




A Procurement Technical
Assistance Center (PTAC)

A photograph of the Wisconsin State Capitol building at dusk. The building is illuminated with warm lights, and its green dome is a prominent feature. The sky is a deep blue, and trees with autumn foliage are visible in the foreground.

ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS

September 13, 2017



WEBINAR ETIQUETTE

- Please
 - When logging into go-to-meeting, enter the name that you have registered with
 - Put your phone or computer on mute
 - Use the Chat option to ask your question(s): We will read them and our guest speaker will provide an answer to the group
- Thank you!

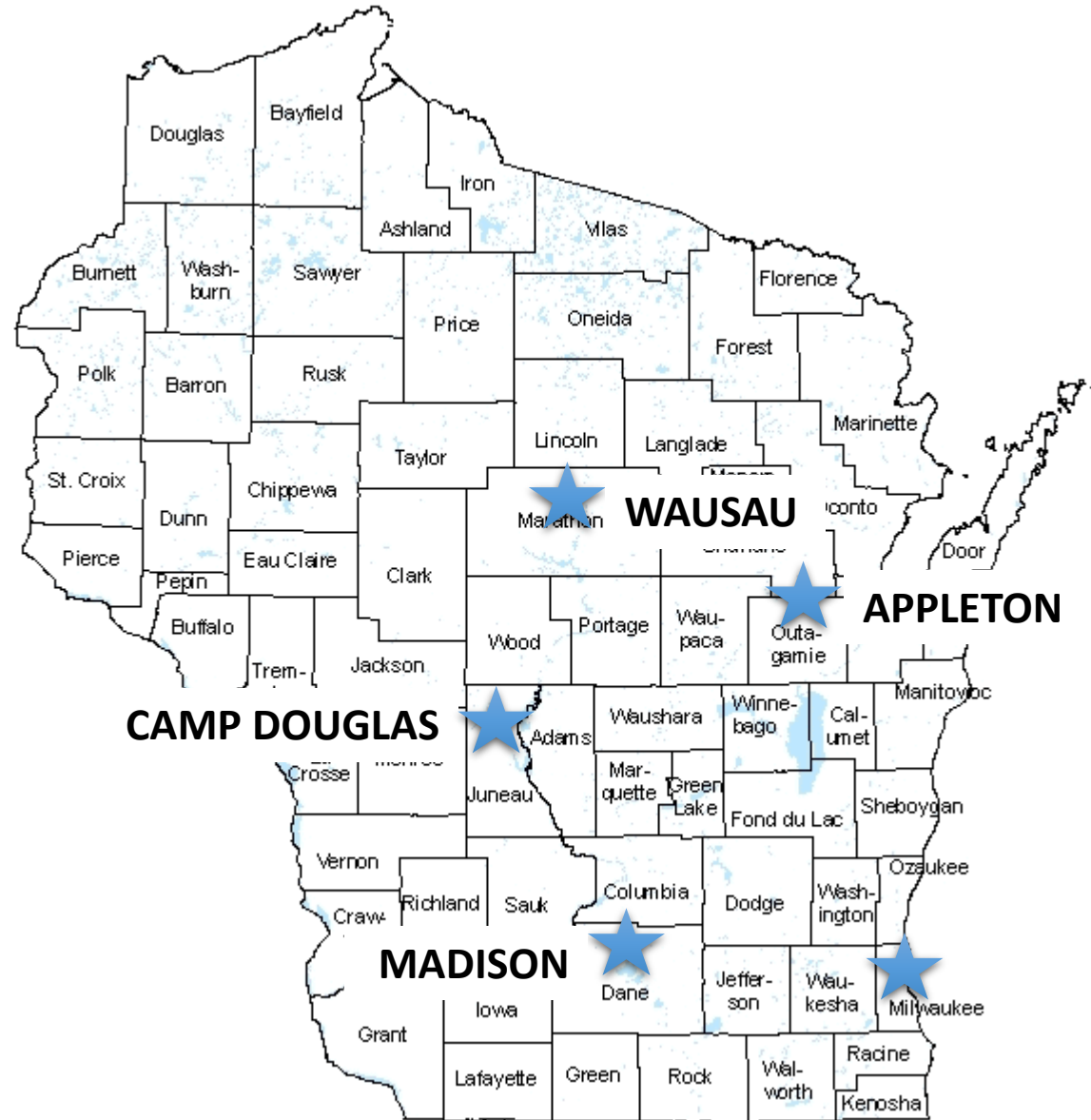
ABOUT WPI

SUPPORTING THE MISSION

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

WPI OFFICE LOCATIONS

- MILWAUKEE – *Technology Innovation Center*
- MADISON –
 - *Madison Enterprise Center*
 - *FEED Kitchens*
- CAMP DOUGLAS – *Juneau County Economic Development Corporation (JCEDC)*
- WAUSAU – *Wausau Region Chamber of Commerce*
- APPLETON – *Fox Valley Technical College*



Search ...

BLOG

SERVICES

ABOUT

MY ACCOUNT

DONATE

CONTACT



EVENT
CALENDAR

FEDERAL
GOVERNMENT

STATE & LOCAL
GOVERNMENT

OTHER
GOVERNMENT &
GRANTS

SUCCESS &
AWARDS

FAQS

WPI'S CURRENT NEWSLETTER

www.wispro.org

UPCOMING EVENTS [→](#)

AUGUST 16 2017

ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS

AUGUST 17 2017

ACQUISITION HOUR - THE END OF THE FISCAL YEAR IS HERE: WHAT IS HOT AND WHAT IS NOT

SEPTEMBER 19 2017

ACQUISITION HOUR: SELLING TO THE STATE OF WISCONSIN AND LOCAL GOVERNMENTS

SEPTEMBER 20 2017

ACQUISITION HOUR: OVERVIEW OF THE FEDERAL ACQUISITION REGULATIONS (FAR)

OCTOBER 4 2017

ACQUISITION HOUR: ESRS INDIVIDUAL SUBCONTRACTOR REPORTING (ISR) BASICS

CURRENT OPPORTUNITIES (5) [→](#)

SERVICES OFFERED BY WPI

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

CYBER FUNDAMENTALS FOR DFARS 252.204-7012 IMPLEMENTATION

Marc N. Violante

Wisconsin Procurement Institute

September 13, 2017



Image source: readywisconsin.wi.gov

Webinar Overview

1. Background
2. Definitions
3. Threats
4. Actions
5. Resources
6. Moving forward





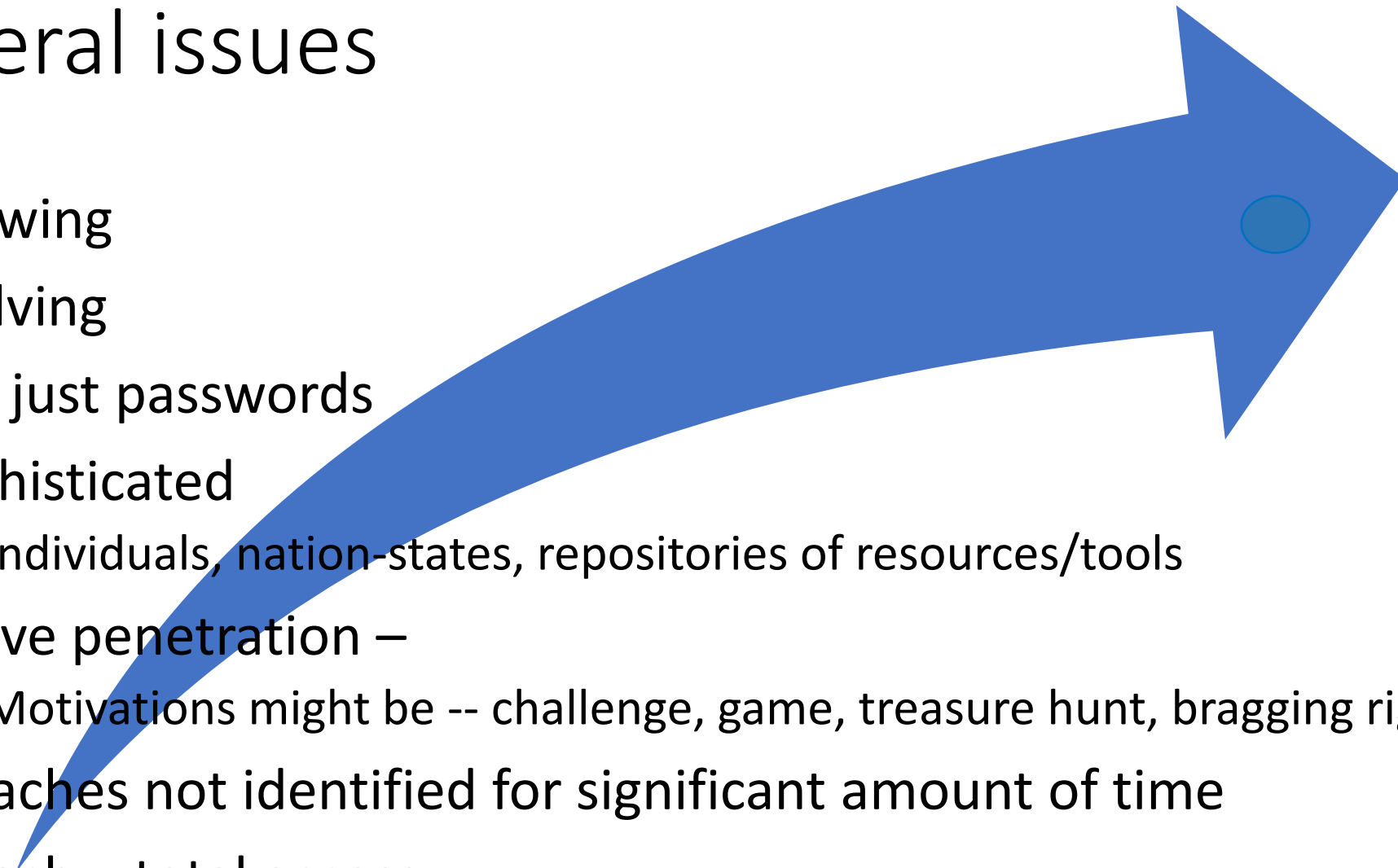
US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

