Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

INTEGRATING DFARS INTO YOUR DAY-TO-DAY CYBER PRACTICES ACQUISITION HOUR WEBINAR

June 25, 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

SERVING WISCONSIN COMPANIES FOR 31 YEARS!

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

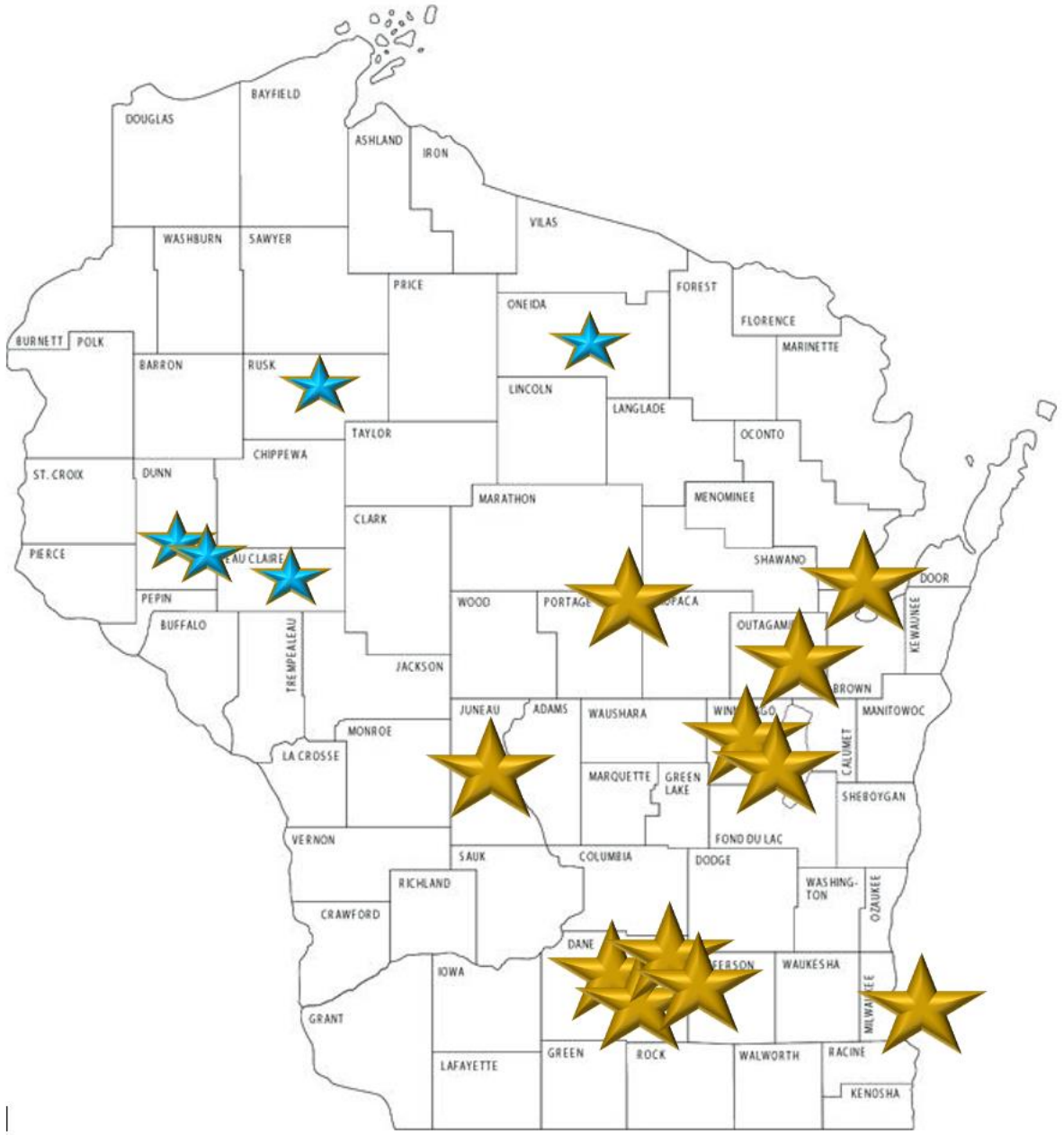
Assist businesses in creating, development and growing their sales, revenue and jobs through Federal, state and local government contracts.

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

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*
- CAMP DOUGLAS– *Juneau County Economic Development Corporation (JCEDC)*
- STEVENS POINT – *IDEA Center*
- GREEN BAY - *Advance Business & Manufacturing 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*
  - *UW Stout - Manufacturing Outreach Center*
- LADYSMITH – *Indianhead Community Action Agency*
- RHINELANDER – *Nicolet Area Technical College*



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

UPCOMING EVENTS

TUE 25
Acquisition Hour: Integrating DFARS Requirements Into Your Day-to-Day Cyber Practices
June 25 @ 1:00 pm - 2:00 pm

WED 26
Acquisition Hour: Current Trends in Department of Defense Acquisition
June 26 @ 12:00 pm - 1:00 pm

JUL 09
Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)
July 9 @ 1:00 pm - 2:00 pm

JUL 18
2nd Annual Building Your Business – Developing the Tools for Growth and Success for Native and Tribal Small Businesses
July 18 @ 8:30 am - 12:00 pm
Hales Corners

View More…

CURRENT OPPORTUNITIES (4)

SERVICES OFFERED BY WPI

- FREE Bid Matching Services
- Individual Counseling and Assistance
- Locating Local, State and Federal Opportunities
- Government Market Strategy Development
- Training in use of Government websites and tools
- Assistance with System for Award Management (SAM) Registration
- Assisting in Market Research Process
- Development of Market Profile
- Small Business Subcontracting Plans Development, Outreach and Reporting
- Small Group Training
- Outreach and training with Local, State and Federal agencies
- Assist with Pre and Post Award Functions
- Assistance with Agency Specific Contracting Requirements
- Assistance with Contracting Regulations and Requirements, including FAR, DFAR, CFR
- Assistance with GSA Schedule Preparation and Administration
- Assistance with Local, State and Federal Certifications, including:
    - Service Disabled & Veteran Owned Small Business, HUBZone, Woman Owned Small Business, 8(a) Business Development Program
    - State
    - Local
    - DBE
- Bid review and Submission Assistance
- Proposal review and Submission Assistance
- Capabilities Statement and Related Government Marketing Material Development
- Assistance in Locating and Developing Teaming Partners and Subcontractors
- Updated Government Market Information

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

Marc N. Violante

Wisconsin Procurement Institute

June 25, 2019

DFARS- general requirements (review)

- Clause 252.204-7008
- Clause 252.204-7012
- 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

Leakage – heat loss or information loss?

