Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

DEVELOPING AND IMPLEMENTING PRACTICES, POLICIES AND PROCEDURES USING CMMC REFERENCE DOCUMENTS

Cyber Friday Webinar

December 18, 2020




WEBINAR ETIQUETTE

PLEASE

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

THANK YOU!

ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

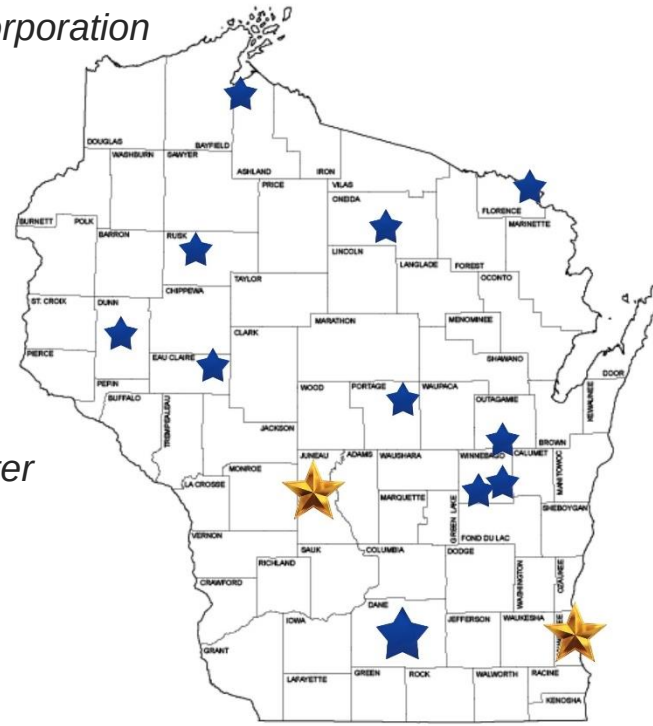
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

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 (PTAC)

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*
- **FLORENCE**
  - *Florence County Economic Development*
- **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*
- **ASHLAND**
  - *Ashland Area Development Corporation*



Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

12/18/20


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.

Developing and implementing practices, policies and procedures using CMMC reference documents

Marc N. Violante

December 18, 2020

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Today’s topics

- Perspective
- Requirements
- Context
- Regulations/Resources
- Policies/Procedures
- Monitoring
- Watch for changes

Become “mimic” qualities of an assessor

- Approach
- Mindset
- Bearing
- Personality
- Focused
- Not overly interesting in “niceties”
- First impressions
- Mental video starts upon arrival on premise

They are not –
- Your friend
- Colleague
- Career Coach
- Sales Manager

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

Create an “avatar”

- Roll play
- Practice
- Walk in and start questioning
- Call team members to the conference room
- Create tension

Issue -

Bottom line, technology theft puts the United States at a disadvantage in its strategic competition with China and Russia, the general said.

https://www.defense.gov/Explore/News/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong/

Protecting Critical Technology Task Force

- “The task force's beginnings date back about four years, when a nation stole technology after hacking into a company's computer network, Murphy said. Which nation and what technology aren't relevant — what is relevant is that DOD didn't find out about the loss for over a year, he said.”

https://www.defense.gov/Explore/News/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong Nov 29, 2019

Goals of changes/requirements

- *Adequate Security*
- *CMMC certification*
- *Supply Chain visibility*
- *Efficiency*

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

CMMC Rollout Strategy

- The CMMC Framework Given the enterprise-wide implementation of CMMC, the Department developed a five-year phased rollout strategy. The rollout is intended to minimize the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain. The Office of the Secretary of Defense staff is coordinating with the Military
- Services and Department Agencies to identify candidate contracts during the first five years of implementation that will include the CMMC requirement in the statement of work. Prior to October 1, 2025, this rule impacts certain large and small businesses that are competing on acquisitions that specify a requirement for CMMC in the statement of work. These businesses will be required to have the stated CMMC certification level at the time of contract award. Inclusion of a CMMC requirement in a solicitation during this time period must be approved by the USD(A&S).

Federal Register Vol 85, No. 189, September 29, 2020 page 61510

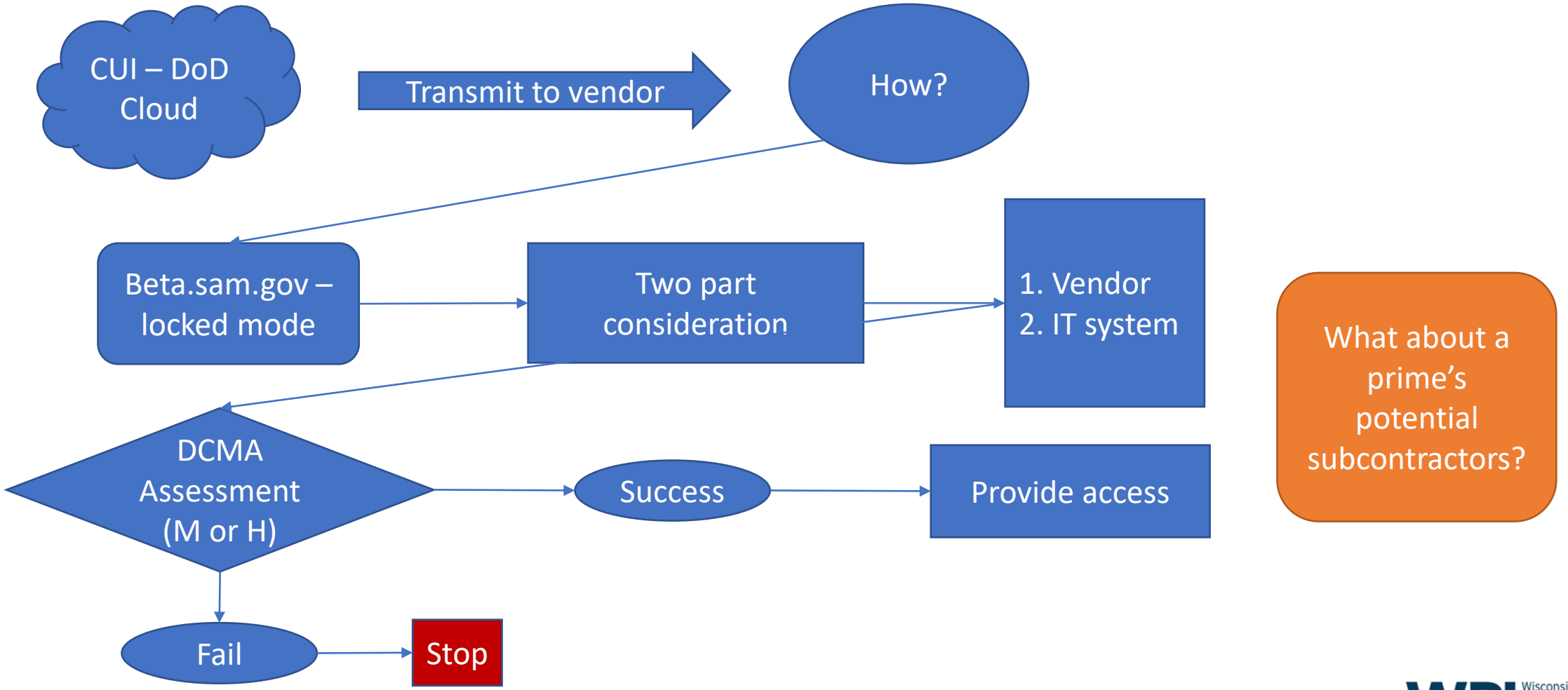
CMMC - 252.204-7021

- Controlled rollout starting in FY-2021
- the CISO team is currently reviewing the following pilot nominations from the military services and defense agencies and anticipates awards in late 2021:

