Emerging Issues:

Foreign Ownership, Control, and Influence (FOCI)

November 30| 1:00 – 2:00 pm

Presented by:

Marc Violante, WPI

Webinar Etiquette

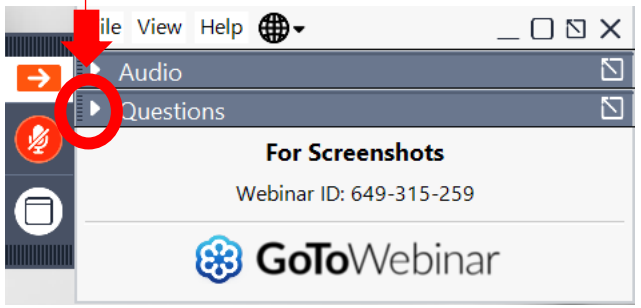
PLEASE

- § 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!

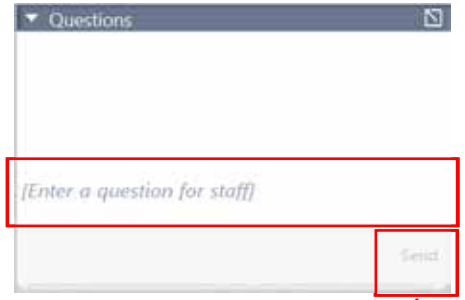
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute

APEX ACCELERATORS

Assisting Wisconsin businesses compete in the government marketplace.

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.

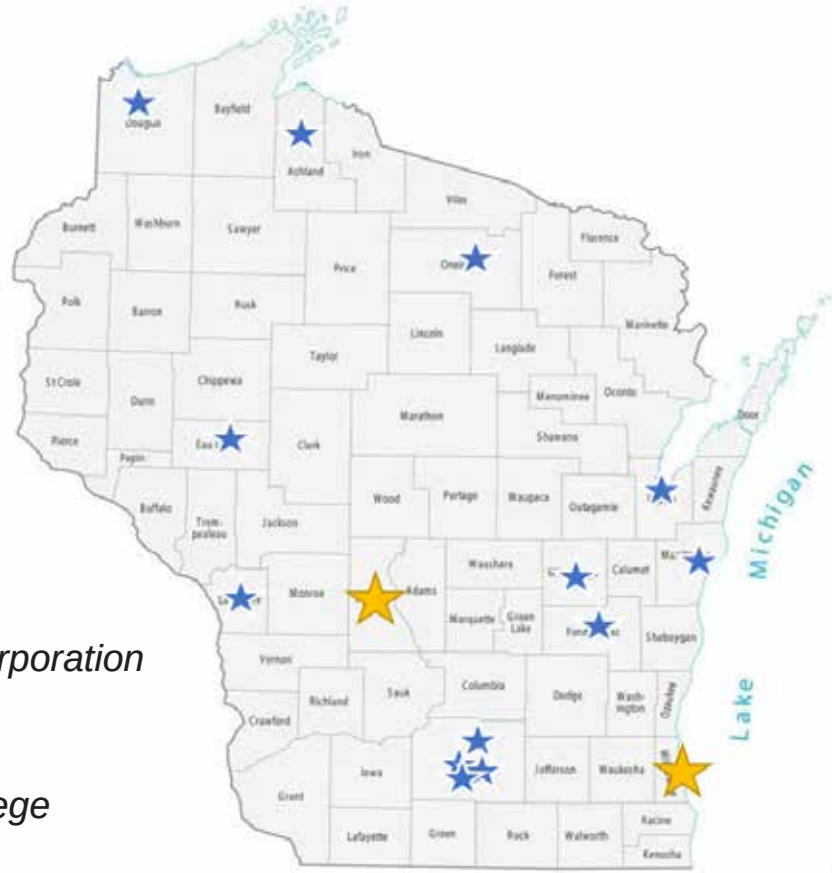
WPI provides services to all of Wisconsin's 72 counties

- 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

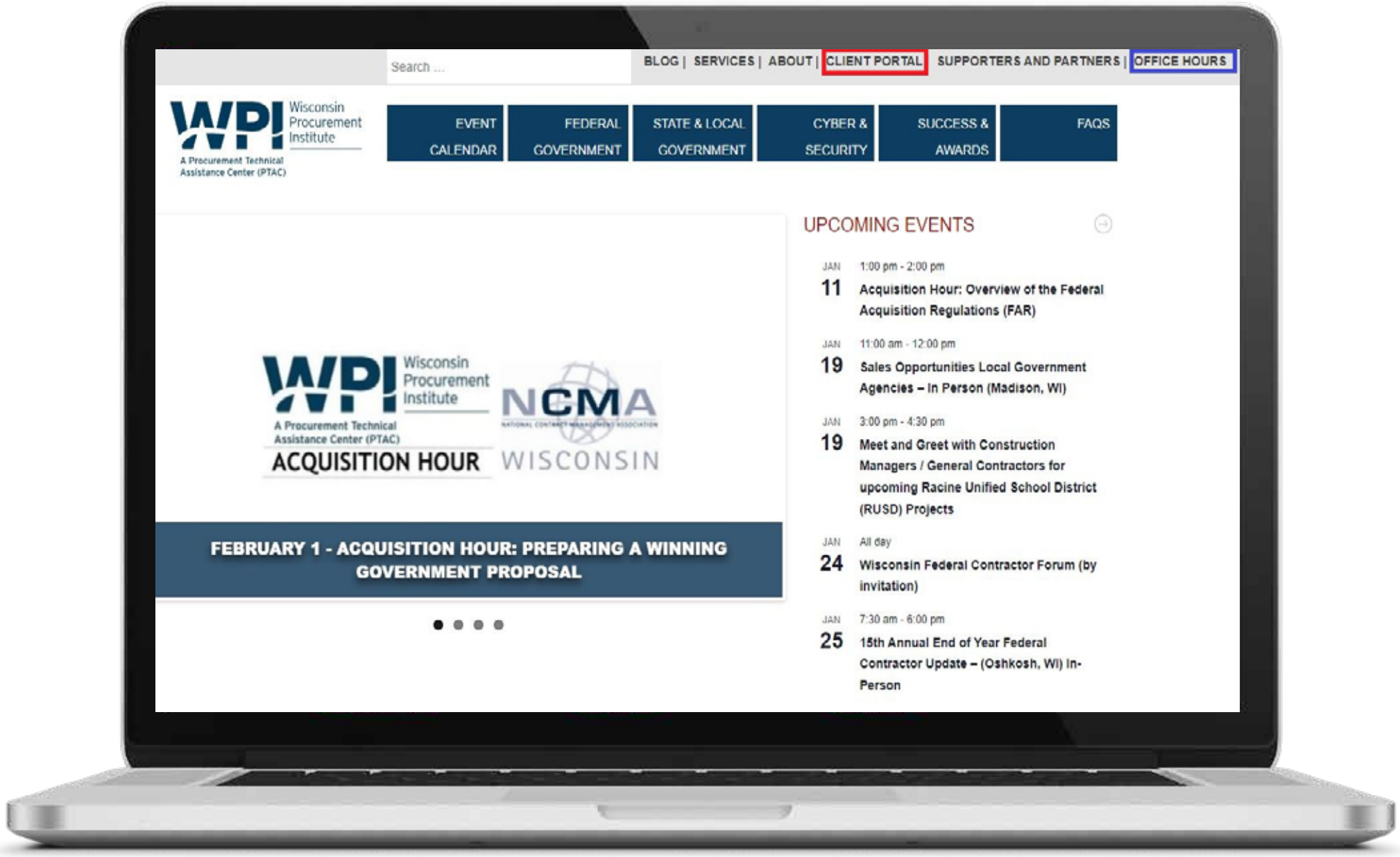
- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **CAMP DOUGLAS**
  - *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*



