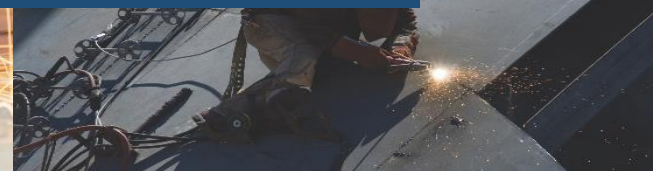
Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

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

October 18, 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!

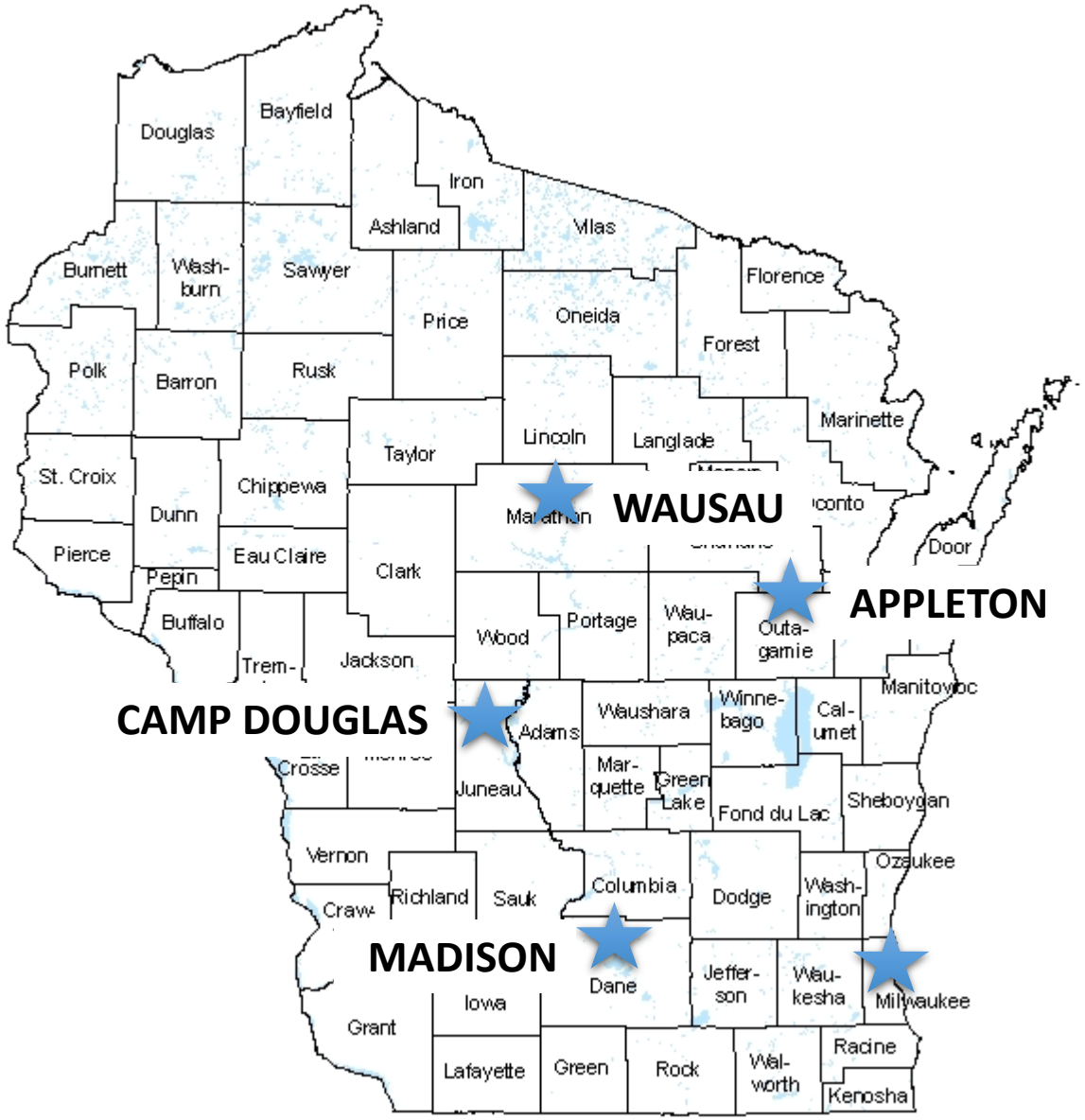
ABOUT WPI
SUPPORTING THE MISSION

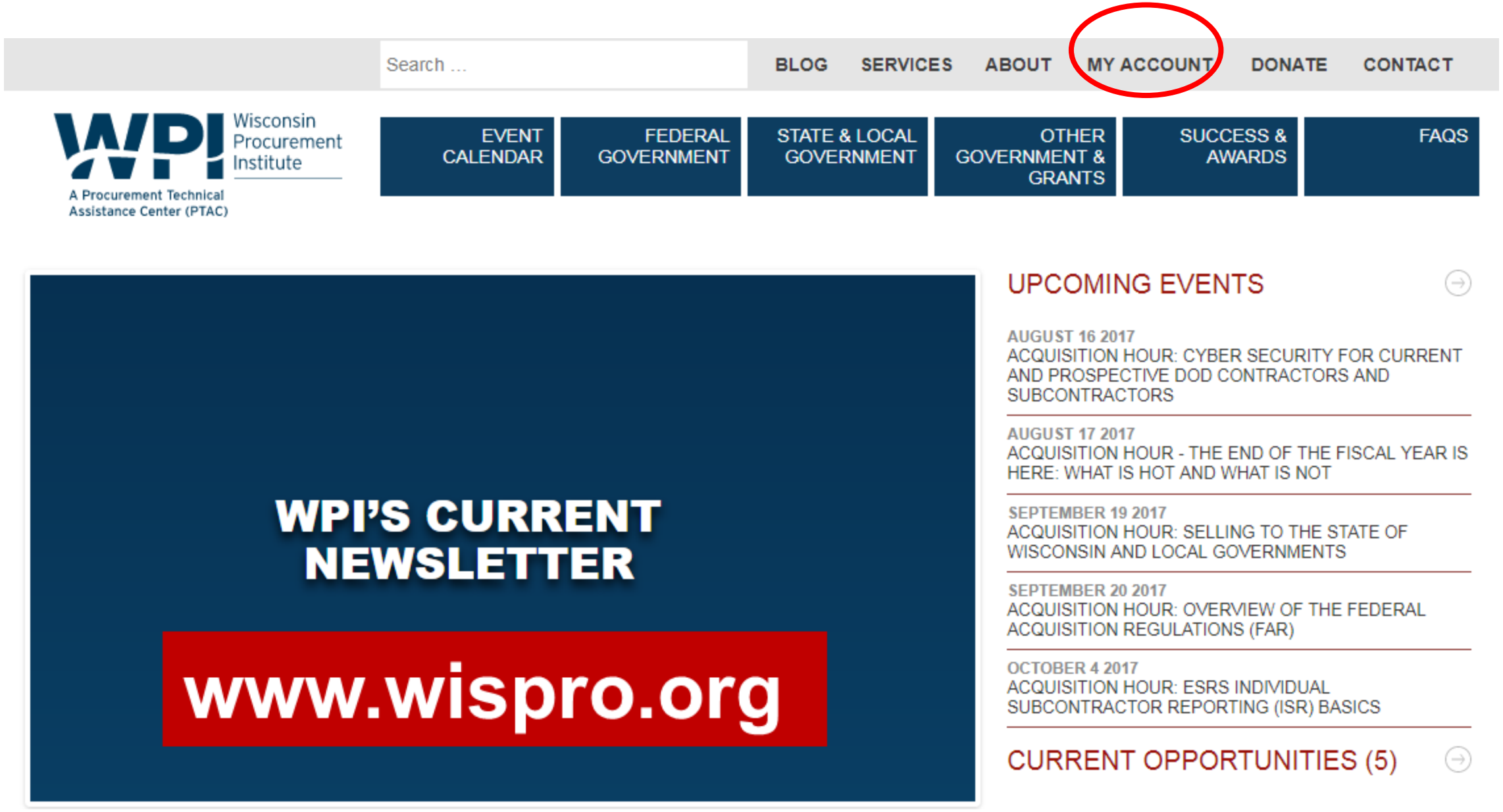
Assist businesses in creating, development and growing their sales, revenue and jobs through Federal, state and local government contracts.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

