Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

INFORMATION MANAGEMENT AND SECURITY FOR FEDERAL CONTRACTORS

(CYBER SECURITY SERIES PART 1 OF 5)

ACQUISITION HOUR WEBINAR

September 24, 2019




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

Celebrating 31 Years of serving Wisconsin Business!

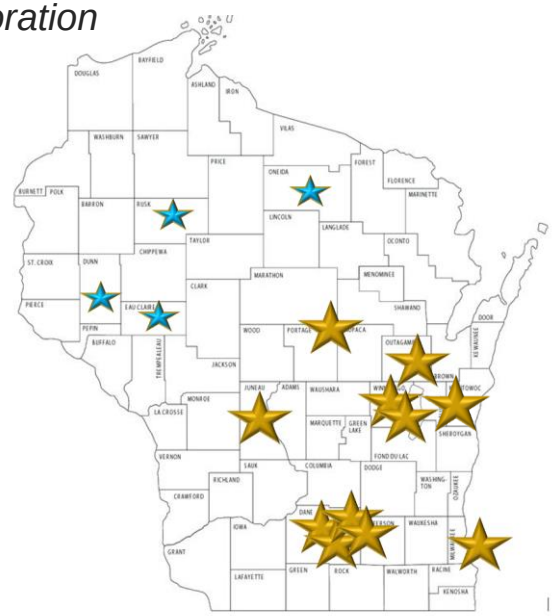
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **GREEN BAY**
  - *Advance Business & Manufacturing Center*



WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
WED 21
Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
THU 22
Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
THU 22
NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
SEP 11
Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm
View More...
CURRENT OPPORTUNITIES (1)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

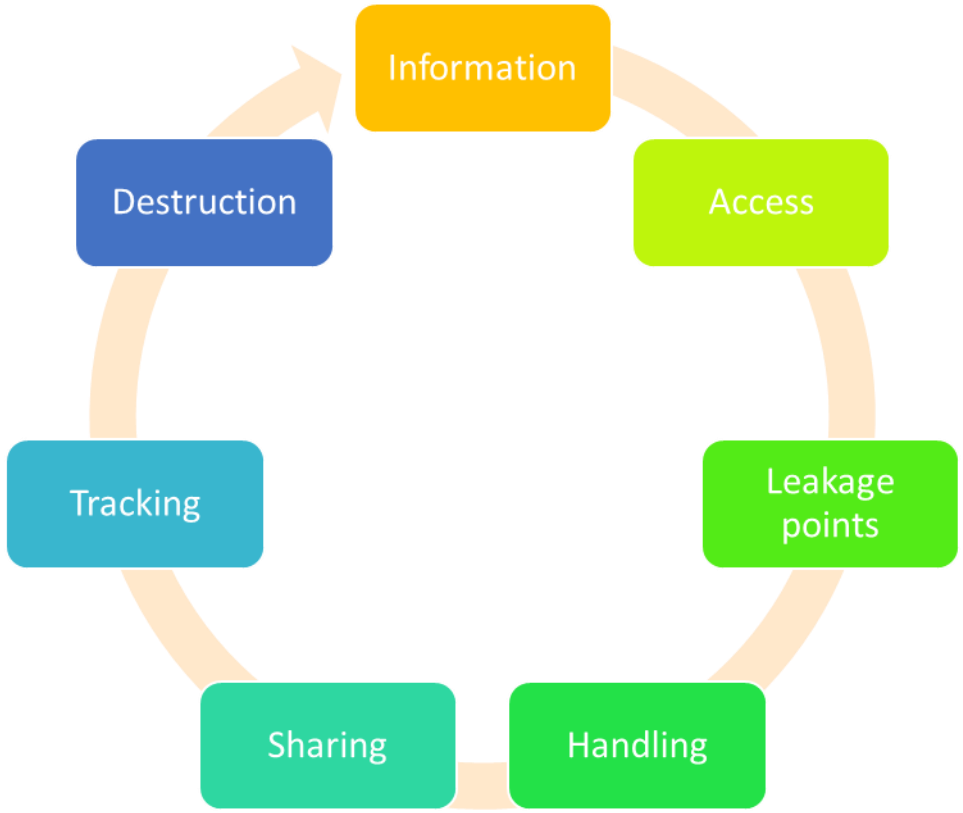
WHAT WPI DOES

Provides technical assistance to CURRENT and POTENTIAL Contractors and subcontractors