- U.S. Navy
  - *Integrated Common Processor*
  - *F/A-18E/F Full Mod of the SBAR and Shut off Valve*
  - *DDG-51 Lead Yard Services / Follow Yard Services*
- U.S. Air Force
  - *Mobility Air Force Tactical Data Links*
  - *Consolidated Broadband Global Area Network Follow-On*
  - *Azure Cloud Solution*
- Missile Defense Agency
  - *Technical Advisory and Assistance Contract*

Cybersecurity Maturity Model Certification Pilots for Fiscal Year 2021; Dec. 15, 2020 – https://www.defense.gov Newsroom

Maintaining a secure channel



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

The process going forward

- For approved pilots, all offerors will undergo the appropriate CMMC assessment, and awardee must achieve the required CMMC level at time of contract award, and flow down the appropriate CMMC requirement to subcontractors.
  - This does not define the term – CMMC assessment re: offerors
    - Based upon the term assessment and the requirement to complete a Basic Assessment the use of the term implies that an appropriate assessment would be either a Medium or High level assessment conducted by DCMA DIBCAC*
  - Awardees must achieve the required CMMC level at time of contract award

M. Violante – December 17, 2020*
https://www.defense.gov/Newsroom/Releases/Release/Article/2447770/cybersecurity-maturity-model-certification-pilots-for-fiscal-year-2021/

Access to Facilities

- The new DFARS clause 252.204–7020 requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment. The clause
- also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments. The clause also provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments. B

Flowdow – also “flow up”

- Flowdown of the requirements is necessary to respond to threats that reach even the lowest tiers in the supply chain. Therefore, to achieve the desired policy outcome, DoD intends to apply the new provision and clauses to contracts and subcontracts for the acquisition of commercial items and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold.
- The provision and clauses will not be applicable to contracts or subcontracts exclusively for the acquisition of commercially available off-the-shelf items.
- 252.204-7012 – Reporting of cyber incidents “flow up”
- 252.204-7000 – Request of permission to share info – “flow up”

Federal Register Vol 85, No. 189, September 29, 2020 page 61507

Terms and wording

- There are differences between
  - Assessment, Certification and CMMC
  - A compliant system and compliance
    - A system does not in and of itself create compliance – actions do
  - Eligibility and permission to share
    - An individual may meet the necessary criteria to be a recipient or hold specified information. Do they have –
      - A need to know everything
      - Only a portion
      - Continued access | hold copies | share copies – derivative works
      - A good example may be developing a proposal and sharing information with the proposal team.
  - Provision and Clause

General ideas, questions

Provision v. Clause

- *Solicitation provision or provision* means a term or condition used only in solicitations and applying only before contract award.
- *Contract clause* or "clause" means a term or condition used in contracts or in both solicitations and contracts, and applying after contract award or both before and after award.

252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(c) *Procedures.*

(1) The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) for all covered contractor information systems relevant to the offer.

FAR Part 2 – Definitions
DFARS 252.204-7019

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

Current Cyber requirements

FAR

Executive Agency contracts

52.204-21
15 elements
Contract specific requirements

DFAR - Now

DoD Contracts subject to 252.204-7012

252.204-7008
252.204-7012
252.204-7019
252.204-7020

DFAR - Future

DoD Contract subject to 252.204-7021

252.204-7021
https://www.acq.osd.mil/cmmc
https://www.cmmcab.org

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

Assessments

Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

"Medium Assessment" means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

"High Assessment" means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "High" in the resulting score.

DFARS 252.204-7020 Definitions

Basic Assessment – 252.204-7020

- To submit the Basic Assessment, the contractor is required to complete 6 fields:
  - System security plan name (if more than one system is involved);
  - CAGE code associated with the plan;
  - a brief description of the plan architecture;
  - date of the assessment;
  - total score;
  - and the date a score of 110 will be achieved.
    - All of this data is available from the Basic Assessment itself, the existing system security plan, and the plans of action. The contractor selects the date when the last plan of action will be complete as the date when a score of 110 will be achieved.

Understand the goal (110 or bust)

- The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action. In general, CMMC takes a risk-based approach to addressing cyber threats. Based on the type and sensitivity of the information to be protected, a DIB company must achieve the appropriate CMMC level and demonstrate implementation of the requisite set of processes and practices.

Federal Register Vol 85, No. 189, September 29, 2020 page 61509

Part of the “why” behind CMMC

- Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security. The various industry surveys and Government assessments conducted to date illustrate the following: Absent a requirement for defense contractors to demonstrate implementation of standard cybersecurity processes and practices, cybersecurity requirements will not be fully implemented, leaving DoD and the DIB unprotected and vulnerable to malicious cyber activity.

Federal Register Vol 85, No. 189, September 29, 2020 page 61518

Supply Chain considerations

- Although DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program

Federal Register Vol 85, No. 189, September 29, 2020 page 61508

Strategic Approach

- DFARS 252.204-7008 – contract by contract attestation
- *"This individual contract approach is inefficient for both Industry and Government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information for contracts containing DFARS clause 252.204-7012."*
  - Document industry cybersecurity readiness at a strategic level;
  - Apply a standard methodology to recognize industry cybersecurity readiness at a strategic level and include a process to update this recognition as cybersecurity readiness changes over time; and

Strategically Implementing Cybersecurity Contract Clauses, USD(A&S) Memorandum, dated February 5, 2019, directs development of a standard methodology to recognize industry cybersecurity readiness at a strategic level.

Assessing Contractor Implementation of Cybersecurity Requirements, USD(A&S) Memorandum, dated November 14, 2019, provides standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171.

/s/ Ellen Lord

https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

Multiple Drivers of CMMC –

- Scale and Depth. DoD contractors must include DFARS clause 252.204– 7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi- tier supply chain for any given program or technology development effort. Given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years.

