Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

INFORMATION MANAGEMENT FOR FEDERAL CONTACTORS ACQUISITION HOUR WEBINAR

March 13, 2018




WEBINAR ETIQUETTE

PLEASE

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

THANK YOU!

ABOUT WPI
SUPPORTING THE MISSION

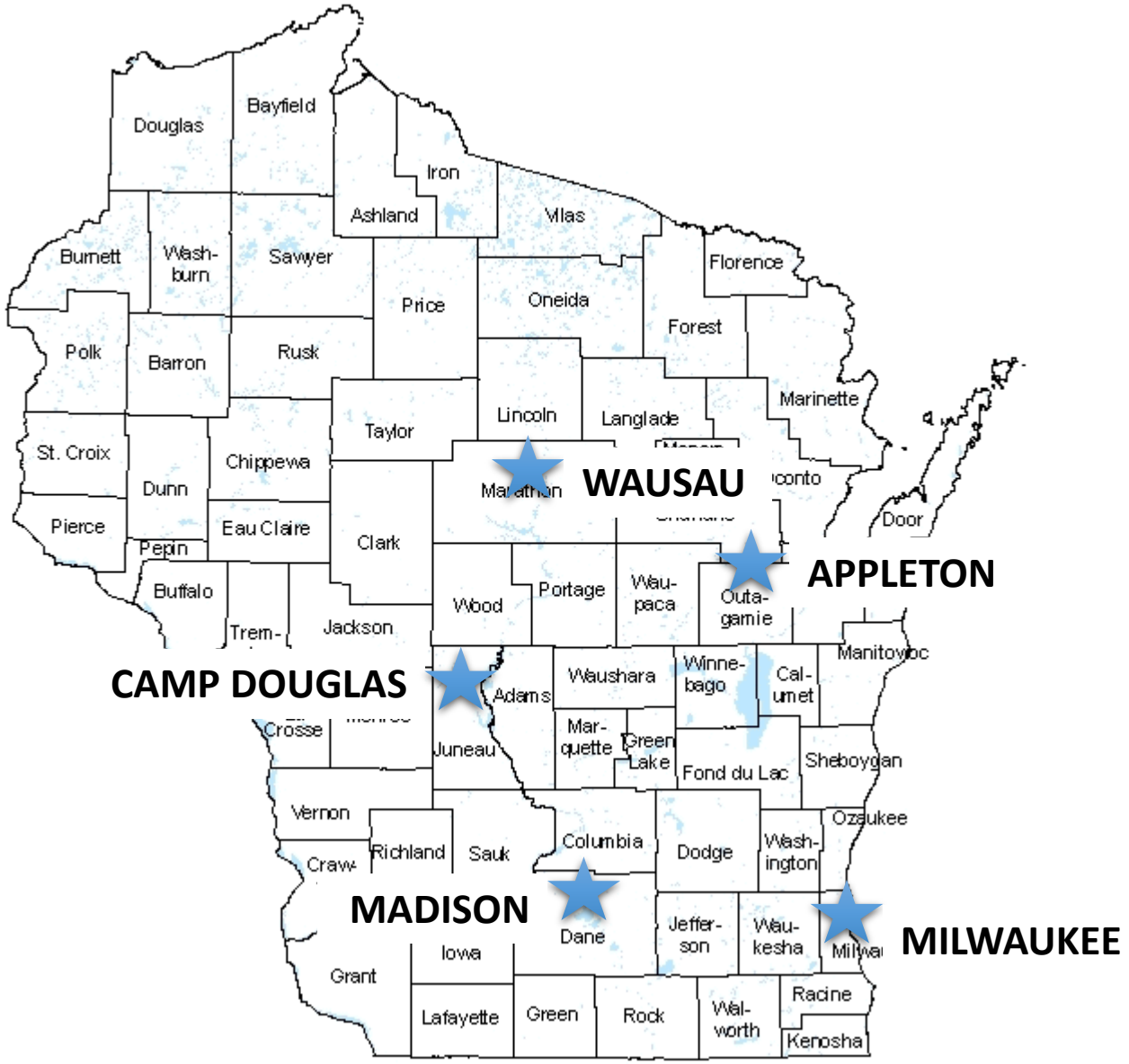
SERVING WISCONSIN COMPANIES FOR 30 YEARS!

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

WPI OFFICE LOCATIONS

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




Search ...
BLOG
SERVICES
ABOUT
MY ACCOUNT
DONATE
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
OTHER GOVERNMENT & GRANTS
SUCCESS & AWARDS
FAQS
CLICK HERE TO VIEW WPI NEWSLETTER
www.wispro.org
UPCOMING EVENTS
JANUARY 10 2018
SELLING TO UNCLE SAM-UNDERSTANDING THE GOVERNMENT MARKETPLACE
IRON MOUNTAIN, MI »
JANUARY 17 2018
END OF YEAR FEDERAL CONTRACTOR UPDATE
MILWAUKEE »
JANUARY 23 2018
PREPARING A WINNING GOVERNMENT PROPOSAL
MILWAUKEE »
JANUARY 23 2018
ACQUISITION HOUR: MARKET RESEARCH – USING THE FEDERAL PROCUREMENT DATA SYSTEMS (FPDS)
WEBINAR »
JANUARY 24 2018
ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS
WEBINAR »
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

Information Management for Federal Contractors

Marc N. Violante

Wisconsin Procurement Institute

March 13, 2018

Important reminder

Image copied from: https://www.nh.gov/nhsl/ww2/ww59prt.html


$13 BILLION LOST
PROTECT AMERICA'S TRADE SECRETS
WWW.FBI.GOV

COUNTERINTELLIGENCE

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

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

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."

