CMTC

Santa Clarita Valley Economic Development Corporation

Secure and Resilient

Oct 19, 2017

Chris Buthe
Manager of Delivery Resources,
and Cyber Physical Security Services

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

“It is hard to know what I can do about Cyber ?

→ What should I do ?

→ What must I do ?

→ When ?

→ Can you make it more simple ?

→ How do I evaluate Cyber Providers ?

→ What does it cost ?

© 2017 CMTC all rights reserved

Topics

Partners

Lessons Learned from Cyber Incidents

DFARS 252.204-7012 and NIST SP800-171

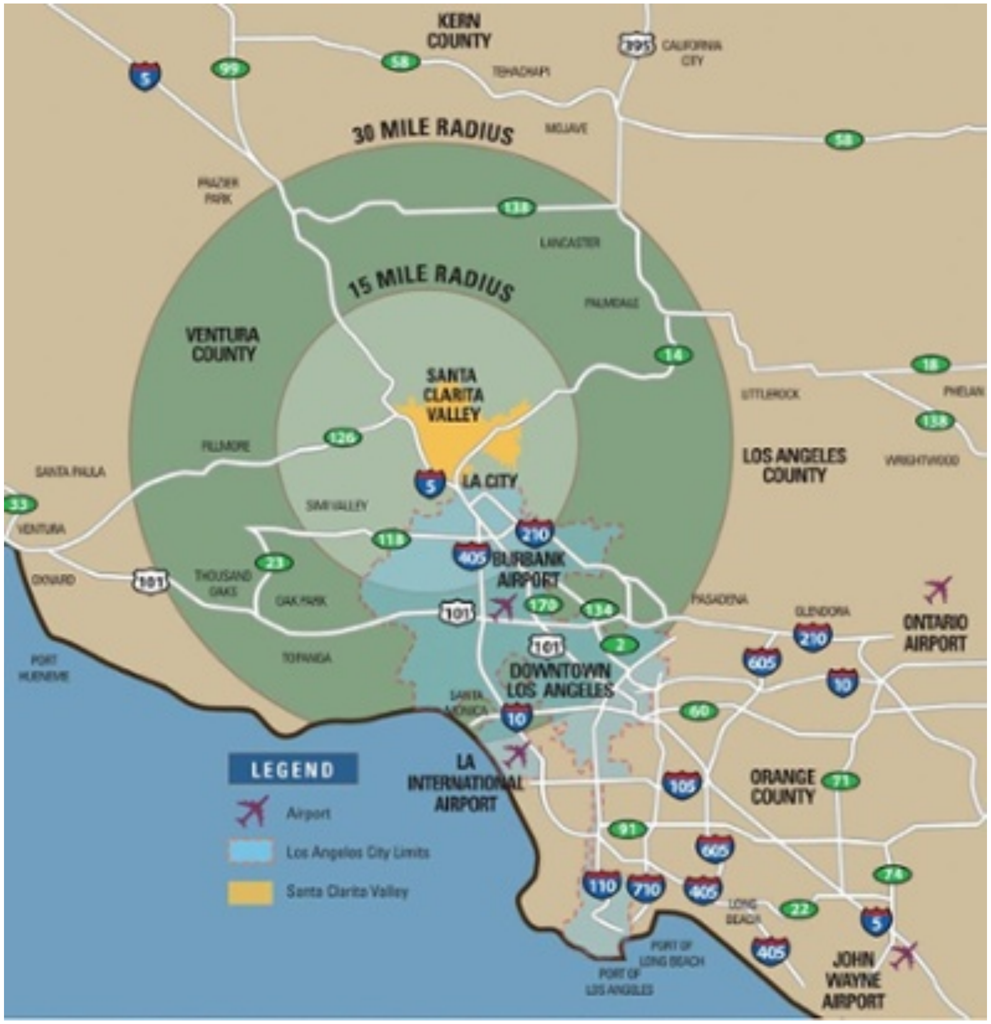
Self-Attestation

Security & Compliance Roadmap

Resources

© 2017 CMTC all rights reserved

Santa Clarita Valley
Economic Development Corporation



Map Courtesy of SCVEDC

Business Attraction

Growth

Security

Aerospace & Defense Coalition

CMTC®

California's Manufacturing Resource

© 2017 CMTC all rights reserved

CMTC U.S. Manufacturing Cybersecurity

U.S. Department of Commerce

National Institute of Standards & Technology

Manufacturing Extension Partnership (MEP)

CMTC 1 of 51 MEP Centers in the U.S.

CMTC®

California's Manufacturing Resource

© 2017 CMTC all rights reserved

CMTC Strategic Partners on Cybersecurity

Homeland Security

Department of Homeland Security

ICS-CERT VLP
VIRTUAL LEARNING PORTAL

Industrial Control Systems

Computer Emergency Response Teams

DAU

Defense Acquisition University

NDIA

Cybersecurity for
Advanced Manufacturing

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

FORTUNE

Equifax Breach

Sept 20, 2017

What: *“145.5 million consumer records”*

When: *Breached in May 2017 - - - Reported Sept 2017*

Why: *Slow patching of new known vulnerability*

Insufficient detection or reaction

How: *Detection +78 days, Reporting +39 days.*

Results: *“extensive and extreme”*

© 2017 CMTC all rights reserved

Australian Defense Breach

Oct 12, 2017

What: *"Sensitive but Unclassified"*

When: *Breached in July 2016 - - - - Reported Nov 2016*

Why: *Contractor did not update software*

Contractor did not update passwords

How: *Methodical, slow, deliberate*

Results: *"extensive and extreme"*

California's Manufacturing Resource

© 2017 CMTC all rights reserved

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

Controls as prescribed in the NIST SP800-171

Adequate security that safeguards:

Controlled Unclassified Information

Controlled Technical Information

Controlled Defense Information

Cyber Incident Reporting

© 2017 CMTC all rights reserved

What does compliance include ?

DFARS Compliance includes

→ Completing a self-assessment, and a Security Plan

→ Achieving 100% by December 31, 2017

→ Having an Incident Reporting Plan

Non Compliance includes

→ Corrective Action Report

→ Breach of Contract

→ Legal Liability

© 2017 CMTC all rights reserved

What does DoD want to see ?

DFARS documentation includes:

