Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS

(CYBER SECURITY SERIES PART 3 OF 5)

ACQUISITION HOUR WEBINAR

October 30, 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 31 Years of serving Wisconsin Business!

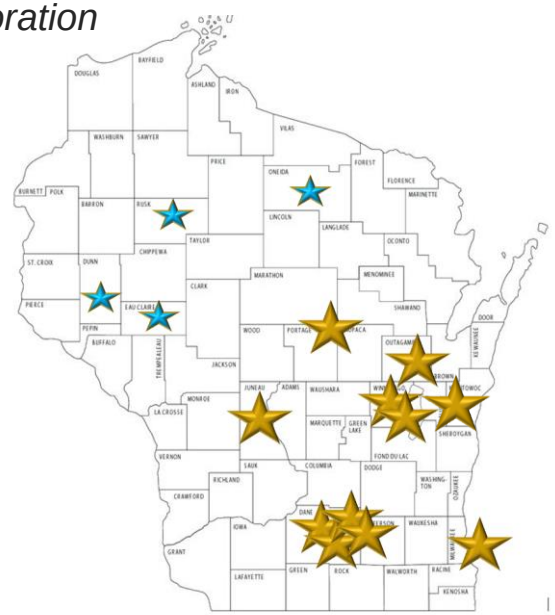
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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

CYBER FUNDAMENTALS FOR DFARS 252.204-7012 IMPLEMENTATION

Image source: readywisconsin.wi.gov

Marc N. Violante

Wisconsin Procurement Institute

October 30, 2019

Small Business risk – “it won’t happen to us”

- 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

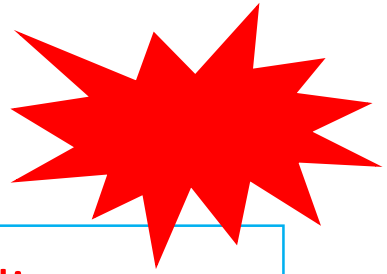
Id'ing the digital spy

"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

In the News – Summer of 2015



- Several of NY must prestigious trusted law firms
- Under cyberattack – trio of Chinese hackers
- Snuck in to law firm network via tricking partners into revealing email passwords
- Once in – snooped – highly sensitive document related to M&A's
- Then from ½ around the world, traded on that info – netting $4M
- "You are and will be the targets of cyberhacking, because you have information valuable to would-be criminals"
- Aha moment – how vulnerable and defenseless

Jeff John Robers and Adam Lashinsky, Fortune, July 1, 2017, 52-59

In the News – Summer of 2015 – Hacker's view

- "Expensive data-security systems and high-priced information security consultants don't faze today's hackers."
- Hackers have – time and resources

They also share

- In the NY Law firm case, "attackers attempted to penetrate targeted servicers more than 100,000 times over seven months."
- "It has become abundantly clear that no network is completely safe. "

Jeff John Robers and Adam Lashinsky, Fortune, July 1, 2017, 52-59

Federal supply chain – the soft underbelly

Vulnerabilities Email Security Virus & Malware IoT Security Endpoint Security

Home › Risk Management

U.S. Government Contractors Score Poorly on Cyber Risk Tests

By Kevin Townsend on February 16, 2018

Share G+ Tweet Recommend 17 RSS

Report Analyzes Cyber Risk of Federal Supply Chain

Attacks against the supply chain are not uncommon. It represents the soft underbelly of large organizations that are otherwise well defended. The federal government is not an exception -- in fact, federal agencies are especially reliant on their supply chain; and the security posture of that supply chain is of national importance.

This importance is not unrecognized. The May 2017 presidential Executive Order specified that the supply chain be included in security improvements: it called for a report, "on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks."

Google™ Custom Search Search

SECURITYWEEK DAILY BRIEFING

BRIEFING

Business Email Address SUBSCRIBE

SECURITYWEEK

ICS CYBER SECURITY CONFERENCE

THE ORIGINAL

https://www.securityweek.com/us-government-contractors-score-poorly-cyber-risk-tests

Cyber incident – the lost USB

- **London Heathrow Airport's security laid bare by one lost USB stick**

  If someone set out to invent a risky way to transport important data around it's hard to imagine they'd better the USB flash stick for calamitous efficiency.

  They're cheap enough to feel disposable, store large numbers of files, and despite years of mishaps barely any are sold with encryption security.

  They're also incredibly popular – which is why in 2017 we're still writing about cases like the USB stick found in a west London street that turned out to contain 2.5Gb of unprotected files detailing many of the anti-terrorism procedures and systems used to protect one of the world's busiest airports.

  This included: the route taken by the Queen, politicians and dignitaries when using the airport's secure departure suite; radio codes used to indicate hijackings; …

https://nakedsecurity.sophos.com/2017/10/31/london-heathrow-airports-security-laid-bare-by-one-lost-usb-stick/

Cybersecurity Landscape

Cyber threats targeting government unclassified information have dramatically increased

Cybersecurity incidents have surged 38% since 2014

The Global State of Information Security ® Survey 2016

Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%).

AT&T Cybersecurity Insights Vol. 4

Cyber attacks cost companies $400 billion every year

Inga Beale, CEO, Lloyds

89% of breaches had a financial or espionage motive

64% of confirmed data breaches involved weak, default or stolen passwords

2016 Data Breach Investigations Report, Verizon

Cybercrime will cost businesses over $2 trillion by 2019

Juniper Research

In a study of 200 corporate directors, 80% said that cyber security is discussed at most or all board meetings. However, two-thirds of CIOs and CISOs say senior leaders in their organization don't view cyber security as a strategic priority.

NYSE Governance Services and security vendor Veracode

Unclassified 3

http://dodprocurementtoolbox.com/site-pages/cybersecurity-other-resources - What happens on December 31, 2017

General issues

- Growing
- Evolving
- Not just passwords
- Sophisticated
  - Individuals, nation-states, repositories of resources/tools
- Active penetration –
  - Motivations might be -- challenge, game, treasure hunt, bragging rights
- Breaches not identified for significant amount of time
- Breach = total access

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Information Security – key elements

- **Confidentiality** - protecting information from unauthorized access and disclosure.

