WPI Wisconsin Procurement Institute

APEX ACCELERATORS

Emerging Issues:

Information Security

October 19| 1:00 - 2:00 pm

Presented by:

Marc Violante, WPI

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

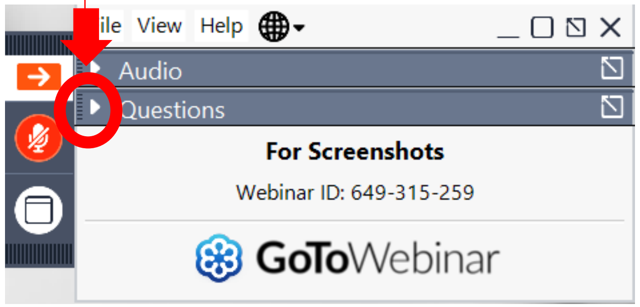
PLEASE

- 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!

OPENING THE QUESTIONS BOX

Click here to access within the Control Panel

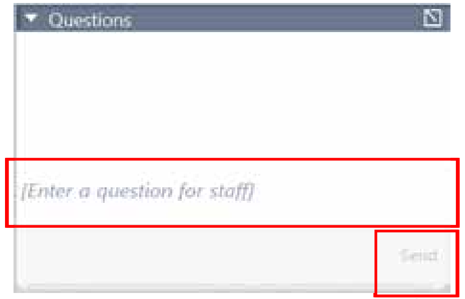


For Screenshots

Webinar ID: 649-315-259

USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

WPI Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

WPI is Wisconsin's APEX ACCLERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

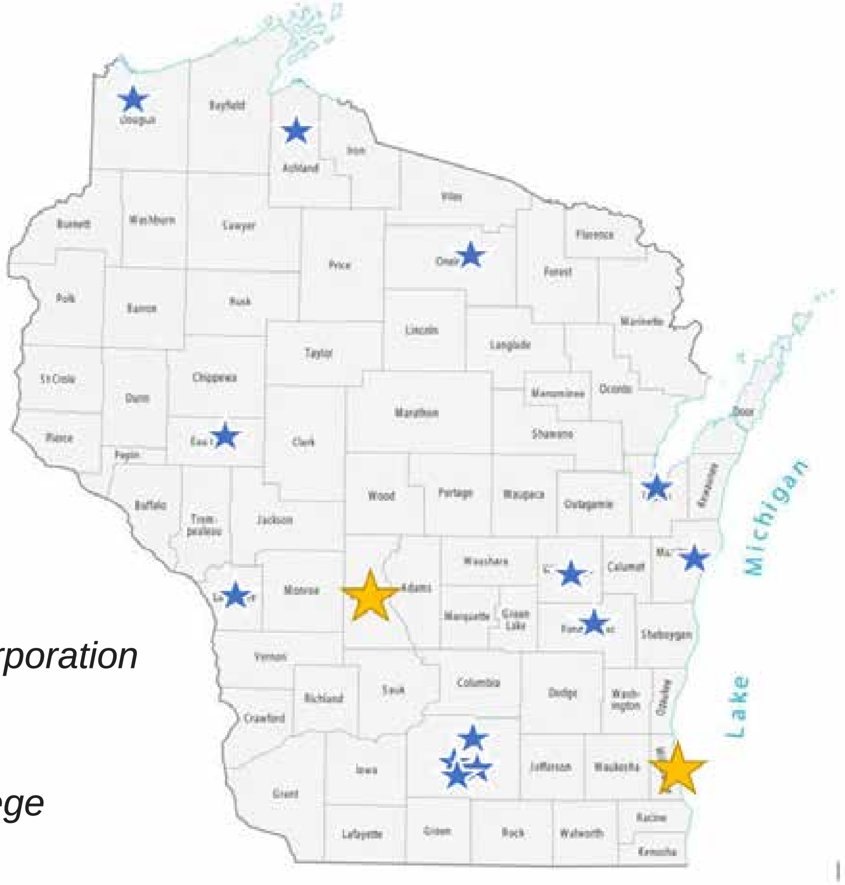
WPI provides services to all of Wisconsin's 72 counties

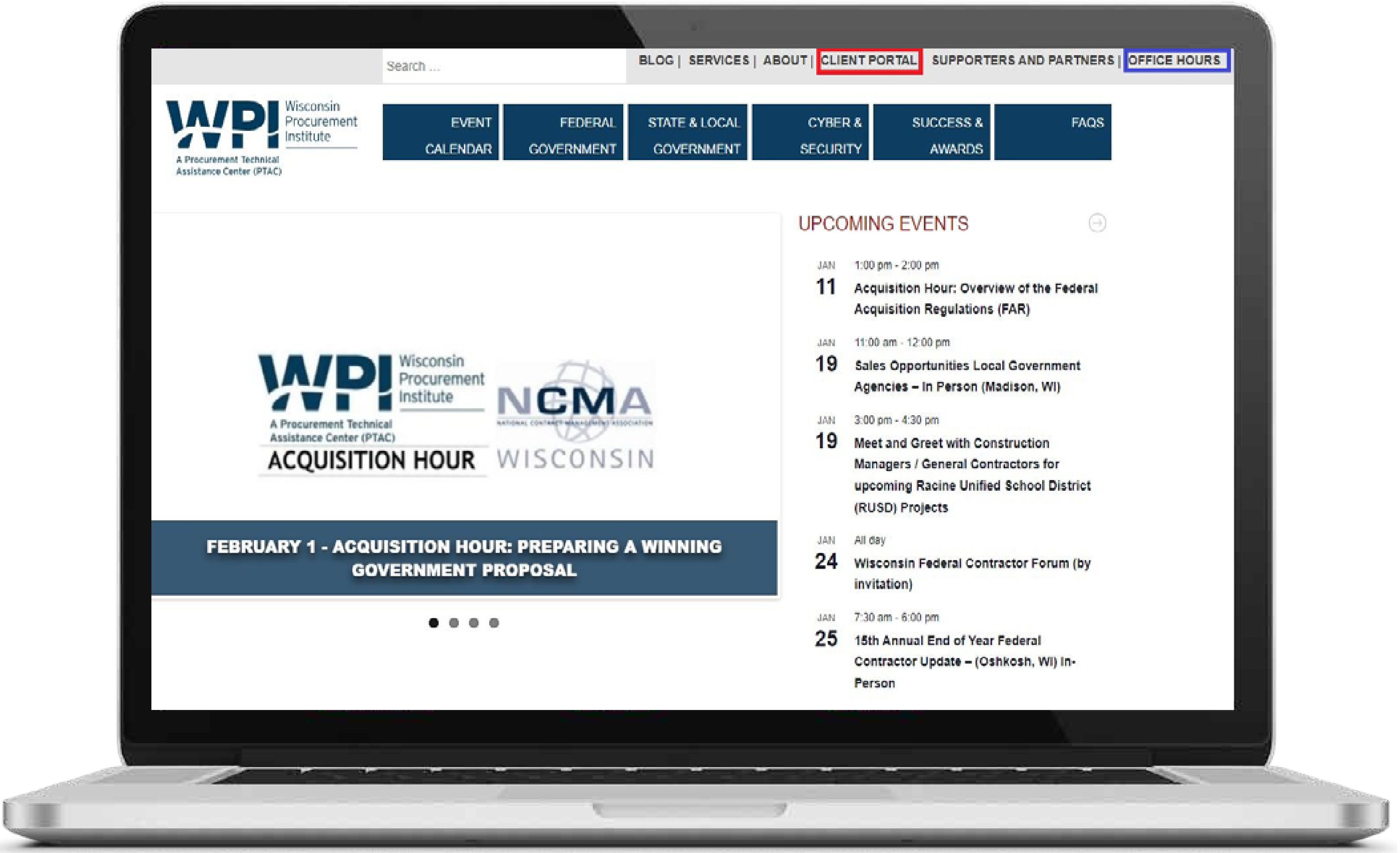
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

www.wispro.org

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)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*




Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR
NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

FEBRUARY 1 - ACQUISITION HOUR: PREPARING A WINNING GOVERNMENT PROPOSAL

UPCOMING EVENTS

JAN 11 — 1:00 pm - 2:00 pm
Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)

JAN 19 — 11:00 am - 12:00 pm
Sales Opportunities Local Government Agencies – In Person (Madison, WI)

JAN 19 — 3:00 pm - 4:30 pm
Meet and Greet with Construction Managers / General Contractors for upcoming Racine Unified School District (RUSD) Projects

JAN 24 — All day
Wisconsin Federal Contractor Forum (by invitation)

JAN 25 — 7:30 am - 6:00 pm
15th Annual End of Year Federal Contractor Update – (Oshkosh, WI) In-Person

Emerging Issues
Information Security

Marc N. Violante

October 19, 2023

Wisconsin Procurement Institute

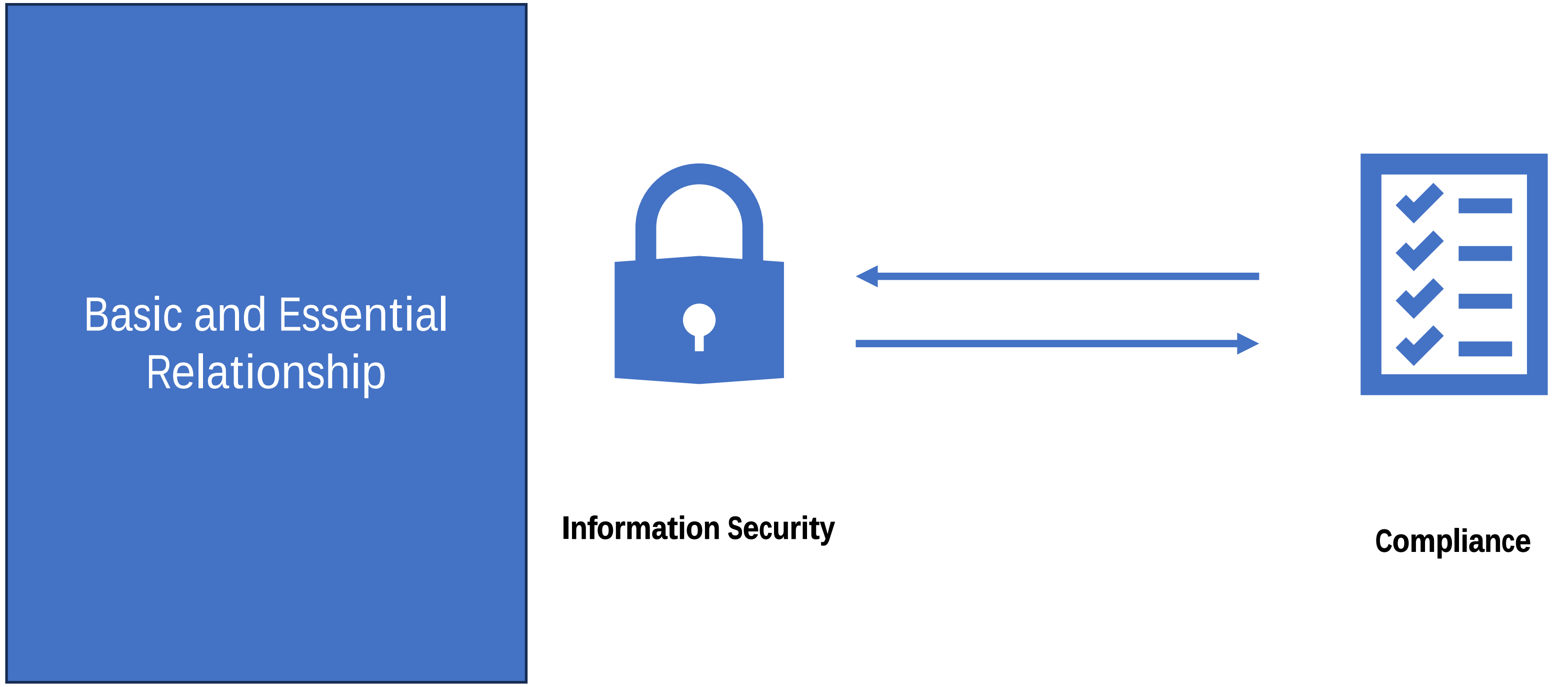
What do I want the attendees to learn – think about?