Copied from Google search: infrared heat loss image

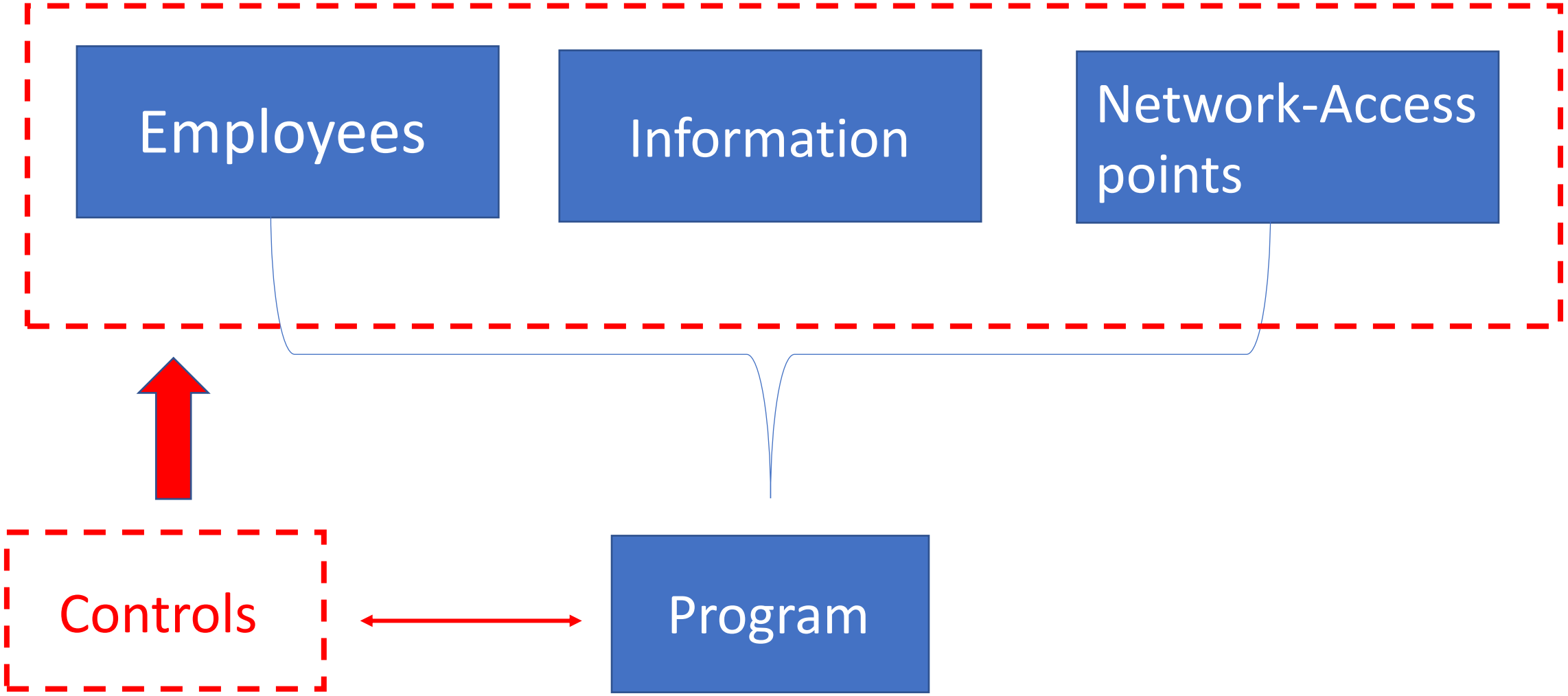
Starting point – key questions

- 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

Identify key elements- what is needed?

Security – top level factors



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

Create-Drive the importance

- Seal Belts
- Thunder
- Water on road
- It won’t happen to me!
- It cost’s too much
- I’ll let them worry about that
- That’s not important

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

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

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

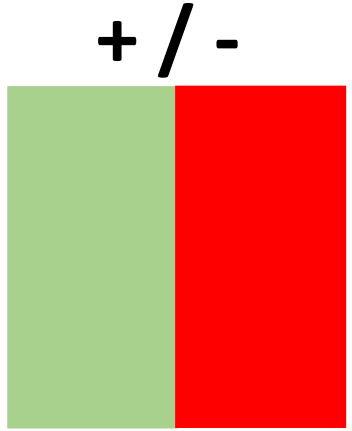
5 Questions CEOs Should Ask About Cyber Risks

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?

General Approach

- Company processes and procedures
- NIST - Requirement

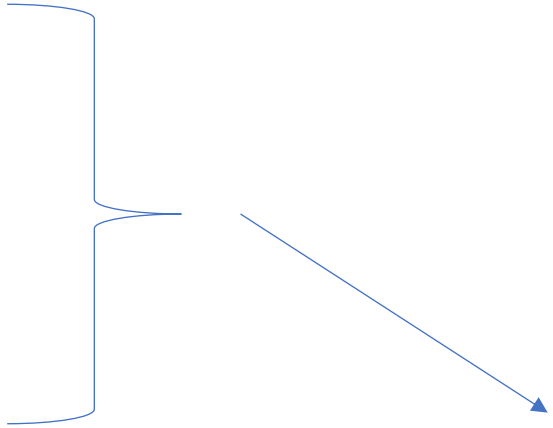
MAP into common vocabulary - NIST



Compare

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

Assess your system

What data/information is on your computer?

