Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

DoD Supplier Roadmap Series

Information Types and Handling Procedures

November 10, 2022




Webinar Etiquette

PLEASE

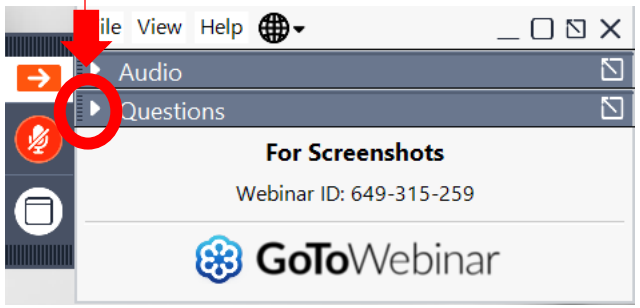
- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

QUESTIONS?

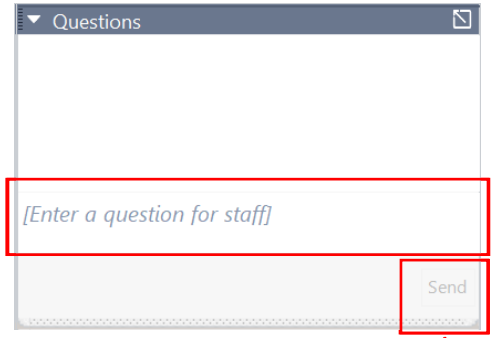
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

ABOUT WPI
Supporting the mission

Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's 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 and provided service to over 1,200 companies

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Department of Defense (DOD), WEDC and other funding sources.

Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

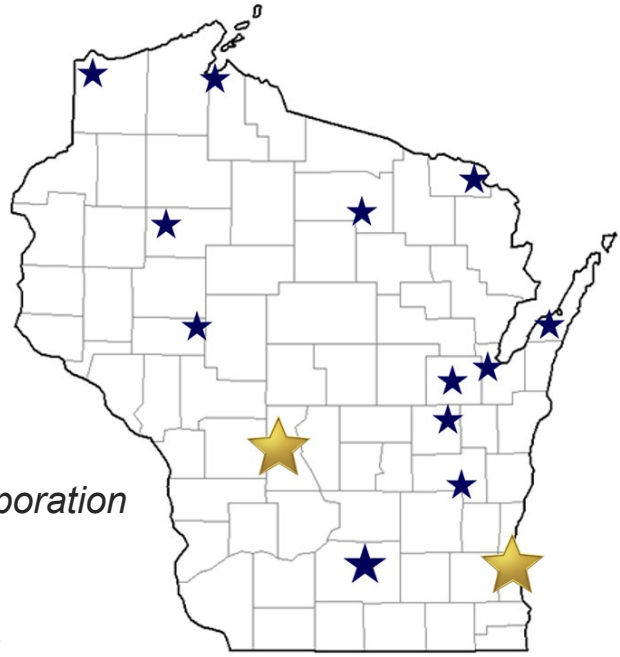
Sign-up for our Newsletter

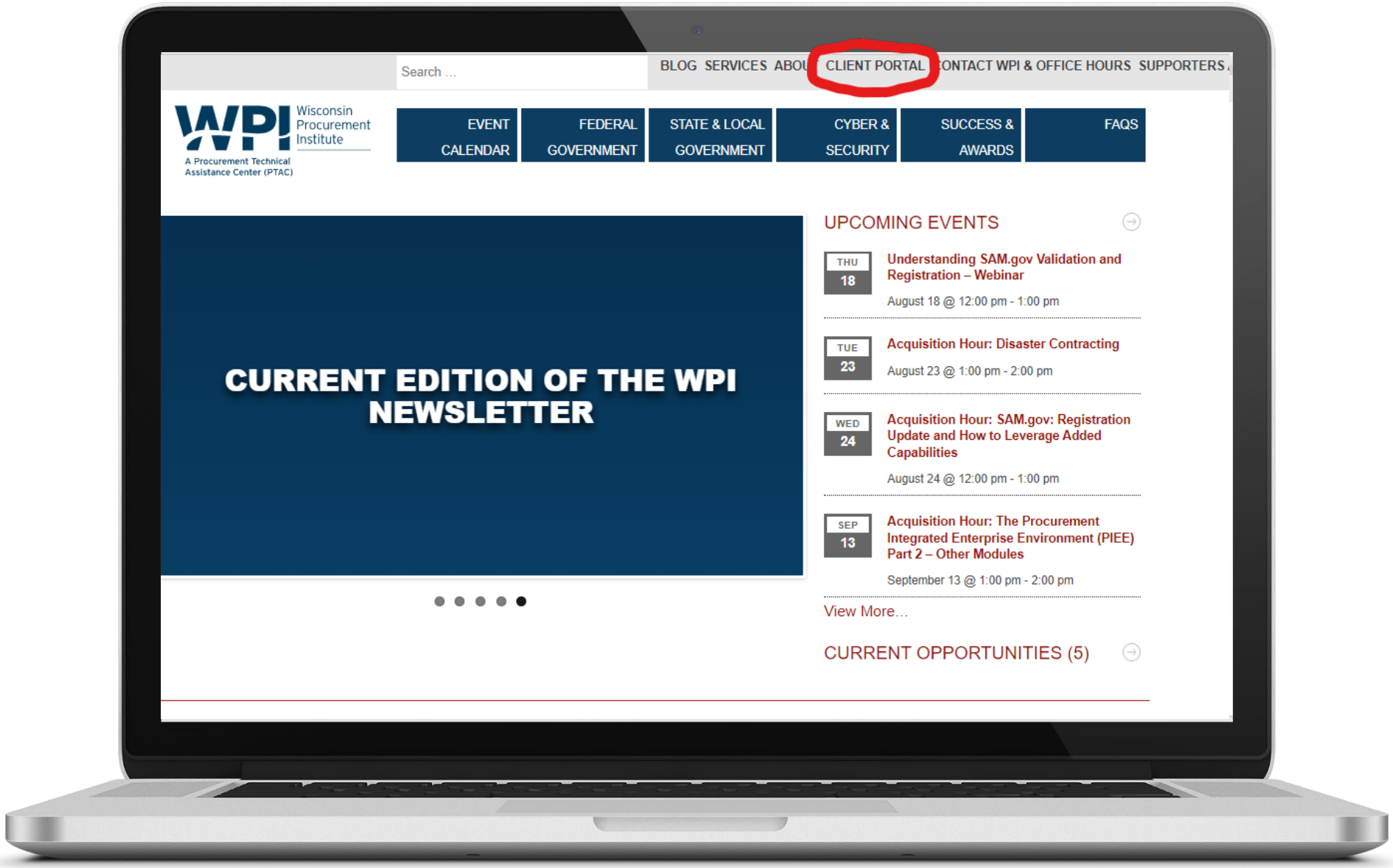
Stay up-to-date with the latest WPI news and events.

https://www.wispro.org/newsletter-signup/

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)*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **APPLETON**
  - *Fox Valley Technical College*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **FLORENCE**
  - *Florence County Economic Development*
- **DOOR COUNTY**
  - *NE WI Technical College*
  - *Door County Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

