




A Procurement Technical
Assistance Center (PTAC)

A large, white, neoclassical building with a prominent green dome, illuminated at dusk. The building is surrounded by trees and a fence. The sky is a deep blue.

Cyber Security for Current and Prospective DOD Contractors and Subcontractors ACQUISITION HOUR WEBINAR February 28, 2018



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!

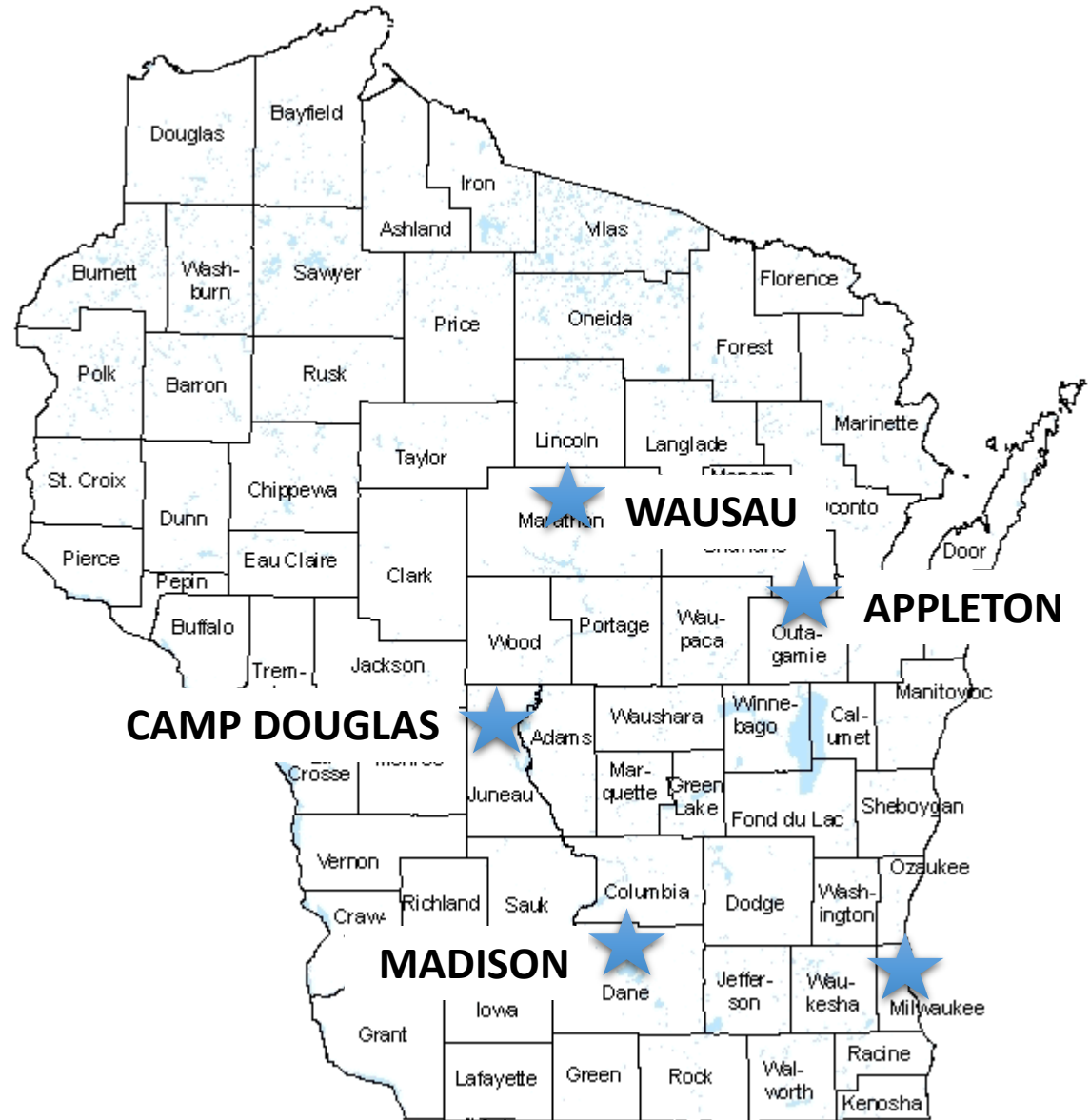
ABOUT WPI SUPPORTING THE MISSION

SERVING WISCONSIN
COMPANIES FOR 30 YEARS!

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*



JULY DLA "THE LINK" ISSUES AVAILABLE ONLINE

www.wispro.org

UPCOMING EVENTS

AUGUST 2 2017
ACQUISITION HOUR: GOVERNMENT PROPERTY MANAGEMENT FOR FEDERAL CONTRACTORS AND SUBCONTRACTORS

AUGUST 2 2017
HOW TO DO BUSINESS WITH THE DEPARTMENT OF VETERANS AFFAIRS
IRON MOUNTAIN, MI »

AUGUST 3 2017
HOW TO DO BUSINESS WITH THE DEPARTMENT OF VETERANS AFFAIRS
APPLETON, WI »

AUGUST 16 2017
ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS

SEPTEMBER 19 2017
ACQUISITION HOUR: SELLING TO THE STATE OF WISCONSIN AND LOCAL GOVERNMENTS

CURRENT OPPORTUNITIES (4)

