Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Acquisition hour: New Federal Cybersecurity Requirements are here!

June 28, 2016

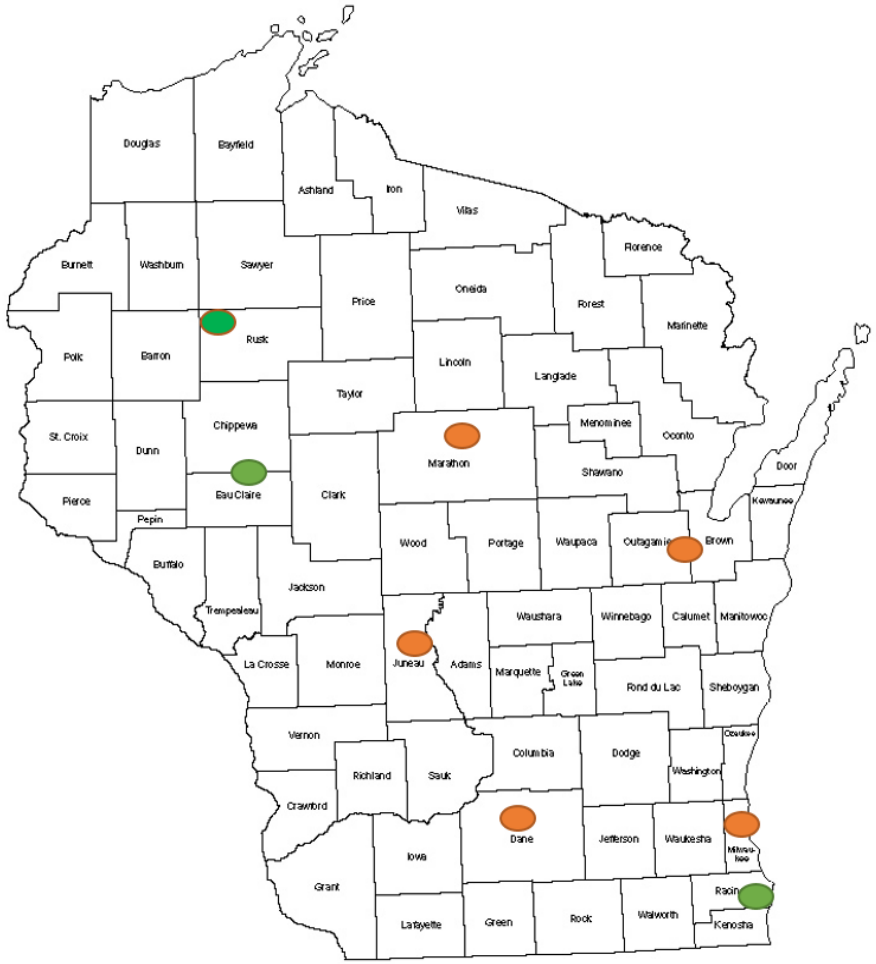



Wisconsin Procurement Institute (WPI)

"Assisting Wisconsin businesses in creating, developing and growing their Federal, State and Local Government sales, revenues, profits and jobs."

A Procurement Technical Assistance Center (PTAC)

WPI Wisconsin Procurement Institute



LOCATIONS:

- ***Primary office*** – **Milwaukee** - Technology Innovation Center

- ***Staffed Satellite offices***
  - **Madison** (FEED – Food Enterprise & Economic Development / MEC – Madison Enterprise Center)
  - **Camp Douglas** (Juneau County Economic Development Corporation)
  - **Wausau** (Wausau Regional Chamber of Commerce)
  - **Appleton** (Fox Valley Technical College)

- ***Active Partnerships***
  - **Racine** – LaunchBox
  - **Eau Claire** - Western Dairyland
  - **Ladysmith** – Indianhead Community Action

www.wispro.org

Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)