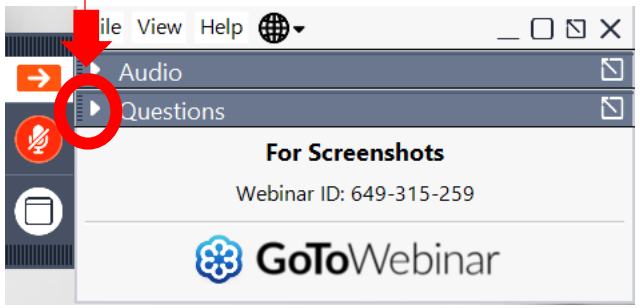



Search ...
BLOG SERVICES ABOU CLIENT PORTAL ONTACT WPI & OFFICE HOURS SUPPORTERS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
THU 18
Understanding SAM.gov Validation and Registration – Webinar
August 18 @ 12:00 pm - 1:00 pm
TUE 23
Acquisition Hour: Disaster Contracting
August 23 @ 1:00 pm - 2:00 pm
WED 24
Acquisition Hour: SAM.gov: Registration Update and How to Leverage Added Capabilities
August 24 @ 12:00 pm - 1:00 pm
SEP 13
Acquisition Hour: The Procurement Integrated Enterprise Environment (PIEE) Part 2 – Other Modules
September 13 @ 1:00 pm - 2:00 pm
View More...
CURRENT OPPORTUNITIES (5)

QUESTIONS?

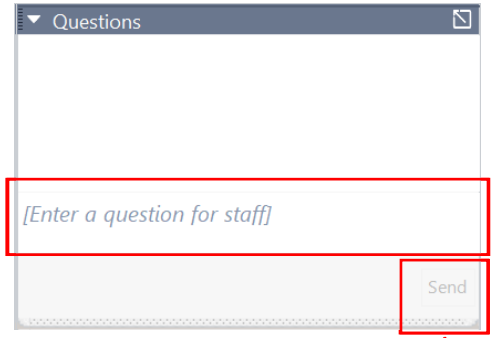
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

Information types and handling procedures

Marc N. Violante

Wisconsin Procurement Institute

November 10, 2022

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

Webinar Description

- Information handling procedures for DoD contractors can encompasses ITAR requirements, the Joint Certification Program (JCP), Controlled Unclassified Information (CUI), and DIBBS C Folders. This session will share how to determine if these requirements apply and an overview of the application and compliance process. During this session, we will also share advice on how to prepare and implement processes to support continued confidence in your information handling procedures.

Awareness is key

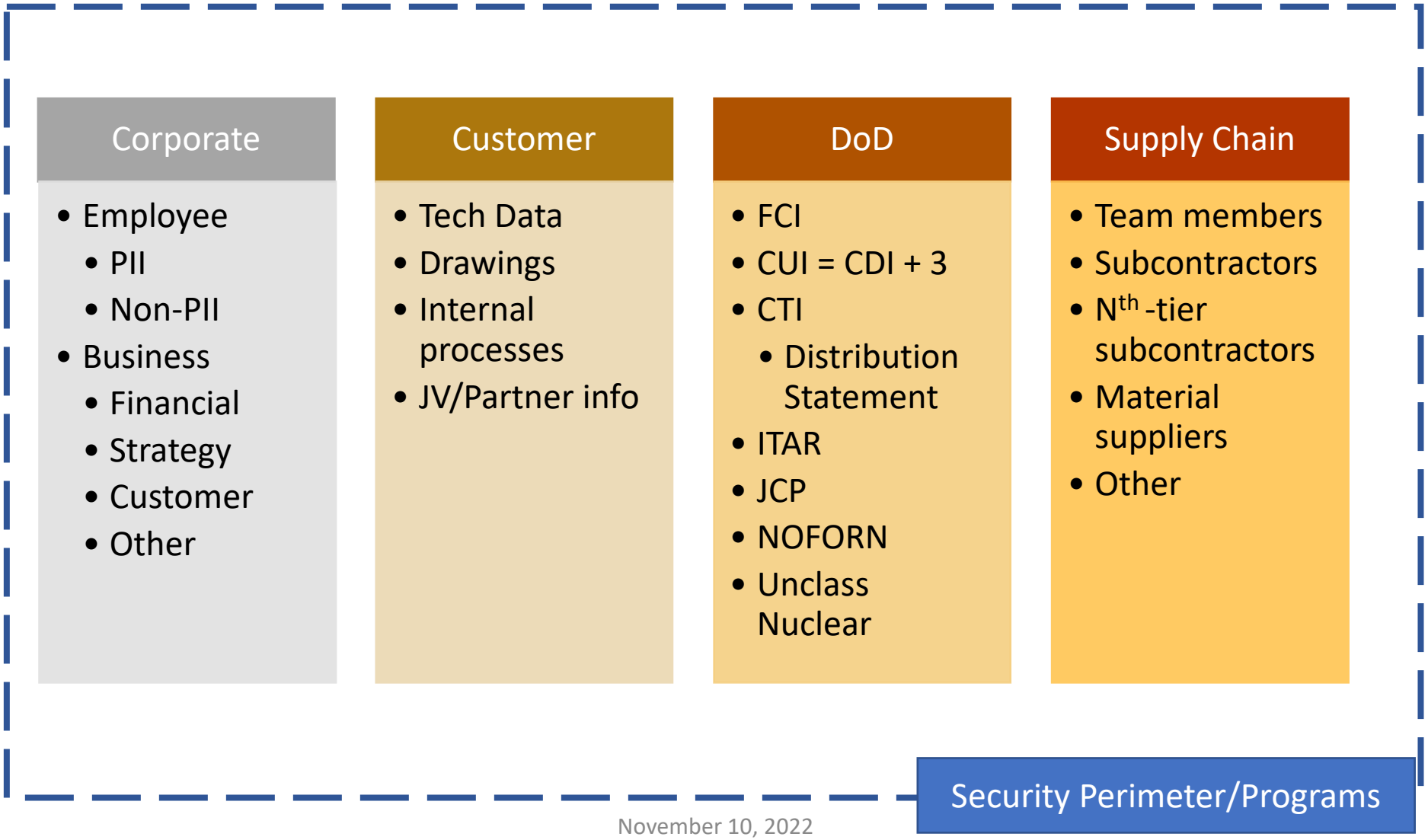
Information

- If there is nothing to protect
- If there is no concern
- If your company, your files, your computers and networks hold nothing of any importance
- Then,
- There is no need for any type of security measures either physical or cybersecurity
- But ….