5 Questions CEOs Should Ask About Cyber Risks

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

General issues

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

U.S. Steel is now claiming research on creating the next generation of high-strength steel was taken and reproduced in China. “

They couldn't figure out how to move to the next level,” said Debbie Shon, an attorney representing U.S. Steel in the petition. “After the hack they were able to.”

<http://www.engineering.com/AdvancedManufacturing/ArticleID/12050/Manufacturing-Sector-Identified-as-Leading-Target-of-Infrastructure-Cyber-Attacks.aspx>

Manufacturing Sector Identified as Leading Target of Infrastructure Cyber-Attacks; visited May 9, 2016

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

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



Hid for two years!

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

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

In the News – Summer of 2016

CHINESE HACKERS TARGET US MILITARY

In July this year, a Chinese national was sentenced in Los Angeles to three years and 10 months in prison for hacking US defense contractors to steal trade secrets on Beijing's behalf.

Su Bin, 51, who went by the names Stephen Su and Stephen Subin, was also ordered by a federal judge to pay a \$10,000 fine.

Su in March had admitted in a plea agreement with US authorities to conspiring with two unnamed military officers in China to try to acquire plans for F-22 and F-35 fighter jets and Boeing's C-17 military transport aircraft.

According to court documents, the trio managed to steal sensitive data by hacking into the computer networks of major defense contractors and sent the information to China.

Washington and Beijing have repeatedly clashed over what the US describes as rampant cyberspying by the Chinese government on US industry.

<http://www.dailymail.co.uk/sciencetech/article-3888942/Chinese-stealth-fighter-shed-cloak-secrecy.html> Visited: 9/12/2017

9/13/2017

“The Spies had come without warning. They plied their craft silently, stealing secrets from the world’s most powerful military. They were at work for months before anyone noticed their presence. And when American officials finally detected the thieves, they saw that it was too late. The damage done.”

Prologue: @War the Rise of the Military Internet Complex



Image copied from: fbi.gov

What happens when ----



Ours



Theirs

Images copied from: eglin.af.mil

9/13/2017

DoD awareness of the issue

Secretary of Defense Jim Mattis visits Google Headquarters

Press Operations

Release No: NR-287-17

Aug. 11, 2017 Alpha [15](#)

[PRINT](#) | [E-MAIL](#)

Chief Pentagon Spokesperson Dana W. White provided the following readout:

Today Secretary Jim Mattis visited Google headquarters and met with leadership to discuss innovative new technologies and methods to best leverage advancements in artificial intelligence, cloud computing and cybersecurity for the Department of Defense.

The secretary emphasized that the DoD must continue to be a smart user of commercial technology and able to innovate at the speed of relevancy.

In the News – Summer of 2015

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

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

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

- “Expensive data-security systems and high-priced information security consultants don’t faze today’s hackers.”
- Hackers have – time and resources They also share
- In the NY Law firm case, “attackers **attempted to penetrate targeted servicers more than 100,000 times over seven months.**”
- “It has become abundantly clear that no network is completely safe. “

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

9/13/2017

In the News – Summer of 2015 – key point

“Where once companies thought that they could defend themselves against an onslaught, they’re now realizing that resistance is, if not futile, certainly less important than have a plan in place to detect and neutralize intruders when they strike.”

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

9/13/2017

Key Decision(s) related to Cyber preparedness

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

Information Security – formal definition

“The protection of information and information systems from **unauthorized** access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” [44USC].

Information Security – key elements

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

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

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

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

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

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

Cyber Security

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

What is a cyber incident?

- A cyber incident is defined as actions taken through the use of computer networks that result in a **compromise** or an **actual or potentially adverse effect** on an information **system and/or the information** residing therein.

According to - DoD's DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal; the recipient of the required cyber incident report.

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

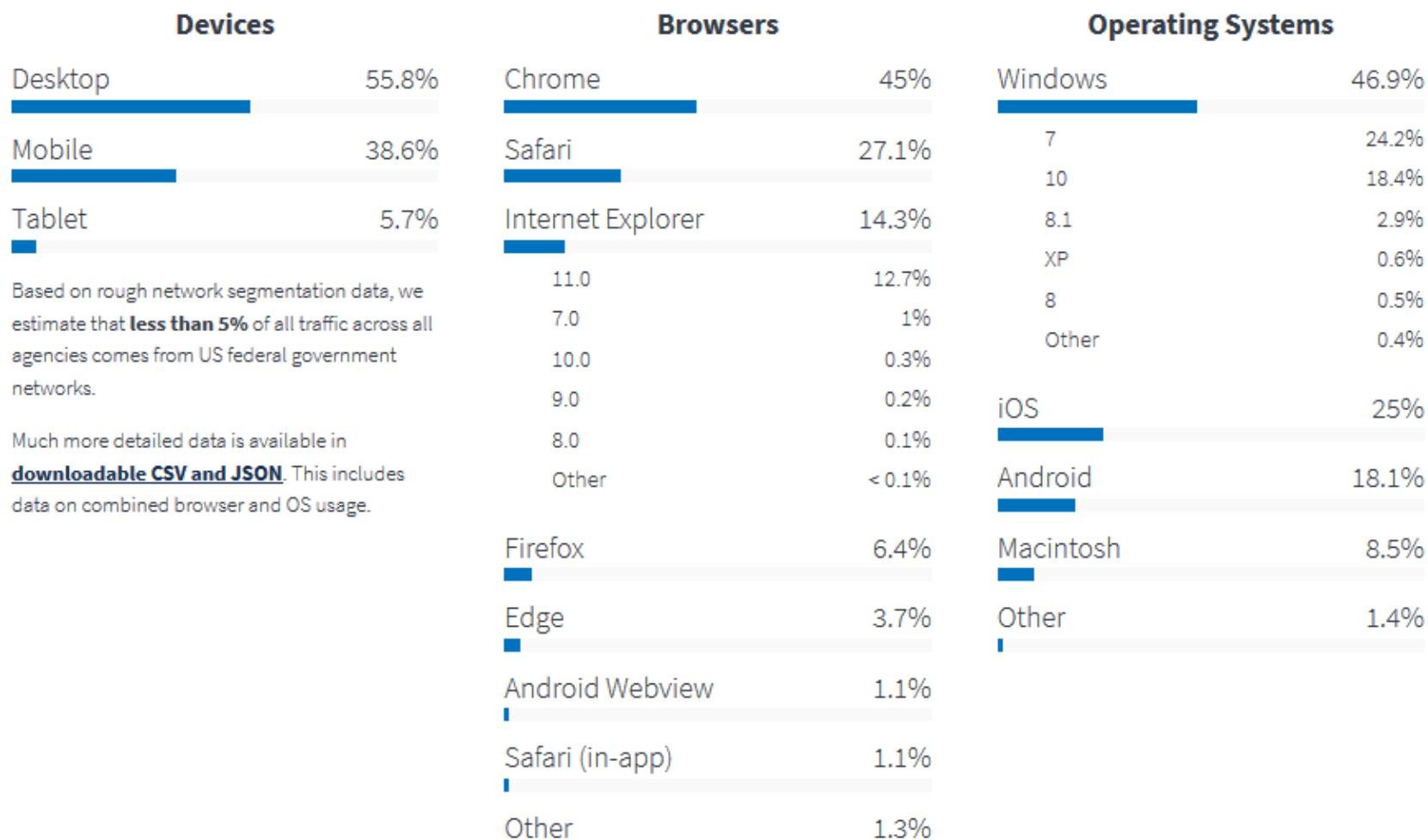
Who is visiting your site?