- INDIVIDUAL CONSELING – At our offices, at clients facility or via telephone/GoToMeeting
- SMALL GROUP TRAINING – Workshops and webinars
- CONFERENCES to include one on one or roundtable sessions

Last year WPI provided training at over 100 events, provided service to over 1,000 companies

Information Management Considerations for Federal Contracting



Marc N. Violante

Wisconsin Procurement Institute

September 24, 2019

Probably not the intended approach

Awareness is key – active efforts/processes

Attention to details!

Example – Integrated requirements (slide 1 of 3)

- **59 - Single Channel Ground & Radio System (1) – FBO Item**
- These items are the components of Interconnecting Group ON-373B/GRC; end system Single Channel Ground and Airborne Radio System (SINCGARS).
- The Government owns the technical data package (TDP) for the items. The TDPs will include drawings and Gerber files. The TDPs are subject to ITAR; refer to statement below.
- NOTE: The TDPs will NOT be released at this time.
- INTERNATIONAL TRAFFIC IN ARMS REGULATIONS
- The technical data package (TDP) for this item is subject to the International Traffic in Arms Regulations (ITAR). All technical documents for SINCGARS include but not limited to, test plans, test reports, drawings and specifications contains information that is subject to the controls defined in the International Traffic in Arms Regulation (ITAR). This information shall not be provided to non- U.S. persons or transferred by any means to any location outside the United States Department of State.

https://www.fbo.gov/notices/0e1d8fa0af22781f98263ce131214688 - posted February 25, 2019

Integrated example (slide 2 of 3)

- A company wishing to receive the TDPs must have an active status in the Defense Logistics Agency Joint Certification Program (JCP).
- Once your company has been verified to have active status in JCP, we will upload the TDPs will be uploaded into AMRDEC Safe Access File Exchange (SAFE). You will then receive an e-mail from the AMRDEC SAFE site, https://safe/amrdec.army.mil/safe/, with a link to the package ID and a password.
- The TDPs may contain drawings in C4 format. Software to view C4 drawings is available for download through

https://www.fbo.gov/notices/0e1d8fa0af22781f98263ce131214688 - posted February 25, 2019

Integrated example (slide 3 of 3)

- COVERED DEFENSE INFORMATION (CDI)

Note regarding DFARS 252.204-7008 and DFARS 252.204-7012: The Government not including or identifying CDI at this time does not constitute a lack of CDI for this solicitation/award

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS JUN/2016

(a) Definitions. As used in this clause-

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

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

One solicitation – ITAR – JCP – CDI (252.204-7012) & FAR 52.204-21

Mother may I? - 252.204-7000 Disclosure of Information

- (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

As prescribed in 204.404-70(a), use the following clause: DISCLOSURE OF INFORMATION (AUG 2013)

Joint Certification Program - requirements

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

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.

Further dissemination of JCP Technical Data

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

Solicitation instructions to access TDP

- a. Log on to the FBO web site.
- b. Enter your Marketing Partner Identification Number (MPIN).
- c. Search for the solicitation number.
- d. If solicitation is Export Controlled, select Verify MPIN.

Detailed language

- (1) TDPs that have an Export Control Warning Notice are subject to the Arms Export Control Act (Title 22, U.S.C.,
- Sec 2751, et.seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C, App. 2401 et. seq..
- (2) Further dissemination must be in accordance with provisions of DoD Directive 5230.25. This also applies to distribution of the TDP to all SUBCONTRACTORS at every level.

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!