Marc N. Violante

Wisconsin Procurement Institute

June 28, 2016

WPI Wisconsin Procurement Institute

Webinar Overview

- Relevant background
  - Why we are here
  - Issues, the threats, are – ubiquitous, omnipresent, and growing
- Review of new clause requirements
- Main differences (requirements) of DFARS 252.204-7012
- Organizations – resources
- Training/Information resources
- Questions

Wisconsin Procurement Institute

If it were only so easy

Source: Cone of Silence - Wikipedia, the free encyclopedia en.wikipedia.org

Wisconsin Procurement Institute

The World today

Part of the issue

Cybercrime cost businesses around $500 billion in 2015, and a new report from Juniper Research says it will quadruple to $2 trillion by 2019. There are 1 million cybersecurity jobs open in 2016... nearly 300,000 of them in the U.S., and the labor shortage is getting worse, not better. There will be $100 billion in spending on cybersecurity over the next four to five years, cybercrime is on the rise, and cybersecurity talent is hard to come by.

http://www.csoonline.com/article/3027383/security/top-five-u-s-defense-contractors-bungle-commercial-cybersecurity-market-opportunity.html

Another issue

Wisconsin Procurement Institute

Rippling impacts

June 27, IDG News Service – (National) **IRS kills electronic filing PIN feature due to repeated attacks.** The U.S. Internal Revenue Service announced the week of June 20 that it will retire its Electronic Filing (E-File) Personal Identification Numbers (PINs) Web application, which was used for obtaining PINs that taxpayers could use to file tax returns electronically due to questionable activity after hackers used stolen taxpayer information to obtain 101,000 E-file PINs through its Web site on several occasions. Source: http://www.networkworld.com/article/3088671/irs-kills-electronic-filing-pin-feature-due-to-repeated-attacks.html

Copied from: DHS Open Source Daily Infrastructure Report, Item 17, June 28, 2016

Wisconsin Procurement Institute

Unseen, unexpected threats

June 26, Softpedia – (International) **Uber bugs allowed hackers to gather details on rides, drivers, passengers.** Security researchers from Integrity discovered 14 issues in Uber Technologies Inc.'s system that could be exploited to extract user details via the mobile app's Help Section, obtain a driver's and user's universally unique identifier (UUID) and request private information such as names, pictures, location, car types, status, among other data, and use over 1,000 active promo codes that could have added $100 to each driver's fair earnings, among other flaws.
Source: http://news.softpedia.com/news/uber-bugs-allowed-hackers-to-gather-details-on-uber-rides-drivers-passengers-505663.shtml

Copied from: DHS Open Source Daily Infrastructure Report, Item 24, June 28, 2016

What happens when ----

Ours

Theirs

Images copied from: eglin.af.mil

Wisconsin Procurement Institute

Threat Landscape

- Ransomware
- Spear fishing
- Cyber Threats
- Social Engineering
- Spoofing
- Impersonation

Wisconsin Procurement Institute

Perspective

- Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before.
- In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before.
- In 2015, a record-setting total of nine mega-breaches were reported. (A mega-breach is defined as a breach of more than 10 million records.)
- **Major Security Vulnerabilities in Three Quarters of Popular Websites Put Us All at Risk**

