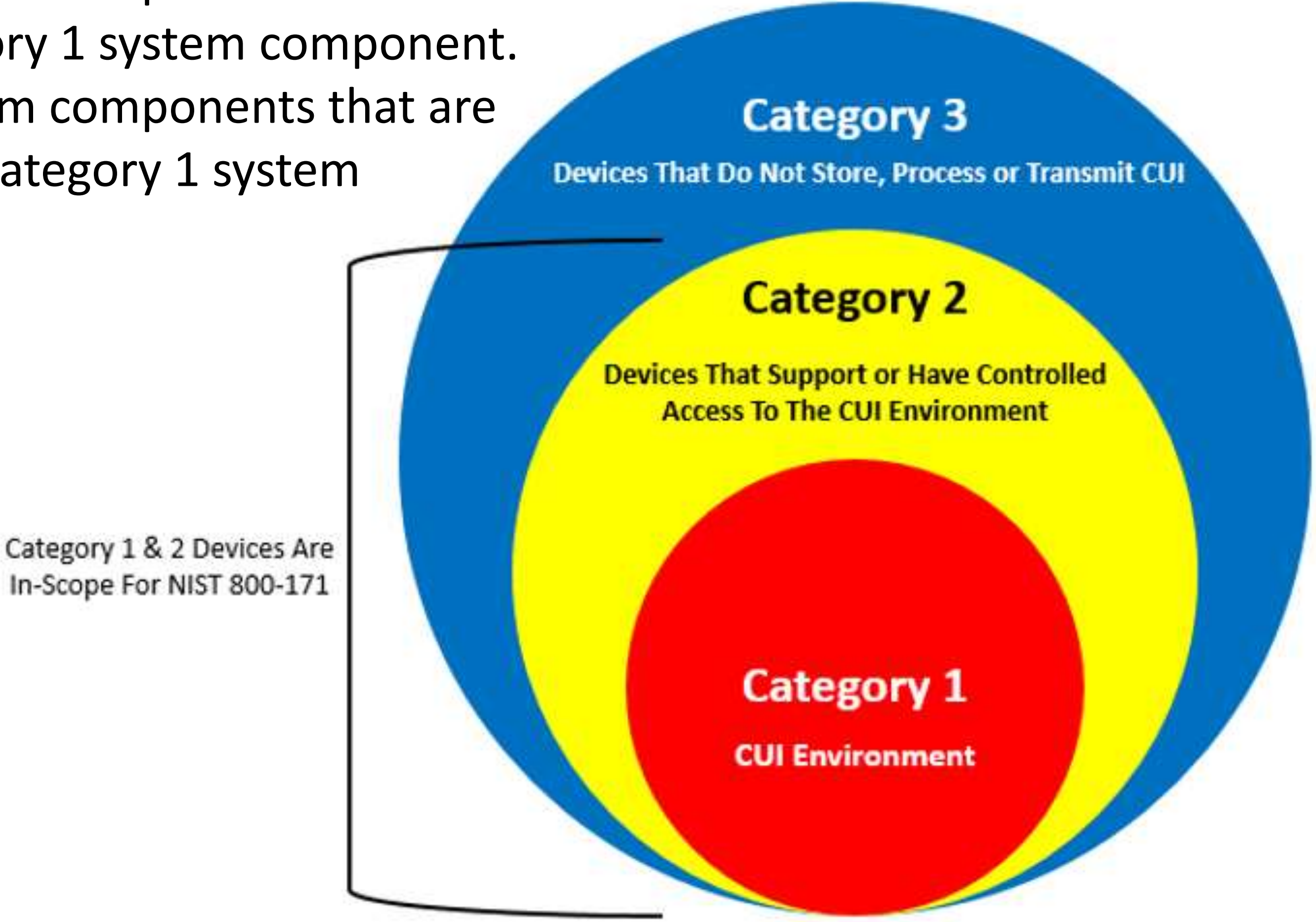
NIST categorizes system components as being either in or out of the scope for NIST 800-171, so there is no official guidance at a more granular-level.

