Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

KEY IDEAS ASSOCIATED WITH CUI REQUIREMENTS AND DFARS 252.204-7012

(CYBER SECURITY SERIES PART 4 OF 5)

ACQUISITION HOUR WEBINAR

November 6, 2019




WEBINAR ETIQUETTE

PLEASE

- Log into the GoToMeeting session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the CHAT option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

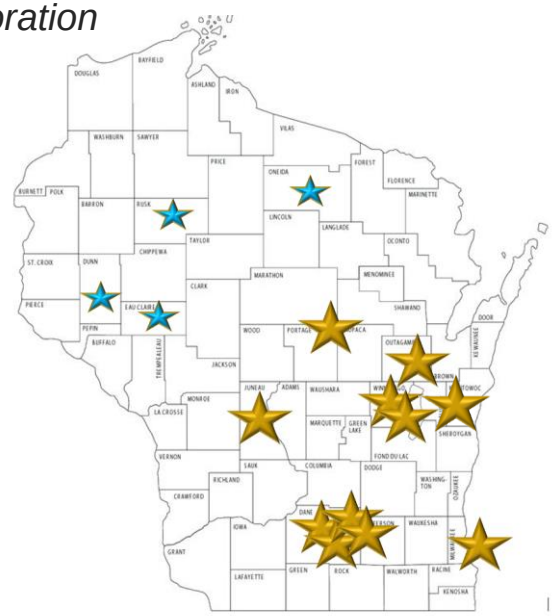
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, development and growing their sales, revenue and jobs through Federal, state and local government contracts.

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **GREEN BAY**
  - *Advance Business & Manufacturing Center*



WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
WED 21
Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
THU 22
Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
THU 22
NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
SEP 11
Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm
View More...
CURRENT OPPORTUNITIES (1)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

SO…. WHAT DOES WPI REALLY DO?

Provides technical assistance to CURRENT and POTENTIAL Contractors and subcontractors

- INDIVIDUAL CONSELING – At our offices, at clients facility or via telephone/GoToMeeting
- SMALL GROUP TRAINING – Workshops and webinars
- CONFERENCES to include one on one or roundtable sessions

Last year WPI provided training at over 100 events, provided service to over 1,000 companies

DFARS – Key, top-level elements

Marc N. Violante

Wisconsin Procurement Institute

November 6, 2019

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

DFARS 252.204-7012 - actions

- Requires Adequate Security
  - Implementation of NIST 800-171 rx (x being the current version)
    - System Security Plan
    - Plan of Action
    - Monitor for Malware
      - If Malware is identified, found
      - Inactivate and send to Contracting Officer
    - Monitor for intrusions/incidents
      - Conduct investigation for suspicious activity – abide by relevant laws (eg wire tapping)
      - Required report for validated incidents within 72 hours – requires Medium assurance cert
      - Take image of system
      - Retain for up to 90 days
  - Flow down to subcontractors – only if there is CUI

Subcontracts – flowdown

The Department's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flowdown of information requiring protection.

Key thoughts – deliberate management & minimize flowdown

Train-the-Trainer Unabridged DFARS 252.204-7012 May 2018_0 – accessed from www.dodprocurementtoolbox.com/cybersecurity - slide 15

Implementation – Contractor's responsibility

- Ultimately, **it is the contractor's responsibility** to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information).
- **Third party assessments or certifications of compliance <u>are not</u>**
  - required,
  - authorized,
  - or recognized by DoD,
  - nor will DoD certify that a contractor is compliant with the NIST SP 800-171 security requirements.