<https://analytics.usa.gov/> visited 8/9/2017

9/13/2017

There were **2.28 billion** visits over the past 90 days.



Visitor Locations Right Now

Cities	
New York	4%
Washington	3.1%
Chicago	1.7%
Los Angeles	1.6%
Plano	1.6%
Houston	1.3%
Dallas	1%
San Diego	1%
Seattle	0.9%
Kansas City	0.8%

Countries	
United States	85.5%
International	14.5%
Mexico	1.6%
Canada	1.4%
India	1.1%
United Kingdom	0.9%
Colombia	0.6%
Spain	0.6%
Argentina	0.5%
Brazil	0.4%
Chile	0.4%
Germany	0.3%
Peru	0.3%
Puerto Rico	0.3%
Philippines	0.2%
Ecuador	0.2%
France	0.2%

Visitor demographics for all participating agencies

Description	Download	Update frequency
Language	CSV JSON	Daily
Visitors per country	JSON	Every 5 minutes
Visitors per city	JSON	Every 5 minutes
Desktop/mobile/tablet	CSV	Daily
Web browsers	CSV JSON	Daily
<ul style="list-style-type: none"> Versions of Internet Explorer 	CSV JSON	Daily
Operating systems	CSV JSON	Daily
<ul style="list-style-type: none"> Versions of Windows 	CSV JSON	Daily
OS & browser (combined)	CSV JSON	Daily
Windows & browser (combined)	CSV JSON	Daily
Windows & IE (combined)	CSV JSON	Daily
Screen sizes	CSV JSON	Daily
Device model	CSV JSON	Daily

Vulnerabilities lead to different paths of attack

Notes by CVSS Environmental Score

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

What data/information is on your computer?

On your Network?

What devices are being used?

What are the entry points?

Are the security/safeguarding requirements all the same? – different customers, different types of data/information



Risks - Identify and Prioritize Information Types

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

Current Status – ongoing process

No issues

- Review complete, no issues identified

Unknown

- Reviews in progress
- Issues/questions require resolution

Issues present

- Unauthorized logins
- Questionable log activity
- External information – complaints, issues, other

Key Documents – information, ready access

Partial list

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

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

Cyber Incident Record Retention/Availability

- Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor **shall preserve and protect** images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data **for at least 90 days** from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with **access to additional information or equipment** that is necessary to conduct a forensic analysis.

DFAR 252.204-7012

- Contractor systems with – Covered Defense Information
 - transiting | stored | transmitted from
- Required to provide Adequate Security
 - Implement NIST(SP) 800-171 **at a minimum**
- Monitor network/system
- Perform investigation when required – breach
- Report to dibnet.mil within 72 hours
 - IASE Medium Security Certificate required, 3 – 7 days
 - Account with dibnet.mil, requires certificate

Covered contractor information system

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

DFARS 252.204-7012 Definitions

Subcontracts – the contractor shall

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

Indications of CDI

What came first? The
Chicken or the Egg?

- Review/inventory of computer/system files / storage
- DFAR clause – 252.204-7012
- DFAR clause – 252.204-7000 (“Mother may I”)
- Reference to the Joint Certification Program (JCP)
- Reference to Distribution Statements
- Language (ex) Controlling Unclassified Military Technology
- Item – listed on USML, ITAR
- Prime - states or requires
- Defined: <https://www.archives.gov/cui/registry>

DFARS incorporated into contract

- THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED INTO THE SOLICITATION:
- DFARS 252.204-7008-Compliance with Safeguarding Covered Defense Information Controls (DEVIATION 2016-O0001) (OCT 2015) and
- DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (DEVIATION 2016- O0001) (OCT 2015) are incorporated by reference via the DPAP class deviation website (http://www.acq.osd.mil/dpap/dars/class_deviations.html).
 - Example only showing the incorporating language

“Mother may I” 252.204-7000

- (a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—
 - (1) The Contracting Officer has given prior written approval;
 - (2) The information is otherwise in the public domain before the date of release; or
 - (3) determined in writing by the contracting officer to be fundamental research in accordance with National Security Decision Directive 189 ... and other requirements

Joint Certification Program - requirements

- TO MANUFACTURE THIS ITEM, **NON-JCP CERTIFIED SUPPLIERS MUST SUBMIT A** CURRENT MANUFACTURING LICENSE AGREEMENT, TECHNICAL ASSISTANCE AGREEMENT, DISTRIBUTION AGREEMENT OR OFF-SHORE PROCUREMENT AGREEMENT APPROVED BY THE DIRECTORATE OF DEFENSE TRADE CONTROLS WITH THE OFFER, UNLESS AN EXEMPTION UNDER THE PROVISIONS OF ITAR SECTION, 125.4 EXEMPTIONS OF GENERAL APPLICABILITY, AND/OR EAR PART 740 ARE APPLICABLE.

Further dissemination of JCP Technical Data

- NOTE: JCP CERTIFIED CONTRACTORS WHO RECEIVE TECHNICAL DATA PURSUANT TO THEIR DD FORM 2345 CERTIFICATION **MAY NOT FURTHER DISSEMINATE SUCH DATA UNLESS FURTHER DISSEMINATION OF THE TECHNICAL DATA IS EXPRESSLY PERMITTED BY DODD 5230.25.**

NON-JCP certified suppliers

- NON-JCP CERTIFIED SUPPLIERS SEEKING EXPORT CONTROLLED TECHNICAL DATA ARE REQUIRED TO **PROVIDE** THE CONTRACTING OFFICER WITH AN **APPLICABLE AGREEMENT OR IDENTIFY** WHICH ITAR/EAR **EXEMPTION** APPLIES TO RECEIVE A COPY OF THE EXPORT CONTROLLED TECHNICAL DATA.

Controlled Technical Information

- Technical information with **military or space application** that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- - is to be **marked with one of the distribution statements B-through-F**, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical documents.
- The term **does not include information that is lawfully publicly available without restrictions.**



Distribution Statements

- A. Approved for public release.
- B. U.S. Government agencies only
- C. U.S. Government agencies and their contractors
- D. Department of Defense and U.S. DoD contractors only
- E. DoD Components only
- F. Further dissemination only as directed by

DoD Instruction 5230.24 August 23, 2012

Requirements for multiple individuals

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

Destruction notice

- Upon completion of the purposes for which Government Technical Data has been provided, the Contractor is
 - required to destroy all documents, including all reproductions, duplications, or copies thereof as may have been further distributed by the Contractor.
 - Destruction of this technical data shall be accomplished by: shredding, pulping, burning, or melting any physical copies of the TDP and/or deletion or removal of downloaded TDP files from computer drives and electronic devices, and any copies of those files.

Okay – now prove it!

Threat Landscape



- Detection
- Cyber Issues
- Ransomware
- Spear fishing
- Insider Threats
- Social Engineering
- Spoofing
- Impersonation

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>

9/13/2017

Indications of a Cyber Incident

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

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

9/13/2017

Logs & Cyber Incidents

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

Ransomware

- Individuals
- Police Department
- Hollywood Hospital
- Bitcoin
 - Several days to install
 - Must have access to a machine – may need to be dedicated
- Evolving threats – sophistication
 - Network backup
 - Mirrored systems

Ransomware

May 5, Softpedia – (International) **Ransomware infections grew 14 percent in early 2016, April the worst month.** Kaspersky, Enigma Software Group, and the FBI issued a warning to companies about the increase in ransomware infections following reports of at least 2,900 new ransomware variants, representing a 14 percent increase in Quarter 1 of 2016. Researchers also found a significant increase in the number of attacks during April.

Source: <http://news.softpedia.com/news/ransomware-infections-grew-14-percent-in-early-2016-april-the-worst-month-503743.shtml>
May 9th; DHS Daily Open Source

Uncharted waters - Bitcoin

March 6, Softpedia – (International) **First fully functional Mac ransomware spread via transmission BitTorrent client.** Researchers from Palo Alto reported that the official Transmission BitTorrent Web site used by Mac customers was allegedly hacked after researchers found that the Transmission Web site was replaced for Mac version 2.90, which came embedded with the KeRanger ransomware. The

- ➔ **ransomware targets** over 300 file extension types, uses Advanced Encryption Standard (AES) encryption to lock files, and demands a 1
- ➔ **Bitcoin** payment fee.

