Step 1: Know the CUI You're Responsible For and Determining Your Boundary

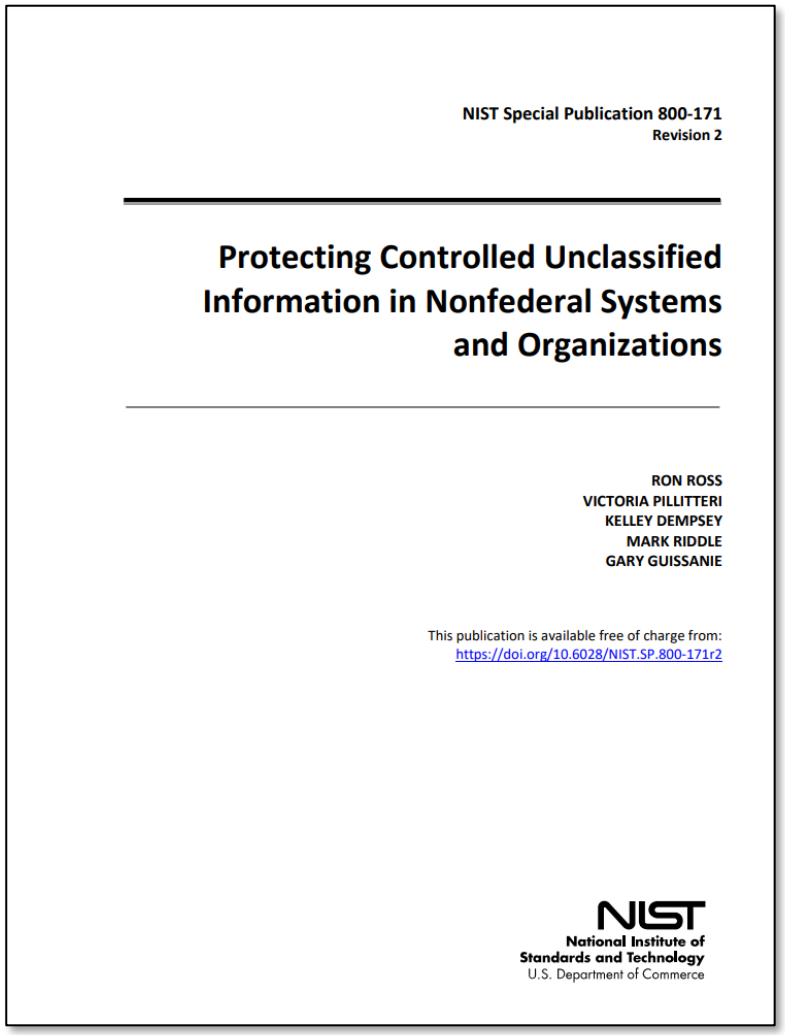
Stuart Itkin
Vice President, NeoSystems

A Bit About Me

- Key contributor to LOGMARS standard and the application of automation technologies to the DoD supply chain starting in the 1990s
- Currently Vice President at NeoSystems, focused on bringing managed services and professional services to small and medium businesses to address their DoD cybersecurity requirements
- Previously:
  - Vice President of CMMC and FedRAMP Assurance at Coalfire Federal, an authorized C3PAO and RPO
  - Vice President of Products and Marketing at Exostar, a Boeing, Lockheed Martin, Raytheon Technologies, BAE Systems, Rolls Royce formed joint venture company
  - Lead mentor at Virginia State Government funded MACH37 cybersecurity product accelerator
- BA, MA, and ABD from the University of Illinois at Urbana-Champaign

What We'll Talk About

- CMMC and NIST 800-171 are about protecting information
- Protecting that information involves
  - People
  - Processes
  - Facilities
  - Information Technology
- Before you start, you need to know what information to protect
- You need to know who, where, and what is in scope – and you may want to reduce that


NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Easy Part: The CUI I Am Responsible For