Google™ Custom Search Search

SECURITYWEEK DAILY BRIEFING

BRIEFING

Business Email Address SUBSCRIBE

SECURITYWEEK

ICS CYBER SECURITY CONFERENCE

THE ORIGINAL

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

So, this isn't important!

1. Air Force orders freeze on public outreach

(Defense News) The Air Force is slashing access to media embeds, base visits and interviews as it seeks to put the entire public affairs apparatus through retraining — a move it says is necessary for operational security, but one which could lead to a broader freeze in how the service interacts with the public.

According to March 1 guidance obtained by Defense News, public affairs officials and commanders down to the wing level must go through new training on how to avoid divulging sensitive information before being allowed to interact with the press.

The effort, which represents the third major Defense Department entity to push out guidance restricting public communication over the past 18 months, creates a massive information bureaucracy in which even the most benign human-interest stories must be cleared at the four-star command level.

Early Bird Brief, Tuesday, March 13, 2018 & https://www.defensenews.com/breaking-news/2018/03/13/air-force-orders-freeze-on-public-outreach/?utm_source

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

Prologue: @War the Rise of the Military Internet Complex

Key threat

Google search: cell phone site:.gov Oklahoma State Bureau of Investigation - Digital Evidence Service

Pentagon & Congress

Trump pardons sailor convicted of taking illegal photos aboard submarine

By: Leo Shane III 3 days ago

https://www.navytimes.com/news/pentagon-congress/2018/03/09/trump-pardons-sailor-convicted-of-taking-illegal-photos-aboard-submarine/ Visited: March 12, 2018

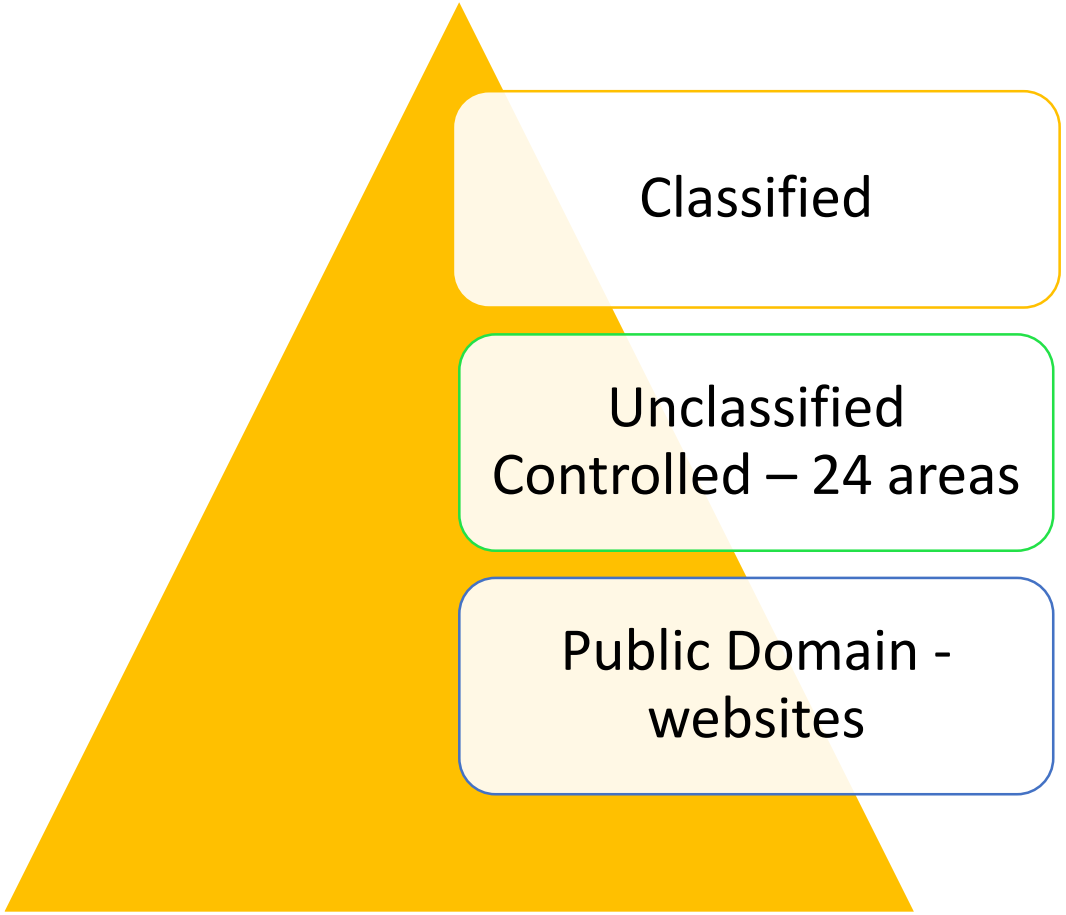
Information Security – formal definition