Source: <http://news.softpedia.com/news/first-fully-functional-mac-ransomware-spread-via-transmission-bittorrent-client-501411.shtml>

Copied from: DHS Open Source Daily Infrastructure Report, Item 22, March 8, 2016

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

Spyware

Class of malware that collect information from a computing system without the owner's consent – keystrokes, screenshots, credentials, personal email addresses, web form filed data, Internet usage habits and other

- Who would want to spy on me?
 - Marketers
 - Advertisers
 - Bad actors – data thieves
 - Employers
 - Trusted Insider
 - Employee – spyware to collect corporate information to sell
 - Spouse/family member/close relation
 - Cleaning crew/Contractor

Phishing – Tackle Box

- Bots/Botnets
 - Phishing Kits
 - Technical Deceit
 - Session Hijacking
 - Abuse of Domain Name Service (DNS)
 - Specialized Malware
- Normal user reactions – close pop-ups; what did I just click on?

Situational Awareness – users - Phishing

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

Insider threat

“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.”

May 5, KUSA 9 Denver – (Colorado) **CDOT employee stole contractors' personal information.** A Colorado Department of Transportation (CDOT) spokesperson announced May 5 that the personal information of hundreds of CDOT contractors may have been compromised after a data breach involving a CDOT employee who had access to a database for Emerging Small Business (ESB) and Disadvantaged Business Enterprise (DBE) which contained confidential information. Authorities stated that the businesses potentially impacted by the breach submitted information to CDOT in order to qualify for ESB and DBE programs.

Source: <http://www.9news.com/news/cdot-employee-stole-contractors-personal-information/175000302>

May 9th DHS Daily Open Source

Social Media Risk

- “The threats and exposures are many and varied. They range from a single rogue employee to organized crime to terrorists to spying by other nations. The threats can be theft of confidential personal data or proprietary competitive information, to malicious acts causing loss of data or actual disruption of operations.
- For the energy industry, which handles hazardous materials, a hacking event that leads to a spill becomes more than just a bad day at the office. “
- “Energy companies do not think of themselves as big users of social media,” said Westby, “but their employees are, and they tend to have employees in some very sensitive areas of the world.”

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

Cyber – phishing, spoofing, impersonation

*“February 29, ZDNet – (International) **Snapchat falls foul of CEO impersonation, hands over employee pay data.** The video messaging application, Snapchat reported that many of its current and former employees’ payroll information was compromised **after a cyber-attacker impersonated the firm’s chief executive officer (CEO) via a phishing campaign and collected employee payroll information from staff at the firm.** Snapchat stated that the incident was contained and reported the scheme to the FBI.*

Source: <http://www.zdnet.com/article/snapchat-falls-foul-of-ceo-impersonation-hands-over-employee-pay-data/> “

Copied from: DHS Open Source Daily Infrastructure Report, Item 14, March 1, 2016

CEO impersonation

“Glen, I have assigned you to manage file T521,” the phony message to the accounting director **Glen Wurm** allegedly read. “This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do not speak with anyone by email or phone regarding this. Regards, Gean Stalcup.”

Roughly 30 minutes later, Mr. Wurm said he was contacted via phone and email by Mr. Shapiro stating that due diligence fees associated with the China acquisition in the amount of \$480,000 were needed. AFGlobal claims a Mr. Shapiro followed up via email with wiring instructions.

<http://krebsonsecurity.com/tag/ceo-fraud/>


General principles

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

**Beware of free AV Software

Routers (partial list)

- Turn ping feature off – harder to locate
- Turn off the Auto ID feature
- Turn the device off when not needed/ limit footprint
- Change default login username and password
- Change the default SSID (Service set identifier)
- Password protect – min 8 characters
- Configure WPA2-AES for data confidentiality
- Enable router firewall – most (home) include
- Monitor wireless traffic – routine log scan unauthorized users*



Garbage
Boxes
Yard overgrown

PING'ng

- Turn ping feature off – harder to locate

```
TCP    192.168.5.216:50313    172.217.9.46:443      ESTABLISHED    8288
TCP    192.168.5.216:50315    172.217.8.197:443     ESTABLISHED    4732
TCP    192.168.5.216:50316    216.58.192.238:80     ESTABLISHED    8288
```

IP Lookup Result for 216.58.192.238			
IP Address:	216.58.192.238	City:	Mountain View
Host of this IP:	ord30s26-in-f14.1e100.net	Country:	United States 
Organization:	Google	State:	California
ISP/Hosting:	Google	Postal Code:	94043
Updated:	09/10/2017 11:31 AM	Timezone:	America/Los_Angeles
User Rating:	 Rated 4.5 / 5	Local Time:	09/13/2017 09:24 AM

Top screen shot from personal computer using netstat -aon; IP Lookup Results from ipaddress.com

9/13/2017

PING'ng - 2

- Turn ping feature off – harder to locate

```
C:\>ping 216.58.192.238

Pinging 216.58.192.238 with 32 bytes of data:
Reply from 216.58.192.238: bytes=32 time=36ms TTL=50
Reply from 216.58.192.238: bytes=32 time=32ms TTL=50
Reply from 216.58.192.238: bytes=32 time=34ms TTL=50
Reply from 216.58.192.238: bytes=32 time=31ms TTL=50

Ping statistics for 216.58.192.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 36ms, Average = 33ms
```

Free – well maybe sort of

- USB drives
 - Trade show – from who, what company
 - In the parking lot? – oh really
 - Let someone else be the good Samaritan!
- Software/Apps
 - It's free, but what access is required?
 - What do you know about the company?
 - Who have you trusted with your data/information?

Questionable Host – Reputation Risk method

- Site names recently registered –
 - Time registered loosely relates to risk
- Listed in threat resources (Robtex, malwaredomain, etc)
- No reverse lookup value
- Short / low TTL (<1 day, for example)
- IP address changes frequently
- Site names – “gibberish” can’t be read

Identifying a Suspicious host

- Contact the IP Address Owner
- Send Network Traffic to the IP Address
- Seek ISP Assistance
- Research the History of the IP Address
- Look for Clues in Application Content

NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 6.4.4 Attacker Identification page 6-17-6-18

Reputation Risk – resource sites

- <http://www.barracudacentral.org/lookups>
- <http://ipremoval.sms.Symantec.com/lookup/>
- <http://www.brightcloud.com/services/ip-reputation.php>
- <http://www.avgthreatlabs.com/website-safety-reports/>
- <http://www.malwaredomainlist.com/mdl.php>
- Others

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 114

Top 10 Ports – by Report

Port	Reports	Port	Targets	Port	Sources
<u>22</u>	106450	<u>23</u>	12254	<u>23</u>	39312
<u>23</u>	73916	<u>1433</u>	3822	<u>22</u>	4283
<u>53</u>	28051	<u>22</u>	3803	<u>445</u>	4105
<u>80</u>	27462	<u>445</u>	2765	<u>5358</u>	3738
<u>1433</u>	15769	<u>3389</u>	2244	<u>2323</u>	2834
<u>445</u>	12187	<u>2323</u>	1949	<u>1433</u>	2580
<u>3884</u>	6336	<u>8080</u>	1926	<u>53</u>	939
<u>2323</u>	4760	<u>5358</u>	1832	<u>2222</u>	679
<u>5358</u>	4475	<u>80</u>	1516	<u>80</u>	652
<u>8080</u>	3894	<u>7547</u>	1287	<u>51413</u>	639

www.dshield.org/top10.html; visited August 15, 2017

9/13/2017

Top 10 Source IP Addresses; associated with attacks

IP Address	Reports	Target IPs	First Seen	Last Seen
047.044.013.106 ()	2,498	2,498	2017-08-14	2017-08-14
190.082.065.155 ()	1,266	1,266	2017-08-15	2017-08-15
095.037.160.073 ()	781	313	2017-08-14	2017-08-14
045.021.028.162 ()	460	269	2017-08-15	2017-08-15
073.205.092.142 ()	387	264	2017-08-15	2017-08-15
207.255.216.192 ()	405	260	2017-08-15	2017-08-15
051.015.042.034 ()	259	259	2017-08-14	2017-08-14
119.001.109.096 ()	258	258	2017-08-14	2017-08-14
072.019.038.249 ()	423	257	2017-08-15	2017-08-15
125.077.017.172 ()	513	257	2017-08-14	2017-08-14

Option: Apply the Top 10 blacklist automatically to your firewall via ThreatSTOP.
Also can apply these IP's to a router.

www.dshield.org/top10.html; visited August 15, 2017

Threat Feeds

BOTS

[bebloh C&C server](#)
[Cryptowall C&C server](#)
[Dyreza Servers](#)
[Hesperbot C&C server](#)
[matsnu C&C server](#)
[Palevo C&C IP](#)
[qakbot C&C server](#)
[ramnit C&C server](#)
[Ransomips](#)
[Spyeye C&C server](#)
[Symmi C&C server](#)
[TinyBanker C&C server](#)
[Upatr Servers](#)
[Weblron Bots](#)
[Zeus C&C server](#)

OTHERS

[CI Army List](#)
[Emergingthreats](#)
[Forum Spammers](#)
[Malc0de Blacklist](#)
[TLD Name Servers](#)
[Tor Exit Node](#) ✓