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

Small Business at risk

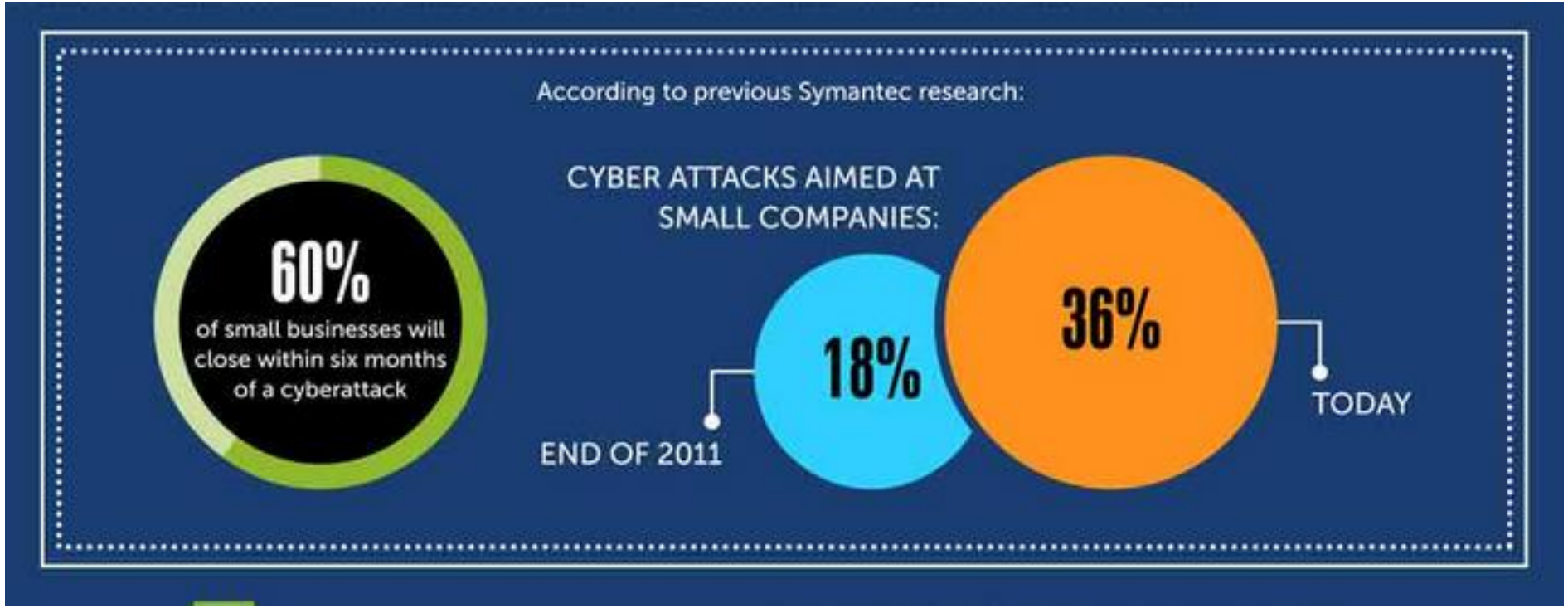
- It's not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and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

Hid for two years!

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

Wisconsin Procurement Institute

There is more to it that the clause



Source: https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

WPI Wisconsin Procurement Institute

The Insider Threat

- While insider theft only accounted for around 10 percent of data breaches in 2015, the NetDiligence Cyber Claims study reported that there was insider involvement in 32 percent of the claims submitted in 2015.
- According to its CEO, a disgruntled insider was alleged to have been responsible for one of the most publicized data breaches of the year, at Ashley Madison. Although this has not been confirmed, if true, it highlights the potential damage a malicious insider can inflict.

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

Who is really working for you?

June 24, KRCR 7 Redding/Chico – (California) **Mercy Medical patient records compromised.** Mercy Medical Center in California announced June 24 that it will notify 520 Redding patients after files containing the patients' personal and medical information were inappropriately accessed by the medical center's business partner, naviHealth, Inc., June 6. Officials stated that from June 2015 – May 2016 naviHealth unknowingly employed an individual who worked under an assumed identity and nursing license, and accessed patient files.
Source: http://www.krcrtv.com/mercy-medical-patient-records-compromised/40213616

Copied from: DHS Open Source Daily Infrastructure Report, Item 16, June 28, 2016

Wisconsin Procurement Institute

COUNTERINTELLIGENCE

"Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016. The sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact."

The Insider Threat

- More than three-quarters of US government agencies surveyed in the MeriTalk Federal Insider Threat Report say their agency is more focused on combating insider threats today than one year ago.