On your Network?

What devices are being used?

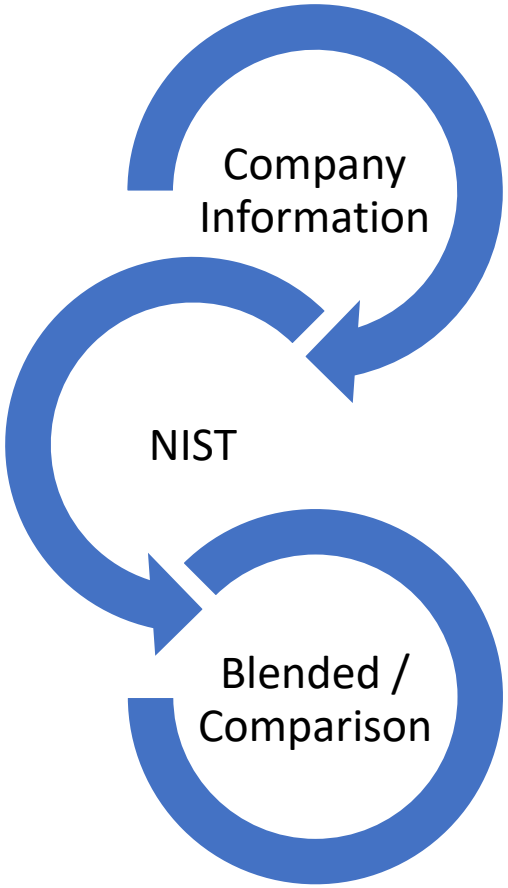
What are the entry points?

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


Company Information
NIST
Blended / Comparison

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

Family member

Specifics

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.

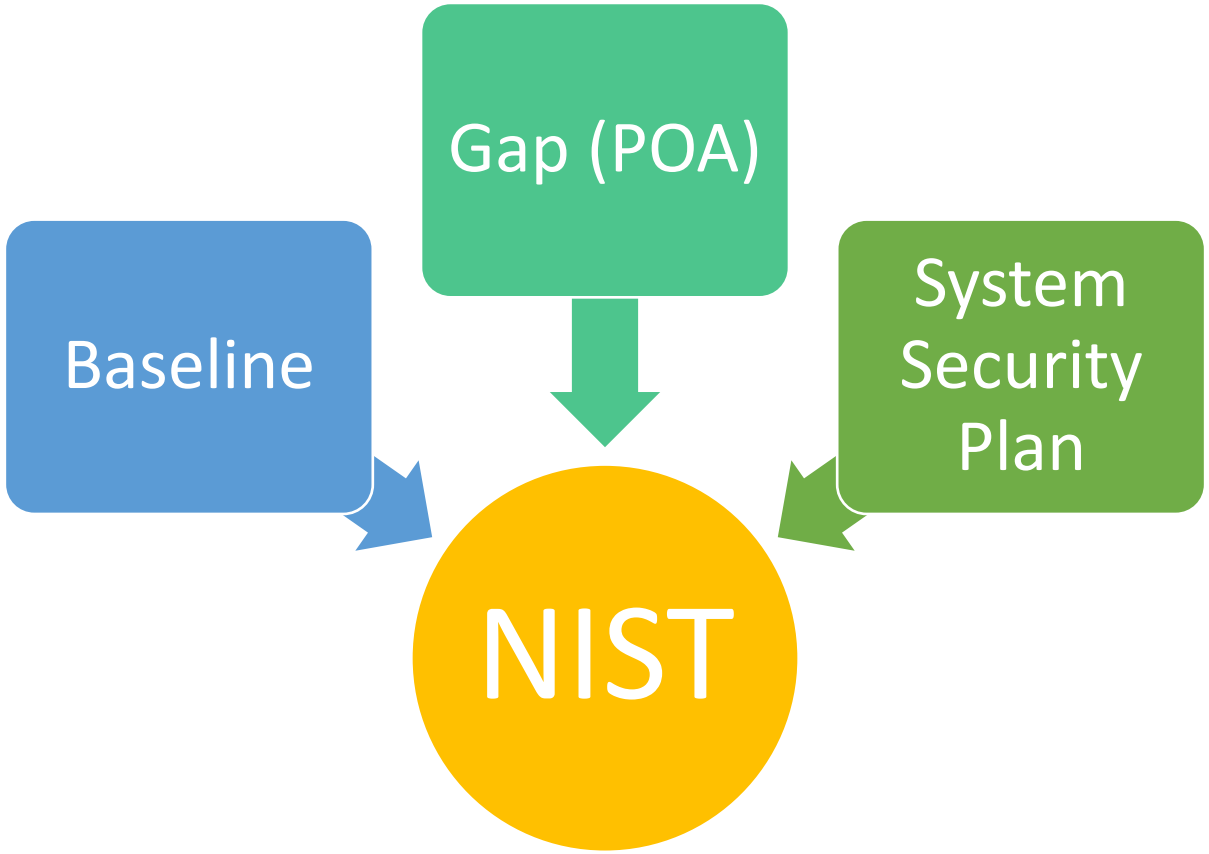
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