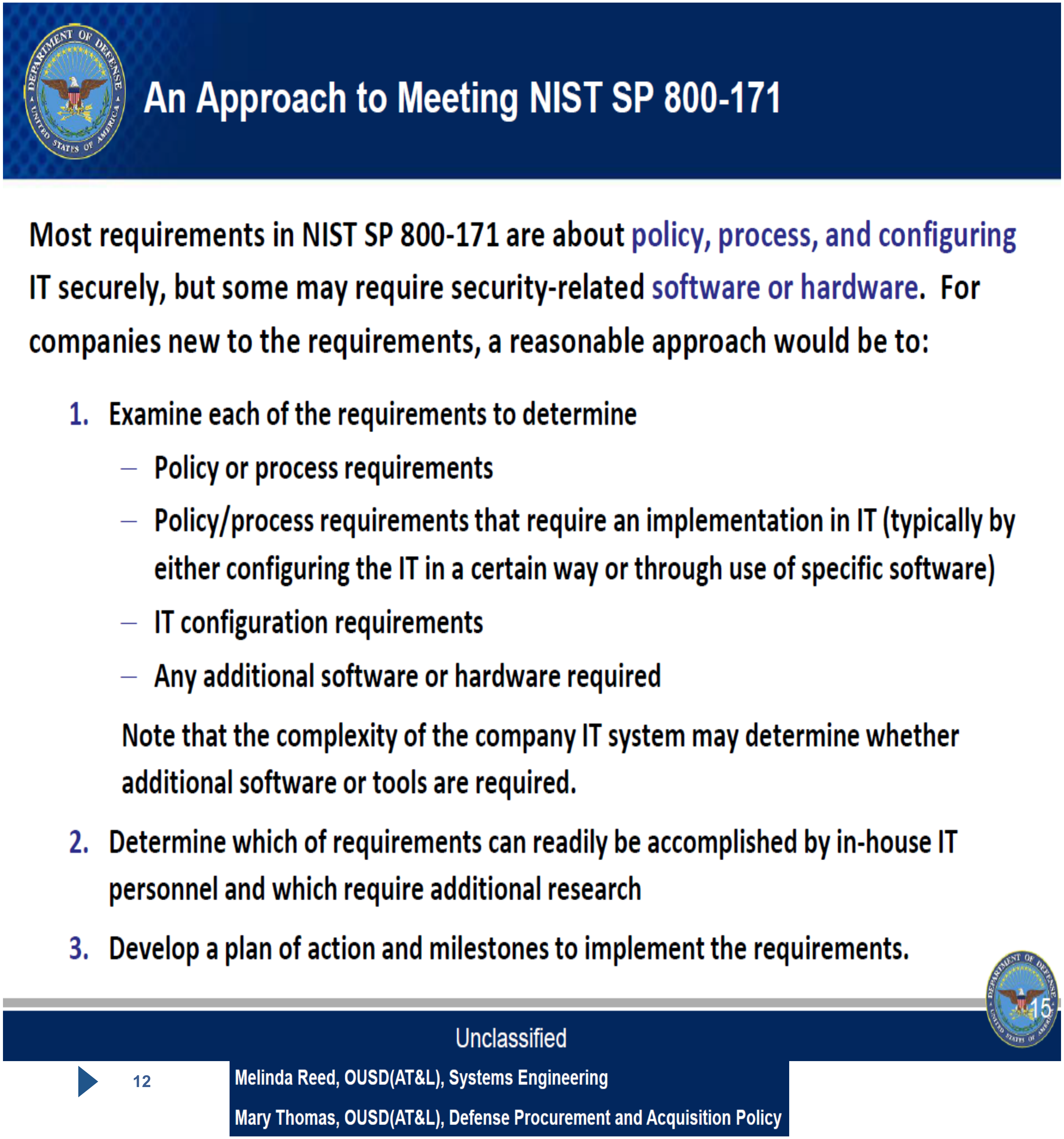
→ Your Self-Attestation

→ Systems Security Plan

→ Plan of Action & Milestones

→ Incident Reporting Plan

© 2017 CMTC all rights reserved



An Approach to Meeting NIST SP 800-171

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware. For companies new to the requirements, a reasonable approach would be to:

1. Examine each of the requirements to determine
   - Policy or process requirements
   - Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)
   - IT configuration requirements
   - Any additional software or hardware required

   Note that the complexity of the company IT system may determine whether additional software or tools are required.
2. Determine which of requirements can readily be accomplished by in-house IT personnel and which require additional research
3. Develop a plan of action and milestones to implement the requirements.

Unclassified

Melinda Reed, OUSD(AT&L), Systems Engineering

Mary Thomas, OUSD(AT&L), Defense Procurement and Acquisition Policy

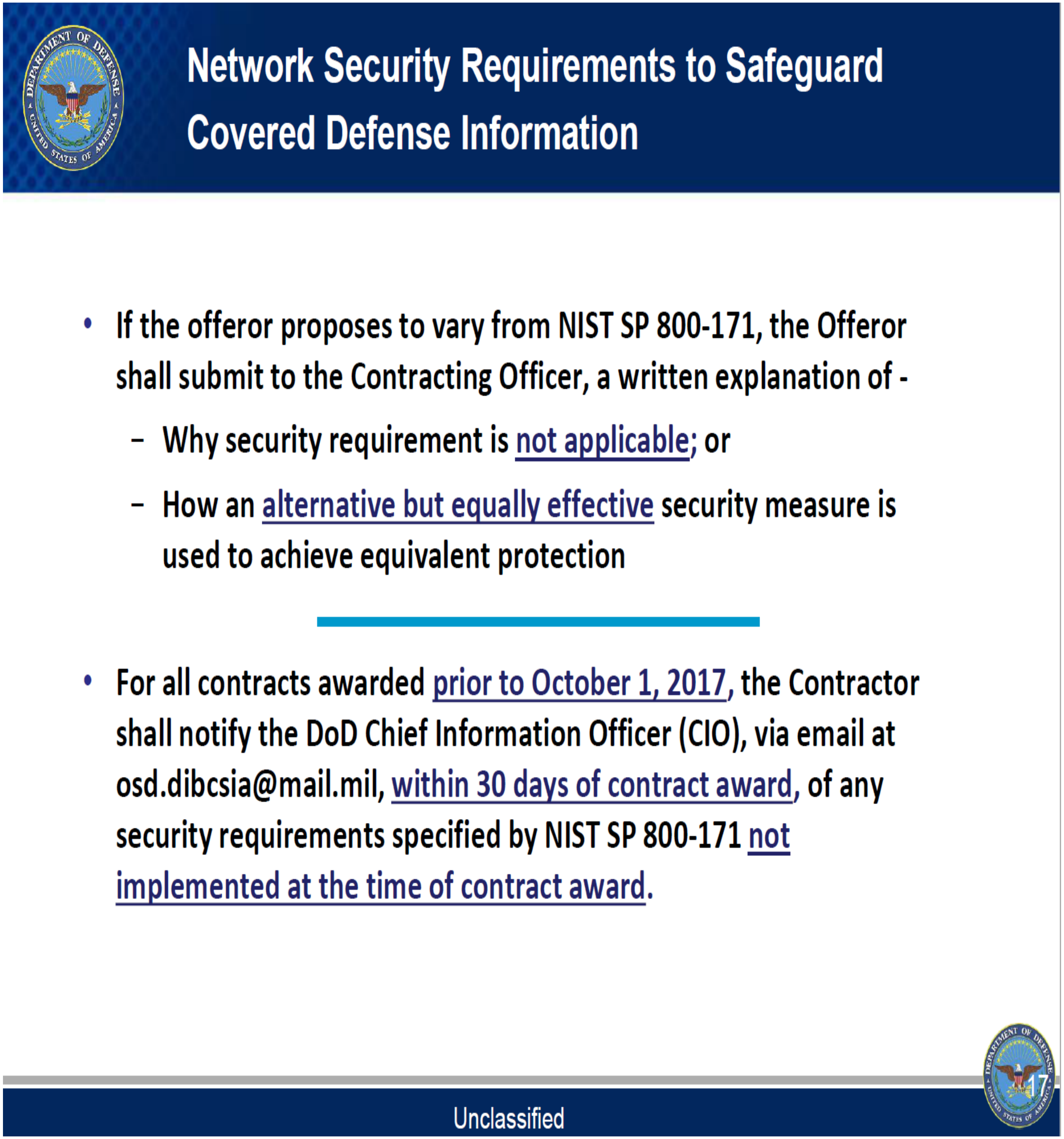
POA&M

Plan of Actions & Milestones

SSP

Systems Security Plan

CMTC®
California's Manufacturing Resource
© 2017 CMTC all rights reserved



Network Security Requirements to Safeguard Covered Defense Information

- If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, a written explanation of -
  - Why security requirement is not applicable; or
  - How an alternative but equally effective security measure is used to achieve equivalent protection