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
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
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

Image source: readywisconsin.wi.gov

Marc N. Violante

Wisconsin Procurement Institute

October 18, 2017

Webinar Overview

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

Official website of the Department of Homeland Security

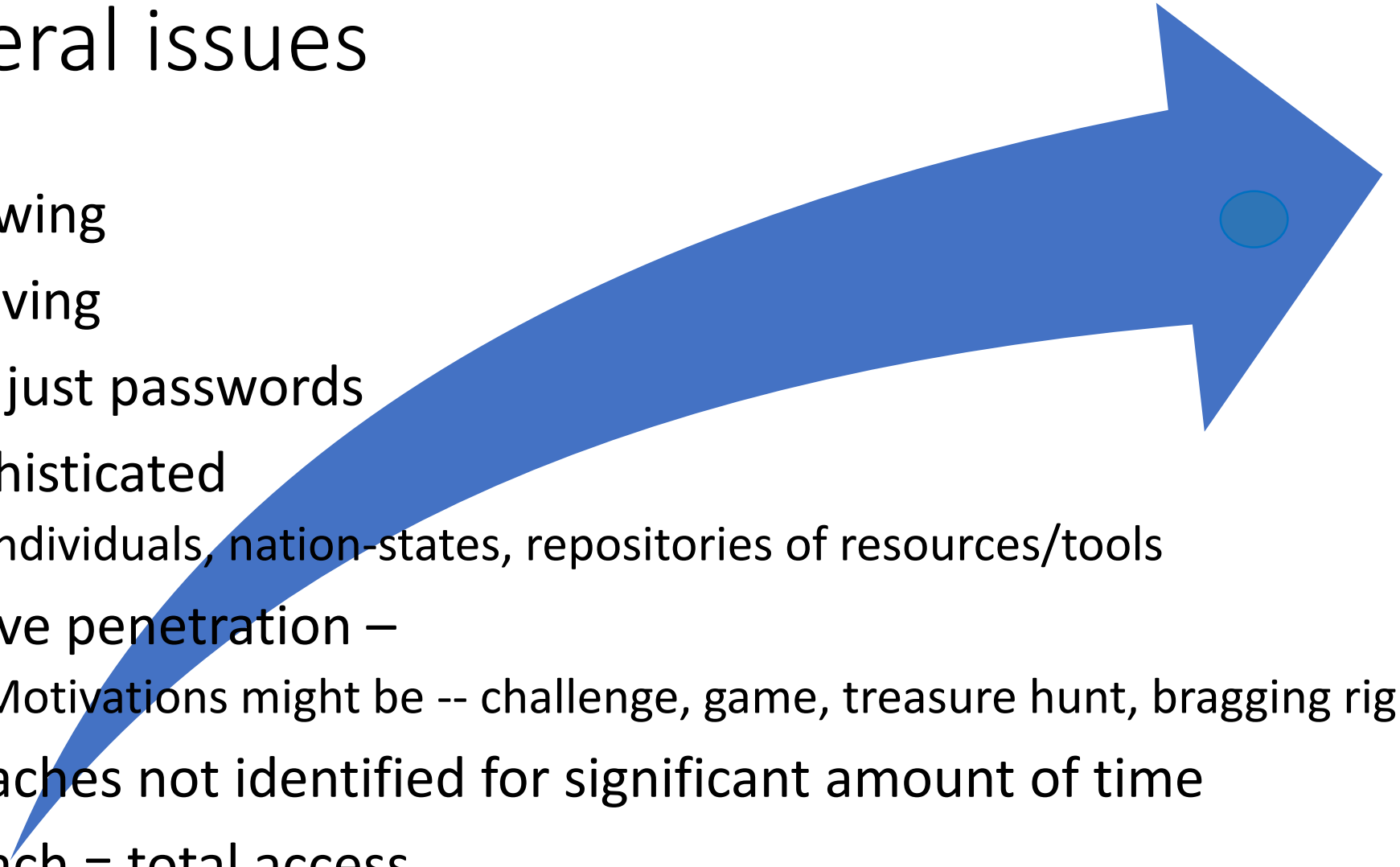
US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