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

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

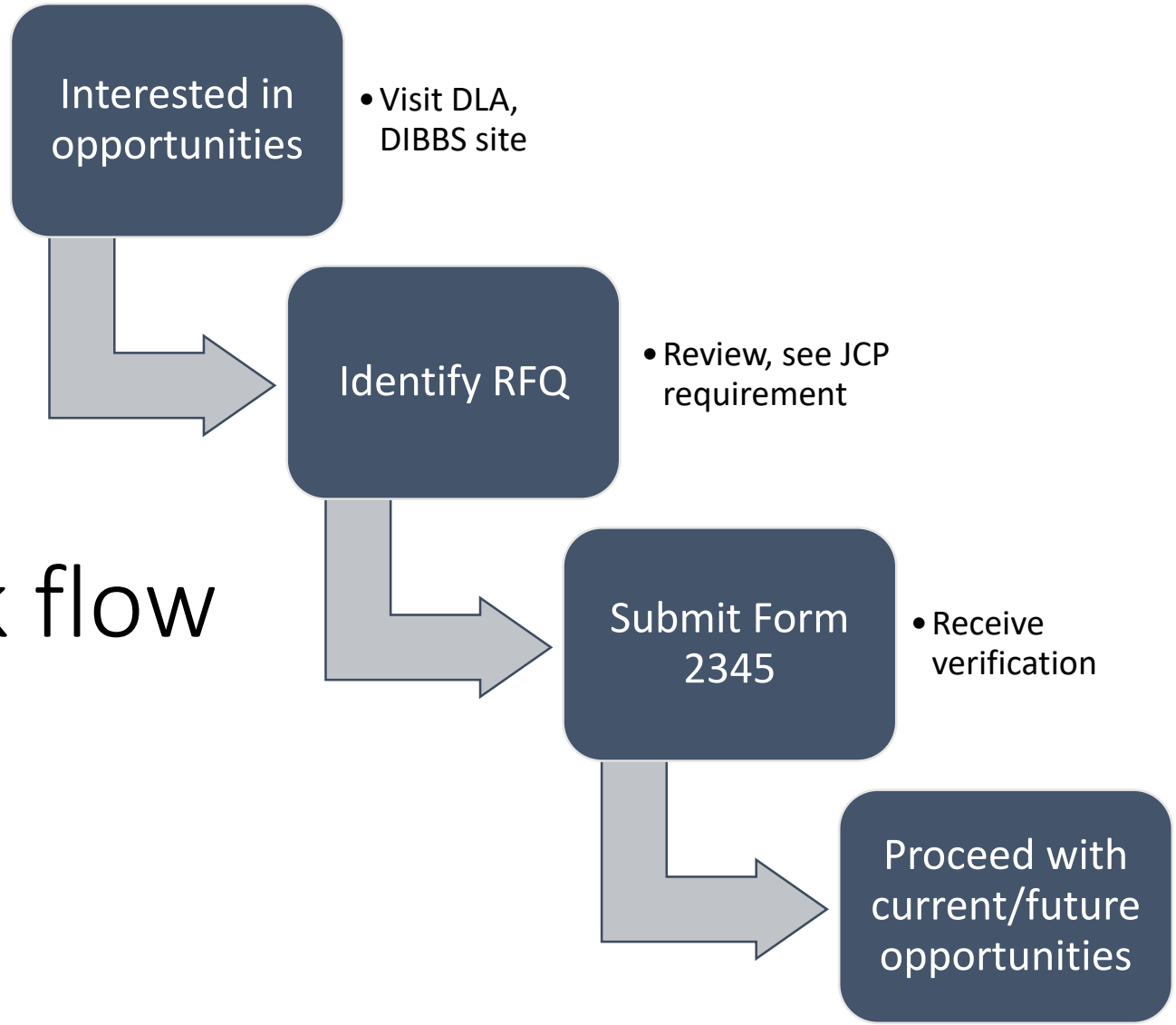
Identify the type and handling requirements

Step 1 -



3/13/2018

Typical work flow



US/Canada – Joint Certification Program

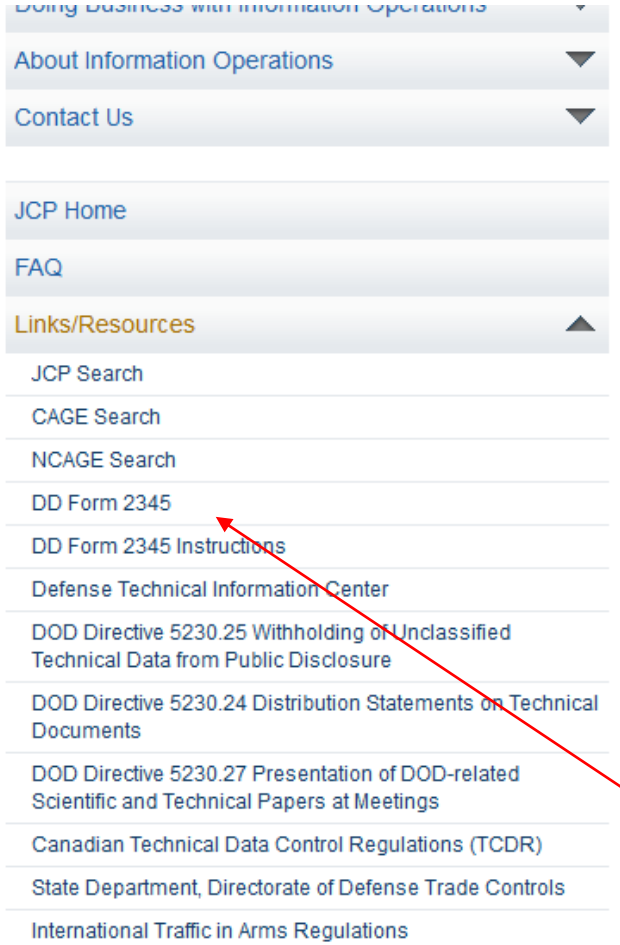
THIS ITEM HAS TECHNICAL DATA SOME OR ALL OF WHICH IS SUBJECT TO EXPORT-CONTROL REGULATIONS. DISTRIBUTION OF THE TECHNICAL DATA AND ELIGIBILITY FOR AWARD ARE LIMITED TO THOSE SUPPLIERS QUALIFIED THROUGH JCP CERTIFICATION, OR TO THOSE LICENSED BY EITHER THE DEPARTMENTS OF STATE OR COMMERCE; OR TO FOREIGN SUPPLIERS PURSUANT TO INTERNATIONAL AGREEMENTS.