  For example, what would happen to your company if customer information such as usernames, passwords, or credit card information was stolen?

- **Integrity** - protecting information from unauthorized modification.

  For example, what if your payroll information or a proposed product design was changed?

- **Availability** - preventing disruption in how you access information.

  For example, what if you couldn't log in to your bank account or access your customer's information, or your customers couldn't access you?

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

Leakage – heat loss or information loss?

Copied from Google search: infrared heat loss image

What data/information is on your computer?

On your Network?

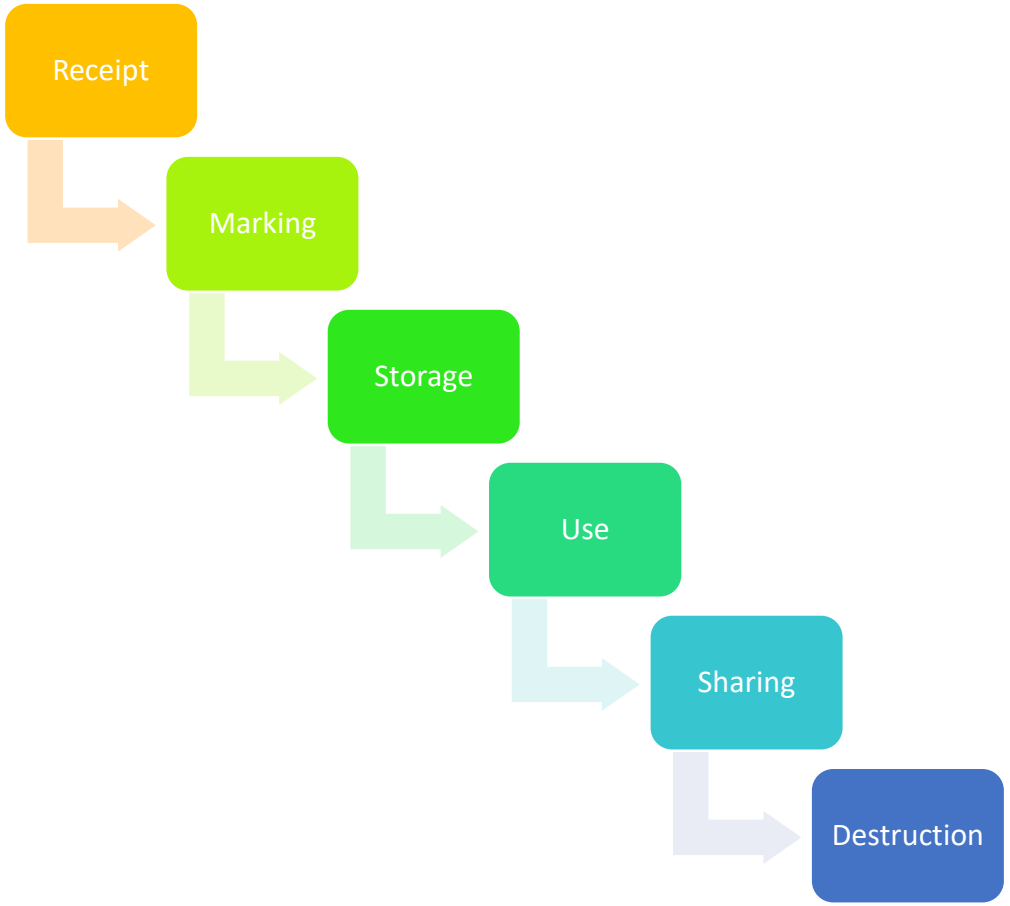
What devices are being used?

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

Information – life cycle – NIST (examples)

Receipt - 3.1.3 Control the flow of CUI in accordance with approved authorizations.

Marking - 3.8.4 Mark media with necessary CUI markings and distribution limitations

Storage -- 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Use - 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

Sharing - 3.10.3 Escort visitors and monitor visitor activity.

Destruction - 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Overview – protection of CUI

Prime

- Clause – 252.204-7012
- Clause – 252.204-7008
- Identified – marked material
- CUI may exist with JCP, ITAR, EAR
- Flow down
  - If CUI flow down 252.204-7012
  - If only commercial, remove CUI requirements

Subcontractor

- If contract contains CUI, must adhere to CUI program/DFARS clause requirements.
- May include derivative/created information – technical data
- Includes incident reporting
- Possible flow-down to sub-tiers

Covered Defense Information(CDI)

- Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely.
- These requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy.
- Some requirements will require security-related software (such as anti-virus) or additional hardware (e.g., firewall).

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

Cyber Security – over arching idea

- "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [CNSSI4009][HSPD23].

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

Compliance – (in general)

- Providing Adequate Security - Implementation of NIST 800-171 r1, Industry Best Practices, Other actions to prevent unauthorized access to and use of a network.
- All actions and measures taken to monitor and indicate activity consistent with a behaviors, activities associated with reportable incidents.
- Actions to determine if there was a reportable incident and reporting consistent with requirements – includes breach & malware
- Forensic analysis, system image (preservation) up to 90 days

Cybersecurity in DoD Acquisition Regulations

The threats facing the DoD's unclassified information have dramatically increased as we provide more services online, digitally store data, and rely on contractors for a variety of information technology services. Recent high-profile incidents involving government information demand that information system security requirements are clearly, effectively, and consistently communicated to both government and industry.

The contents of this "Cybersecurity in Acquisition Regulations" page addresses the DoD's ongoing efforts –executed in partnership with industry – to improve the nation's cybersecurity. Specifically, it addresses DoD's effort to:

- Ensure that unclassified DoD information residing on or transiting through covered contractor networks or information systems is safeguarded from cyber incidents and that any consequences associated with loss of this information are assessed and minimized, and
- Understand when a cyber incident impacts a company's ability to provide operationally critical support to DoD.

The DoD needs to protect it's information – whether it resides on the Department's networks and systems, or on the networks and systems of our partners in industry – so that our capabilities are not exploited, misdirected, countered, or cloned. Protecting this information will save warfighter lives. The cyber threat is not going away – we must defend our networks and systems, and the information that resides on them. Cybersecurity is a shared challenge, and we must work together to address it and reduce risk.

http://dodprocurementtoolbox.com/site-pages/cybersecurity-dod-acquisition-regulations - visited Nov 7, 2017

Q6: When must the requirements in DFARS clause 252.204-7012 be implemented?