Types of Information

- Non-sensitive – general information
- Company Proprietary
- Employee sensitive information – medical, employment, other
- Customer (x) Proprietary
- Federal Contract Information
- Controlled Unclassified Information
- Joint Certification Program (JCP)
- International Traffic in Arms Regulation (ITAR)

General Information Sources



Information – access / sharing

- ITAR – US Person to US Person – see definition (individual + company)
  - Email – FIPS 140-2 (end to end encryption)
- JCP – Active SAM, Active CAGE code, Active JCP Program
  - Data Custodian to Data Custodian
  - JCP may also be or contain ITAR
- CUI – Lawful Governmental Purpose and allowed by Dissemination Controls
  - Holder makes determination
  - CUI may also be or contain either or JCP and ITAR
- **Other program requirements and handling requirements apply**

Example: Clauses incorporated by reference

Screen shot from Master solicitation

DFARS 252.204-7008 (Oct 2016)	Compliance with Safeguarding Covered Defense Information Controls
DFARS 252.204-7009 (Oct 2016)	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
DFARS 252.204-7012 (Dec 2019)	Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.204-7015 (May 2016)	Notice of Authorized Disclosure of Information for Litigation Support
DFARS 252.204-7017 (Dec 2019)	Prohibition of Acquisition of Covered Defense Telecommunications Equipment or Services-- Representation
DFARS 252.204-7018 (Jan 2021)	Prohibition of Acquisition of Covered Defense Telecommunications Equipment or Services
DFARS 252.204-7019 (Nov 2020)	Notice Of NIST SP 800-171 DoD Assessment Requirements
DFARS 252.204-7020 (Nov 2020)	NIST SP 800-171 DoD Assessment Requirements
DFARS 252.213-7000 (Sep 2019)	Notice to Prospective Suppliers on Use of Supplier Performance Risk System in Past Performance Evaluations
DFARS 252.223-7001 (Dec 1991)	Hazard Warning Labels
DFARS 252.223-7006 (Sep 2014)	Prohibition On Storage, Treatment, And Disposal Of Toxic Or Hazardous Materials—Basic
DFARS 252.223-7008 (Jun 2013)	Prohibition Of Hexavalent Chromium
DFARS 252.225-7007 (Dec 2018)	Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies
DFARS 252.225-7048 (Jun 2013)	Export-Controlled Items

FAR clauses: https://www.acquisition.gov "Browse Far" Go to Number 52 on left and select. Clauses appear in numerical order

DFAR clauses: https://www.acquisition.gov Top horizontal menu – Regulations then DFARS on upper left pop-up. Select number 252 on left. Clauses appear in numerical order

Notification – JCP, ITAR, EAR information

RQ032: EXPORT CONTROL OF TECHNICAL DATA

This item has technical data some or all of which is subject to export-control of either the International Traffic in Arms regulations (ITAR) or the Export Administration Regulations (EAR), and cannot be exported without prior authorization from either the Department of State or the Department of Commerce. Export includes disclosure of technical data to foreign persons and nationals whether located in the United States or abroad. This requirement applies equally to foreign national employees and U.S. companies and their foreign subsidiaries. DFARS 252.225-7048 is applicable to this data.

The Defense Logistics Agency (DLA) limits distribution of export-control technical data to DLA contractors that have an approved US/Canada Joint Certification Program (JCP) certification, have completed the Introduction to Proper Handling of DOD Export-Controlled Technical Data Training and the DLA Export-Controlled Technical Data Questionnaire (both are available at the web address given below), and have been approved by the DLA controlling authority to access the export-controlled data. Instructions for obtaining access to the export-controlled data can be found at: https://www.dla.mil/HQ/LogisticsOperations/EnhancedValidation/

To be eligible for award, offerors and any sources of supply proposed for use are required to have an approved JCP certification and have been approved by the DLA controlling authority to access export-controlled data managed by DLA. DLA will not delay award in order for an offeror or its supplier to apply for and receive approval by the DLA controlling authority to access the export-controlled data.

ITAR
EAR

JCP

Copied from: https://dibbs2.bsm.dla.mil/Downloads/RFQ/9/SPE7L022T1769.PDF - pages 7 and 8

Securely

Focus of DFARS 252.204-7012/NIST 800-171 r2

- Confidentiality*
  - Information shared with designated and eligible recipients
- Integrity
  - Information remains in-tact
- Availability
  - Can access when needed

Start with the goal in mind.

