MICHIGAN
MANUFACTURING
TECHNOLOGY
CENTER

MANUFACTURE SMARTER

Navigating Unclassified Cyber/Information Security Protections

MICHIGAN
MANUFACTURING
TECHNOLOGY
CENTER

MANUFACTURE SMARTER

ABOUT US...

We are…

- Dedicated to Michigan manufacturers
- Experts who live and breathe manufacturing
    - Resources to work smarter, compete and prosper
- Champions for them every day

This is what drive us. This is why we exist.

MEDC
MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

NIST

the-center.org

888.414.6682

OUR SERVICES

- CYBERSECURITY
- GROWTH
- OPERATIONAL EXCELLENCE
- LEADERSHIP DEVELOPMENT
- SKILL DEVELOPMENT
- ACCELERATING TECHNOLOGY
- RESEARCH SERVICES
- FOOD PROCESSING

MICHIGAN MANUFACTURING TECHNOLOGY CENTER

MANUFACTURE SMARTER

RESULTS DEMONSTRATED

During the past 12 months, **377** of our Michigan clients have seen…

EVERY **$1** SPENT WITH THE CENTER RETURNS
$106 BACK IN FINANCIAL IMPROVEMENTS.

WHEN WE THINK OF THIEVES…


EQUIFAX


31001

歼-31

F-35

The New “Normal”


Continue to Evolve

SECURITY ENVIRONMENT - THE BURNING PLATFORM

National Security

U.S. competitive technological advantage

*the FBI estimates that **$400 billion** of IP is leaving the US each year because of cyber-attacks*