TO APPLY FOR JCP CERTIFICATION, COMPLETE DD FORM 2345, MILITARY CRITICAL TECHNICAL DATA AGREEMENT, FORM IS AVAILABLE AT THE WORLD WIDE WEB ADDRESS:

https://public.logisticsinformationservice.dla.mil/PublicHome/jcp/default.aspx

DIBBS RFQ: 5330 01 121 8530 Seal, plain encased

US/Canada – Joint Certification Program



JCP Search

The JCP established in 1985 to allow United States (U.S.)/Canadian contractors to apply for access to Departm Defense/Department of National Defence (DOD/DND) unclassified export controlled technical data/critical techn equally favorable basis in accordance with DODI 5320.25 "Withholding of Unclassified Technical Data and Techn Public Disclosure", and Canadian Technical Data Control Regulations.

The JCO:

- is a jointly staffed office and the only DOD/DND agency that reviews and certifies the DD Form 2345.
- provides customer support to defense contractors applying for certification.
- receives, processes and maintains approximately 9,000 DD Form 2345s annually.
- establishes JCP policy based on DOD/DND Directives.
- consults and cooperates with government stakeholders in the development of common industrial security pol procedures and technology controls.
- partners with DOD legal counsel and federal law enforcement on debarment actions.

DD Form 2345 is used:

- for U.S./Canadian defense contractors to obtain DOD/DND unclassified export controlled technical data.
- to attend gatherings such as:

http://www.dla.mil/HQ/InformationOperations/Offers/Products/LogisticsApplications/JCP.aspx

US/Canada – Joint Certification Program

Focus

DD Form 2345 is used:

- for U.S./Canadian defense contractors to obtain DOD/DND unclassified export controlled technical data.
- to attend gatherings such as:
  - Symposiums
  - Program briefings
  - Meetings designed to publicize advance requirements of contracting agencies
  - Pre-solicitation, pre-bid, pre-proposal, pre-award conferences, workshops and tours
- to request unclassified visits directly with other certified U.S. or Canadian defense contractors or U.S. and Canadian military facilities.

http://www.dla.mil/HQ/InformationOperations/Offers/Products/LogisticsApplications/JCP.aspx

Details – Details - Details

JCP Search

The JCP established in 1985 to allow United States (U.S.)/Canadian contractors to apply for access to Department of Defense/Department of National Defence (DOD/DND) unclassified export controlled technical data/critical technology on an equally favorable basis in accordance with DODI 5320.25 "Withholding of Unclassified Technical Data and Technology from Public Disclosure", and Canadian Technical Data Control Regulations.

http://www.dla.mil/HQ/InformationOperations/Offers/Products/LogisticsApplications/JCP.aspx

What is often overlooked!

NUMBER 5230.25
November 6, 1984

Incorporating Change 1, August 18, 1995
USDR&E

SUBJECT: Withholding of Unclassified Technical Data From Public Disclosure

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

REFERENCES, continued

(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.

