Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

INTEGRATING DFARS REQUIREMENTS INTO YOUR DAY-TO-DAY CYBER PRACTICES

(CYBER SECURITY SERIES PART 2 OF 5)

ACQUISITION HOUR WEBINAR

October 16, 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!

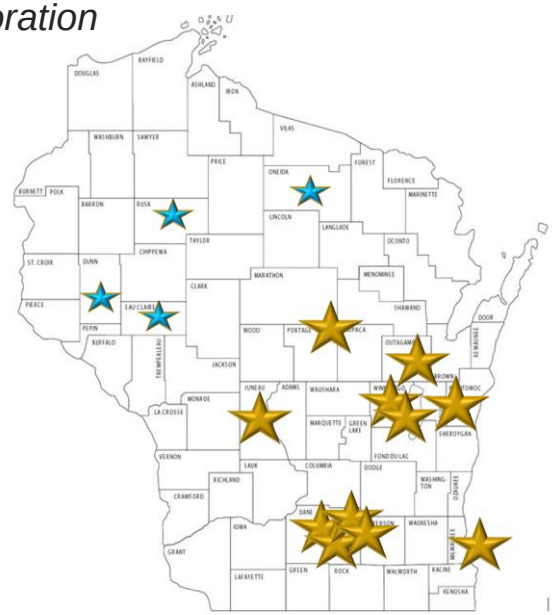
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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

Integrating DFARS Requirements Into Your Day-to-Day Cyber Practices

Marc N. Violante

Wisconsin Procurement Institute

October 16, 2019

Develop a Project Plan

- Determine the end point – the goal
- Assemble resources
  - DFARS 252.204-7012
  - NIST 800-171 r1
  - NIST 800-171 A
  - Company – hardware
  - Company – software
  - Company – POC's
- Create a timeline & budget
- Define and prioritize risks
- Specify information/documentation to develop and/or compile

Official website of the Department of Homeland Security

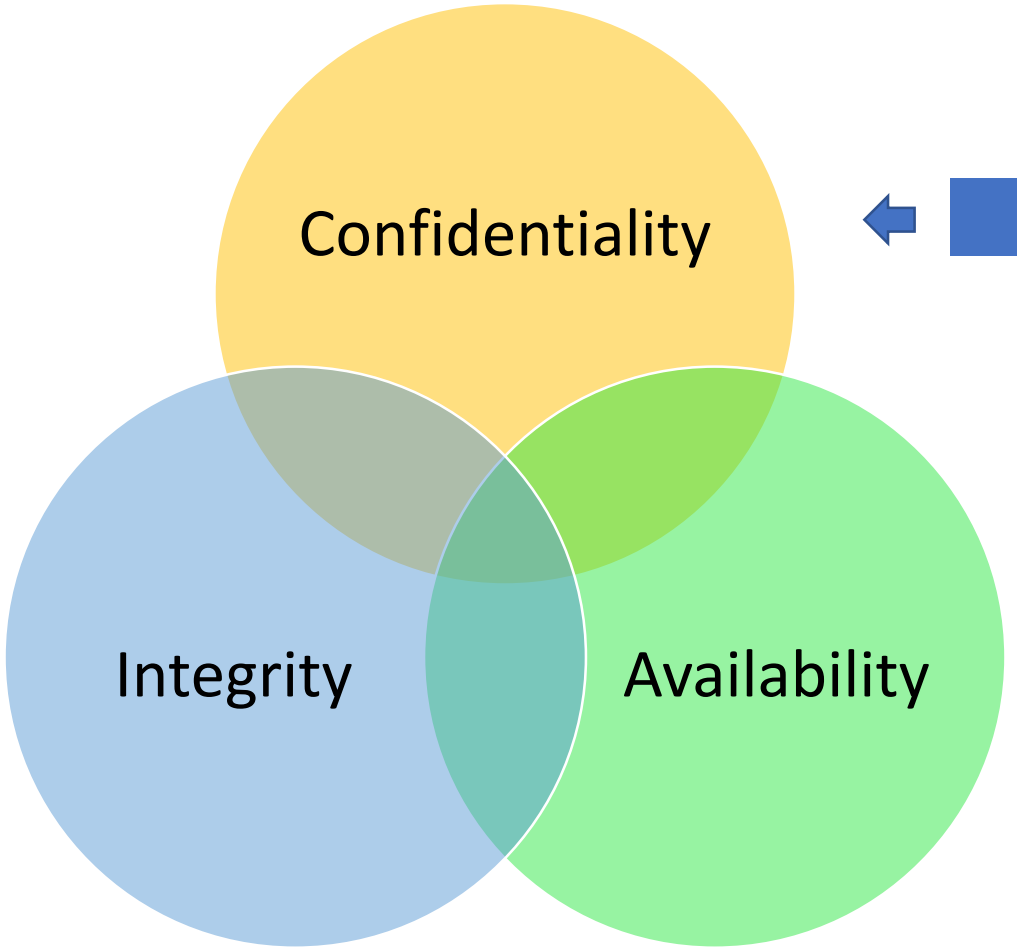
US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