Given that there are similarities between scoping for NIST 800-171 and the Payment Card Industry Data Security Standard (PCI DSS), it is possible to leverage the ***Open PCI DSS Scoping Toolkit*** and apply that similar methodology to NIST 800-171.

Every system component within a company's computing environment can be categorized into one of three (3) categories.

NIST 800-171 Scoping

- **Category 1** – System components that process, store or transmit CUI or are not isolated or restricted through controlled access from other Category 1 system components.
- **Category 2** – System components that have controlled access to a Category 1 system component.
- **Category 3** – System components that are isolated from all Category 1 system components.


Category 3
Devices That Do Not Store, Process or Transmit CUI
Category 2
Devices That Support or Have Controlled Access To The CUI Environment
Category 1
CUI Environment
Category 1 & 2 Devices Are In-Scope For NIST 800-171

NIST 800-171 Scoping

Where this approach is useful is in helping identify interactions with the CUI. Ideally, CUI is either isolated or has controlled access:

- **Isolation** – This is where network traffic between system components is not permitted at all (logical or physical gap).
- **Controlled Access** – This is where access between system components is restricted to defined parameters. Restrictions may include the source, type and direction of traffic.

Scoping Considerations

Categorizing each system component into one of these categories achieves several key results:

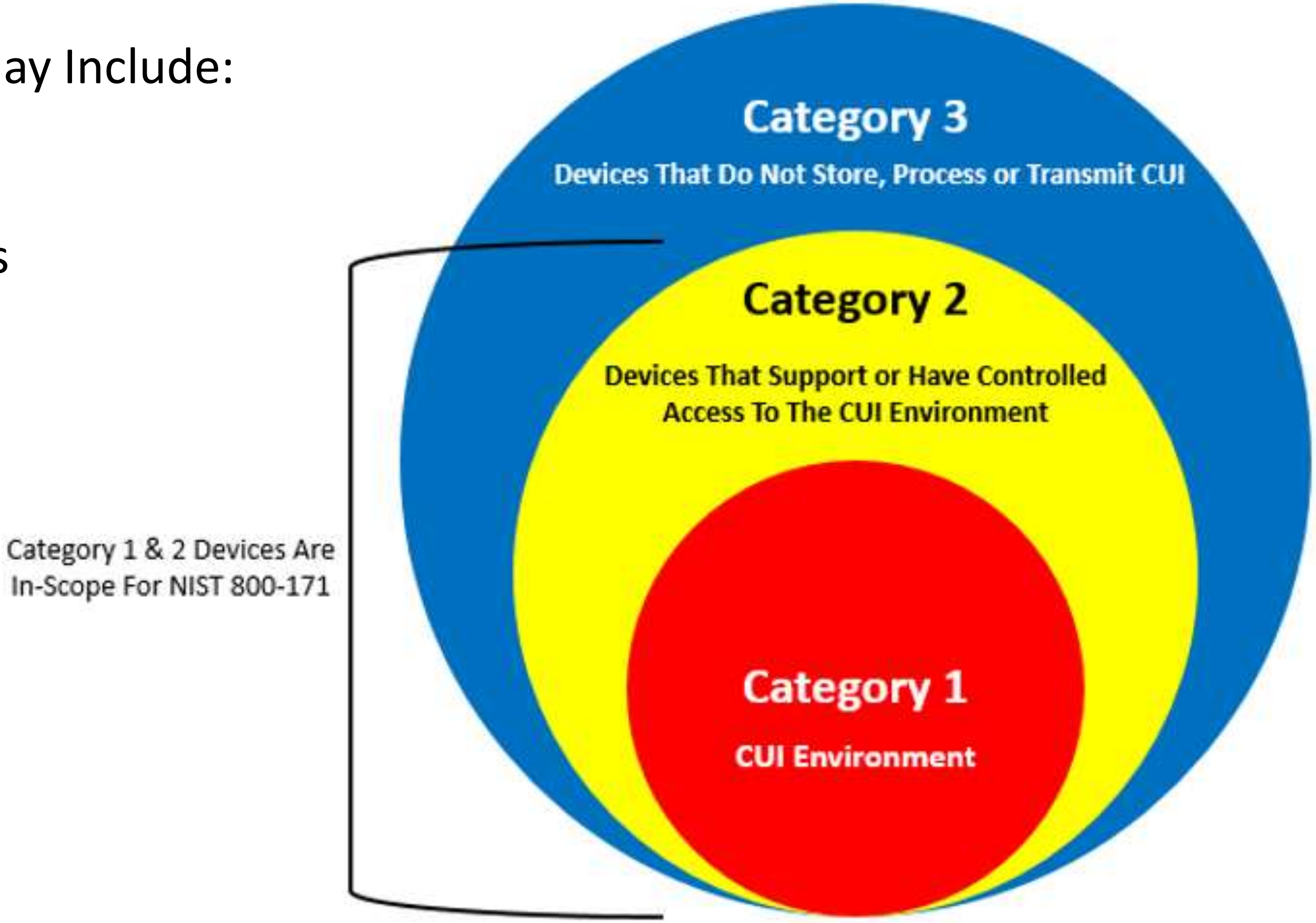
- Identifies all system components that are within the scope of NIST 800-171 compliance;
- Aids in documenting risks to CUI as each system component within the environment is analyzed; and
- Enables the objective evaluation of CUI controls for applicability and necessity.