SERVICES OFFERED BY WPI

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

CYBER FUNDAMENTALS FOR DFARS 252.204-7012 IMPLEMENTATION

Marc N. Violante

Wisconsin Procurement Institute

February 28, 2018



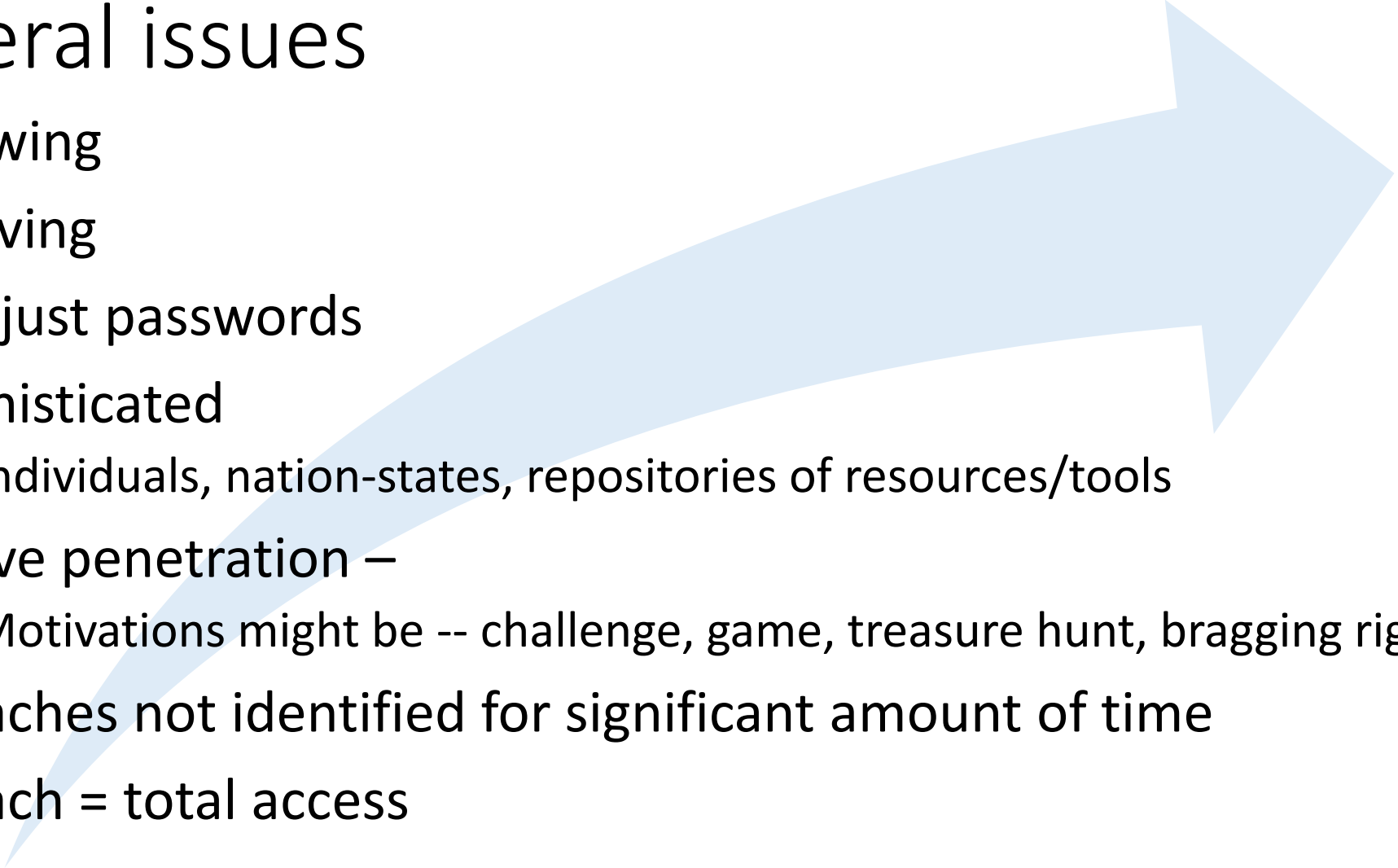
Image source: readywisconsin.wi.gov

Webinar Overview

1. General background
2. Overview of NIST requirements
3. Overview of related requirements
4. Perspective
5. Starting points for implementation
6. References



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
- 

Snap shot of current stories

[North Korea Is Upping Its Offensive Cyber Operations](#) // Patrick Tucker

As Pyongyang runs out of money for missile tests, expect more hacking.

[Just Over Half of Agencies Met a Web Encryption Security Deadline](#) // Joseph Marks

Fifty-four percent of federal websites met the deadline for HTTPS encryption and other security upgrades.

[Justice Launches Cyber Task Force](#) // Joseph Marks

The task force will examine cyber efforts to undermine elections and critical infrastructure.

[Beware of W-2-Related Phishing Scams](#) // Heather Kuldell

Don't get scammed this tax season.

[Secretaries of State Find Federal Election Cyber Intelligence Elusive](#) // Dave Nyczepir

With the upcoming midterm elections, it's a race to establish better information sharing between Homeland Security and state and local elections officials.

Federal supply chain – the soft underbelly

[Vulnerabilities](#) [Email Security](#) [Virus & Malware](#) [IoT Security](#) [Endpoint Security](#)

Home > Risk Management



U.S. Government Contractors Score Poorly on Cyber Risk Tests

By [Kevin Townsend](#) on February 16, 2018

in Share
G+
Tweet
Recommend 17
RSS

Report Analyzes Cyber Risk of Federal Supply Chain

Attacks against the supply chain are not uncommon. It represents the soft underbelly of large organizations that are otherwise well defended. The federal government is not an exception -- in fact, federal agencies are especially reliant on their supply chain; and the security posture of that supply chain is of national importance.

This importance is not unrecognized. The May 2017 [presidential Executive Order](#) specified that the supply chain be included in security improvements: it called for a report, "on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks."

SECURITYWEEK DAILY BRIEFING

BRIEFING






SECURITYWEEK



ICS

CYBER SECURITY
CONFERENCE

THE ORIGINAL

<https://www.securityweek.com/us-government-contractors-score-poorly-cyber-risk-tests>

2/28/2018

What happens when ----



Ours



Theirs

Images copied from: eglin.af.mil

2/28/2018

What if there is a potential breach?

“Don’t panic. Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. **DoD does not penalize contractors acting in good faith.** The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.”



Cybersecurity Landscape

Cyber threats targeting government unclassified information have dramatically increased

Cybersecurity incidents have surged 38% since 2014

The Global State of Information Security @ Survey 2016

Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%).

AT&T Cybersecurity Insights Vol. 4

Cyber attacks cost companies \$400 billion every year

Inga Beale, CEO, Lloyds

89% of breaches had a financial or espionage motive

64% of confirmed data breaches involved weak, default or stolen passwords

2016 Data Breach Investigations Report, Verizon

Cybercrime will cost businesses over \$2 trillion by 2019

Juniper Research

In a study of 200 corporate directors, 80% said that cyber security is discussed at most or all board meetings. However, two-thirds of CIOs and CISOs say senior leaders in their organization don't view cyber security as a strategic priority.

NYSE Governance Services and security vendor Veracode



Unclassified

3

Cybersecurity in DoD Acquisition Regulations

The threats facing the DoD's unclassified information have dramatically increased as we provide more services online, digitally store data, and rely on contractors for a variety of information technology services. Recent high-profile incidents involving government information demand that information system security requirements are clearly, effectively, and consistently communicated to both government and industry.

The contents of this "Cybersecurity in Acquisition Regulations" page addresses the DoD's ongoing efforts –executed in partnership with industry – to improve the nation's cybersecurity. Specifically, it addresses DoD's effort to:

- Ensure that unclassified DoD information residing on or transiting through covered contractor networks or information systems is safeguarded from cyber incidents and that any consequences associated with loss of this information are assessed and minimized, and
- Understand when a cyber incident impacts a company's ability to provide operationally critical support to DoD.

The DoD needs to protect it's information – whether it resides on the Department's networks and systems, or on the networks and systems of our partners in industry – so that our capabilities are not exploited, misdirected, countered, or cloned. Protecting this information will save warfighter lives. The cyber threat is not going away – we must defend our networks and systems, and the information that resides on them. Cybersecurity is a shared challenge, and we must work together to address it and reduce risk.