Controlled Unclassified Information is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. 32 CFR § 2002.4 (h)

Your responsibility:

- Understand, Identify, & Handle CUI
- Understand the CUI Security Requirements
  - ✓ Implement Correctly
  - ✓ Operate as intended
  - ✓ Produce the desired outcome

Any information that is lawfully publicly available is **NOT** CUI

Received or Created by or on behalf of the DoD

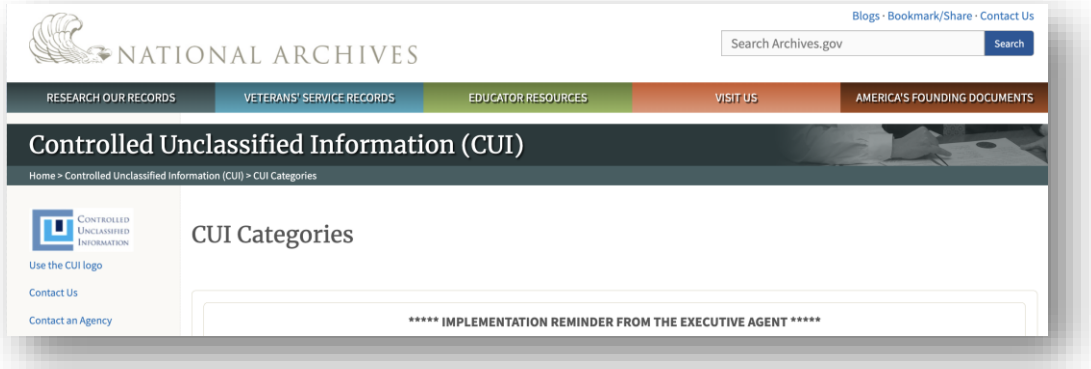
Who Can Create CUI ?

"Anyone can create CUI as long as it is generated for, or on behalf of, an Executive Branch agency under a contract and it falls into one of the over one hundred DOD CUI categories."

- DCSA FAQ

Identifying CUI

National Archives and Records Administration (NARA), Information Security Oversight Office (ISOO) as CUI Executive Agent for the CUI Registry.



ISOO Registry

- Is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice
- Includes a Category List, CUI Markings, Limited Dissemination Controls, Decontrol, and a Registry Change Log
- Provides Policy and Guidance and a Glossary

DoD Registry

- Is built on the ISOO Registry with the addition of the DOD issuance alignment
- Includes a breakout of other types of information which could meet the CUI threshold, particularly under the OPSEC category

Identifying CUI

ISOO Registry

- Within the ISOO CUI Registry, there are 125 total CUI categories divided into 20 index groupings
- Each CUI category is designated as either CUI-Basic or CUI-Specified
  - **CUI Basic** is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in DODI 5200.48 and the DOD CUI Registry.
  - **CUI Specified (SP)** is the subset of CUI in which the authorizing law, regulation, or governmentwide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The distinction is the underlying authority spells out the controls for CUI Specified (SP) information and does not for CUI Basic information.

DoD Registry

- Within the DoD CUI Registry there are four categories of Defense CUI
  - Controlled Technical Information
  - DoD Critical Infrastructure Security Information
  - Naval Nuclear Propulsion Information
  - Unclassified Controlled Nuclear Information – Defense

Controlled Technical Information

Export Controlled Information

ITAR

Identifying CUI

Controlled Technical Information

- Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- Technical Information means technical data or computer software, as those terms are defined in DFARS 252.227-7013, Rights in Technical Data - Noncommercial Items (48 CFR 252.227-7013).
  - Research and engineering data
  - Engineering drawings and associated lists
  - Specifications
  - Standards
  - Process sheets
  - Manuals
  - Technical reports
  - Technical orders
  - Catalog-item identifications
  - Data sets
  - Studies and analyses and related information
  - Computer software executable code and source code

CUI Is Easy to Identify. It's All Marked, right?