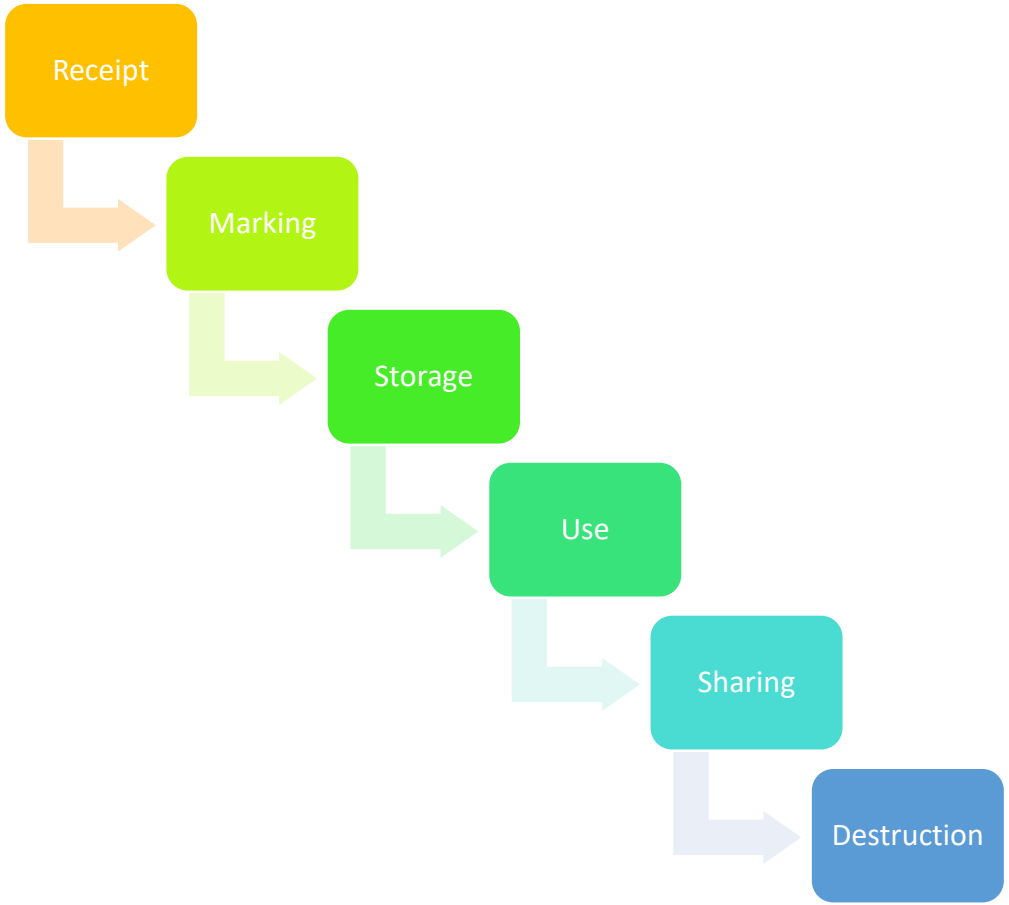
Requirements for multiple individuals

- 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 https://www.fbo.gov/index The FBO helpdesk phone number is
- (866) 606-8220. Vendors are responsible for placing correct information in FBO.
- g. 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.

Other contract criteria

- h. A user guide for FBO can be found at https://http://www.fbo.gov - on the right is User Guides - click on Vendor.
- [ ] 4. The Government requires a Use and Non-Disclosure Agreement (NDA) to be signed by an authorized representative of your firm before you are granted access to the technical data.
- The appropriate Agreement is:
- [ ] available at http://contracting.tacom.army.mil/acqinfo/contractorforms.htm
- titled: N/A
- [ ] available as an attachment to this solicitation.