<http://dodprocurementtoolbox.com/site-pages/cybersecurity-dod-acquisition-regulations> - visited Nov 7, 2017

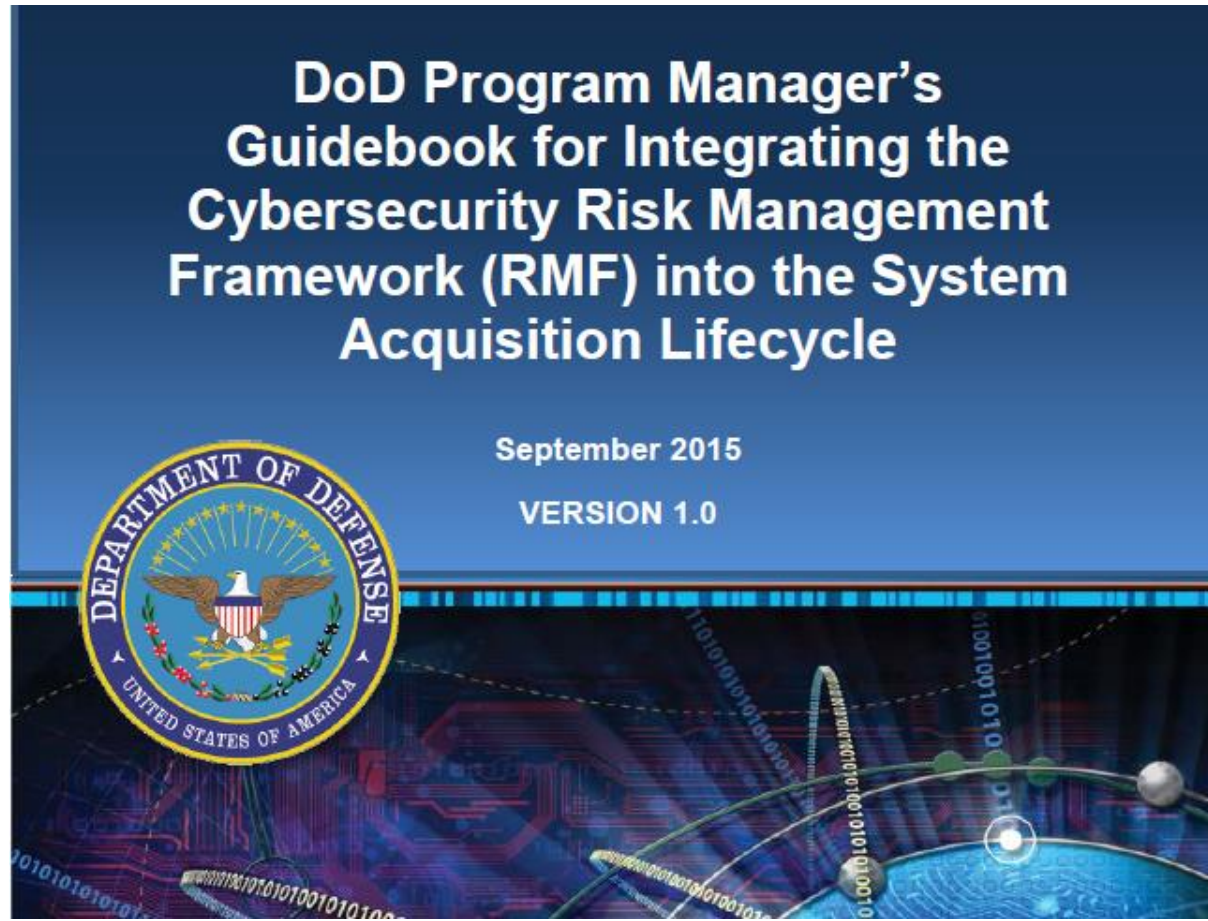
Other DoD Requirements exist

Policy/Regulations

Safeguarding Covered Defense Information and Cyber Incident Reporting

Name	Date	
DFARS Rule 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting	Current Version	View >>
DFARS Provision 252.204-7008 - Compliance with Safeguarding Covered Defense Information Controls	Current Version	View >>
DFARS Clause 252.204-7009 - Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	Current Version	View >>
DFARS Clause 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting	Current Version	View >>
DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Final Rule, dated October 21, 2016	10/2016	View >>
DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Interim Rule, dated December 30, 2015	12/2015	View >>
DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Interim Rule, August 26, 2015	8/2015	View >>

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>

2/28/2018

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

New medium – same requirements; tailored

NUMBER 5230.25
November 6, 1984

Incorporating Change 1, August 18, 1995
USDR&E

SUBJECT: Withholding of Unclassified Technical Data From Public Disclosure

REFERENCES, continued

- References: (a) Title 10, United States Code, Section 140c, as added by Public Law 98-94, "Department of Defense Authorization Act, 1984," Section 1217, September 24, 1983
- (b) Executive Order 12470, "Continuation of Export Control Regulations," March 30, 1984
- (c) Public Law 90-629, "Arms Export Control Act," as amended (22 U.S.C. 2751 et seq.)
- (d) through (n), see enclosure 1

- (d) DoD Instruction 5200.21, "Dissemination of DoD Technical Information," September 27, 1979
- (e) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980
- (f) Export Administration Regulations
- (g) International Traffic in Arms Regulations
- (h) DoD Federal Acquisition Regulation Supplement
- (i) Public Law 89-487, "Freedom of Information Act," as amended (5 U.S.C. 552(b)(3) and (4))
- (j) Executive Order 12356, "National Security Information," April 2, 1982
- (k) DoD 5200.1-R, "Information Security Program Regulation," August 1982
- (l) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
- (m) Militarily Critical Technologies List, October 1984
- (n) DoD Instruction 7230.7, "User Charges," June 12, 1979

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both **paper and digital**.

DFAR 252.204-7012

- Contractor systems with – Covered Defense Information (CDI)
 - transiting | stored | transmitted from
- **CDI** – unclassified controlled technical information in **CUI** Registry
- Required to provide Adequate Security
 - Implement NIST(SP) 800-171 **at a minimum**
- Monitor network/system – “capture/submit – malware”
- 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

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

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.

Subcontracts – the contractor shall

“Subcontract” means a contract or contractual action entered into by a prime contractor or subcontractor for the purpose of obtaining supplies, materials, equipment, or services of any kind under a prime contract.”

“Subcontractor” (1) means any person, other than the prime contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract; and (2) includes any person who offers to furnish or furnishes general supplies to the prime contractor or a higher tier subcontractor.

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.

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).

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 (SP) 800-171 Revision 1

an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the information security requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute,



In addition to the security objective of *confidentiality*, the objectives of *integrity* and *availability* remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program. While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Organizations that are interested in or required to comply with

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

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.

NIST (SP) 800-171 Revision 1 - Requirements

3.1	ACCESS CONTROL	10
3.2	AWARENESS AND TRAINING	11
3.3	AUDIT AND ACCOUNTABILITY	11
3.4	CONFIGURATION MANAGEMENT	11
3.5	IDENTIFICATION AND AUTHENTICATION	12
3.6	INCIDENT RESPONSE	12
3.7	MAINTENANCE	13
3.8	MEDIA PROTECTION	13
3.9	PERSONNEL SECURITY	13
3.10	PHYSICAL PROTECTION	14
3.11	RISK ASSESSMENT	14
3.12	SECURITY ASSESSMENT	14
3.13	SYSTEM AND COMMUNICATIONS PROTECTION	15
3.14	SYSTEM AND INFORMATION INTEGRITY	15

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.

Security Controls

By Stephen Northcutt

Version 1.2

Control categories: (examples)

- Physical control
 - Lock
 - fence
- Access controls
- Admin controls
 - Segregation of duties

Security controls are technical or administrative safeguards or counter measures to avoid, counteract or minimize loss or unavailability due to threats acting on their matching vulnerability, i.e., security risk. Controls are referenced all the time in security, but they are rarely defined. The purpose of this section is to define technical, administrative/personnel, preventative, detective, and corrective compensating controls, as well as general controls.