PORT SCANNERS

[Port 110 Scanner](#)
[Port 143 Scanner](#)
[Port 21 Scanner](#)
[Port 22 Scanner](#)
[Port 25 Scanner](#)
[Port 443 Scanner](#)
[Port 80 Scanner](#)
[Port 993 Scanner](#)
[Apache Web Server Scanner](#)
[Asterisk VoIP Scanner](#)
[Suspect Bots/Infected](#)
[Bruteforce](#)
[courier imap attacker](#)
[courier pop3 attacker](#)
[OpenBL FTP Scanners](#)
[OpenBL HTTP Scanners](#)
[OpenBL MAIL Scanners](#)
[OpenBL SMTP Scanners](#)
[OpenBL SSH Scanners](#)

RESEARCH

[Blindferret](#)
[Erratasec Masscan](#)
[Rapid7Sonar](#)
[Shadowserver](#)
[ShodanHQ](#)
[UMichigan scans.io](#)

Forensics – planning considerations

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

Computer Security Logs

- Generated by many sources; provide documentation of activity
 - including security software,
 - antivirus software
 - Firewalls
 - Networking equipment
 - Servers
 - Routers
 - Switches
 - Intrusion detection prevention systems
 - Operating systems
 - Workstations

Log management

- Log identification
- Log generation
- Log transmission
- Log analysis
 - Staff
 - Collection
 - Tools - software
 - Periodicity
- Log storage and disposal procedures/protocol

Log analysis

What to Look For in **Logs**

An administrator should look for all of the following things in log files:

- Probes to ports that have no application services running
- Unsuccessful logins to the firewall
- Suspicious outbound connections
- Source-routed packets
- Host operating system log messages
- Changes to network interfaces
- Changes to firewall policy
- Additions, deletions, and changes of administrative accounts
- Dropped and rejected connections
- Time, protocol, IP addresses, and usernames for allowed connections

Log Protection

- logs contain records of system and network security
- they need to be protected from breaches of their confidentiality and integrity
- Improperly securing - intentional and unintentional alteration and destruction
 - May allow malicious activity to go on unnoticed
 - For example, many rootkits are specifically designed to alter logs
- Protect availability of logs – maximum size / overwriting

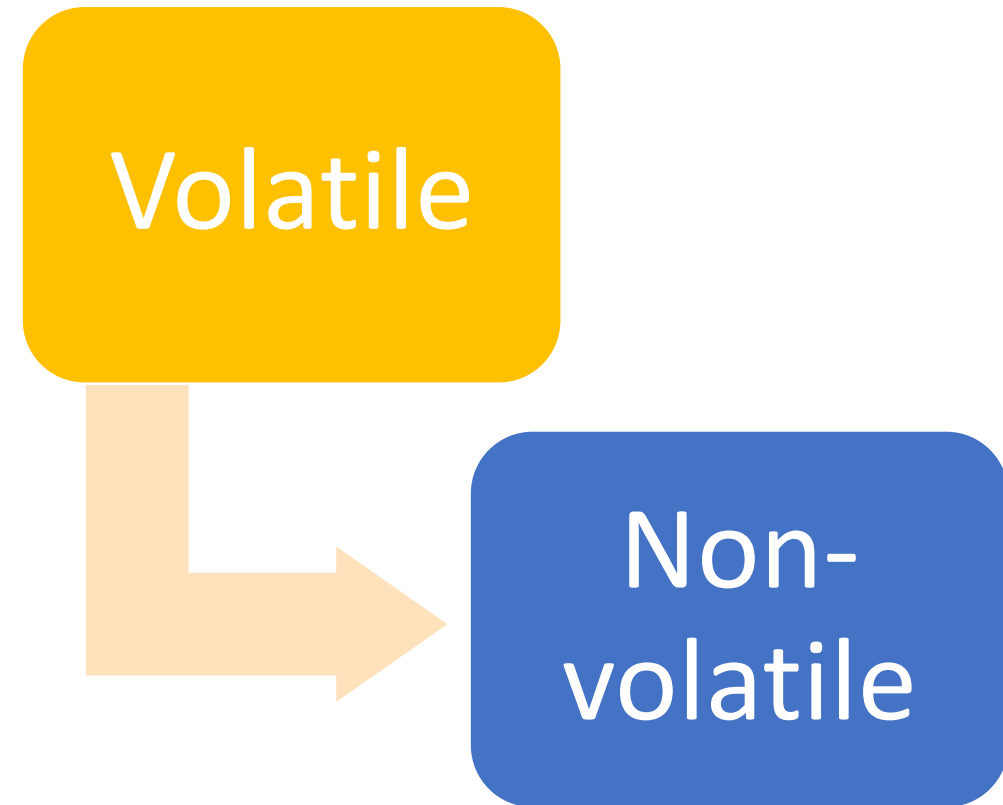
Maximizing Log value

- Identify as high priority
 - Combat the notion of boring and of low benefit
- Provide sufficient tools
 - Assists with automation
 - Helps to identify patterns that a human will not see
- Provide training for efficient performance
- Reactive tool
 - After an event

Collecting & Prioritizing Data Collection

Volatile Data - prioritized

1. Network connections
2. Login sessions
3. Contents of memory
4. Running processes
5. Open files
6. Network configuration
7. Operating system time



Volatile Data collection – trusted tools

- Netstat.exe –an - Lists active connects/open ports
- Netstat.ext –m - Lists the local routine table
- Pslist.exe - List running processes and associated data
- Openports.ext - Lists active connects and open ports
- Psloggedon.exe - Lists users logged on locally and via network share
- Psfile.ext - Lists files opened remotely
- Ipconfig.exe/all - Lists network adapter information
- Now.exe - Displays system date and time – (Time/Date – DOS)

Examining and Analyzing Network Traffic

- Establish monitoring level
- Identification of an event of interest
 - Assess
 - Extract
 - Analyze
- Goal –
 - What happened
 - Affect to/on the systems and network
- Simple – reviewing few logs
- Complex – review and analyze multiple sources

Examining and Analyzing Network Traffic

- Identify an Event of Interest
 - Someone, received indication – alert, complaint, operational issue – crash
 - Information results from security log review
- Examine Data Sources
- Examination and Analysis Tools
- Draw Conclusions

Network Security - approaches

- CM – Continuous Monitoring (DHS & NIST approach)
 - Vulnerability centric
 - Focuses on configuration and software weaknesses
- NSM – Network Security Monitoring
 - Threat-centric
 - Adversaries are the focus
 - Visibility vice control
- Others – eg. Firewall, antivirus, whitelisting
 - Each of these
 - Blocking, filtering, denying mechanism
 - Recognize malicious activity and stop it

Threats

- Can be internal
 - Staff
 - Purchased equipment
- External
 - Hacker
- Blend
 - External threat
 - Internal, accidental initiation

Passive Information Gathering

- Key employees
- Dumpster diving
- Analyzing Web Page Code
- Exploiting Website Authentication Methods
- Mining Job Ads and Financial Data
- Using Google to Mine Sensitive Information
- Exploring Domain ownership
 - Whois | Domain Name System | Identifying web server Software & Location