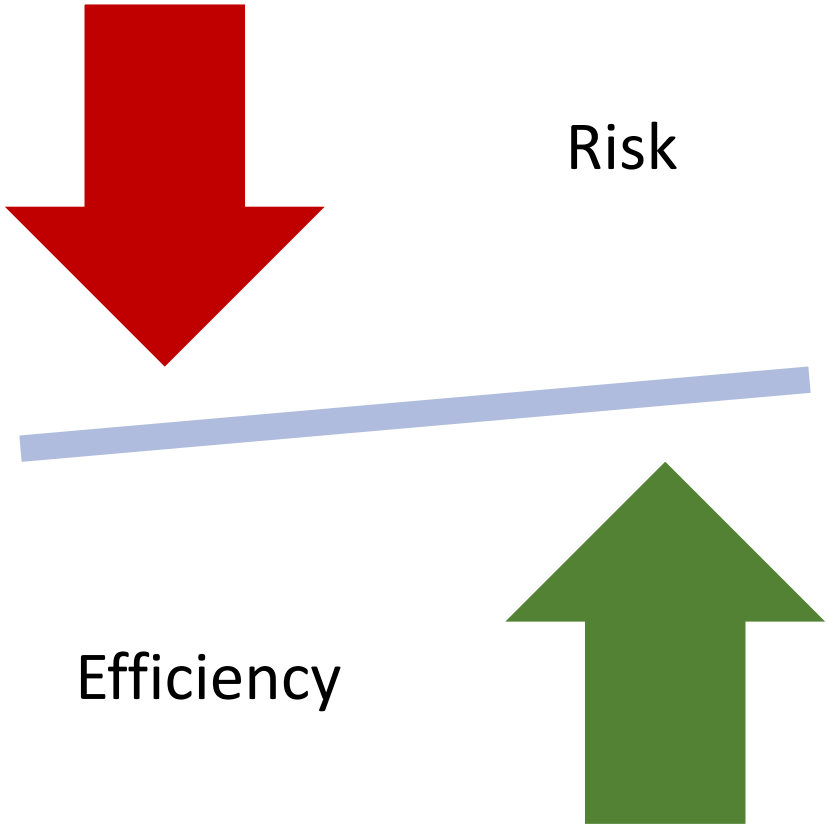
Federal Register Vol 85, No. 189, September 29, 2020 page 61509-61510

Managing Risk and Efficiency

252.204-7008

252.204-7020

252.204-7021



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

Institutionalization

- The term institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization [9,10]. The more deeply ingrained an activity, the more likely it is that an organization will continue to perform the activity – including under times of stress – and that the outcomes will be consistent, repeatable, and of high quality [9,10].

9. *Cybersecurity Capability Maturity Model (C2M2)*, Version 1.1, Department of Energy, Department of Homeland Security, and Carnegie Mellon University Software Engineering Institute, February 2017

10. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*, Technical Note CMU/SEI-2013-TN-028, M. J. Butkovic and R. A. Caralli, Carnegie Mellon University Software Engineering Institute, November 2013

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 9

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

The contractor is accountable

- (c) *Cyber incident reporting requirement*.
- (1) When the Contractor discovers a cyber incident that affects a covered contractor information system or …
- (d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software …
- (e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall …

DFARS 252.204-7012

Assemble Applicable References

Include references for related programs

- DFARS 252.204-7021
- DFARS 252.204-7008
- DFARS 252.204-7012
- NIST 800-171 revision 2 – Feb 2021
- NIST 800-171A
- NIST Handbook 162
- FAR 52.204-21
- NISTIR 8286 -Integrating Cybersecurity and Enterprise Risk Management (ERM)
- CMMC Model
- CMMC Assessment – appropriate level
- 32 CFR 2002
- *Export Control program & references (EAR, ITAR, JCP, NOFORN)
- NIST Cybersecurity Framework
- Regulations
- MITRE ATT&CK

Be familiar with requirements

DEFENSE LOGISTICS AGENCY (DLA) MASTER SOLICITATION
FOR AUTOMATED SIMPLIFIED ACQUISITIONS
REVISION 74 (DEC 3 2020)

DFARS 252.204-7000 (Oct 2016) Disclosure of Information
DFARS 252.204-7003 (Apr 1992) Control of Government Personnel Work Product
DFARS 252.204-7007 (Dec 2019) Alternate A, Annual Representations and Certifications. ***(Includes DFARS 252.204-7016 (Dec 2019), Covered Defense Telecommunications Equipment Or Services – Representation)***
DFARS 252.204-7008 (Oct 2016) Compliance with Safeguarding Covered Defense Information Controls
DFARS 252.204-7009 (Oct 2016) Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
DFARS 252.204-7012 (Dec 2019) Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.204-7015 (May 2016) Notice of Authorized Disclosure of Information for Litigation Support
DFARS 252.204-7019 (Nov 2020) Notice Of NIST SP 800-171 DoD Assessment Requirements
DFARS 252.204-7020 (Nov 2020) NIST SP 800-171 DoD Assessment Requirements
DFARS 252.213-7000 (Sep 2019) Notice to Prospective Suppliers on Use of Supplier Performance Risk System in Past Performance Evaluations.
DFARS 252.222-7999 (Nov 2020) Combating Race And Sex Stereotyping (Deviation 2021-O0001)
https://www.acq.osd.mil/dpap/policy/policyvault/USA002235-20-DPC.pdf

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

C001- Establish system access requirements –a

- AC.1.001
  Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

  - FAR Clause 52.204-21 b.1.i
  - NIST SP 800-171 Rev 1 3.1.1
  - CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11
  - NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
  - CERT RMM v1.2 TM:SG4.SP1
  - NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17
  - AU ACSC Essential Eight

Access & Controlled Environment

https://www.archives.gov/cui/training.html#controlled-environments

Benefit from self-doubt

- We've all worked with people who are overconfident and cocky. I used to work with one particularly egregious example of this personality type. He would routinely take indefensible positions, make grandiose statements, and even threaten consequences if others did not do what he demanded. When I was first exposed to this behavior, I too was convinced by his certainness. I got wise to the behavior over time, as I saw him retreat with his tail between his legs time after time when someone called his bluff.

- Why am I sharing this with you? As you may have guessed, there is an information security lesson we can learn from this. In security, we need to be sure we know how to successfully mitigate risk continually amidst a changing threat landscape. We also need to gain the confidence of our customers, partners, peers, executives, and other stakeholders. That being said, being overconfident in these areas can be quite dangerous. In other words, a healthy dose of self-doubt can go a long way towards keeping us on our toes and continually improving the security posture of our respective organizations.

https://www.securityweek.com/how-self-doubt-can-keep-your-security-team-sharp

Be Familiar with information categories, definitions & requirements

Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Unclassified Controlled Nuclear Information - Defense
Export Control	• Export Controlled • Export Controlled Research

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

https://www.archives.gov/cui/registry/category-list
DFARS 252.204-7012

Familiarity with references can help

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.

FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems; pg 2

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

C001- Establish system access requirements – nb

- As companies seek to comply with CMMC — which features different standards depending on the nature of the work being done, with level 1 standards being the least demanding and level 5 the most burdensome — they should be aware of undetected devices on their networks that could pose risks to their certifications, said Katherine Gronberg, vice president of government affairs at Forescout Technologies, a San Jose, California-based security firm.

- "On average we can go into a company in any sector and find about 30 to 40 percent more devices than they knew about," she said.

https://www.nationaldefensemagazine.org/articles/2020/6/8/undetected-devices-may-pose-cmmc-issues

C040 - Identify and manage information system flaws

- SI.1.210
  Identify, report, and correct information and information system flaws in a timely manner.
  - FAR Clause 52.204-21 b.1.xii
  - NIST SP 800-171 Rev 1 3.14.1
  - NIST CSF v1.1 RS.CO-2, RS.MI-3
  - CERT RMM v1.2 VAR:SG2.SP2
  - NIST SP 800-53 Rev 4 SI-2
  - UK NCSC Cyber Essentials
  - AU ACSC Essential Eight

- Should there be documentation?
- What should be documented?
- By whom?
- Should there be a reviewer?
- Who should receive internal reports?
- What should be escalated?

Stay Informed – there are options

Supply Chain Attack: CISA Warns of New Initial Attack Vectors Posing 'Grave Risk': The U.S. government added a new wrinkle to the global emergency response to the SolarWinds software supply chain attack, warning of additional initial access vectors that have not yet been documented. **Read More**

Killswitch Found for Malware Used in SolarWinds Hack: A killswitch has been identified and activated for the SUNBURST malware delivered by threat actors as part of the attack targeting SolarWinds. **Read More**

FBI, CISA, ODNI Describe Response to SolarWinds Attack: The FBI, CISA and ODNI have described each of their roles in investigating the SolarWinds hack and responding to the incident. **Read More**

FBI Warns of DoppelPaymer Ransomware Targeting Critical Infrastructure: The FBI says DoppelPaymer ransomware continues to target healthcare, emergency services, and education. **Read More**

Little-Known SolarWinds Gets Scrutiny Over Hack, Stock Sales: Before this week, few people were aware of SolarWinds, but the revelation that it has been targeted by elite cyber spies has put many of its customers on high alert, and it's raising questions about why its biggest investors sold off stock. **Read More**

NATIONAL DEFENSE INFORMATION SHARING AND ANALYSIS CENTER

The National Defense ISAC is the Information Sharing and Analysis Center for the Defense Industrial Base, offering defense sector companies, their suppliers, and related interests a community and forum for sharing cyber and physical security threat indicators, best practices and mitigation strategies.

ND-ISAC gives defense industry entities and suppliers the ability to leverage the best security data, tools, services, and best practices available in a high-trust, collaborative industry environment. Through ND-ISAC, members share intelligence on cyber and physical security, insider threats, vulnerabilities, and associated threat remediation. ND-ISAC enables members to develop and continually mature their secure enterprise. ND-ISAC serves as the national defense sector's principal focal point for all hazards to the sector.

ND-ISAC Cybersecurity Services

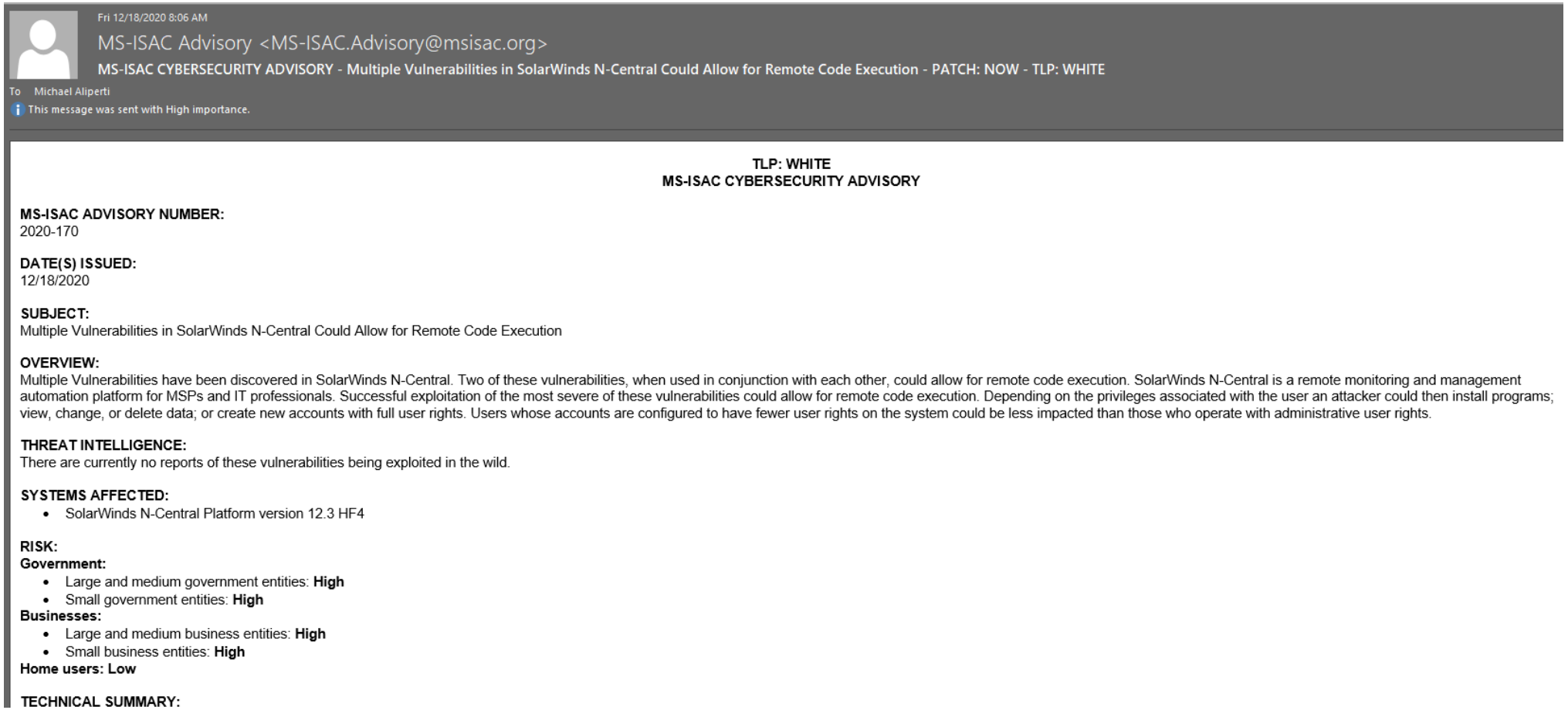
ND-ISAC provides members access to affordable cybersecurity services and discounted pricing

Continuous Risk Monitoring

Attack Surface Management

As an example - SecurityWeek Briefing https://www.nationalisacs.org/member-isacs https://ndisac.org/

Staying informed – example TLP: White info



Fri 12/18/2020 8:06 AM

MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>

MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in SolarWinds N-Central Could Allow for Remote Code Execution - PATCH: NOW - TLP: WHITE

To Michael Aliperti

This message was sent with High importance.