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?

Threat target areas / Protection schemes



Focus of NIST 800-171 r1

Use standard/accepted descriptions

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.

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

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)

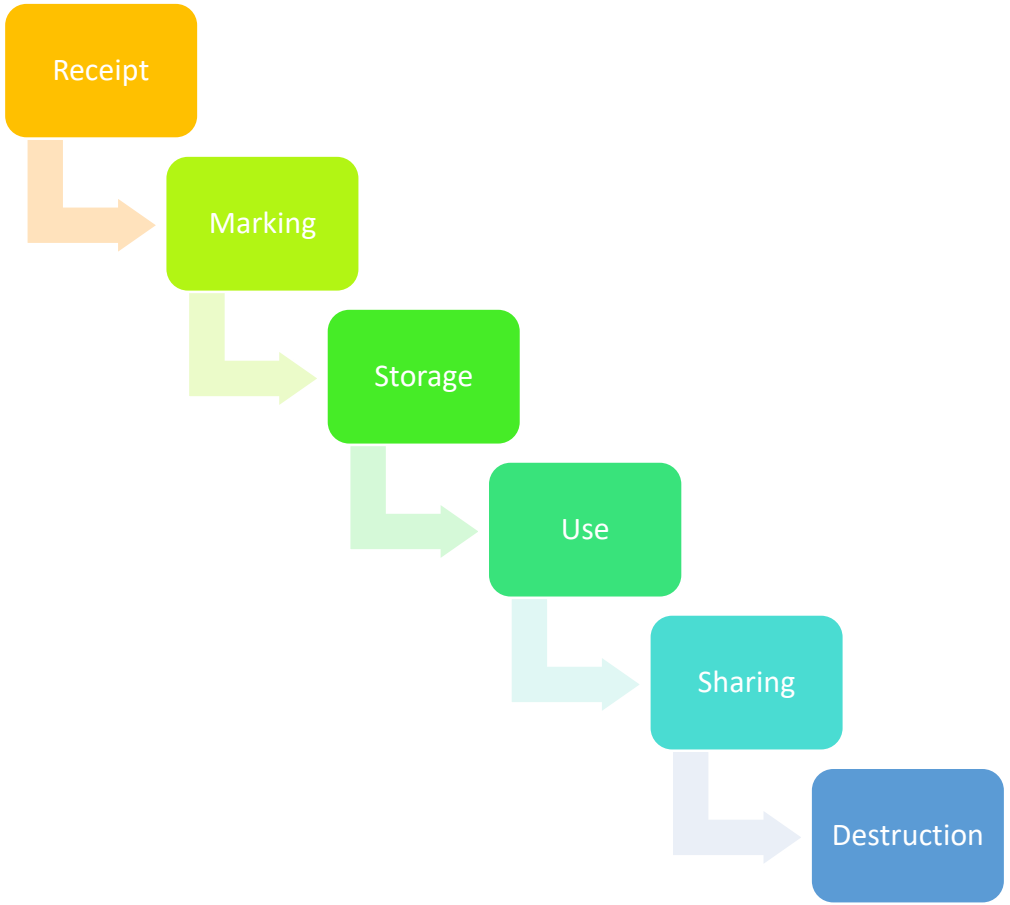
Become familiar with the requirements

- Clause 52.204-21 (Federal Contract Information)
- Clause 252.204-7008 (Attestation – implementation of 800-171 r1)
- Clause 252.204-7012 (CUI – CTI/CDI)
  - Adequate security – NIST 800-171 rev 1
  - Monitor for Malware, capture, defang, send to KO
  - Identify incidents
  - Forensic investigation, report within 72 hours
  - System image for up to 90 days
  - Flow-down only when required

Don’t over-complicate the requirements

- System Security Plan
- New house
  - Change locks
  - Basketball hoop – garage keypad – change code
  - Shrubbery overgrown windows – trim for visibility
  - House number not visible from street – police/fire
  - Backyard & side – dark; add lighting

Information – life-cycle, general elements



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

Assess your system

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.