5 Questions CEOs Should Ask About Cyber Risks

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

General 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

Evolving requirements

- **Enhance Email and Web Security**
- Based on current network scan data and a clear potential for harm, this directive requires actions related to two topics: email security and web security.
- Implement – email authentication:
  - Offer: STARTTLS
  - Implement - SPF/DKIM, DMARC
  - Utilize – HTTPS protocol on publically accessible web servers

DHS - Binding Operational Directive 18-01; https://cyber.dhs.gov/, visited – Oct 17, 2017

Evolving threats

Homeland Security

US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

IC3 Issues Alert on DDoS Attacks

10/17/2017 08:39 PM EDT

Original release date: October 17, 2017

The Internet Crime Complaint Center (IC3) has issued an alert on distributed denial-of-service (DDoS)-for-hire services advertised on criminal forums and marketplaces. Using DDoS attacks to prevent legitimate users from accessing websites or information can lead to serious consequences.

US-CERT encourages users and administrators to review the IC3 Alert for more information and US-CERT's Alert on Heightened DDoS Threat Posed by Mirai and Other Botnets.

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!

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

Id'ing the digital spy

"When businesses do eventually notice that they have a digital spy in their midst and that their vital information systems have been compromised, an appalling 92 percent of the time it is not the company's chief information officer, security team, or system administrator who discovers the breach."

- How do companies find out that they have been breached?
  - Law enforcement
  - Angry customer
  - Contractor

Marc Goodman, Future Crimes: everything is connected, everyone is vulnerable and what we can do about it, (New York: DOUBLEDAY, 2015), 16-17
Verizon's 2013 Data Breach Investigations Report is cited as the source

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

What happens when ----

Ours

Theirs

Images copied from: eglin.af.mil

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 cyber-security 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

In the News – Summer of 2015 – key point

"Where once companies thought that they could defend themselves against and 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

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

Is it a priority for you?

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].

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

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?

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

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].

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

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

Visits in the Past 90 Days

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

Devices

Desktop	55.8%
Mobile	38.6%
Tablet	5.7%

Based on rough network segmentation data, we estimate that **less than 5%** of all traffic across all agencies comes from US federal government networks.

Much more detailed data is available in **downloadable CSV and JSON**. This includes data on combined browser and OS usage.

Browsers

Chrome	45%
Safari	27.1%
Internet Explorer	14.3%
11.0	12.7%
7.0	1%
10.0	0.3%
9.0	0.2%
8.0	0.1%
Other	< 0.1%
Firefox	6.4%
Edge	3.7%
Android Webview	1.1%
Safari (in-app)	1.1%
Other	1.3%

Operating Systems

Windows	46.9%
7	24.2%
10	18.4%
8.1	2.9%
XP	0.6%
8	0.5%
Other	0.4%
iOS	25%
Android	18.1%
Macintosh	8.5%
Other	1.4%

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

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%

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

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
• Versions of Internet Explorer	CSV JSON	Daily
Operating systems	CSV JSON	Daily
• 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

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

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...

https://www.kb.cert.org/vuls/byCVSS visited 9/12/2017

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

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

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, Table 1, 10

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.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (e) & (f)

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.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (m)

Covered Defense Information(CDI)

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to provide “adequate security” for covered defense information that is processed, stored, or transmitted on the contractor’s internal information system or network. The Department must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirement for the contractor to mark covered defense information developed in performance of the contract.

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

Implementation of DFARS 252.204-7012

There is no single or prescribed manner in which a contractor may choose to implement the requirements of NIST SP 800-171, or to assess their own compliance with those requirements.

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

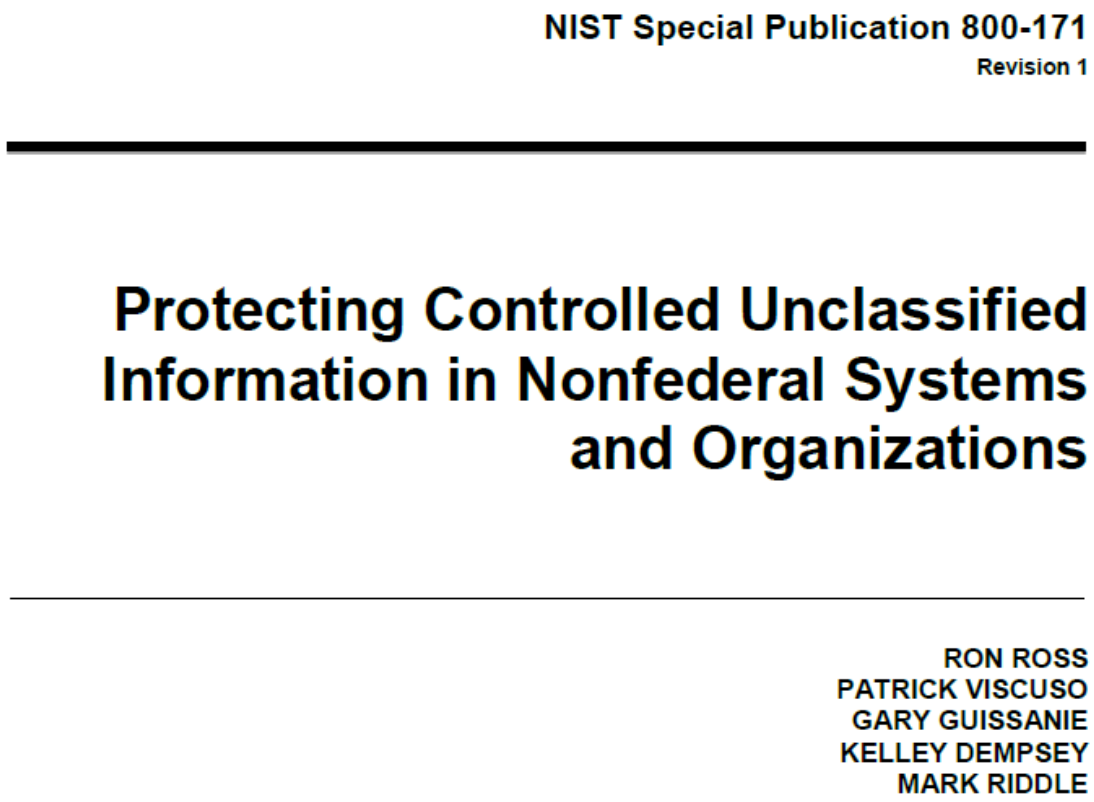
Covered Defense Information(CDI)