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2020-170

DATE(S) ISSUED:
12/18/2020

SUBJECT:
Multiple Vulnerabilities in SolarWinds N-Central Could Allow for Remote Code Execution

OVERVIEW:
Multiple Vulnerabilities have been discovered in SolarWinds N-Central. Two of these vulnerabilities, when used in conjunction with each other, could allow for remote code execution. SolarWinds N-Central is a remote monitoring and management automation platform for MSPs and IT professionals. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- SolarWinds N-Central Platform version 12.3 HF4

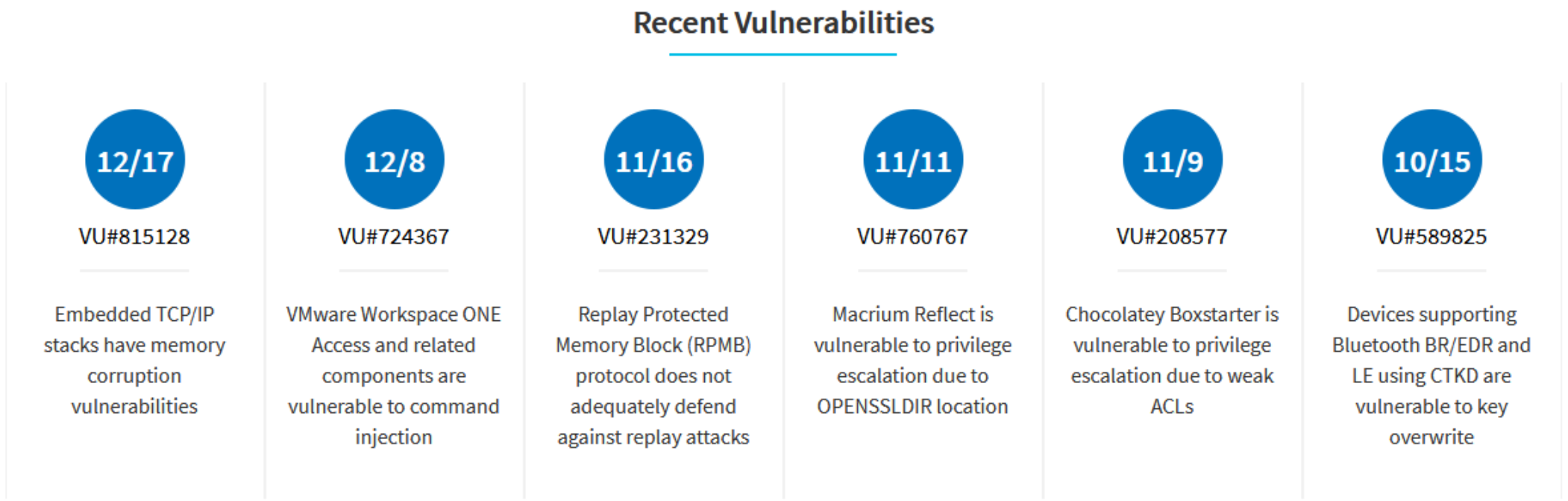
RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Develop – active | dynamic processes



https://us-cert.cisa.gov/

Don’t minimize the risk!

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

Hid for two years!

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

Cyber – breach detection

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

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

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

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

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

British Airways hit with UK data watchdog's biggest-ever fine

(Reuters) — Britain's data protection watchdog said on Friday it has fined British Airways PLC £20 million - its biggest such penalty to date - for failing to protect data that left more than 400,000 of its customers' details the subject of a 2018 cyber attack.

The Information Commissioner's Office (ICO) said its investigators found BA should have identified weaknesses in its security and resolved them with measures available at the time, which would have prevented the data breach.

"Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result," the ICO said.

Severe failing

Announcing the penalty, the regulator said its investigators found that BA did not detect the attack on June 22, 2018 - but was alerted by a third party more than two months later, on Sept. 5.

The ICO added that it was not clear whether or when the company would have identified the attack itself.

https://www.reuters.com/article/us-british-airways-cyber-fine/british-airways-hit-with-uk-data-watchdogs-biggest-ever-fine-idUSKBN2711AX

Consider all access points

OctoPrint is a free and open source web interface for 3D printers that allows users to monitor and control every aspect of their device and printing jobs. OctoPrint can be used to start, stop or pause a print job, it provides access to the printer's embedded webcam, it supplies information on the progress of a print job, and monitors the temperature of key components.