Collect/Identify current processes

- Systems
- Passwords
- Configurations
- Software / Data / Licenses
- Vendors / Contractors
- Staff assignments
- Training – training files

Communication channels

- Location – work station, conference room, public area
- Network
- Hardwire – USB
- CD
- Removable drive
- Thumb drive
- WiFi – footprint/availability – does it need to be on 24/7?
- Remote access

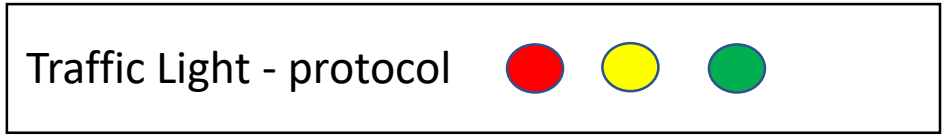
How do you know?

- - only authorized users have accessed the network?
- - information requiring destruction was destroyed appropriately?
- - email/ftp/other digital communications were handled correctly?
- - there is no malware on the network / computers / devices?
- - there have been no reportable incidents?
- - all other issues

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

Review the details

- **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.

NIST 800-171 r1

- 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

Identify Information & Requirements

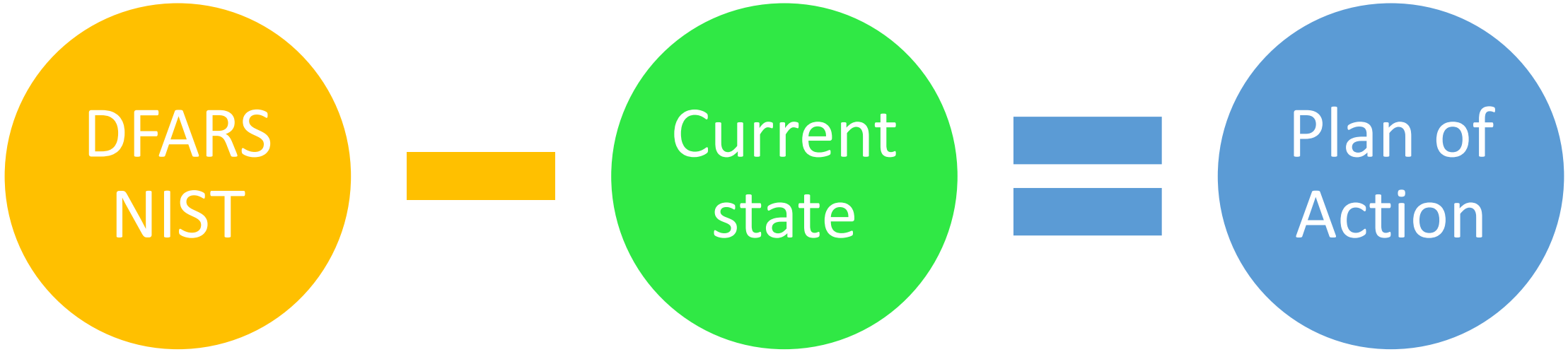
- Review information (prints, TDP, other)
- Determine
  - Program affiliation – ITAR, JCP, EAR, CUI, CUI – program, other
  - Marking
  - Handling – restrictions/limitations
  - CUI Control requirements – CUI Basic/CUI Specified
  - Decontrol
  - Destruction requirements
  - Contract retention requirements

Assess

NIST Item	Applies completed	Applies not completed	In progress	Not applicable
Security Plan				
Plan of Action				
	1			
	1			
		1		
	…	…	…	…
				1
			1	
Total	sum_a	sum_b	sum_c	sum_d

$$\boldsymbol{sum_a + sum_b + sum_c + sum_d = 110}$$

Document System Security Plan



Conduct System Security Plan review

Copied from Google search: infrared heat loss image

Starting point – key questions – ID Risks

- What are we trying to protect?
- What are the threats?
- How do we detect them? (the threats)
- How do we respond?