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

Distribution Statements

A. Approved for public release.

B. U.S. Government agencies only

C. U.S. Government agencies and their contractors

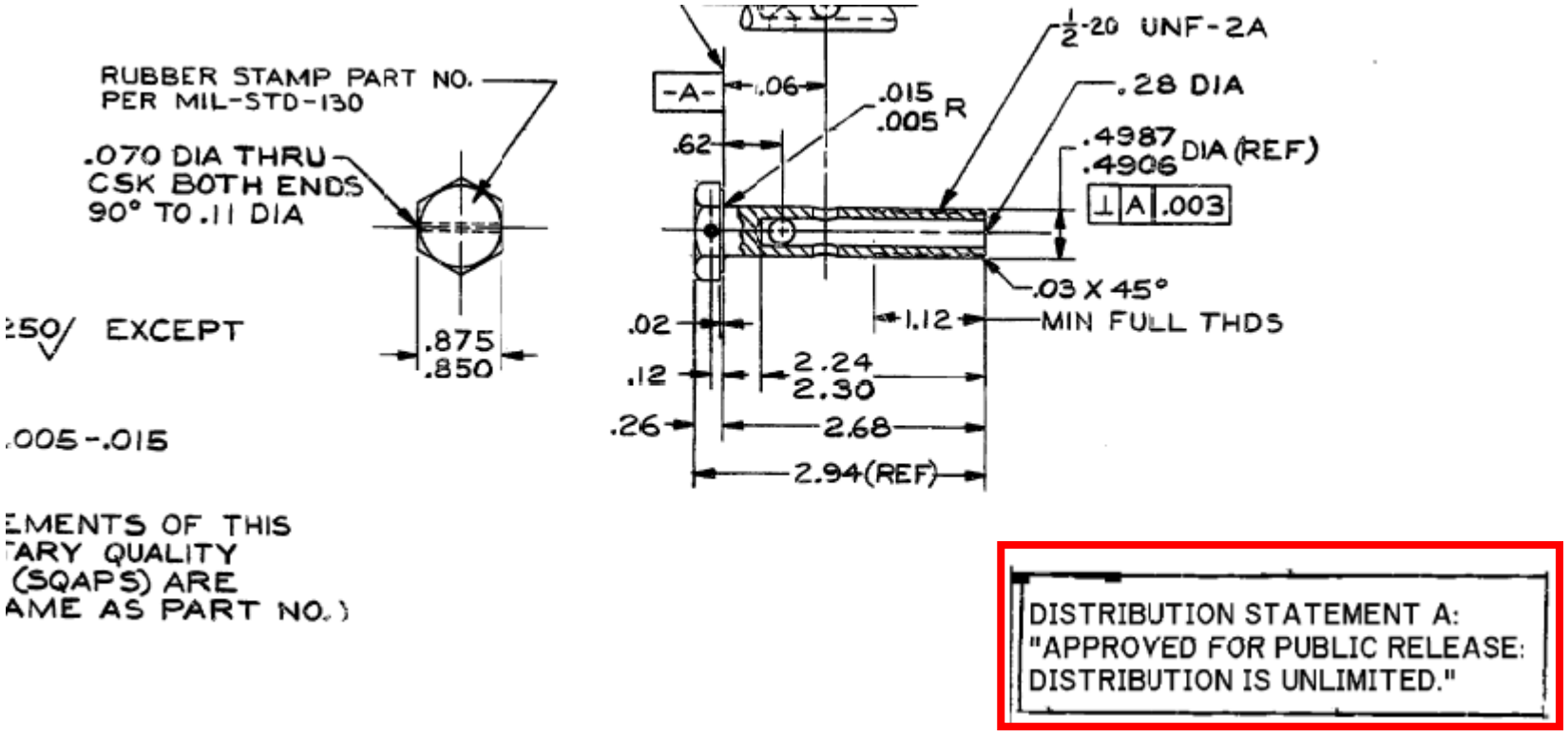
D. Department of Defense and U.S. DoD contractors only

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

“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—

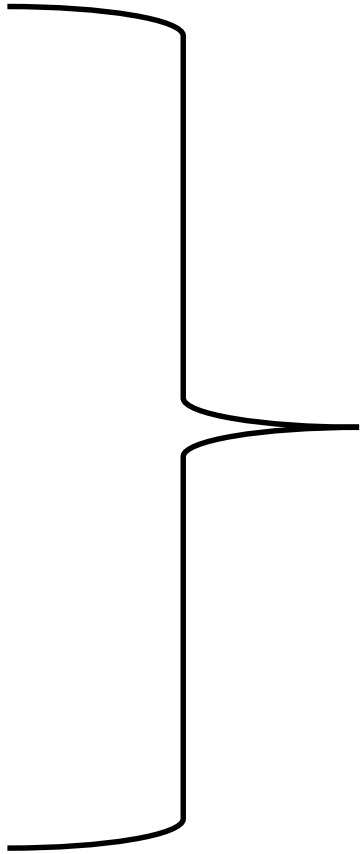
  (1) The Contracting Officer has given prior written approval;

  (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

Mediums

- Text
- Digital
- Audio
- Photographic
- Drawings
- Oral
- Patterns
- Mock-up
- End product



- Key programs
- FAR 52.204
- DFARS 252.204-7012
- ITAR
- EAR
- Other - CUI

ITAR – forgings, casting, unfinished products…

§120.6 Defense article.

Defense article means any item or technical data designated in §121.1 of this subchapter. The policy described in §120.3 is applicable to designations of additional items. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in §121.1 of this subchapter. It also includes forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles. It does not include basic marketing information on function or purpose or general system descriptions.

[79 FR 61227, Oct. 10, 2014]

https://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.1.13.57&rgn=div5#se22.1.120_110 visited: 12 March 2018

Broadly defined

§120.10 Technical data.

(a) *Technical data* means, for purposes of this subchapter:

(1) Information, other than software as defined in §120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;

https://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.57&rgn=div5#se22.1.120_110 visited: 12 March 2018

Broad extent of these ideas

§120.50 Release.

(a) Technical data is released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; or

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.

(b) [Reserved]

[81 FR 35616, June 3, 2016]

(b) Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

[81 FR 35616, June 3, 2016]

§127.1 Violations.

(a) Without first obtaining the required license or other written approval from the Directorate of Defense Trade Controls, it is unlawful:

(1) To export or attempt to export from the United States any defense article or technical data or to furnish or attempt to furnish any defense service for which a license or written approval is required by this subchapter;

Title 22 Chapter I Subchapter M visited: 12 March 2018 Part 120 – Definitions & 127.1 - visited March 18, 2018

3/13/2018

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.