WPI Wisconsin Procurement Institute

February 1, 2024

NCMA WISCONSIN


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 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

Sharing Sensitive Information (CUI, JCP, ITAR)

Marc N. Violante

Wisconsin Procurement Institute

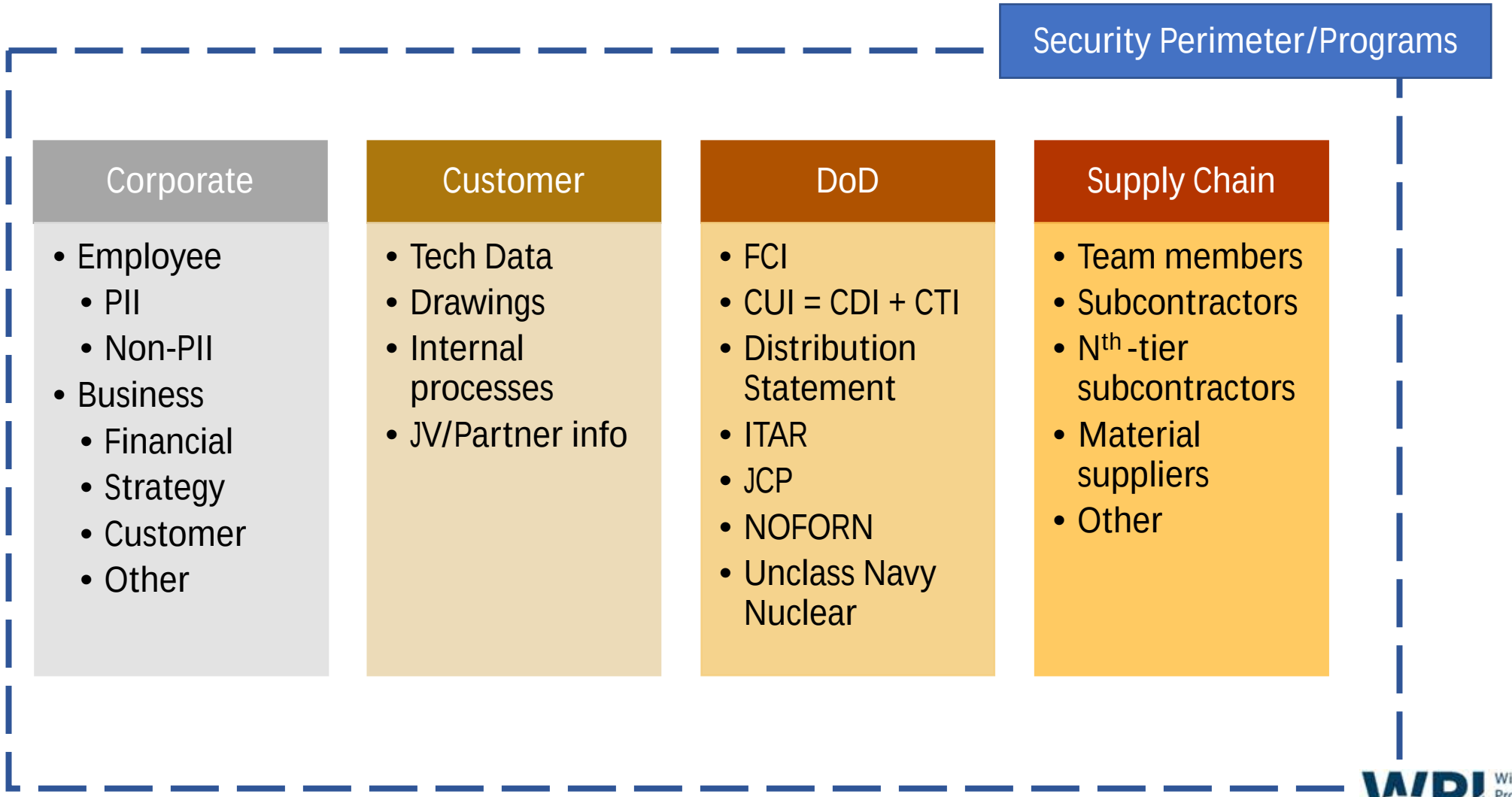
February 1, 2024

One inadvertent click is all it takes

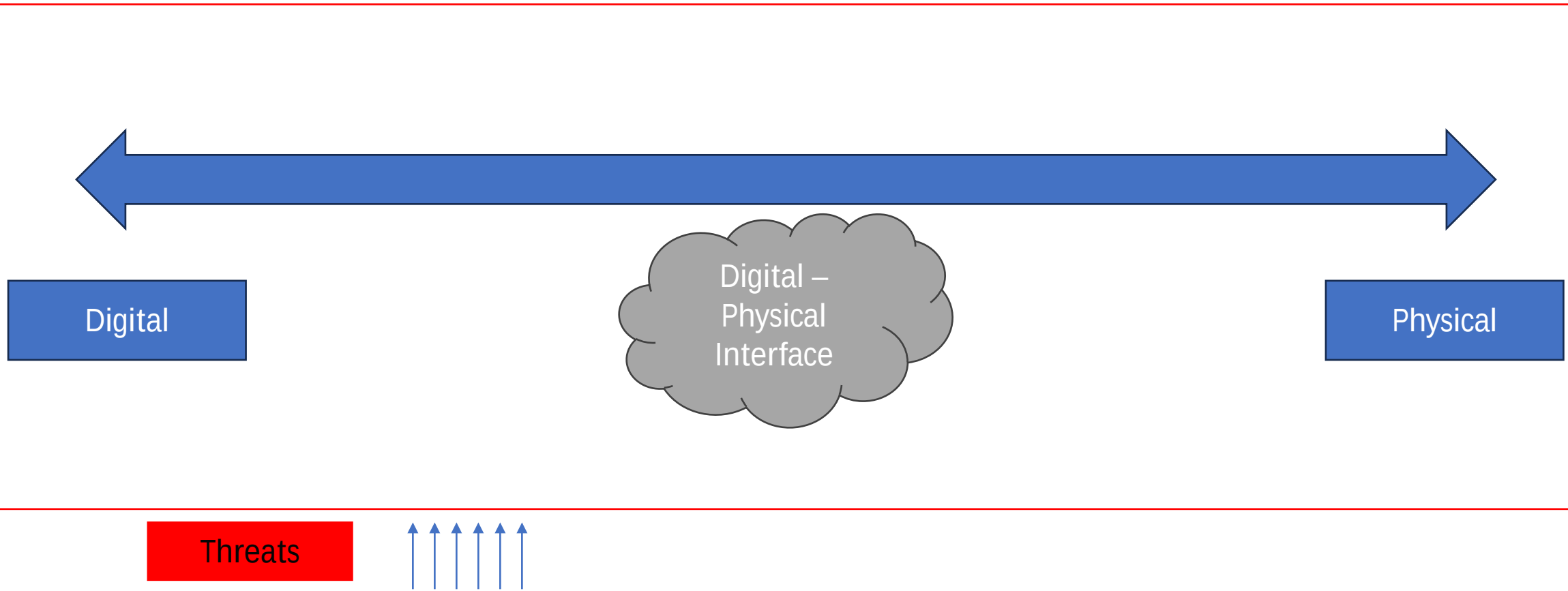
Information Loss