Information – life cycle, general elements



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

The W's of Information

- What information is being shared?
- What are the handling requirements?
- Who should have access?
- With whom is information being shared?
- Where – how is the information being shared?
- When – normal hours / off hours
- Why is it being shared?
- Others "W's"

Key Elements

Federal Programs - partial

- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR) – Export Control
- Joint Certification Regulation (JCP)
- Joint Certification Regulation – Enhance; specific NSN's
- Distribution Statement
- CDI/CTI/CUI > CUI Basic req & CUI Specified (e.g. DFARS)
- Other ? – must be on the "look out for hints"
- DFAR Clauses
- Contract/Flow Down Clauses

Controlled Unclassified Information (CUI)

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- North Atlantic Treaty Organization (NATO)
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation

https://www.archives.gov/cui/registry/category-list

Establish and Maintain a Compliance Program

Program elements:

- Fully supported by senior management
- Regularly reviewed/updated
- Research & apply references
- Clearly documented in writing
- Tailored to the business
- Tailored to information being handled
- Training (periodic/as needed) conducted; documented
- Outward looking component – feedback, current external issues

Why? – Why, create a formal document with such details?

- Question – if there is a fire in your kitchen do you want the fire extinguisher readily available and operational? Or do you want to go in search of it?
- Trust memory? Trust instincts? Or utilize company resource manual?
- Documented program
  - Requires research, thought and addressing relevant issues/topics
  - Tailored
  - Proof of effort in working to comply
  - Process may uncover issues
  - Outcome is a working, desk guide, a *handy everyday reference to use and consult*

Create/manage information census

- Identify –
  - Information held
  - Responsible individual
  - Location
  - Program
  - Storage requirements
  - Marking requirements
  - Sharing restrictions
  - Destruction requirements
  - Update records as needed

Key management/security requirements

- Solicitation Review
- Identification of data/information requirements
- Identify team members
- Advise of requirements
- Create limited access space
- Control access, information and time (functional, specified, unlimited)
- Detail requirements – sharing, copying, transmission

Information management considerations

- ITAR – Definition: Defense Article
- 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.

22 CFR §120.6 Defense article.

Understand definitions/program requirements

- **§120.17 Export.**
- (a) Except as set forth in §126.16 or §126.17, export means:
- (1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;
- (2) Releasing or otherwise transferring technical data to a foreign person in the United States (a “deemed export”);
- (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.

ITAR – Release - **§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]

ITAR §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.

DoDD 5230.25 re: JCP Change 2, 10/15/2018

- 3.2.1. The individual who will act as recipient of the export-controlled technical data on behalf of the U.S. contractor is a U.S. citizen or a person admitted lawfully into the United States for permanent residence and is located in the United States.
- 3.2.3. The U.S. contractor acknowledges its responsibilities under U.S. export control laws and regulations
- 3.2.4. The U.S. contractor also agrees that, unless dissemination is permitted by paragraph 5.8., below, it will not provide access to export-controlled technical data subject to this Directive to persons other than its employees or persons acting on its behalf, without the permission of the DoD Component that provided the technical data.

Portions copied

DoDD 5230.25 re: JCP - Change 2, 10/15/2018

- 4.2. Because public disclosure of technical data subject to this Directive is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest. Unclassified technical data that are not governed by this Directive, unless otherwise restricted, shall continue to be made available to the public as well as to State and local governments.

DFARS 252.204-7012 – top level requirements

- Adequate Security
- Identify – report Malware
- Monitor for “breaches”
- Investigate – comply with applicable laws (wire tapping, etc)
- Freeze “create image” hold for up to 90 days
- Report to DIBNET if needed – Medium Assurance Certificate required

The importance of a *Signature* *re:252.204-7008*

- (b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

- (c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—

  - (1) ***By submission of this offer,*** the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

The importance of a *Signature* - continued

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.

More later

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

Flexibility, tracking, communications

9. COVERED DEFENSE INFORMATION (CDI)

- Note regarding DFARS 252.204-7008 and DFARS 252.204-7012: The Government not including or identifying CDI at this time does not constitute a lack of CDI for this solicitation/award.