- A6: The requirements in DFARS clause 252.204-7012 must be implemented when covered defense information is processed, stored, or transits through an information system that is owned, or operated by or for, the contractor, or when performance of the contract involves operationally critical support. The solicitation/contract shall indicate when performance of the contract will involve, or is expected to involve, covered defense information or operationally critical support. All covered defense information provided to the contractor by the Government will be marked or otherwise identified in the contract, task order, or delivery order.

https://isoo.blogs.archives.gov/ Please see the attached slides from our last update: CUI Update to Stakeholders Apr, 17 2019 Slide: 13

DFAR 252.204-7012

DFARS 252.204-7012 directs how the contractor shall protect covered defense information;
The requirement to protect it is based in law, regulation, or Government wide policy.

Train-the-Trainer Unabridged DFARS 252.204-7012 May 2018_0 – accessed from www.dodprocurementtoolbox.com/cybersecurity - slide 17

Covered contractor information system

- Means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
- Derived requirement – covered defense information must be handled with "adequate security" **at all times**.
- DOD's IASE Certificate provides for
  - Digitally signing of documents (ID, entity affiliation, citizenship)
  - Encrypting documents
  - See: https://iase.disa.mil/Pages/index.aspx Information Assurance Support Environment

DFARS 252.204-7012 Definitions

DFARS - 252.204-7012

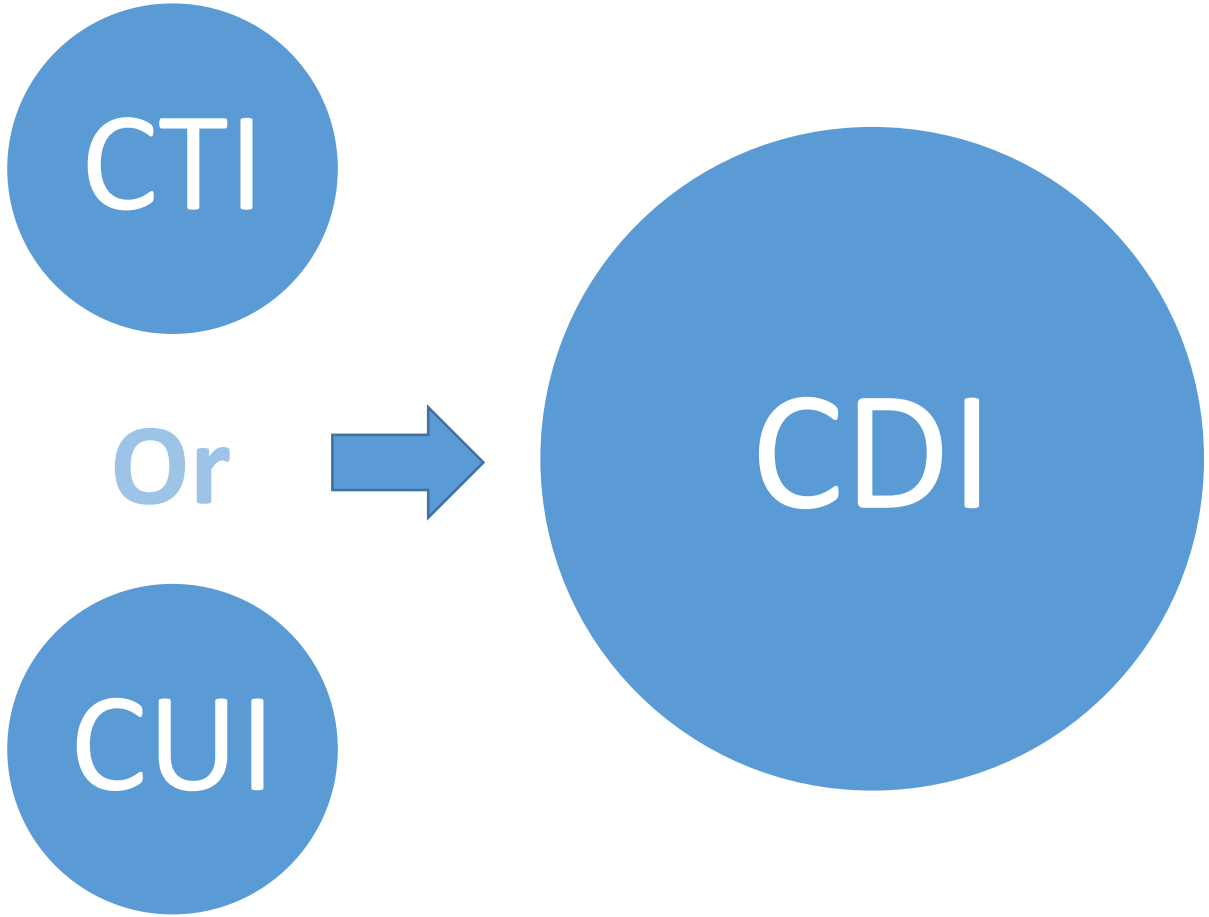
Safeguarding Covered Defense Information and Cyber Incident Reporting.