https://www.energy.gov/energysaver/thermographic-inspections

General Information Sources



Information Continuum



Information Sharing

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

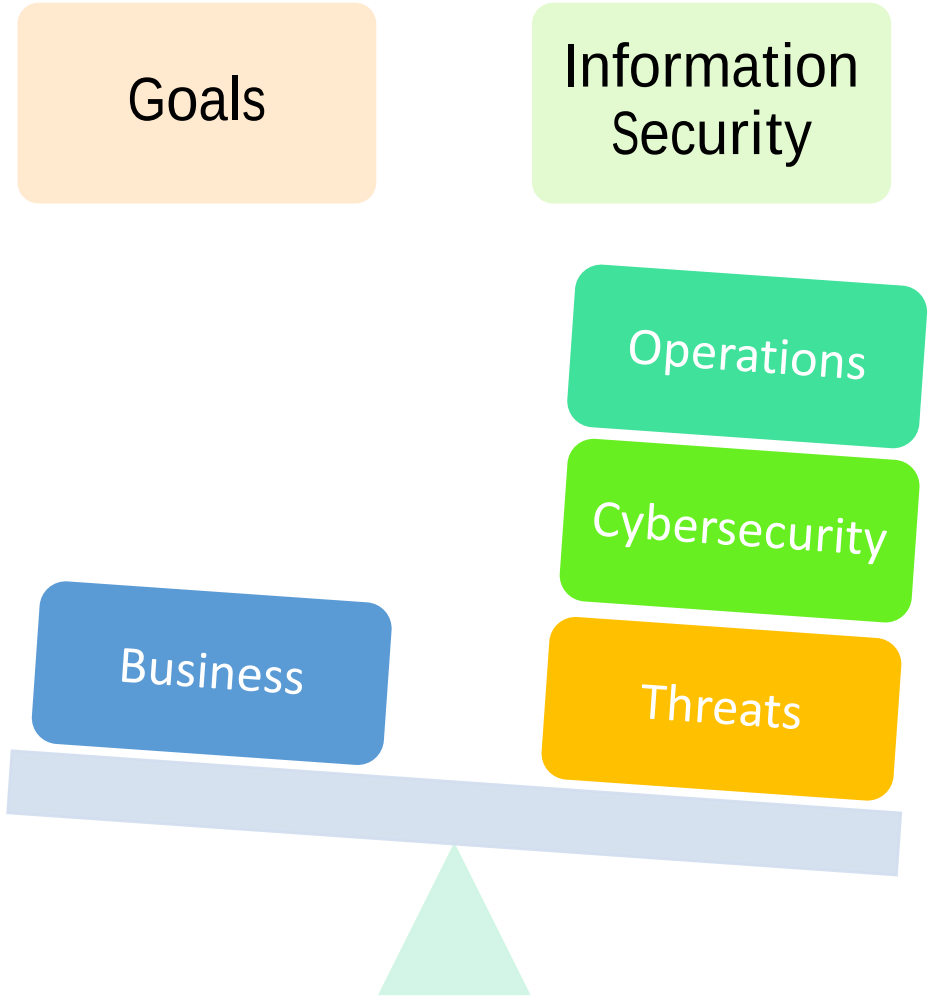
Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

NIST 800-171 r2; final, Protecting Controlled Unclassified Information, pg 6 **Note**: NIST 800-171 r1 to be withdrawn Feb 21, 2021