According to the GAO, "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people." [1]

<https://www.sans.edu/cyber-research/security-laboratory/article/security-controls> visited 2/28/2017

2/28/2018

DFARS / NIST Implementation

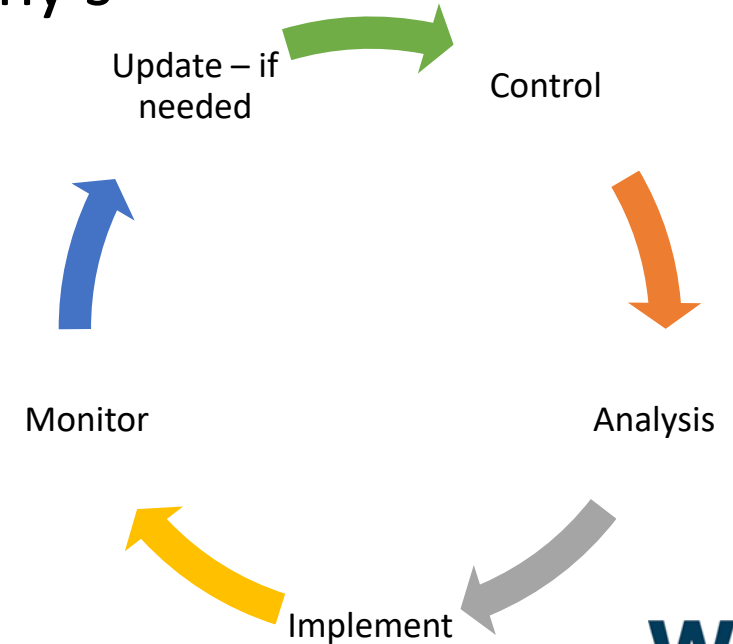
A reasonable first step may be for company personnel with knowledge of their information systems security practices to

- 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

NIST (SP) 800-171 Revision 1 – key idea

3.4.4 Analyze the security impact of changes prior to implementation.

- Don't act too quickly
- Ask questions – in quality there are the 5 why's
- Test first if possible
- Look for unintended consequences
- Monitor impact
- Look for ...



NIST (SP) 800-171 Revision 1, December 2016 : refers to 3.4.4 only

DFARS 252.204-7012 – Implementation Compliance

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.

DFARS 252.204-7012 – Implementation Compliance - background

(d) A cyber incident that is reported by a contractor or subcontractor shall **not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security** on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at [252.204-7012](#), Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see [PGI 204.7303-3\(a\)\(3\)](#) ([DFARS/PGI view](#))). The contracting officer shall consider such cyber incidents **in the context of an overall assessment of a contractor's compliance** with the requirements of the clause at [252.204-7012](#).

DFARS 252.204-7012 – Implementation Compliance – Contracting Officer's actions

(ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and

Risk Assessment – NIST (SP)800-39

- A fundamental component of an organizational risk management process – may be conducted at different organizational tiers
 - Organization, mission/business, IT systems level
- Identify, estimate and prioritize risk to an organization
- Purpose – inform and advise, decision makers and support risk responses by
 - Identifying relevant threats
 - Vulnerabilities
 - Impact
 - Likelihood that harm will occur
- Outcome is a determination of risk

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



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?

2/28/2018

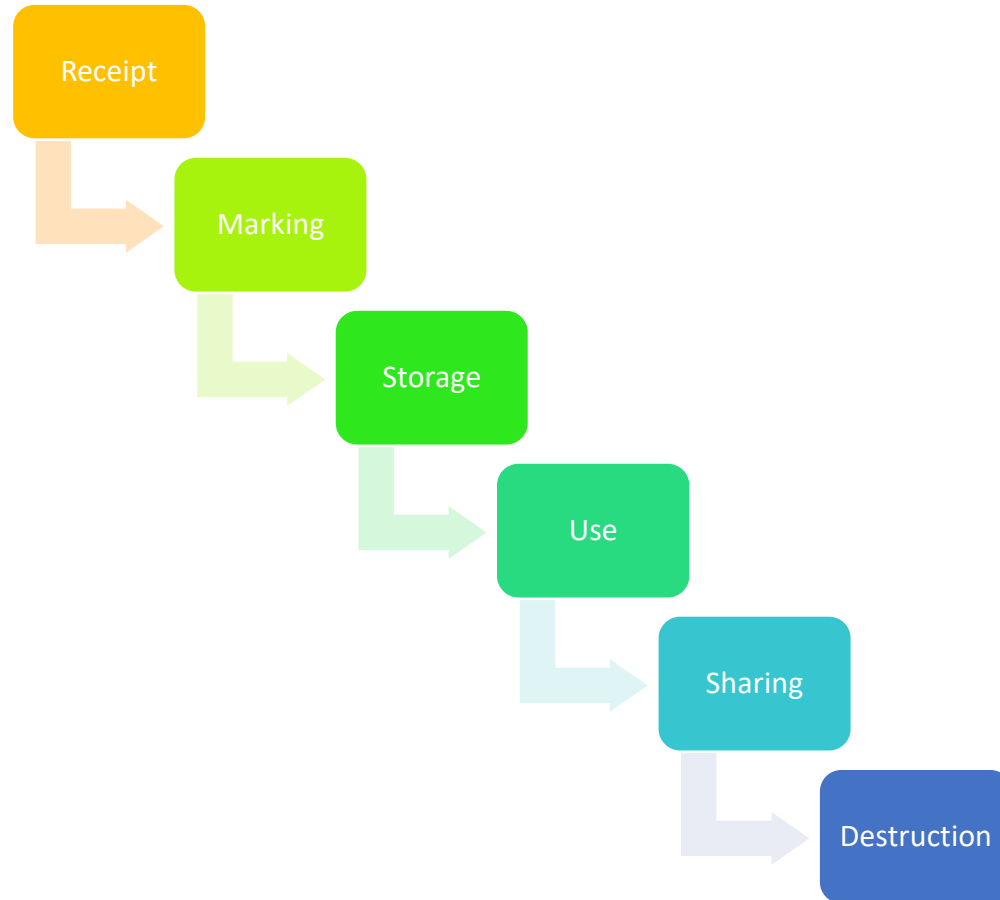
Implementation – Contractor's responsibility

- Ultimately, it is the contractor's responsibility to determine whether it 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.

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.

Information – life cycle, general elements



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

Information – life cycle – NIST (examples)

Receipt - 3.1.3 Control the flow of CUI in accordance with approved authorizations.

Marking - 3.8.4 Mark media with necessary CUI markings and distribution limitations

Storage -- 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Use - 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

Sharing - 3.10.3 Escort visitors and monitor visitor activity.

Destruction - 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

The Existence of CUI is the controlling factor

Marking email

Posted on [October 23, 2017](#) by [Mark Riddle](#)

The principles for marking CUI are the same when sending email; the banner must appear at the top portion of the email. In addition to the banner marking, an indicator

[Continue reading →](#)

Posted in [Marking & examples](#) | Tagged [email](#), [marking](#), [marking emails](#), [marking example](#), [sample marking](#) | [Leave a comment](#)

Marking Controlled Technical Information

- Is it required by contract or other reference?
- Does it make good business/security sense?
- Internal circulation v. external
 - Similar thoughts related to communicating – hot, fragile, dangerous material
 - How will external entities be informed/know?
- If started, marking, can it be stopped and started? – consistency
- Why this one but not that one?