Security Software

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

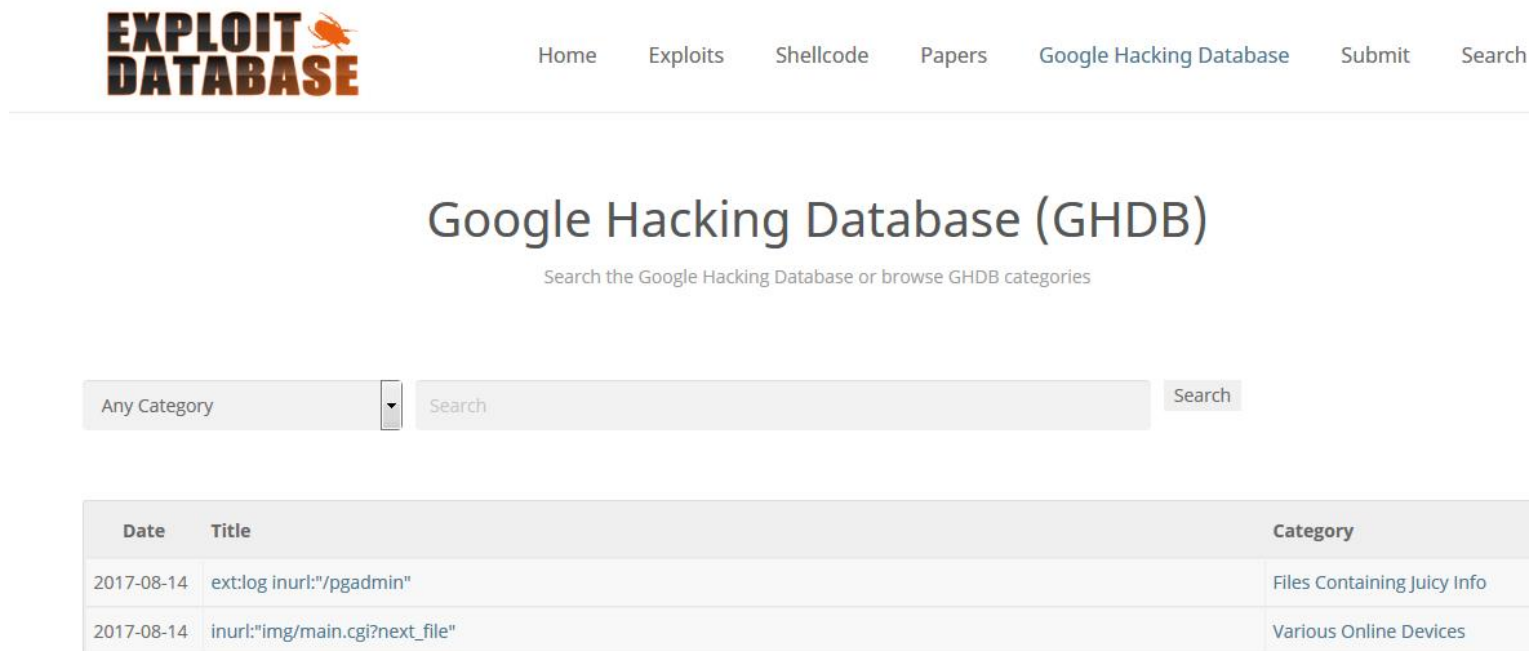
Looking forward

Scenario Questions

- 1. What are the potential sources of data?
- 2. Of the potential sources of data, which are the most likely to contain helpful information and why?
- 3. Which data source would be checked first and why?
- 4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used?
- 5. Which groups and individuals within the organization would probably be involved in the forensic activities?
- 6. What communications with external parties might occur, if any?
- 7. From a forensic standpoint, what would be done differently if the scenario had occurred on a different day or at a different time (regular hours versus off-hours)?
- 8. From a forensic standpoint, what would be done differently if the scenario had occurred at a different physical location (onsite versus offsite)?

What a difference a URL can make!

- www.exploit-db.com/google-dorks



The screenshot shows the Exploit Database website interface. At the top left is the logo for "EXPLOIT DATABASE" with a bug icon. To the right of the logo is a navigation menu with links for "Home", "Exploits", "Shellcode", "Papers", "Google Hacking Database", "Submit", and "Search". Below the navigation menu is a horizontal line. Underneath the line, the text "Google Hacking Database (GHDB)" is displayed in a large font, followed by the subtitle "Search the Google Hacking Database or browse GHDB categories". Below this is a search interface consisting of a dropdown menu labeled "Any Category", a search input field with the placeholder text "Search", and a "Search" button. Below the search interface is a table with three columns: "Date", "Title", and "Category". The table contains two rows of data.

Date	Title	Category
2017-08-14	ext:log inurl:"/pgadmin"	Files Containing Juicy Info
2017-08-14	inurl:"img/main.cgi?next_file"	Various Online Devices

Information for good and/or bad


[Home](#)
[Exploits](#)
[Shellcode](#)
[Papers](#)
[Google Hacking Database](#)
[Submit](#)
[Search](#)

Papers

Archived security papers and articles in various languages.

1,228 total entries

<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	Title	Language	Author
2017-09-04	↓	Code Injection - HTML Injection	English	Shritam Bho...
2017-08-30	↓	Command Injection - Shell Injection	English	Shritam Bho...
2017-08-28	↓	Abusing Token Privileges For LPE	English	drone and b...

Ports – loose analogy

- Discrete communication endpoint
 - Physical – socket, plug-in
 - Logical – application or process
 - Numbered - hundreds
- Ports in a business setting
 - Doors
 - Reception area
 - Telephones
 - Loading dock

Sleuthing with netstat -aon

```



TCP    192.168.5.216:49417    162.125.34.6:443    CLOSE_WAIT    4760
TCP    192.168.5.216:49421    52.201.32.182:443    CLOSE_WAIT    4760
TCP    192.168.5.216:49423    172.217.1.35:443     ESTABLISHED   6124
TCP    192.168.5.216:49424    216.58.216.206:443   ESTABLISHED   6124
TCP    192.168.5.216:49425    208.80.154.224:443   ESTABLISHED   6124
TCP    192.168.5.216:49427    208.80.154.240:443   ESTABLISHED   6124
TCP    192.168.5.216:49434    172.217.6.106:443    ESTABLISHED   4148
TCP    192.168.5.216:49435    172.217.9.37:443     ESTABLISHED   4148
TCP    192.168.5.216:49437    34.209.12.3:443      TIME_WAIT     0
TCP    192.168.5.216:49438    72.21.91.29:80       ESTABLISHED   6124
TCP    192.168.5.216:49439    72.21.91.29:80       ESTABLISHED   6124
TCP    192.168.5.216:49440    72.21.91.29:80       TIME_WAIT     0
TCP    192.168.5.216:49441    54.191.246.135:443   TIME_WAIT     0
TCP    192.168.5.216:49442    52.84.64.228:443     TIME_WAIT     0
TCP    192.168.5.216:49443    52.84.64.228:443     TIME_WAIT     0
TCP    192.168.5.216:49444    52.84.64.228:443     TIME_WAIT     0
TCP    192.168.5.216:49445    52.84.64.228:443     TIME_WAIT     0
TCP    192.168.5.216:49446    172.217.8.196:443    ESTABLISHED   4148
TCP    192.168.5.216:49447    172.217.6.106:443    ESTABLISHED   4148
TCP    192.168.5.216:49448    172.217.6.106:443    ESTABLISHED   4148
TCP    [::]:135              [::]:0               LISTENING     884
TCP    [::]:445              [::]:0               LISTENING     4
TCP    [::]:554              [::]:0               LISTENING     5588

```

Google: Whois 192.168.5.216 – slide 1

192.168.5.216

City	Rome
Country	Italy
Country Code	IT
Longitude	0
Latitude	0



Based on several IP databases the most probable location for IP adresse 192.168.5.216 is Rome, Italy, IT.
Latitude and longitude: 0 and 0

Whois 192.168.5.216 – slide 2

Network information

ASN	137
IP starting by	192.167.0.0
IP ending by	192.167.255.255
Ip starting with	192.168.5
ASN Name	Consortium GARR
CDIR	192.167.0.0/16
Numerical IP	3232237016
Registry	ripenc
Last update	04/07/2017



Whois 172.217.6.106

Network information

ASN	15169
IP starting by	172.217.0.0
IP ending by	172.217.255.255
Ip starting with	172.217.6
ASN Name	Google Inc.
CDIR	172.217.0.0/16
Numerical IP	2899904106
Registry	arin
Last update	10/07/2017



Local Address

The IP address **192.168.5.216** is provided by Consortium GARR, it's belong to the CDIR (Classless Inter-Domain Routing) 192.167.0.0/16 (range 192.167.0.0 to 192.167.255.255). The autonomous system number (ASN) is 137 and the numerical IP for 192.168.5.216 is 3232237016.

Foreign Address

The IP address **172.217.6.106** is provided by Google Inc., it's belong to the CDIR (Classless Inter-Domain Routing) 172.217.0.0/16 (range 172.217.0.0 to 172.217.255.255). The autonomous system number (ASN) is 15169 and the numerical IP for 172.217.6.106 is 2899904106.

Information related to PID 2404

Name	PID	Description	Status	Group
lltdsvc		Link-Layer Topology Discovery ...	Stopped	LocalService
FontCache	156	Windows Font Cache Service	Running	LocalService
fdPHost		Function Discovery Provider Host	Stopped	LocalService
EventSystem	156	COM+ Event System	Running	LocalService
wcnscvc		Windows Connect Now - Config ...	Stopped	LocalServic...
upnpshost	● 2404	UPnP Device Host	Running	LocalServic...
SSDPSRV	● 2404	SSDP Discovery	Running	LocalServic...
SensrSvc		Adaptive Brightness	Stopped	LocalServic...
				LocalServic...
				LocalServic...
				LocalServic...
				LocalServic...
				LocalServic...
				LocalServic...

```

UDP      0.0.0.0:63566      ***      1684
UDP      127.0.0.1:1900     ***      2404
UDP      127.0.0.1:56842   ***      2404
UDP      192.168.5.216:137 ***      4
UDP      192.168.5.216:138 ***      4
UDP      192.168.5.216:1900 ***      2404
UDP      192.168.5.216:56841 ***      2404
UDP      [::]:500           ***      376
UDP      [::]:3702          ***      2404
UDP      [::]:3702          ***      2404
UDP      [::]:4500          ***      376
    
```