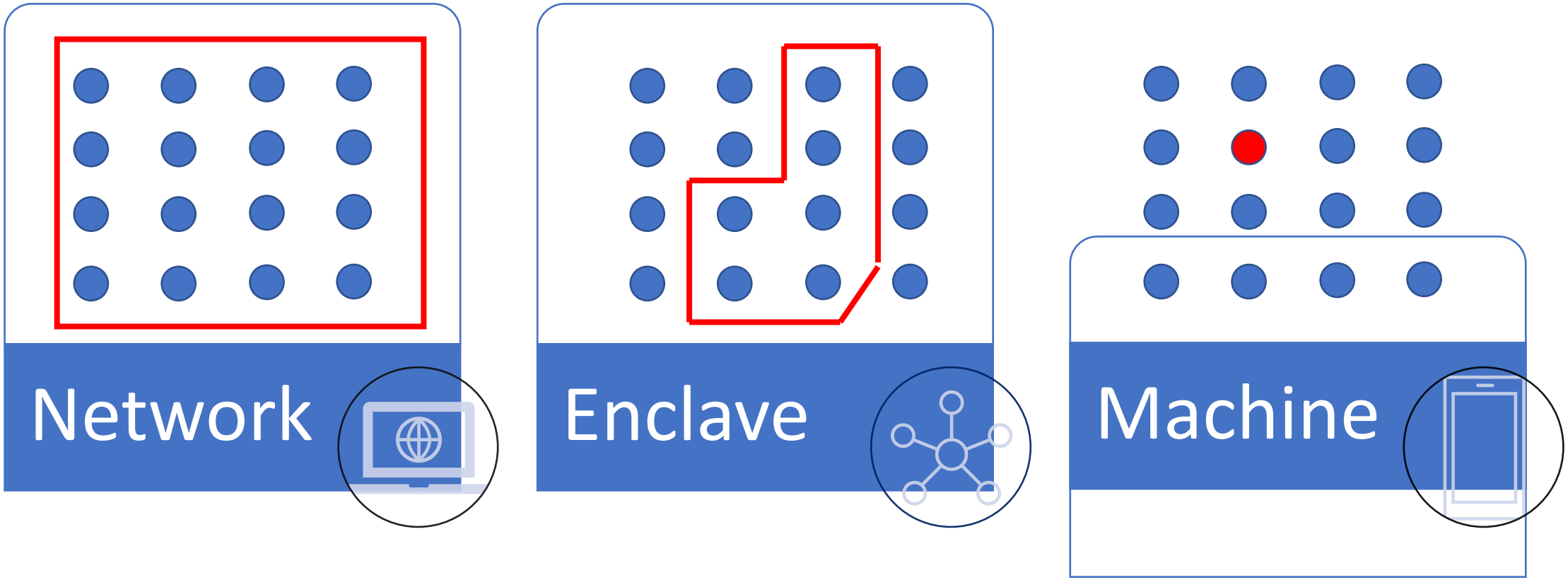
Information Handling Considerations

Security Protection Asset Examples

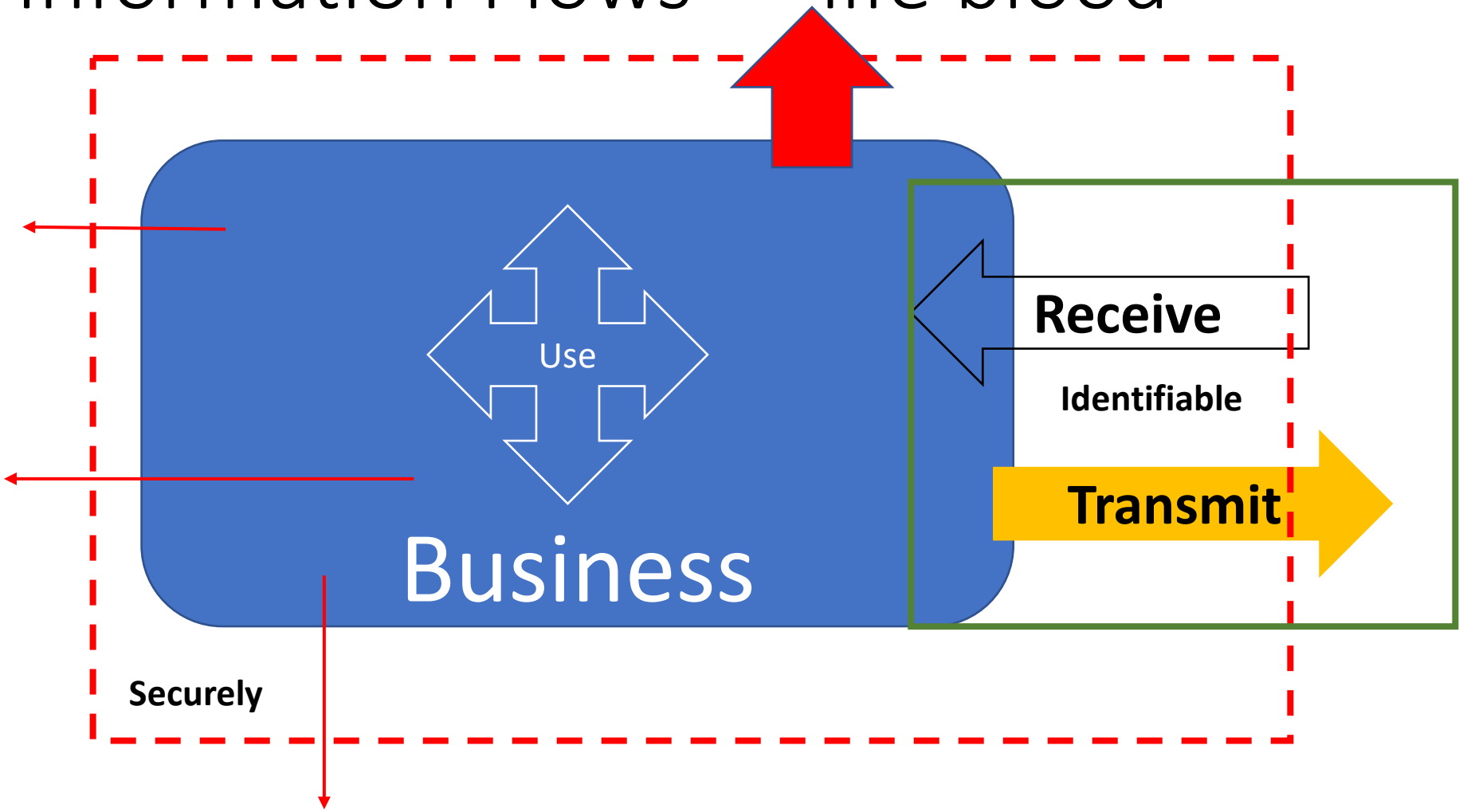
Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings

CMMC Assessment Scope – Level 2 | Version 2.0; page 4

Determine needs to be secured



Information Flows = “life blood”

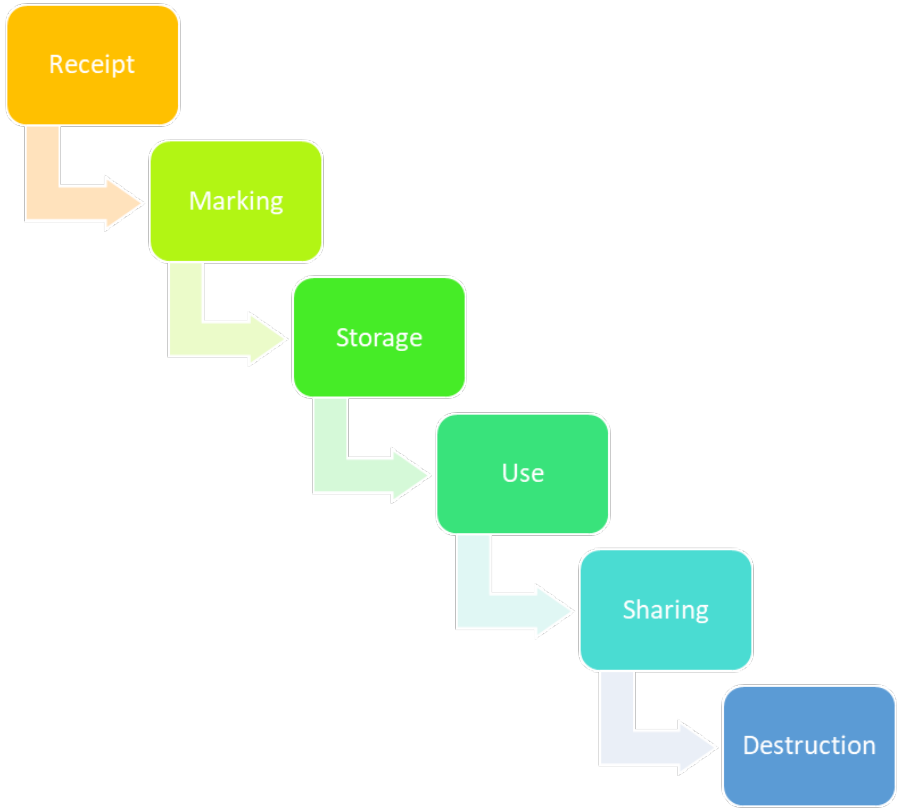


Leakage/unauthorized transfer, sharing, and/or theft

Handle/Share Information with Purpose

- What information do we have?
- How does it arrive?
- Who has access to it?
- How is it controlled and accounted for?
- What information is being shared – with whom, how?
- What are the handling requirements?
- Why is it being shared?
- How is the information stored?
- What threats have been identified?
- Other questions ---

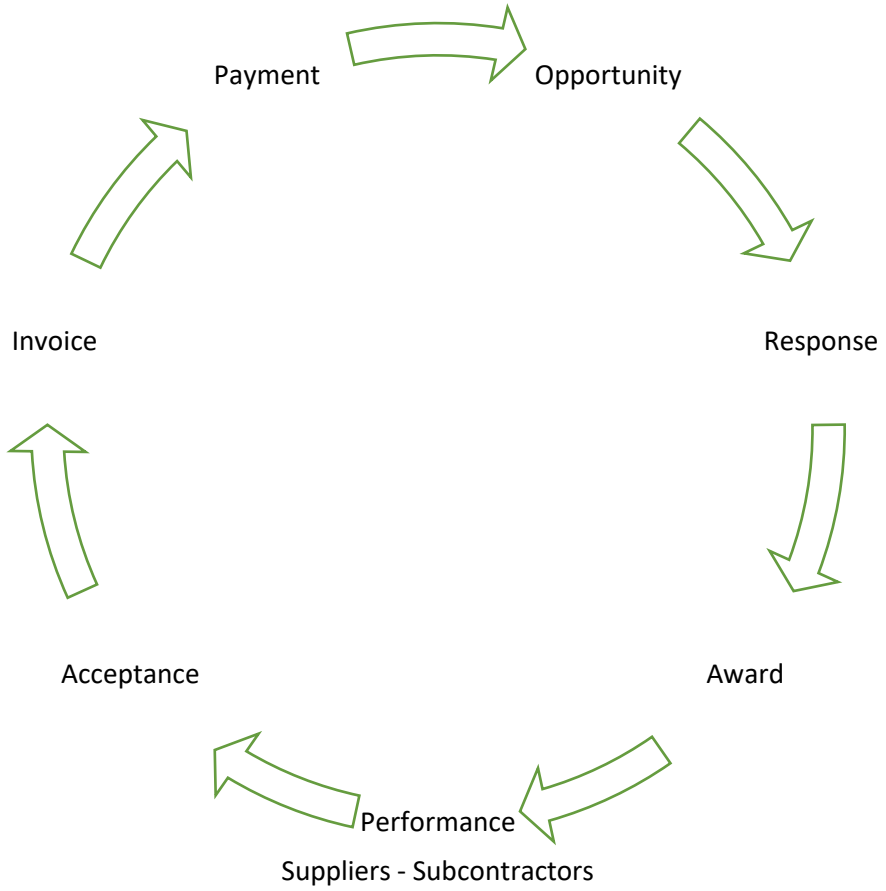
Information – life cycle, general elements



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

M.N. Violante, WPI – Nov 2017

Business Information Flow?