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

Covered Defense Information



DFARS 252.204-7012

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

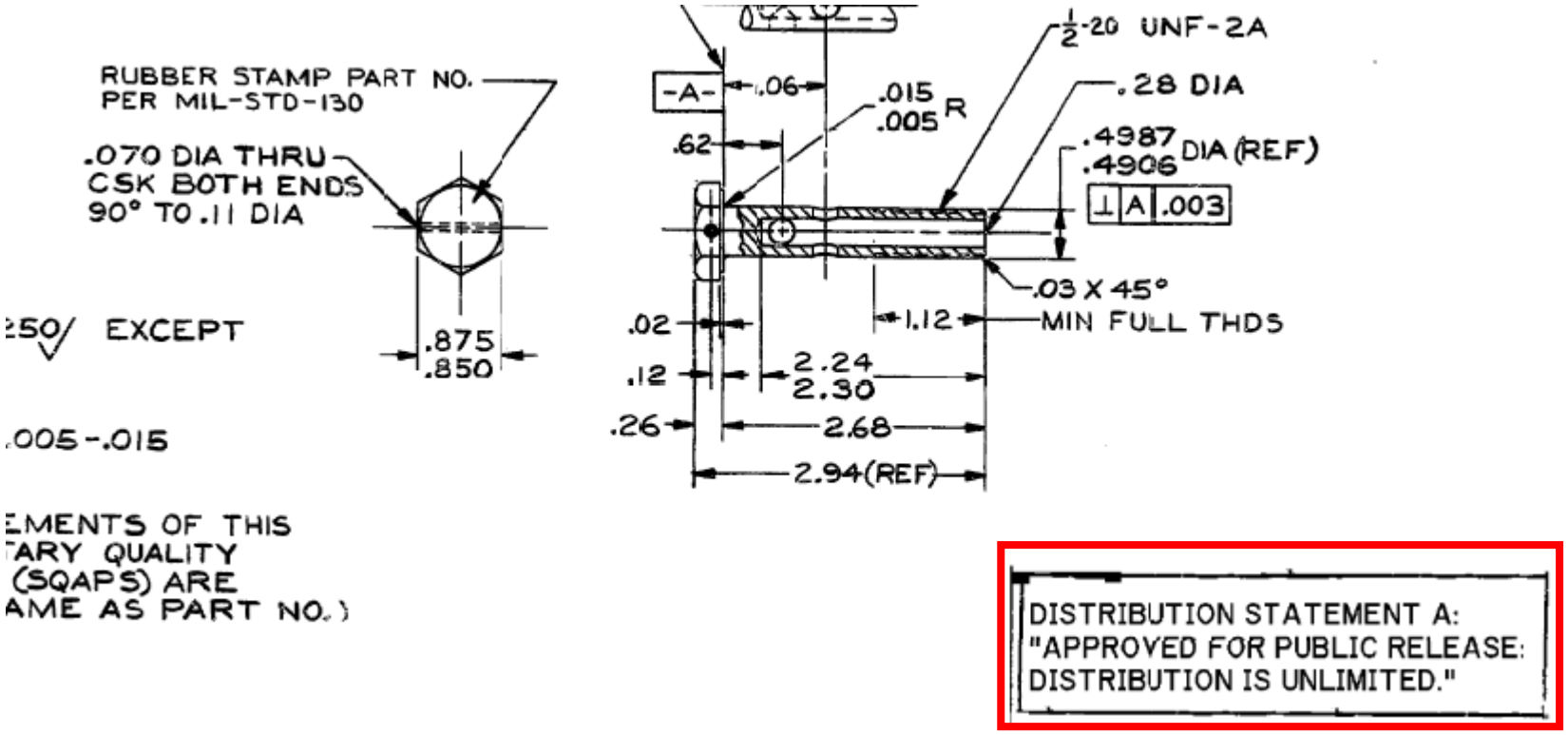
D. Department of Defense and U.S. DoD contractors only

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

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)

Federal Contract Information – definition

- "Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
- "Safeguarding" means measures or controls that are prescribed to protect information systems.

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

Federal Contract Information – examples req.

- “Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information. “Safeguarding” means measures or controls that are prescribed to protect information systems.
- Other definitions and 15 requirements such as –

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

“Mother may I” 252.204-7000

- (a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

  (1) The Contracting Officer has given prior written approval;

  (2) The information is otherwise in the public domain before the date of release; or

  (3) determined in writing by the contracting officer to be fundamental research in accordance with National Security Decision Directive 189 … and other requirements

Additional Resources –

NIST 200 – Minimum Security Requirements for Federal information and Information Systems

Specifications for Minimum Security Requirements

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

https://csrc.nist.gov/publications/detail/fips/200/final

Additional Resources –

NIST 800-171A – Assessing Security Requirements for Controlled Unclassified Information (Final Draft)

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE *Determine if, for an organizational system that processes, stores, or transmits CUI:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (including other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit records; other relevant documents or records; list of devices and other systems authorized to connect to organizational systems]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes account management on the system; mechanisms for implementing account management].	
	SUPPLEMENTAL GUIDANCE FOR SECURITY REQUIREMENT 3.1.1	

Final Draft: https://csrc.nist.gov/publications/detail/sp/800-171a/draft

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

Subcontracts – the contractor shall

- Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties.
- The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and
- Require subcontractors to—
  - Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and
  - Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (m)

Subcontracts – the contractor shall

“Subcontract” means a contract or contractual action entered into by a prime contractor or subcontractor for the purpose of obtaining supplies, materials, equipment, or services of any kind under a prime contract.”

“Subcontractor” (1) means any person, other than the prime contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract; and (2) includes any person who offers to furnish or furnishes general supplies to the prime contractor or a higher tier subcontractor.

FAR 3.502-1 Definitions

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.

DFARS 252.204-7012 – Implementation Compliance

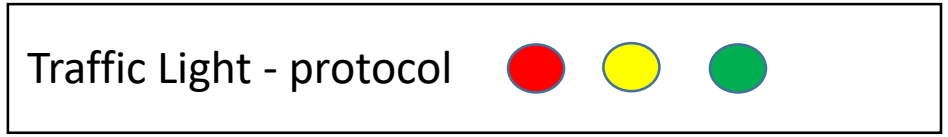
There is no single or prescribed manner in which a contractor may choose to implement the requirements of NIST SP 800-171, or to assess their own compliance with those requirements.