Scoping - Category 1

- **Category 1** – System components that process, store or transmit CUI or are not isolated or restricted through controlled access from other Category 1 system components.

Category 1 Systems May Include:

- File Servers
- E-mail Servers
- Backup Servers
- SharePoint


Category 3
Devices That Do Not Store, Process or Transmit CUI
Category 2
Devices That Support or Have Controlled Access To The CUI Environment
Category 1
CUI Environment
Category 1 & 2 Devices Are In-Scope For NIST 800-171

Scoping - Category 1

Category	Description
1a	Devices that store, process or transmit CUI.
1b	Devices that do not store, process or transmit CUI, but, are "infected by" Category 1a devices due to the absence of controlled access or isolation.

Implications of Category 1 system components:

- All Category 1 system components are **"infectious"** towards other non-isolated systems;
- All Category 1 system components are always within the scope of NIST 800-171;
- Each Category 1 system component must be evaluated against all NIST 800-171 requirements to determine the applicability of each requirement; and
- All applicable NIST 800-171 control requirements are necessary for every Category 1 device.

Scoping - Category 1

The idea of an asset being **"infectious"** is an interesting concept to consider:

- **INFECTIOUS** - A system is considered Category 1a if it stores, transmits or processes CUI.
  - These systems that stores, processes or transmits CUI data are "infectious" to other systems.