Crafting the InfoSec Playbook, Security Monitoring and Incident Response Master Plan, J. Bollinger, Enright & Valites; O'Reilly Media Inc, pg 16

Create awareness at all levels

- For example, while more than two thirds (67%) of SMBs experienced a cyberattack in the last year,
- only a small fraction (7%) of CEOs, corporate chairs and owners think a cyberattack is “very likely.”
- Conversely, nearly half (43%) of top leadership believe an attack is “not at all likely” – higher than any other management group surveyed.

https://www.forbes.com/sites/suzannerowankelleher/2019/10/09/why-ceos-of-smbs-make-easy-cyber-targets/#359c5cde7808

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 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf pg 6

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

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

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

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.

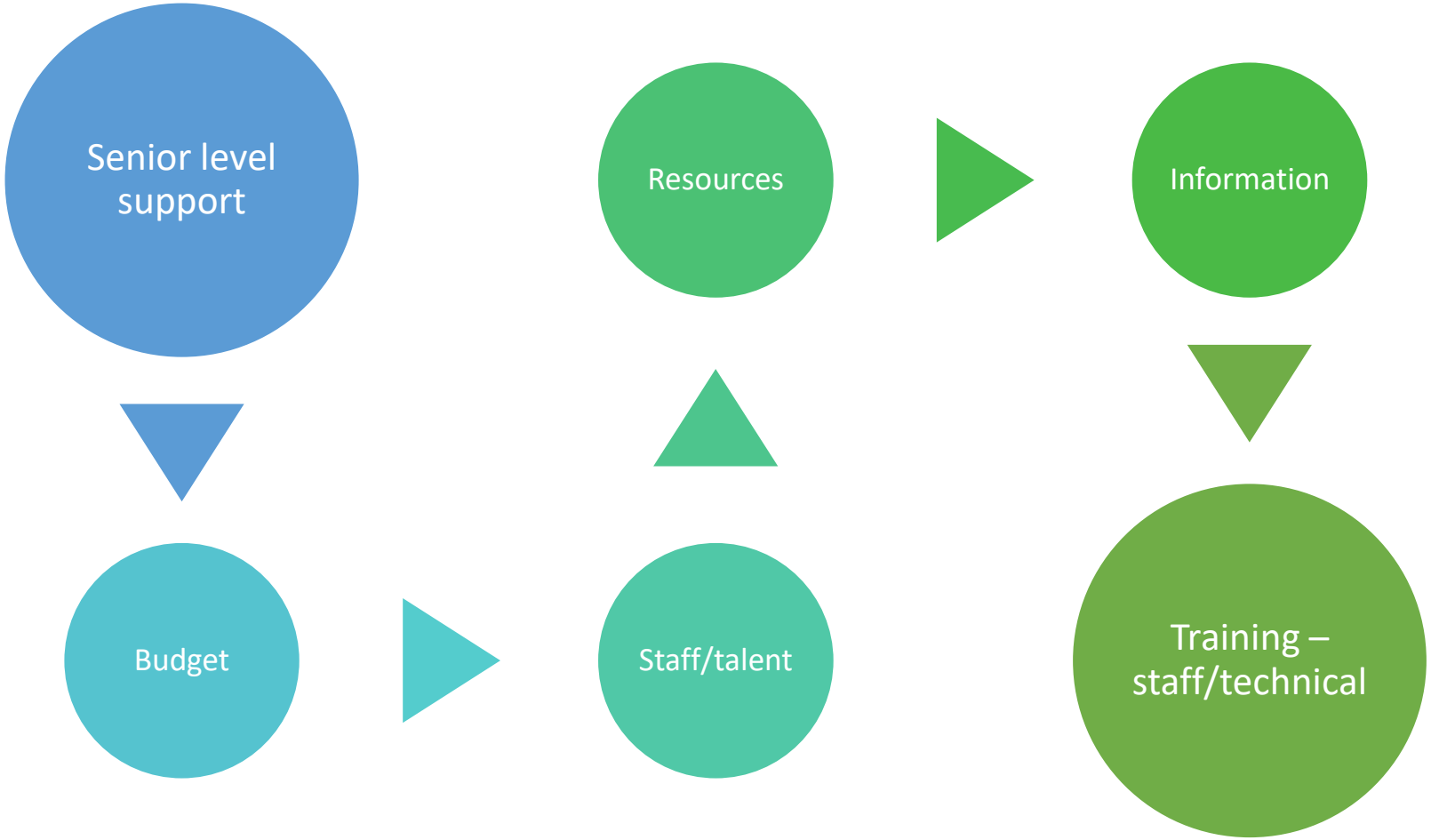
Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

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

Identify key elements- what is needed?