- The multiple dimensions of information flow
- The various types of information
- The handling, security requirements for different information
- The need to mark – identify information – all
- The need to know who the recipient is and if they are eligible to receive the information – both person and company

The Coffee Shop

SUNDAY NEWSPAPER

BUSINESS PROPOSAL

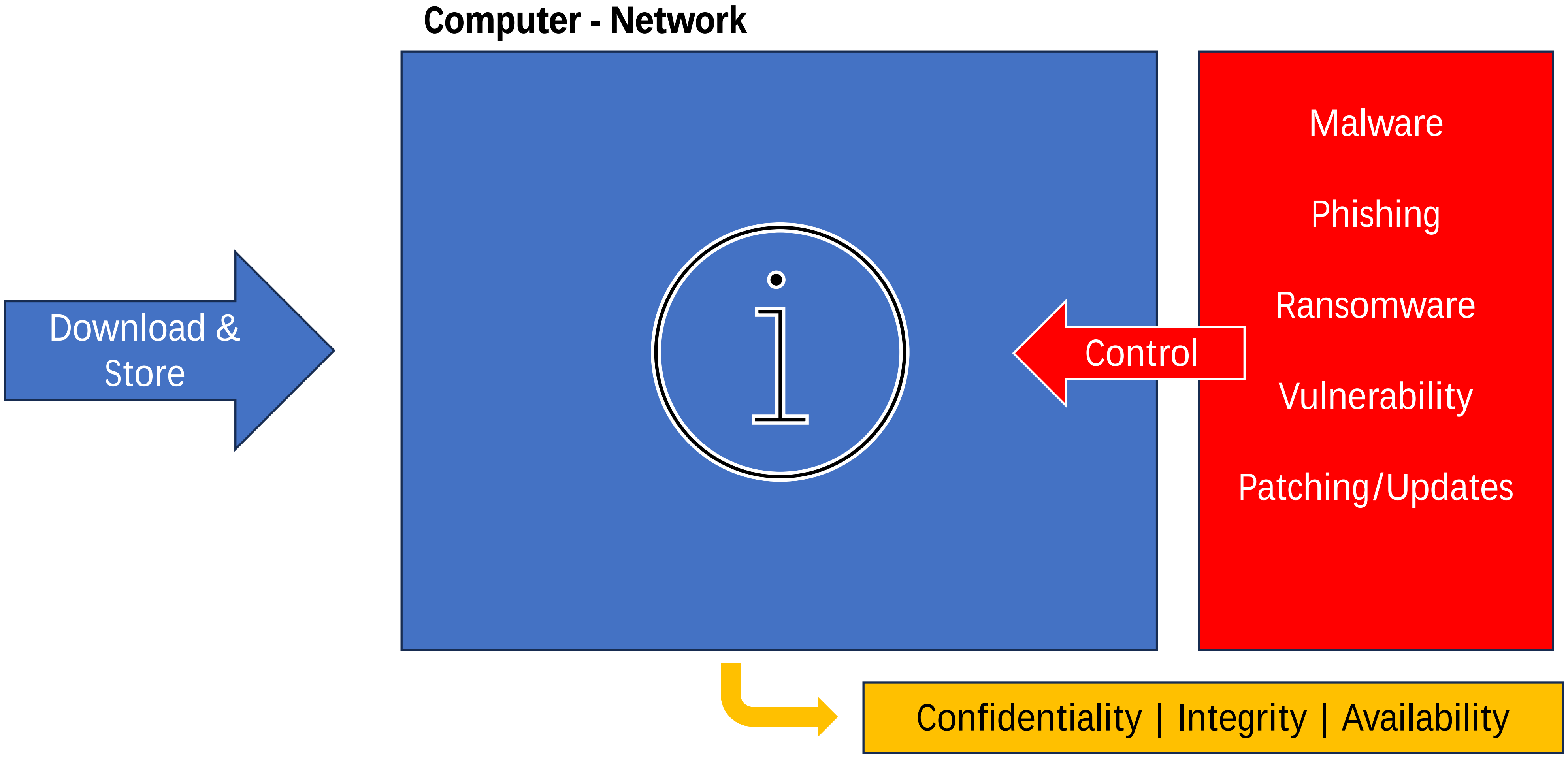


Basic and Essential Relationship

Information Security

Compliance

Prevalent Model



Computer - Network

Download & Store

Control

Malware

Phishing

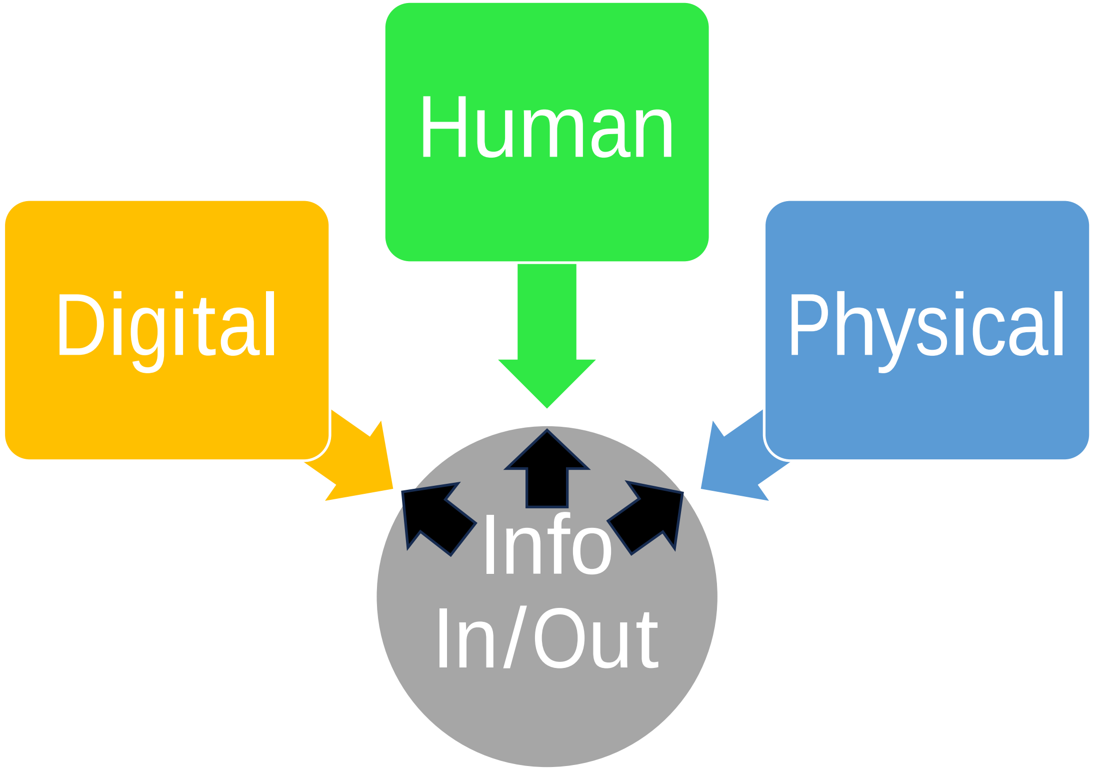
Ransomware

Vulnerability

Patching/Updates

Confidentiality | Integrity | Availability

Information Flows / Channel



- What pathways are used?
- Who uses?
- How is it protected?
- Where is it stored?
- How is it tracked?
- How is dissemination tracked?
- How is the process audited?
- How is information destroyed?

Background Questions

- Number of staff assigned to IT security?
- Who is the lead?
- Is the lead formally appointed?
- Does the lead have the background, experience, authority to act?
- What is the company's IT Security budget?
- How are threats identified?
- How are threats communicated to company leadership?
- Are employees provided formal training?
- Are employee training records maintained, with agenda?

Information Security

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

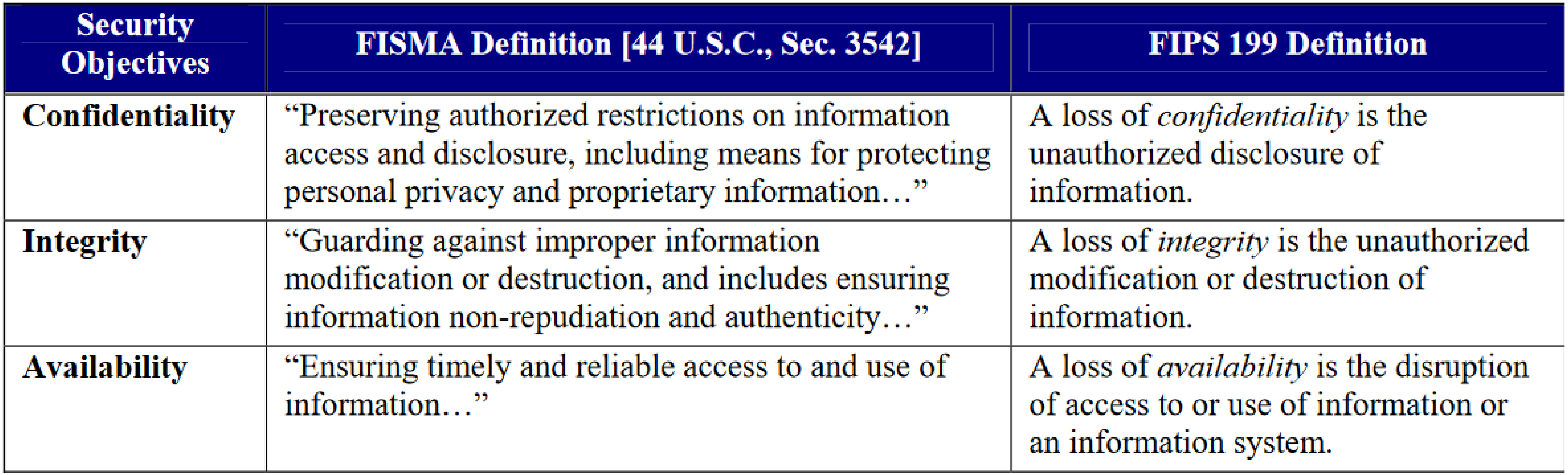
[44 U.S.C., Sec. 3542]

Confidentiality | Integrity | Availability

- Confidentiality
  - Grandma’s secret ingredient is cornflakes.

- Integrity
  - Grandma’s recipe calls for 1/8 of a cup
  - After changes – Grandma’s recipe calls for ½ of a cup

- Availability
  - I need to bake cookies tonight; why can’t I access the recipe?



Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of *availability* is the disruption of access to or use of information or an information system.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf, page 9

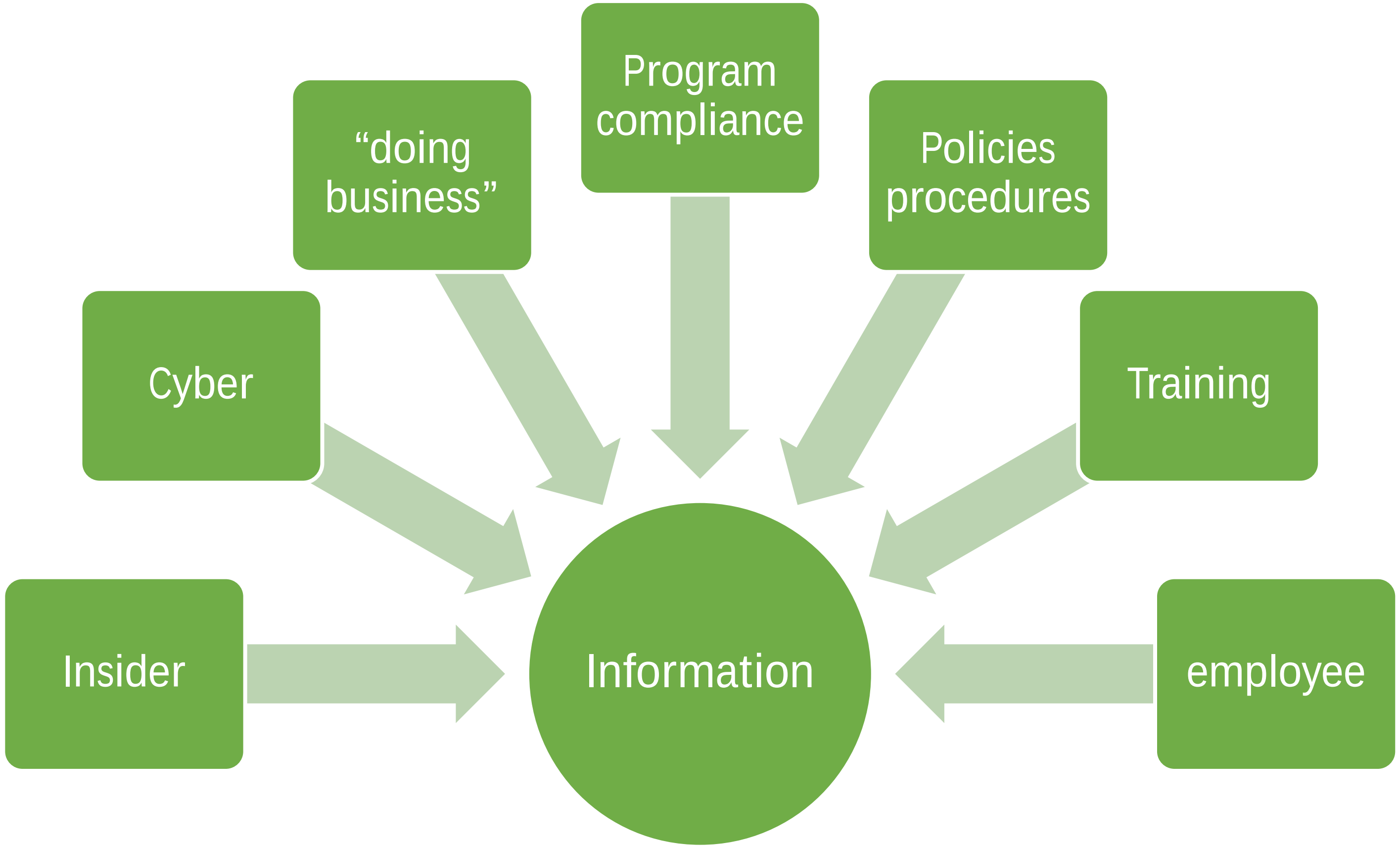
Security Category v. Impact

- Security Category information type =

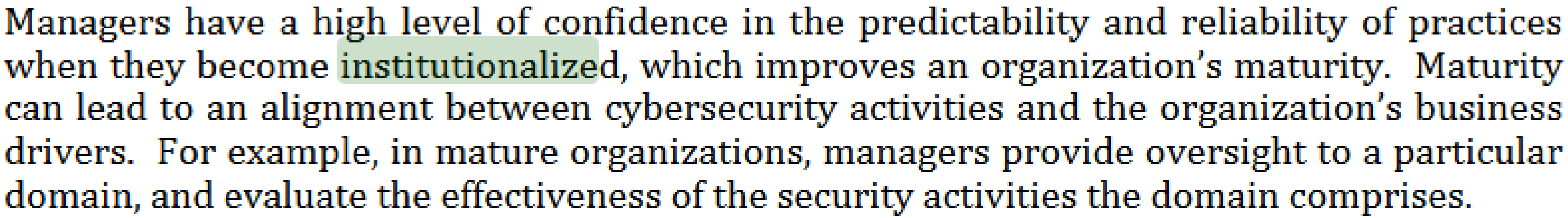
{(confidentiality, impact), (integrity, impact), (availability, impact)}

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf, page 11

Threat awareness - examples



Institutionalized – (passe) but a good concept



Managers have a high level of confidence in the predictability and reliability of practices when they become institutionalized, which improves an organization's maturity. Maturity can lead to an alignment between cybersecurity activities and the organization's business drivers. For example, in mature organizations, managers provide oversight to a particular domain, and evaluate the effectiveness of the security activities the domain comprises.

- Institutionalization is the process of making CMMC practices repeatable and effective against current and future threats – practices become a deeper, more lasting part of an organization because they are <u>managed and supported in meaningful ways</u>.
- Institutionalization makes practices more likely to be <u>sustained during times of disruption or stress </u>to the organization.

Cybersecurity Maturity Model Certification | Version 1.02, B.2 Process Maturity, pg B-1

Use standard/accepted descriptions

What is a cyber incident? -

- A cyber incident is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

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

Security Controls

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

[FIPS 199]

Start with the end in mind

Pick an approach for success!

Identify key elements- what is needed?

Senior level support

Funding

Staff/talent

Resources

Information

Training – staff/technical

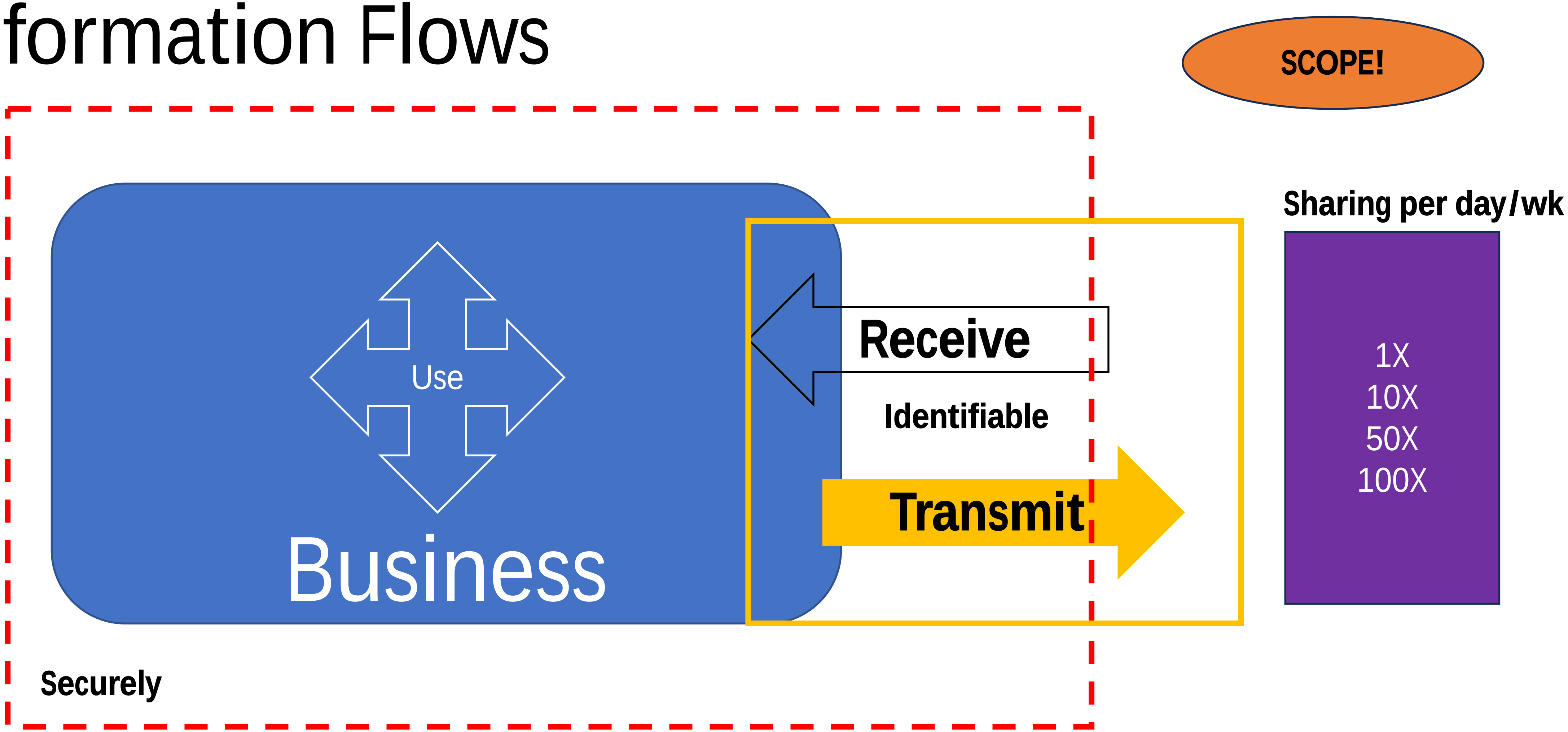
Program considerations

- Requirements (combined)
- Defined SCOPE – all, subnet, enclave, single machine
- System Security Plan
- Assessment plan, policy, procedures
- Assessment results – maintained
- Status tracking/monitoring – SPRS
- Plan of Action and Milestones
- Corrective Actions, maintenance, required updates

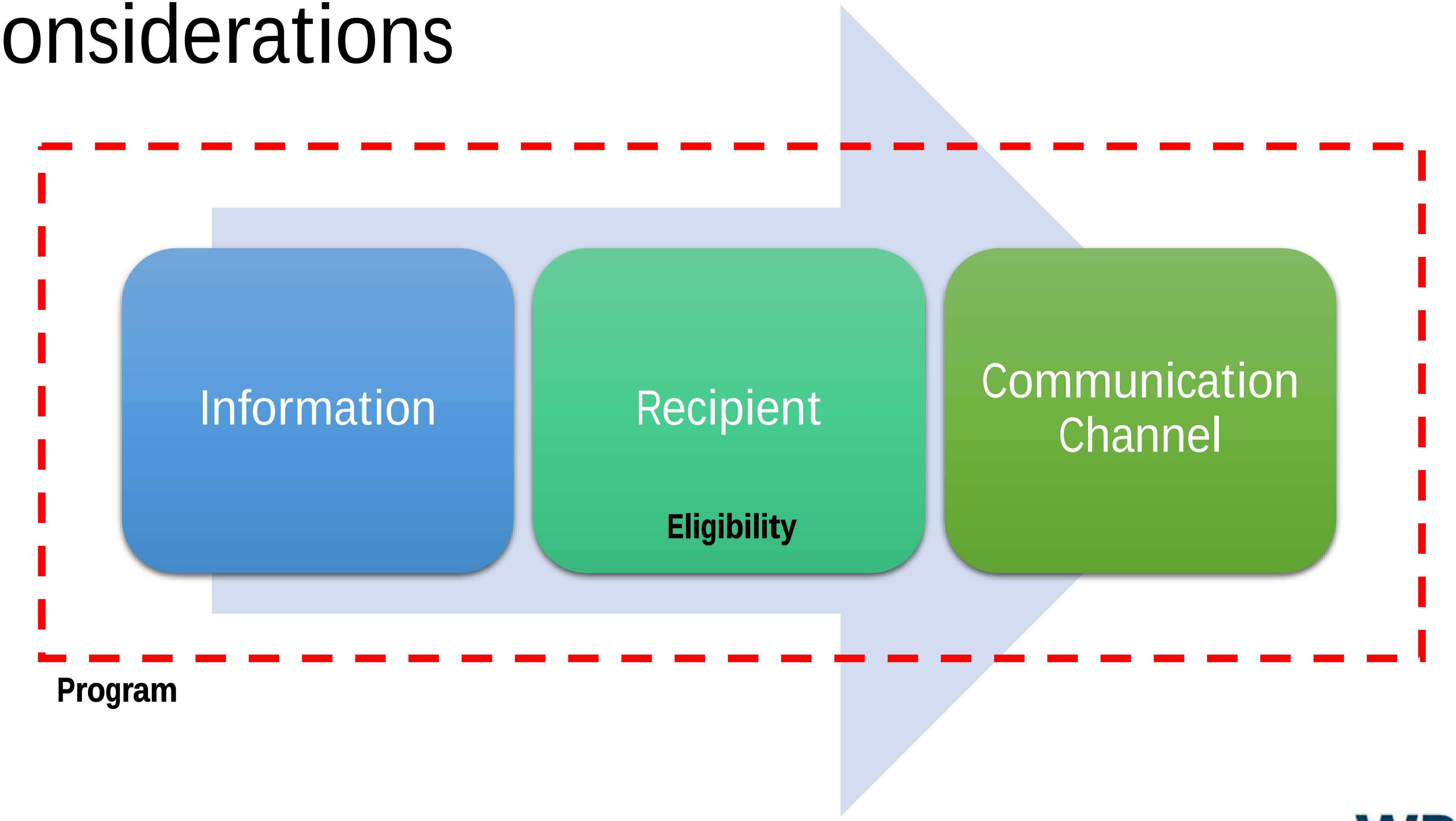
Information Security – the issue

What security controls are needed for these documents?