CUI is EITHER marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by, or on behalf of, DoD in support of the performance of the contract;

OR collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.

The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable handling requirements as described in the 32 CFR §2002, and the CUI Registry.

Not Marked ≠ Not CUI

COTS Products, Aren't They Exempt?

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

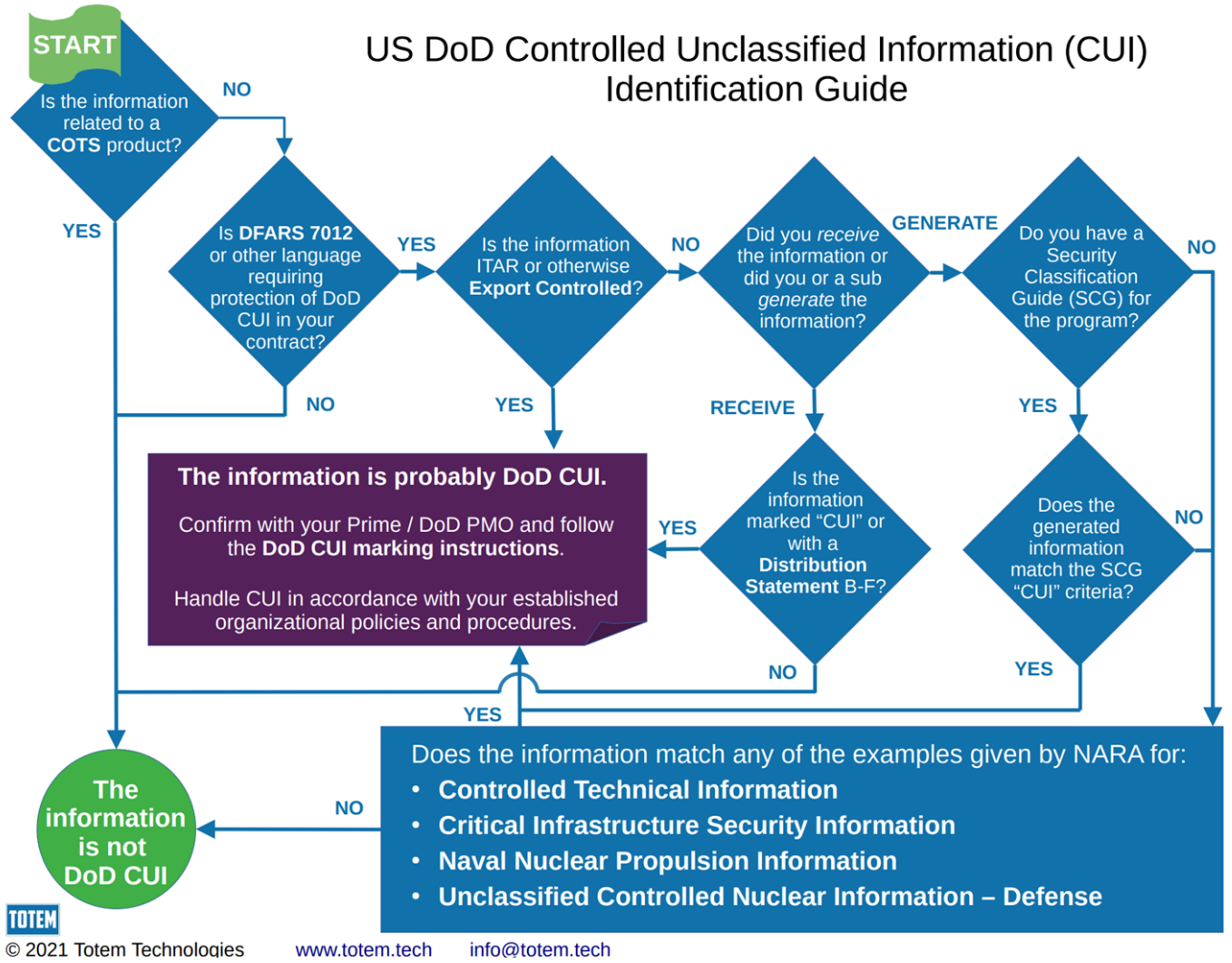
The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system..