In the past year, **nearly half** of Federal agencies were targets of insider threats and **nearly one in three** (29 percent) lost data to an insider incident. As agencies are entrusted with storing and managing a range of sensitive information, the potential channels for data loss are becoming more complex, and breaches perpetrated by insiders – whether **malicious** or **unintentional** – are a growing problem.

Internet Security Threat Report, Volume 21, April 2016, Symantec & https://www.meritalk.com/study/inside-job/

However…

- 65% say it is **common** for employees/contractors to email documents to personal accounts
- 51% say it is **common** for employees/contractors to not follow appropriate protocols
- 40% say **unauthorized employees** access government information they shouldn't at least weekly

https://www.meritalk.com/study/inside-job/

Wisconsin Procurement Institute

June 24, Toledo Blade – (Ohio) **Ex-therapist found guilty of accessing patient records.** A former respiratory therapist at ProMedica Bay Park Hospital in Ohio was found guilty June 23 of accessing nearly 600 confidential patient records between March 2013 and March 2014 in order to determine which patients' were prescribed pain medication in an attempt to take the pills.

Source: http://www.toledoblade.com/Courts/2016/06/24/Ex-therapist-found-guilty-of-accessing-patient-records.html

June 24, Help Net Security – (International) **Crypto-ransomware attacks hit over 700,000 users in one year.** Security researchers from Kaspersky Lab reported that there was a 17.7 percent increase in encryption ransomware attacks between April 2015 and March 2016 after discovering 718,536 users were infected with crypto-ransomware. Researchers advised customers to use a reliable security solution, back-up all files, and keep all software up-to-date to avoid infection, among other recommendations.

Source: https://www.helpnetsecurity.com/2016/06/24/crypto-ransomware-attacks-hit-700000-users/

June 23, Softpedia – (International) **Six malicious Android apps removed from the Google Play store.** Google reported that it removed six Android applications that were reported to have malicious actions after a security researcher from Dr. Web discovered the apps infected more than 55,000 users with the Android.Valeriy malware via the Google Play store. Once the malware is installed, it connects to a command-and-control (C&C) server from which it receives a list of Uniform Resource Locators (URLs) and opens the links in the WebView browser component.

Source: http://news.softpedia.com/news/six-malicious-android-apps-removed-from-the-google-play-store-505604.shtml

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

Infrastructure

- A major US network equipment manufacturer acknowledged last December that someone repeatedly gained access to its network to change source code in order to make its products' default encryption breakable. The intruders also introduced a default password to enable undetected access to some target networks worldwide.

Cyber – just the tip of the iceberg?

"I have one energy client that conducted an online search as part of an exposure assessment and found critical plans for some of its facilities out there on the Internet."

Copied from: http://www.riskandinsurance.com/fueling-cybersecurity/ visited, March 5, 2016

Wisconsin Procurement Institute

Cyber attackers are playing the long game against large companies, but all businesses of all sizes are vulnerable to targeted attacks. **In fact, the number of spear-phishing campaigns targeting employees increased 55% in 2015.**

2013	2014	2015
779	841	1,305
+91%	+8%	+55%

Source: Symantec

Wisconsin Procurement Institute

BUSINESS | SMALL BUSINESS

Hackers Trick Email Systems Into Wiring Them Large Sums

Scrap processor thought it paid $100,000 to its vendor: 'We in fact had sent a wire to who knows where'

THE WALL STREET JOURNAL.

By RUTH SIMON

87 COMMENTS

July 29, 2015 6:43 p.m. ET

Cybercriminals are exploiting publicly available information and weaknesses in corporate email systems to trick small businesses into transferring large sums of money into fraudulent bank accounts, in schemes known as "corporate account takeover" or "business email fraud."

Seagate Technology – phishing email

- Seagate Technology reported that its employees' personal information was compromised after a phishing email disguised as a legitimate internal company request **prompted an employee to disclose employee data** to an unauthorized third party. – *CNBC*

Copied from: DHS Open Source Daily Infrastructure Report, Top Stories, March 8, 2016

Wisconsin Procurement Institute

Small Business – security practices

https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

4.1903 Contract clause.

- The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

Wisconsin Procurement Institute

“Covered contractor information system”

- means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

➢If you take a USB home, and work on your personal computer is that system now a “covered” system?