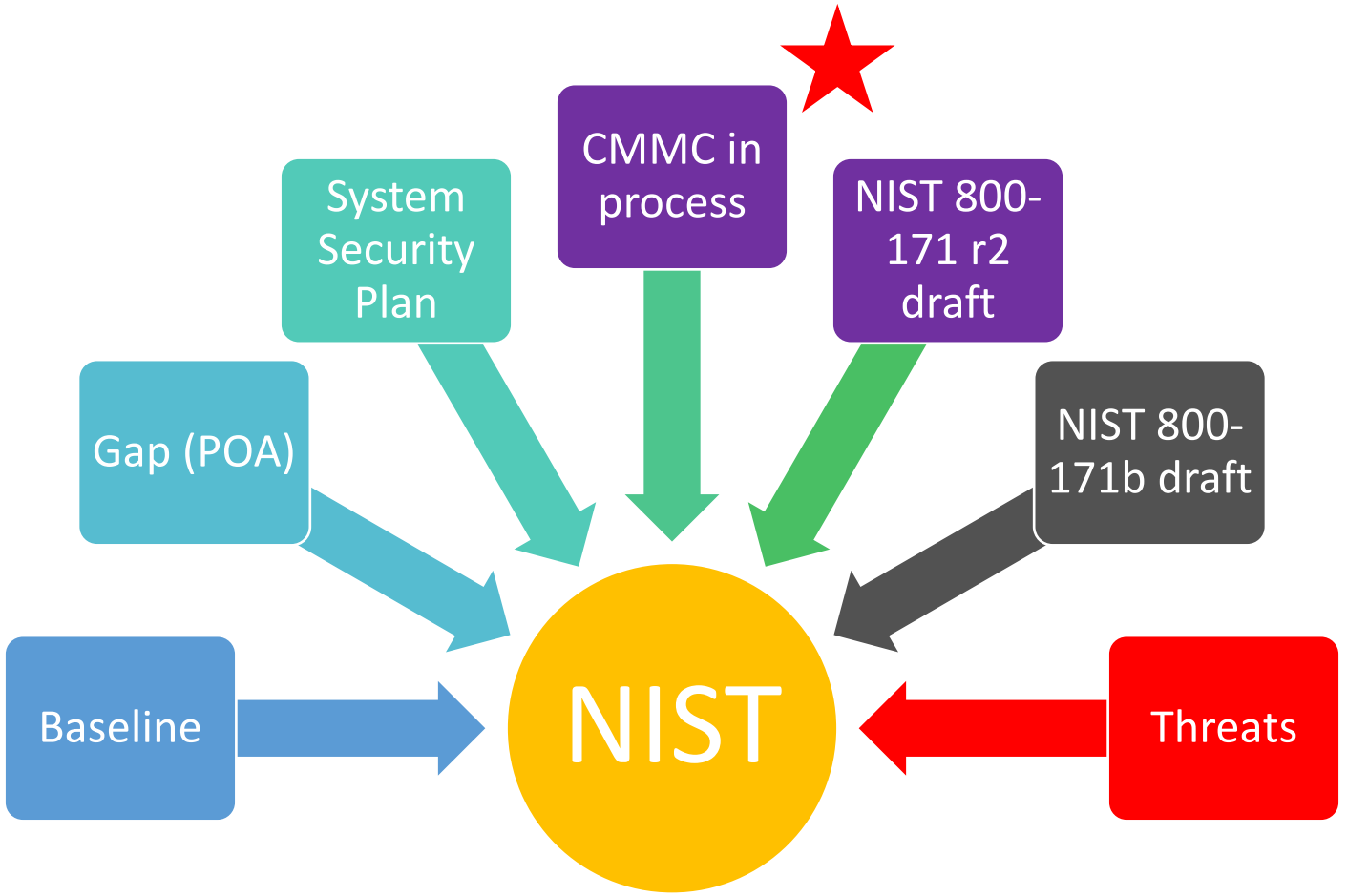
3.1.8 Limit unsuccessful logon attempts.