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

Identifying CUI



So Why Is CUI Hard to Identify* ?

1. Vague contract details

   Even when you're talking to experts about whether a particular data type is CUI or not, the answer is often "probably" or "it depends." Context dependencies and other ambiguities enter in.

2. Pushing risk down the food chain

   Historically, contract clauses that direct the implementation of CUI protections have too often been "thrown into contracts" as a "CYA" effort. It's risk management for the government and/or the prime as they push the risk down.

3. "Better safe than sorry"

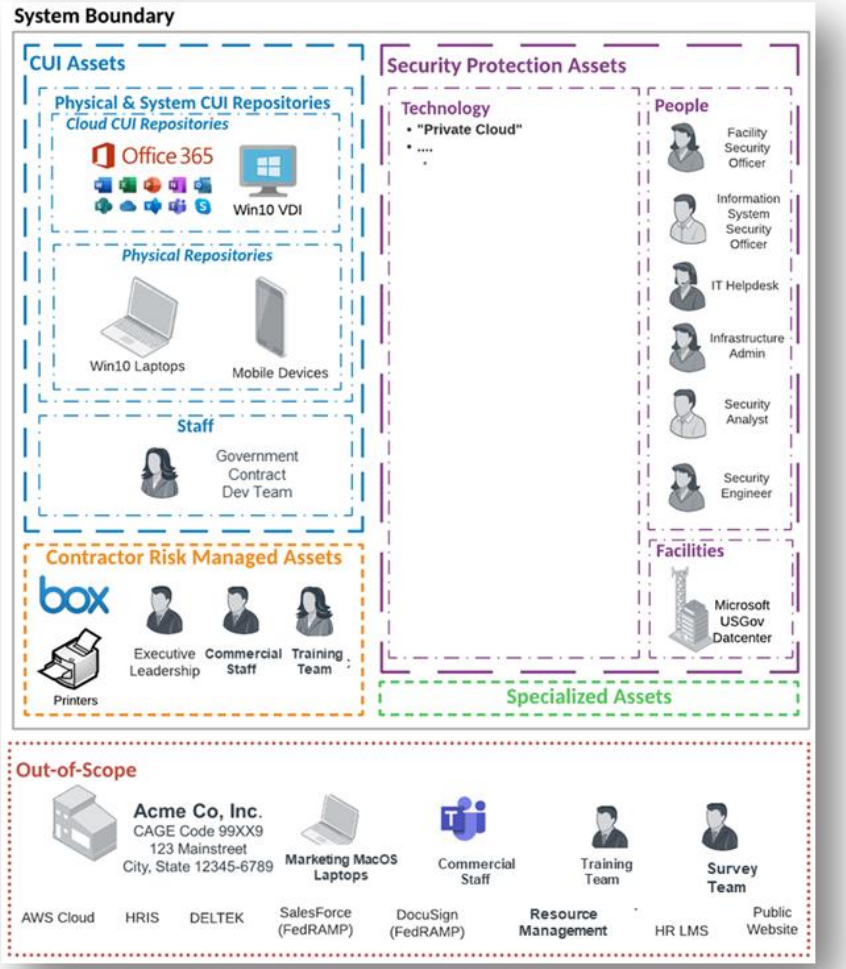
   With so much uncertainty across the board about CUI, what should you do if you're not sure? Is the default "treat it as CUI to be on the safe side"? Go to the prime or DoD first, especially in the case of data that you're receiving from upstream. If you can't get a definitive answer, dive into the CUI Registry online.