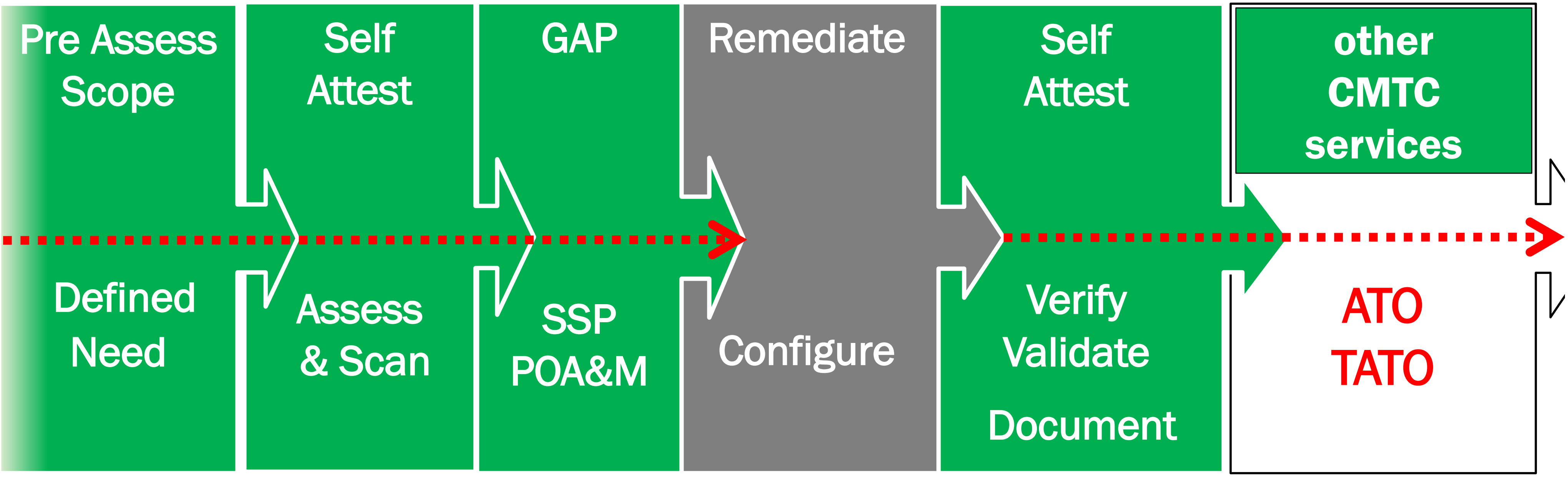
- For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

Contracting Officer

CIO

CMTC®
California's Manufacturing Resource
© 2017 CMTC all rights reserved

Security & Compliance Roadmap



Pre Assess Scope

Defined Need

Self Attest

Assess & Scan

GAP

SSP POA&M

Remediate

Configure

Self Attest

Verify Validate

Document

other CMTC services

ATO TATO

Color LEGEND
CMTC
Remediator
Client

SSP
Systems Security Plan

POA&M
Plan of Actions & Milestones

ATO
Authorization to Operate

ATO
Temporary Authorization to Operate

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

5 Questions to Ask

1. What is in your interest ?
2. What do you need to protect ?
3. Who are your customers ?
4. How many employees and devices ?
5. What systems do you have ?

© 2017 CMTC all rights reserved

Questions to Ask Ourselves

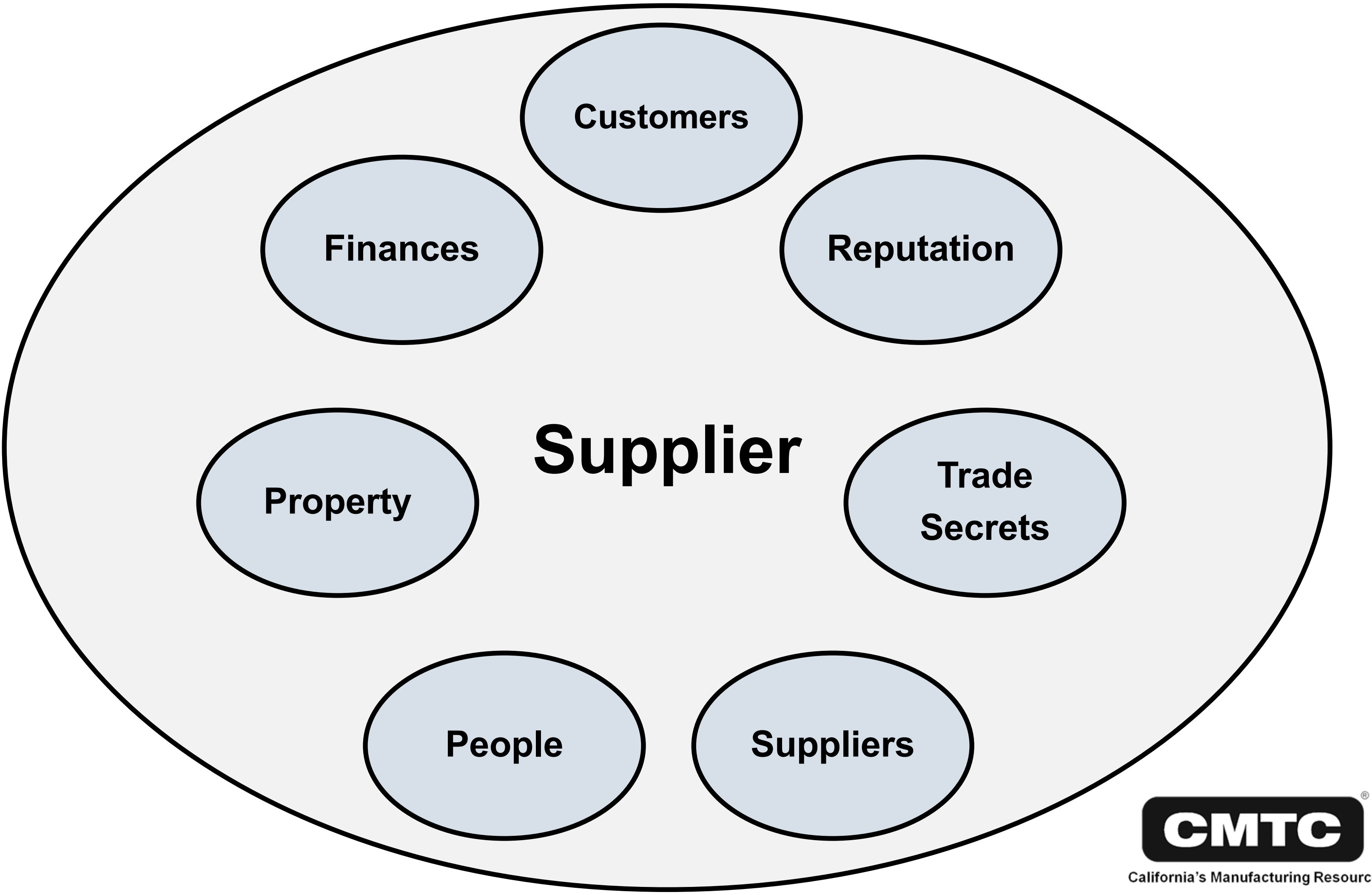
1. What is in your interest ?

Intrusion (known)	Financial & Legal	Reactive
Attack (known-unknown)	Threat	Reactive
Suspicion (unknown-known)	Financial	Reactive
Compliance - regulations	Legal	Reactive
Compliance - requirements	Customers	Reactive
Growth Strategy	Competitive	Proactive
Resilience	Thrive	Proactive

© 2017 CMTC all rights reserved

Questions to Ask Ourselves

2. What do you need to protect ?



CMTC
California's Manufacturing Resource

© 2017 CMTC all rights reserved

Questions to Ask Ourselves

3. Who are your customers ?

Department of Defense

DoD Suppliers

Federal Customers (GSA NASA DOE)

Automotive Industry

Food Industry

Medical Industry

© 2017 CMTC all rights reserved

Questions to Ask Ourselves

4. How many employees ?

   below 49 employees

   50-100

   101-200

   201-300

   301-400

   401-500

How many devices ?