➢How about a work computer used at home and which connects to the family’s WiFi?

Wisconsin Procurement Institute

“Federal contract information”

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

➢Formal review or casual process?

➢“generated for the Government” – internally created, stored, id’d?

Wisconsin Procurement Institute

“Information”

- means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

➢See: https://www.cnss.gov

➢Document 4009 – IT term glossary (103 pages)

Our Mission

➢The Committee on National Security Systems (CNSS) sets national-level Information Assurance policies, directives, instructions, operational procedures, guidance and advisories for United States Government (USG) departments and agencies for the security of National Security Systems (NSS). It provides a comprehensive forum for strategic planning and operational decision-making to protect NSS and approves the release of INFOSEC products and information to Foreign Governments.

“Safeguarding”

- means measures or controls that are prescribed to protect information systems.

➢---- something happens, a breach of some sort
  - Are you relying on a “home brew solution”
  - A NIST framework
  - Center for Internet Security – 20 controls, framework
  - Other

Wisconsin Procurement Institute

Minimum Security Controls (i - iii)

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.

Limit! Limit! Limit! – restrict, control, determine access required

Wisconsin Procurement Institute

Minimum Security Controls (iv - vi)

- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Control, Identify, Authenticate – if something happens, can you document your actions, processes and corrections?

Minimum Security Controls (vii – ix)

- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

Sanitize or destroy, Limit physical access, Escort visitors –

-- know and understand
-- establish process, train
-- evaluate, test (audit)
-- document

WPI Wisconsin Procurement Institute

Minimum Security Controls (x – xii)

- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.

Identify, report, and correct

Wisconsin Procurement Institute

Minimum Security Controls (xiii – xv)

- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Provide protection (AV+), Update, scan – active, consistent involvement
Is everyone on the same page? Sales, satellite offices, other, is there an inventory, who maintains, frequency. Is the inventory, part of the plan?

Wisconsin Procurement Institute

Other requirements

- This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

-DFARS
-Distribution Statements
-Joint Certification Program
-ITAR
-Other

Wisconsin Procurement Institute

Frameworks – Other requirements

- SP 800-53
- SP 800-171
- NIST 32 – Establishing or Improving a Cyber Security Program
- Referenced in DFARS (252.204-7008/7012)
- 252.204-7000 “Mother may I”
- Solicitation/contract/subcontract requirements
- Framework for Improving Critical Infrastructure Cybersecurity, NIST, February 12, 2014

WPI Wisconsin Procurement Institute

Subcontracts (flow-down required)

- The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

➢How do you “on-board” your subcontractors?

- Vetting
- Training
- Reviews
- May impact costs, & other performance

Wisconsin Procurement Institute

General thoughts

- Adhoc or formal compliance –
  - Do you have a plan?
  - Can you prove that actions have been completed?
- Be wary of “free”products/services
  - Software – google docs – “Harry Potter”
  - Networks – Wireshark, able to view
  - What networks are used
- Wireless router placement/operation
  - Access from outside the office/building?
  - Access 24/7 – is this access needed?
- Cyber Insurance
  - Do you have – do you need?