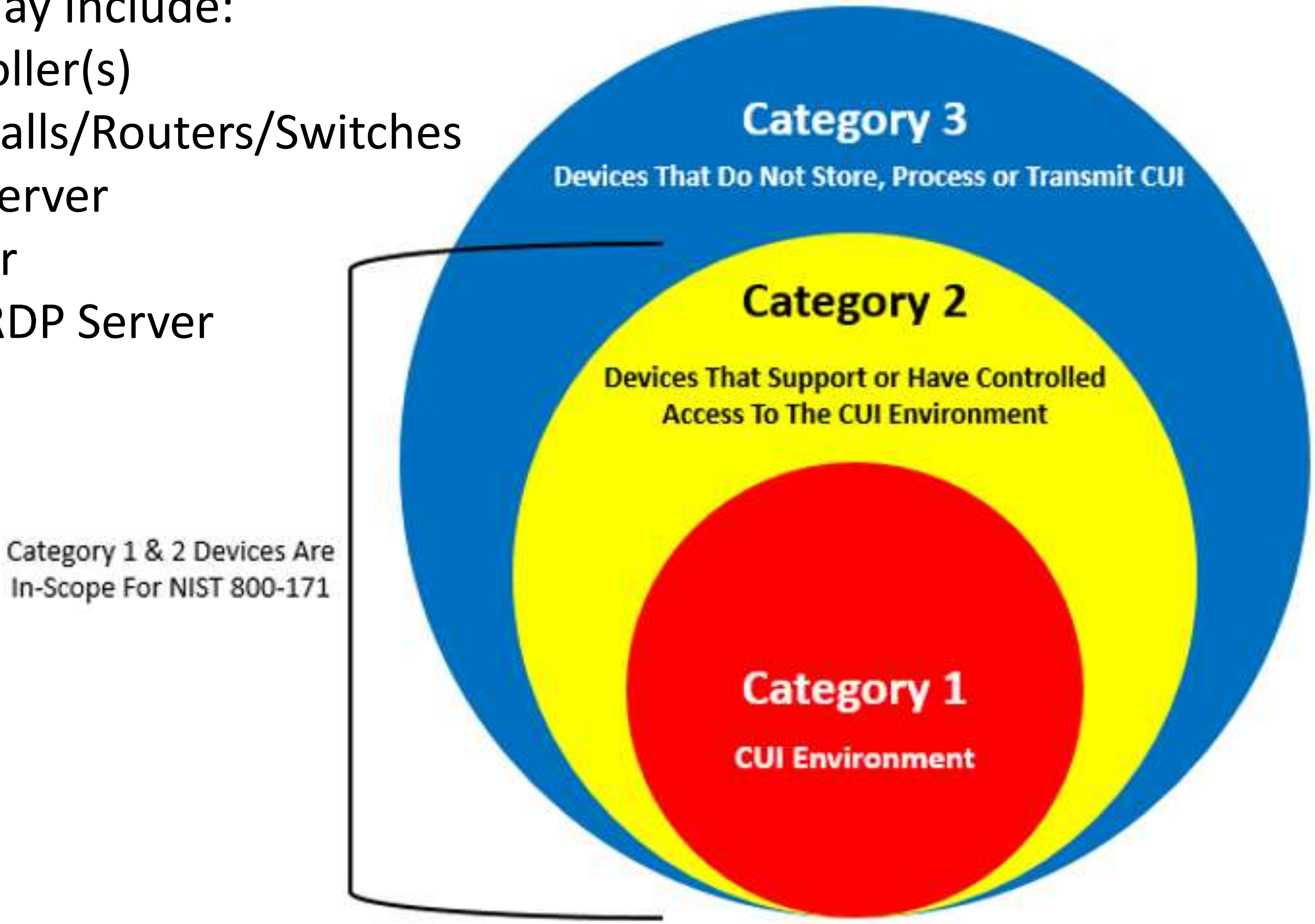
- **INFECTABLE** – All devices that have unrestricted network access to that Category 1a device become Category 1b devices, even if they do not store, process or transmit CUI.
  - Essentially, by lacking controlled access, these systems are "infectible" by devices that contain CUI.

Scoping - Category 2

- **Category 2** – System components that have controlled access to a Category 1 system component.

Category 2 Systems May Include:

- Domain Controller(s)
- Network Firewalls/Routers/Switches
- Antimalware Server
- Patching Server
- “Jump Box” / RDP Server


Category 3
Devices That Do Not Store, Process or Transmit CUI
Category 2
Devices That Support or Have Controlled Access To The CUI Environment
Category 1
CUI Environment
Category 1 & 2 Devices Are In-Scope For NIST 800-171

Scoping - Category 2

Category	Description
2a	System components which, through controlled access, provide security services (e.g., Active Directory, remote access, centralized antimalware, logging, monitoring, IPS/IDS, etc.) to a Category 1 device.
2b	System components which, through controlled access, can initiate an inbound connection to a Category 1 device.
2c	System components which, through controlled access, can only receive a connection from a Category 1 device (i.e., cannot initiate a connection).
2x	System components which, through indirect and controlled access, have the ability to administer Category 1 devices. <u>Note:</u> Category 2x devices have no direct access to/from Category 1 devices (e.g., access through a jump box).