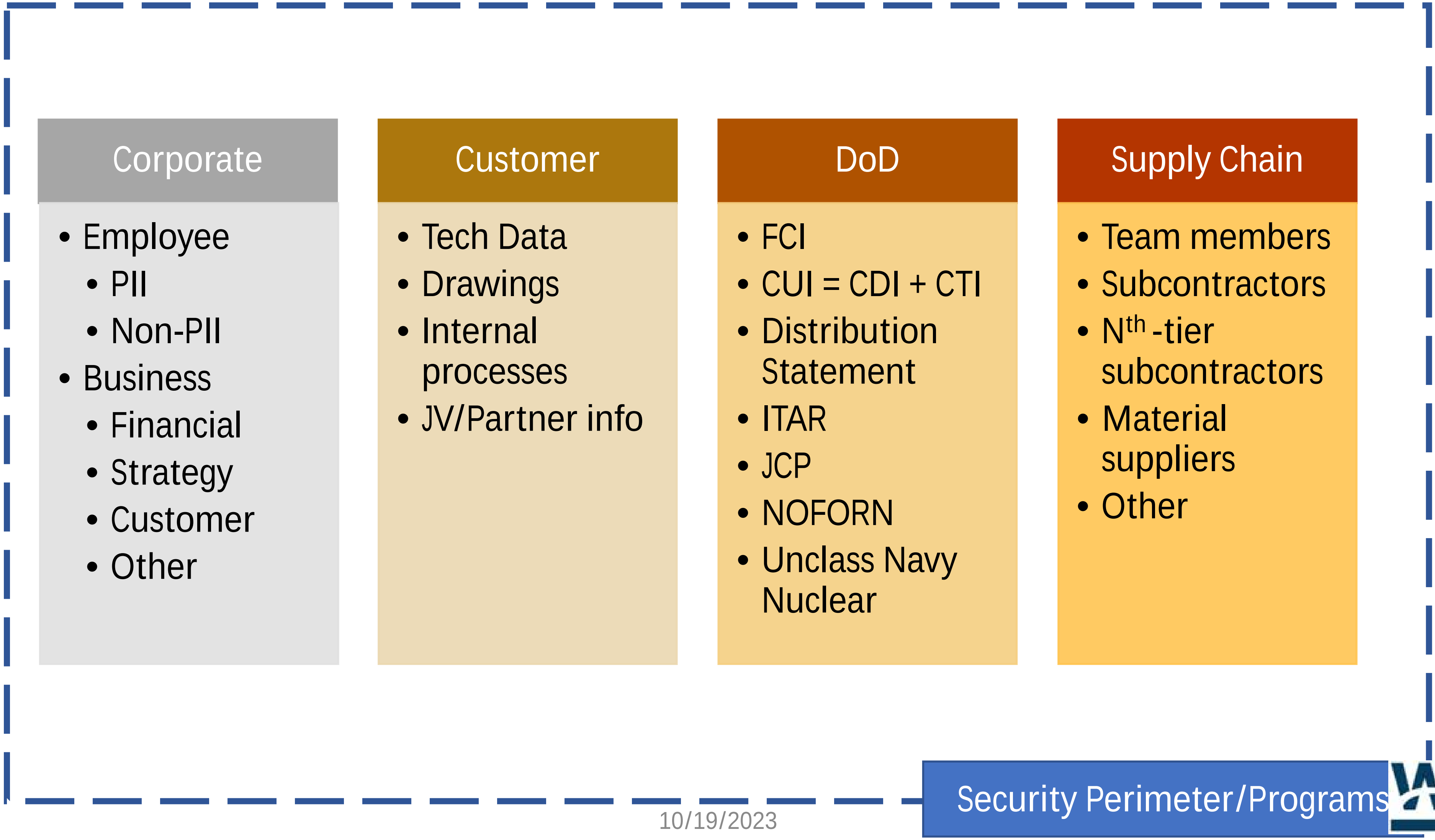
Information Flows



Considerations



General Information Sources



Corporate

- Employee
  - PII
  - Non-PII
- Business
  - Financial
  - Strategy
  - Customer
  - Other

Customer

- Tech Data
- Drawings
- Internal processes
- JV/Partner info

DoD

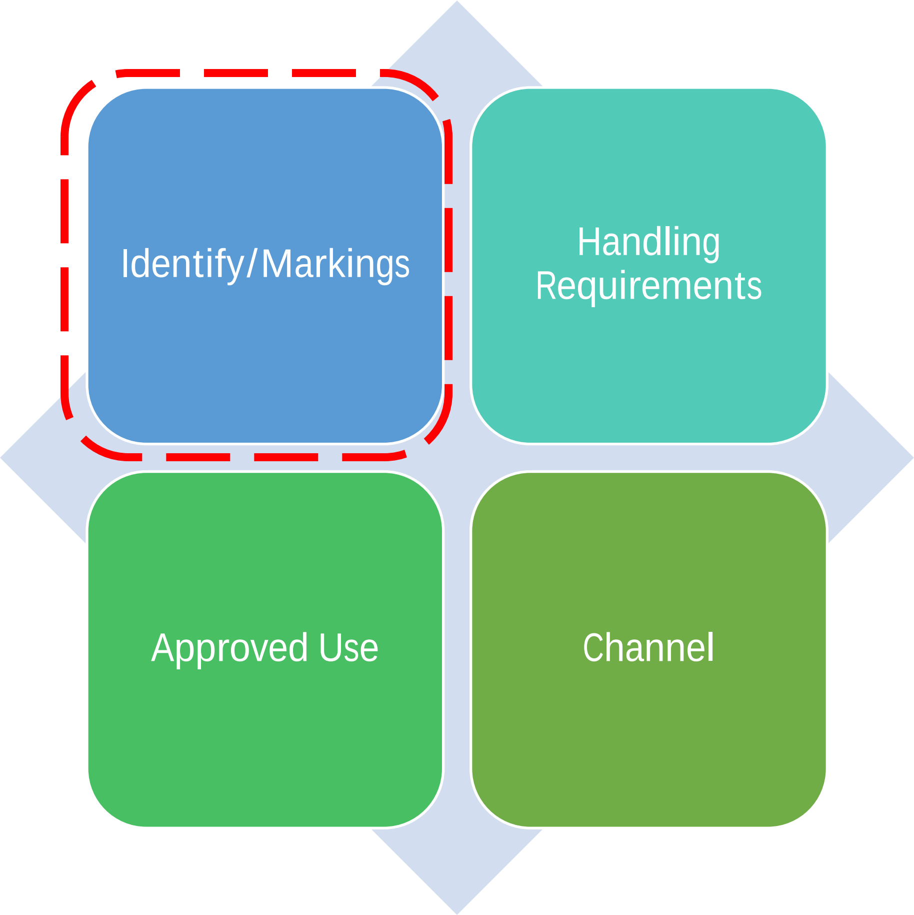
- FCI
- CUI = CDI + CTI
- Distribution Statement
- ITAR
- JCP
- NOFORN
- Unclass Navy Nuclear

Supply Chain

- Team members
- Subcontractors
- Nth -tier subcontractors
- Material suppliers
- Other

Security Perimeter/Programs

Information Handling Considerations



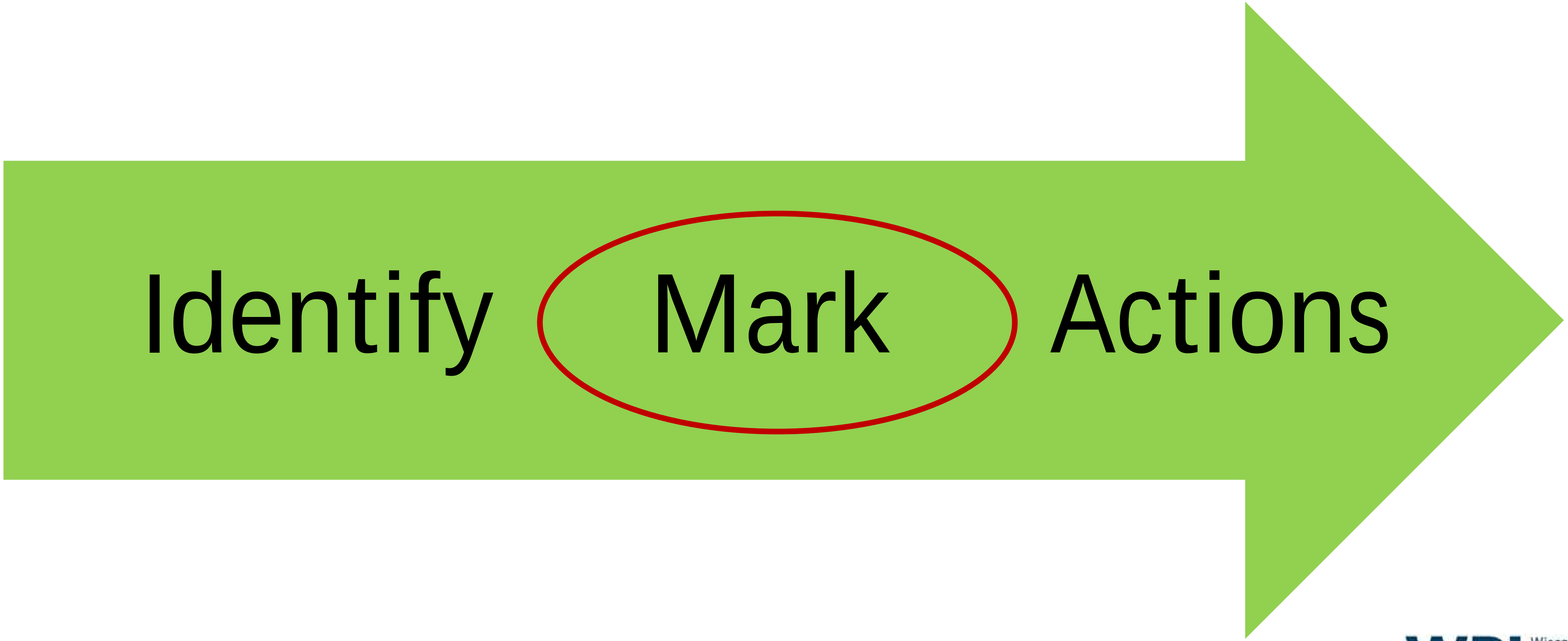
Identify/Markings

Handling Requirements

Approved Use

Channel

The Starting Point



Identify

Mark

Actions

Additional Considerations

- **What qualifies**
- Information life-cycle
- Registrations
- Company policies
- Company POC's
- Markings
- Storage
- Information Sharing Agreement
- Sharing
- Communication channels
- Retention
- Destruction
- Documentation
- Incident requirements
- Special considerations
- Training requirements

Information Sharing and System Interconnection Agreements

- As an example –
  - DFARS 252.204-7012 + NIST 800-171 r2 & DFARS 252.204-7019 and DFARS 252.204-7020 – DD2345 – DDTC ITAR -- …
  - Form the basis of a sharing agreement
  - DoD says, I will share information with you under these circumstances

  - These documents form or should form the basis of sharing agreements between Primes and Subcontractors/Suppliers and other tiers.
  - The sharing agreement should come first, not as an after thought.