A reasonable first step may be for company personnel with knowledge of their information systems security practices to

- read through the publication,
- examining each requirement
- determine if it may require a change to company policy or processes, a configuration change for existing company information technology (IT), or if it requires an additional software or hardware solution. Most requirements

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

NIST (SP) 800-171 Revision 1



NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

NIST Document – cover page

NIST (SP) 800-171 Revision 1

- 3 Chapters – 80 pages
  - Introduction
  - The Fundamentals
    - The Requirements
- References
- Glossary
- Mapping Table
  - Requirement <> NIST (SP) 800-53 <> ISO/IEC 27001 – as applicable
- Tailored Criteria

NIST (SP) 800-171 Revision 1, December 2016

NIST (SP) 800-171 Revision 1 - example

3.12 SECURITY ASSESSMENT

Basic Security Requirements:

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.[26]

- Derived Security Requirements: None.

NIST (SP) 800-171 Revision 1, December 2016

NIST (SP) 800-171 Tailored Criteria

There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.

NIST (SP) 800-171 Revision 1, December 2016

Covered Defense Information(CDI)

- Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely.
- These requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy.
- Some requirements will require security-related software (such as anti-virus) or additional hardware (e.g., firewall).

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

Implementation – Complexity & Size

- The complexity of the company IT system may determine whether additional software or tools are required.
- For smaller systems, the company may accomplish many requirements manually, such as
  - configuration management
  - patch management,
- Larger and more complex systems may require automated software tools to perform the same task.

Implementation – Decisions

- Having reviewed all of the security requirements, a company may then determine which of the requirements,
  1) can be accomplished by their own in-house IT personnel,
  2) require additional research in order to be accomplished by company personnel,
  3) require outside assistance.

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

Implementation – Contractor's responsibility

- Ultimately, it is the contractor's responsibility to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information).
- Third party assessments or certifications of compliance are not
  - required,
  - authorized,
  - or recognized by DoD,
  - nor will DoD certify that a contractor is compliant with the NIST SP 800-171 security requirements.

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

Security requirement 3.12.4 (System Security Plan, added by NIST SP 800-171, Revision 1)

- Requires the contractor to
  - develop,
  - document,
  - and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

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

System Security Plan - purpose

- The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.
- The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.
- The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO). Additional information may be included in the basic plan and the structure and format organized according to needs

Guide for Developing Security Plans for Federal Information Systems - NIST Special Publication 800-18 Revision 1, February 2006, Executive Summary

Security Controls [FIPS 199]

- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Guide for Developing Security Plans for Federal Information Systems - NIST Special Publication 800-18 Revision 1, February 2006, Appendix B: Glossary

¶

National Heart, Lung, and Blood Institute

¶

Information·Technology·Security·Plan·(IT-SP)·¶
For·Moderate·Impact·Level·¶
Nonfederal·Information·Systems·and·Organizations·¶

Purpose:

The purpose of an information technology security plan (IT-SP) is to outline the management, operational, and technical safeguards or countermeasures prescribed for an information system.

This template should be used as a guide. It is tailored after the guidance provided by NIST Special Publication 800-171 which outlines how non-federal information systems and organizations should protect sensitive information also known throughout this document as controlled unclassified information (CUI). You are encouraged to review NIST SP 800-171, , *Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations,* and NIST SP 800-18*, Guide for Developing Security Plans for Federal Information Systems,* prior to completing the template below. This will aid you in meeting the expectations for an IT-SP.

NIH Template – Google Search

Implement the Controls

System Security Plan (SSP)

- The SSP for each system includes necessary information for the Authorizing Official (AO) to grant an ATO. The plan contains:
  - System identification, which includes the system owner, general description and purpose of the system, and equipment list;
  - A list of minimum security controls; and
  - Security documents that were developed during the EPLC.
- The SSP should be reviewed and updated or verified at least annually once the system is operational.
- If the system has changed (system environment, software, hardware, user groups, etc.), the SSP should be updated as soon as the change is made.

< Previous | Contents | Next >

https://irtsectraining.nih.gov/ISManager_2013/infosecurity-managers/part30.htm - visited October 17, 2017

RUTGERS Information Protection and Security

Search

About | Training & Awareness | RBHS Community | Resources | Trending Now | Events | Contact Us

Main menu

- About
- Training & Awareness
  - Students & Home Users

Developing a Security Plan

No computer or workstation is immune to compromise. Un
value and protecting them is the responsibility of everyon
to develop a security plan.

- Step 1. Inventory Assessment
- Step 2. Risk Assessment
- Step 3. Checklist
- Step 4. Evaluation
- Step 5. IT Security Plan

https://rusecure.rutgers.edu/content/developing-security-plan - visited October 17, 2017

Security Requirement 3.12.2 (Plans of Action)

- Requires the contractor to
  - develop and implement plans of action
  - designed to
    - correct deficiencies and reduce or eliminate vulnerabilities in their systems.

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

Note: NIST SP 800-171 v. NIST SP 800-171 Rev 1

- Note that DFARS Clause 252.204-7012 requires the contractor to implement the version of the NIST SP 800-171 that is in effect at the time of the solicitation, or such other version that is authorized by the contracting officer.
- Thus, if Revision 1 of NIST SP 800-171 was not in effect at the time of the solicitation, the contractor should work with the contracting officer to modify the contract to authorize the use of NIST SP 800-171, Revision 1, dated December 2016.
- DoD guidance is for contracting officers to work with contractors who request assistance in the consistent implementation of the latest version of DFARS Clause 252.204-7012 and NIST SP 800-171, Revision 1.