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

Sort to Broader categories –

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

NIST 800-171 (3.1 Access Control) example

Basic Security Requirements

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements

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

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

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 capture the execution of such functions in audit logs.

3.1.8 Limit unsuccessful logon attempts.

3.1.9 – 3.1.22 Not shown

Translation process

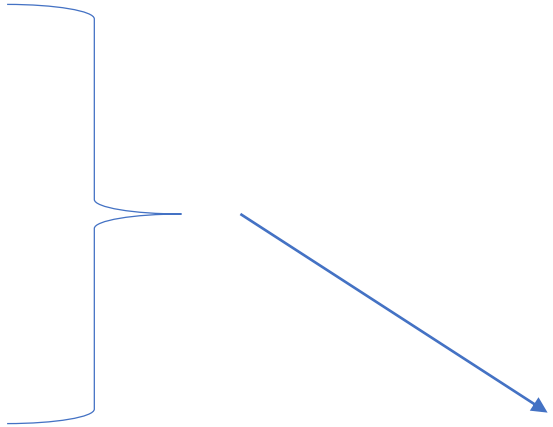
Company Information

NIST 14 Family Members

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

Example - Recipes

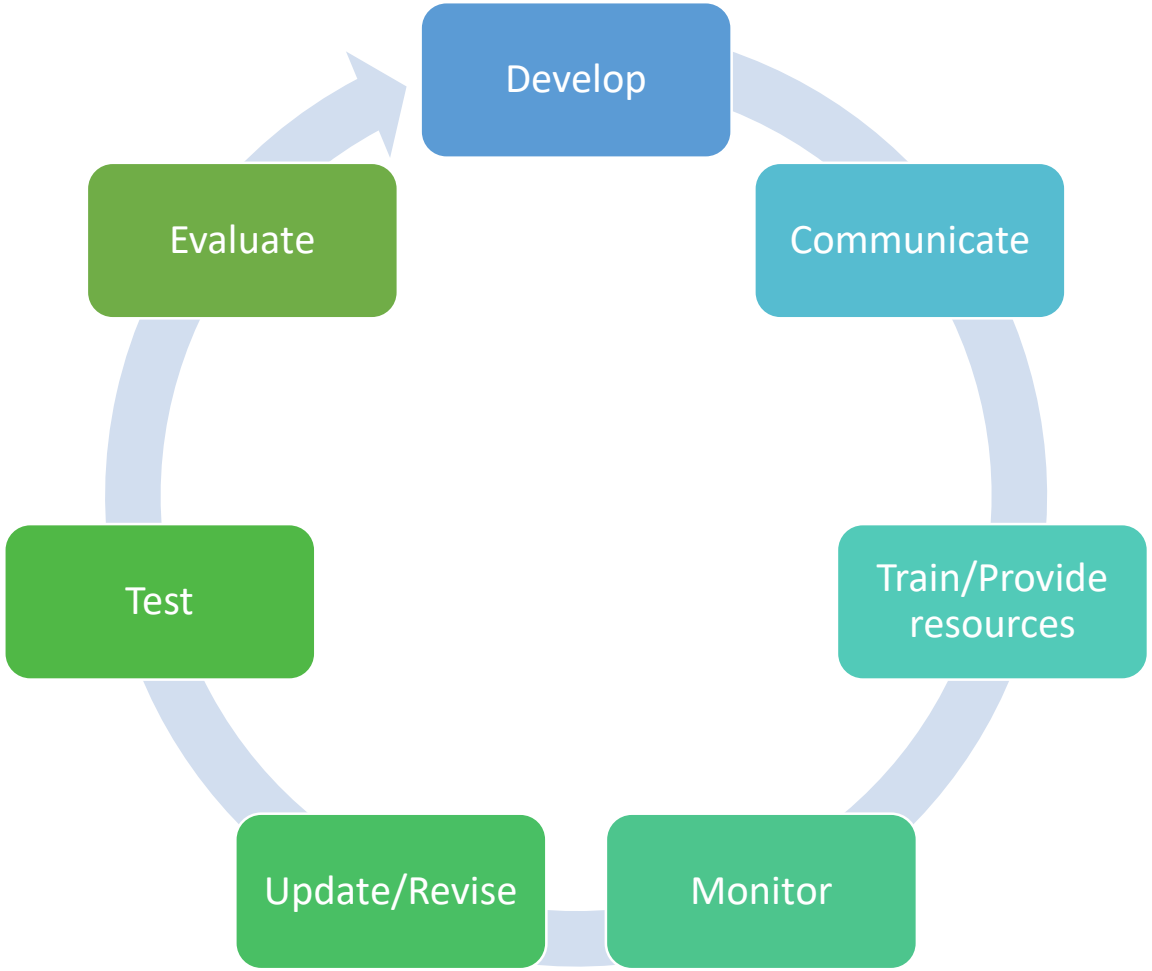
- Family recipe cards
  - Add some butter
  - Dash
  - Lightly salt
  - Pinch
  - Splash
  - Sprinkle