Considerations for Information Sharing

- Company Proprietary Information
- Customer Proprietary Information
  - Commercial Customer
  - Government
- Supply Chain Background, Knowledge
  - What is known? – in general, specific
- Supply Chain: Information Sharing Agreement
  - Government generally specifies
  - Supplier agreements & subcontracting agreements should also specify

Sharing – Key Questions

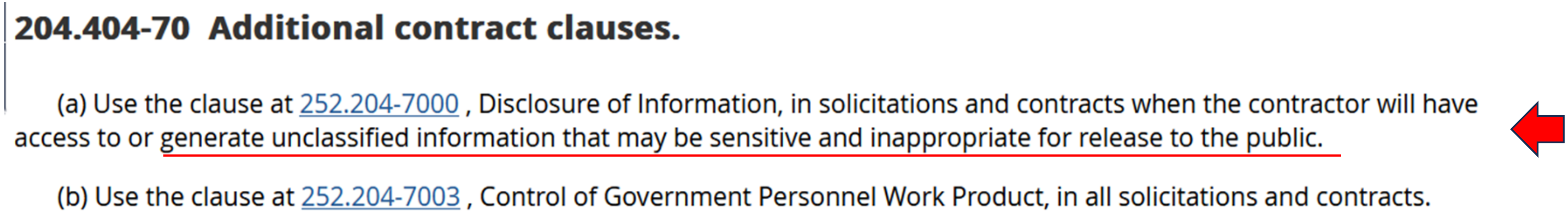
- What is the information?
- What are the requirements?
- Who is the recipient?
- What is the pathway?
- What procedure will be used? – coordination
- Has it been tested? Is there a periodicity?
- Was the test documented?

Sharing information – the critical question

- Is the recipient **eligible** to receive the type (category) of information being sent?
  - FCI – *Federal Contract Information -- Federal*
  - CUI – *Controlled Unclassified Information – Federal*
    - Is there a lawful governmental purpose?
    - Has the intended recipient met all required requirements? (SSP, POA, SPRS)
  - JCP – *Joint Certification Program - DoD*
    - Data Custodian to Data Custodian
  - ITAR – *International Traffic in Arms Regulation – Department of State*
    - U.S. Person to U.S. Person without license/other formal authorization
    - Full encryption (FIP 140-2) for email
      - Good overview with key ideas: https://www.nsa.gov/business/programs/export-control-policy/

** Requirements not inclusive

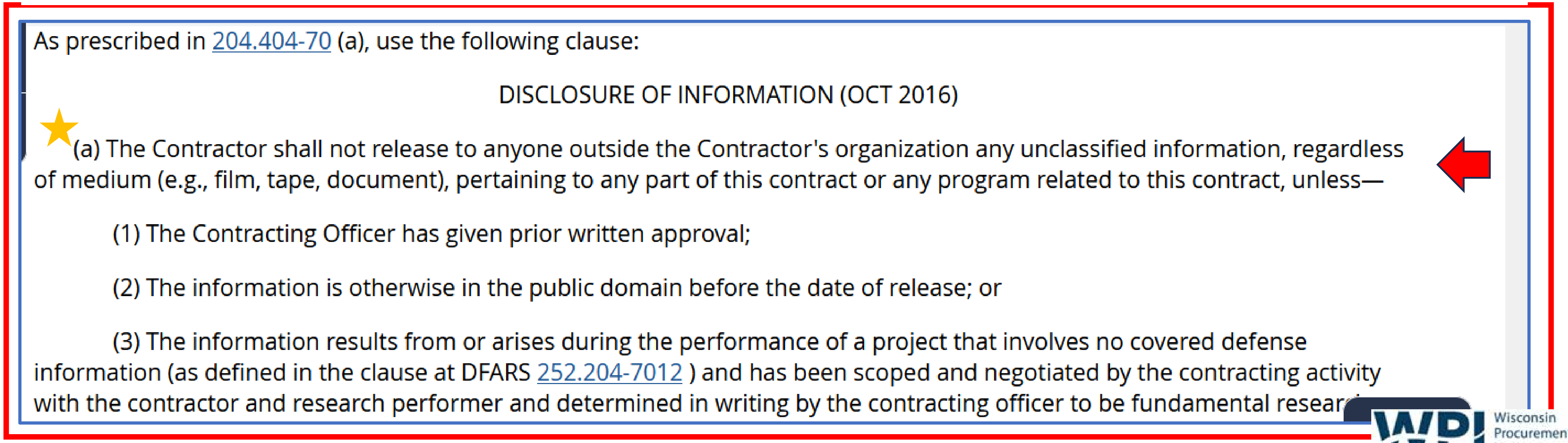
DFARS 252.204 -7000



204.404-70 Additional contract clauses.

(a) Use the clause at 252.204-7000 , Disclosure of Information, in solicitations and contracts when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate for release to the public.

(b) Use the clause at 252.204-7003 , Control of Government Personnel Work Product, in all solicitations and contracts.



As prescribed in 204.404-70 (a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

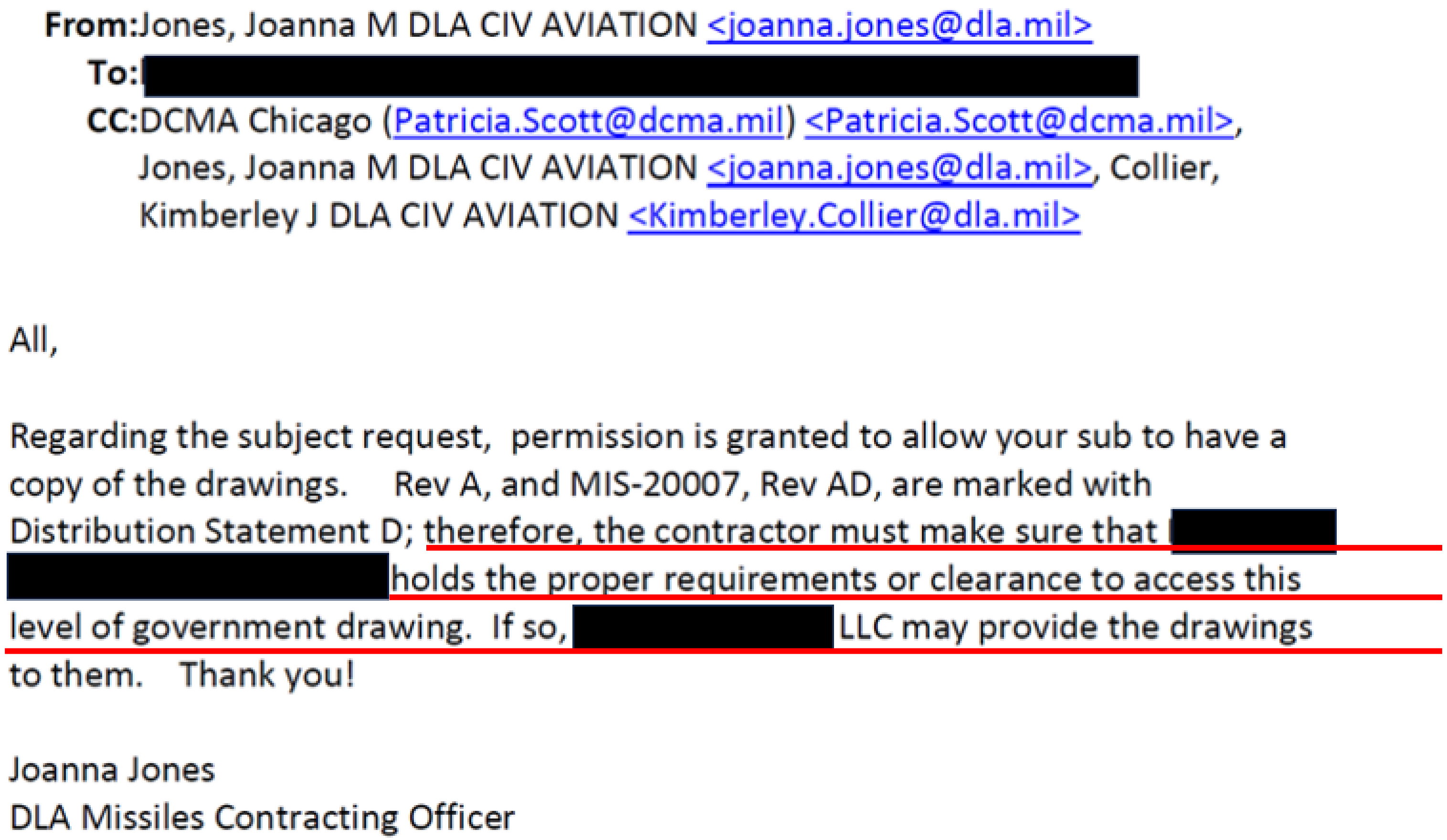
★ (a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(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) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental resear

Example Response to 252.204-7000 request



From: Jones, Joanna M DLA CIV AVIATION <joanna.jones@dla.mil>
To:[redacted]
CC:DCMA Chicago (Patricia.Scott@dcma.mil) <Patricia.Scott@dcma.mil>, Jones, Joanna M DLA CIV AVIATION <joanna.jones@dla.mil>, Collier, Kimberley J DLA CIV AVIATION <Kimberley.Collier@dla.mil>

All,

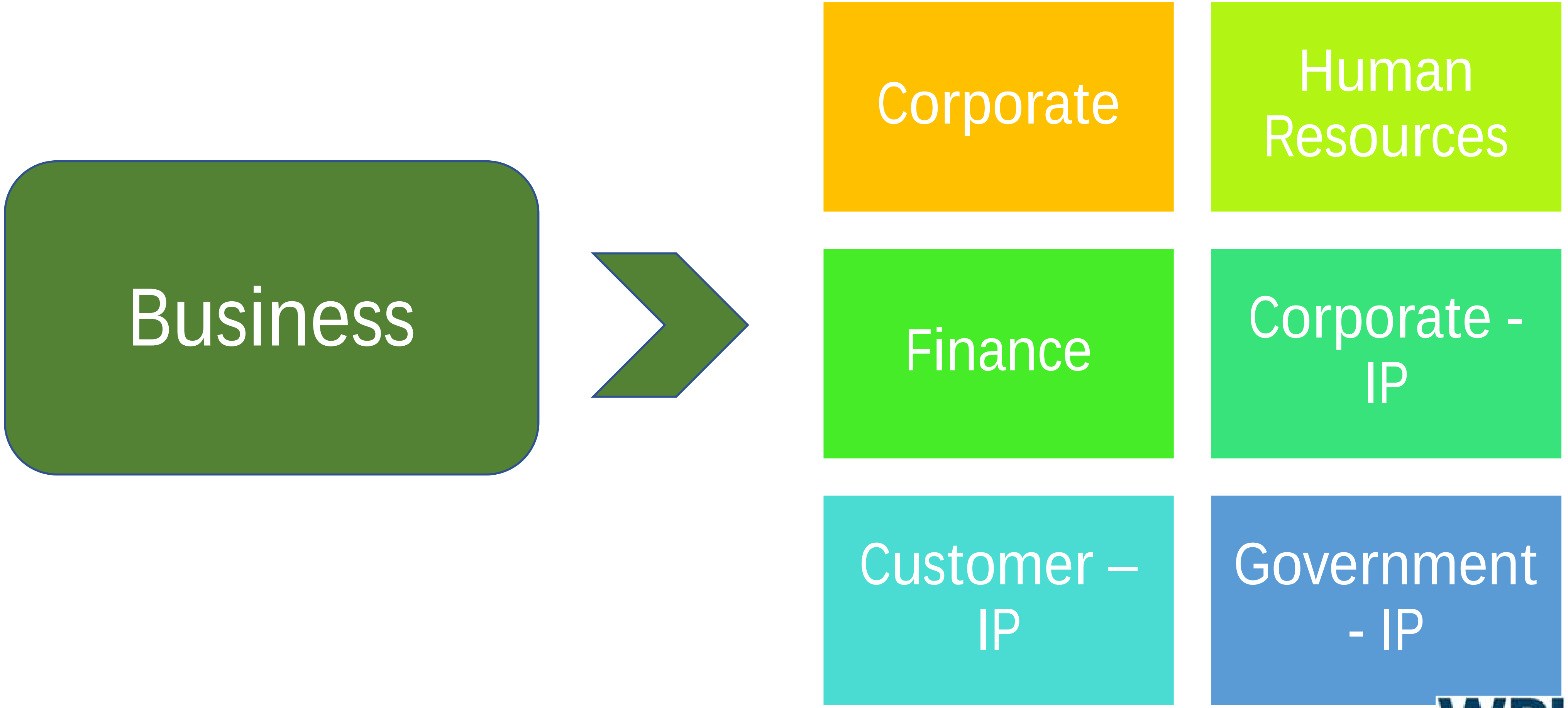
Regarding the subject request, permission is granted to allow your sub to have a copy of the drawings. Rev A, and MIS-20007, Rev AD, are marked with Distribution Statement D; therefore, the contractor must make sure that [redacted] holds the proper requirements or clearance to access this level of government drawing. If so, [redacted] LLC may provide the drawings to them. Thank you!