How will it be controlled?

- Internally
- Shared – vetting procedures; currency; consistency
- Flow-down clauses
- Purchase Orders
- Reproduced – controlled, managed
- Stored – physical, digital
- Destroyed – allowable method - equipment

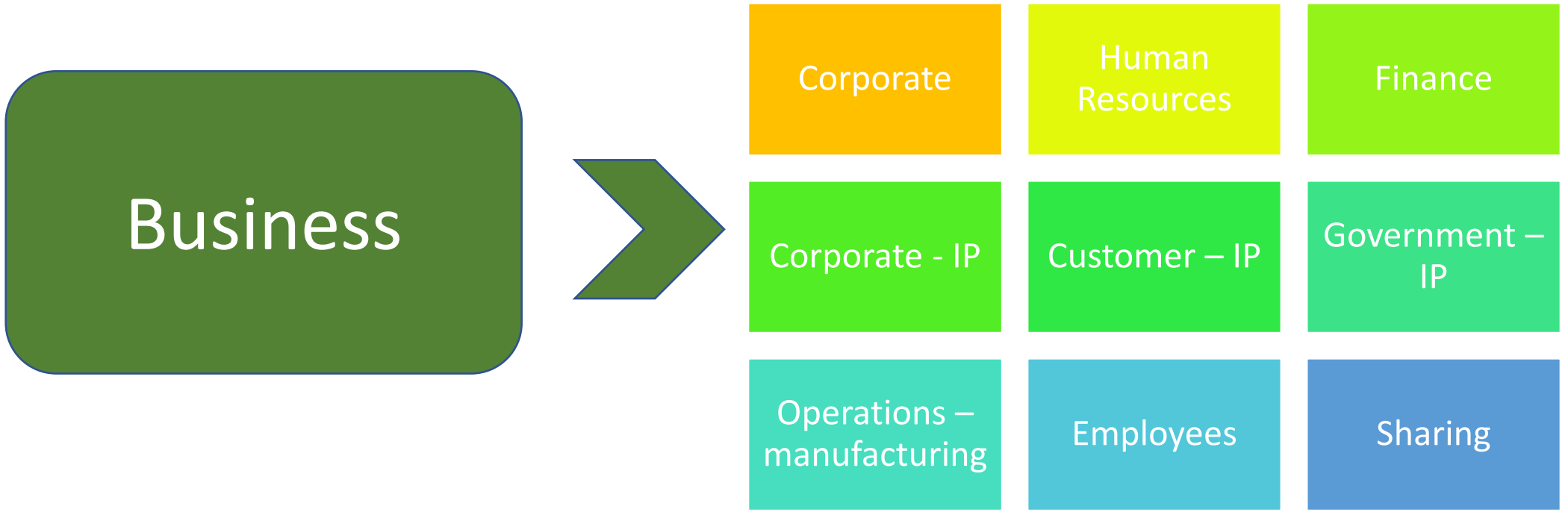
What is a Security Policy Model?

- Top-Down
  - Threat model – Security policy – Security mechanisms

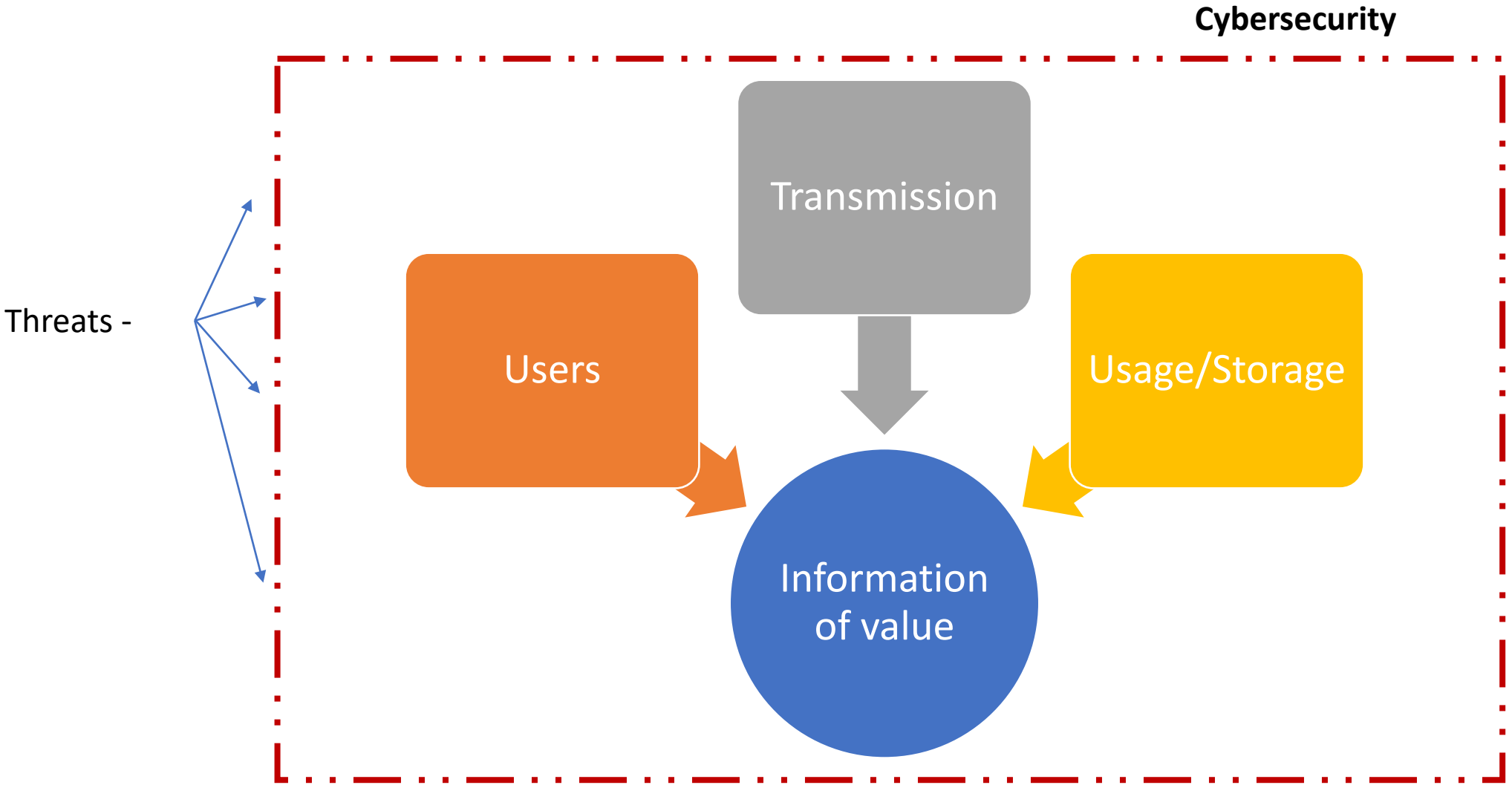
- Security Policy – “critical, and often neglected”
- “By a security policy, we mean a document that expresses clearly and concisely what the protection mechanisms are to achieve. It is driven by our understanding of threats, and in turn drives our system design. It will often take the form of statements about which users may access which data.”