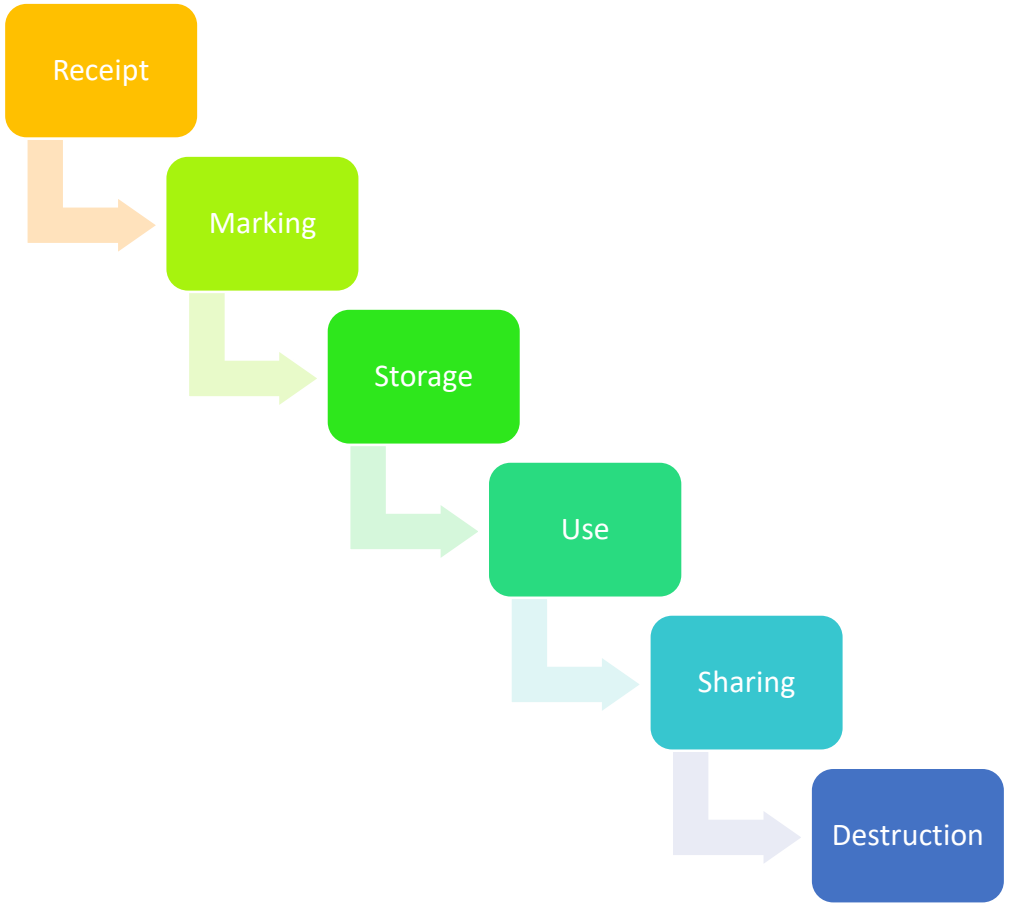
➢ Destruction of this technical data shall be accomplished by: shredding, pulping, burning, or melting any physical copies of the TDP and/or deletion or removal of downloaded TDP files from computer drives and electronic devices, and any copies of those files.

Okay – now prove it!

Identify and account for

- Handling requirements
- Marking requirements
- Sharing
- Storage
- Destruction

Information – life cycle, general elements

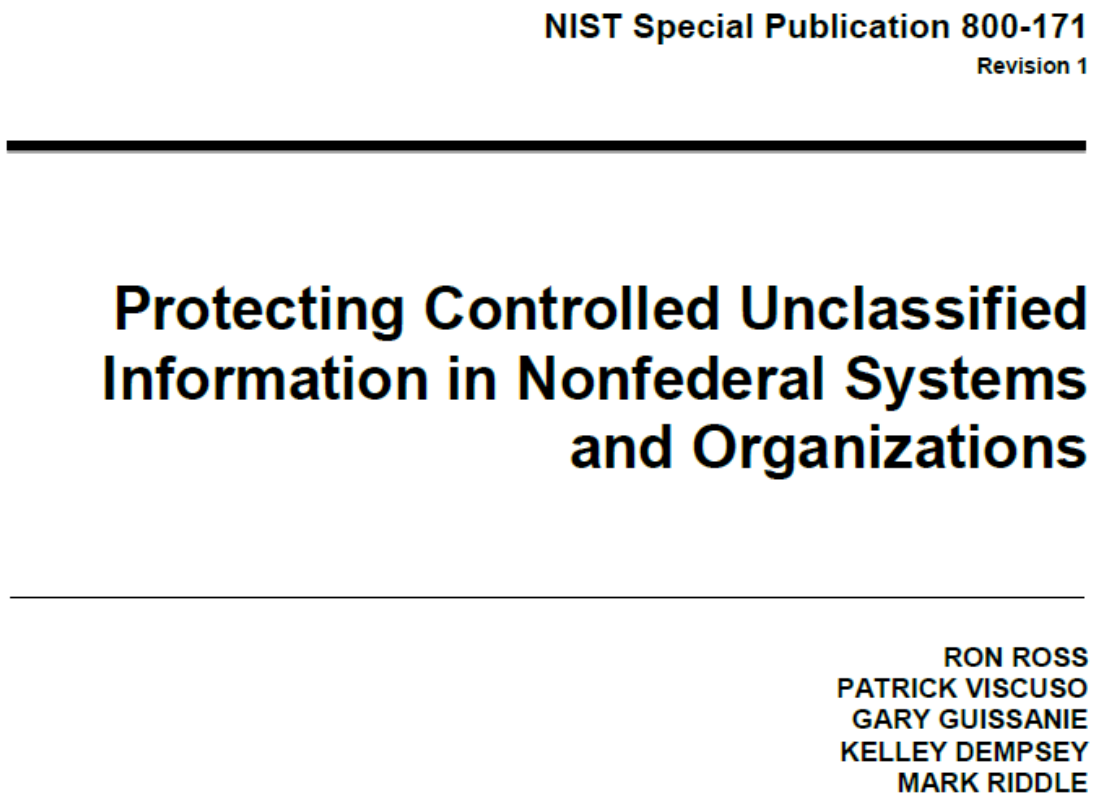


- Auditing
- Awareness
- Controls
- ★ Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- ★ Transmittal registry
- Update procedures

Information Resources / References

- Locate
- Identify
- Categorize
- Determine if labeling is needed
- Inform – information custodians, others
- Provide training
- Determine if there are any access limitations for suppliers – subcontractors, etc.