-
-
-
-

Grouping by PID

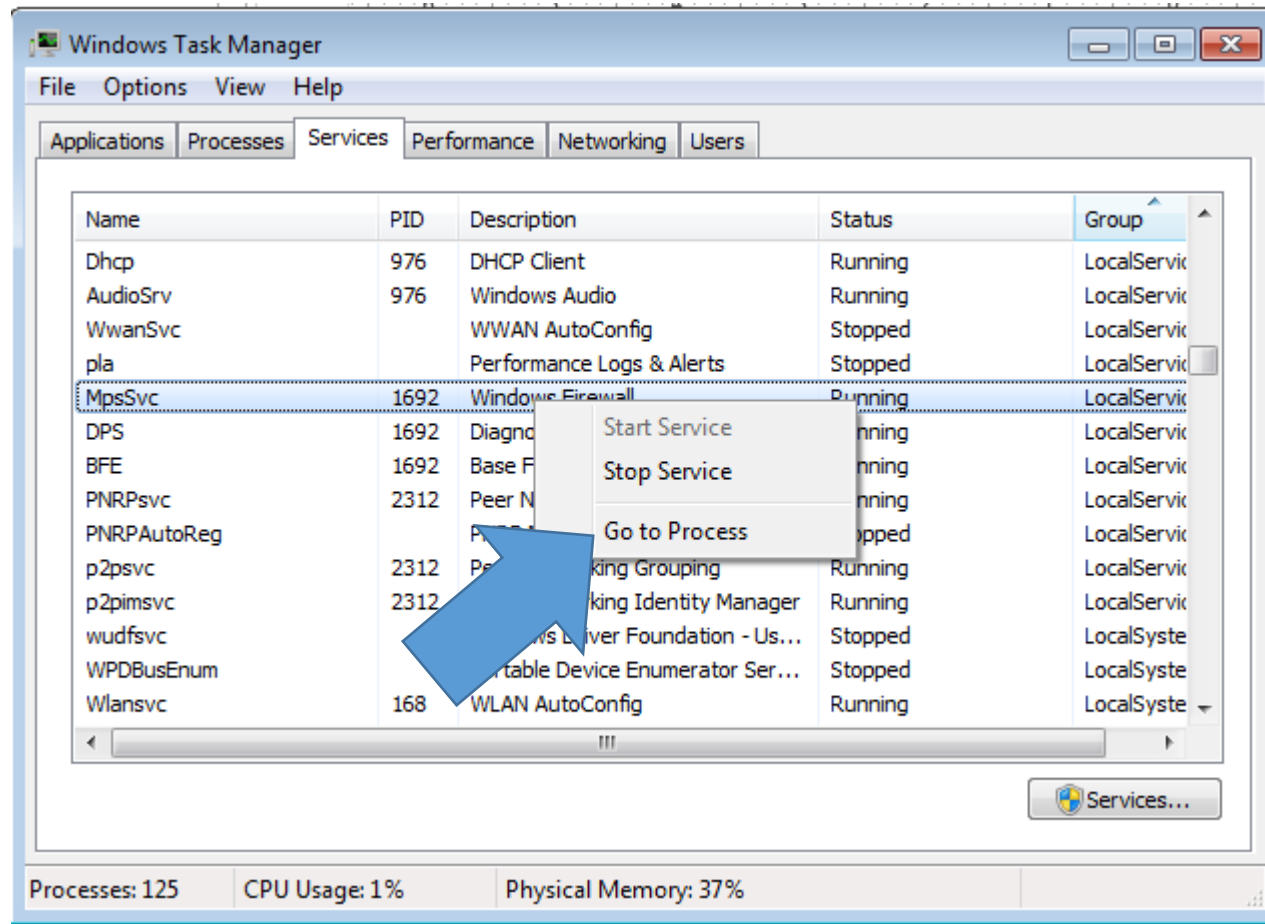
Mouse over; right click

The screenshot shows the Windows Task Manager 'Services' tab. The services are listed in a table with columns for Name, PID, Description, Status, and Group. The services are grouped by their PID values. A blue arrow points to the 'MpsSvc' service, which has a PID of 1692. The status bar at the bottom shows 123 processes, 4% CPU usage, and 36% physical memory usage.

Name	PID	Description	Status	Group
Dhcp	976	DHCP Client	Running	LocalService
AudioSrv	976	Windows Audio	Running	LocalService
WwanSvc		WWAN AutoConfig	Stopped	LocalService
pla		Performance Logs & Alerts	Stopped	LocalService
MpsSvc	1692	Windows Firewall	Running	LocalService
DPS	1692	Diagnostic Policy Service	Running	LocalService
BFE	1692	Base Filtering Engine	Running	LocalService
PNRPsvc	2312	Peer Name Resolution Protocol	Running	LocalService
PNRPAutoReg		PNRP Machine Name Publication...	Stopped	LocalService
p2psvc	2312	Peer Networking Grouping	Running	LocalService
p2pimsvc	2312	Peer Networking Identity Manager	Running	LocalService
wudfsvc		Windows Driver Foundation - Us...	Stopped	LocalSystem
WPDBusEnum		Portable Device Enumerator Ser...	Stopped	LocalSystem
Wlansvc	168	WLAN AutoConfig	Running	LocalSystem

Show all PID related processes

Select Go to Process



Processes related to PID 1692

Image Name	User Name	CPU	Memory (...)	Description
BrCcUxSys.exe *32	Marc Violante	00	1,784 K	ControlCenter UX System
BrCtrlCntr.exe *32	Marc Violante	00	2,092 K	ControlCenter Main Proces
BrotherHelp.exe *32	Marc Violante	00	1,808 K	Brother Help Application
BrStMonW.exe *32	Marc Violante	00	12,120 K	Status Monitor Application
BtvStack.exe	Marc Violante	00	6,340 K	Extension Core
conhost.exe	Marc Violante	00	1,528 K	Console Window Host
conhost.exe	Marc Violante	00	1,300 K	Console Window Host
csrss.exe		00	2,360 K	
DBRCrawler.exe	Marc Violante	00	8,696 K	DBRCrawler
Dropbox.exe *32	Marc Violante	00	1,596 K	Dropbox
Dropbox.exe *32	Marc Violante	00	1,060 K	Dropbox
Dropbox.exe *32	Marc Violante	00	114,140 K	Dropbox
dwm.exe	Marc Violante	00	11,628 K	Desktop Window Manager
esrv.exe	Marc Violante	00	8,336 K	Intel(R) System Usage Rep

Processes: 122 CPU Usage: 1% Physical Memory: 38%

Cyber Incident – Reporting Requirements

- Actions required when
 - Cyber incident discovered
 - Cyber incident affects ability to perform
- Actions
 - Conduct a review for evidence to include
 - Rapidly report (within 72 hours) to <https://dibnet.dod.mil>
- Reporting required
 - Dibnet account
 - DoD Medium Assurance Certificate

Cyber incident report

- The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <http://dibnet.dod.mil>.

Cyber Incident Reporting -

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident

- Company name
- Company point of contact information (address, position, telephone, email)
- Data Universal Numbering System (DUNS) Number
- Contract number(s) or other type of agreement affected or potentially affected
- Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
- USG Program Manager point of contact (address, position, telephone, email)
- Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Facility CAGE code
- Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Impact to Covered Defense Information
- Ability to provide operationally critical support
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- DoD programs, platforms or systems involved
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative
- Any additional information

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

Other requirements

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

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

IP 192.168.0.8 – Identified using tracert

```
C:\>
C:\>tracert 192.168.0.8

Tracing route to MarcViolante-PC [192.168.0.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    MarcViolante-PC [192.168.0.8]

Trace complete.
```

- All good
- No system breach
- No report required

Resources



Image copied from: innovation.ed.gov

9/13/2017

Frameworks/References

- SP 800-53
- SP 800-171
- NIST 32 – Establishing or Improving a Cyber Security Program
- NIST SP 800-86 Integrating Forensic techniques into Incident Response
- NIST SP 800-92 Computer Security and Logs
- NIST IR 7621 r1 Small Business Information Security Fundamentals
- Framework for Improving Critical Infrastructure Cybersecurity, NIST, February 12, 2014

DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program ¹¹²

- 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.

National Initiative for Cybersecurity Careers and Studies

NICCS™ is the One Stop Shop for Cybersecurity Careers and Studies!

Information For

- Federal Employees
- General Public
- Students
- Educators
- Parents
- Cybersecurity Professionals
- Human Capital Managers
- Cybersecurity Managers
- Policy Makers
- Veterans
- State, Local, Tribal and Territorial Governments (SLTT)
- Women & Minorities



STAY SAFE ONLINE

View our Cybersecurity How-To Guide to learn safe online strategies and find additional Awareness resources.



EXPLORE THE WORKFORCE FRAMEWORK

Explore the Cybersecurity Specialty Areas, Tasks, and KSAs defined in the Workforce Framework.



FIND COURSES

Find the education and training courses you need to keep up with changing threats.