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

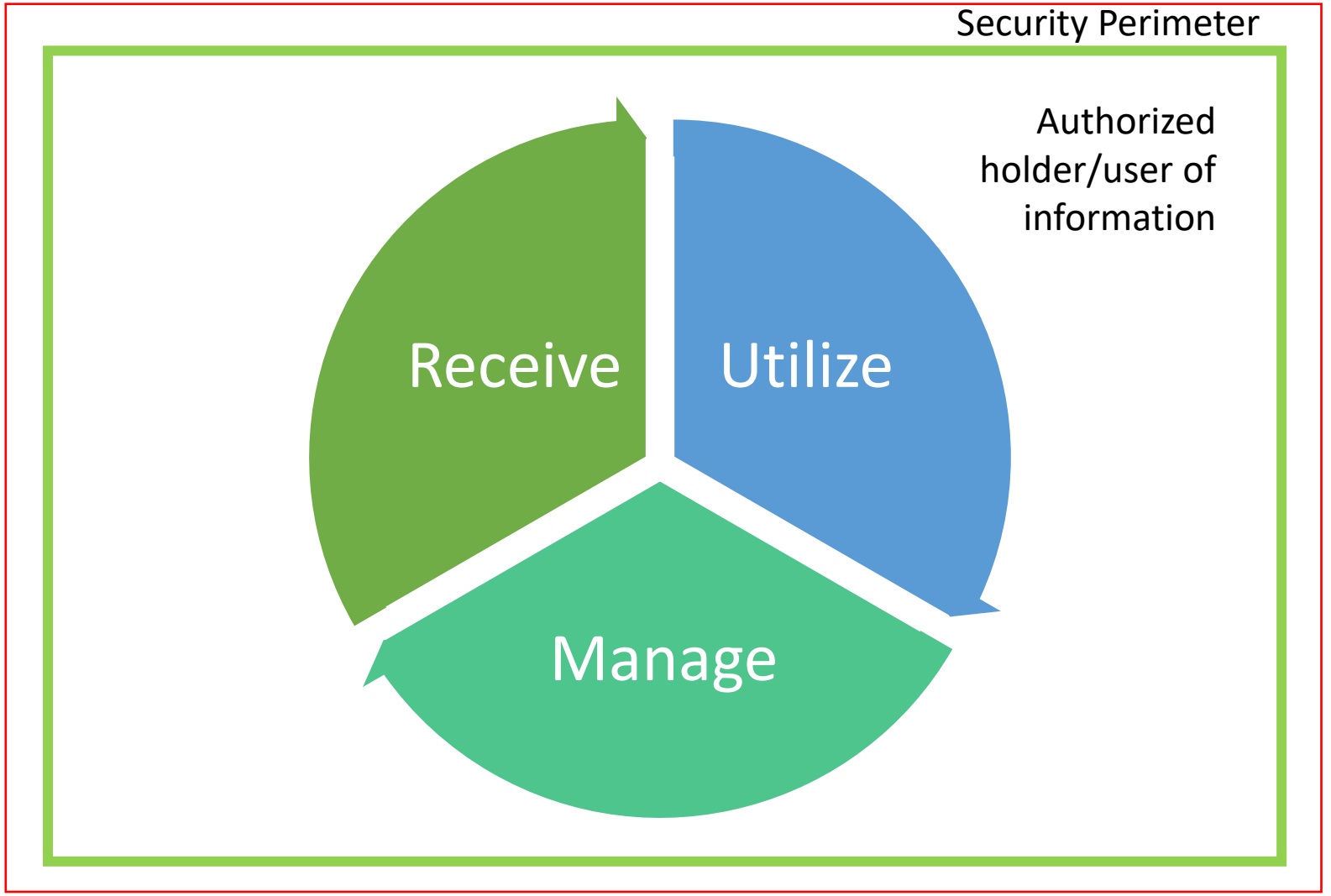
What is the purpose of implementation & reporting?

- Manage risk
- The concept of "Single State Information"
  - Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the security requirements contained in this publication are consistent with and complementary to the standards and guidelines used by federal agencies to protect CUI.
- Help prevent incidents
- Understand – who, what, where, and how
- Determine – what information was lost / how much / criticality

Three dimensions of cyber security

- Confidentiality
- Integrity
- Availability

Information – cycle – in general



What data/information is on your computer?

On your Network?

What devices are being used?

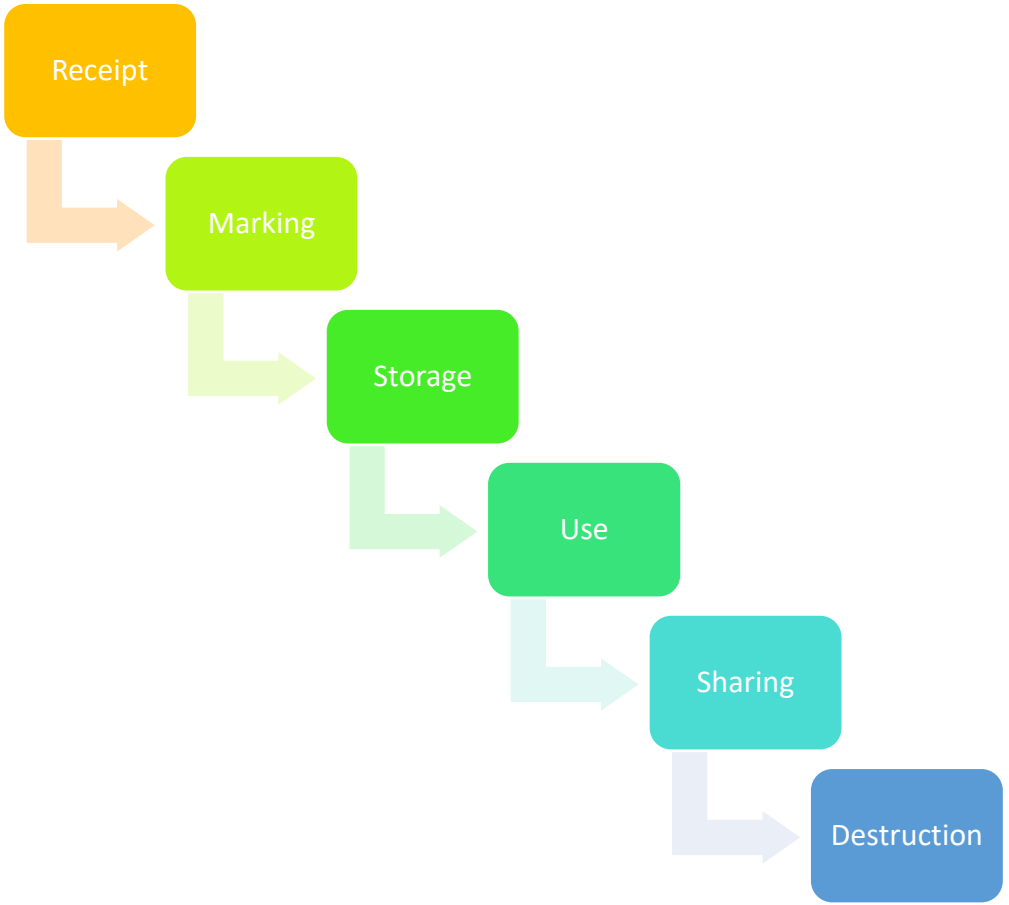
Who has access?