Security Engineering A Guide to Building Dependable Distributed Systems, 3 rd Edition, Ross Anderson, Wiley Publishing, page 316

Business – the term v. reality



The issue


Cybersecurity
Threats -
Transmission
Users
Usage/Storage
Information of value

Information Security

How do you manage this stack of documents?

Does it matter?

General Ideas/principles

- Prevent unauthorized access to systems & information
- Be aware of requirements and system/network status
- Detect unauthorized usage – logs/logging

★ Prevent write down

- Secure information placed (written) to open (web) location

★ Prevent read up

- Member of the public viewing (reading) sensitive information

★ Bell-LaPadula model

Identify – “leakage points”

Copied from Google search: infrared heat loss image

References

Can there be a compliant program without the use of references?

- Are all references available?
- Is there a master list of references?
- Is each reference reviewed for being current?
- Is there evidence that they have been used?
- Are references cited in the materials?

Reference – DD Form 2345 - JCP

Department of Defense

DIRECTIVE

NUMBER 5230.25
November 6, 1984

Incorporating Change 2, October 15, 2018
USD(R&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 (o), 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 2, page 29; Jan 28, 2021

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 Defense for Intelligence (USD(I))," November 23, 2005
(j) DoD Instruction 5200.01, "DoD Information Sec
Compartmented Information," October 9, 2008
(k) DoD Directive 5230.09, "Clearance of DoD Info
August 22, 2008
(l) DoD Instruction 5230.29, "Security and Policy R
Release," January 8, 2009
(m) DoD Manual 5200.01-V2, "DoD Information Se
Information," February 24, 2012
(n) DoD Manual 5200.01-V1, "DoD Information Se
and Declassification," February 24, 2012
(o) DoD Instruction 3200.14, "Principles and Operat
and Technical Information Program," May 13, 1
(p) DoD Instruction 5200.39, "Critical Program Info
Department of Defense," July 16, 2008
(q) Parts 120-130 of title 22, Code of Federal Regula
Traffic in Arms Regulations")
(r) Parts 730-774 of title 15, Code of Federal Regula
Administration Regulations")
(s) Subparts 203, 227 and 252 of title 48, Code of F
(t) DoD Directive 5122.05, "Assistant Secretary of
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

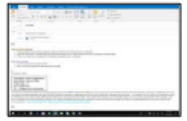
USD(AT&L)

SUBJECT: Distribution Statements on Technical Documents

References: See Enclosure 1

CUI

What requirements apply?

Banner & CUI Designation Indicator	LDC – DISTRO	PORTION Marking
		
Administrative Markings	Coversheets & Labels	Waivers - Legacy
		
Decontrol	IT Systems	Email
		
Shipping/Mailing	Transmittal Documents	Co-mingled
		
Policy & Forms	PPTs & Spreadsheets	Storage
		

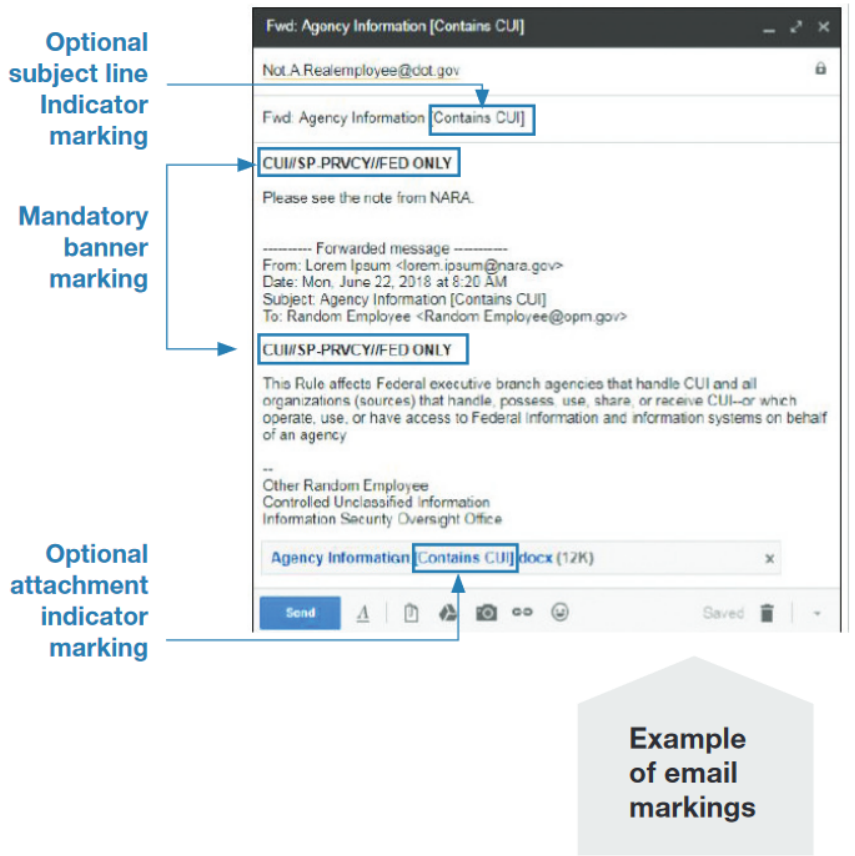
https://www.cdse.edu/Portals/124/Documents/jobaids/CUI-Quick-Marking-Tips.pdf

Marking CUI – emails, example

MARKING EMAILS

- It is mandatory to include banner markings to indicate that an email contains CUI.
- If an email is forwarded, the banner marking must be carried forward.
- If sending an attachment that contains CUI, the name of the file can contain a CUI indicator.
- If an attachment is removed, and the email no longer contains CUI, add the following statement below the banner marking "Uncontrolled Unclassified Information."
- Emails that contain CUI must be encrypted.

Note: Once you begin marking a document, every page in the document must also be marked.