Marking CTI - NIST

The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include **inconsistent markings**, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI *Registry*.

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.4 Mark media with necessary CUI markings and distribution limitations. Footnote #25

Marking Media



Removable Hard drive

3.8.4 Mark media with necessary CUI markings and distribution limitations. Footnote #25 NIST SP 800-171 r1

Equipment can be marked or labeled to indicate that CUI is stored on the device.




NOTE: DOGW is an acronym for Department of Good Works.

Marking Controlled Technical Information

Category-Subcategory	Marking
Agriculture	AG
Controlled Technical Information	CTI
Critical Infrastructure	CRIT
Critical Infrastructure-Ammonium Nitrate	CRITAN
Critical Infrastructure-Chemical-terrorism Vulnerability Information	CVI
Critical Infrastructure-Critical Energy Infrastructure Information	CEII

Basic v. Specified

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012 	Specified	

CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

Other categories that may apply

Proprietary Business Information	PROPIN
Proprietary Business Information-Manufacturer	MFC
Proprietary Business Information-Ocean Common Carrier and Marine Terminal Operator Agreements	OCCMTO
Proprietary Business Information-Ocean Common Carrier Service Contracts	SERV
Proprietary Business Information-Postal	POST
Proprietary Business Information-System for Award Management	CONREG

Marking email – for example

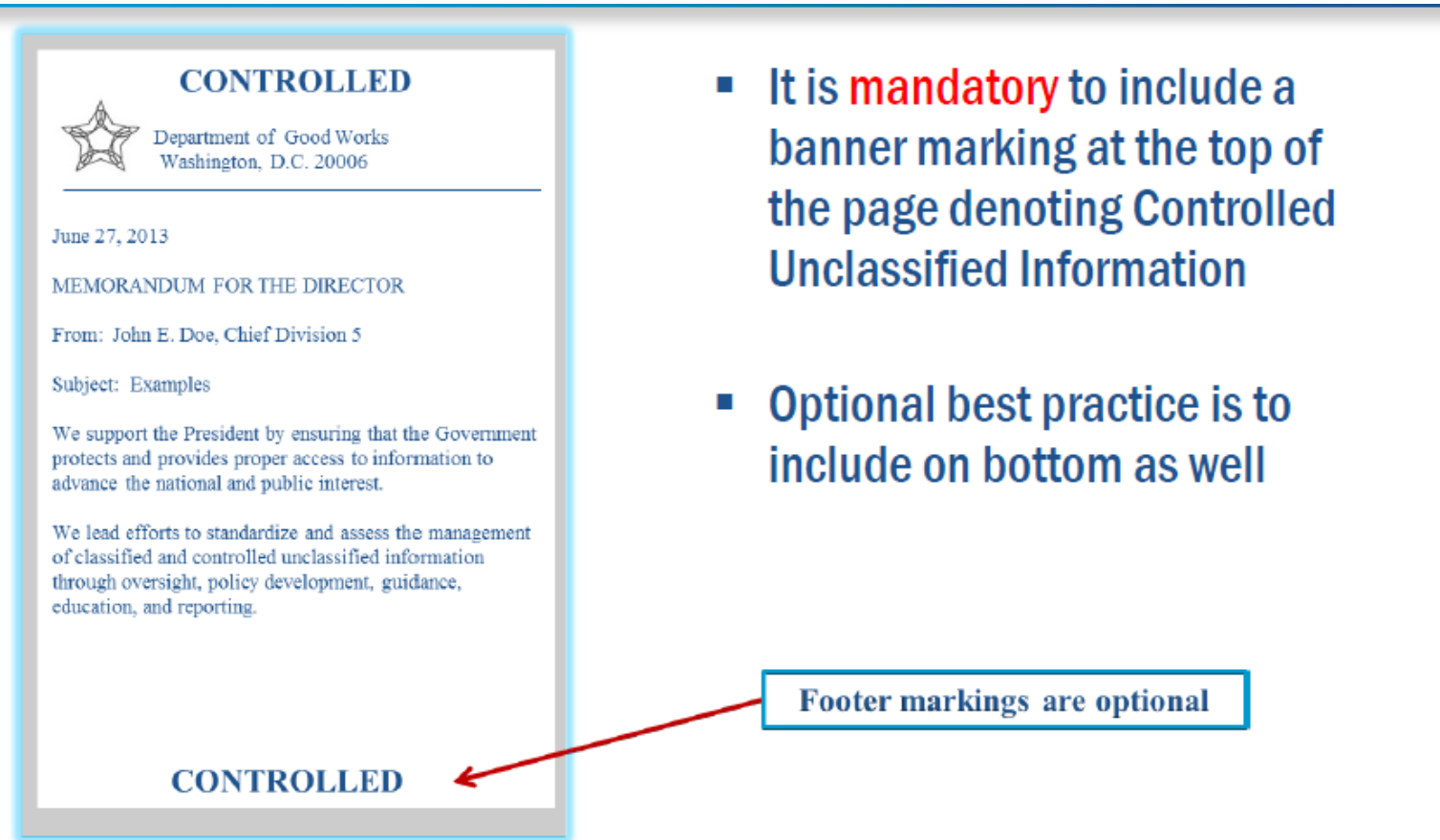
- From <https://www.archives.gov/cui/registry/category-marking-list>

Send	To...	Secret Squirrel
	Cc...	
	Bcc...	
Subject		CUI/CTI - Controlled Information -


(U) Public Information

(CUI/CTI) This paragraph contains CUI|

Mandatory CUI Banner Marking - Agency



CONTROLLED

 Department of Good Works
Washington, D.C. 20006

June 27, 2013

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

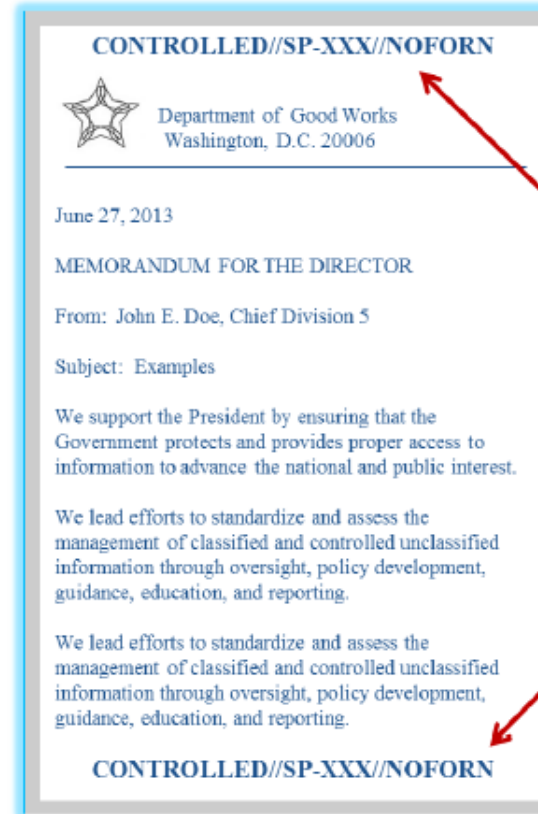
CONTROLLED

Footer markings are optional

- It is **mandatory** to include a banner marking at the top of the page denoting Controlled Unclassified Information
- Optional best practice is to include on bottom as well

Limited Dissemination Marking




- Limited Dissemination Controls are not mandatory
- Limited Dissemination Control Markings are separated from other elements of the banner by two forward slashes (//)
- When a document contains multiple Limited Dissemination Control Markings, those Limited Dissemination Control Markings separated by a single slash (/)



In this example, the specified category is indicated by SP-XXX, and the “No Foreign dissemination” control is used.