3 to 5 times the employee count

CMTC®

California's Manufacturing Resource

© 2017 CMTC all rights reserved

Questions to Ask Ourselves

5. What systems do the you have ?

IT processing

Storage

Transmission

Cloud

IoT

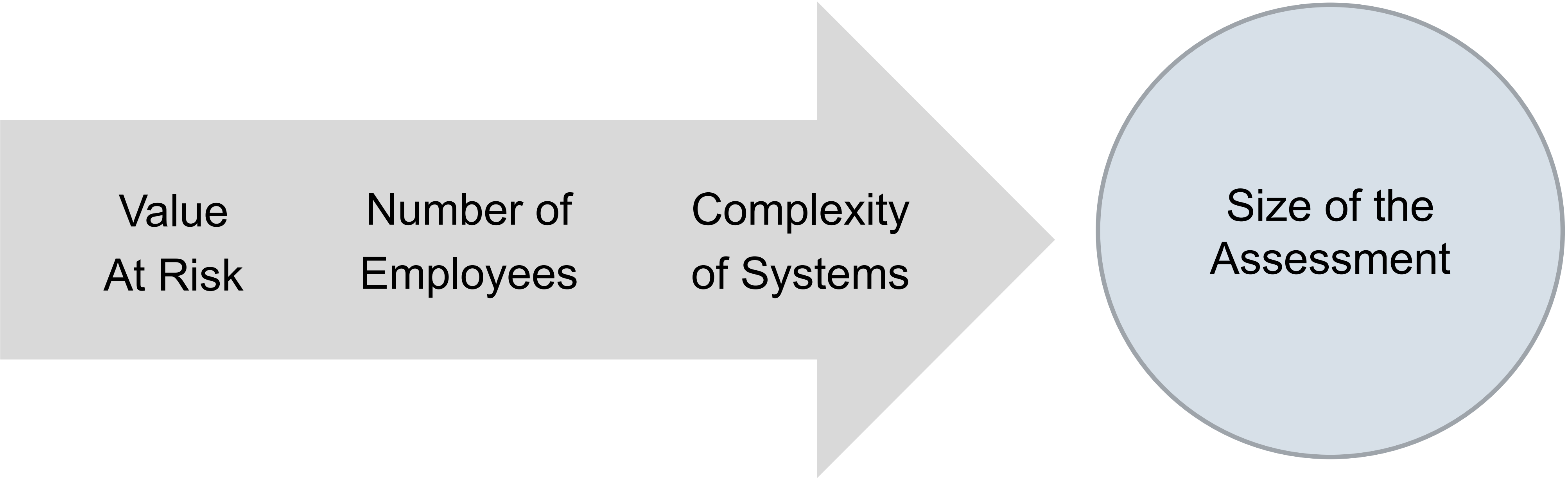
APPs

Operational Technology

Industrial Control Systems

© 2017 CMTC all rights reserved

Pre-Assessment



© 2017 CMTC all rights reserved

Cyber Assessment Market Pricing

Example: Small Manufacturer

100 employees, 400 IP addresses, IT, IoT, little Operational Tech

Compliance Assessment, Monitor, Detect, Security Operations Center

BRAND	Entry Level	High Level
Famous A&D corp	$50,000	$100,000
Famous Software corp	$60,000	$100,000
Famous National Consultants	$70,000	$120,000
Famous Cyber Specialists	$40,000	$ 80,000
Small Independent Providers	$40,000	$ 50,000

© 2017 CMTC all rights reserved

Internal Planning Process

DISCOVER

DEFINE

APPROACH

PLAN

PROJECT

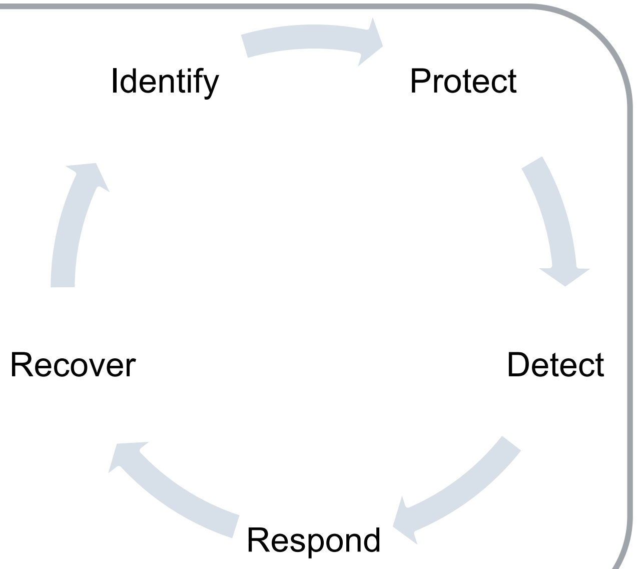
CLOSE

California's Manufacturing Resource

© 2017 CMTC all rights reserved

Cybersecurity Engagement Milestones

1. Champion
2. Security triage
3. Pre-assessment
4. Awareness
5. Scope, SOW, Reach Agreement
6. Initial Assessment
7. GAP
8. POA&M Plan of Actions & Milestones
9. SSP Systems Security Plan
10. Remediation
11. Verification & Validation
12. Continuous Monitoring and Detection
13. Intrusion Reporting
14. Incidenty Reporting
15. Compliance Final Report
16. ATO Authority to Operate



Identify

Protect

Detect

Respond

Recover

California's Manufacturing Resource

© 2017 CMTC all rights reserved

Controlled Unclassified Information (CUI)

CUI is unclassified information that requires additional protections.

Some examples of the 107 unique markers for additional protection:

Manufacturing & Business

- ✓ Proprietary Information & Trade Secrets
- ✓ Sensitive But Unclassified
- ✓ For Official Use Only
- ✓ Personally Identifying Information
- ✓ Source Selection Data

Infrastructure & Government

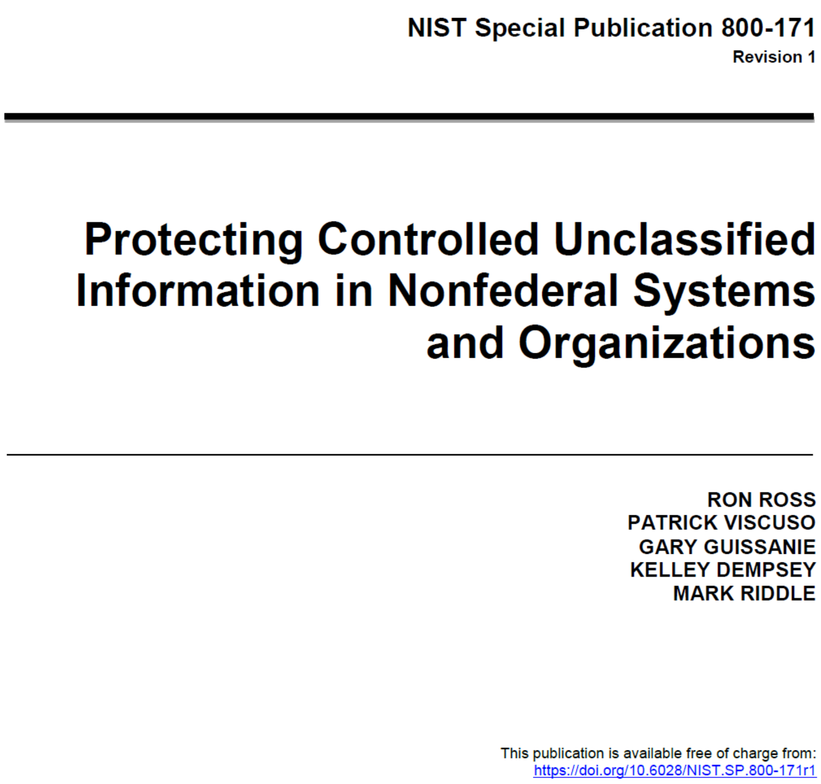
- ✓ Sensitive Security Information
- ✓ Protected Critical Infrastructure Data
- ✓ Operations Security (OPSEC)
- ✓ Law Enforcement Sensitive
- ✓ Export-Controlled Information