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

DFARS / NIST Implementation

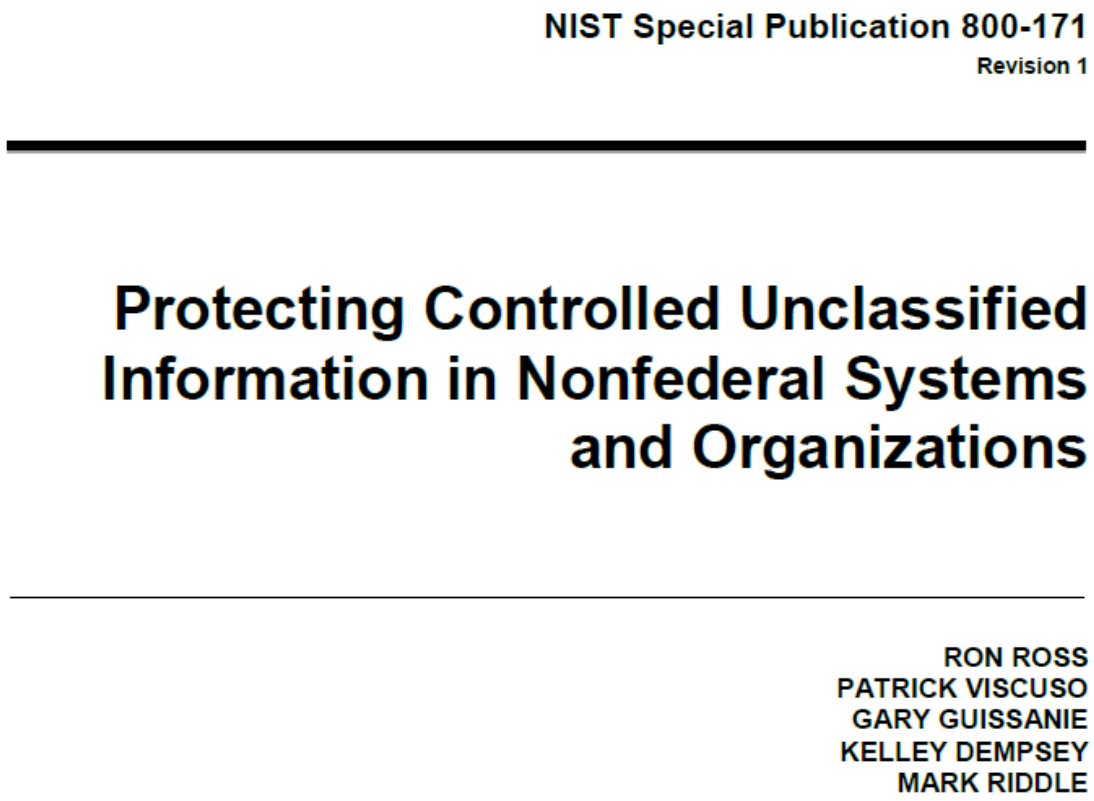
A reasonable first step may be for company personnel with knowledge of their information systems security practices to

- 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

NIST (SP) 800-171 Revision 1



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

NIST Document – cover page

NIST (SP) 800-171 Revision 1

- 3 Chapters – 125 pages
  - Introduction
  - The Fundamentals
  - The Requirements
  - Appendices
    - A - References
    - B - Glossary
    - C - Acronyms
    - D – Mapping Tables
    - E – Tailoring Criteria
    - F - Discussion

NIST (SP) 800-171 Revision 1, December 2016

NIST (SP) 800-171 Revision 1

an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the information security requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute,

In addition to the security objective of *confidentiality*, the objectives of *integrity* and *availability* remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program. While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Organizations that are interested in or required to comply with

NIST (SP) 800-171 r1 – Cautionary Note, page iv

Note: NIST SP 800-171 v. NIST SP 800-171 Rev 1

- Note that DFARS Clause 252.204-7012 requires the contractor to implement the version of the NIST SP 800-171 that is in effect at the time of the solicitation, or such other version that is authorized by the contracting officer.
- Thus, if Revision 1 of NIST SP 800-171 was not in effect at the time of the solicitation, the contractor should work with the contracting officer to modify the contract to authorize the use of NIST SP 800-171, Revision 1, dated December 2016.
- DoD guidance is for contracting officers to work with contractors who request assistance in the consistent implementation of the latest version of DFARS Clause 252.204-7012 and NIST SP 800-171, Revision 1.

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

NIST (SP) 800-171 Tailored Criteria

There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.
- Communicated/communication with KO / Approval

NIST (SP) 800-171 Revision 1, December 2016

NIST (SP) 800-171 R1 – request to vary

- Per DFARS Clause 252.205-7012(b)(2)(ii)(B), if the offeror proposes to vary fromNIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, 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

Train-the-Trainer Unabridged DFARS 252.204-7012 May 2018_0 – accessed from www.dodprocurementtoolbox.com/cybersecurity - slide 28

NIST (SP) 800-171 Revision 1 - Requirements

NIST (SP) 800-171 Revision 1, December 2016

NIST (SP) 800-171 Revision 1 - example

3.12 SECURITY ASSESSMENT

Basic Security Requirements:

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 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]

- Derived Security Requirements: None.

NIST (SP) 800-171 Revision 1, December 2016

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

Security Controls [FIPS 199]

- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Guide for Developing Security Plans for Federal Information Systems - NIST Special Publication 800-18 Revision 1, February 2006, Appendix B: Glossary

Security Controls

Control categories: (examples)

- Physical control
  - Lock
  - fence
- Access controls
- Admin controls
  - Segregation of duties

By Stephen Northcutt
Version 1.2

Security controls are technical or administrative safeguards or counter measures to avoid, counteract or minimize loss or unavailability due to threats acting on their matching vulnerability, i.e., security risk. Controls are referenced all the time in security, but they are rarely defined. The purpose of this section is to define technical, administrative/personnel, preventative, detective, and corrective compensating controls, as well as general controls.