LEARN ABOUT WORKFORCE PLANNING

Learn about skill gap analysis, training strategies, and other activities to keep your Cybersecurity workforce on top.

UPCOMING EVENTS

Federal Executive Cybersecurity Seminar
Apr 6, Homeland Security Acquisition...

4th USA Science & Engineering Festival
Apr 16 to Apr 17, Walter E. Washington...

FedVTE Live! Information Assurance (IA) Compliance
May 10, Virtual World

[VIEW ALL EVENTS](#)

RECENT HEADLINES

Emergency Update Coming for Flash Vulnerability Under Attack [↗](#)

WhatsApp Adds End-to-End Encryption To One Billion Users [↗](#)

WhatsApp Toughens Encryption After Apple-FBI Row [↗](#)



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

9/13/2017


[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.

Backdoors using modems?



A BIG headache.

Latest 25 Papers Added to the Reading Room

SANS
eNewsletters

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

Get Newsletters

InfraGard

Username:

Password:

[Log in](#)

[Forgot User Name?](#)

[Forgot Password?](#)

[Home](#) [In the News](#) [Chapters](#) [Events](#) [Join Today!](#) [Contact Us](#)

You are here: [Home](#)

CYBER 2026

InfraGard San Diego's 2nd Annual Cyber Futurist Symposium

MARCH 24, 2016

Qualcomm's Irwin Jacobs Hall

TIME_ 0800 - 1200 COST_ \$10 USD

[Apply Online](#)

[16 Critical Infrastructures](#) [Find a Chapter Near You](#) [FBI News Feeds](#)

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

9/13/2017

First.org

Current FIRST SIGs

Botnet Mitigation and Remediation
To share experiences about botnet mitigation and remediation and to identify different approaches and best practices that can be implemented to address this problem.

CVSS SIG: Common Vulnerability Scoring System
For a global approach towards scoring metrics for vulnerabilities.

IEP SIG: Information Exchange Policy
The initial goals of this SIG are to collaboratively develop an extensible framework for defining information exchange policy and a set of standard definitions for most common aspects.

Vendors SIG: Internet Infrastructure Vendors
The goal of this SIG is to provide forum for internet infrastructure vendors.

Malware Analysis
This SIG will advocate and promote the sharing of malware analysis tools and techniques to enable CSIRTs to combat and analyze malicious code.

Metrics SIG
To improve CSIRT incident management practices within the FIRST community.

Network Monitoring SIG
To advocate and develop collection and analysis of network sensor.

Red Teaming SIG
Red Team exercises deliver end-to-end breach simulations that provide, as realistically as possible, security incidents that prepare those involved with dealing with actual breaches.

Events at spotlight

28th ANNUAL FIRST CONFERENCE SEUL
JULY 16 - 17, 2016

2016 FIRST Technical Colloquium
Amsterdam, Netherlands
April 19 - 20, 2016

What's new

Thu, 11 Feb 2016
Call for Speakers Notification Delayed to February 25 (14:20 +0100)
Due to the record high number of submissions this year, the review process is running slightly behind schedule. We appreciate your patience and hope to issue notifications February 25, 2016. For questions regarding your submission, please contact the Program Chair at first-2016chair@first.org.

What is FIRST to you?

What is FIRST to you?

FIRST is the global Forum for Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

- access to up-to-date best practice documents
- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and webservices
- special interest groups

Currently FIRST has more than 300 members, spread over Africa, the Americas, Asia, Europe and Oceania.

DIB ISAC



DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

News and Events

- Homeland Security Today
- US-CERT

Private Industry Sharing Threat Data and Analysis to Support the Warfighter

- CONTACT
- MISSION
- MEMBERSHIP
- PREPAREDNESS
- CYBER SECURITY
- ISAC LINKS
- RESOURCES

Cyber Attacks

- Sharing
- Analysis
- Training
- Awareness
- Prevention
- Response

All Hazards Preparedness

- Mitigation
- Response
- Recovery
- Accountability
- Training

TERRORISM

- Vigilance
- Active Shooter
- Awareness
- Mitigation
- Planning

Take advantage of resources and tools

CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT

How to Build a Strong Cybersecurity Workforce

Resources

- NISTIR 7621 Revision 1 Small Business Information Security:
 - *The Fundamentals*
- 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 www.sans.org

Veterans have access to free training

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

A better pipeline for cyber talent

- Vets get free SANS training and certifications in cybersecurity
- Employers get highly qualified talent for critical jobs in cybersecurity

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

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

Create a 30 day action plan

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

Office procedures

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

Information handling requirements

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

Disposal

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

Personnel

- Are employees provided any IT training?
- Are employees screened prior to granting access to the IT system?
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?

Business Continuity Plan

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

Cyber Insurance – Top Considerations

1. Establish the correct level of coverage you might need. While quantifying cyber risk in financial terms may still be more art than science, one starting point is through an internal audit to determine the total value of your company's data as well as the aggregate cost of a possible breach.

2. Carefully check definitions of terms such as “hackers,” “attacks” or “incidents,” and “breach”

3. Make sure that policies (and situations) meet your needs.

Keep in mind that your business might also need specific coverages such as extortion, intellectual property infringement and advertising injury.

4. Consider that many cyber insurance policies do not cover nontechnical attacks, such as an authorized person stealing confidential data.

Cyber Insurance – Considerations

5. Know which business insurance policy covers that contingency.
6. Make sure that one policy does not negate another.
7. Ensure that policies cover more than just the immediate damage and any possible losses from litigation following a breach.
 - The ideal level of cyber insurance protection should cover a business for all costs associated with an
 - incident—discovery, investigation and remediation, as well as any court costs, judgments or penalties.
8. When you're talking to underwriters, find out how much weight they put on the security controls you already have in place. Judgments about the degree to which those controls reduce your company's risk, and therefore its cyber insurance premiums, can be made based on your company's history or the underwriter's own data and calculations.
9. Work closely with a broker you trust,



It's easy to sleep when
your information is
secure

ACQUISITION HOUR LIVE WEBINAR SERIES

- September 19, 2017 – **Selling to the State of Wisconsin and Local Governments** – **FULL** – presented by Kate Hill, Heartland Information Research, Inc
- September 20, 2017 – **Overview of the Federal Acquisition Regulations (FAR)** – [CLICK HERE](#) for additional information – presented by Carol Murphy – Wisconsin Procurement Institute (WPI)
- October 4, 2017 – **eSRS Individual Subcontractor Reporting (ISR) Basics** – [CLICK HERE](#) for additional information – presented by Kim Garber, Wisconsin Procurement Institute (WPI)
- October 17, 2017 – **Packaging Shipping and Invoicing Using WAWF I-RAPT** – [CLICK HERE](#) for additional information – presented by Pat Hotton, Bentley World Packaging Ltd. & Ben Blanc, Wisconsin Procurement Institute (WPI)
- October 18, 2017 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – [CLICK HERE](#) for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)

ACQUISITION HOUR LIVE WEBINAR SERIES

- October 24, 2017 – **The Contractor Purchasing System Review (CPSR) Series part 1 of 4** – [CLICK HERE](#) for additional information – presented by Phil Bail, Phil Bail and Associates
- October 31, 2017 – **The Contractor Purchasing System Review (CPSR) Series part 2 of 4** – [CLICK HERE](#) for additional information – presented by Phil Bail, Phil Bail and Associates
- November 1, 2017 – **Flow-down Clauses – Management and Responsibilities for Federal Contractors** – [CLICK HERE](#) for additional information – presented by Carol Murphy – Wisconsin Procurement Institute (WPI)
- November 7, 2017 – **The Contractor Purchasing System Review (CPSR) Series part 3 of 4** – [CLICK HERE](#) for additional information – presented by Phil Bail, Phil Bail and Associates
- November 8, 2017 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – [CLICK HERE](#) for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)
- November 14, 2017 – **The Contractor Purchasing System Review (CPSR) Series part 4 of 4** – [CLICK HERE](#) for additional information – presented by Phil Bail, Phil Bail and Associates
- November 28, 2017 – **The HUBZone Program – Certification Benefits and New Regulations** – [CLICK HERE](#) for additional information – presented by Shane Mahaffy, Lead Business Opportunity Specialist, US Small Business Administration (SBA)

MARKETPLACE 2017

Save the date: December 13 – 14

PRE-MARKETPLACE Series presented by WPI
<https://premarketplacewi.org/>



QUESTIONS?

SURVEY



CONTINUING PROFESSIONAL EDUCATION



CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Marc Violante | Director Federal Market Strategies

Wisconsin Procurement Institute (WPI)

marcv@wispro.org 414-270-3600

Benjamin Blanc, CFCM, CPPS | Government Contract Specialist

Benjaminb@wispro.org 414-270-3600

**10437 Innovation Drive, Suite 320
Milwaukee, WI 53226**