Link to CUI Registry: https://www.archives.gov/cui/registry/category-list

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

NIST SP800-171 (rev1)

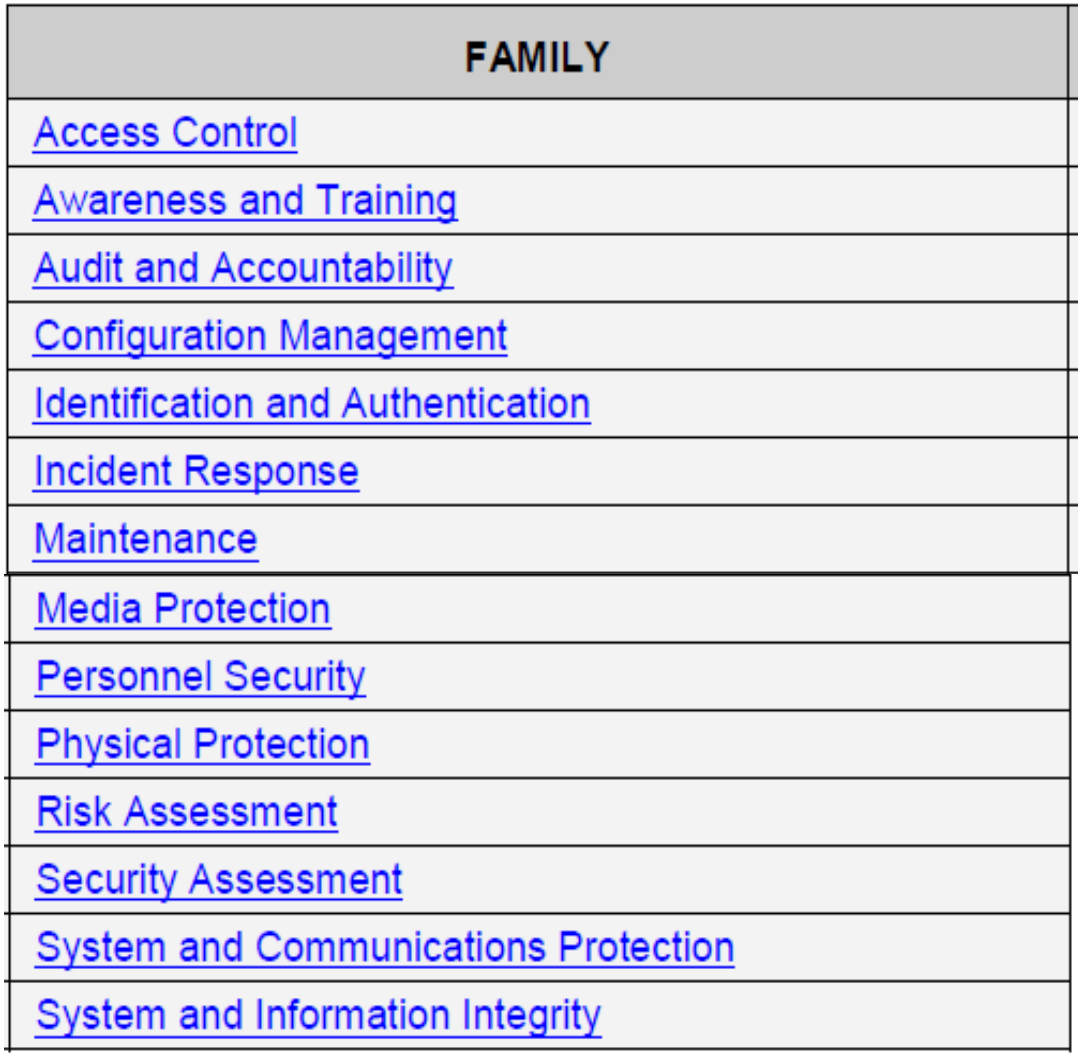


NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

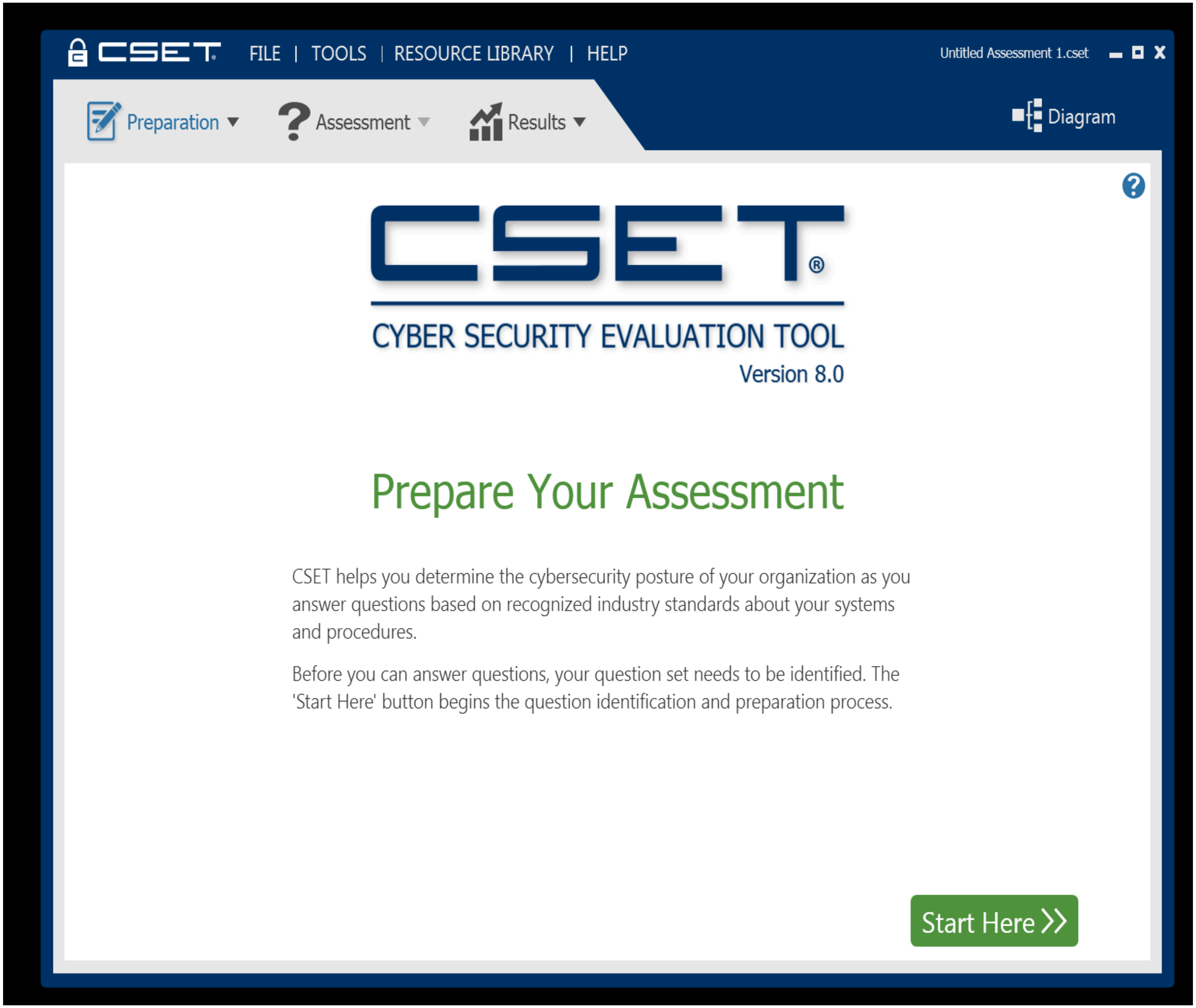
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1