CUI Coversheets

Agencies may use coversheets to identify CUI, alert observers that CUI is present from a distance, and serve as a shield to protect CUI from inadvertent disclosure. If an agency chooses to use coversheets, it must use one of the following CUI EA-approved coversheets:

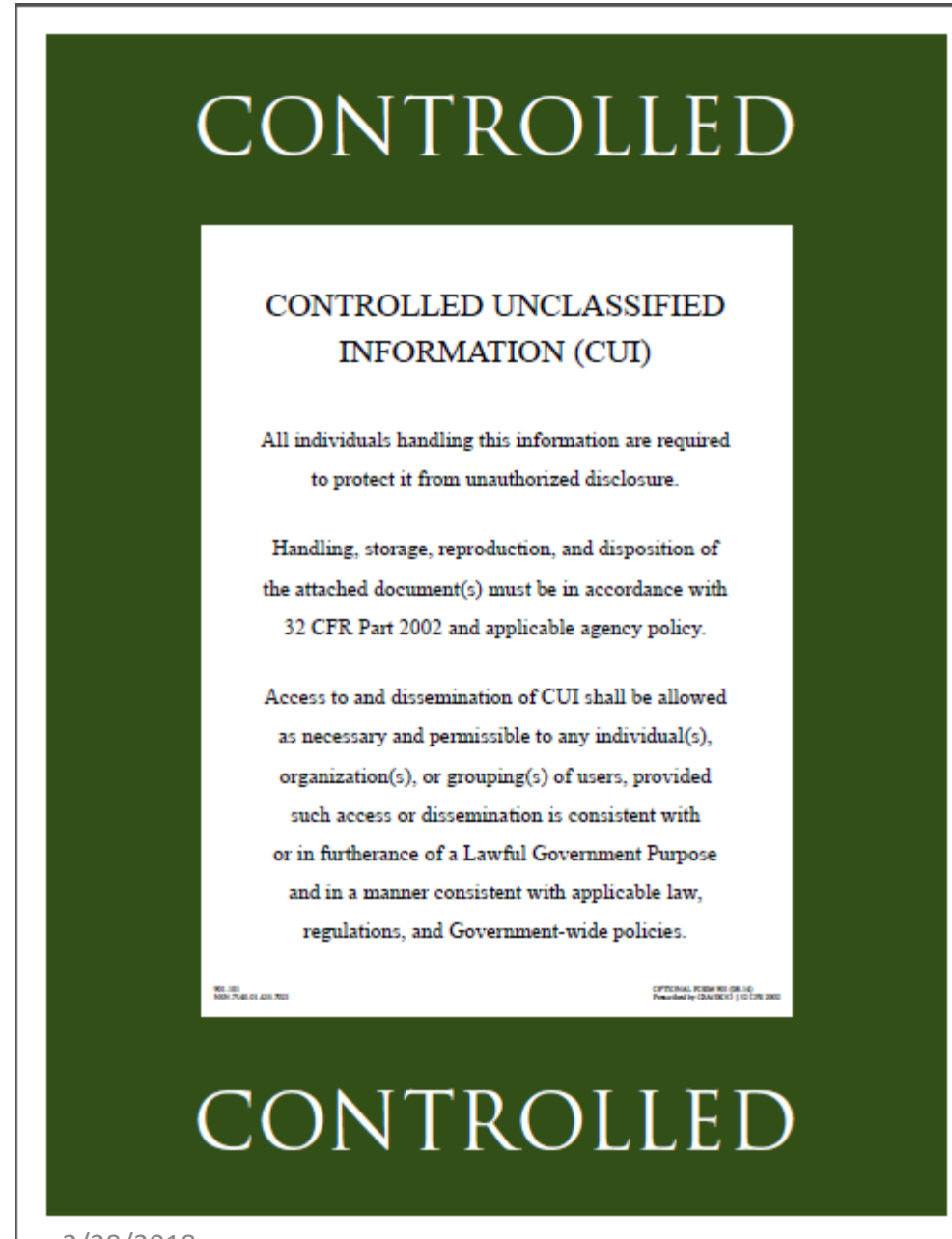
Form	Name	Description
OF 901 	Controlled Coversheet	This coversheet can serve as a shield to protect CUI from inadvertent disclosure and to alert observers that CUI is attached to it.
OF 902 	Controlled Coversheet – Category and Subcategory	This coversheet can serve as a shield to protect CUI from inadvertent disclosure and to alert observers that CUI is attached to it. This coversheet is a fillable pdf that allows holders to populate any applicable category/subcategory of CUI contained in the document.
OF 903 	Controlled Coversheet - Attention	This coversheet can serve as a shield to protect CUI from inadvertent disclosure and to alert observers that CUI is attached to it. This coversheet is a fillable pdf that allows holders to populate any applicable category/subcategory of CUI contained in the document as well as any other pertinent information related to handling or dissemination.



<https://www.archives.gov/cui/additional-tools>

2/28/2018

CUI Coversheets - example



<https://www.archives.gov/cui/additional-tools>

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?



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.

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

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

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

2/28/2018

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

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 – over arching idea

- “**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>

Cyber incident – the lost USB

- **London Heathrow Airport’s security laid bare by one lost USB stick**

If someone set out to invent a risky way to transport important data around it’s hard to imagine they’d better the USB flash stick for calamitous efficiency.

They’re cheap enough to feel disposable, store large numbers of files, and despite years of mishaps barely any are sold with encryption security.

They’re also incredibly popular – which is why in 2017 we’re still writing about cases like the [USB stick found in a west London street](#) that turned out to contain **2.5Gb of unprotected files detailing many of the anti-terrorism procedures and systems used to protect one of the world’s busiest airports.**

This included: the route taken by the Queen, politicians and dignitaries when using the airport’s secure departure suite; radio codes used to indicate hijackings;

<https://nakedsecurity.sophos.com/2017/10/31/london-heathrow-airports-security-laid-bare-by-one-lost-usb-stick/>

Protective measures - NIST

- ➔ **3.8.4** Mark media with necessary CUI markings and distribution limitations.²⁵
- 3.8.5** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- ➔ **3.8.6** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- 3.8.7** Control the use of removable media on system components.

- 3.13.10** Establish and manage cryptographic keys for cryptography employed in organizational systems.
- ➔ **3.13.11** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

What data/information is on your computer?

On your Network?

What devices are being used?

What are the entry points?

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



- 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.



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...

Who is visiting your site?



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

2/28/2018

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

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>				

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.

Security requirement 3.12.4 (System Security Plan, added by NIST SP 800-171, Revision 1)⁸⁰

- 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.

²⁶ There is no prescribed format or specified level of detail for *system security plans*. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans. [Footnote 26 page 14](#)

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

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.