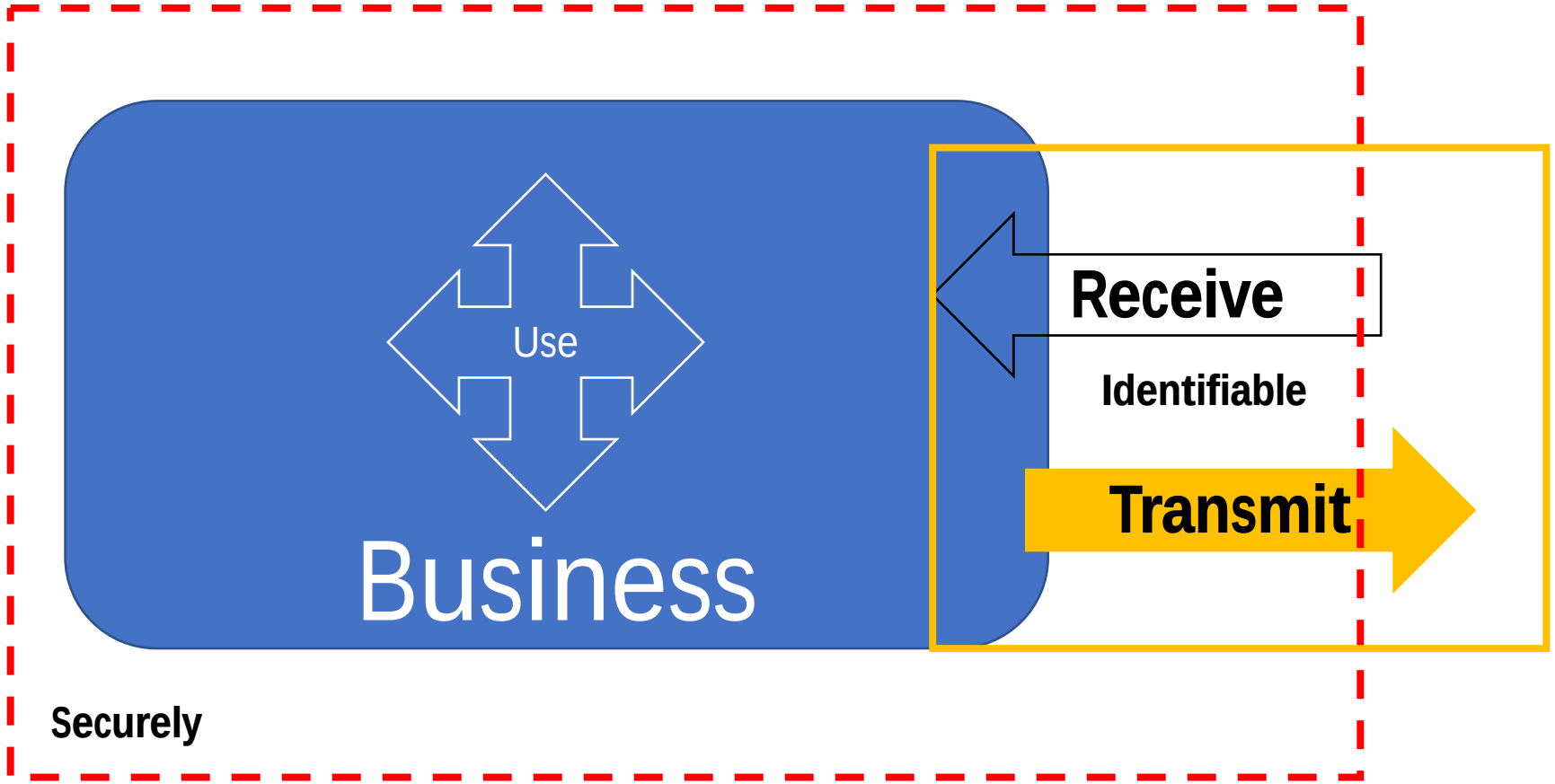
Start with the end in mind

Pick an approach for success!

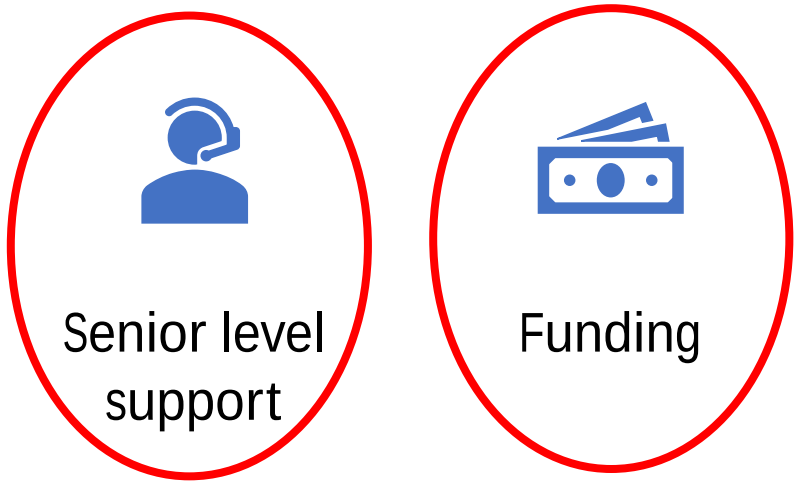
Business Environment



Information – “life blood”



Identify key elements- what is needed?



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

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.

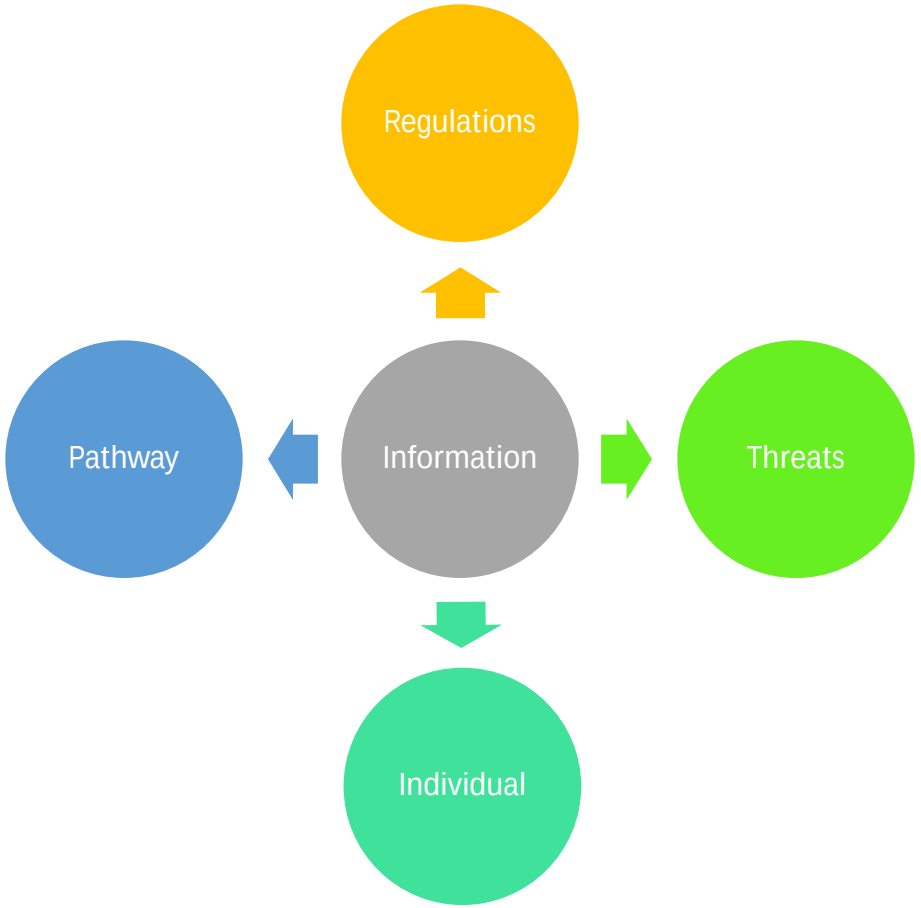
(c) The policy described in § 120.3 is applicable to designations of additional items.