WPI Wisconsin Procurement Institute

Major differences with 252.204-7012

- Requires – adequate security
- Defines –
  - compromise
  - controlled technical information
  - cyber incident
  - exfiltration
  - rapidly reporting - ~ 72 hours after cyber incident
- Requires - security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171
- !!! *Cyber incident reporting requirement*

Wisconsin Procurement Institute

Resources

- General information
- Keeping current
- Getting assistance
- Sharing information
- Best practices
- Training resources

Wisconsin Procurement Institute

NIST SP 800-171

TABLE 1: SECURITY REQUIREMENT FAMILIES

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

Wisconsin Procurement Institute

NIST SP 800-171 – example (access control)

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	A.9.1.2	Access to networks and network services
				A.9.2.3	Management of privileged access rights
				A.9.4.4	Use of privileged utility programs
				A.9.4.5	Access control to program source code
		AC-6(1)	Least Privilege *Authorize Access to Security Functions*	*No direct mapping.*	
		AC-6(5)	Least Privilege *Privileged Accounts*	*No direct mapping.*	

Wisconsin Procurement Institute

The CIS Critical Security Controls for Effective Cyber Defense

The CIS Critical Security Controls for Effective Cyber Defense

The CIS Critical Security Controls for Effective Cyber Defense

CSC 2: Inventory of Authorized and Unauthorized Software		
Family	**Control**	**Control Description**
System	**2.1**	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

The CIS Critical Security Controls for Effective Cyber Defense

The CIS Critical Security Controls for Effective Cyber Defense

DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program

- Part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities" of title 32, Code of Federal Regulations (CFR),
- DoD shares
  - unclassified and classified cyber threat information
  - IA best practices and related information, with participating DIB companies.
- In addition, relationships are established with company senior officials (e.g., Chief Information Officer (CIO), Chief Information Security Officer (CISO), etc) and their respective staffs. Your company's Chief/Facility Security Officer(s) also will be involved since DoD shares classified under the program.
- Eligibility

  Have or acquire DoD-approved medium assurance External Certificate Authority (ECA) certificates.

  Have an existing active Facility Security Clearance (FCL) granted under the National Industrial Security Program Operating Manual (NISPOM) (see DoD 5220.22-M) with approved safeguarding for at least Secret information

  Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM, Chapter 9, Section 4.

  Obtain access to DoD's secure voice and data transmission system supporting the DIB CS/IA program.

  Own or operate an unclassified information system that processes, stores, or transmits DoD information.

  Execute the standardized Framework Agreement (FA), which implements the requirements set forth in part 236, title 32 CFR, sections 236.4 through 236.6.