¶

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.

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



Main menu

About

Training & Awareness

Students & Home Users

Developing a Security Plan

No computer or workstation is immune to compromise. Understanding the value and protecting them is the responsibility of everyone 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

Developing a Security Plan

“No computer or workstation is immune to compromise.”

“The IT Security Plan and process can implemented and maintained with minimum effort and resources. It is a first step to eliminating the bulk of vulnerabilities which cause compromises.

1. Take an inventory of your physical and information assets (what are you protecting?).
2. Perform a risk assessment to determine what level of security is needed to protect your information assets.
3. Complete the checklist to make you aware of your security strengths and weaknesses
4. Complete an evaluation. Evaluate your findings and discuss recommendations to correct deficiencies and/or improve security with departmental administration and IT staff.
5. Develop a security plan. Create a Security Plan with target dates for implementation.

Assign responsibilities and target dates for the plan. Then **monitor progress** with reports on improvements and security initiatives.”

<https://rusecure.rutgers.edu/content/developing-security-plan> - visited January 24, 2018

2/28/2018

Sample Security Plan – see slide reference

All of the following bulleted items were marked 'no' on the Security Checklist. (corrective actions)

- Regular testing of UPSs will take place monthly on the 1st.
- Maintain diagnostic software onsite-diagnostic software will be researched and purchased at the discretion of the Systems Administrator. Said software will be locked in the storeroom.
- Target date to move database to new software-Database will take place within two months (target date)
- Provisions to continue operations in the event central services (RIAS) software is not available-A team will be created to develop a plan for business continuity in the event of central services downtime.
- Network documentation for computers and network devices-Part-time students will be hired for the purpose of creating documentation.

<https://rusecure.rutgers.edu/content/developing-security-plan> - visited January 24, 2018

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

2/28/2018

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.

Additional NIST 800-171 R1 requirements –

3.14.1 Identify, report, and correct information and system flaws in a timely manner.

3.14.3 Monitor system security alerts and advisories and take appropriate actions in response.

Comment: Don't view the requirements in isolation.

Look for related requirements

- **3.1.13** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- **3.1.17** Protect wireless access using authentication and encryption
- **3.1.19** Encrypt CUI on mobile devices and mobile computing platforms.21
- **3.5.10** Store and transmit only cryptographically-protected passwords.
- **3.13.8** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- **3.13.10** Establish and manage cryptographic keys for cryptography employed in organizational systems.
- **3.13.11** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

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.

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

Indications of CUI

- 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>

CUI – National Archives

Controlled Unclassified Info... x

https://www.archives.gov/cui

Search...

NATIONAL ARCHIVES

RESEARCH OUR RECORDS VETERANS' SERVICE RECORDS EDUCATOR RESOURCES VISIT US AMERICA'S FOUNDING DOCUMENTS

Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI)

Please visit the CUI blog: [Controlled Unclassified Information](#) for more information.

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. [Learn About CUI](#) →

Registry

The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry: Go

Categories, Markings and Controls:

- Category-Subcategory List
- Category-Subcategory Markings
- Limited Dissemination Controls

Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook

Blog

Training Tools

News and Notices

- October 23, 2017 - The [CUI Blog](#) has been launched
- September 12, 2017 - New [Training Tools](#) have been posted
- September 12, 2017 - [Destruction Labels](#) have been posted
- August 17, 2017 - New [Policy and Guidance](#) documents have been posted

CONTROLLED UNCLASSIFIED INFORMATION

Use the CUI Logo

Contact Us

CUI Categories and Subcategories - examples

- Agriculture
- Controlled Technical Information
- Critical Infrastructure
- Export Control
- Financial
- Immigration
- Intelligence
- Law Enforcement
- NATO
- Others categories (14 other categories)

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.**

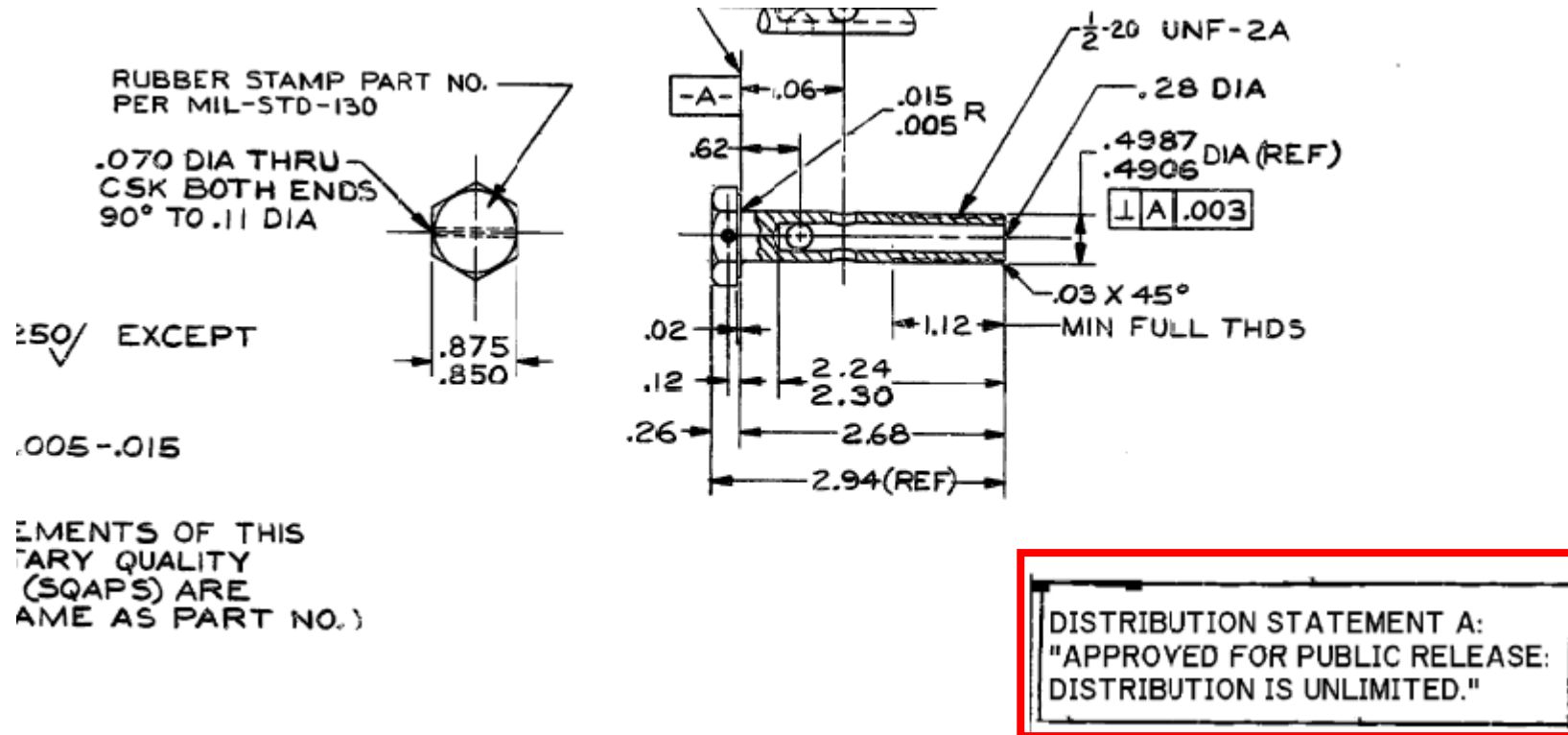


Distribution Statements

- 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

Distribution Statement A - example



Attachment to client email

2/28/2018

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 – the why



- DoS
- 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

2/28/2018

Denial of Service



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](#).