Joanna Jones
DLA Missiles Contracting Officer

Why speaking in code may be detrimental

- We speak in code – use acronyms
  - FAR
  - DFARS
  - Cyber
  - 7012 (252.204-7012)
  - NIST
  - The list goes on and on …

Business – the term v. reality



Clause Analysis – re:impact of using Codes

- Federal Contract Information (52.204-21)
- 15 requirements (only 15 – easy peasy -
- Includes the following two definitions
- *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).

FAR 52.204-21 para (xii)

- (xii) Identify, report, and correct *information* and *information system* flaws in a timely manner.
  - Appears to be straight-forward
  - Is it?

52.204-21 (xii) - analysis

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

1. Identify information flaws in a timely manner
2. Report information flaws in a timely manner
3. Correct information flaws in a timely manner

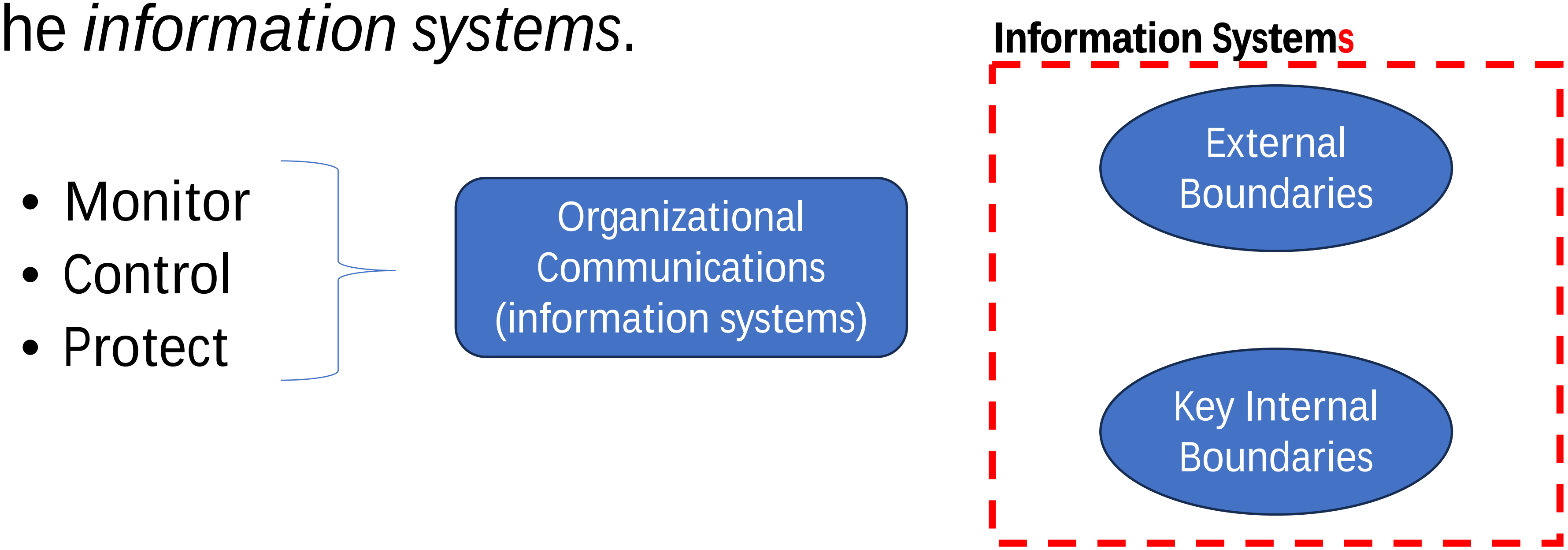
Information

4. Identify information system flaws in a timely manner
5. Report information system flaws in a timely manner
6. Correct information system flaws in a timely manner

Information system

Additionally -- 52.204-21 Para (x)

- Monitor, control, and protect organizational communications (*i.e.*, *information* transmitted or received by organizational *information systems*) at the external boundaries and key internal boundaries of the *information systems*.



- Monitor
- Control
- Protect

Organizational Communications (information systems)

Information Systems

External Boundaries

Key Internal Boundaries

Looking beyond code (re: speaking in code)

- 252.204-7012 paragraph (l)
- *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.
- 252.204-7012 is synonymous with CUI but paragraph (l) pertaining to its unclassified information systems is not dependent upon CUI!

Federal Contract Information

- FAR 52.204-21 - **Basic Safeguarding of Covered Contractor Information Systems.**
- *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 websites) or simple transactional information, such as necessary to process payments.
- *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).

Federal Contract Information

- FAR 52.204-21 - **Basic Safeguarding of Covered Contractor Information Systems.**
- **A closer look -**
- *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,

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 paragraph 5.8

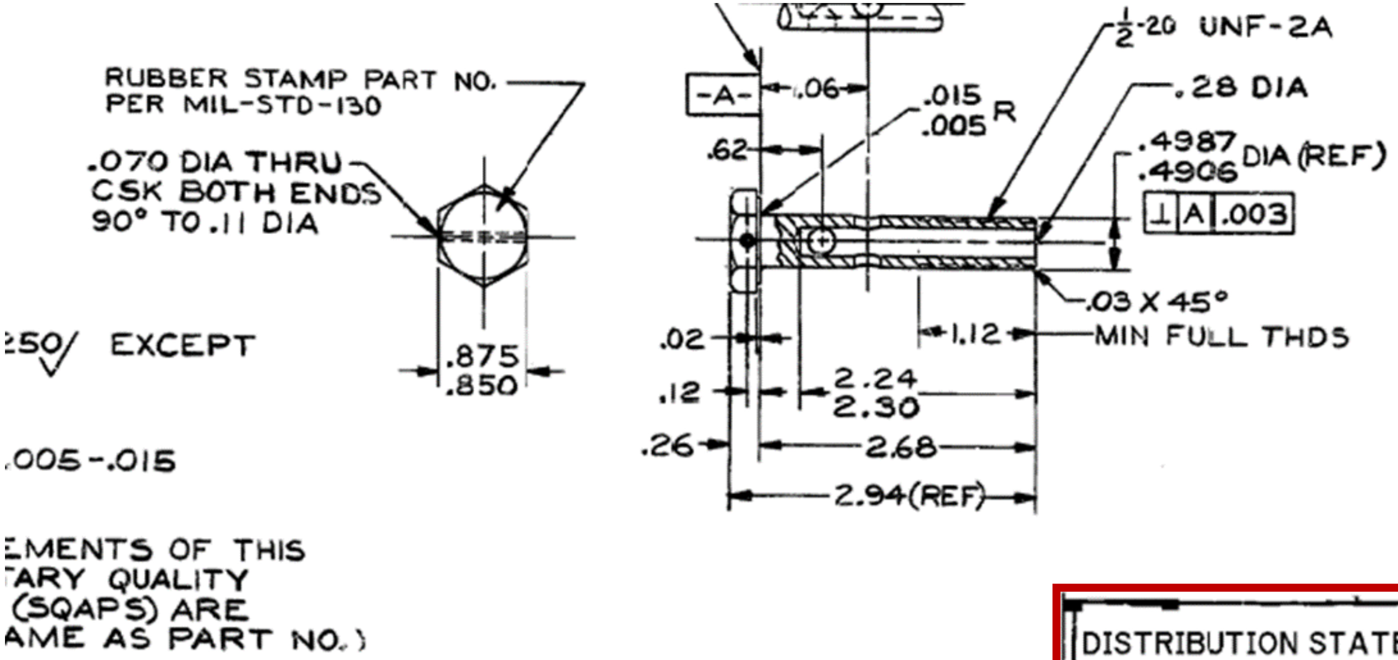
https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/523025p.pdf

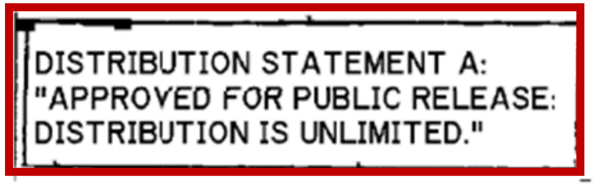
Distribution Statements – as an example

- 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 controlling office

DoDI 5230.24, August 23, 2012 Change 3, 10/15/2018

Distribution Statement A - example




DISTRIBUTION STATEMENT A:
"APPROVED FOR PUBLIC RELEASE:
DISTRIBUTION IS UNLIMITED."

Attachment to client email

Distribution Statement B

- Administrative or Operational Use
- Contractor Performance Evaluation
- Critical Technology
- Export Controlled
- Foreign Government Information
- Operations Security
- Premature Dissemination

DoDI 5230.24, August 23, 2012 Change 3, 10/15/2018; Table 1
Reasons to Assign Distribution Statement B

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]

May be part of ITAR but may also be a cautionary idea.