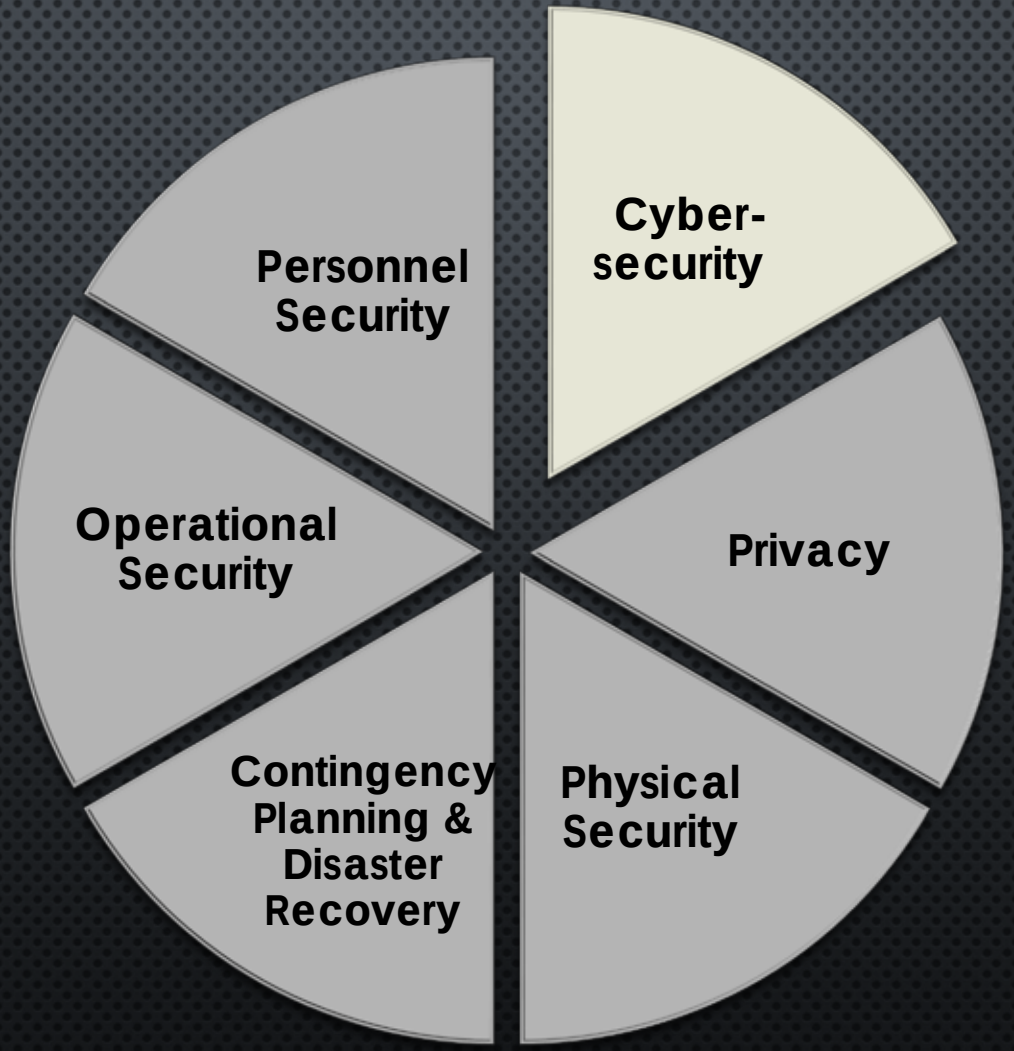
3 TAKE-AWAYS

1. CYBER THREAT

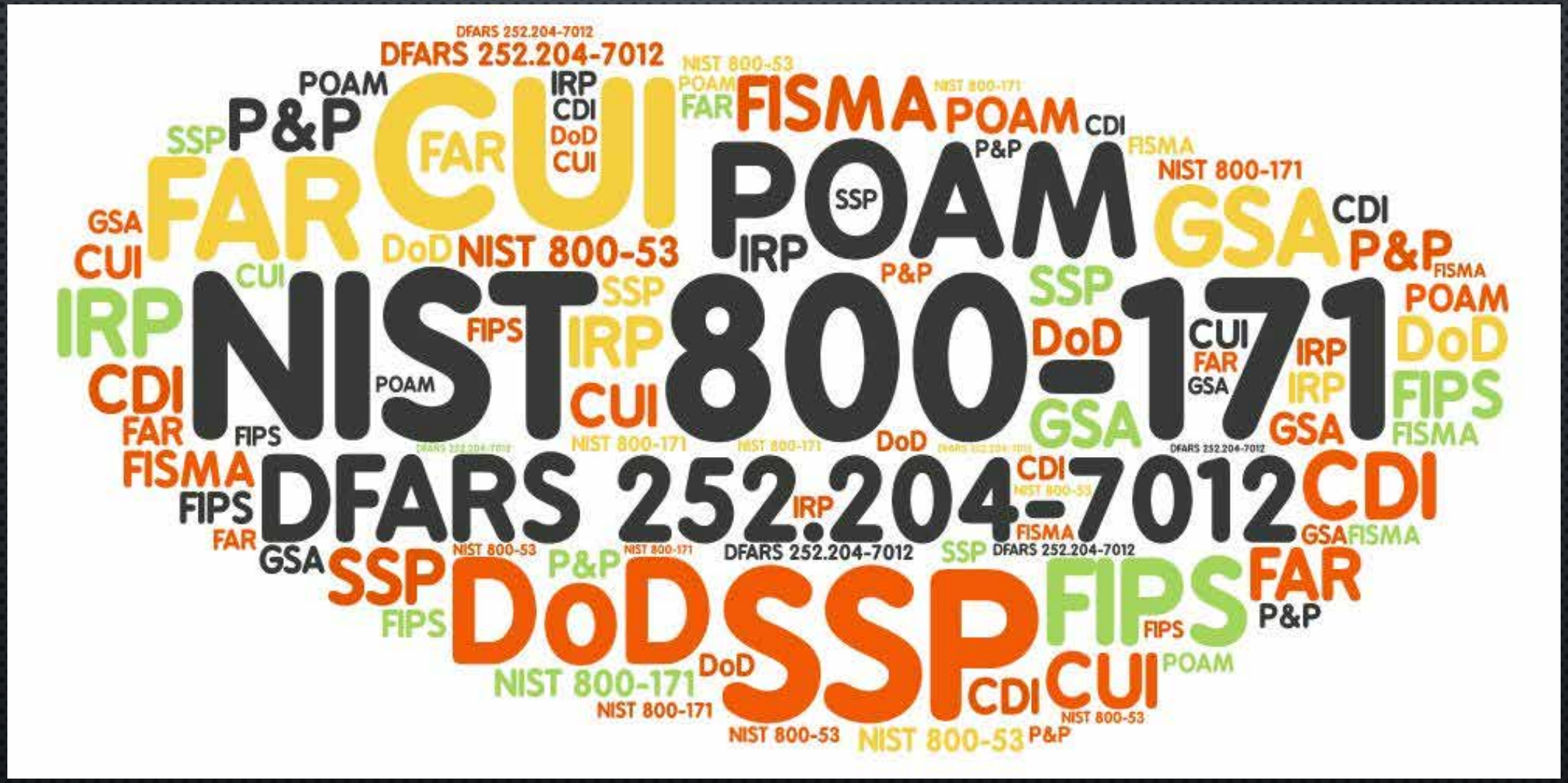
2. FAR/DFARS REQUIREMENTS