3.1.9 – 3.1.22 Not shown

Establish a baseline – NIST terminology



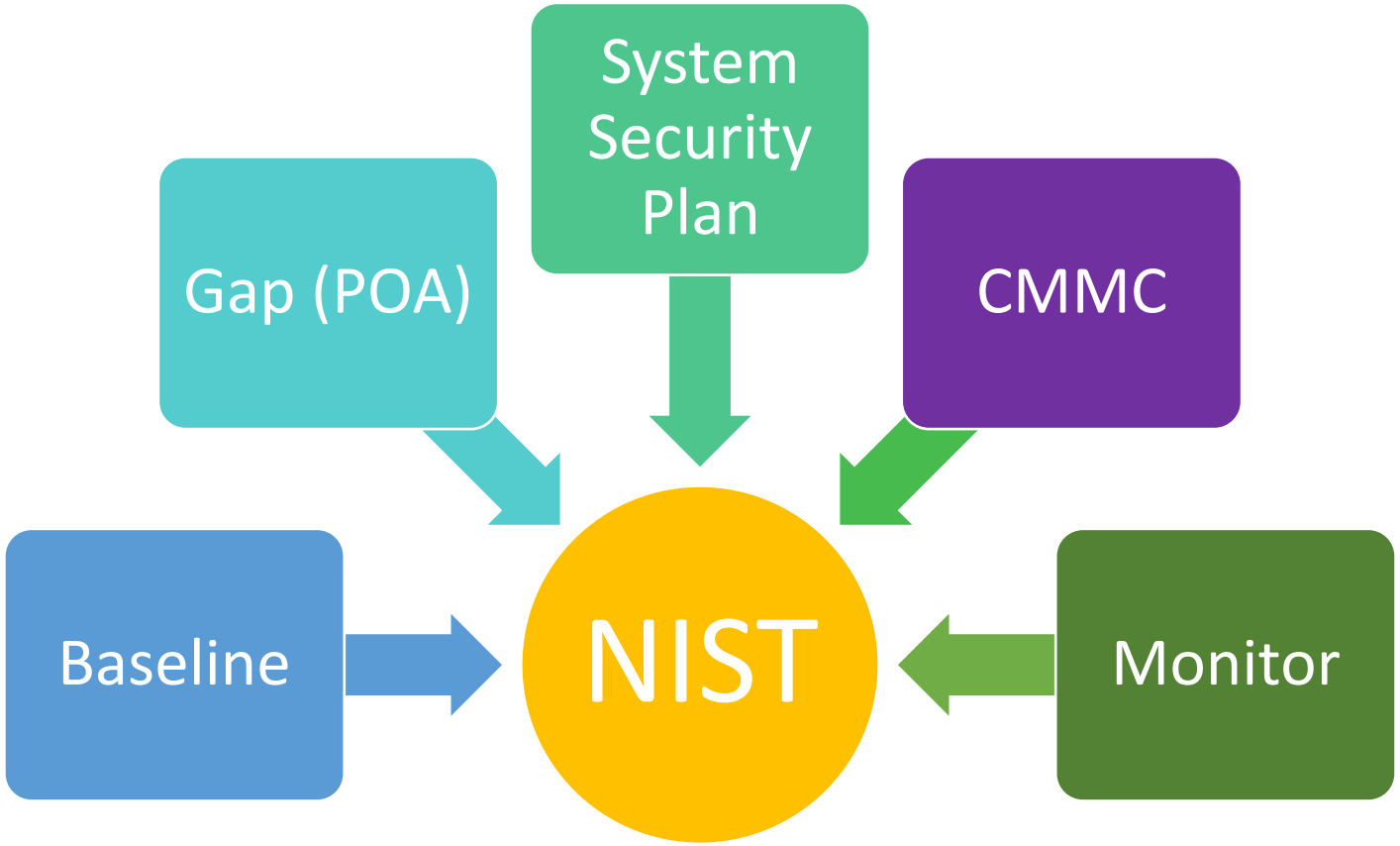
Design in – Flexibility - monitor



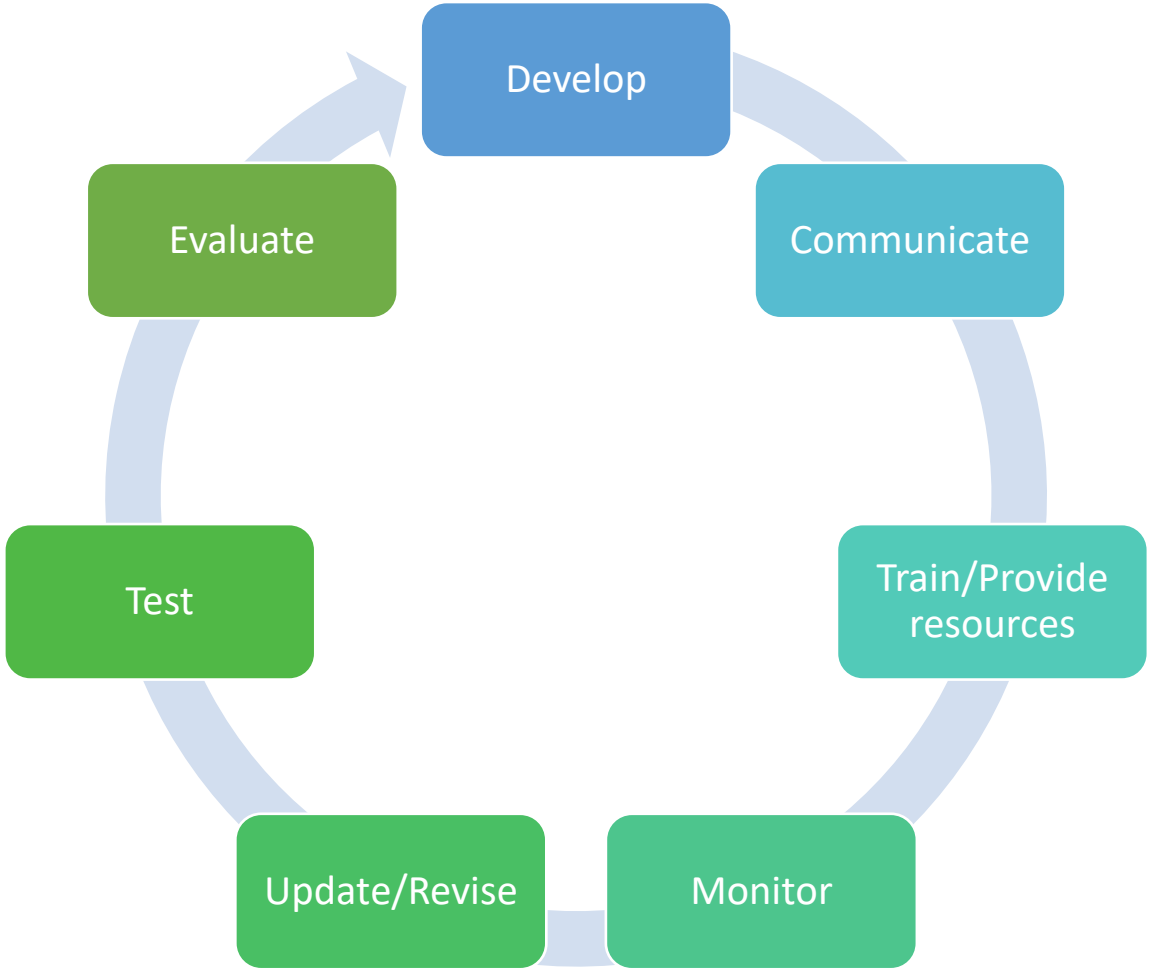
CMMC – on the horizon

- Cybersecurity Maturity Model Certification
- DoD – driven, self-attestation is not working, too much “leakage”
- Developed by Johns Hopkins & SEI Carnegie Mellon
- Five levels – (1) basic cyber hygiene - (5) 24 x 7 monitoring/response
- Each notice will designate level (1 -5)
- Contractor eligibility – Go / No-go Certified/Not-certified
- Listening sessions (11) – this summer
- Initial publishing of program this summer