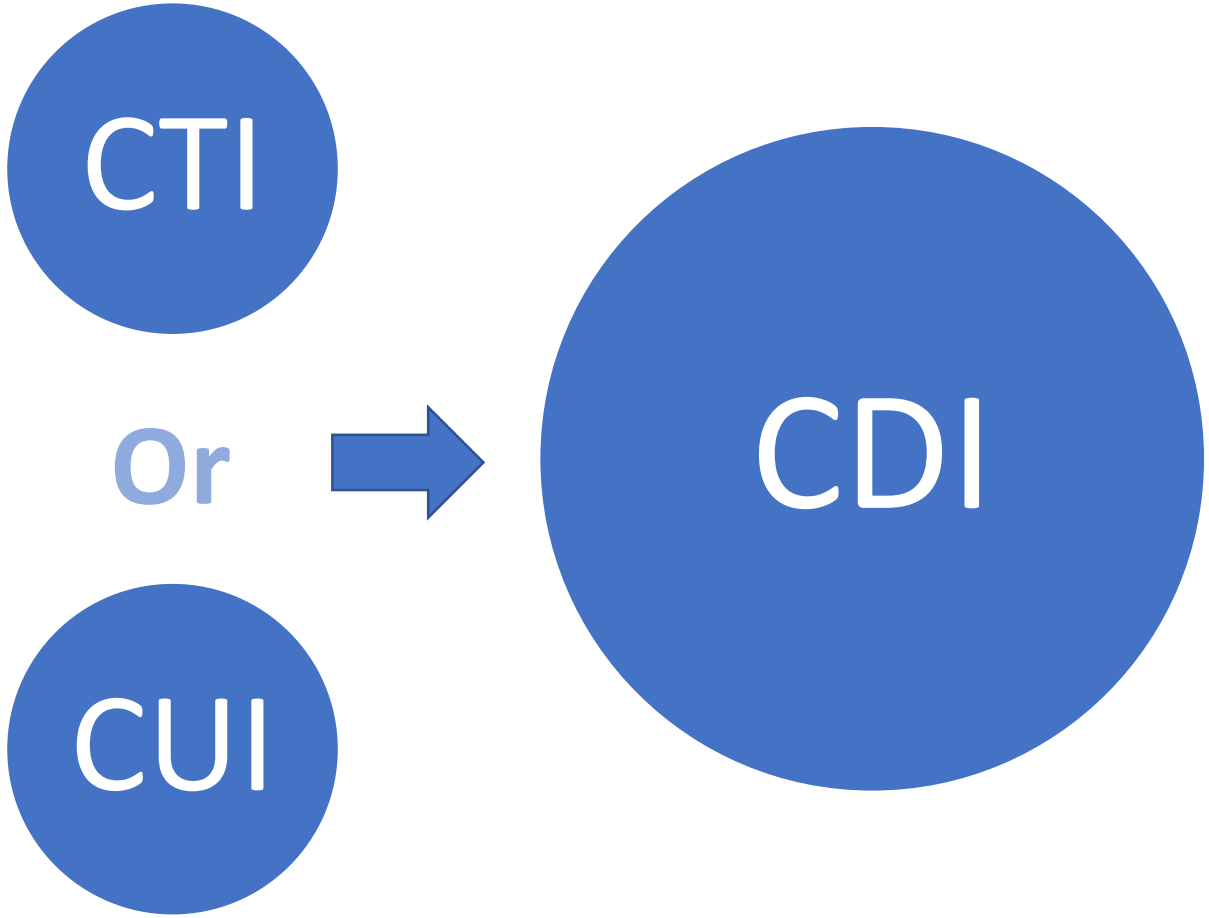
"Covered defense information" means unclassified **controlled technical information** or other information, as described in the **Controlled Unclassified Information** (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Solicitation: SPRBL1-19-R-0015 page 3 of 54 paragraph 9

Covered Defense Information



“Controlled technical information”