3. SUPPLY CHAIN IMPLICATIONS

WHAT IS INFORMATION SECURITY?



Confusing Alphabet Soup



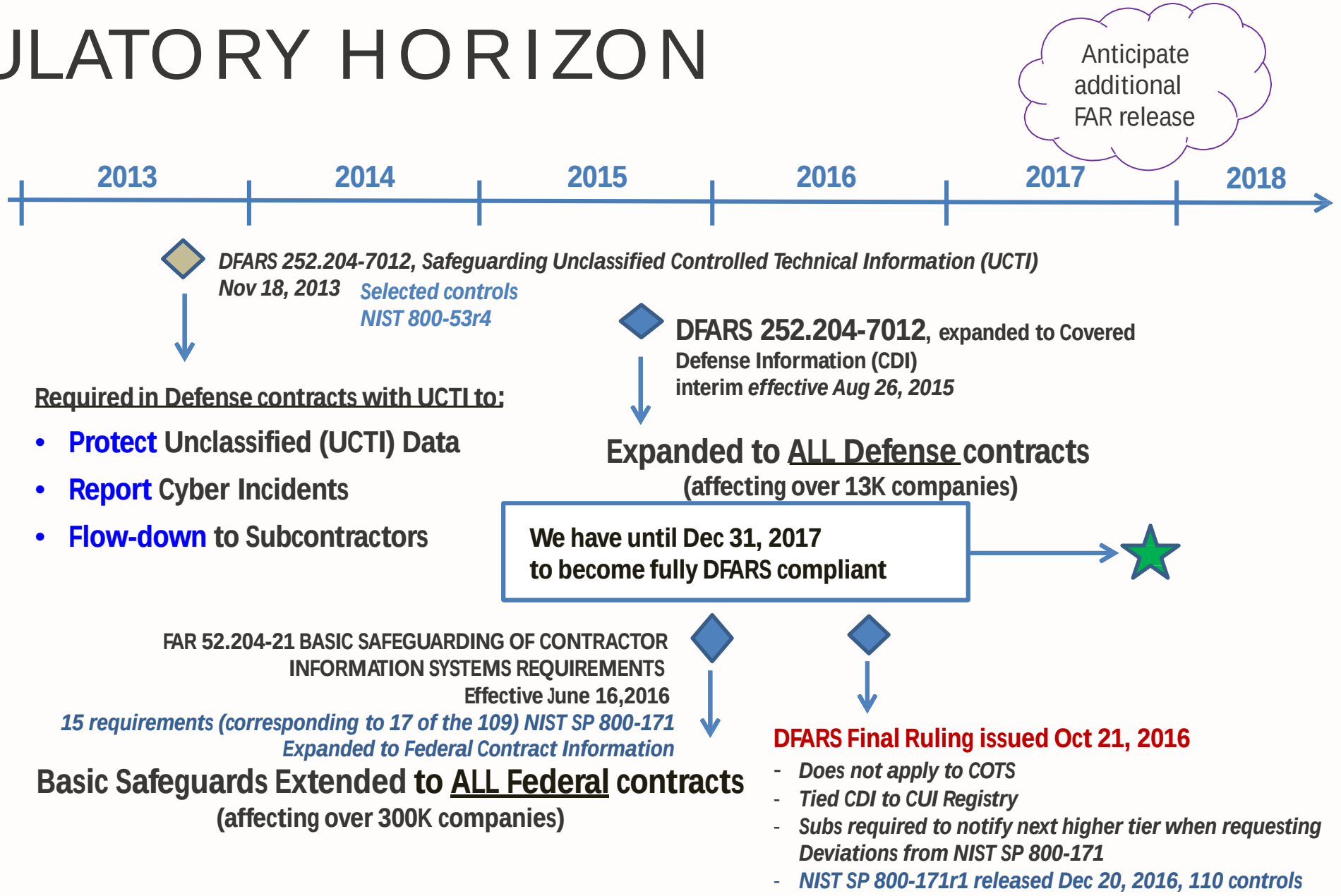
WHAT IS THE FAR / DFARS?