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

Link to NIST SP800-171: https://csrc.nist.gov/csrc/media/publications/sp/800-171/rev-1/archive/2016-08-16/documents/sp800_171r1_draft_markup.pdf

© 2017 CMTC all rights reserved


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset
Preparation ▼
Assessment ▼
Results ▼
Diagram

CSET®

CYBER SECURITY EVALUATION TOOL

Version 8.0

Prepare Your Assessment

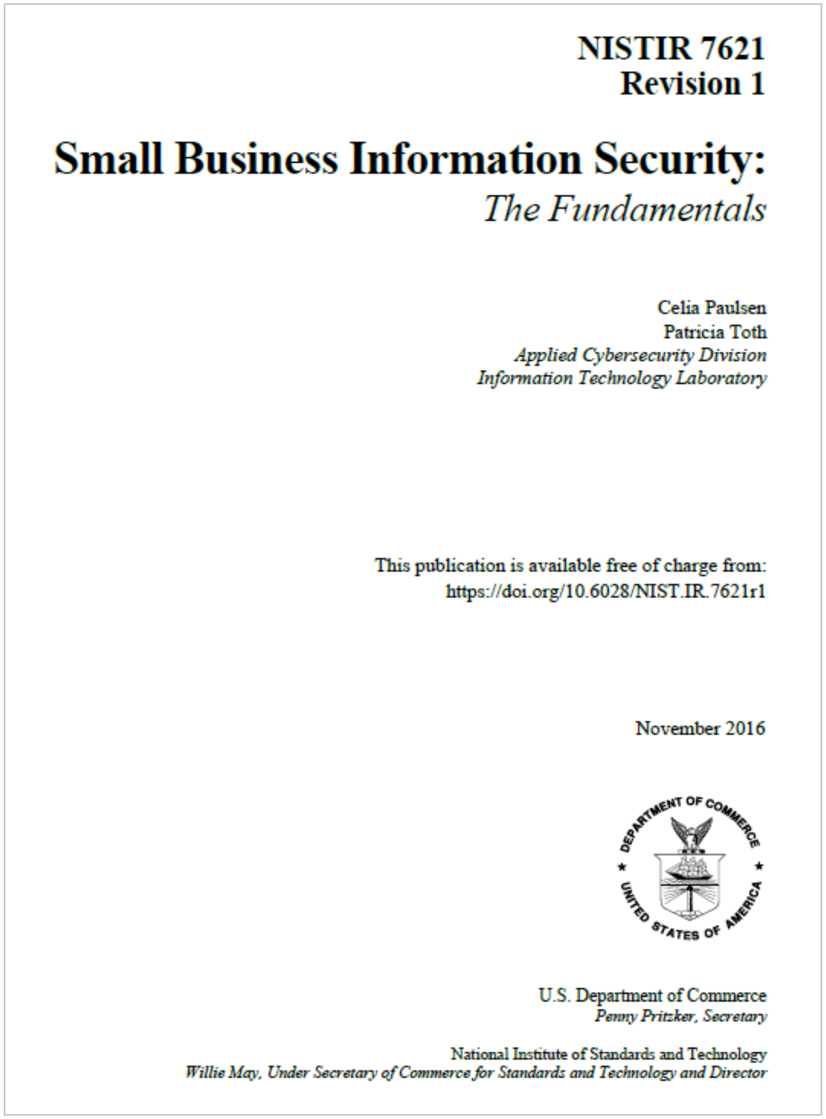
CSET helps you determine the cybersecurity posture of your organization as you answer questions based on recognized industry standards about your systems and procedures.

Before you can answer questions, your question set needs to be identified. The 'Start Here' button begins the question identification and preparation process.

Link to CSET: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

© 2017 CMTC all rights reserved

NIST Resources for all Manufacturers



NISTIR 7621
Revision 1

Small Business Information Security:
The Fundamentals

Celia Paulsen
Patricia Toth
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1

November 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NISTIR 7621 Rev 1,   (Nov 2016)
Small Business Information Security: The Fundamentals
http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

NIST Cybersecurity Framework Manufacturers Profile (Mar 2017)
http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft2.pdf

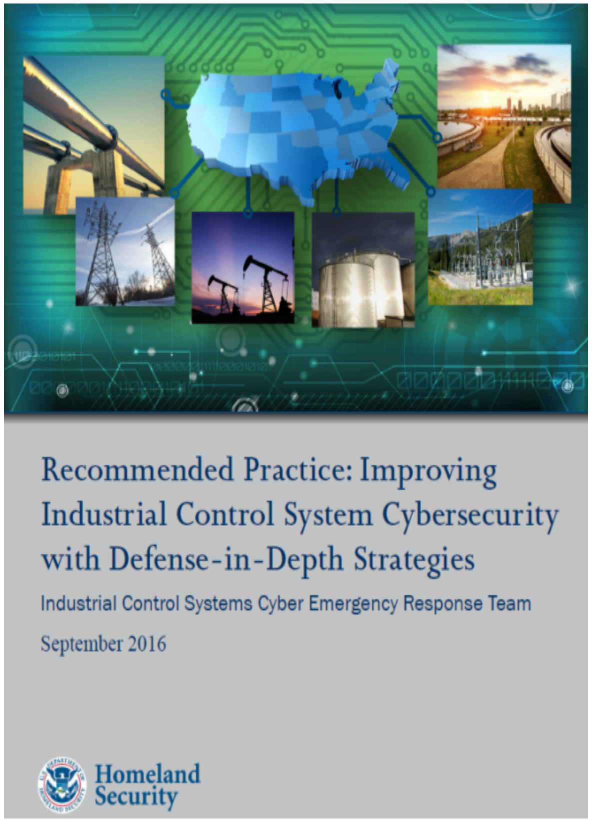
NIST SP 800-82 Rev 2,   (May 2015)
Guide to Industrial Control Systems (ICS) Security,

NIST Cybersecurity Framework (update Jan 2017)
https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf

Framework for Improving Critical Infrastructure Cybersecurity
UPDATE

© 2017 CMTC all rights reserved

Resources for all Manufacturers

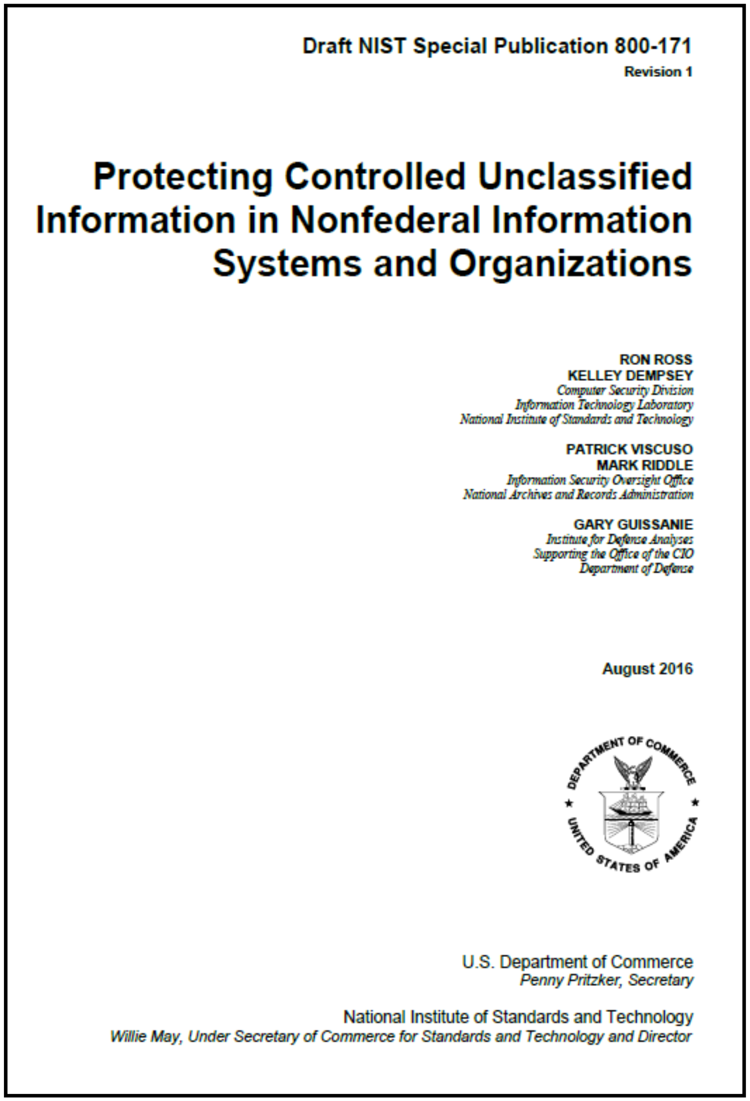


Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team

September 2016

Homeland Security



Draft NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

August 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

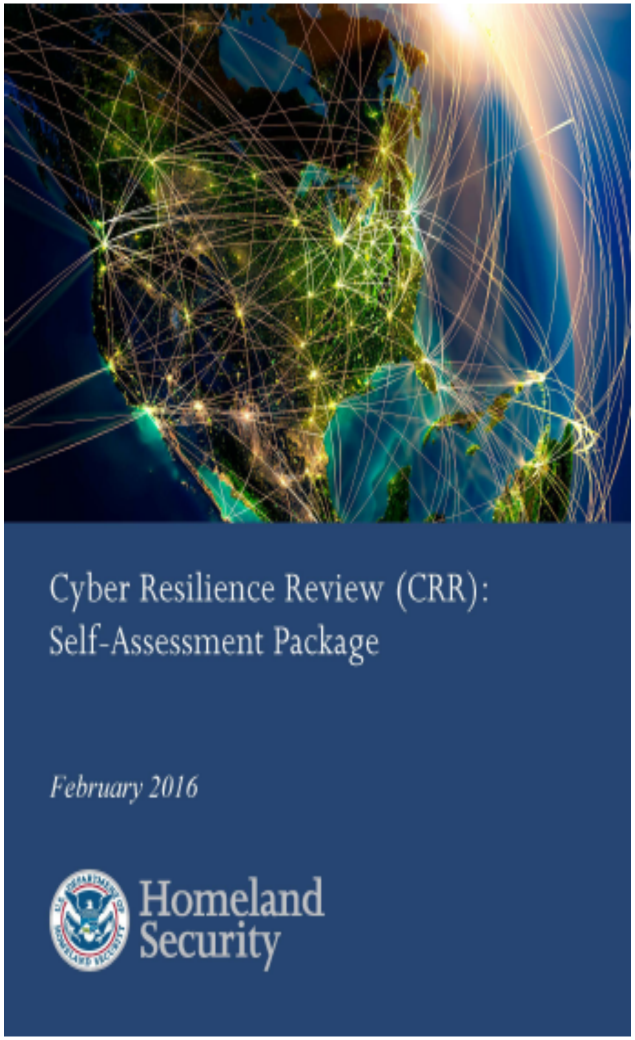
ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