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

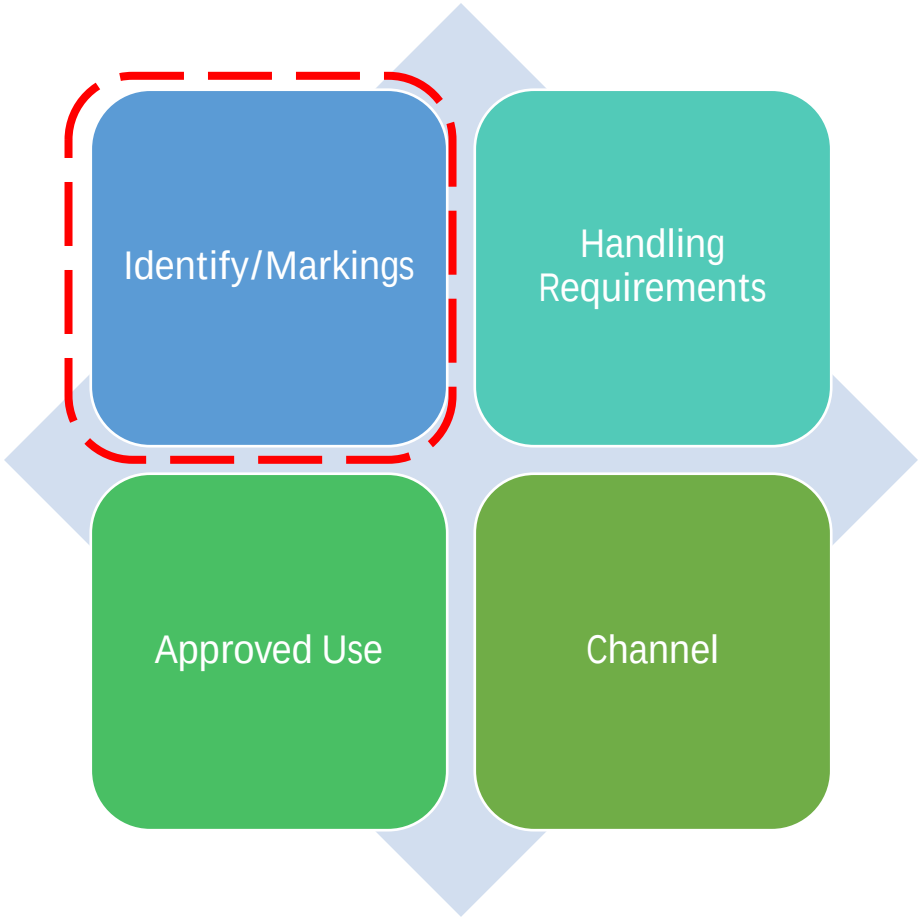
Information Security – the issue

What security controls are needed for these documents?