What are the entry points?

Are the security/safeguarding requirements all the same? – different customers, different types of data/information

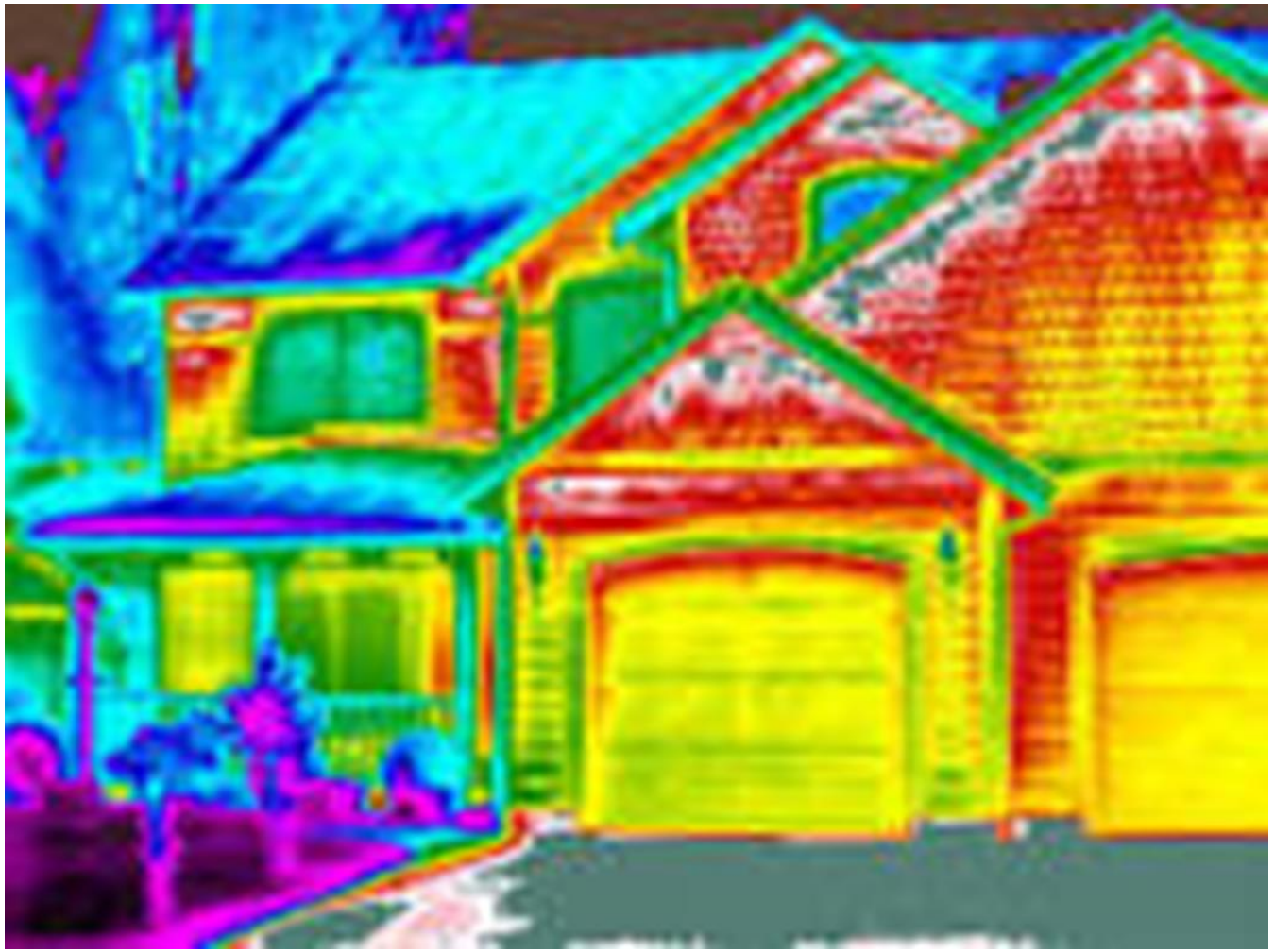
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Information – life cycle, general elements