NIST (SP) 800-171 Revision 1



NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

NIST Document – cover page

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

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

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

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

FAR 52.204-21 visited: 12 March 2018

3/13/2018

Information Systems - defined

(6) the term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology;
(7) the term "information resources management" means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public;
(8) the term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;
(9) the term "information technology" has the meaning given that term in section 11101 of title 40 but does not include national security systems as defined in section 11103 of title 40;

44 U.S.C. 3502 visited Marc 12, 2018

Risks - Identify and Prioritize Information Types

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

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

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

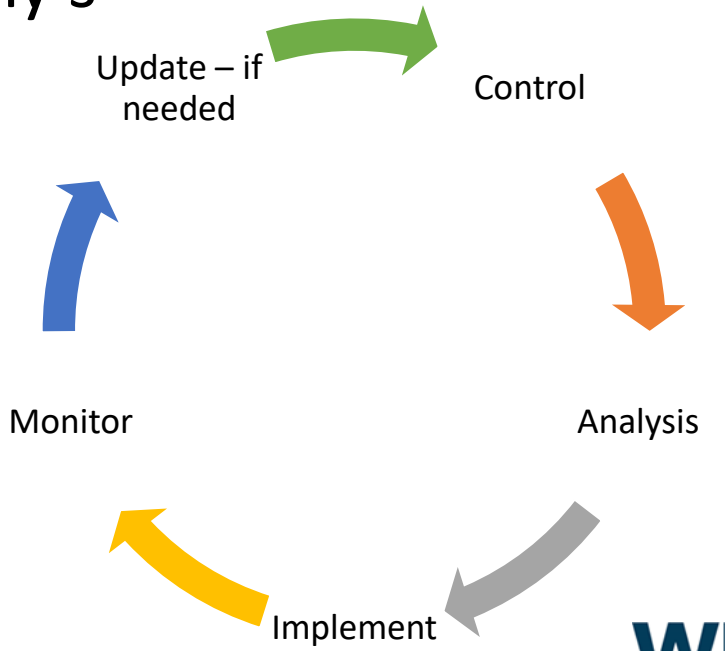
5 Questions CEOs Should Ask About Cyber Risks

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

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

Security Controls

Control categories: (examples)

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

By Stephen Northcutt
Version 1.2

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

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

NIST 800-30 r1 Guide for Conducting Risk Assessments, Chapter 1, page 1

Marking Media

Removable Hard drive

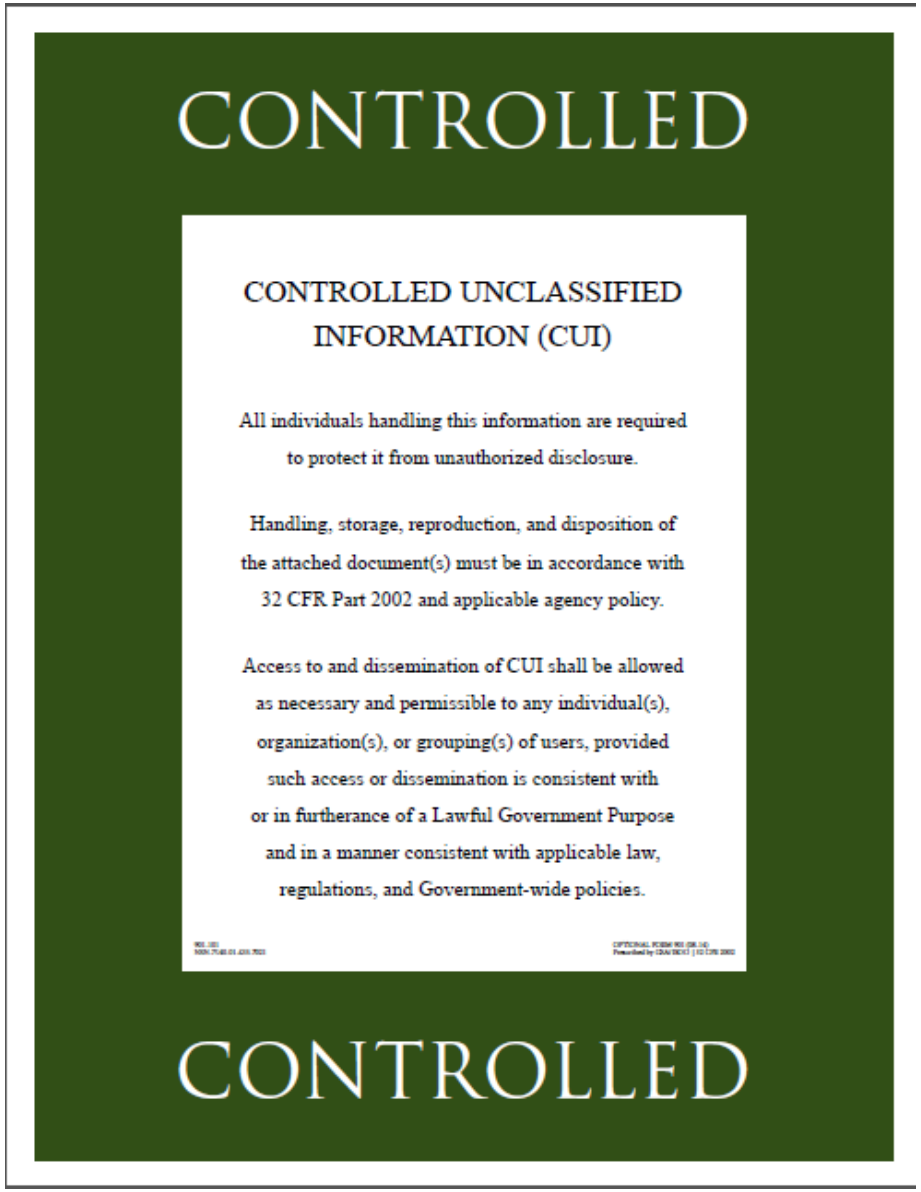
Equipment can be marked or labeled to indicate that CUI is stored on the device.