- Federal
- Acquisition
- Regulation

- Defense
- Federal
- Acquisition
- Regulations
- System


Fine print

REGULATORY HORIZON



FAR 52.204-21

BASIC SAFEGUARDING OF CONTRACTOR INFORMATION SYSTEMS REQUIREMENTS

- Final **FAR** rule published May 16, 2016 **effective June 15, 2016**
- Applies to all federal contracts and subcontracts at **any tier** (except those for COTS products) and requires basic safeguarding of contractor systems that contain ***Federal Contract Information***
  - *Information, not intended for public release, provided by or generated for the Government, but not public information or transactional information, such as that necessary to process payments.*
- Mandatory flowdown at all tiers
- Imposes 15 requirements that correlate to **NIST 800-171** security controls (limited subset)
- No incident reporting requirement

DFARS CLAUSE 252.204-7012

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

- Must provide adequate security for covered contractor (internal) systems with Covered Defense Information **(CDI)**
  - At a minimum must comply with **all NIST 800-171 security controls** as soon as practical but **not later than *December 31, 2017***
  - For contracts awarded through 9/30/17, submit a report NLT 30 days after contract award to DoD-CIO listing controls not fully implemented at time of award

This is a self assessment/attestation
(no certification authority exists and won't be considered by the DoD)

DFARS CLAUSE 252.204-7012 (CONTINUED)

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

- In addition to 110 security controls, contractors and subcontractors ***must report cyber incidents on covered contractor information systems*** with CDI, or that affects the contractor's ability to perform operationally critical support under a contract
  - Upon discovery must conduct a review for evidence of compromise
  - Rapidly report within 72 hours directly to DoD via specified online portal
  - Must provide DoD-assigned incident report number to prime/higher tiered subcontractor
  - Must preserve and protect images of known affected images and systems for 90 days
  - Must provide DoD access to additional information or equipment necessary to conduct forensics analysis

CYBER INCIDENT REPORTING

- Contractors are required to rapidly report cyber incident directly to DoD at http://dibnet.dod.mil.
- A medium assurance certificate is required to access the reporting module.
- When the contractor completes the online form and submits the report, the DoD Cyber Crime Center (DC3) receives the report. DC3 sends an unclassified encrypted email to the contracting officer with the reported information.
- DC3 is the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DoD contractors.

NETWORK PENETRATION REPORTING - DAMAGE ASSESSMENT

DFARS 252.204-7012 (g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered.