- Auditing
- Awareness
- Controls
- ★ Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- ★ Transmittal registry
- Update procedures

800-171 r1 --Focuses on Confidentiality



Copied from Google search: infrared heat loss image

Sensitive Information – don't view in isolation

- Federal Contract Information FAR – 52.204-21
- Covered Defense Information DFARS – 252.204-7012
- Joint Certification Program DD- 2345
- International Traffic In Arm Regulation (ITAR)
- Disclosure of Information DFARS – 252.204-7000

Definitions

- Critical elements to understanding requirements

Adequate Security

- “Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

DFARS 252.204-7012

Compromise

- “Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

DFARS 252.204-7012

Cyber incident?

- A cyber incident is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

According to - DoD's DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal; the recipient of the required cyber incident report.

https://dibnet.dod.mil/portal/intranet/Splashpage/ReportCyberIncident

Don’t minimize the risk!

- It’s not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

Cyber – breach detection

"February 25, SecurityWeek – (International) **Breach detection time improves, destructive attacks rise: FireEye.** FireEye-owned Mandiant released a report titled, M-Trends which stated that current organizations were improving their breach detection rates after an investigation on real-life incidences revealed that the median detection rate improved from 205 days in 2014 to 146 days in 2015. The report also stated that disruptive attacks were a legitimate threat and gave insight into how organizations can prepare for and deal with such attacks.

Source: http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye "

Copied from: DHS Open Source Daily Infrastructure Report, Item 18, February 29, 2016

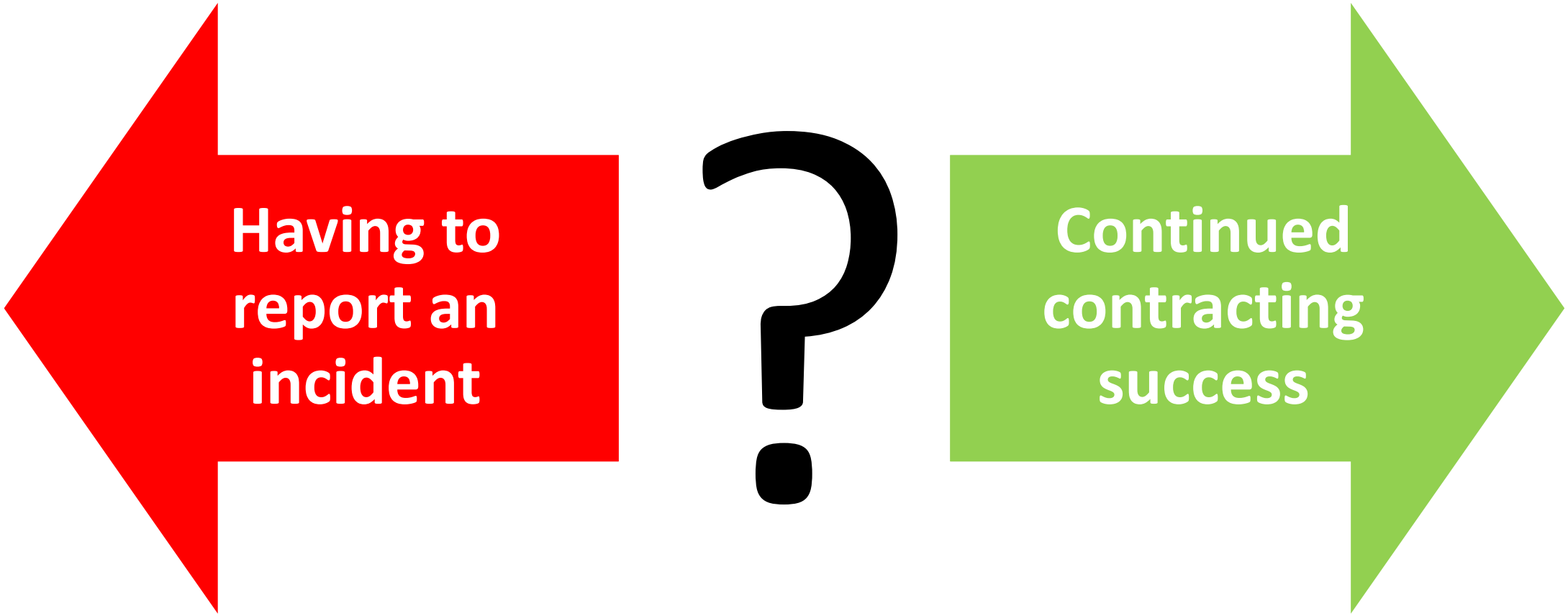
Id'ing the digital spy

"When businesses do eventually notice that they have a digital spy in their midst and that their vital information systems have been compromised, an appalling 92 percent of the time it is not the company's chief information officer, security team, or system administrator who discovers the breach."