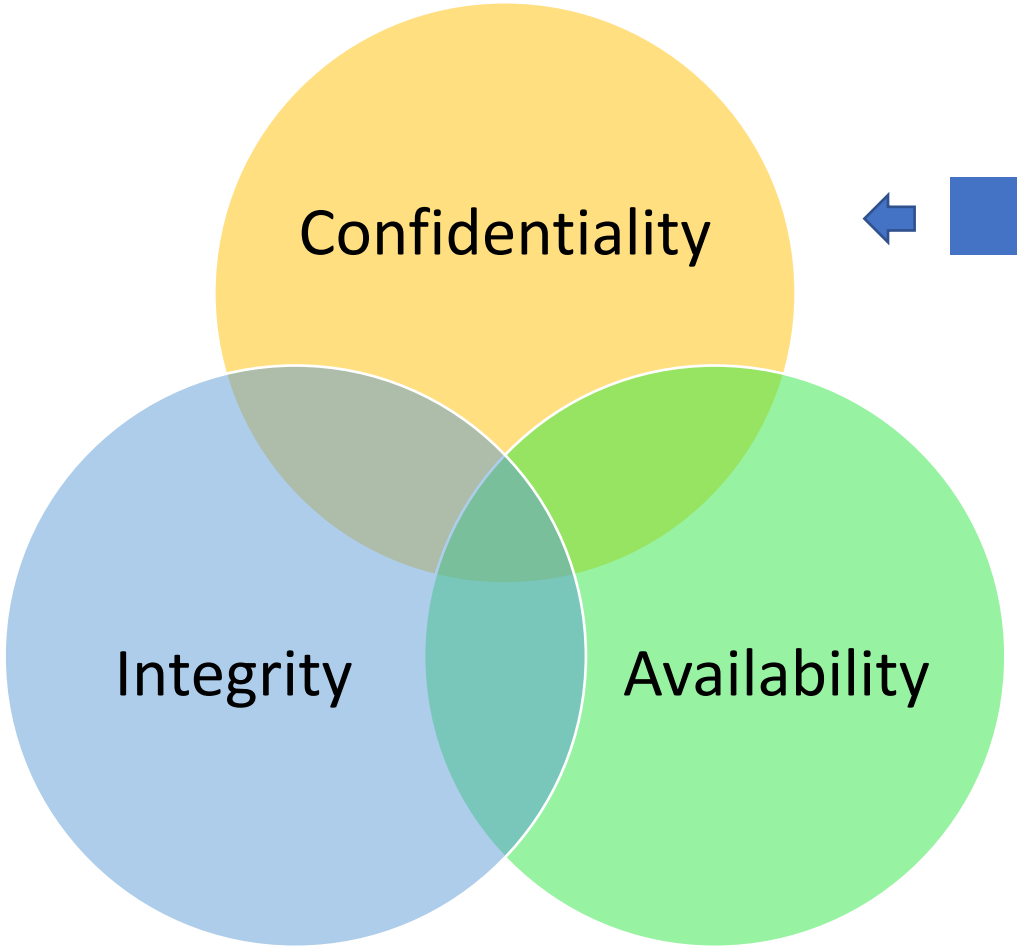
Monitor -



Include Active Involvement - test|check|verify

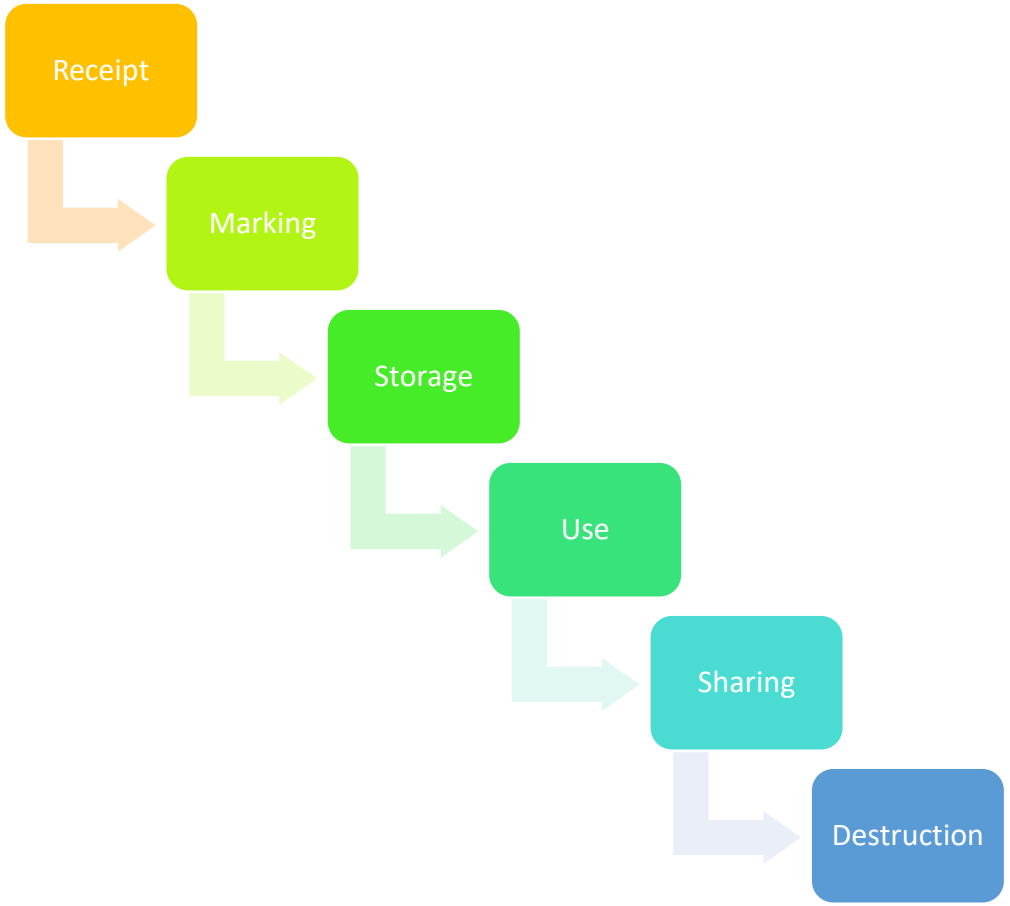


Threat target areas / Protection schemes



Focus of NIST 800-171 r1

Information – life-cycle, general elements



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

Get technical!