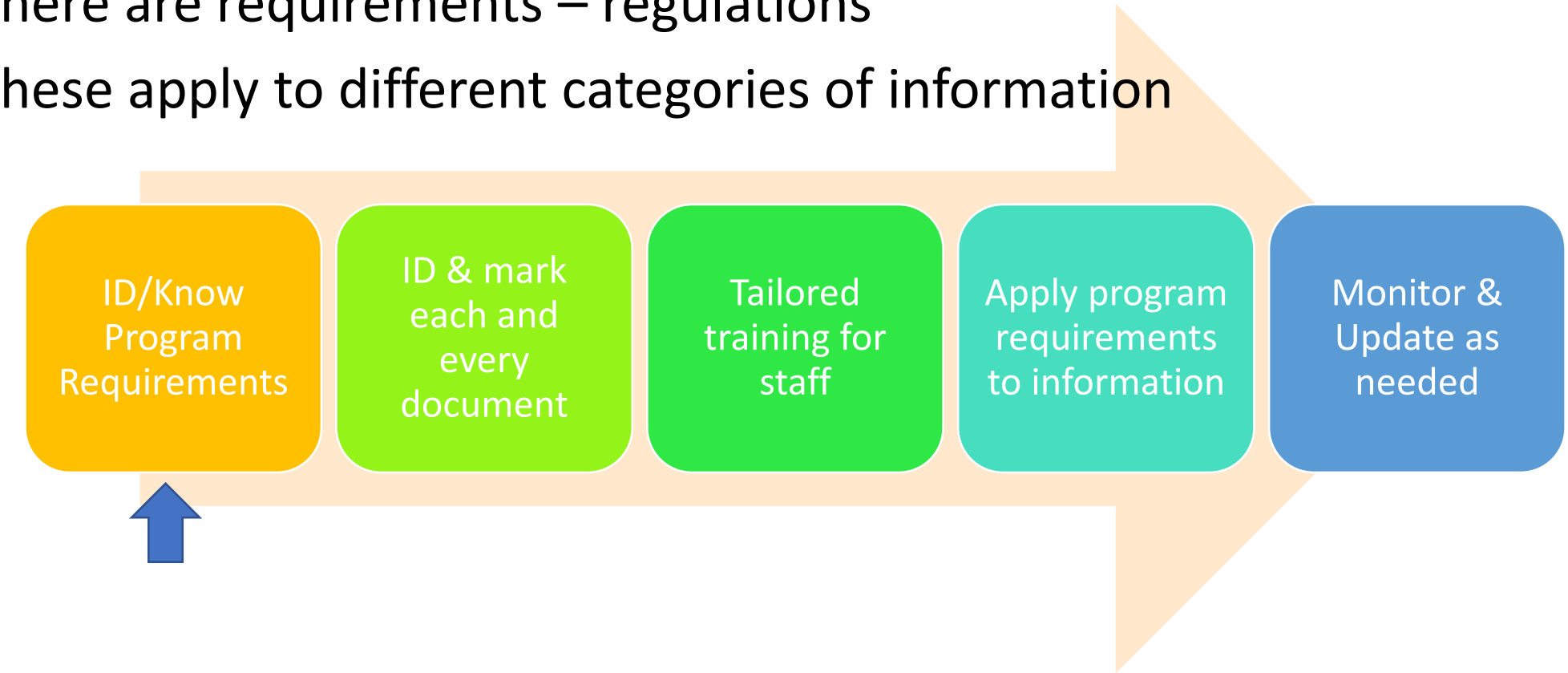


Example of email markings

https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/21-10-18%20CUI%20MARKING%20JOB%20AID%20FINAL.pdf

Document Management

- There are requirements – regulations
- These apply to different categories of information



What needs to be considered (what changes)?

- Facilities
  - Structure
  - Access
  - Security – physical, cyber
- People – staff, external
- Network
- Devices – Desktop, Laptop, Smart Devices, IoT, other
- Software

Utilize definitions

- ***Defense article*** means any item or technical data designated in § 121.1 of this subchapter and includes:

  (1) 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; and

  (2) 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.

Utilize definitions - § 120.62 U.S. person.

- *U.S. person* means a person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. It also includes any governmental (Federal, state, or local) entity. It does not include any foreign person as defined in § 120.63.

Questions

- Has a Security Manager been assigned?
- How will sensitive information be managed?
- How will it be stored? – physical storage / digital storage
- How will eligibility and access be determined.
- What training will be required?
- How will the company remain current?
- Are there Security Policies? – Procedures?
- Is there a Compliance Program?

Hypothetical Question - 1

- How do you determine who has access to CUI?

d. Unlike classified information, an individual or organization generally does not need to demonstrate a need-to-know to access CUI, unless required by a law, regulation, or government-wide policy, but must have a lawful governmental purpose for such access. One example of a requirement for need-to-know established by law, regulation, or government-wide policy is Section 223.6 of Title 32, CFR, which requires a person to have a need-to-know to be granted access to DoD Unclassified Nuclear Information (UCNI).

(1) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 12 & 19

Hypothetical Question - 2

- Can you provide some examples of how you define a lawful governmental purpose?
- Who else should I speak to about this issue?

> (2) The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 19

Lawful Governmental Purpose

Eleonore: CUI? Interesting. I've never been on a project that deals with all that much CUI. You know what you should do? Send some of it over to me this afternoon. I've got free time and I'm happy to help. And, anyway, I've always been interested in that project.

Employee: As an employee of an executive branch agency that stores, handles, or accesses CUI, you may be asked share CUI with a coworker, another agency, or non-Federal partner at some point. Therefore, you should familiarize yourself with the principle of "Lawful Government Purpose," or LGP, which is the standard for sharing and providing access to CUI under the CUI program.

Slide 2 LAWFUL GOVERNMNET PURPOSE

Employee: Lawful Government Purpose is a dynamic standard for deciding when to share and when not to share CUI with other coworkers, executive branch agencies or non-Federal partners who handle CUI. LGP concerns itself with the purposes CUI may serve as a resource in achieving the mission objectives of government operations and projects. CUI should only be shared when the contents of CUI will help achieve the goals of a common project or operation. On the other hand, if sharing a CUI resource would obstruct or harm the government purpose, then the CUI should be withheld.

Scene 1 INT. BUSY CAFETERIA – LUNCHTIME

Blair: You know what, Eleonore, that's a really nice offer but you don't have lawful government purpose to view the CUI. And anyway, most of the CUI I'm handling is DL only anyway.

https://www.archives.gov/files/cui/documents/lawful-government-purpose-transcript-201808.pdf

Hypothetical Question – 2a

- How does a business purpose differ from a lawful governmental purpose?
- With respect to outside consultants, IT providers and others should they have access to CUI?
  - An outside party may have a “business purpose” or a “business need” to have access to CUI; do they have a lawful governmental purpose?

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 19

Hypothetical Question - 3

- Do you have records of completion for the mandatory annual training?
- Should this training be a stated requirement to any business – their employees who will access CUI?
  - b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 17 - 18

Plan, Policies, Procedures

- Is there a Master List?
- Is each document identified by revision number/date?
- Who signed the document?
  - If the signer is other than the CEO/President is there a Letter of Designation authorizing them to act on behalf of the company
- Have all applicable documents been reviewed/approved by the board?
  - Formally approved

Review | Assessment Framework

- Is there a program assessment policy?
- Are responsibilities detailed?
- Are there required periodicities?
- Are formal reports submitted? To whom?
- Are deficiencies identified?
- Are action items identified?
  - Are they prioritized?
  - Are they tracked?
  - Are there repeat deficiencies?

Internal Audit Report

- Periodicity
- Conducted by
- Training, experience, qualifications
- Findings
- Action items
- Corrective actions
- Open items
- Status
- Management review – comments
- Tools for tracking?

Hypothetical Question - 3

- Do you have records of completion for the mandatory annual training?
- Should this training be a stated requirement to any business – their employees who will access CUI?
  - b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 17 - 18

Are specific requirements identified?

https://www.dodcui.mil/Home/Training/

Training records

Are there training records?

What documentation is included?