- How do companies find out that they have been breached?
  - Law enforcement
  - Angry customer
  - Contractor

Marc Goodman, Future Crimes: everything is connected, everyone is vulnerable and what we can do about it, (New York: DOUBLEDAY, 2015), 16-17
Verizon's 2013 Data Breach Investigations Report is cited as the source

The dilemma


Having to report an incident
?
Continued contracting success

Cyber incident reporting requirement.

- (1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

- (i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This 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), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

- (ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil

DFARS 252.204-7012

What if there is a potential breach?

"Don't panic. Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize contractors acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers."

http://business.defense.gov/Small-Business/Cybersecurity/

DFARS 252.204-7012 – Implementation Compliance - background

(d) A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see PGI 204.7303-3(a)(3) (DFARS/PGI view)). The contracting officer shall consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements of the clause at 252.204-7012.

SUBPART 204.73--SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING(Revised December 28, 2017)

DFARS 252.204-7012 – Implementation Compliance – Contracting Officer's actions

(ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and

PGI 204.7303-3 Cyber incident and compromise reporting.

What is the purpose of implementation & reporting?

- Manage risk
- The concept of “Single State Information”
  - Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the security requirements contained in this publication are consistent with and complementary to the standards and guidelines used by federal agencies to protect CUI.
- Help prevent incidents
- Understand – who, what, where, and how
- Determine – what information was lost / how much / criticality

Cyber Incident – Reporting Requirements

- Actions required when
  - Cyber incident discovered
  - Cyber incident affects ability to perform
- Actions
  - Conduct a review for evidence to include
  - Rapidly report (within 72 hours) to https://dibnet.dod.mil
- Reporting required
  - Dibnet account
  - **DoD Medium Assurance Certificate – requires minimum 72 hours to obtain**

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C)

Cyber incident report

- The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C) (2)

Cyber Incident Reporting -

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident

- Company name
- Company point of contact information (address, position, telephone, email)
- Data Universal Numbering System (DUNS) Number
- Contract number(s) or other type of agreement affected or potentially affected
- Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
- USG Program Manager point of contact (address, position, telephone, email)
- Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Facility CAGE code
- Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)

https://dibnet.dod.mil/portal/intranet/Splashpage/ReportCyberIncident

- Impact to Covered Defense Information
- Ability to provide operationally critical support
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- DoD programs, platforms or systems involved
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative
- Any additional information

Cyber Incident Record Retention/Availability

- Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (e) & (f)

Security requirement 3.12.4 (System Security Plan, added by NIST SP 800-171, Revision 1)

- Requires the contractor to
  - develop
  - document
  - and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

[26] There is no prescribed format or specified level of detail for *system security plans*. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans. Footnote 26 page 14

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

System Security Plan - purpose

- The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.
- The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.
- The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO). Additional information may be included in the basic plan and the structure and format organized according to needs

Guide for Developing Security Plans for Federal Information Systems - NIST Special Publication 800-18 Revision 1, February 2006, Executive Summary

Security Requirement 3.12.2 (Plans of Action)

- Requires the contractor to
  - develop and implement plans of action
  - designed to
    - correct deficiencies and reduce or eliminate vulnerabilities in their systems.