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

Documenting implementation

- To document implementation of the NIST SP 800-171 r1 security requirements by the December 31, 2017, implementation deadline, -
  - companies should have a system security plan in place,
  - in addition to any associated plans of action to describe
    - how and when any unimplemented security requirements will be met,
    - how any planned mitigations will be implemented, and
    - how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems.
- Organizations can document the system security plan and plans of action as separate or combined documents in any chosen format.

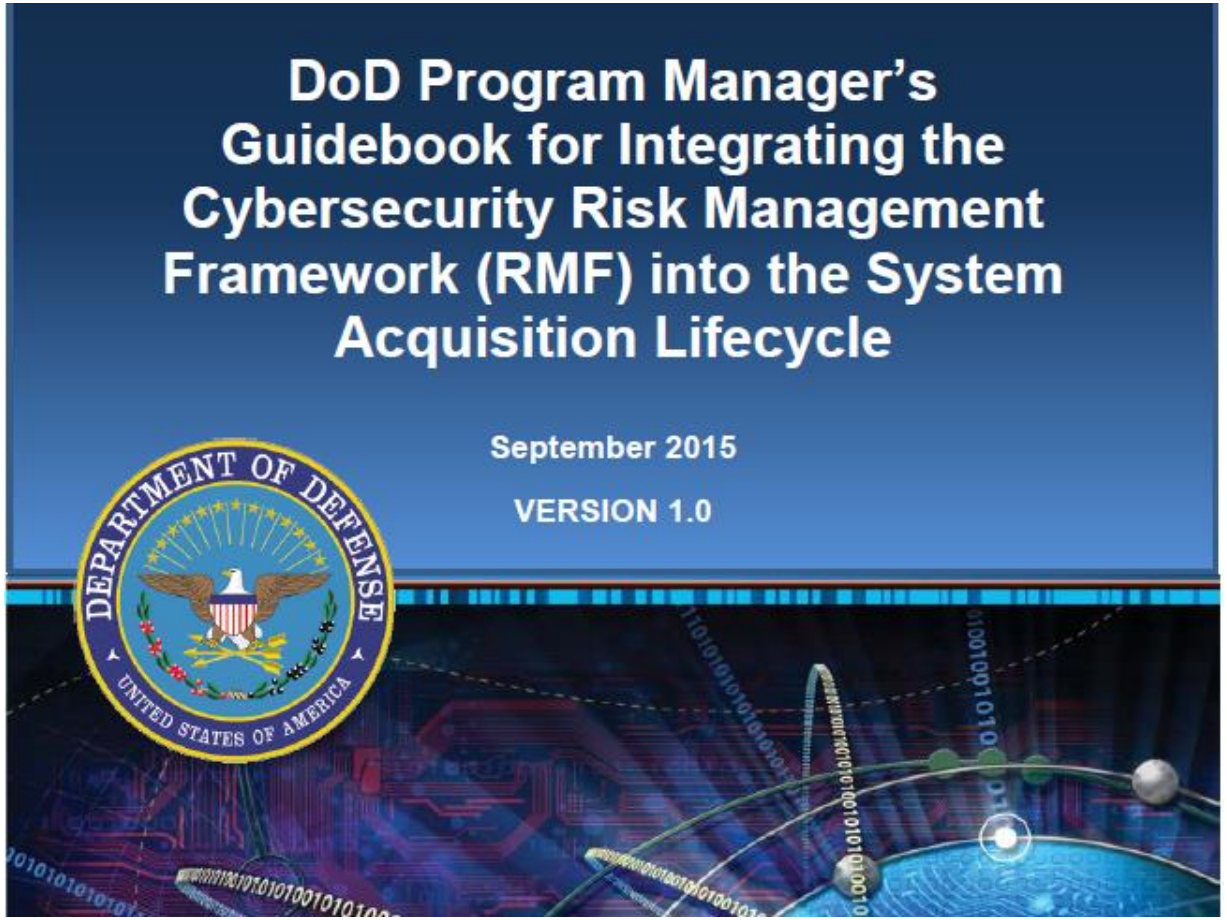
Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, Implementing DFARS 252.204-7012 Memorandum, Sep 21, 2017

NIST SP 800-171 Rev 1 – evaluation factor

- Chapter 3 NIST SP 800-171 Rev 1
  - states that Federal agencies may consider the contractor's system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization,
  - and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization.
  - NIST SP 800-171 Rev 1 – not structured to be a mandatory evaluation factor
  - Can be used to evaluate the overall risk
- Acquiring activity must state – how & whether NIST implementation will be used

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

Cybersecurity Risk Management Framework (RMF)



http://www.acqnotes.com/wp-content/uploads/2014/09/PM-Guidebook-for-Integrating-Cybersecurity-RMF-into-System-Acquisition-Lifecycle-Sep-2015.pdf

Annex A - Cybersecurity Throughout the Acquisition Lifecycle

- A.1 Materiel Solution Analysis (MSA) Phase
- A.1.1 Cybersecurity Assessment Criteria for Analysis of Alternatives (AoA)
- A.1.2 Develop Initial Cybersecurity Strategy and Include Cybersecurity in MS A Documentation
- A.2 Technology Maturation and Risk Reduction (TMRR) Phase
- A.2.1 Include Cybersecurity in System Design and Development RFP Release Decision
- Documentation
- A.2.2 Include Cybersecurity in Preliminary Design and Final MS B Documentation
- A.3 Engineering and Manufacturing Development (EMD) Phase
- A.3.1 Include Cybersecurity in Detailed Final Design

http://www.acqnotes.com/wp-content/uploads/2014/09/PM-Guidebook-for-Integrating-Cybersecurity-RMF-into-System-Acquisition-Lifecycle-Sep-2015.pdf -- TOC

Indications of CDI

- 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 GENERALAPPLICABILITY, 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 PERMITTEDBY 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 ACOPY 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.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

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

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

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.