Is there a master training schedule?

Is training tailored based upon position?

How are the training needs evaluated?

How is the effectiveness of the training assessed?

How are instructors selected?

Is there a company instruction – policy that addresses training?

Logs

- Visitor
- Training
- Internal Audits
- System activity – usage
- Maintenance
- Repair
- Upgrades
- Access

Applicability of Checklists

Consistency – removes personal element (knowledge, experience)
Creates a reusable process
Ensures all required elements are addressed
Developed from corporate experience
Does not rely upon memory
Reproducible
Reference: The Checklist Manifesto
Reference: The Goal

Hypothetical Question - 4

- Do you for see a need to print any documents identified as CUI?
  - Answer – No: How will prevent a staff member from inadvertently printing a document or other information?
  - Follow up – have you tested these procedures?
  - Follow up – do you train on these procedures?
    - Assessor makes note to review training materials for this specific point
  - Answer – Yes: Where are these documents stored?
  - Follow up – how do you destroy these documents?
  - Follow up – can I see the shredder? / can I see the specifications of the shredding service provider agreement

CUI - Destruction

4.5. DESTRUCTION.

Guidance for destroying CUI documents and materials is provided in this issuance, the CUI Registry, and ISOO Notice 2019-03. CUI documents and materials will be formally reviewed in accordance with Paragraphs 4.5.a. and 4.5.b. before approved disposition authorities are applied, including destruction. Media containing CUI must include decontrolling indicators.

→ https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; page 30 of 40

This guidance document does not have the force and effect of law and is not meant to bind the public, except as authorized by law or regulation or as incorporated into a contract. Accordingly, with regard to the public, this document only provides clarity regarding existing requirements under the law or agency policies. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority.

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form

July 15, 2019

Purpose

1. This Notice provides guidance for destroying (via single and multi-step methods) Controlled Unclassified Information in paper form.

CUI – Destruction (2)

Single-step paper destruction standard

6. For the single-step paper destruction method, agencies must:

   a. Use cross-cut shredders that produce 1 mm x 5 mm (0.04 in. x 0.2 in.) particles (or smaller); or

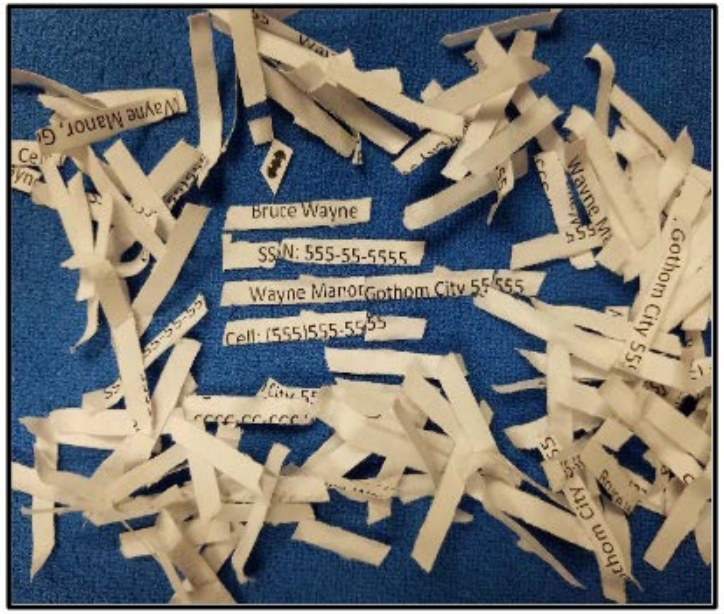
   b. Pulverize/disintegrate paper using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.

   (NIST SP 800-88, rev 1, Table A-1: Hard Copy Storage Sanitization)

7. The National Security Agency (NSA) maintains an Evaluated Products List (EPL) of equipment it authorizes to destroy hard copy (paper) Classified National Security Information. This equipment also meets CUI single-step paper destruction standards. The most updated NSA EPL for "Paper Shredders" can be found at: https://www.nsa.gov/resources/everyone/media-destruction/

Use approved equipment/processes

NOT APPROVED



Destroy paper using cross cut shredders that produce particles that are 1mm by 5 mm.

APPROVED

https://www.archives.gov/files/cui/documents/cui-overview-powerpoint.pdf; slide 13 of 16

CYBER FRIDAY LIVE WEBINAR SERIES

- November 4, 2022

  Developing and Implementing Essential Security Policies, Practices, and Procedures

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- November 18, 2022

  Incident Identification, Reporting Requirements, and Recovery

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- December 2, 2022

  Designing and Using Security Exercises to Test and Improve Security Programs

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

PRESENTED BY

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

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 16
  Certifications for Veteran Owned Businesses
- November 16
  Preparing for One-on-One Buyer Meetings
- November 29
  The HUBZone Program – Certification Benefits and Regulations
- January 10
  The SBA 8(a) Program and Small Disadvantaged Business (SDB) Program

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR

…More information and registrations at wispro.org/events

LOCAL GOVERNMENT SALES OPPORTUNITIES

- ~~October 13~~
  ~~SE WI and the Milwaukee Area - Virtual~~

- ~~October 20~~
  ~~Sales Opportunities with the City of Madison – In Person~~

- November 9
  Sales Opportunities with Dane County – In Person

- November 10
  Green Bay Area (Virtual)

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
LOCAL GOV'T SALES OPPS

…More information and registrations at wispro.org/events

DOD SUPPLIER ROADMAP SERIES

- November 3
  Non-Traditional Acquisition Methods
- November 10
  Information Types & Handling Procedures
- November 17
  Developing a DoD Business Strategy

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
DOD SUPPLIER ROADMAP

…More information and registrations at wispro.org/events

Government Opportunities Business Day in Partnership with Truax Field/115th Fighter Wing

November 15

Including 1-1 Buyer Meetings

Wispro.org/Events

Registration now open

MARKETPLACE WISCONSIN

Plus 1-1 Buyer Meetings

The Contracting Academy

Developing and Growing Government Contractors

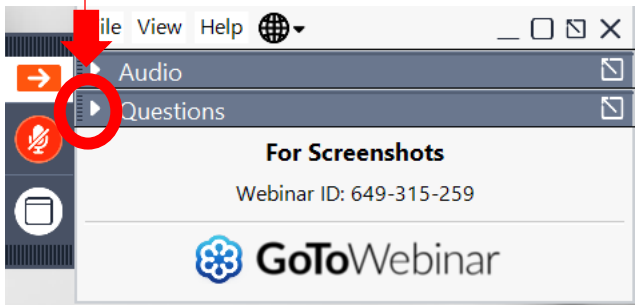
December 6-7, 2022

MarketplaceWisconsin.com

QUESTIONS?

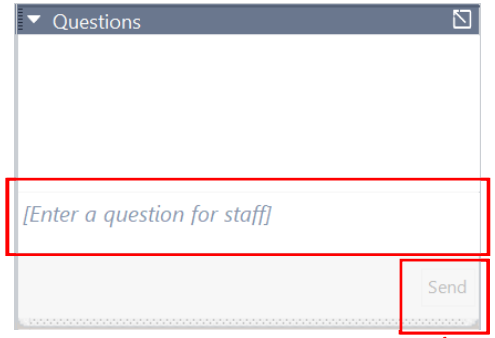
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

SURVEY

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit, please contact:

Caroline Boettcher
carolineb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226