According to the GAO, "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people."[1]

https://www.sans.edu/cyber-research/security-laboratory/article/security-controls visited 2/28/2017

Risk Assessment – NIST (SP)800-39

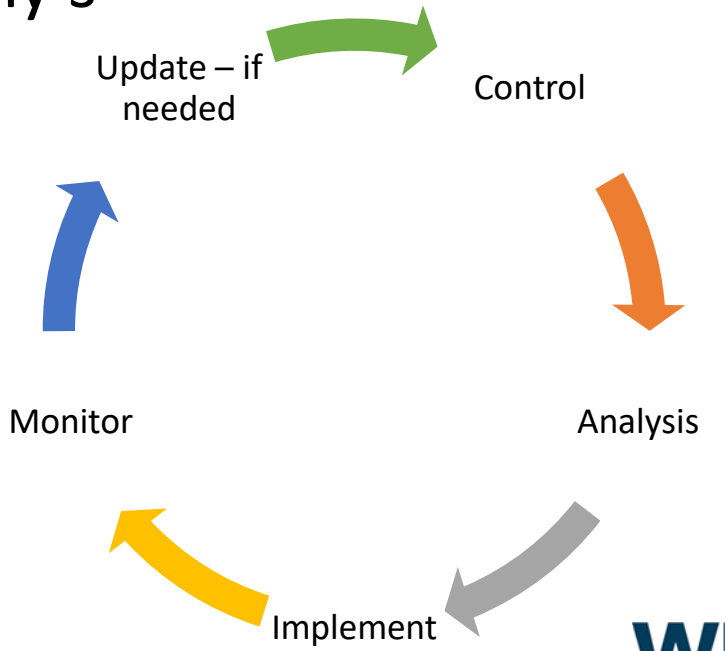
- A fundamental component of an organizational risk management process – may be conducted at different organizational tiers
  - Organization, mission/business, IT systems level
- Identify, estimate and prioritize risk to an organization
- Purpose – inform and advise, decision makers and support risk responses by
  - Identifying relevant threats
  - Vulnerabilities
  - Impact
  - Likelihood that harm will occur
- Outcome is a determination of risk

NIST 800-30 r1 Guide for Conducting Risk Assessments, Chapter 1, page 1

NIST (SP) 800-171 Revision 1 – key idea

3.4.4 Analyze the security impact of changes prior to implementation.

- Don’t act too quickly
- Ask questions – in quality there are the 5 why’s
- Test first if possible
- Look for unintended consequences
- Monitor impact
- Look for …



NIST (SP) 800-171 Revision 1, December 2016 : refers to 3.4.4 only

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

Implementation – Decisions

- Having reviewed all of the security requirements, a company may then determine which of the requirements,
  1) can be accomplished by their own in-house IT personnel,
  2) require additional research in order to be accomplished by company personnel,
  3) require outside assistance.

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017 & DoD Procurement Toolbox – What Happens on December 31, 2017 – slide 11

Extend compliance and security controls beyond employees

- Employees need to understand if data shared with outside partners is subject to specific regulatory requirements while being compliant, and if so, how to securely share that information with low risk. Additionally, companies should adopt compliance standards for their partners and vendors, and ensure that basic education is done before allowing access to any regulated information.
- To help staff and third party partners understand whether data is sensitive, technology such as data loss prevention or data classification can provide an automatic and visual prompt to users (e.g. warning a user before an email is sent that sensitive data is attached, or applying a watermark to documents to remind the user it contains private data). Adopting such an approach will allow organizations to ensure that data protection standards and policies are understood and can be acted on effectively.

https://www.securityweek.com/are-you-securing-your-contract-workforce

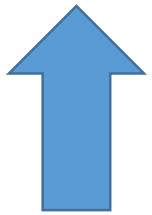
Marking Controlled Technical Information

- Is it required by contract or other reference?
- Does it make good business/security sense?
- Alerting suppliers/subcontractors
- Internal circulation v. external
  - Similar thoughts related to communicating – hot, fragile, dangerous material
  - How will external entities be informed/know?
- If started, marking, can it be stopped and started? – consistency
  - Why this one but not that one?

Key Decision(s) related to Cyber preparedness

- Internal
  - Staff, full time, other duty as assign
  - Staff, part time, dedicated
- External – subcontract/consultant
- Staff
  - Awareness
  - Training
  - Refresher training
  - Updates to requirements

Is it a priority for you?



What is a 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

Protective measures - NIST

3.8.4 Mark media with necessary CUI markings and distribution limitations.[25]

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7 Control the use of removable media on system components.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

NIST (SP) 800-171 Revision 1, December 2016
https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search 3.13.11

NIST SP 800-171 Security Requirement 3.13.11 – FIPS Validated Encryption

See FAQ 68

- Security Requirement 3.13.11 requires use of FIPS-validated cryptography when used to protect the confidentiality of CUI
- FIPS-validated cryptography means the cryptographic module has been tested and validated to meet FIPS 140-1 and -2 requirements
- FIPS-validated cryptography is required only to protect CUI and only when transmitted or stored outside the protected environment (including wireless/remote access) of the covered information system if not separately protected (e.g., by a protected distribution system)
  - FIPS validated encryption is required due to the high failure rate experienced during validation process
  - Encryption used for other purposes, such as within applications or devices, within the protected environment of the covered information system does not need to be FIPS-validated

Unclassified 26

Train-the-Trainer Unabridged DFARS 252.204-7012 May 2018_0 – accessed from www.dodprocurementtoolbox.com/cybersecurity - slide 26

Vulnerabilities lead to different paths of attack

Notes by CVSS Environmental Score

CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField() ...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...
9.4	2013-03-04	VU#688246	Oracle Java contains multiple vulnerabilities
9.3	2011-12-27	VU#723755	WiFi Protected Setup (WPS) PIN brute force vulnerability
9.2	2014-08-07	VU#578598	Iridium Pilot and OpenPort contain multiple vulnerabilities
9.0	2014-11-11	VU#505120	Microsoft Secure Channel (Schannel) vulnerable to remote code exe...

https://www.kb.cert.org/vuls/byCVSS visited 9/12/2017

Risks - Identify and Prioritize Information Types

	Example: Customer Contact Information	Info type 1	Info type 2	Info type 3	…
Cost of revelation (Confidentiality)	*Med*				
Cost to verify information (Integrity)	*High*				
Cost of lost access (Availability)	*High.*				
Cost of lost work	*High*				
Fines, penalties, customer notification	*Med*				
Other legal costs	*Low*				
Reputation / public Relations costs	*High*				
Cost to identify and repair problem	*High*				
Overall Score:	*High*				

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, Table 1, 10 - sample

Implementation – Complexity & Size

- The complexity of the company IT system may determine whether additional software or tools are required.
- For smaller systems, the company may accomplish many requirements manually, such as
  - configuration management
  - patch management,
- Larger and more complex systems may require automated software tools to perform the same task.