Purpose of damage assessment:

- **To understand impact of compromised information on U.S. military capability underpinned by technology**
- **Initiated after review of reported cyber incident**
- **Focused on determining impact of compromised intellectual property, not on mechanism of cyber intrusion**
- **An assessment is not possible without access to compromised material**

KEY CHANGES IN OCTOBER 2016 FINAL RULE

- Expands the definition of CDI, including items required on the CUI Registry
- **COTS** exemption (does not extend to commercial items)
- Clarifies the definition of “operationally critical support”
- Contemplates that primes and higher tiered subcontractors may consult with contracting officer for guidance as to whether the clause needs to be flowed down
- Subs are required to notify higher tiered subcontractor or prime of requests for alternative but equally effective solutions
- Incident report ID Numbers must be provided to next higher tier subcontractor or prime
- Contracts signed after 9/30/17 do not require a 30 day notice submittal

WHAT IS “COVERED DEFENSE INFORMATION”?

Covered Defense Information (CDI) is ***unclassified information*** that:

- Is provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or
- Is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract, and
- Falls within the four categories:
  - Controlled Technical Information
  - Critical Information
  - Export Controlled Information
  - Other information that requires safeguarding or dissemination controls

Unclassified and used in support of contract with DFARS clause

THE 4 CATEGORIES OF CDI

Controlled Technical Information

- Technical information subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination
- Distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents.

Critical Information

- Operations Security Process
- Friendly intentions, capabilities, and activities needed by adversaries to guarantee failure or unacceptable consequences for friendly mission

Export Control

- Unclassified information whose export could reasonably affect national security and nonproliferation objectives
- Includes: Dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

Other

- Other Information identified in the contract, that requires safeguarding or dissemination controls (e.g., privacy, proprietary business information)

EXAMPLES OF POSSIBLE CDI

- 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

HOW TO PROTECT CDI?