Sharing Sensitive Information



Information Handling Considerations



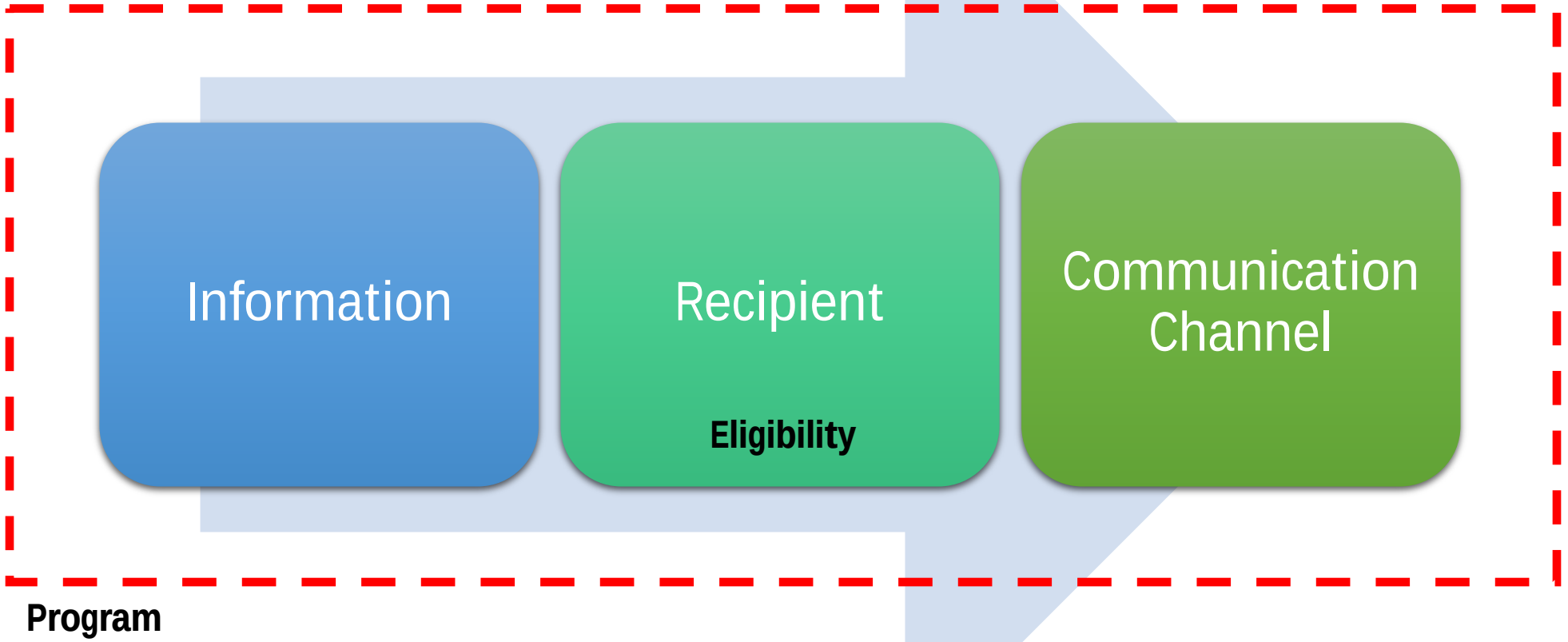
General Security Framework

- Awareness of security requirements
  - Information
  - Business framework – current
- Awareness of the presence of and type of information
  - CUI | Export Controlled (JCP/ITAR/NOFORN)
- Ability to know where the information is at a point in time
  - Who has access to the information
  - Who has accessed/used/using the information

Access Lists
Logs

Policies formal appointment – Data Custodian, Procedures (check in/out), logs

Sharing – general framework



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.

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**

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

The W’s of Information handling

- What information do we have?
- What information do we use?
- With whom is information being shared?
- What information is being shared?
- What are the handling requirements?
- Where – how is the information being shared?
- When – normal hours / off hours
- Why is it being shared?
- Other questions ---

Other questions

- Each type will specify requirements
- Critical questions
  - With whom is the information being shared?
  - Are they eligible?
  - Is there a current data-sharing agreement?
  - Are the parties still current?
  - Have there been any changes to ownership?

Determine – “who are you doing business with?”

- Current security philosophy/posture – Basic (required) or better* (enhanced)
- Designation of Company Information Security Officer or equivalent
- Ownership, Control, Foreign Investors
- Keeping current
- References use – maintained
- Determination of Governmental Purpose
- Minimizing access
- Handling of Export-Controlled information
- Awareness and Management of CTI
- Understanding of requirements – details
- Storage capability
- Ability to decontrol – destroy various information types (disposition)
- Publication requirements/procedures

Red Flag Questions - EAR

1. Buyer is reluctant to offer information about the end-use of the ordered product
2. Product's capabilities do not fit the buyer's line of business
3. Buyer's IP address does not match the stated location
4. Company receives the same request for a quote (RFQ) from multiple customers
5. The RFQ appears to be cut-and-pasted into the email
6. Buyer carbon copies unknown individuals
7. A freight forwarder, Importer/ Exporter, or General Trading Company is listed as the final
8. Routine installation, training, warranty, or maintenance services are declined by the buyer
9. Buyer is unfamiliar with the product’s performance.
10. Buyer is evasive when asked about whether parts are for domestic use or re-export
11. Buyer has little to no presence on the Internet
12. The shipping address is a residence or a building that leases virtual office space
13. Unusual method of payment or unexpected source of payment

https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators

Info type = handling requirements

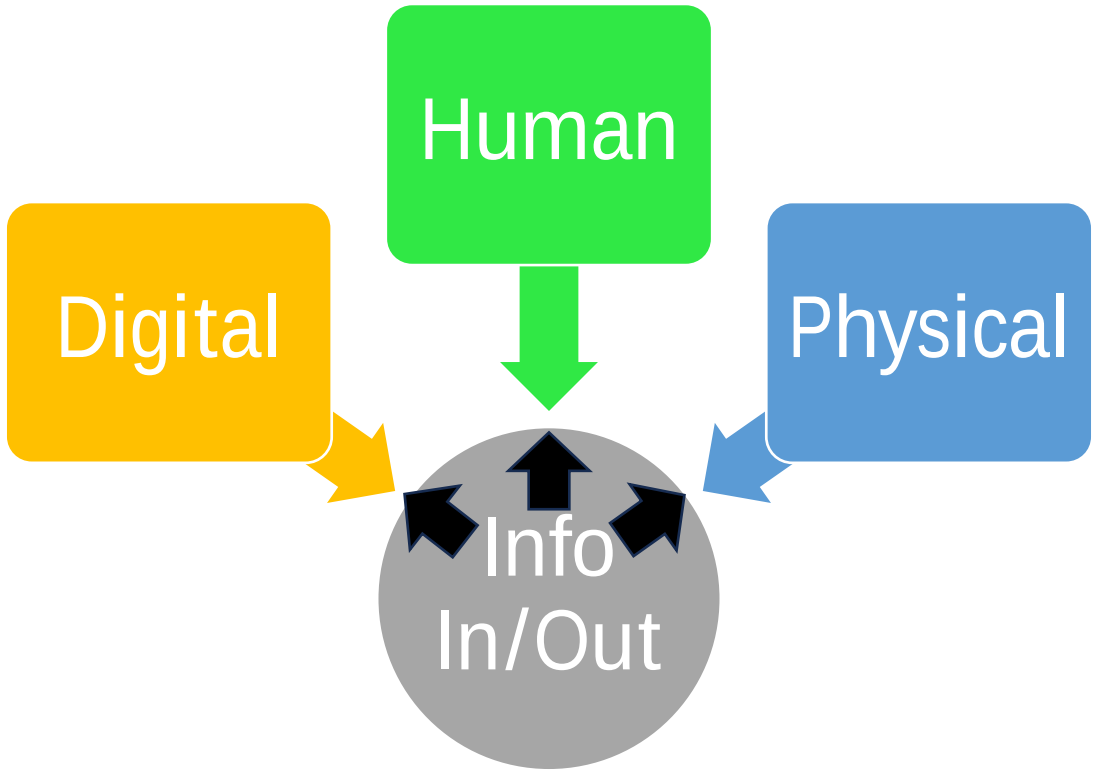
1. *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.
2. *Other requirements.* This clause does not relieve the Contractor of any other specific *safeguarding* requirements specified by *Federal agencies* and departments relating to *covered contractor information systems* generally or other Federal *safeguarding* requirements for controlled unclassified *information* (CUI) as established by Executive Order 13556.