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

Look for related requirements - Family elements 1, 5 and 13

- **3.1.13** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- **3.1.17** Protect wireless access using authentication and encryption
- **3.1.19** Encrypt CUI on mobile devices and mobile computing platforms.21
- **3.5.10** Store and transmit only cryptographically-protected passwords.
- **3.13.8** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- **3.13.10** Establish and manage cryptographic keys for cryptography employed in organizational systems.
- **3.13.11** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

NIST 800-171 r1

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

NIST SP 800-171 Rev 1 – evaluation factor

- Chapter 3 NIST SP 800-171 Rev 1
  - states that Federal agencies may consider the contractor's system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization,
  - and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization.
  - NIST SP 800-171 Rev 1 – not structured to be a mandatory evaluation factor
  - Can be used to evaluate the overall risk
- Acquiring activity must state – how & whether NIST implementation will be used

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017
NIST SP 800-171 r1 page 9

Requirements for multiple individuals

- If multiple individuals in your company need access to the Technical Data Package (TDP) for a solicitation and an explicit
- access request is required, each individual MUST submit an explicit access request to be granted approval to view the TDP. Those
- same individuals MUST be registered in Federal Business Opportunities (FBO). Any individuals no longer with the company should be deleted. Questions related to registration in FBO should be directed to <deleted>
- Vendors are responsible for placing correct information in FBO.
- It is strongly suggested that you submit the explicit access request and provide the buyer with the completed Use and Non-Disclosure Agreement at the same time if the solicitation requires both to gain access to view the TDP.

Destruction notice

- Upon completion of the purposes for which Government Technical Data has been provided, the Contractor is

➢ required to destroy all documents, including all reproductions, duplications, or copies thereof as may have been further distributed by the Contractor.

➢ Destruction of this technical data shall be accomplished by: shredding, pulping, burning, or melting any physical copies of the TDP and/or deletion or removal of downloaded TDP files from computer drives and electronic devices, and any copies of those files.

Okay – now prove it!

Indications of a Cyber Incident

- Unusual/unaccounted for outbound traffic and between client networks.
- Privileged Account Anomalous usage
- User Account Activity from anomalous Ips
- Excessive failed logins
- Changes/large queries against web server pages
- Well known port vs. application usage
- Files – storage/transmission
- Other Web Browsing “spikes”

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 60-65

Situational Awareness – users - Phishing

- > eight million results of sanctioned phishing tests in 2015; multiple security awareness vendors
- 30% of phishing messages were opened by the target across all campaigns.
- About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed. The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds.
- The median time to the first click on the attachment was 3 minutes, 45 seconds

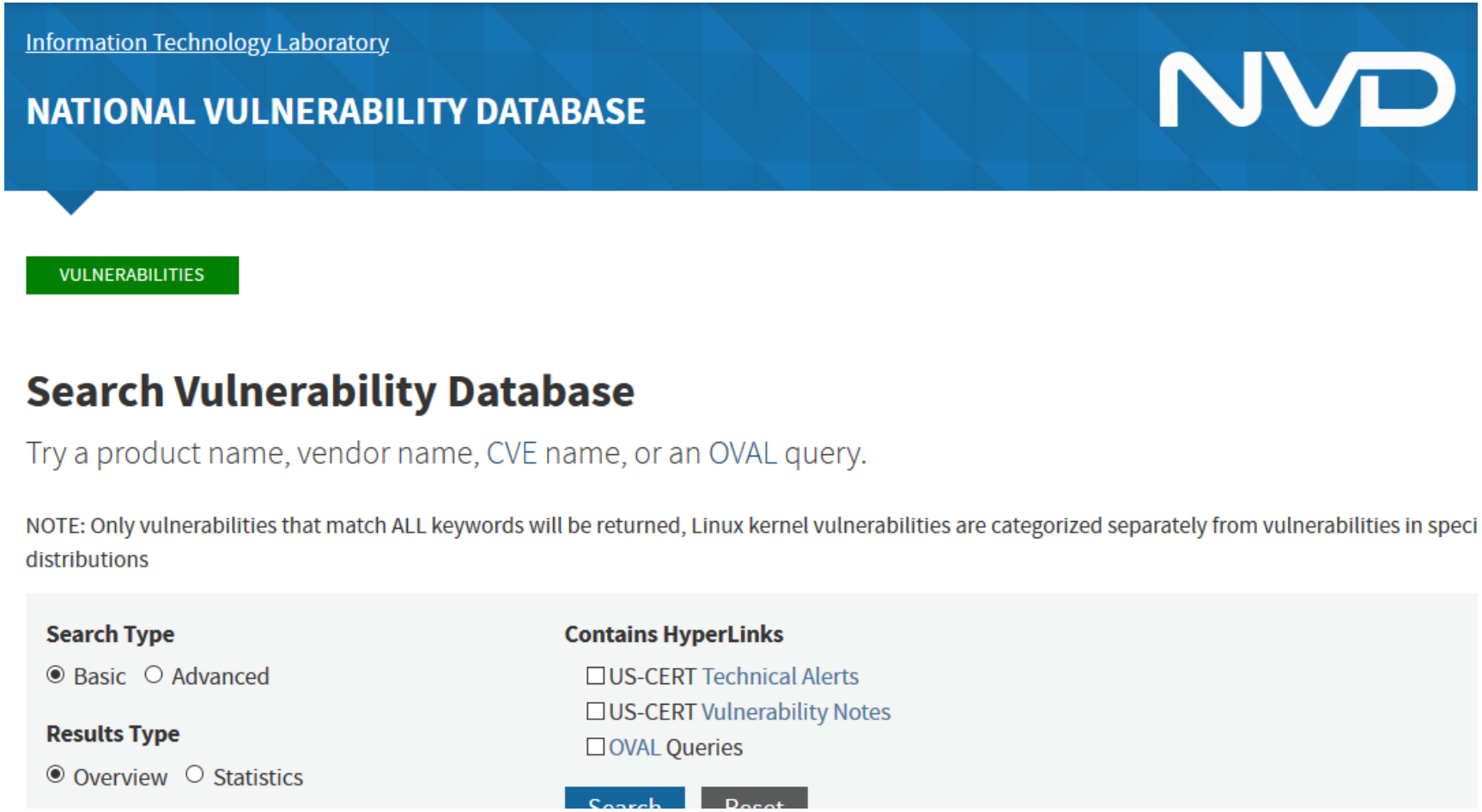
2016 Verizon, Data Breach Investigation Report, 18