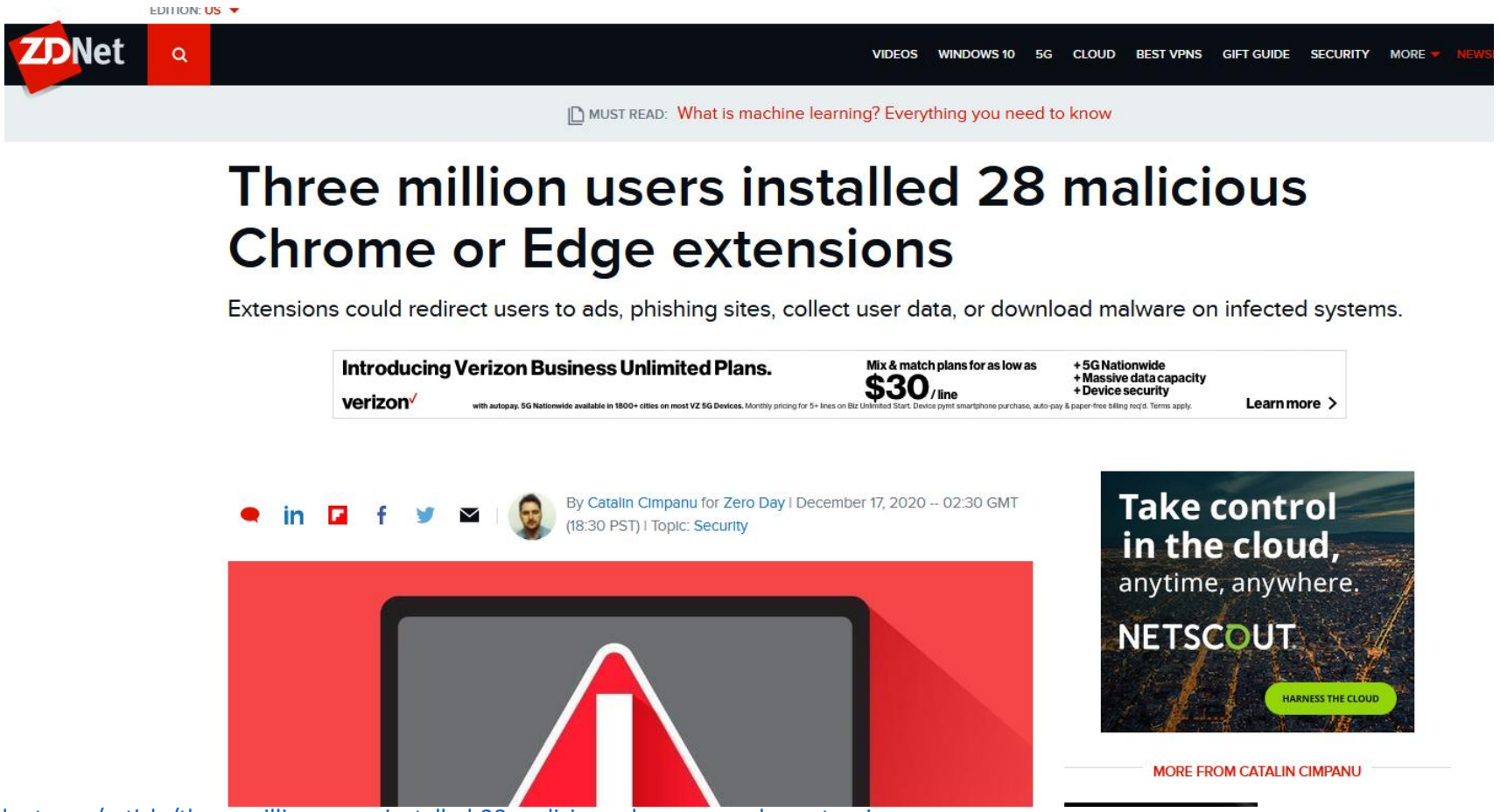
While it may seem that failure to protect a 3D printer against unauthorized access cannot pose a major risk, SANS's Xavier Mertens warns that an attacker can conduct a wide range of malicious activities.
For instance, they can access G-code files, which are text files that contain the instructions needed to print a 3D object. In the case of organizations, these files could store valuable trade secrets.
"Indeed, many companies' R&D departments are using 3D printers to develop and test some pieces of their future product," Mertens noted.

The researcher pointed out that an attacker could also upload specially crafted G-code files to an unprotected printer. They could instruct the device to start printing when nobody is around, or they could make small changes to the code.

"By changing the G-code instructions, you will instruct the device to print the object but the altered one won't have the same physical capabilities and could be a potential danger once used," Mertens explained. "Think about 3D-printed guns but also 3D-printed objects used in drones. Drone owners are big fans of self-printed hardware."

https://www.securityweek.com/thousands-3d-printers-exposed-remote-attacks

Develop scenarios from real-world events



https://www.zdnet.com/article/three-million-users-installed-28-malicious-chrome-or-edge-extensions

Integrate requirements

- “Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.
- (d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.
- Develop processes/procedures to deal with the issue
- Determine if there was a reportable cyber incident
- Cyber forensic image
- Review update System Security Plan | Procedures | Policies

DFARS 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)

SI.1.212 Update malicious code protection mechanisms when new releases are available

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

Test

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

SI.1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the frequency for malicious code scans is defined;

[b] malicious code scans are performed with the defined frequency; and

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].

Interview

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 46

SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1

SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.
SI.1.212	Update malicious code protection mechanisms when new releases are available.
SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 22

Understand how events relate to requirements

SI.1.211

Provide protection from malicious code at appropriate locations within organizational information systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] designated locations for malicious code protection are identified; and

[b] protection from malicious code at designated locations is provided.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf

Mitre ATT&CK

Initial Access (9 techniques)	Execution (10 techniques)	Persistence (18 techniques)	Privilege Escalation (12 techniques)	Defense Evasion (34 techniques)	Credential Access (14 techniques)	Discovery (24 techniques)	Lateral Movement (9 techniques)	Collection (16 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
		Valid Accounts (4)		Modify Registry		System Information Discovery					
				Obfuscated Files or Information (5)		System Network Configuration Discovery					
				Pre-OS Boot (3)		System Network Connections Discovery					
				Process Injection (11)		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Signed Binary Proxy Execution (10)		Virtualization/Sandbox Evasion (3)					
				Signed Script Proxy Execution (1)							
				Subvert Trust Controls (4)							
				Template Injection							
				Traffic Signaling (1)							
				Trusted Developer Utilities Proxy Execution (1)							
				Unused/Unsupported Cloud Regions							
				Use Alternate Authentication Material (4)							
				Valid Accounts (4)							
				Virtualization/Sandbox Evasion (3)							
				XSL Script Processing							

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

https://attack.mitre.org/versions/v7/

Mitre ATT&CK - Example

- Select item
- Description of the issue
- Examples of processes utilized
- Procedure examples (drill down capability)
- Mitigation
- Detection
- References

https://attack.mitre.org/versions/v7/techniques/T1189/

MITRE ATT&CK - Malware

T1587	Develop Capabilities	Before compromising a victim, adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.
.001	Malware	Before compromising a victim, adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors, packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.
.002	Code Signing Certificates	Before compromising a victim, adversaries may create self-signed code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with. Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Cybersecurity Capability Maturity Model (C2M2) – Overview

- The Cybersecurity Capability Maturity Model (C2M2) contains a set of common cybersecurity practices that can be used to evaluate, prioritize, and improve cybersecurity capabilities. As a maturity model, C2M2 includes practices that range from foundational ones that are considered basic cybersecurity activities to those that are more advanced in terms of either technical sophistication or consistency and repeatability. This enables use of C2M2 to understand the current state of a cybersecurity program and track growth over time.
- The C2M2 that is available today from the C2M2 Program of the United States Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response website[1] is a derivative of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0, which was first published in 2012.

https://securityboulevard.com/2020/12/cybersecurity-capability-maturity-model-c2m2-overview/ December 17, 2020

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

Defining Policy

- A policy is a high-level statement from an organization's senior management that documents the requirements for a given activity. It is intended to establish organizational expectations for planning and performing the activity, and communicate those expectations to the organization. Senior management should sign policies to show its support of the activity.