- Published cookbook
  - Add 2 table spoons of butter
  - Add 1/8 cup of …
  - etc

Translate

Include Active Involvement - test|check|verify



Create a Culture of Awareness

https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield - **The National Counterintelligenceand Security Center**

DON Review / Report – some findings

- ***Annual training was "far too basic***
- Annual training philosophy - one-size-fits-all"
- It "underemphasizes the realities of the cyber threat" to the point that "the workforce is led to believe that cybersecurity is simply a matter of routine compliance
- (Routine compliance) enables seeing security practices such as password protection and email vigilance as needlessly burdensome."

https://fcw.com/articles/2019/05/07/navy-cyber-sanctions-williams.aspx

Stay aware & up to date (password spraying)

- Use SSO or web-based applications with federated authentication method
- Lack multifactor authentication (MFA)
- Allow easy-to-guess passwords (e.g., “Winter2018”, “Password123!”)
- Use inbox synchronization, allowing email to be pulled from cloud environments to remote devices
- Allow email forwarding to be setup at the user level
- Limited logging setup creating difficulty during post-event investigations

Brute Force Attacks Conducted by Cyber Actors https://www.us-cert.gov/ncas/alerts/TA18-086A

Passwords – how did they know?

- “Users have long been considered the weakest link of any security system[25-28]. Across different authentication schemas users tend to choose passwords, which are easy to remember, and so are easy to guess. “
- It has been shown [5] that user's passwords can be grouped into four broad categories: family oriented, fans, fantasies, and cryptic.
- "Family oriented" users, which comprise 47.5% of users, select their own name or last name or other personal information such as pet or child's name as their password. Those are usually less experienced computer users.

Analyzing User Password Selection Behavior for Reduction of Password Space; Roman V. Yampolskiy Department of Computer Science and Engineering and IGERT in GIS University at Buffalo, Buffalo, NY 14260, USA rvy@buffalo.edu

Passwords – general selection biases

TABLE 7
TOPIC PREFERENCES BY GENDER

User	Female	Male
Animals	20.8%	10.4%
Cars	14.6%	17.9%
Women	6.3%	13.6%
Food	14.6%	11.0%
Children	8.3%	6.8%
Men	4.2%	4.6%
Objects	12.5%	11.0%
Nature	14.6%	17.2%
Sports	4.2%	7.5%

TABLE 8
TOPIC PREFERENCES BY RACE

User	Asian	Hispanic	White
Animals	10.7%	12.5%	12.5%
Cars	18.6%	12.5%	16.8%
Women	11.4%	25.0%	13.0%
Food	11.4%	12.5%	11.5%
Children	8.6%	0.0%	6.3%
Men	4.3%	12.5%	11.5%
Nature	17.1%	12.5%	11.1%

Utilizing the demographic information presented above for the easiest 10% of passwords, which belonged to Asian males, it was shown to be possible to break the Story authentication mechanism in just twenty attempts [18].

Analyzing User Password Selection Behavior for Reduction of Password Space; Roman V. Yampolskiy Department of Computer Science and Engineering andI GERT in GIS University at Buffalo, Buffalo, NY 14260, USA rvy@buffalo.edu

Example - passwords

- “in fact, the password that turned up the most was the same: According to the NCSC’s global breach analysis, 23.2 million of those hacked worldwide used the password “123456”. “
  - UK’s National Cyber Security Center (NCSC)
- **The 20 most used passwords (partial)**
  - 123456 (23.2m)
  - 123456789 (7.7m)
  - qwerty (3.8m)
  - password (3.6m)
  - 1111111 (3.1m)
  - 12345678 (2.9m)

https://www.forbes.com/sites/kateoflahertyuk/2019/04/21/these-are-the-worlds-most-hacked-passwords-is-yours-on-the-list/#26c614cb289c