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 – what is the risk?

- “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

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

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

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 the solution for the need - encryption

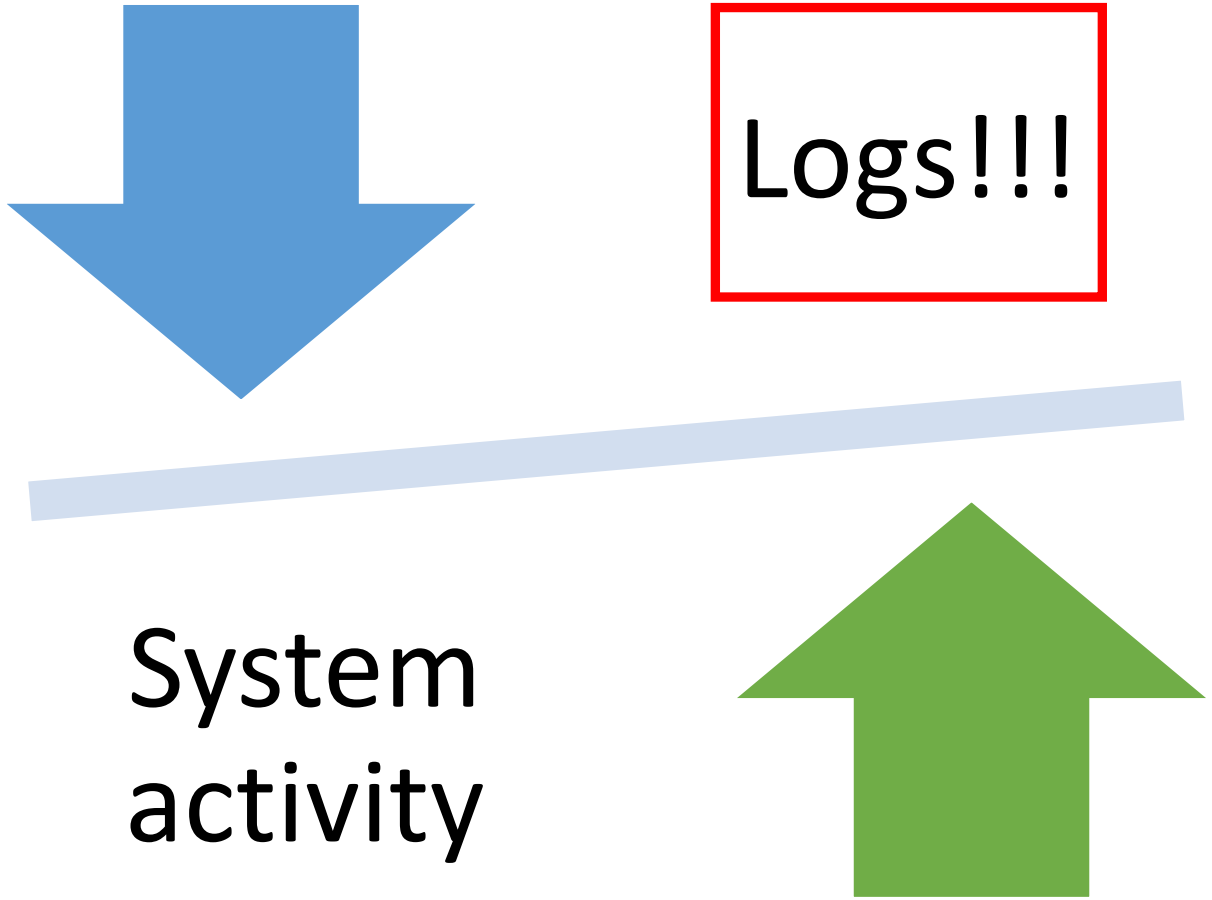
- Use Case 1 – Sharing a Laptop
- Use Case 2 – Transferring Files Between Computers
- Use Case 3 – Sharing Data with Contractor
- Use Case 4 – Traveling with a Laptop
- Use Case 5 – Traveling with a Dual-Boot Laptop

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?