Policy – at a minimum

- clearly state the purpose of the policy;
- clearly define the scope of the policy: for example, enterprise-wide, department-wide, or information-system specific;
- describe the roles and responsibilities of the activities covered by this policy: the responsibility, authority, and ownership of [DOMAIN NAME] domain activities; and
- establish or direct the establishment of procedures to carry out and meet the intent of the policy, include any regulatory guidelines this policy addresses.

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf; B-2
CERT RMM v1.2 GG2.GP1 Subpractice 2; https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

Policy v. Procedure

- “Policies are guidelines that regulate organization action. They control the conduct of people and the activities of systems.”
- “Procedures supplement the policy guidelines with specifics and complete the information users need. It’s not sufficient to say, “It is our policy to provide the best customer service in the industry and stop there.”
- “Users need to know what that means.”
- “How do I provide the best service.’”

Writing Effect Policies and Procedures, Nancy J. Campbell, AMACOM 1998 pages 1 and 3

Policy v. Procedure - considerations

- Writing style and complexity
- Availability and Accessibility
- Table of Contents
- Person/Office responsible
- List of effective pages
- Page change management – incorporates change 1, dtd 18 Dec 2020
- Review procedure and date of last review

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

Explore & utilize resources

- Is the information complete and self-explanatory?
- Does the information only capture the critical ideas?

Suggested questions to ask.

2. Develop and publish organizational policy for the process.

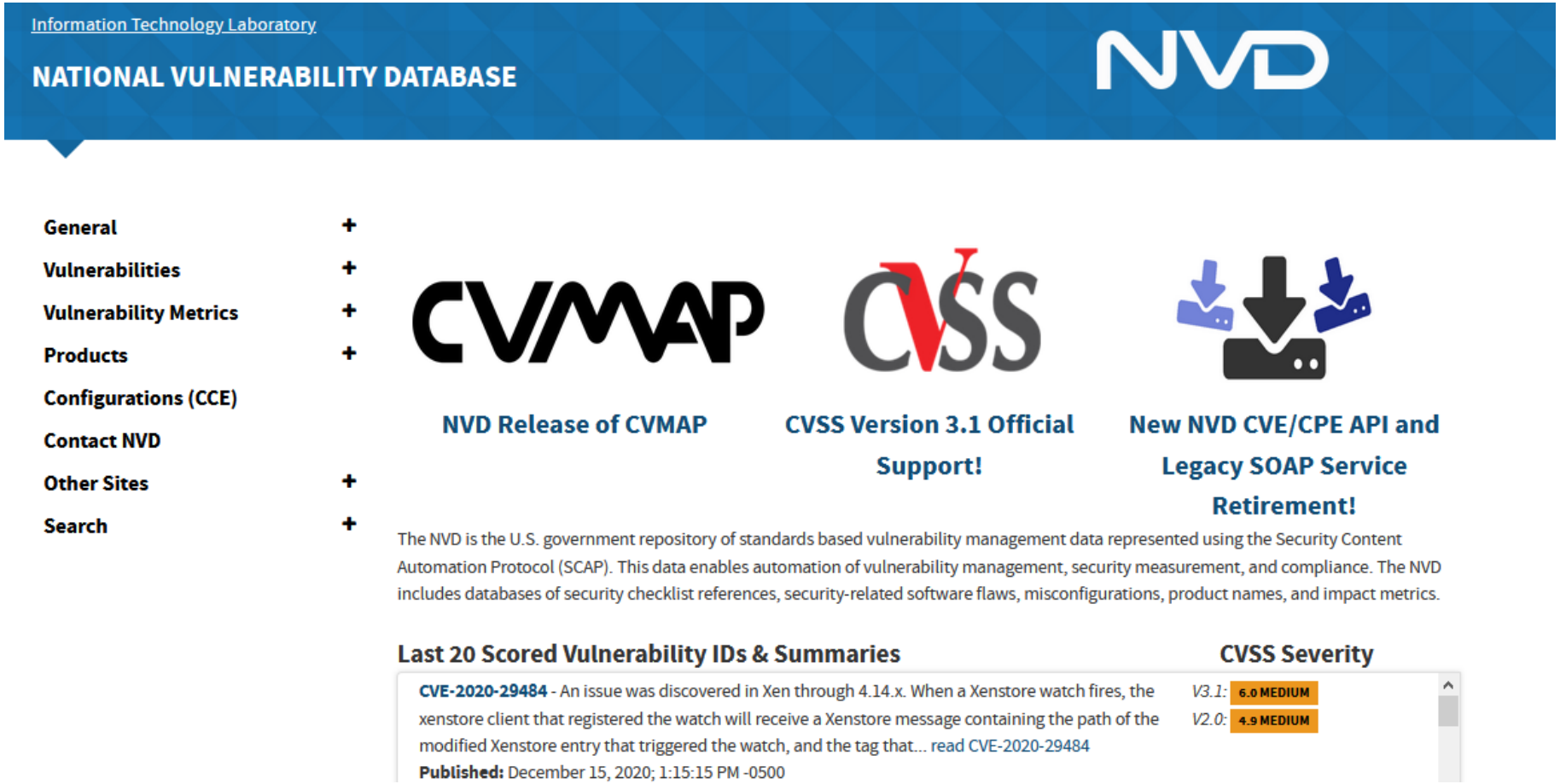
Elaboration:

The asset definition and management policy should address

- responsibility, authority, and ownership for performing process activities, including collecting and documenting asset inventory information
- procedures, standards, and guidelines for
  - documenting asset descriptions and relevant information
  - describing and identifying asset owners
  - describing and identifying asset custodians
- the development of criteria to provide guidance on asset inventory updating, reconciliation, and change control
- the association of assets to core organizational services, and the prioritization of assets in the inventory
- methods for measuring adherence to policy, exceptions granted, and policy violations

CERT RMM v1.2 GG2.GP1 Subpractice 2; https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf; page ADM | 15

Identify – utilize resources



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

Prepare for the worst case!

- If your response plan is on the network, is it now compromised – corrupted?
- Is your response internally resourced – external?
- If external, are their contingency contracts in place?

Understand general ideas/expectations

- Real interest - active engagement
- Live document – modified updated as needed*
- Company-wide participation|– (institutionalization)
- Critical thinking – not treated as a checklist

* No current information on how changes to a company's program will or may impact its certification.

Developing a CMMC program

- Understand
  - the program goals
  - the program criteria
  - Regulations
  - Requirements
  - Assessment processes and approach

Common documents reviewed

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system-level, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive. A contractor may not have these specific documents, and other documents may be used to provide evidence of compliance.

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 5

Common documents reviewed

- Testing is an important part of the assessment process.

Interviews tell the Certified Assessor what the contractor staff believe to be true, documentation provides evidence of intent, andtesting demonstrates what has or has not been done.

For example, contractor staff may talk about how users are identified, documentation may provide details on how users are identified, but seeing a demonstration of identifying users provides evidence that the practice is met.