Additional NIST 800-171 R1 requirements –

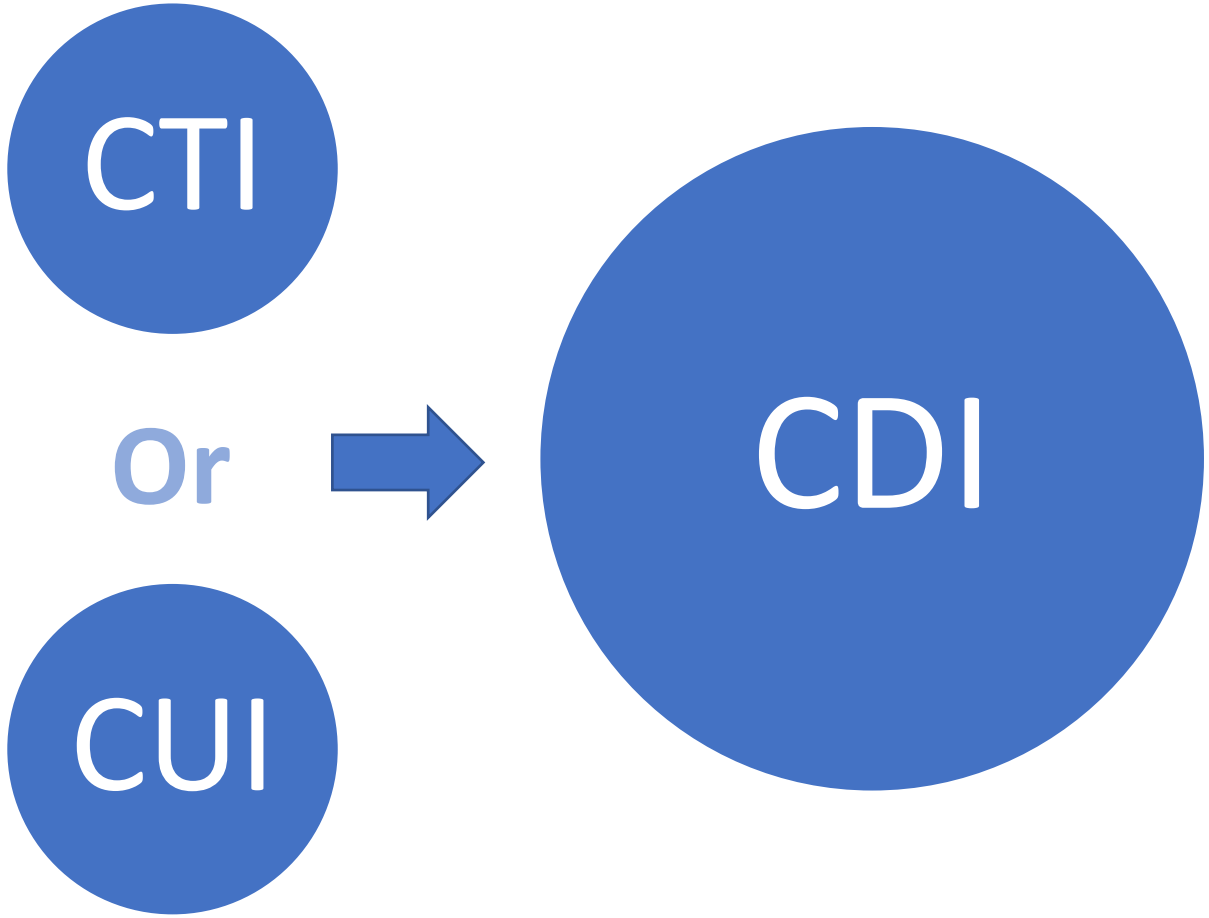
3.14.1 Identify, report, and correct information and system flaws in a timely manner.

3.14.3 Monitor system security alerts and advisories and take appropriate actions in response.

Comment: Don't view the requirements in isolation.

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

Covered Defense Information



DFARS 252.204-7012

Controlled Unclassified Information

- All unclassified information throughout the executive branch that requires any safeguarding or dissemi-nation control is CUI.
- Law, regulation (to include this part), or Government- wide policy must require or permit such controls.
- Agencies therefore may not implement safeguarding or dis-semination controls for any unclassi-fied information other than those con-trols consistent with the CUI Program.

32 CFR PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI) 2002.1 (c)

Covered Defense Information(CDI)

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to provide “adequate security” for covered defense information that is processed, stored, or transmitted on the contractor’s internal information system or network. The Department must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirement for the contractor to mark covered defense information developed in performance of the contract.

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

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.
- - is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical documents.
- The term does not include information that is lawfully publicly available without restrictions.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Distribution Statements