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

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

https://www.archives.gov/cui CUI Marking Handbook – pdf page 23

CUI Coversheets - example



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

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/

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!

Understand what is required

- One set of rules may not be adequate
- Understand the definitions
- Apply literal interpretation not figurative

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

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

Hid for two years!

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

What next?

- Actions to take
- Considerations
- Possible impacts
- Questions to ask

Identify information loss points

- Computers
- Visitors
- Vendors
- Deliveries
- Friends
- Windows
- Other
- Trash

Passive Information Gathering

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

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

Walk the route that data takes

- Receipt
- Intermediate points
- Shop floor
- Copies & external points
- Storage
- Destruction

Impact on supply chain and costs

- Suppliers may have also have to be compliant
- May impact production
- May impact transportation requirements
- May increase costs
- May create a need for greater planning and lead times
- What path are your emails taking?
  - What if the route uses a non-US router?
- Data storage – who has access?/who performs maintenance?

Contract management issues

- Flowdown clauses
- Managing access to information
  - Internally – staff and/or employees
  - On site – in the office
  - Offsite – home, conference, during travel
- Selection of subcontractors
- Print & document control, emails, copy services
- Copier hard drive
- IT systems and IT technical staff – in house / contract
- Visitor control

Employee considerations

- Access to information
  - Country of birth
  - If not U.S.
    - No access
    - Access requires TAA – country of birth, may require more than 1 TAA
  - Segregation of duties
  - Badge identification
  - Document control
  - Hiring policy – administration, briefing
  - Departure process

Gateway to new opportunities or barrier

- Many primes will only work with ITAR registered subcontractors
- Primes seek
  - Partners & problems solvers
  - Companies that help to manage and reduce risk
  - Strengthen and support the overall effort
- For example - ITAR registration
  - Indicates
    - Awareness of program
    - Establishment of procedures
    - Ability to maintain control over information

Program elements

- Organization Structure
- Corporate Commitment and Policy
- Identification, Receipt and Tracking of Items/Tech Data
- Identify Restricted/Prohibited Exports and Transfers
- Recordkeeping
- Internal Monitoring
- Training 
- Violations and Penalties

Information handling requirements

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

Process

- Identification – checklist
- Document – marking
- Internal handling procedures
- Copy – log
- Subcontractor/supplier vetting-agreement – training
- Formal distribution notice, detail requirements, signature
- Audit

Internal procedures

- Color code
- File cabinets
- Access list
- Storage – not in use
- Destruction of working copies
- Corporate records
- Formal document destruction – special handling

Document Control

- Paper
- Digital
- Transmission
- Network
- Email
- Encryption
- Portal
- Copiers/Fax

Personnel

- Are employees provided information management training?
- Are employees screened prior to granting access to information?
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?
- Is access managed as the need changes?
- Are there work from home procedures/training?
- How is staff change managed?

Office procedures - IT

- Who has access to your network – facilities – offices – other areas?
- 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?

Business Relationships

- Do you openly share information/files with suppliers?
- Do you verify that your suppliers can have access to information that you plan to share?
- Are you aware of the different regulations governing protection of data?
- Have you read and researched the regulations that apply to governing data and unclassified information?
- Do you pass down these requirements to your subcontractors/suppliers?

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- 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 Laws** – CLICK HERE for additional information – presented by Corey Walton – 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)

ACQUISITION HOUR LIVE WEBINAR SERIES

- April 3, 2018 – **Contract Closeouts: Preparing for a Smooth Ending** – CLICK HERE for additional information – presented by Mark Dennis– Consultant – La Crosse River Consulting
- April 4, 2018 – **Export Controls – ITAR and Associated Requirements** – CLICK HERE for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)
- April 17, 2018 – **eSRS Individual Subcontractor Reporting (ISR) Basics** – CLICK HERE for additional information – presented by Kim Garber – Wisconsin Procurement Institute (WPI)
- April 25, 2018 – **Learning About Surety Bond Guarantee From the U.S SBA** – CLICK HERE for additional information – presented by Tamara Murray – U.S Small Business Administration, Office of Surety Guarantees
- May 8, 2018 – **How to Quickly Analyze Solicitations** – CLICK HERE for additional information – presented by Carol Murphy– Wisconsin Procurement Institute (WPI)

UPCOMING EVENTS

Federal Acquisition Regulations (FAR) Review – Tuesday Evenings – Webinar

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