- means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

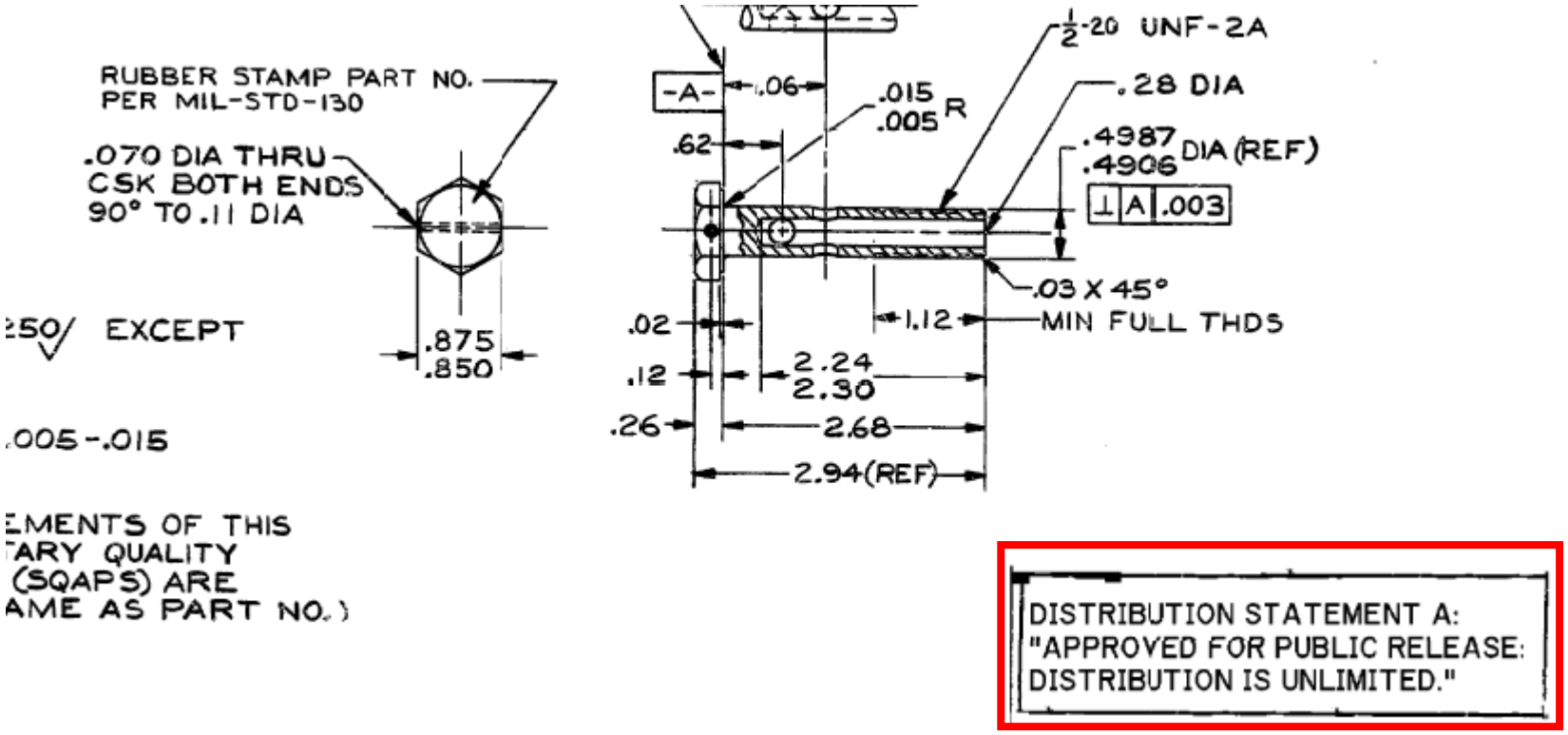
Definition in 252.204-7012

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

Distribution Statement – selection criteria

1. Criteria specified in Enclosure 3 of Reference (l).
2. Export controls in accordance with Reference (d); parts 120-130 of title 22, Code of Federal Regulations (CFR) (also known and hereinafter referred to as the "International Traffic in Arms Regulations" (ITAR)) (Reference (q)); and parts 730-774 of title 15, CFR (also known and hereinafter referred to as the "Export Administration Regulations" (EAR)) (Reference (r)).
3. Intellectual property and data rights licenses for contract deliverables in subpart 227.71 of title 48, CFR (Reference (s)).
4. CPI protection in accordance with Reference (p) Critical Program Information