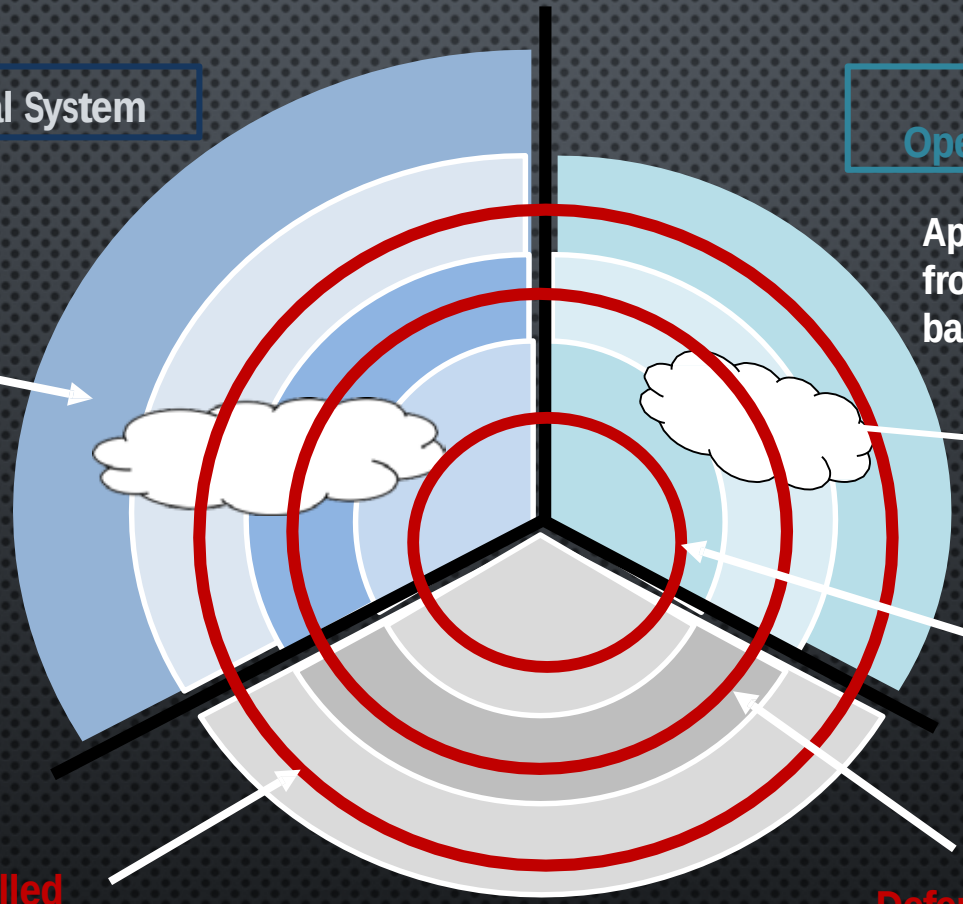

ellen

WHAT IS “ADEQUATE SECURITY”?

- “Adequate Security” means meeting the NIST 800-171 security controls
- Defense contractors have until December 31, 2017 for full compliance to the NIST 800-171 controls
- NIST 800-171 imposes 110 Controls under 14 “families” of basic & derived security requirements
- Requirement for contractors to report (to the DoD-CIO not the PCO) any current areas of non-compliance *within 30 days of contract award*

Navigating Unclassified Information (System) Security Protections

Elements that drive appropriate protections: The information system and the information



Contractor's Internal System

Applicable controls:
NIST SP 800-171

Contractor System Operated on DoD's Behalf

Applicable controls:
from CNSSI 1253,
based on NIST SP 800-53

Federal Contract Information

Cloud Service Provider

Applicable controls:
From the SRG

Unclassified Controlled Technical Information

Covered Defense Information

Controlled Unclassified Information (USG-wide)

DoD Information System

Applicable controls:
From CNSSI 1253, based on NIST SP 800-53

Supply Chain Responsibilities

FLOW-DOWN TO SUBCONTRACTORS/SUPPLIERS

- **Contractor will include clause in solicitations, POs and Subcontracts**
  - Include this clause in all POs supporting all DFARS-applicable contracts
  - Clause is ‘self-deleting’ if subcontractor/supplier’s system does not meet the definition of “covered contractor information system”
  - *COTS Suppliers are exempted from Oct. 2016 final rule- at solicitation, not applicable to flow-down- (not verified by DoD)*
- **Specifically applies to subcontractors who**
  - Provide “operationally critical support”, and/or whose
  - Work involves “covered contractor information systems”

FLOW-DOWN TO SUBCONTRACTORS, SUPPLIERS

- **Requires subcontractors subject to the clause to meet NIST 800-171:**
  - DFARS obligation ends with flowing this clause to Subcontractor
  - Onus is on the Subcontractor to comply
- **Contractor accountability to ensure supply base compliance**
  - Receive assurances of self assessment compliance
  - Means to validate
    - √ System Security Plan
    - √ Incident Response Plan
    - √ PoAM (not compliant but implementing)
- § **Always have provision to audit**

ENGAGE YOUR BUSINESS - *WHAT NEED TO DO?*

- **Start now (if you haven't already)**
- **Read the FAR, DFARS and NIST SP 800-171r1**
- **Work across functions**
  - *IT, Info Security, Contracts, Supply Chain, HR, Engineering, Quality*
- **Designate Business Point of Contact**
  - *Coordinate collection of existing practices, tools, standards*
  - *Map systems architecture and CDI data flow*
  - *Lead cross-org analysis of requirements, gaps in compliance, review of new standards*
- **Understand what CDI AND Federal Contract Information is associated with your contract and what systems it applies to**
  - *Evaluate "covered contractor information system" use, risk, and impact*
    - Which unclassified systems, what data, and who's managing it (various roles)
    - Integrate with Risk Management
  - *Identify CDI and DFARS use cases, so that*
    - Your new standards are compliant and support the business
    - Employees know their role(s) and responsibilities

BUSINESS IMPLICATIONS

COMPLIANT

VS.

IMPLEMENTING

SUMMARY

- Protecting your business is not an option
- Continuously monitor / remove vulnerabilities
- Understand the Regulations are intertwined
- Our National Defense is at stake

QUESTIONS?