NIST SP 800-92 Guide to Computer Security Log Management, Executive Summary

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

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

Situational Awareness – users - Phishing

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

2016 Verizon, Data Breach Investigation Report, 18

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?

Technical Trends in Phishing Attacks, Jason Milletary, US Cert

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

U.S. DHS, US-CERT, Spyware, Aaron Hackworth, CERT Coordination Center, Copyright 2005 Carnegie Mello University

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

Security - 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*

U.S. DHS, US-CERT, Small Office/Home Office Router Security, 2011

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?

U.S. DHS, US-CERT, Software License Agreements: Ignore at Your own Risk, Edward Desautels, Produced 2005 by US-CERT, Updated 2008

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

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 113-114

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

www.dshield.org/top10.html; visited August 15, 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 blocklist 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	OTHERS	PORT SCANNERS	RESEARCH
bebloh C&C server	CI Army List	Port 110 Scanner	Blindferret
Cryptowall C&C server	Emergingthreats	Port 143 Scanner	Erratasec Masscan
Dyreza Servers	Forum Spammers	Port 21 Scanner	Rapid7Sonar
Hesperbot C&C server	Malc0de Blacklist	Port 22 Scanner	Shadowserver
matsnu C&C server	TLD Name Servers	Port 25 Scanner	ShodanHQ
Palevo C&C IP	Tor Exit Node ✓	Port 443 Scanner	UMichigan scans.io
qakbot C&C server		Port 80 Scanner	
ramnit C&C server		Port 993 Scanner	
Ransomips		Apache Web Server Scanner	
Spyeye C&C server		Asterisk VoIP Scanner	
Symmi C&C server		Suspect Bots/Infected	
TinyBanker C&C server		Bruteforce	
Upatr Servers		courier imap attacker	
WebIron Bots		courier pop3 attacker	
Zeus C&C server		OpenBL FTP Scanners	
		OpenBL HTTP Scanners	
		OpenBL MAIL Scanners	
		OpenBL SMTP Scanners	
		OpenBL SSH Scanners	

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

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

Penetration Testing Security Analysis, EC-Council, Page 7-2

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

NIST SP 800-92 Computer Security and Log Management, 2.3.9 page 2-9

Maximizing Log value

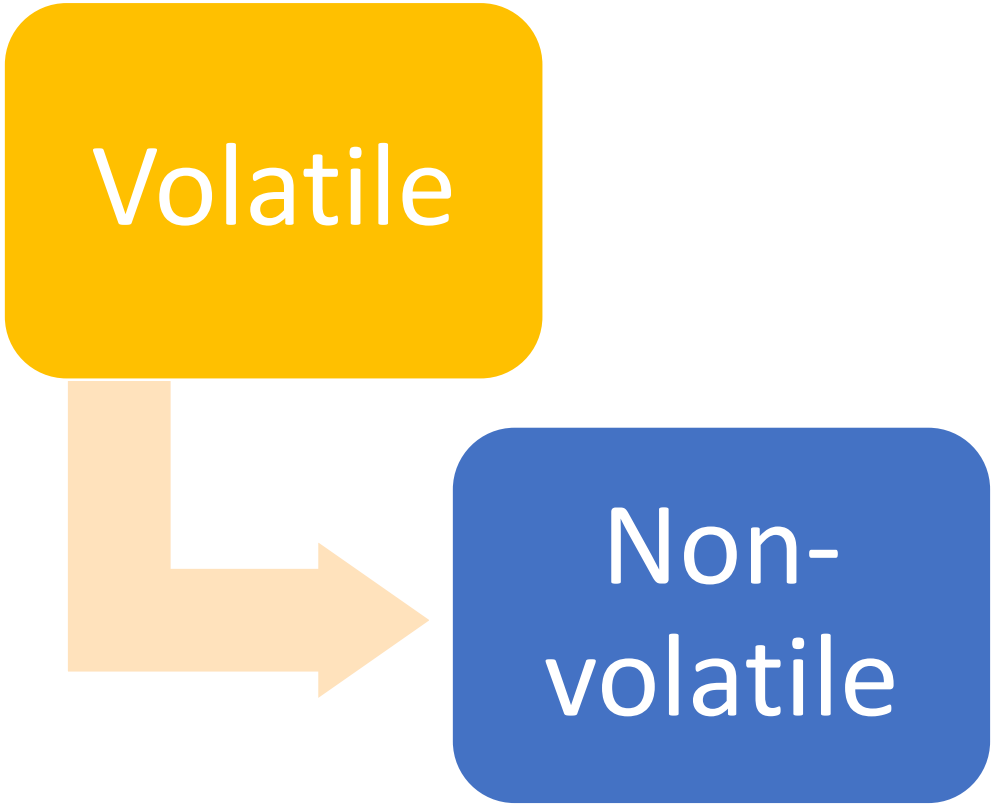
- Identify as high priority
  - Combat the notion of boring and of low benefit
- Provide sufficient tools
  - Assists with automation
  - Helps to identify patterns that a human will not see
- Provide training for efficient performance
- Reactive tool
  - After an event

NIST SP 800-92 Computer Security and Log Management, 2.3.3 page 2-10

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



NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 5.2.1.3 page 5-8

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

NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 6.4 page 6-11

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

Richard Bejtlich, The Practice of network Security Monitoring (No Starch Press, Inc, San Francisco, CA 2013), 9

Threats

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

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

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

Michael Gregg, The Network Security Test Lab; A step-by-Step Guide, (John Wiley & Sons, Inc, Indianapolis, IN 2015), XII