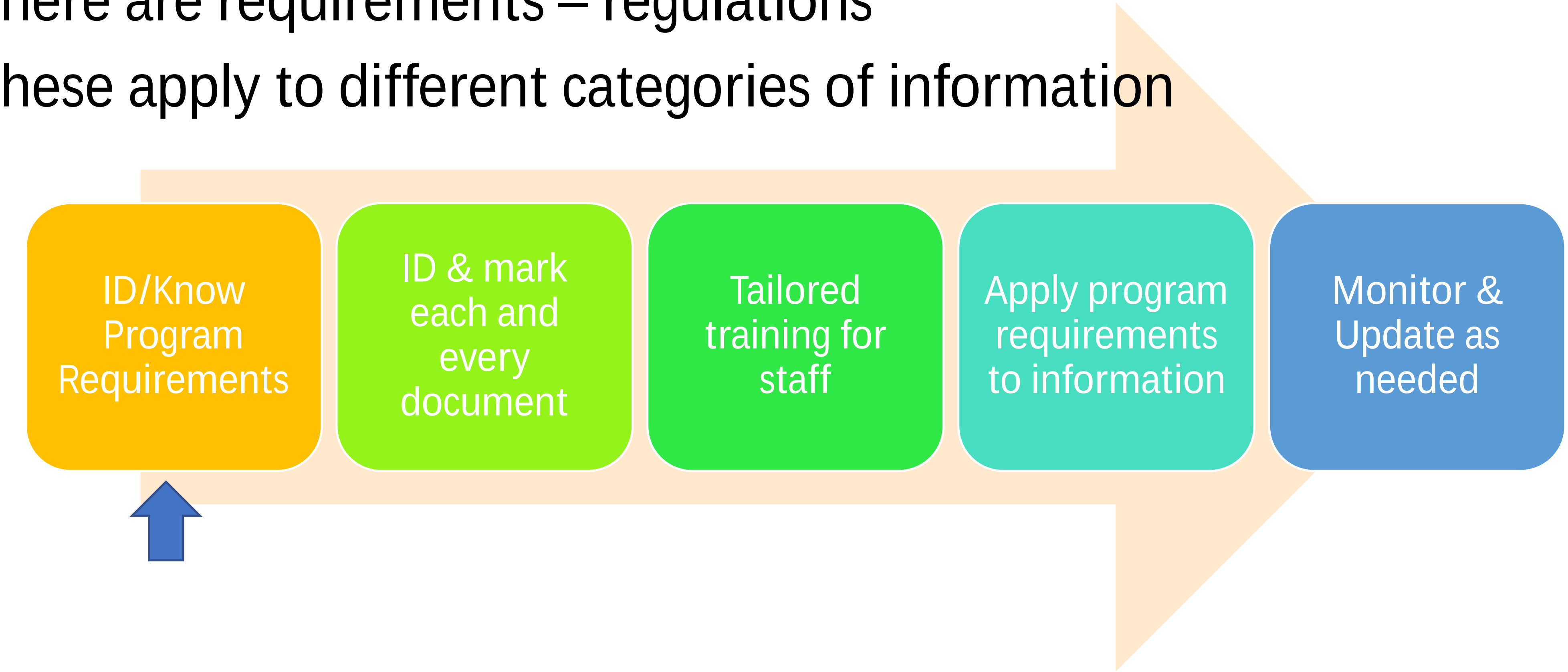
22 CFR §120.50 https://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.57&rgn=div5#se22.1.120_150

Information Security - considerations

- Confidentiality
- Integrity
- Availability

Information Management (digital & physical)

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



ID/Know Program Requirements

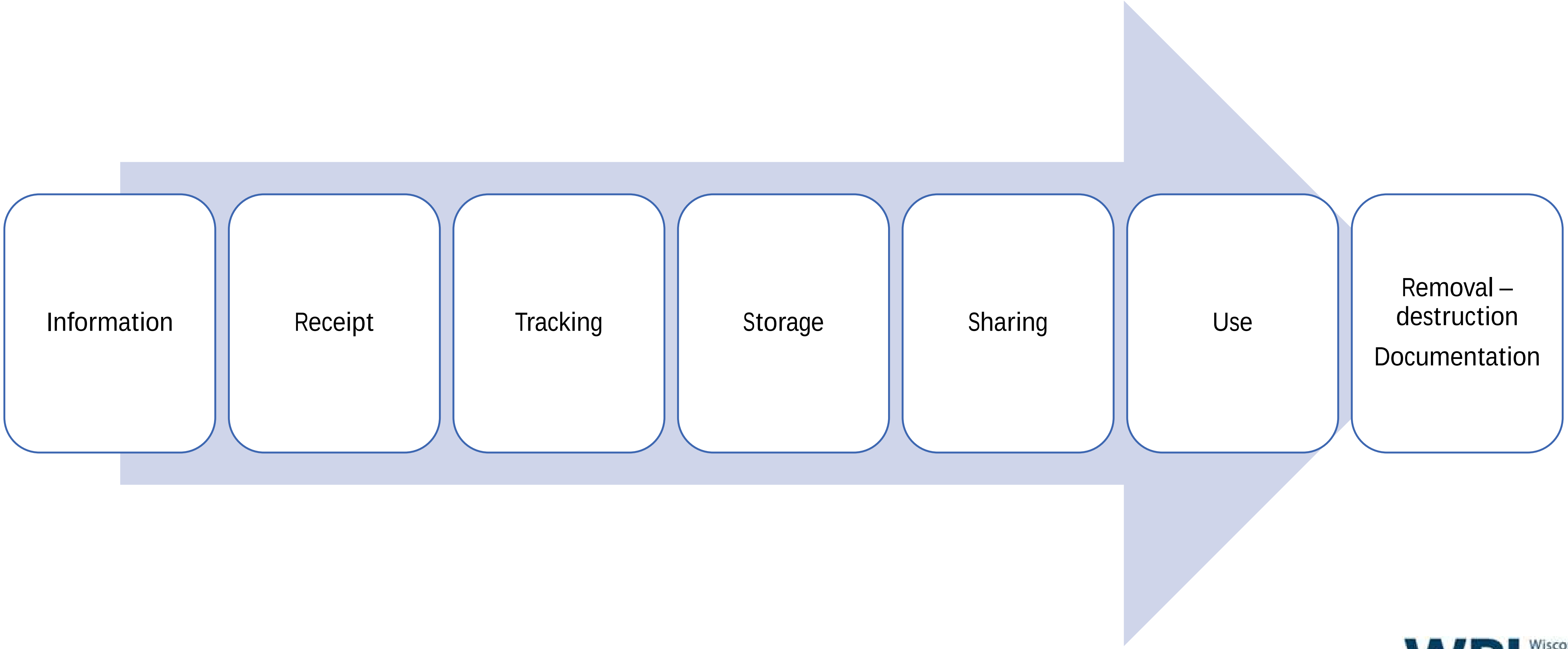
ID & mark each and every document

Tailored training for staff

Apply program requirements to information

Monitor & Update as needed

Information usage lifecycle



Information

Receipt

Tracking

Storage

Sharing

Use

Removal – destruction

Documentation

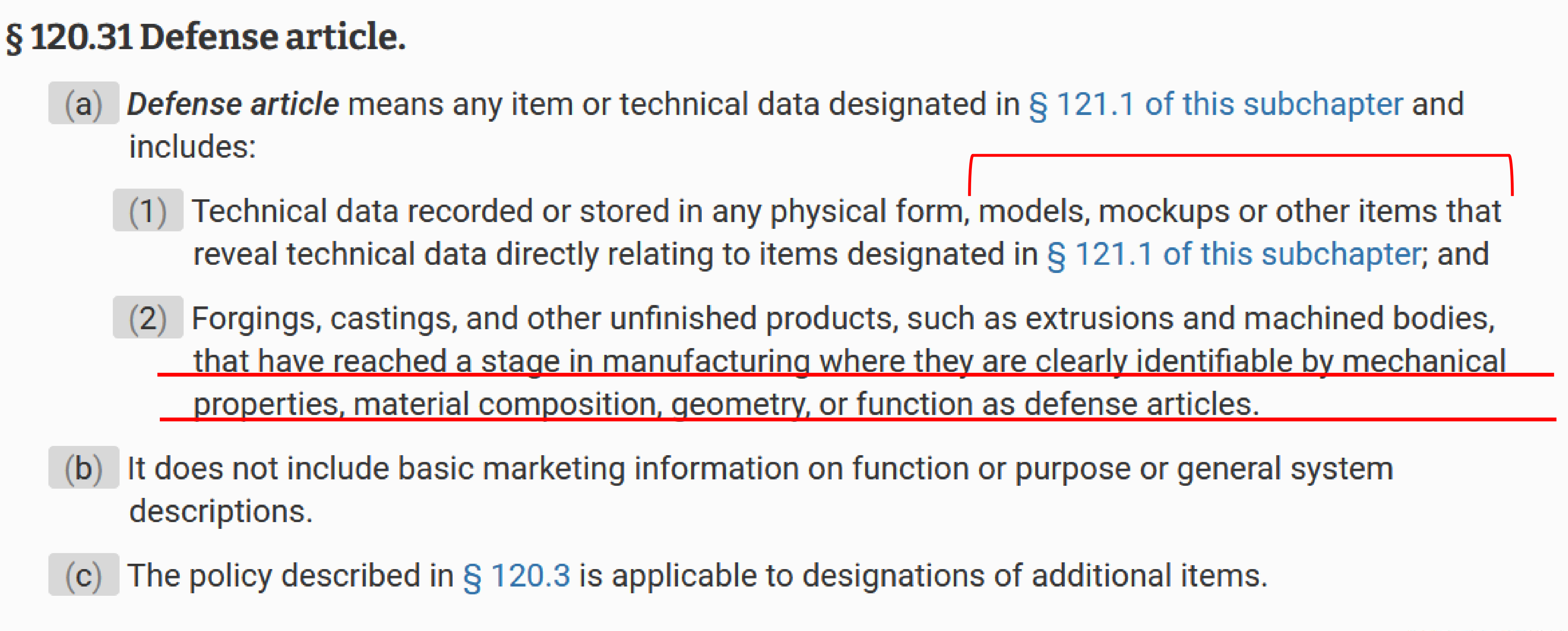
Information Pathways – the importance

- Human
- Physical
- Digital
- Human/Physical
- Human/Digital

Information Flows (Pathways)

- Digital – email/FTP/other
- In person
  - Meeting
    - Discussion
    - RFP review
    - Drawing review/sharing
  - Shop visit
  - Conference
  - Webinar
- Physical
  - Model / Mock-up / Machined Item
  - USPS

Mock-ups / Scrap / Models / etc



§ 120.31 Defense article.

(a) *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

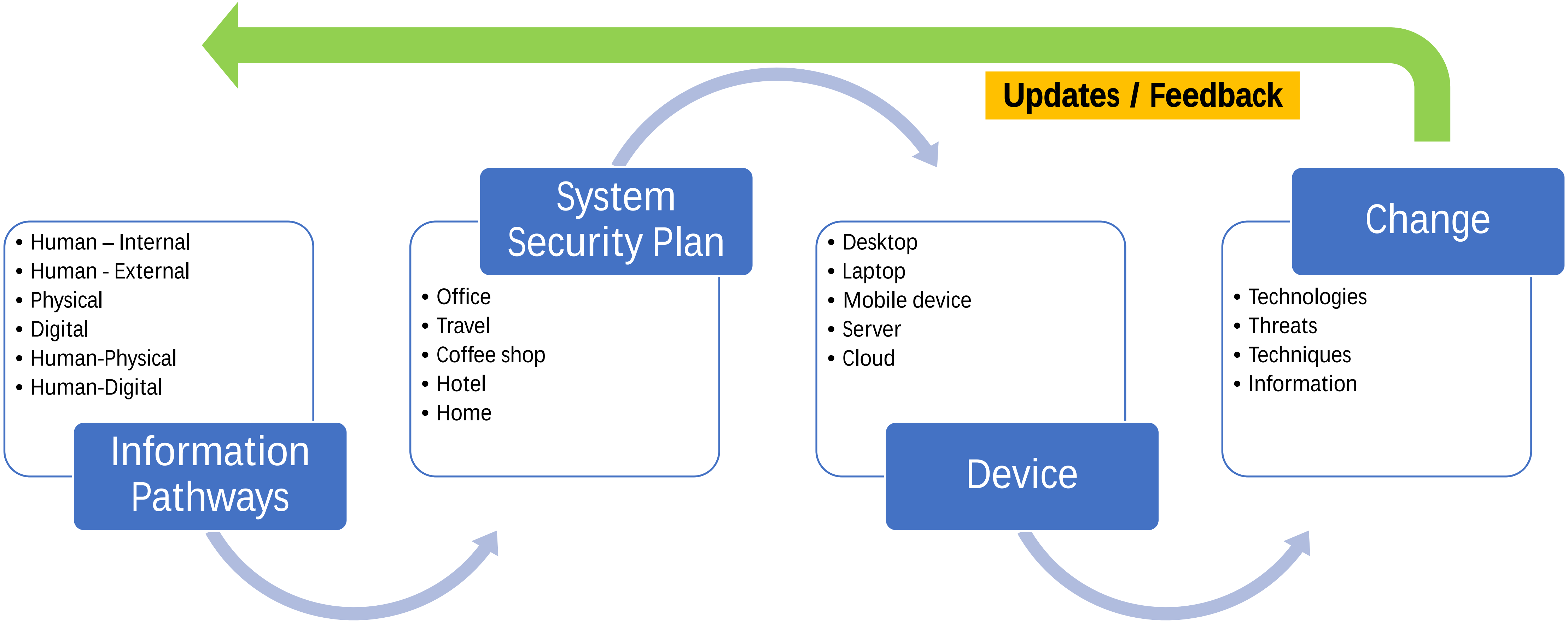
(2) Forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.