DoDI 5230.24, August 23, 2012, Enclosure 3 pages 10 & 11 – references Enclosure 1

Reference – DD Form 2345 - JCP

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

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987 (hereby cancelled)
(b) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005
(c) Sections 133 and 2371 of title 10, United States Code (as amended)
(d) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(e) DoD Directive 3200.12, "DoD Scientific and Technical Information (STI) Program (STIP)," February 11, 1998
(f) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
(g) DoD Directive 2140.2, "Recoupment of Nonrecurring Costs (NCs) on Sales of U.S. Items," January 13, 1993
(h) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(i) DoD Directive 5143.01, "Under Secretary of D
November 23, 2005
(j) DoD Instruction 5200.01, "DoD Information S
Compartmented Information," October 9, 2008
(k) DoD Directive 5230.09, "Clearance of DoD In
August 22, 2008
(l) DoD Instruction 5230.29, "Security and Policy
Release," January 8, 2009
(m) DoD Manual 5200.01-V2, "DoD Information S
Information," February 24, 2012
(n) DoD Manual 5200.01-V1, "DoD Information S
and Declassification," February 24, 2012
(o) DoD Instruction 3200.14, "Principles and Oper
and Technical Information Program," May 13,
(p) DoD Instruction 5200.39, "Critical Program In
Department of Defense," July 16, 2008
(q) Parts 120-130 of title 22, Code of Federal Regu
Traffic in Arms Regulations")
(r) Parts 730-774 of title 15, Code of Federal Regu
Administration Regulations")
(s) Subparts 203, 227 and 252 of title 48, Code of Federal Regulations
(t) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
(u) Subpart 800.209 of title 31, Code of Federal Regulations
(v) Chapter 15 of title 50, United States Code
(w) Executive Order 13526, "Classified National Security Information," December 29, 2009
(x) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012

(y) Section 205 of title 35, United States Code
(z) Public Law 104–294, "Economic Espionage Act of 1996," October 11, 1996
(aa) Section 1498(a) of title 28, United States Code, as amended
(ab) Title 17, United States Code, as amended
(ac) Section 1905 of title 18, United States Code, as amended
(ad) Sections 638 and 3710a of title 15, United States Code, as amended
(ae) Part 311.8 of title 32, Code of Federal Regulations
(af) Public Law 107-296, "Homeland Security Act of 2002," November 25, 2002
(ag) Sections 2751 and 2778(j)(4)(A) of title 22, United States Code
(ah) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
(ai) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

Department of Defense

INSTRUCTION

NUMBER 5230.24
August 23, 2012

USD(AT&L)

SUBJECT: Distribution Statements on Technical Documents

References: See Enclosure 1

Process

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

Information

- Review information (prints, TDP, other)
- Determine
  - Program affiliation – ITAR, JCP, EAR, CUI, CUI – program, other
  - Marking
  - Handling – restrictions/limitations
  - Determine Control requirements – common, specific
  - Decontrol
  - Destruction requirements
  - Contract retention requirements

Internal procedures

- Color code
- File cabinets – meets specification
- Access list – who, why, for how long?
- Storage – not in use
- Destruction of working copies
- Formal document destruction – special handling
- Corporate records

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; documented?

Document Control

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

Personnel

- Are employees provided any IT training?
- Are employees screened prior to granting access to the IT system?
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?
- Is access managed as the need changes?
- Are there work from home procedures/training?
- Employee reporting of issues – malware, virus, ransomware
- How is staff change managed?

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?

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?

Visitors

- Sales/marketing
- Temporary employees
- Visiting engineer
- Customer
- Prospective customers
- Contract Services – repair, janitorial, suppliers, OEM, other
- Friends/family
- Others

Network

- Network
  - Determine everything that connects to it
    - Internally
    - Externally
    - Visitor
    - Operations – equipment
- Production equipment
  - Networked
  - Remote access – production/troubleshooting/periodic reporting

How do you know?