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

NIST SP 800-92 Computer Security and Log Management, 2.1.1 page 2-2

Looking forward – the need to plan, exercise

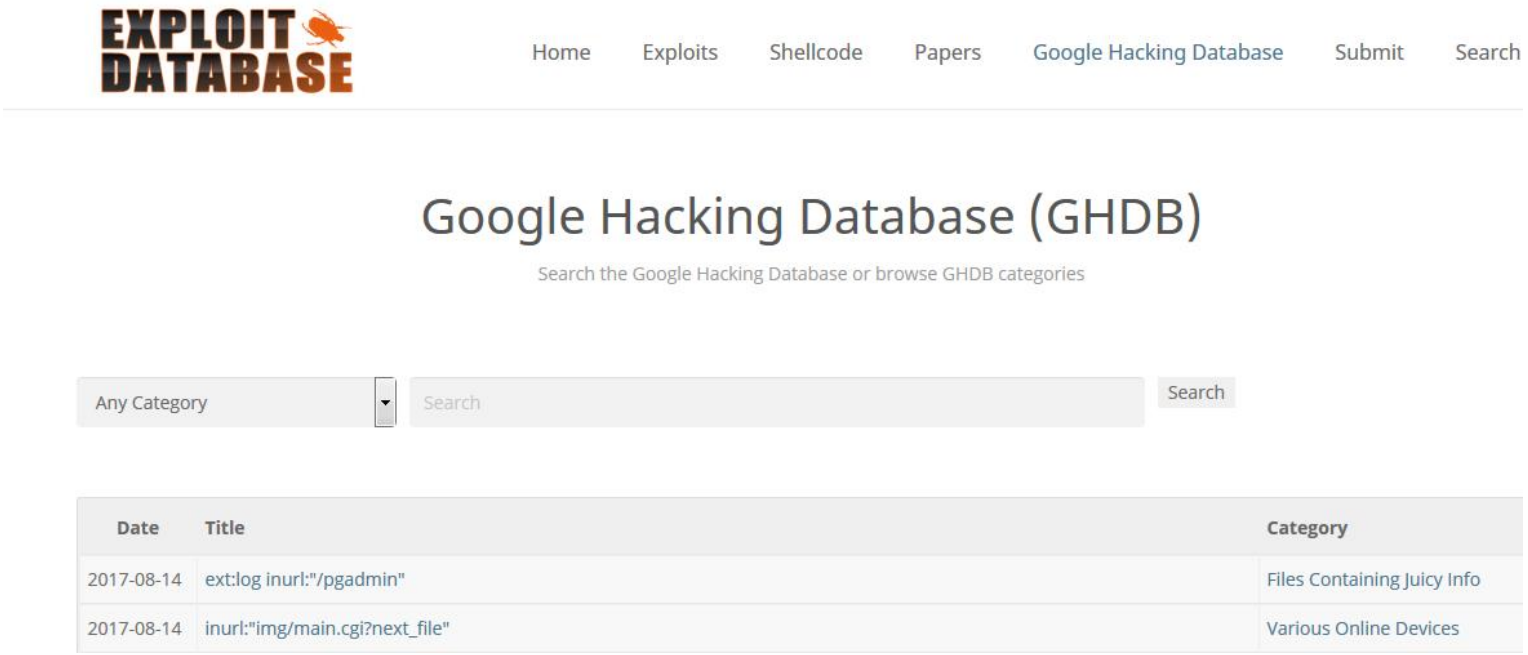
Scenario Questions

- 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)?

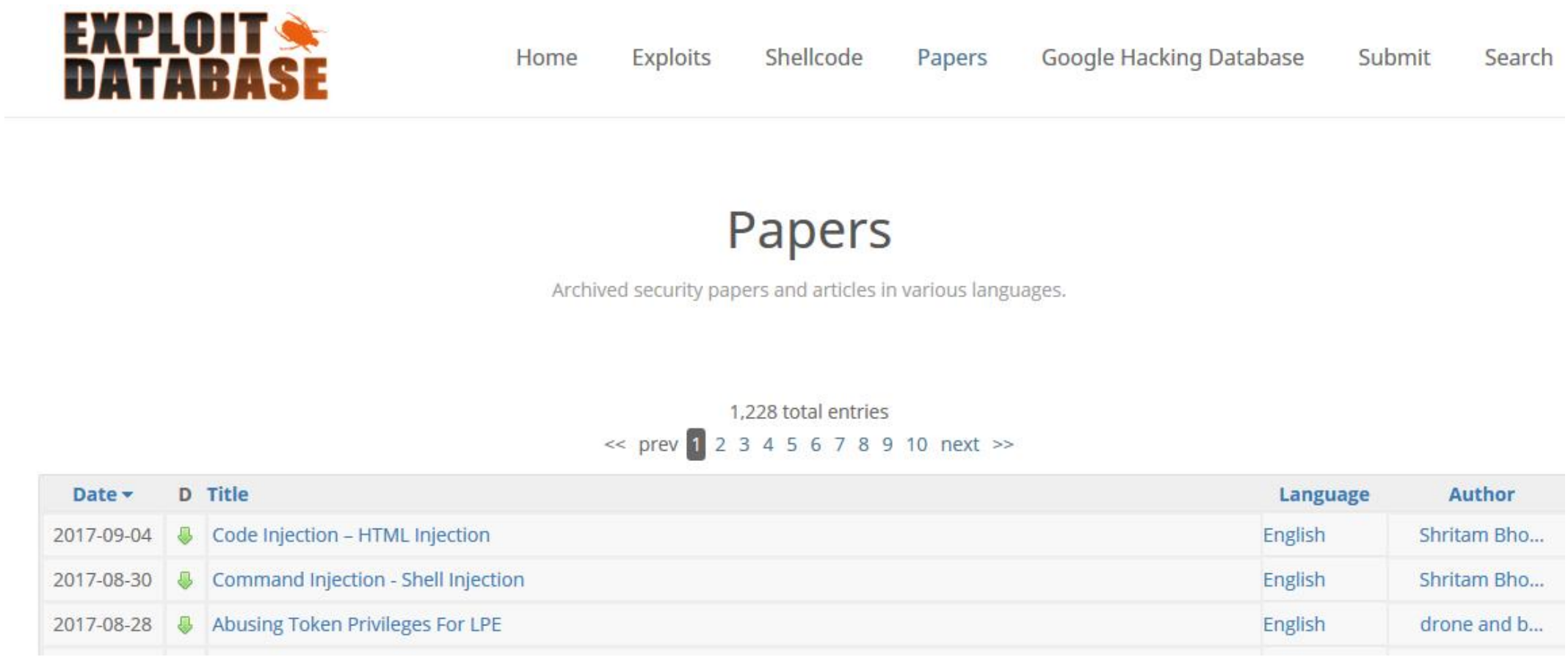
NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, Appendix B - Scenariors page: Appendix B-1

What a difference a URL can make!