A. Approved for public release.

B. U.S. Government agencies only

C. U.S. Government agencies and their contractors

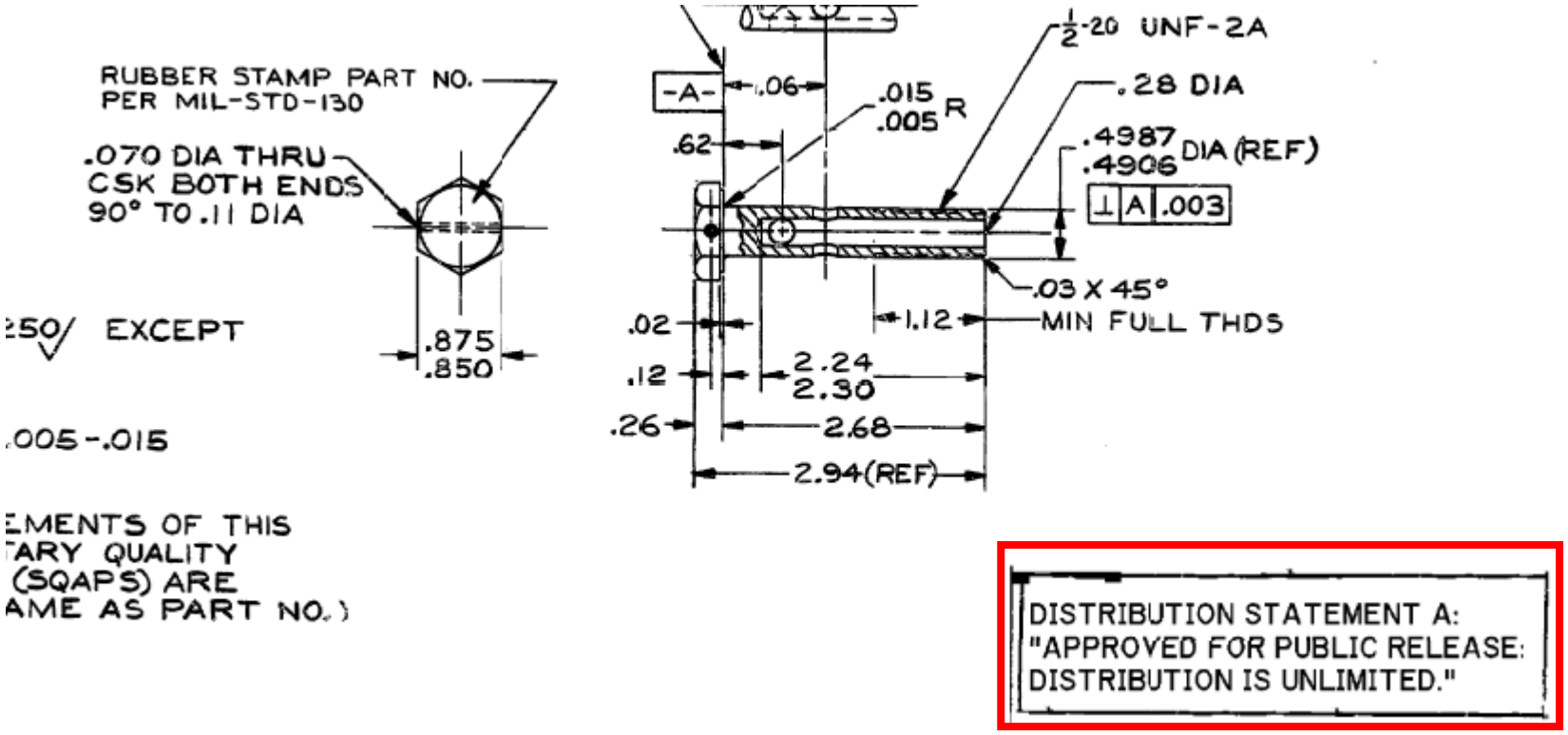
D. Department of Defense and U.S. DoD contractors only

E. DoD Components only

F. Further dissemination only as directed by

DoD Instruction 5230.24 August 23, 2012

Distribution Statement A - example



Attachment to client email

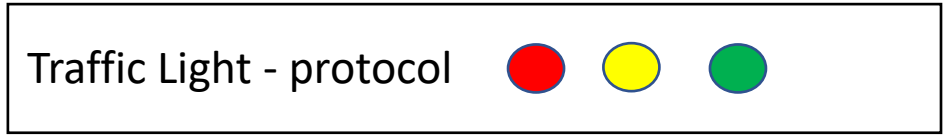
DFARS – 252.204-7012

- Don’t forget DFARS 252.204-7008!
- Know what you need to protect
- Understand Adequate Security
- Trap/capture – isolate Malware
- Test for incidents
- Conduct investigation
- Report as needed

DFARS / NIST Implementation

A reasonable first step may be for company personnel with knowledge of their information systems security practices to

- read through the publication,
- examining each requirement
- determine if it may require a change to company policy or processes, a configuration change for existing company information technology (IT), or if it requires an additional software or hardware solution. Most requirements



Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

Essential requirements

- Senior level involvement - support
- Required systems and procedures
- Awareness
- Knowledge
- Processes
- Resources
- Monitoring
- Updates as required
- Training

Key Roadblocks to implementation

- Funds
- Knowledge
- Resources
- Time
- What happens if ...
- Ultimately, understanding the goal

Documenting implementation

- To document implementation of the NIST SP 800-171 r1 security requirements by the December 31, 2017, implementation deadline, -
  - companies should have a system security plan in place,
  - in addition to any associated plans of action to describe
    - how and when any unimplemented security requirements will be met,
    - how any planned mitigations will be implemented, and
    - how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems.
- Organizations can document the system security plan and plans of action as separate or combined documents in any chosen format.