The Certified Assessor will determine which practices, or objectives within a practice need demonstration or testing. Not all practices will require testing

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 5

CMMC Assessments

- **Identifier and Practice Statement:** is headed by the practice identifier in the format Domain.Level.Number (e.g., AC.1.001) and followed by the CMMC practice statement.
- **Assessment Objectives [NIST SP 800-171A]:** identifies the specific list of objectives that must be met to receive MET for the practice as defined in NIST SP 800-171A.
- **Potential Assessment Methods and Objects [NIST SP 800-171A]:** defines the nature and the extent of the Certified Assessor's actions as defined in NIST SP 800-171A. The methods include *examine*, *interview*, and *test*. Assessment objects identify the items being assessed and can include specifications, mechanisms, activities, and individuals.
- **Discussion [NIST SP 800-171 R2]:** contains discussion written by NIST[2] for the associated NIST SP 800-171 security requirement. CMMC Level 1 aligns with FAR Clause 52.204-21, which focuses on FCI, and the NIST text has been modified to reflect this.
- **Further Discussion:**

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 5

CMMC Assessments

"*A CMMC assessment is the methodology to certify that a contractor is compliant with the CMMC standard. Assessments are conducted by CMMC Third-Party Assessment Organizations (C3PAOs) and Certified Assessors.* "

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 1

Assessment Criteria and Methodology

- The CMMC assessment procedure leverages the Assessment Procedure defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171A Section 2.11:

> *Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, and architectural designs) associated with a system.*
> - *Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.*
> - *Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).*
> - *Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.*

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 4

Example from NIST 800-171A

3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2[a]	*the types of transactions and functions that authorized users are permitted to execute are defined.*
	3.1.2[b]	*system access is limited to the defined types of transactions and functions for authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing access control policy].	

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf; page 9

Example from NIST HB 162

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

Does the company use passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company have an authentication mechanism?

Yes No Partially Does Not Apply Alternative Approach

Does the company require users to logon to gain access?

Yes No Partially Does Not Apply Alternative Approach

Are account requests authorized before system access is granted?

Yes No Partially Does Not Apply Alternative Approach

Does the company maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

User access security refers to the set of procedures by which authorized users access the system and unauthorized users are prevented accessing the system.

Where to Look:

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with 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 information system accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records
- remote access implementation and usage (including restrictions) procedures
- remote access authorizations

Who to Talk to:

- employees with account management responsibilities
- system/network administrators
- employees with responsibilities for managing remote access connections
- employees with information security responsibilities
- employees with access enforcement responsibilities
- system developers

Perform Test On:

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability

Determine applicable sources | regulations

Example

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company has just signed a contract with the DoD, however, and you now need to document who enters and leaves your facility. You work with the reception staff to ensure that all non-employees sign in at the reception area and sign out when they leave [a]. You retain those paper sign-in sheets in a locked filing cabinet for one year. Employees receive badges or key cards that enable tracking and logging access to company facilities.

?

Potential Assessment Considerations

- Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements [a]?[11]
- Are visitor access records retained for as long as required [a]?[12]

KEY REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 Rev 2 3.10.4

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

References

- FAR 52.204-21 – entirety https://www.acquisition.gov
- NIST 800-171 r1 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- NIST 800-171 r2 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-53 Rev 4 - https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- NIST CSF v1.1 - https://doi.org/10.6028/NIST.CSWP.04162018
- CERT RMM v1.2 - https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf
- CISecurity Controls - https://www.cisecurity.org/controls/
- AU ACSC Essential Eight - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- UK NCSC Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

Sept 11, 2020	A Deep Dive into DFARS 252.204-7012 - Looking beyond NIST 800-171 r1
Sept 25, 2020	Information Security - An overview of programs, general requirements and resources
Oct 9, 2020	Economic Espionage - You have what they want.
Oct 23, 2020	Guarding and Securing Intangibles - Protecting what you cannot see and touch
Nov 6, 2020	Tools, practices and resources for your cyber-security toolbox
Nov 20, 2020	An overview of cyber-threats - What you can't see - can put you out of business!
Dec 4, 2020	Securing the Supply Chain - "No man is an island"
Dec 18, 2020	Developing and implementing practices, policies and procedures using CMMC reference documents
Jan 8, 2021	The other side of CMMC
Jan 22, 2021	Overview of CMMC Level 1
Feb 5, 2021	Embarking on the path to CMMC Level 3
Feb 19, 2021	Preparing for a CMMC Certification assessment
Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.

PRESENTED BY

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

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

12/18/20

ACQUISITION HOUR LIVE WEBINAR SERIES

- January 20, 2021

  Acquisition Hour: beta.SAM.gov - An Update and Overview
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- February 17, 2021

  Acquisition Hour: Market Research – Successful Contractors Do Their Homework
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- February 23, 2021

  Acquisition Hour: Update on Federal Wage-Hour Laws
  CLICK HERE for additional information
  Presented by Corey Walton, U.S. Department of Labor

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

…More at wispro.org/events

- SAVE THE DATE-

January 28, 2021

Join Wisconsin's Federal contractors and subcontractors for this annual event. Keep up to date with this series of briefings focusing on changes and challenges in DOD/ Federal contracting.

Program: 8am – 3pm

Networking Hour with Guest Speaker: 3pm – 4pm

More info at https://www.wispro.org/event/13th-annual-end-of-year-federal-contractor-update-virtual/

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

CYBERSECURITY – UPDATE – DECEMBER 2020

- CMMC -
  - Implementation continues
  - Pathfinder contracts to be announced soon – article, Dec 1, 2020
    - CMMC requirements will be included
  - Full implementation expected by Oct 2025
- New clauses and requirements –
  - DFARS 252.204-7019
  - DFARS 252.204-7020 – applies to contracts subject to 252.204-7012
    - With few exceptions, these requirements apply to all Primes and Subcontractors
    - Consistent with philosophy shift of self-attest to verifiable
    - Three levels – Base – self-performed , Medium & High - DCMA

252.204-7020 – BASIC ASSESSMENT

- Requires
  - System Security Plan(SSP)
  - Plan of Action – with dates for outstanding items
  - Basic Assessment
- Six elements uploaded to Supplier Performance Risk System (SPRS)
  1. System Security Plan name (if more than one system is involved)
  2. Brief description of Plan Architecture
  3. CAGE code associated with SSP
  4. Date Assessment performed
  5. Summary Score
  6. Date a score of 110 to be achieved

CURRENT CYBER REQUIREMENTS

- FAR 52.204-21 – Federal Contract Information
- DFARS 252.204-7012
- Requirements cited in solicitation/contract

Need assistance – please contact Marc Violante from WPI at marcv@wispro.org or 920-456-9990

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226