The Internet Sees Nearly 30,000 Distinct DoS Attacks Each Day: Study

The incidence of denial-of-service (DoS) attacks has consistently grown over the last few years, "steadily becoming one of the biggest threats to Internet stability and reliability."

the researchers discovered that the internet suffers an average of 28,700 distinct DoS attacks every day. **This is claimed to be 1000 times greater than other reports have indicated.**

<http://www.securityweek.com/internet-sees-nearly-30000-distinct-dos-attacks-each-day-study>

2/28/2018

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

2/28/2018

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**

Email – Phishing – the ticking time bomb

- Email – “the backbone of business communications”
 - 3.7 billion users
 - 269 billion messages everyday
 - Cyber criminals’ primary vector to attempt to extract information
- Core problem
 - humans are simply vulnerable when it comes to being fooled by email scams – even those at the largest, most high-profile organizations.
- Success will lead to more sophistication of targeted attacks + increase
- Threat – combination of emails with social engineering
- Traditional approaches may not be suitable – see referenced article

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?

Spyware

submit the malicious software to
DoD Cyber Crime Center (DC3)

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

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

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

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

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

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*

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
- Online services
- Who – what is the service and who is the product?

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

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

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

2/28/2018

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](#)

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...

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

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.

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

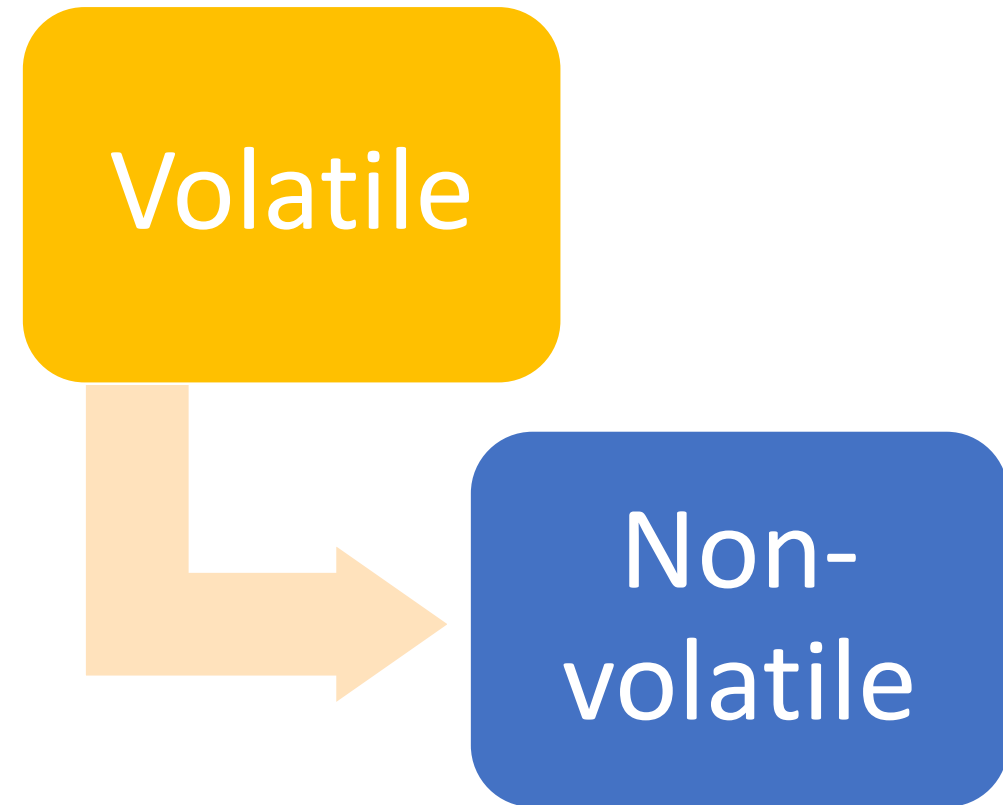
Maximizing Log value

- 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



Examining and Analyzing Network Traffic - 1

- 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 - 2

- 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

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)?

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>

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.

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)

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

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/current - green
 - Technical – will need outside assistance – yellow
 - Technical/investment - red
- 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? - marked
- 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 - partial

- **3.2.1/3.2.2** Are employees provided any IT training?
 - New hires
 - Current
- **3.9.1** Are employees screened prior to granting access to the IT system?
- **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- **3.1.7** Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?
 - **3.1.19** Encrypt CUI on mobile devices and mobile computing platforms.
- **3.9.2** Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

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

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

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

Monitor systems & Audit records

3.14.6 Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7 Identify unauthorized use of organizational systems.

3.3.1 Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

3.3.2 Ensure that the actions of **individual system users** can be uniquely traced to those users so they can be held accountable for their actions.

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



It's easy to sleep when
your information is
secure

Resources



Image copied from: innovation.ed.gov

2/28/2018

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 ¹⁵⁷

- 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

2/28/2018


[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

2/28/2018

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
Register Now

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

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.

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?

DIB ISAC

2/28/2018

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

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- March 13, 2018 – **Information Management for Federal Contractors** – [CLICK HERE](#) for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)
- March 14, 2018 – **Introduction to Certifications Available to Woman Owned Businesses** – [CLICK HERE](#) for additional information – presented by Kim Garber – Wisconsin Procurement Institute (WPI)
- March 27, 2018 – **Update on Federal Hour Wage Labor Laws** – [CLICK HERE](#) for additional information – presented by Corey Walton, Community Outreach and Resource Planning Specialist – U.S. Department of Labor/Wage & Hour Division
- March 27, 2018 – **Growing Your Small Business with the Disadvantaged Business Enterprise (DBE) Program** – [CLICK HERE](#) for additional information – presented by Benjamin Blanc – Wisconsin Procurement Institute (WPI)
- March 28, 2018 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – [CLICK HERE](#) for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)

UPCOMING EVENTS

[Federal Acquisition Regulations \(FAR\) Review](#) – Tuesday Evenings –
Webinar

[Step by Step Process to Start Working as a Federal Government Subcontractor – Part II](#) – February 28, 2018 – Manitowoc, WI

[Growing Your Business in Sawyer County, Wisconsin](#) – March 1, 2018 – Hayward, WI

[Developing your Marketing Materials for Government Sales](#) –
March 13, 2018 – Milwaukee, WI

UPCOMING EVENTS

Society of American Military Engineers (SAME) Joint Industry Days and Federal Agency Forum (JIDFAF) – April 9 – 10, 2018 – Northbrook, IL

Federal Acquisition Regulations, Understanding the Basics – April 11, 2018 – Iron Mountain, MI

Preparing a Winning Government Proposal – April 26, 2018 – Milwaukee, WI

12th Annual Volk Field – Fort McCoy Small Business Conference – June 26 – 27, 2018 – Fort McCoy, WI



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

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