- - only authorized users have access to controlled information?
- - information requiring destruction was destroyed appropriately?
- - email/ftp/other digital communications were handled correctly?
- - there is no malware on the network / computers / devices?
- - there have been no reportable incidents?
- - all other issues

Lines of defense

- Corporate philosophy – protect the core
- Staff – trained, aware, involved
- Points of Contact – accessible, knowledgeable and proactive
- Communications – two way
- Network baseline – what is normal, inventory
- Devices – inventoried, baselined, updates installed
- Reporting mechanisms – necessary, encouraged, emphasized, active
- Device logging – tailored, used, automated
- Copies/Destruction – approved devices, procedures

Communication channels

- Location – work station, conference room, public area
- Network
- Hardwire – USB
- CD
- Removable drive
- Thumb drive
- WiFi – footprint
- Remote access

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

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

- September 25, 2019

  Introduction to Certifications Available to Minority Owned Businesses
  CLICK HERE for additional information – presented by Benjamin Blanc, Wisconsin Procurement Institute (WPI)

- October 15, 2019

  Export Controls – ITAR and Associated Requirements
  CLICK HERE for additional information – presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- October 16, 2019

  Integrating DFARS Requirements Into Your Day-to-Day Cyber Practices
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- October 30, 2019

  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 WEBINARS SERIES

- November 5, 2019

  Services Contracts with Federal Agencies
  CLICK HERE for additional information
  Presented by Carol Murphy, Wisconsin Procurement Institute (WPI)

- November 6, 2019

  Key Ideas Associated with CUI Requirements and DFARS 232.204-7012
  CLICK HERE for additional information – presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- November 19, 2019

  The Future of SAM.gov
  CLICK HERE for additional information – presented by Kim Garber, Wisconsin Procurement Institute (WPI)

- December 10, 2019

  Cyber Trends, Threats and the Evolving Hacker's Marketplace
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

MARKETPLACE WISCONSIN

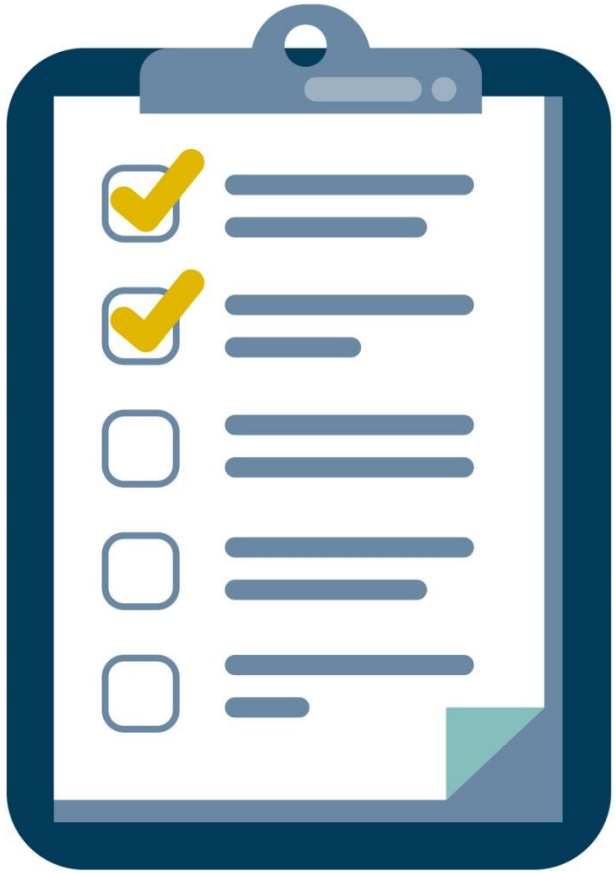
Governor's Conference on Diverse Business Development

OCTOBER 23-24, 2019
POTAWATOMI HOTEL & CONFERENCE CENTER
MILWAUKEE

www.marketplacewisconsin.com

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 | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226