1. DFARS 252.204-7012 (l)
2. FAR 52.204-21 (2)

Handling Concepts

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

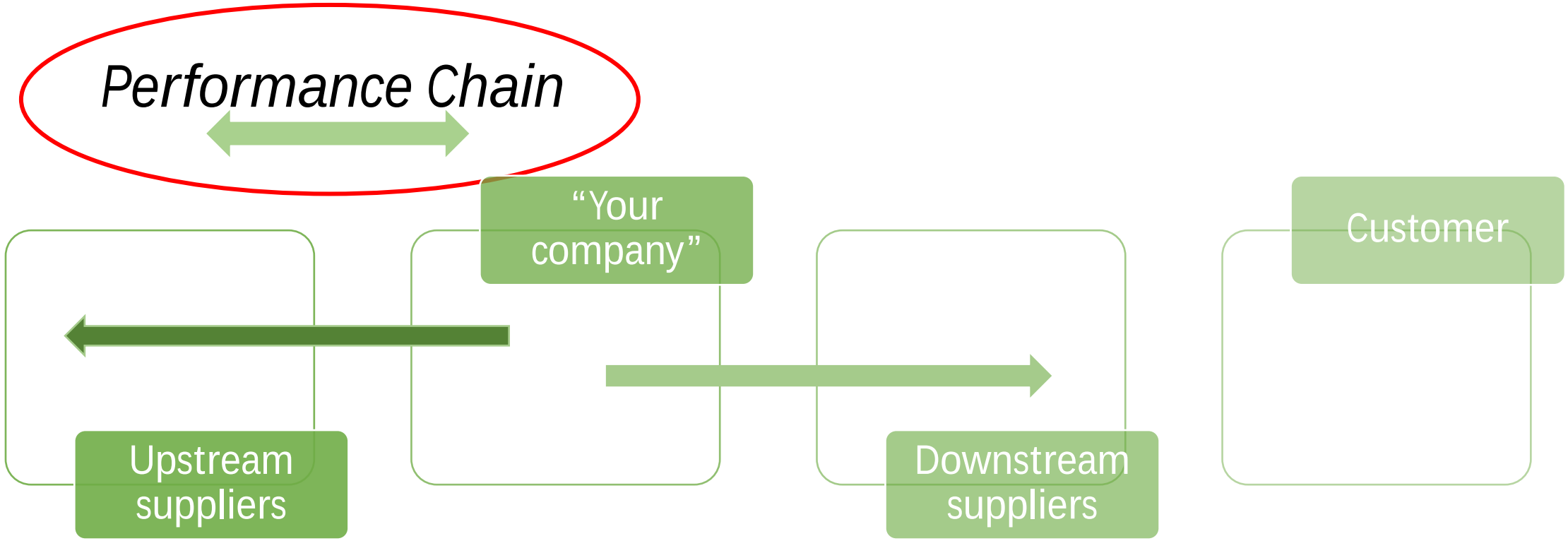
Information Flows / Channel / Sharing



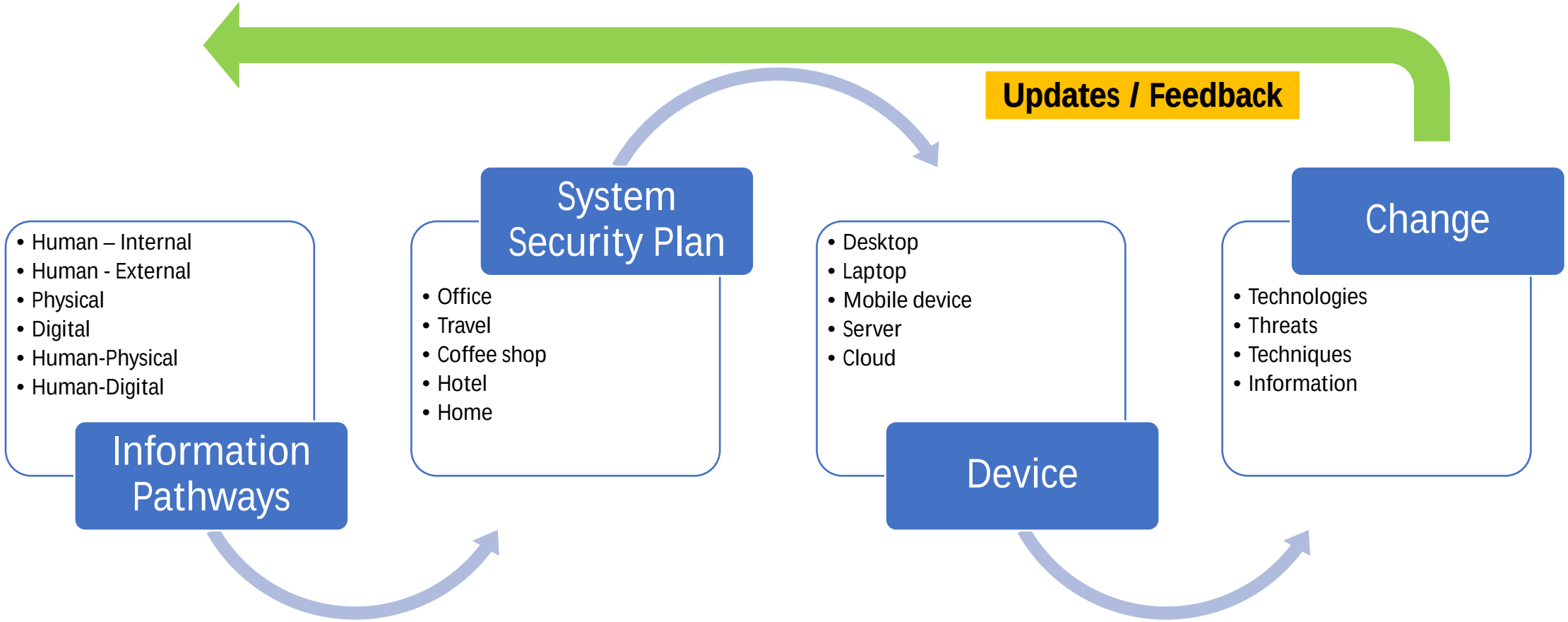
(Threat Avenues)

- What pathways are used?
- Who uses or shared with?
- 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?