(b) It does not include basic marketing information on function or purpose or general system descriptions.

(c) The policy described in § 120.3 is applicable to designations of additional items.

https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120

Dynamic/Evolving Environment



Updates / Feedback

Information Pathways

- Human – Internal
- Human - External
- Physical
- Digital
- Human-Physical
- Human-Digital

System Security Plan

- Office
- Travel
- Coffee shop
- Hotel
- Home

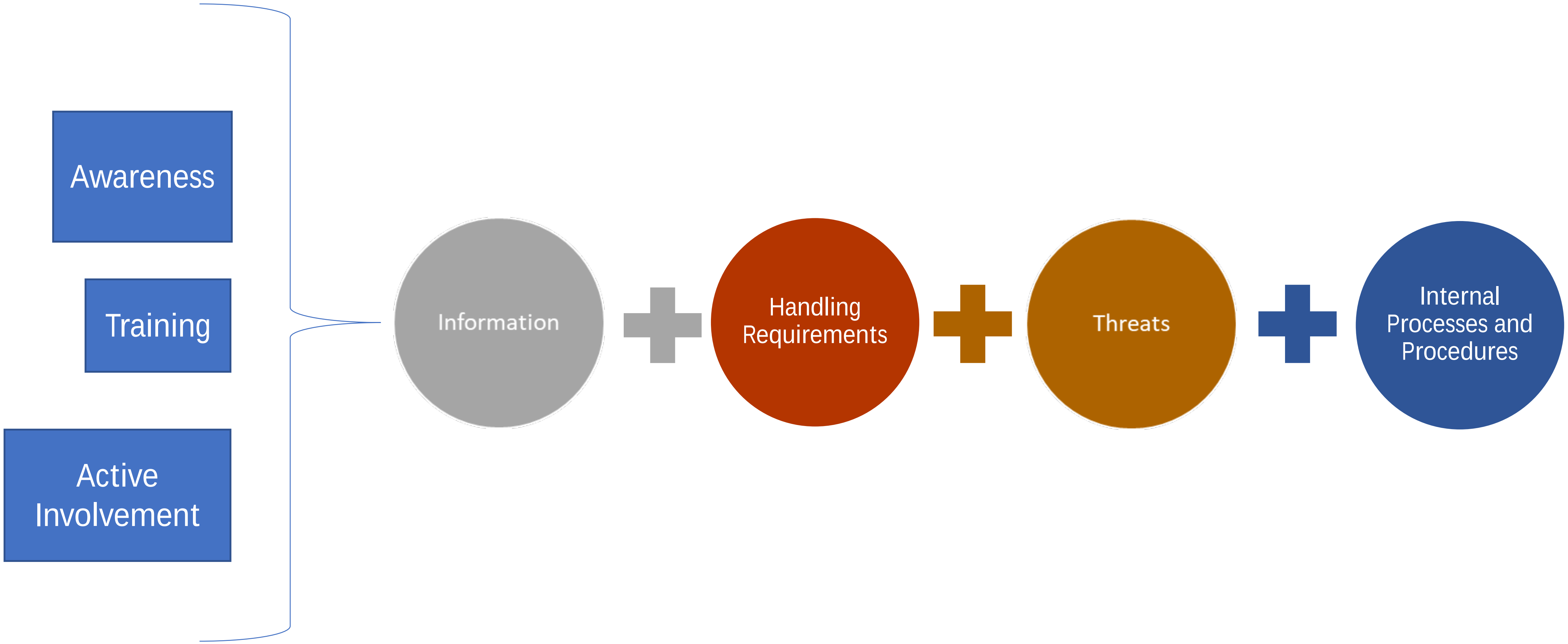
Device

- Desktop
- Laptop
- Mobile device
- Server
- Cloud

Change

- Technologies
- Threats
- Techniques
- Information

Awareness = mindset



Reportable incidents

- Have you defined what is and is not a reportable incident for each type of information held, processed and/or transmitted?
- Are there policies/procedures in place?
- Who is responsible for determining when a reportable incident has occurred?
- Is there a checklist?
- Are the necessary resources for forensic evidence collection available?
- Has the company created formatted reports?

Incidents is there a plan – a process/procedure?

- What happened?
- When did it happen?
- How (why) did it happen?
- How was the incident identified?
- How long did it take to identify?
- Was the causative factor known, being watched or unknown?
- Has the access pathway been remediated?
- Is the remediation – permanent or stop-gap?
- Is the remediation being monitored?

Protection Schemes - Requirements

- Driven by the owner’s requirements
- Driven by the type of (category of) information
- There are some generally accepted principles
- There is no single set of actions that apply to all types of information

Handling concepts

- Responsible party
- Centralized
- Inventory
- Marked
- Managed
- Sharing – log, serialized
- Copy creation – log, serialized
- Destruction – appropriate method, documentation, which documents
  - Witness,

Sharing

1

Identify information type

2

Identify information sharing requirements

3

Identify recipient

4

Validate recipient is eligible to receive the type of information

- Vetting of Suppliers and Subcontractors

Information - lifecycle

- Creation – Contract documents – Supplier – Sub K
- Mark (ID) per company policies/procedures
- Inventory - record creation and management
- Storage – physical/digital security requirements
- Use – access controls (authorization, use management)
- Contract file – appropriate annotations
- Sharing – requirements, DFARS 252.204-7000, per owner
- Destruction – appropriate method
- Inventory – update; removal

Information Flows

- US Mail
- Hand carried
- Conference, outreach, meetings …
- Derivative
- Aggregation
- Digital
- Staff
- Suppliers/Subcontractor

Items to review, watch for

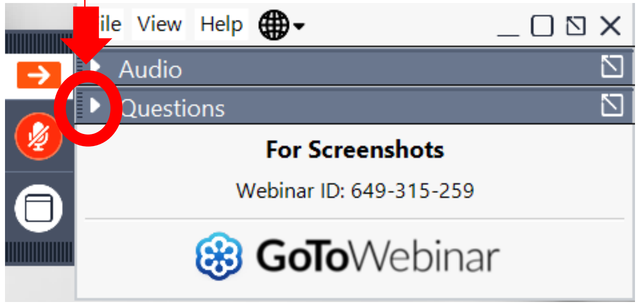
- Cyber attacks / Ransomware / Malware

- DFARS 252.204-7012 → CMMC
- DOJ efforts → Civil Cyber-Fraud initiative
- 52.204-21 → New unifying FAR Cyber Clause
- SEC reporting requirements – Johnson Controls & Simpson
- CISA reporting requirements
- Pending Executive Order
- Joint NSA / CISA Advisory

QUESTIONS?

OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



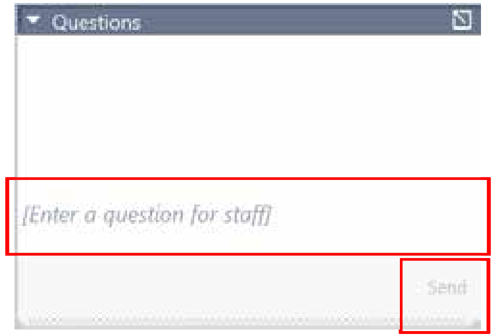
For Screenshots

Webinar ID: 649-315-259

GoToWebinar

USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 8
  Preparing for One-on-One Buyer Meetings

- November 15
  Preparing a Winning Government Proposal

- December 12
  The HUBZone Program – Certification Benefits and Regulations

- December 13
  Analyzing and Responding to Federal Construction Solicitations

…More information and registrations at wispro.org/events

GOVERNMENT CERTIFICATION WORKSHOPS

- October 12
  Federal Certifications
- October 26
  Local Certifications
- November 30
  State Certifications

MADISON
AREA | TECHNICAL
COLLEGE

MATC Goodman-South Campus
2429 Perry Street, Madison, WI 53713

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

CYBER FRIDAY LIVE WEBINAR SERIES

- October 27

  NIST SP 800.171 – 3.9 Personnel Security and 3.10 Physical Protection

- November 3

  NIST SP 800.171 – 3.11 Risk Assessment and 3.12 Security Assessment

- November 9 (Thursday)

  NIST SP 800.171 – 3.13 System and Communications Protection and 3.14 System and Information Integrity

PRESENTED BY

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
Cyber Friday

TECHNOLOGY
INNOVATION CENTER
at RESEARCH PARK

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

Registration Now Open

The Contracting Academy

Developing and Growing Government Contractors

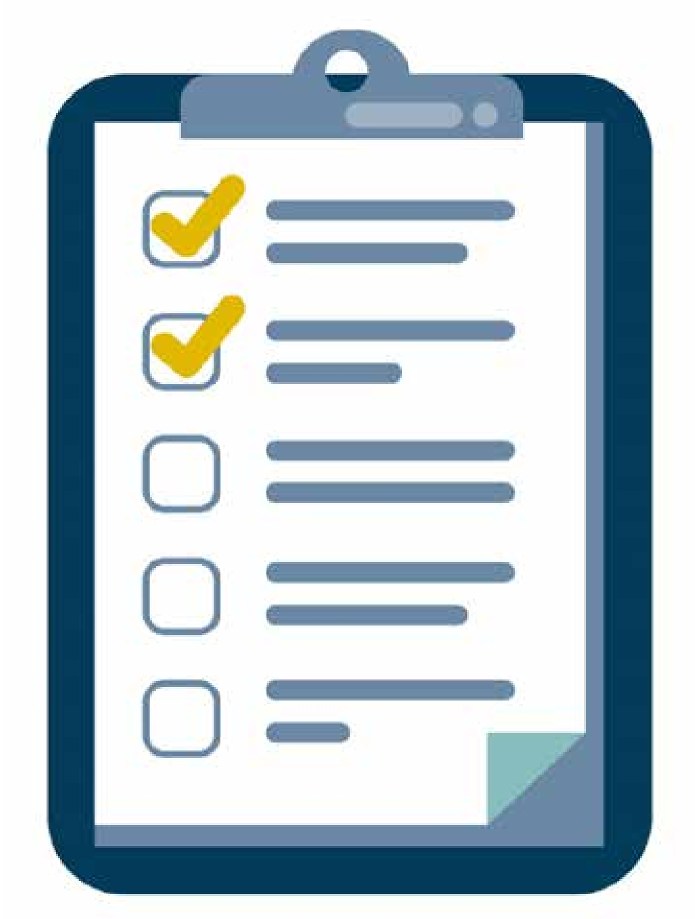
WISCONSIN ECONOMIC DEVELOPMENT
MARKETPLACE WI
GOVERNOR'S CONFERENCE ON DIVERSE BUSINESS DEVELOPMENT
DEC. 5, VIRTUAL | DEC. 6-7, IN PERSON
IN PERSON AT THE BAIRD CENTER, MILWAUKEE

December 5-7, 2023

MarketplaceWisconsin.com

October 19, 2023

SURVEY



CONTINUING PROFESSIONAL EDUCATION

NCMA®

NATIONAL CONTRACT MANAGEMENT ASSOCIATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:
Jack Laufenberg
jackl@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante

Wisconsin Procurement Institute
marcv@wispro.org | 920-456-9990

10437 Innovation Drive Suite 320
Milwaukee WI 53226