Scoping - Category 2

Implications of Category 2 system components:

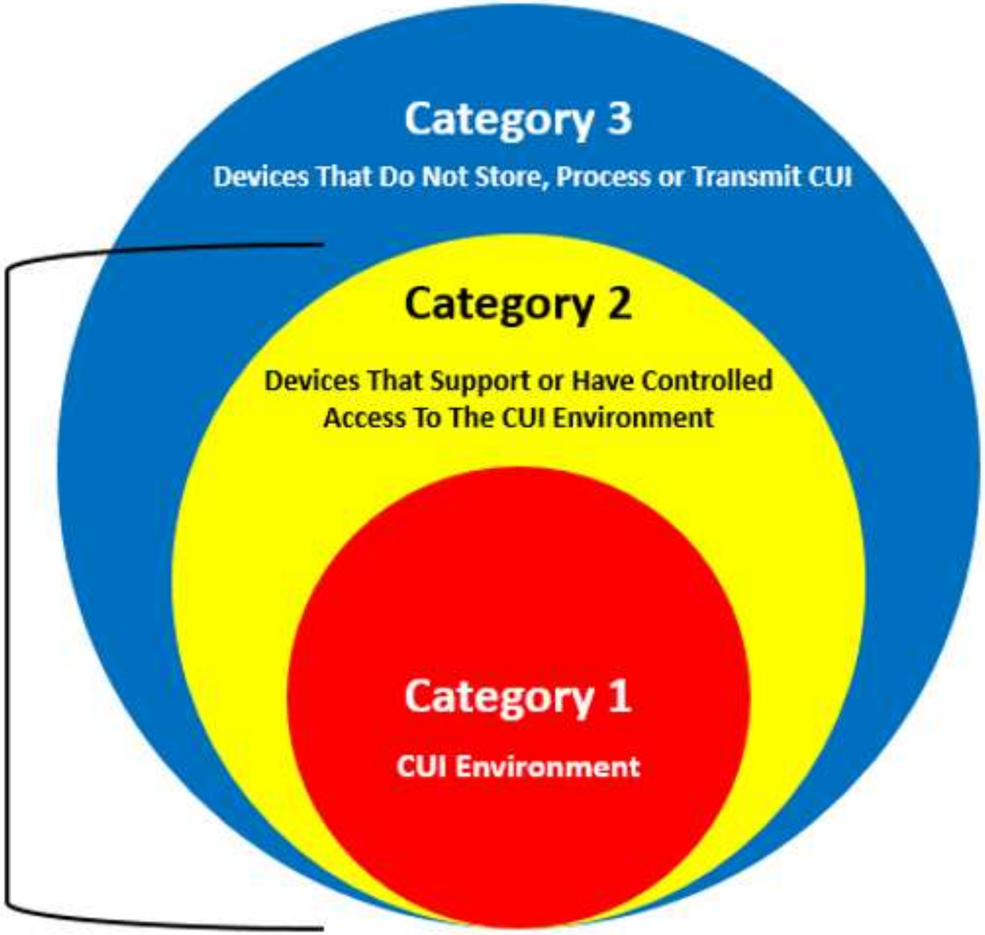
- Category 2 system components have controlled access to the CUI environment;
- Category 2 system components are not infectious;
- Category 2 system components are always within the scope of NIST 800-171;
- Each Category 2 system component must be evaluated against all NIST 800-171 requirements to determine the applicability of each requirement, as well as the necessity of each control based on an assessment of the risk to the CUI environment and the overall control environment.
- Category 2 system components must be adequately protected to prevent Category 3 devices from being a valid vector of attack.

Scoping - Category 3

- **Category 3** – System components that are isolated from all Category 1 system components.

Examples Include:

- Guest Wireless Network
- General User Computers
  (e.g., receptionist's computer)


Category 3
Devices That Do Not Store, Process or Transmit CUI
Category 2
Devices That Support or Have Controlled Access To The CUI Environment
Category 1
CUI Environment

Category 1 & 2 Devices Are In-Scope For NIST 800-171

Scoping - Category 3

Category 3 system components:

- Do not store, process or transmit CUI;
- Are isolated from; and
- Do not provide any services to any Category 1 device.

Therefore, Category 3 system components are not in the scope of NIST 800-171.

Common Questions

1. When do we have to have this done by?
2. How much does NIST 800-171 compliance cost?
3. How long will it take me to become compliant?
4. Is there an official certification process?
5. Do I need full-time security staff to comply?

Open Questions

?

Support@ComplianceForge.com