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

Create a “Balance Sheet” – track progress

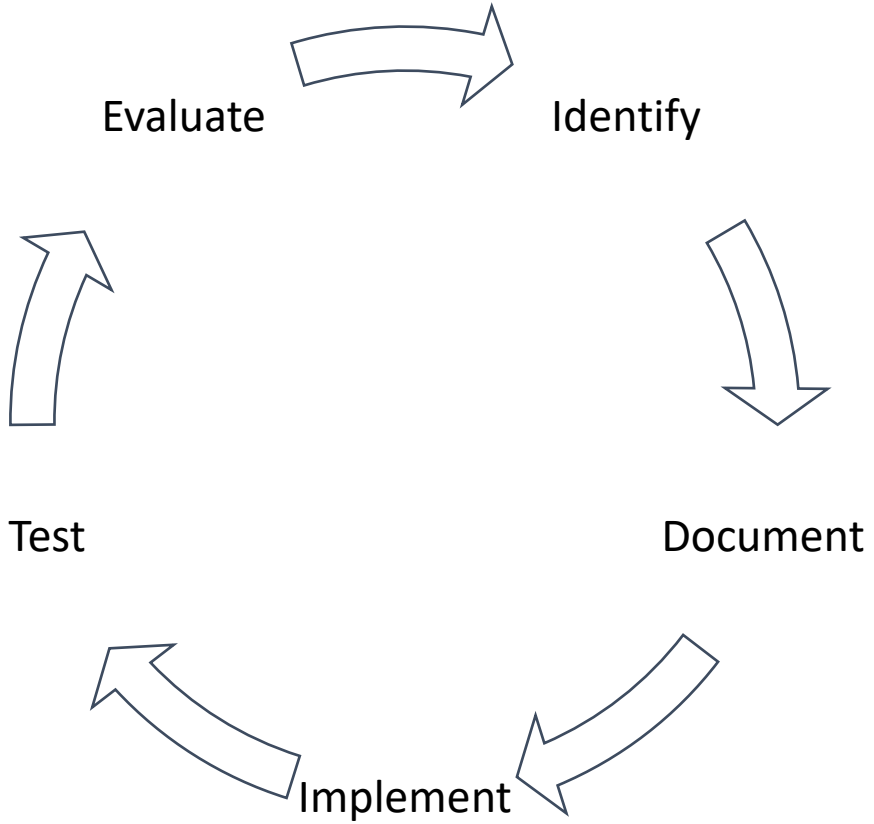
NIST 800-171 r1

	Number	Factor	Sum - positive	Sum - negative
Apply	35	1	35	
Don’t Apply	50	1	0	0
Not complete	25	1		25
Total	110	50	35	25

Identify – opportunities to improve

- Systems change
- Computers change
- Software changes
- Users change
- Needs change
- Threats change
- Today's and the future cyber environment will continue to evolve
- So must our systems

Lastly - Plan for continuing effort/evolution



UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

- November 12, 2019

  Procurement Methods
  CLICK HERE for additional information – presented by Helen Henningsen, Wisconsin Procurement Institute (WPI)

- November 19, 2019

  The Future of SAM.gov
  CLICK HERE for additional information – presented by Kim Garber, Wisconsin Procurement Institute (WPI)

- December 3, 2019

  Types of Federal Contracts
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

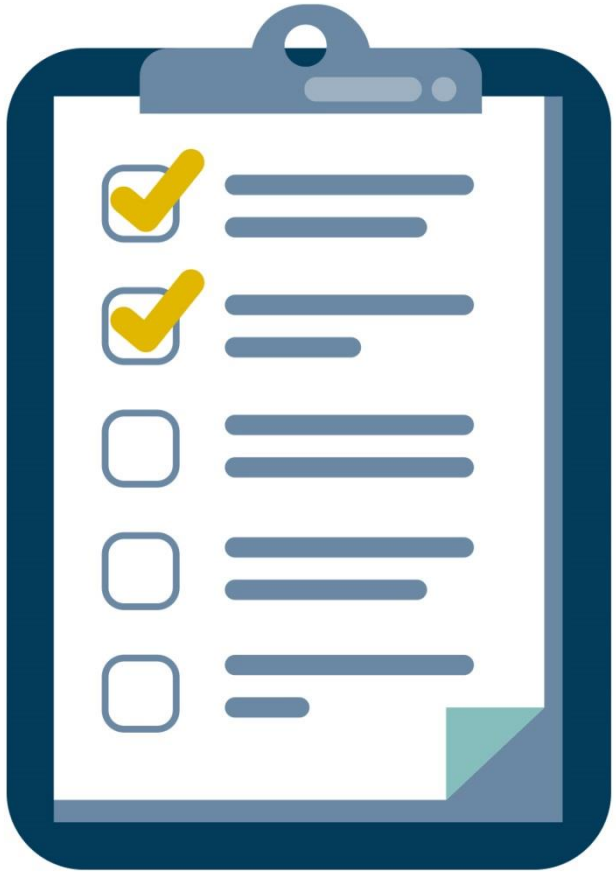
- December 10, 2019

  Cyber Trends, Threats and the Evolving Hacker's Marketplace
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

QUESTIONS?

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

SURVEY



Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante – Director, Federal Market Strategies
marcv@wispro.org | 920-456-9990

Benjamin Blanc, CFCM, CPPS - Government Contract Specialist
benjaminb@wispro.org | 414-270-3600

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226