**3 Reasons Why It's So Hard to Identify CUI,* Pivot Point Security April 5, 2022, www.pivotpointsecurity.com/3-reasons-why-its-so-hard-to-identify-cui/

Establishing (or re-Establishing) Scope

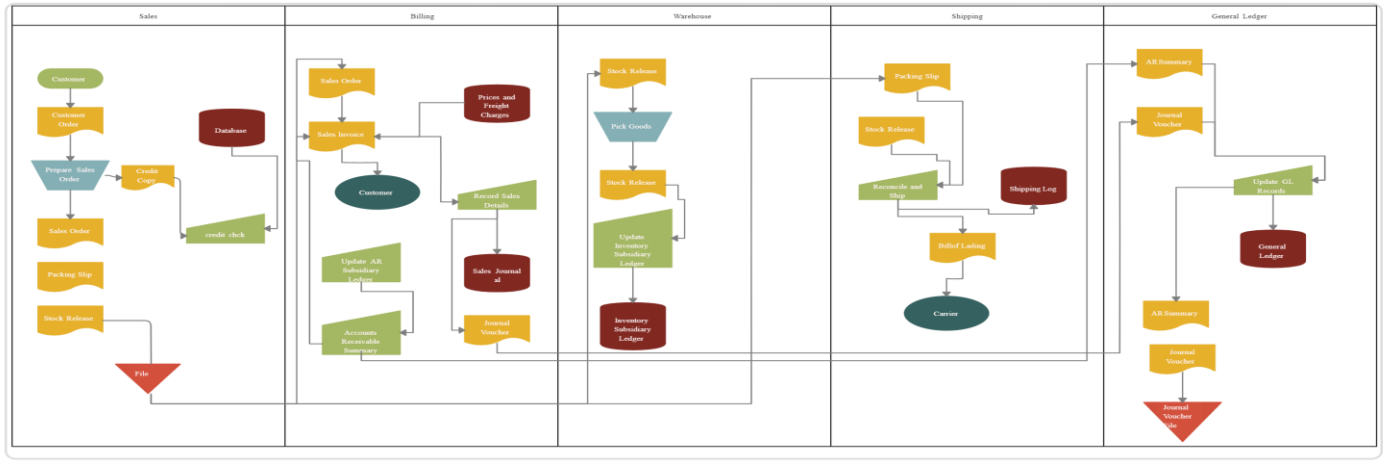
CUI Boundary

- Business processes drive where CUI exists
- 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
- Without adequate segmentation the enterprise environment is in scope



Defining Your CUI Boundary

Follow Each Business Process Associated With Fulfillment of Your DoD Contract



- Which organizations are involved?
  - Who specifically within each organization is involved?
- Where are those people located?
  - Geography
  - Facility
- What business applications/IT are used to support the process
- What special tooling or capital equipment is involved?
- Is any part of the process performed by a 3rd party?