WPI Wisconsin Procurement Institute

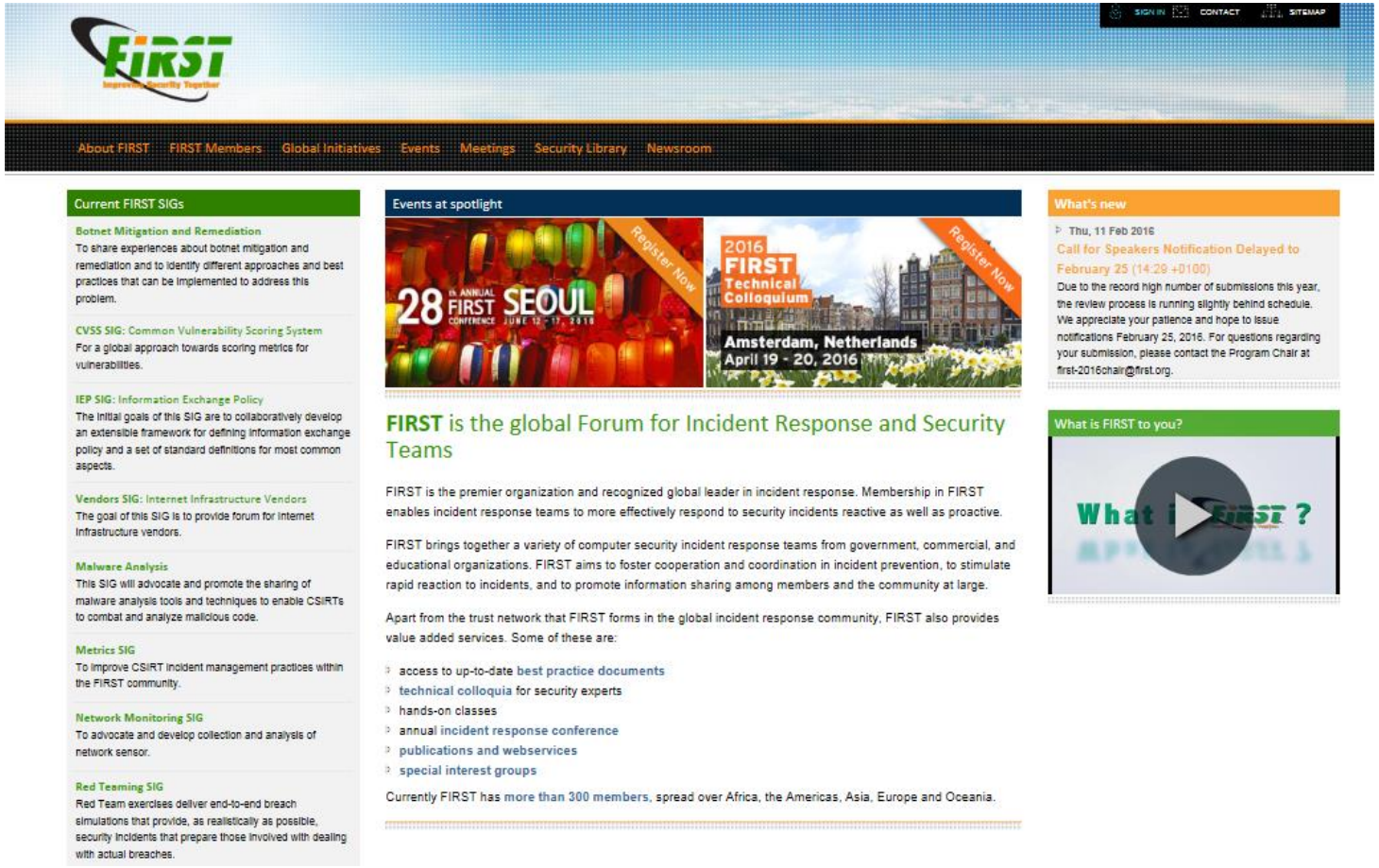
InfraGard

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

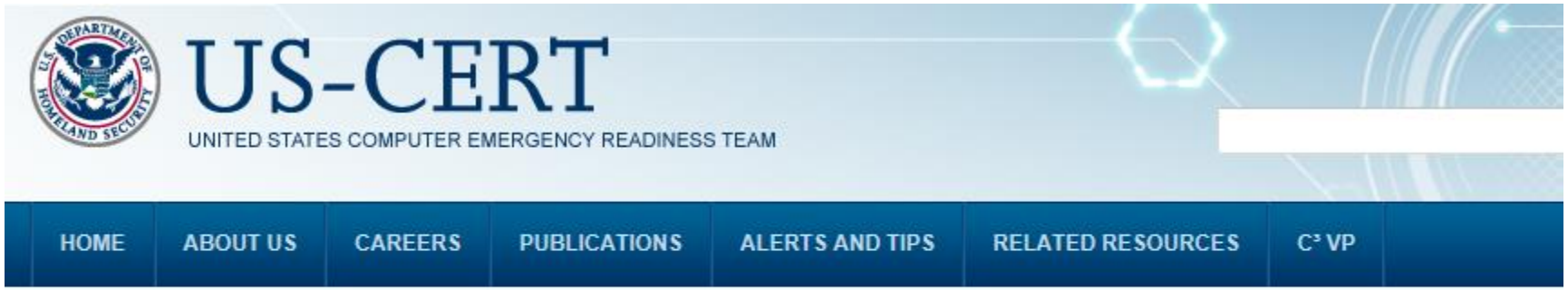
Source: www.infragard.gov

Wisconsin Procurement Institute

First.org



Wisconsin Procurement Institute



Bulletin (SB16-095)