Security - General principles

- Enable auto-software updates
- Install, use, & keep updated antivirus software**
- Avoid unsafe behavior – websites, opening links/attachments
- Follow the principle of least privilege
  - Create secondary, non-admin/root account
  - Admin accounts have universal privileges – malicious software needs this access

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

Identify tools



https://nvd.nist.gov/vuln/search

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**

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)

Other requirements

- *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information. (l)

Forensics – planning considerations

- Applicable laws
  - Wiretap Act (18 U.S.C. 2510-22)
  - Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
  - Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)
  - The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data. DFARS 252.204-7012
- May need to consult with an Attorney
- Plan
- Document
- Capture – save
- Reproducible

Create a 30 day action plan

- Review DFAR 252.204-7012
- Review NIST SP 800-171 Revision 1
  - Group requirements by difficulty/technical requirement
    - Administrative/current - green
    - Technical – will need outside assistance – yellow
    - Technical/investment - red
- Inventory resources
- Inventory information – stored and other (commercial & DoD)
- Prioritize plans required and development schedule

Office procedures

- Who has access to your network?
- Does each employee have their own computer?
- Are computers shared?
- Do all employees have access to all information?
- Are passwords used to protect folders and files?
- Are employees required to change their passwords?
- Does each computer have anti-virus software loaded and enabled?
- Are IT functions accomplished in-house or by a third party?
- Do you monitor your network?

Information handling requirements

- At what level – internally
- To what degree?
- Process for keeping current?
- How is information identified? - marked
- How is it stored?
- Is there one level – two – more?
- How is information shared?
- Are the processes tested? – how often? – by whom? – results?

Disposal

- 1/125” – that’s right! That’s the recommended size that a piece of a hard drive should be after destruction.
- Shredding (CD’s & DVD’s)
- Degaussing – hard drive
- Specialized services will disintegrate, burn, melt, or pulverize your HD
- Beware – do not
  - Use a microwave
  - Burn
  - Use chemicals
- Deleting
- Overwriting

U.S. DHS, US-CERT, Disposing of Devices Safely, 2012 Carnegie Mellon University. Produce for US-CERT

Personnel - partial

- **3.2.1/3.2.2** Are employees provided any IT training?
  - New hires
  - Current
- **3.9.1** Are employees screened prior to granting access to the IT system?
- **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- **3.1.7** Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?
  - **3.1.19** Encrypt CUI on mobile devices and mobile computing platforms.
- **3.9.2** Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Business Continuity Plan

- Identify critical functions
  - Redundancy
  - Training
  - Current information
  - Appropriate/acceptable authorization in place
- Evaluate (S, W, O, T)
- Identify critical vendors
- Succession planning
- Continuing if there is not access to computes/internet
- Bitcoin account – separate computer

Key Documents – information, ready access Partial list

- Diagrams – perspective, context, understanding
- Critical Asset, Data and Services list
- Business Continuity Plan
- Incident Response Plan
- Data and Info disclosure Procedures
- Physical access Requirements
- On call/contracted resource
- Disaster Notification Guidance
- Actions Taken log

Alan White and Ben Clark, BTFM – Blue Team Field Manual, 2017, 9

Security Software

- Antimalware Software
- Intrusion Detection and Intrusion Prevention Systems
- Remote Access Software
- Web Proxies
- Vulnerability Management Software
- Authentication Servers
- Routers
- Firewalls
- Network Quarantine Servers

NIST SP 800-92 Computer Security and Log Management, 2.1.1 page 2-2

Monitor systems & Audit records

3.14.6 Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7 Identify unauthorized use of organizational systems.

3.3.1 Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Develop Resources – references & SME/S

Image copied from: innovation.ed.gov

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

- November 5, 2019

  Services Contracts with Federal Agencies
  CLICK HERE for additional information
  Presented by Carol Murphy, Wisconsin Procurement Institute (WPI)

- November 6, 2019

  Key Ideas Associated with CUI Requirements and DFARS 232.204-7012
  CLICK HERE for additional information – presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- 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)

ACQUISITION HOUR LIVE WEBINARS SERIES

- December 3, 2019

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

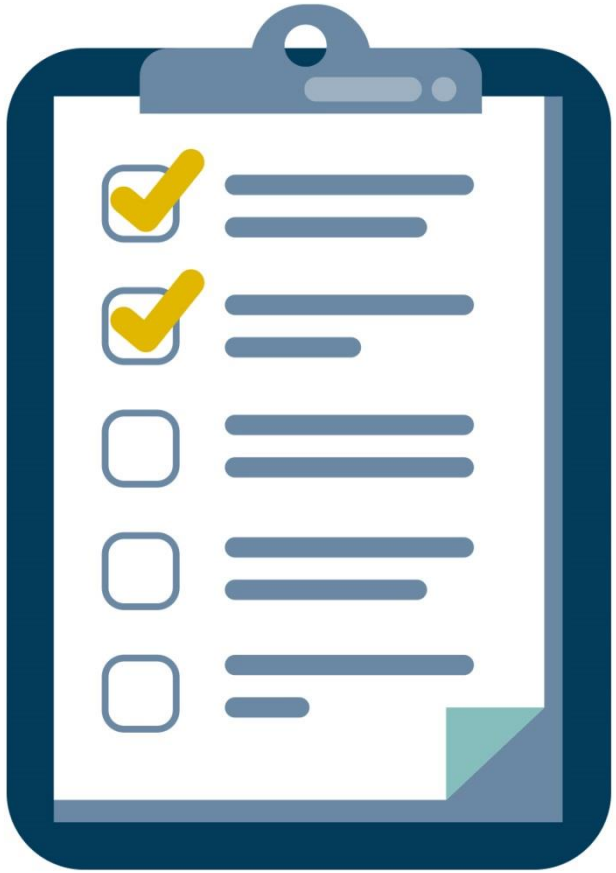
- December 10, 2019

  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