Reduce variables

- Provide training
- Communicate
- Identify & classify system v. individual requirements
- Reduce individual efforts
- Maximize use of system/network level solutions
- Minimize target surface
- Security at the individual level = each individual has to maintain
- Managed security reduces the number of risks

Tailor solutions for the need – eg. encryption

- Use Case 1 – Sharing a Laptop
- Use Case 2 – Transferring Files Between Computers
- Use Case 3 – Sharing Data with Contractor
- Use Case 4 – Traveling with a Laptop
- Use Case 5 – Traveling with a Dual-Boot Laptop

NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices.
If the data is encrypted – how is the paper protects?

“It’s always been that way” may signal trouble

- Visitors
  - Sales/marketing
  - Temporary employees
  - Visiting engineer
  - Customer
  - Prospective customers
  - Contract Services – repair, janitorial, suppliers, OEM, other
  - Friends/family
  - Others

Develop – assemble resources

- **7 SMB Security Tips That Will Keep Your Company Safe**
  - Identify the Company's Most Sensitive Data
  - Protect Company Data by Performing Frequent Updates
  - Create a Cybersecurity Culture
  - Have a Plan for When a Security Event Happens
  - Consider a Managed Security Service Provider
  - Focus on Standards Compliance and Certification
  - Use Stronger Passwords and MFA

https://www.darkreading.com/endpoint/7-smb-security-tips-that-will-keep-your-company-safe----------/d/d-id/1336067?image_number=1

Build cyber into your workforce

- Training
  - Baseline
  - Annual/periodic
  - New hire/New position, responsibility, retiring, termination
- Awareness
- Determine access requirements
- Determine unique needs of position/assignment
- Test: Phishing – 3rd party
- Social Engineering

Develop threat information

- ISAC – Information Sharing and Analysis Center – Industry specific
- Infragard – FBI – Corporate association
- U.S. Cert – publications/notifications
- Industry groups

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

- October 29, 2019

  Changes, delays and disputes in federal construction contracts
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute (WPI)

- October 30, 2019

  Cyber Security for Current and Prospective DOD Contractors and Subcontractors
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- 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)

MARKETPLACE WISCONSIN

Governor's Conference on Diverse Business Development

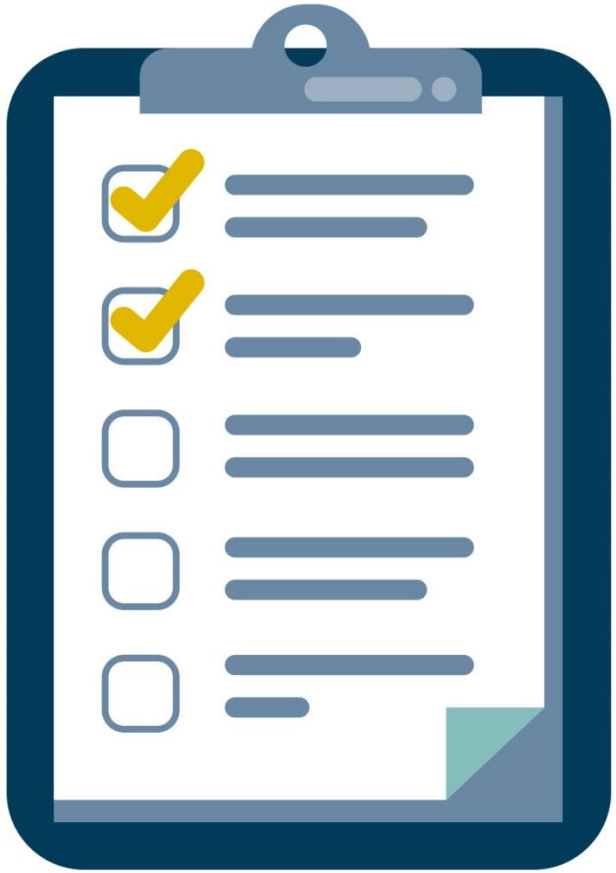
OCTOBER 23-24, 2019
POTAWATOMI HOTEL & CONFERENCE CENTER
MILWAUKEE

www.marketplacewisconsin.com

QUESTIONS?

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

SURVEY



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