DFARS 252.204-7012, NIST 800-171, CDI

… and You

referentia

UNIVERSITY OF HAWAI'I
UA MAU KE EA O KA 'ĀINA I KA PONO
1907

- Overview
- Impacts
- Getting started

- **Overview**
- Impacts
- Getting started

Overview & Evolving Requirements

DFARS 252.204-7012 - "Safeguarding Covered Defense Information and Cyber Incident Reporting"

- **November 2013:**
  - "Unclassified Controlled Technical Information"
  - 50+ controls from NIST 800-53
- **August 2015:**
  - New DFARS 252.204-7012 rules - CDI, NIST 800-171
- **October 2015:**
  - Targeted Class Deviation for (multifactor authentication)
- **December 2015:**
  - Industry feedback: high standards and big impact
  - *Interim* update: reporting of non-implemented controls, Dec 2017 deadline
- **Future**
  - Inclusive FAR update

Protect Covered Defense Info (CDI)

CDI is unclassified information that is

- (A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract
- (B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

And falls in any of the following categories:

- Controlled Technical Information
- Critical information (operations security).
- Export control (including ITAR)
- Identified in the contract as requiring safeguarding
  - e.g. privacy, proprietary business information

DFARS 252.204-7012.a.i and .ii

- Overview
- **Impacts**
- Getting started

Changes – 2015 Expanded Requirements

- Data Covered
  - Was: protecting unclassified technical controlled information
  - Now: protecting **covered defense information**
- Controls Required
  - Was: over 50 NIST 800-53 security controls
  - Now: **109 NIST 800-171 requirements**
- Security Solution Reporting
  - Was: no security solution reporting requirement
  - Now: **report un-implemented security solutions** within 30 days of contract award, **complete NIST 800-171 before 2018**

DFARS 252.204-7012 Incident Response Requirements

- Incidents must be reported to DoD within 72 hours of discovery
- Identify, isolate, and provide a copy of the malicious software in accordance with instructions by the Contracting Officer
- Preserve and protect images of all known affected information systems and all relevant monitoring/packet data must be retained for at least 90 days.
- Report incidents to prime contractor or next higher sub-contractor
- ... review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, **as well as other information systems on the Contractor's network(s)**...

NIST 800-171 Scope

14 families of controls with 109 requirements

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical Protection
- Personnel Security
- Risk Assessment
- Security Assessment
- Systems and Communications Protection
- System and Information Integrity

Maps to over 180 NIST 800-53 security controls

NIST 800-171 Gotcha!

NIST 800-171 identifies some controls as "*Expected to be routinely satisfied by nonfederal organizations* ***without specification***"

- Policies and Procedures
- **Continuous Monitoring**
- Plans (CM/IR/SSP)
- 3rd Party Personnel
- Security Flow Downs
- Secure DNS

BEFORE PURSUING GOV'T CONTRACTS

Know Your NIST 800-171 Status

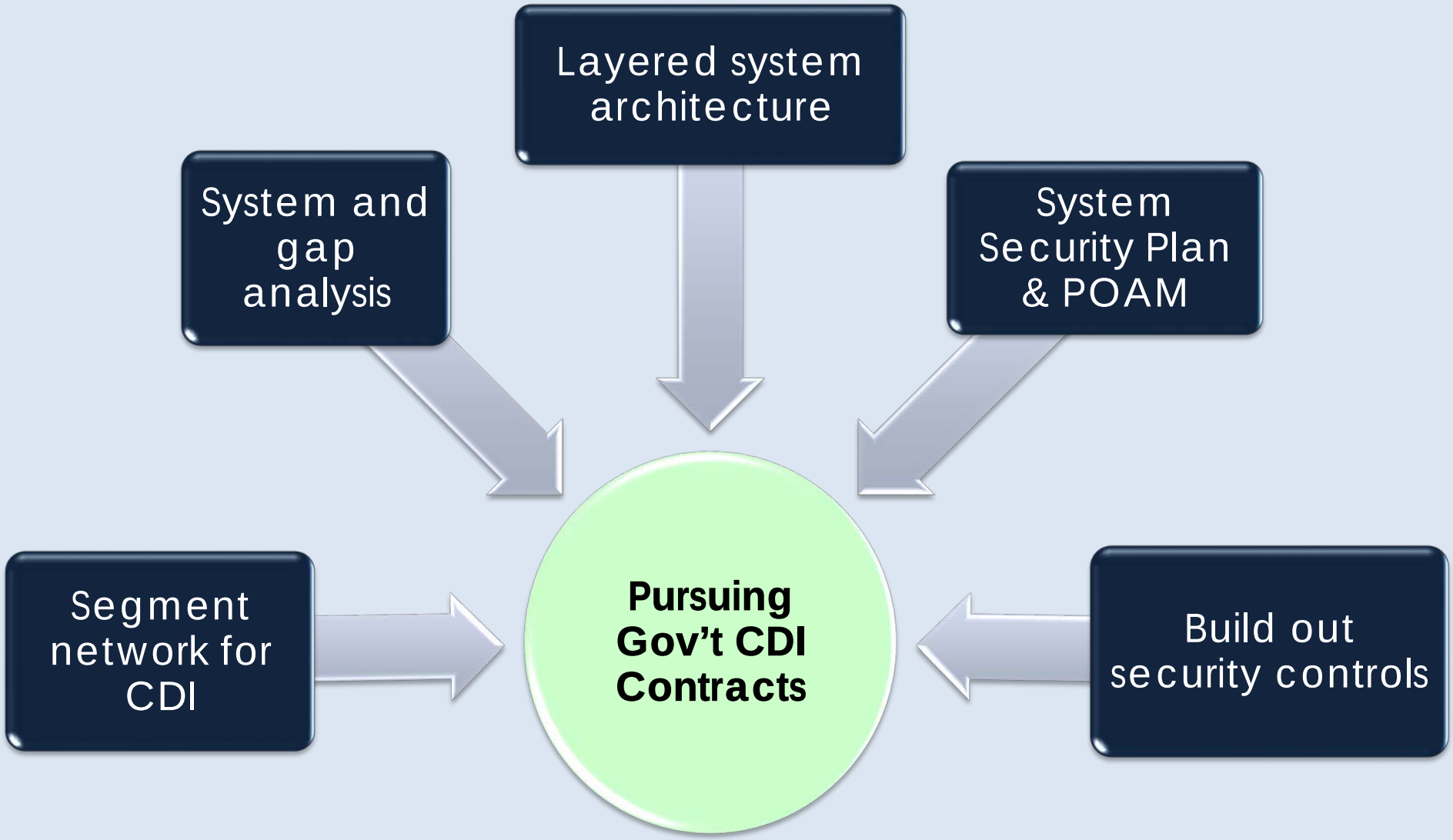
- You **must identify** NIST 800-171 requirements not yet implemented at contract start
  - "notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award"

DFARS 252.204-7012.b.1.ii.A

- Assess where you are and establish a plan to **finish**
  - You **must meet** NIST 800-171 requirements before December 31, 2017
  - There are a lot of requirements to meet
- Proposed deviations from 800-171 need to be approved by authorized DoD CIO representative
- Part of 800-171 requirements is creating and implementing a Plan of Actions

- Overview
- Impacts
- **Getting started**

Suggested Path to Meet Requirements



Questions

For more information please contact David Tribble at dtribble@referentia.com or refinfo@referentia.com