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



Information for good and/or bad



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

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

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C)

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.

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C) (2)

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)

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

- 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

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. (l)

Resources

Image copied from: innovation.ed.gov

Frameworks/References (partial)

- SP 800-53
- SP 800-171 Revision 1
- 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

- 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

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

SANS

Login

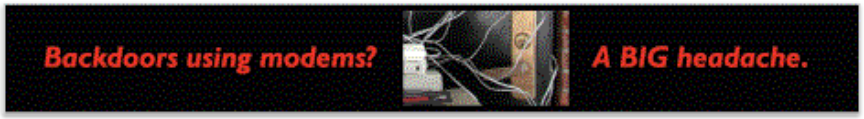
Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

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

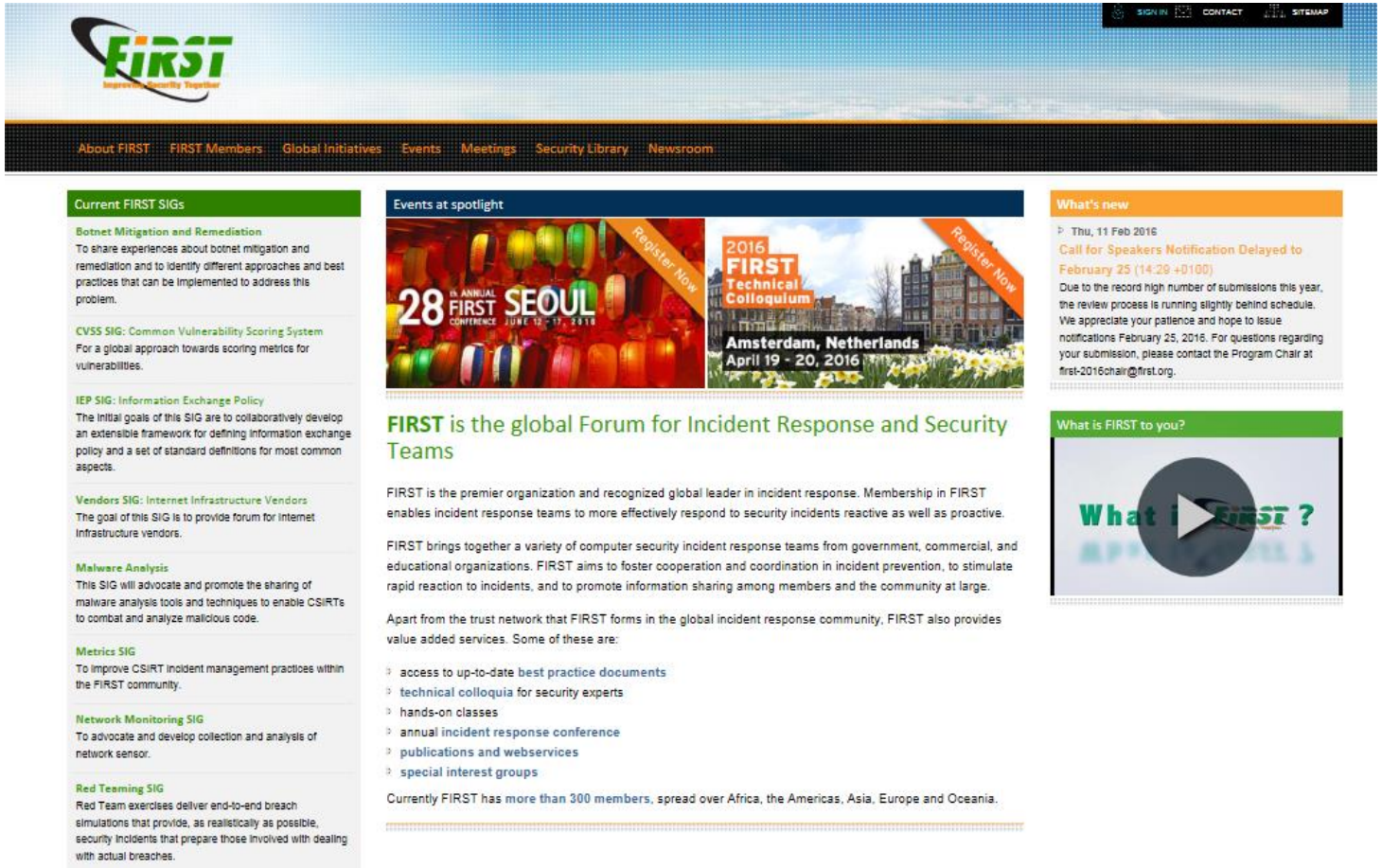
Get Newsletters

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

First.org



DIB ISAC

Take advantage of resources and tools

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

Create a 30 day action plan

- Review DFAR 252.204-7012
- Review NIST SP 800-171 Revision 1
  - Group requirements by difficulty/technical requirement
    - Administrative – 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

U.S. DHS, US-CERT, Disposing of Devices Safely, 2012 Carnegie Mellon University. Produce for US-CERT

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 computes/internet
- Bitcoin account – separate computer

It’s easy to sleep when your information is secure

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)

ACQUISITION HOUR LIVE WEBINAR SERIES

- 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 15, 2017 – **Compliance with NEW DOD regulations on Safeguarding Covered Defense Information – a Legal Perspective** – CLICK HERE for additional information – presented by Husch Blackwell LLP
- 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)
- November 29, 2017 – **Overview of CPARS** – CLICK HERE for additional information – presented by Carol Murphy, Wisconsin Procurement Institute (WPI)
- December 5, 2017 – **The SBA 8(a) certification program** – CLICK HERE for additional information – presented by Shane Mahaffy, Lead Business Opportunity Specialist, US.Small Business Administration (SBA)
- December 6, 2017 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – CLICK HERE for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)

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