Vulnerability Summary for the Week of March 28, 2016

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- autodesk_backburner	Stack-based buffer overflow in manager.exe in Backburner Manager in Autodesk Backburner 2016 2016.0.0.2150 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted command. NOTE: this is only a vulnerability in environments in which the administrator has not followed documentation that outlines the security risks of operating Backburner on untrusted networks.	2016-03-28	7.8	CVE-2016-2344 CERT-VN
cisco -- ios	The IKEv2 implementation in Cisco IOS 15.0 through 15.6 and IOS XE 3.3 through 3.17 allows remote attackers to cause a denial of service (device reload) via fragmented packets, aka Bug ID CSCux38417.	2016-03-25	7.1	CVE-2016-1344 CISCO
cisco -- ios	Cisco IOS 15.0 through 15.5 and IOS XE 3.3 through 3.16 allow remote attackers to cause a denial of service (device reload) via a crafted DHCPv6 Relay message, aka Bug ID CSCus55821.	2016-03-25	7.8	CVE-2016-1348 CISCO

Login

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

Reading Room

Take Cyber Insurance Survey for Chance to Win a $400 Amazon Gift Card!

SURVEY: Tell us how the healthcare industry is - OR should be - addressing infosec

More than **75,000 unique visitors** read papers in the Reading Room every month and it has become the starting point for exploration of topics ranging from SCADA to wireless security, from firewalls to intrusion detection. The SANS Reading Room features over 2,490 original computer security white papers in 96 different categories.

Latest 25 Papers Added to the Reading Room

SANS eNewsletters

Receive the latest security threats, vulnerabilities, and news with expert commentary

Get **Newsletters**

DIB ISAC

Wisconsin Procurement Institute

National Initiative for Cybersecurity Careers and Studies

Wisconsin Procurement Institute

Take advantage of resources and tools

Source -- https://niccs.us-cert.gov/research/cybersecurity-workforce-development-toolkit; visited June 27, 2016

WPI Wisconsin Procurement Institute

NIST ‘RAMPS’ Up Cybersecurity Education and Workforce Development With New Grants

May 12, 2016

The National Institute of Standards and Technology (NIST) is offering up to $1 million in grants to establish up to eight Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development. As part of the Department of Commerce’s “Skills for Business” initiative that has made job-driven training a priority, RAMPS will support the NIST-led National Initiative for Cybersecurity Education (NICE).

Source -- http://www.nist.gov/itl/acd/nist-ramps-up-cybersecurity-education-and-workforce-development-with-new-grants.cfm; visited June 27, 2016

Resources

- Cybersecurity Workforce Planning Diagnostic
  - https://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic
- NICCS: https://niccs.us-cert.gov/training/tc/search - Training Catalog
  - 2,000 courses
- SANS institute

Wisconsin Procurement Institute

Veterans have access to free training

https://niccs.us-cert.gov/training/fedvte

https://www.sans.org/cybertalent/vetsuccess-pilot?msc=sctslider

WPI Wisconsin Procurement Institute

Upcoming WPI Events

- ***Acquisition Hour Live Webinar Series*** *- Tuesdays and Wednesdays including:*

  Acquisition Hour –WHAT'S UP WITH FEDERAL GOVERNMENT END OF YEAR SPENDING FOR 2016? *: June 29th – Noon – 1.00pm*

  Acquisition Hour – MARKET RESEARCH – USING THE FEDERAL PROCUREMENT DATA SYSTEMS (FPDS) – PART 1 *: July 13th - Noon – 1.00pm*

  Acquisition Hour – MARKET RESEARCH – USING THE FEDERAL PROCUREMENT DATA SYSTEMS (FPDS) – PART 2 *: July 17th - Noon – 1.00pm*

QUESTIONS???

Continuing Professional Education

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

For Assistance or Additional Information - Contact

Wisconsin Procurement Institute (WPI)
Benjamin Blanc
10437 Innovation Drive, Suite 320
Milwaukee, WI 53226
414-270-3600 or benjaminb@wispro.org