Defining Your CUI Boundary: 3rd Parties

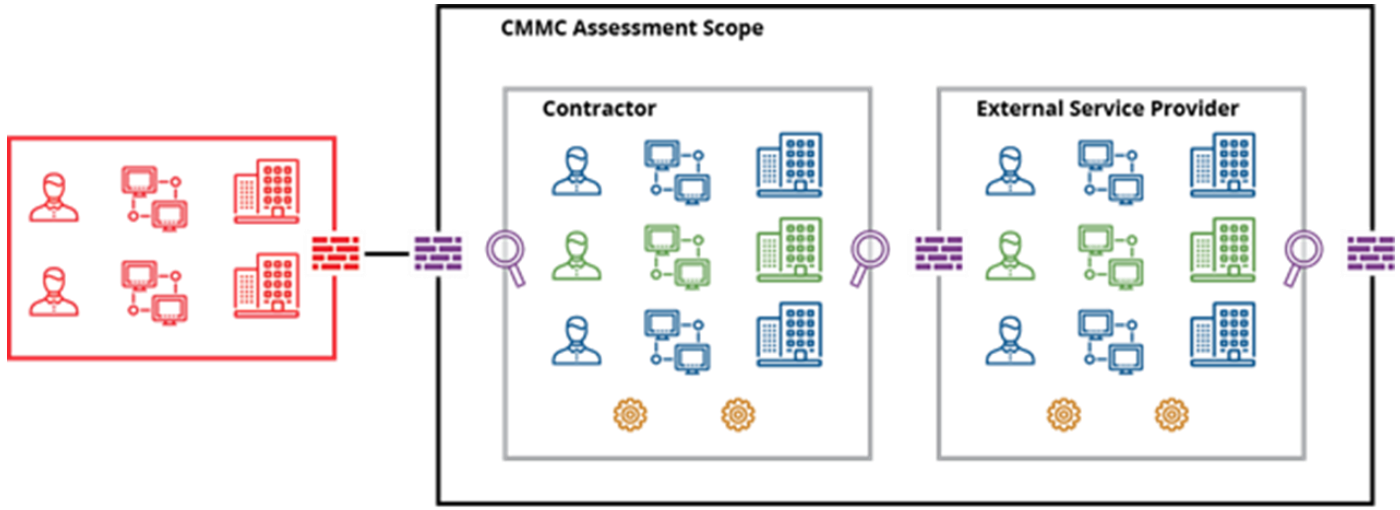
Cloud Services and Managed Services

- 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 NIST 800-171/CMMC

Establishing (or re-Establishing) Scope

In Establishing The CUI Boundary, you must inventory:

- CUI Assets
- Security Protection Assets
- Contractor Risk Managed Assets
- Specialized Assets
- Out-of-Scope Assets



Limiting Scope / Reducing the Boundary

- By separating assets, the CMMC Assessment Scope can be limited.
- Effective separation for CMMC follows the guidance in NIST SP 800-171 r2:

> *If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.*

Scenario 1: Handheld Computer Manufacturer

A COTS manufacturer of handheld data entry computers creates specialized versions of its products for DoD.

The DoD versions use hardened casing to meet MIL-STD 810 D and incorporate higher capacity batteries. Radiation and photo spectrometer sensors are also added per DoD specifications.

The manufacturer managed both DoD and commercial orders through the same processes and with the same people. One engineering group supported product engineering and customer applications engineering. Maintenance and break/fix for DoD and commercial products was supported by the same group. Salesforce, NetSuite, Jira, Confluence, and Solidworks were the primary design tools, Zendesk the primary support tool.

What CUI did they process, store, or transmit. What was their boundary?

Scenario 2: Audit Services Company

A professional services firm performs financial compliance audits for government contractors and for commercial organizations.

The GovCon audit team and commercial audit team are comprised of separate individuals, but the same tools are used by both. The compliance team has access to their client's CUI and the audit data are considered CUI.

What was their boundary? How did they reduce their boundary?

Scenario 3: Security Equipment Installer

A sub-contractor installs and maintains video surveillance and security sensors within DoD facilities.

Subcontractor personnel use tablet computers provided by the prime contractor to display blueprints, schematics and installation instructions.

Printing is not allowed from the table computers and the tablet computers can only access information when in a geofence and only during specific hours.

Does DFARS 252.204-7012 need to be flowed down to the subcontractor? What is the contractor's boundary?

Summary: Step 1

- The CMMC journey starts by knowing what you need to protect
  - Identifying the CUI you received
  - Identifying the CUI you create

  This should be easy, but it's not
- Business processes define where CUI exists, how it flows through your organization
  - People
  - Processes
  - Facilities
  - Information Technology

  This defines scope or your CUI boundary
- Segmentation or isolation can be used to reduce your CUI boundary
- Don't Minimize Step 1

For More Information:

www.NeoSystemsCorp.com
Stuart,Itkin@NeoSystemsCorp.com