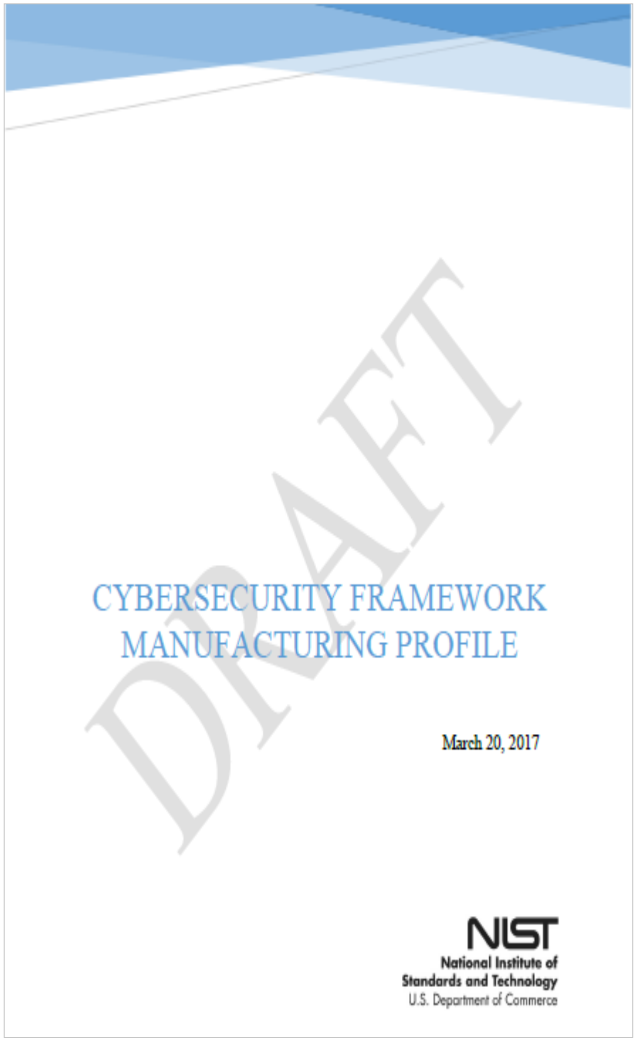
Resources for all Manufacturers



Cyber Resilience Review (CRR):
Self-Assessment Package

February 2016

Homeland
Security



CYBERSECURITY FRAMEWORK
MANUFACTURING PROFILE

March 20, 2017

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

DRAFT

California Data
Breach Report

February 2016

Kamala D. Harris, Attorney General
California Department of Justice

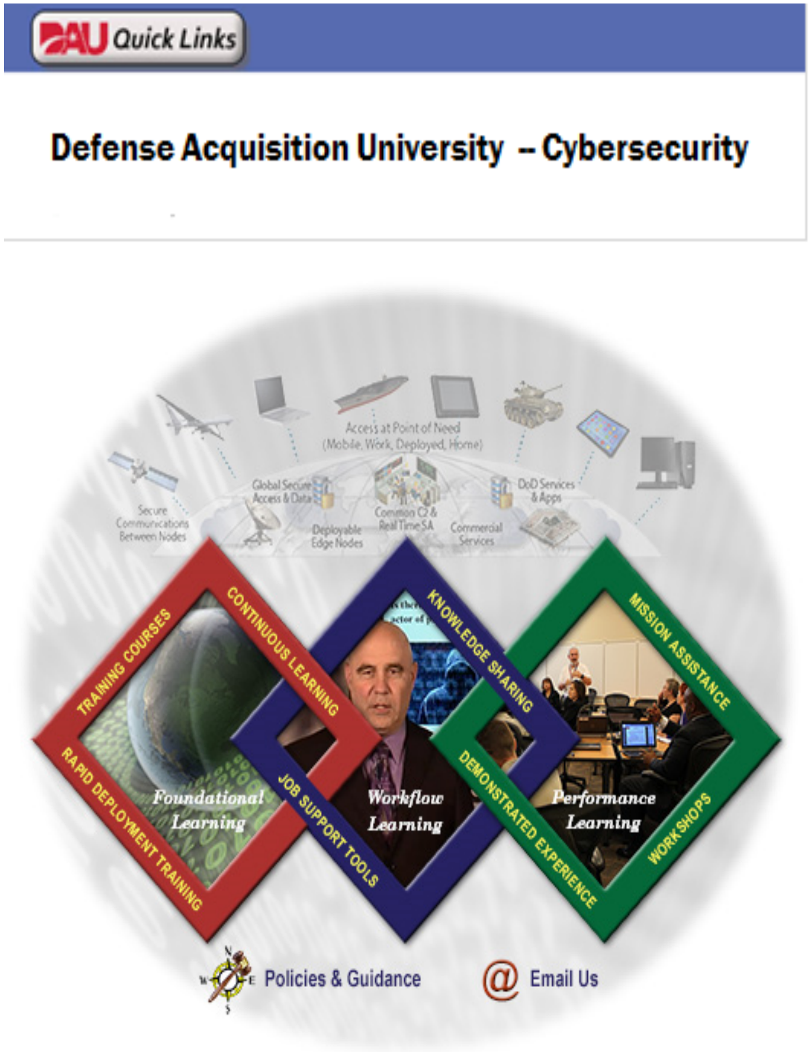
© 2017 CMTC all rights reserved

Resources for all Manufacturers

Federal Acquisition Regulations	FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems **https://www.acquisition.gov/far/html/52_200_206.html**
NIST SP800-171	Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations http://csrc.nist.gov/publications/drafts/800-171r1/sp800_171r1_draft.pdf
CSET download	Download CSET Cybersecurity Evaluation Tool https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
ICS-CERT	Cybersecurity Evaluation Tools Overview https://ics-cert.us-cert.gov/Assessments
CUI	Controlled Unclassified Information https://www.archives.gov/cui/registry
Industrial Control Systems	Industrial Control Systems Cyber Emergency Response Team - Effective Practices https://ics-cert.us-cert.gov/

© 2017 CMTC all rights reserved

Resources for all DoD Manufacturers



DAU Quick Links

Defense Acquisition University -- Cybersecurity

Industry and DoD Acquisition

- Community of Practice
- Videos
- Knowledge Sharing
- DoD Policies & Guidance

Link to DAU: https://www.dau.mil/cop/cybersecurity/Pages/Default.aspx

CMTC®
California's Manufacturing Resource

© 2017 CMTC all rights reserved

Resources for all DoD Manufacturers

DFARS	DFARS 252.204-7021 Defense Federal Acquisition Regulations Supplement Safeguarding Covered Defense Information and Cyber Incident Reporting http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
NIST SP800-171	Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations http://csrc.nist.gov/publications/drafts/800-171r1/sp800_171r1_draft.pdf
CSET download	Download CSET Cybersecurity Evaluation Tool https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
CUI	Controlled Unclassified Information https://www.archives.gov/cui/registry
CTI	Controlled Technical Information http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf
CTI	FAQs on implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 Safeguarding Unclassified Controlled Technical Information (CTI) http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

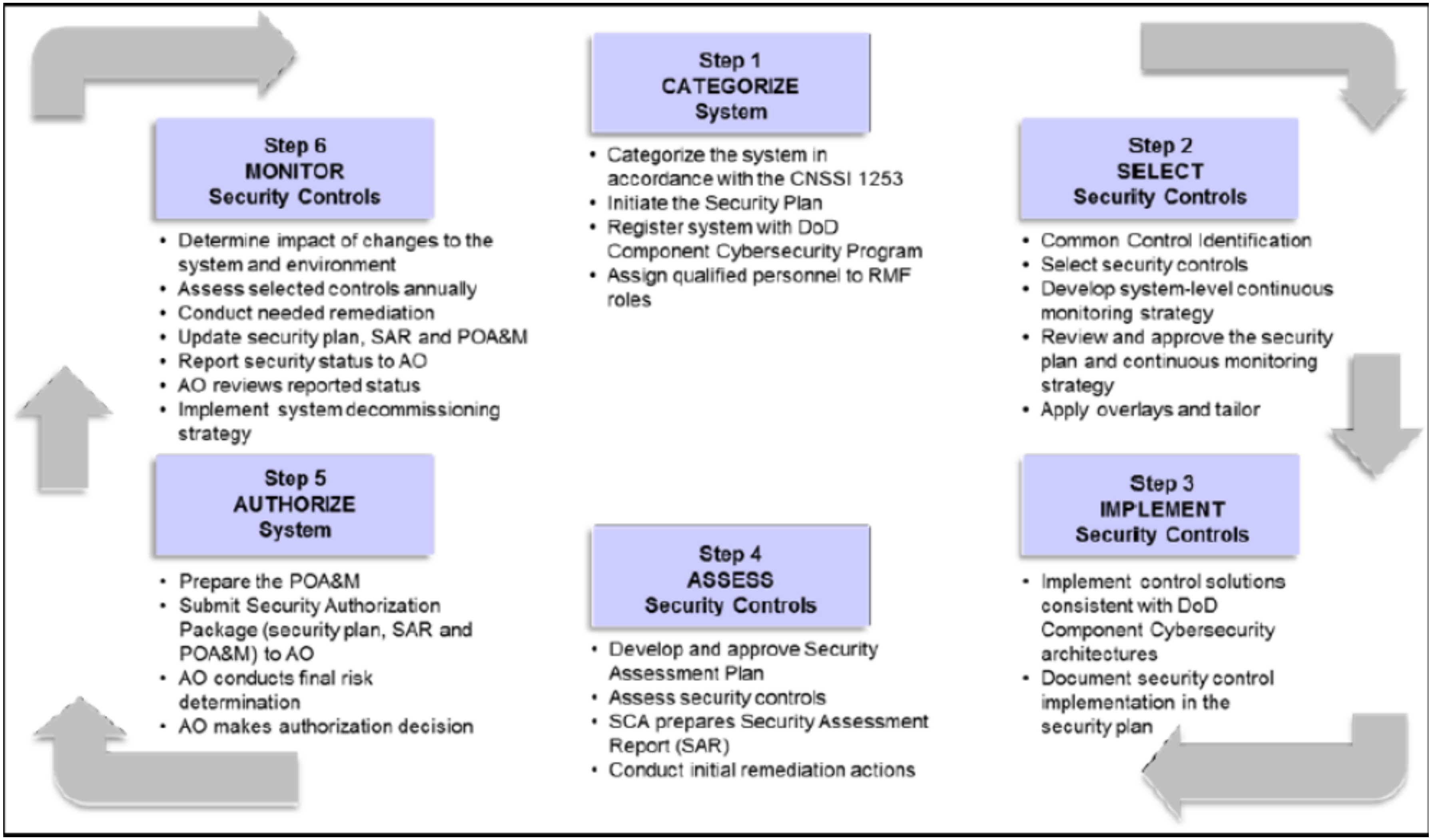
© 2017 CMTC all rights reserved

Additional Resources

DoD DIB	DoD's Defense Industrial Base Cybersecurity program (DIB CS program) http://dibnet.dod.mil
ICS-CERT	Cybersecurity Evaluation Tools Overview https://ics-cert.us-cert.gov/Assessments
ICS-CERT	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
INFRAGARD	FBI Infragard https://www.infragard.org
CDSE	Cyber Training & Awareness CDSE http://www.cdse.edu/toolkits/cybersecurity/training.html#general
NIST NICE	NIST National Initiative for Cybersecurity Education http://csrc.nist.gov/nice/awareness.html

© 2017 CMTC all rights reserved

Risk Management Framework



Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Incorporated into full system life cycle

Significant Requirements Impacts

List any significant items that “may” impact mission:

Items listed below will reflect the DFARS that will require awareness of these requirements and/or Contract Receipt and Review action:

- DFARS:
  - 252.204-7000, Disclosure of Information (Awareness Only and CRR/CTR)
  - 252.204-7003, Control of Government Personnel Work Product: (Awareness Only and CRR/CTR)
  - 252.204-7012, Safeguarding Defense Information and Cyber Incident Reporting (Awareness / Validation)
  - 252.239-7001, Information Assurance Contractor Training and Certification (Surveillance Required)
  - 252.239-7010, Cloud Computing Services (Awareness Only)

START NOW

CMTC

690 Knox Street
Torrance, California 90502
Web: www.cmtc.com

Chris Buthe
Phone 310-634-2908
Email cbuthe@cmtc.com

© 2017 CMTC all rights reserved