Develop threat information

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

Monitor mass-flow of information



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

Employees

- 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

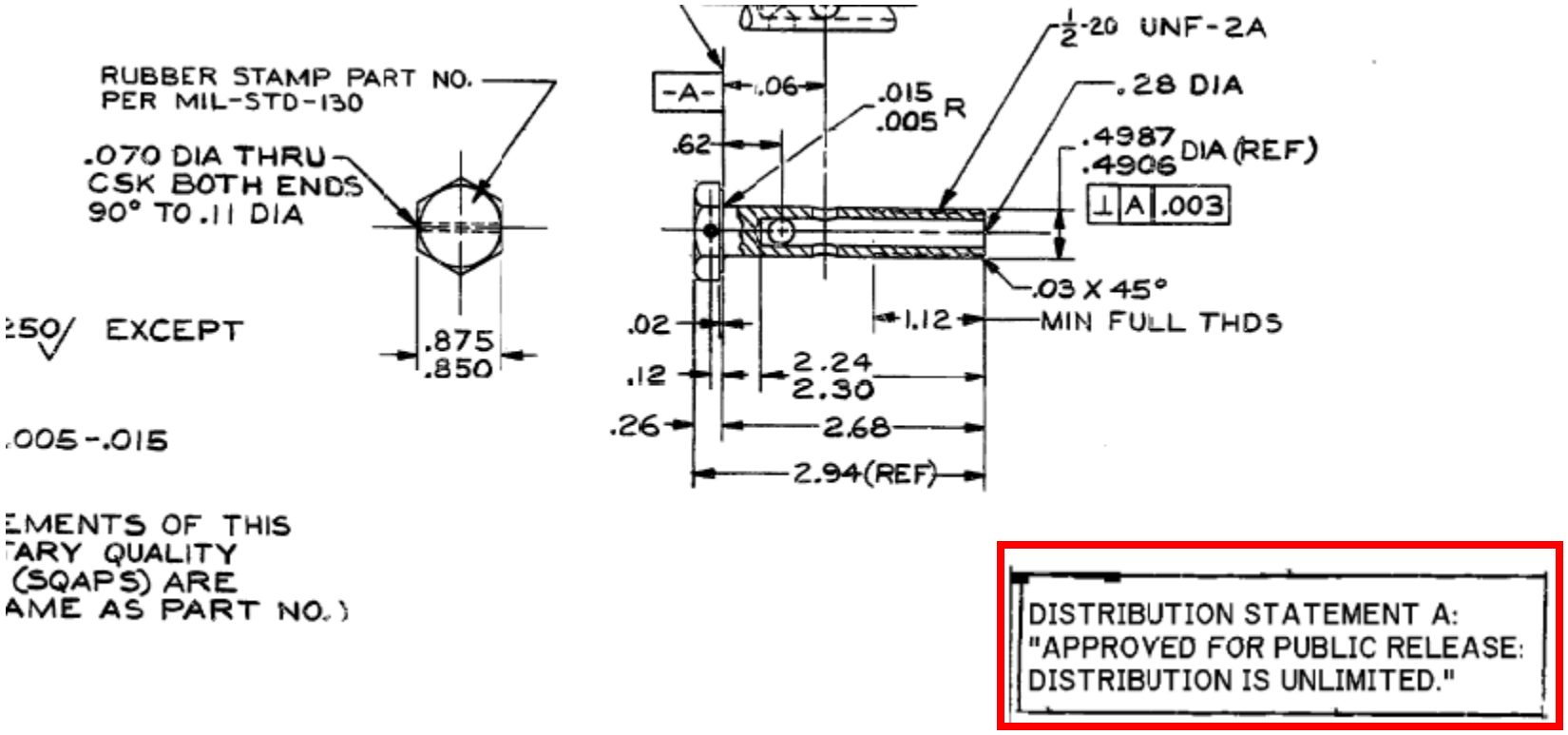
Visitors

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

Information

- 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

Distribution Statement A - example



Attachment to client email

Network

- Network
  - Determine everything that connects to it
    - Internally
    - Externally
    - Visitor
    - Operations - equipment

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

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- June 26, 2019 – **Current Trends in Department of Defense Acquisition** – CLICK HERE for additional information – presented by James Hasik, Senior Fellow, Center for Government Contracting, George Mason University School of Business
- July 9, 2019 – **Overview of the Federal Acquisition Regulations (FAR)** – CLICK HERE for additional information – presented by Carol Murphy, Wisconsin Procurement Institute (WPI)
- July 24, 2019 – **The End of the Fiscal Year is Here: What is Hot and What is Not** – CLICK HERE for additional information – presented by Marc Violante, Wisconsin Procurement Institute (WPI)
- August 7, 2019 – **The NEW WAWF – The Procurement Integrated Enterprise Environment (PIEE)** – CLICK HERE for additional information – presented by Benjamin Blanc, Wisconsin Procurement Institute (WPI)
- August 21, 2019 – **Government Property Management for Federal Contractors and Subcontractors** – CLICK HERE for additional information – presented by Benjamin Blanc, Wisconsin Procurement Institute (WPI)

Search …

REGISTRATION LOCATION

13th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In partnership with Volk Field ANG and Fort McCoy

AGENDA | EVENT HOSTS | SPEAKERS | SPONSORS | EVENT COMPETITIONS | BUYER MEETINGS | EVENT PARTNERS

Registration

For additional information regarding this event, contact Dave Olson at (608) 338-8018.

Location

The 13th Annual Wisconsin Government Opportunities Business Conference (GOBC) will take place at the

Volk Field Air National Guard Base, Building 475 – 100 Independence Drive – Camp Douglas, WI 54618

13TH ANNUAL WISCONSIN GOVERNMENT OPPORTUNITIES BUSINESS CONFERENCE (GOBC)

In Partnership with Volk Field ANG and Fort McCoy

JULY 30-31, 2019

The 13th Annual Wisconsin Government Opportunities Business Conference (GOBC) is scheduled for July 30th and 31st at Volk Field in Camp Douglas, Wisconsin. Businesses from the Midwest will have the opportunity to participate in two days of technical training with a focus on Infrastructure Opportunities, Federal, State and Local Government Opportunities, Information Security, Manufacturing and Teaming.

Attendees will have the opportunity to hear from and meet with regional experts, leaders of the community, potential customers, potential partners and will also have the opportunity to meet one one one with various government and corporate buyers. All businesses including Small, Large, Disadvantaged, HUBZone, Minority-Owned, Native / Tribal Owned, Woman-Owned, Veteran-Owned and Service-Disabled Veteran-Owned firms will benefit from this event.

EARLY REGISTRATION ENDS June 14, 2019 – (Discounted registration may be available)

EVENT REGISTRATION ENDS July 18, 2019

https://volkfieldsbconference.org/

MARKETPLACE 2019 – Milwaukee, WI

October 23-24, 2019

https://www.marketplacewisconsin.com/

QUESTIONS?

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
Wisconsin Procurement Institute
marcv@wispro.org 414-270-3600

Benjamin Blanc | Government Contract Specialist
Wisconsin Procurement Institute
benjaminb@wispro.org 414-270-3600

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226