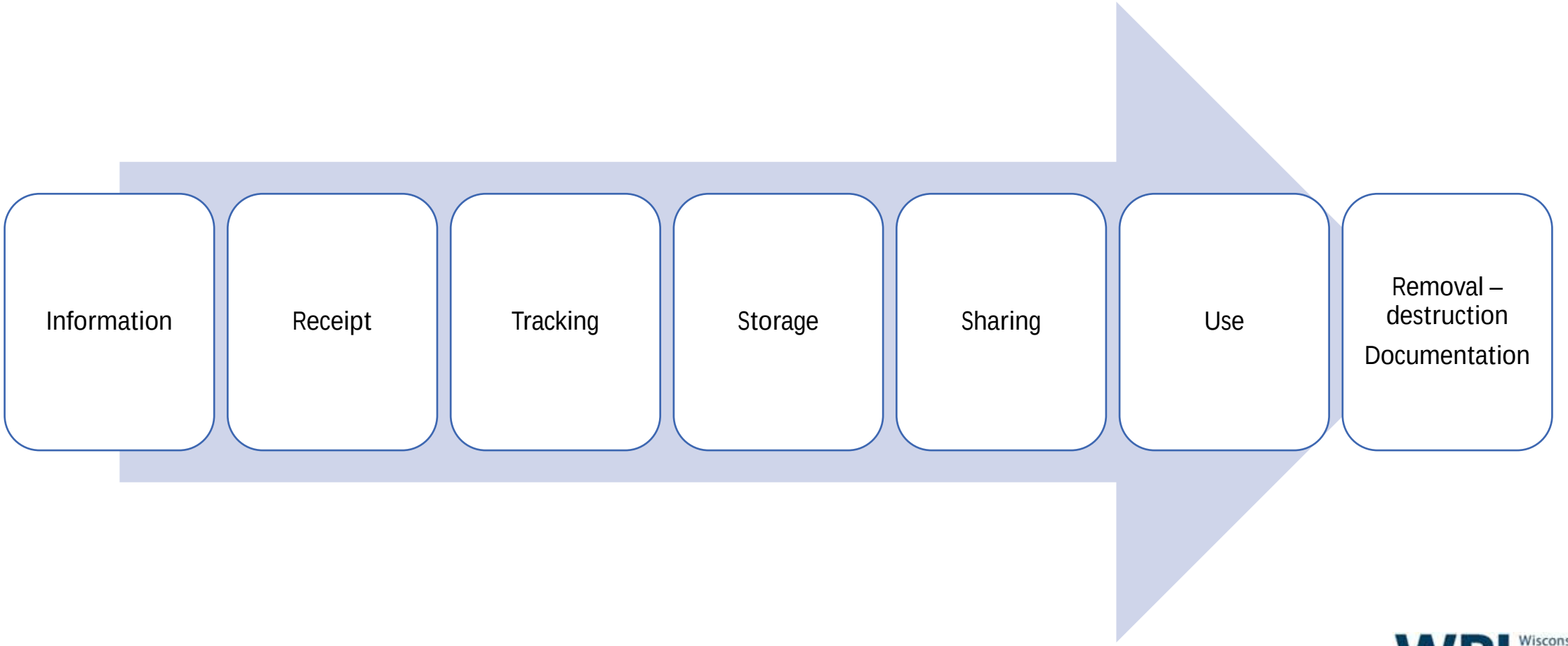
Key Idea – Supply Chain – Not company



Dynamic/Evolving Environment

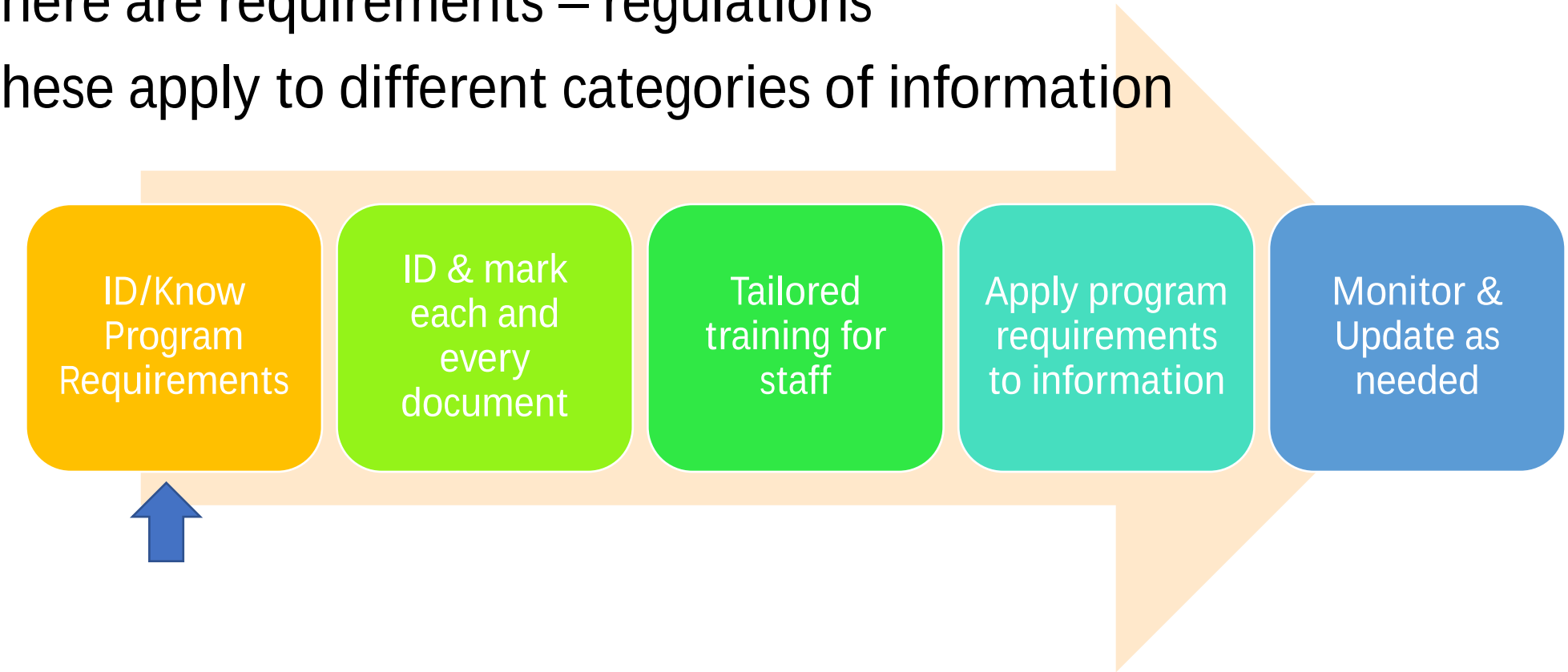


Information usage lifecycle



Information Management (digital & physical)

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



Destruction notice

- Upon completion of the purposes for which Government Technical Data has been provided, the Contractor is

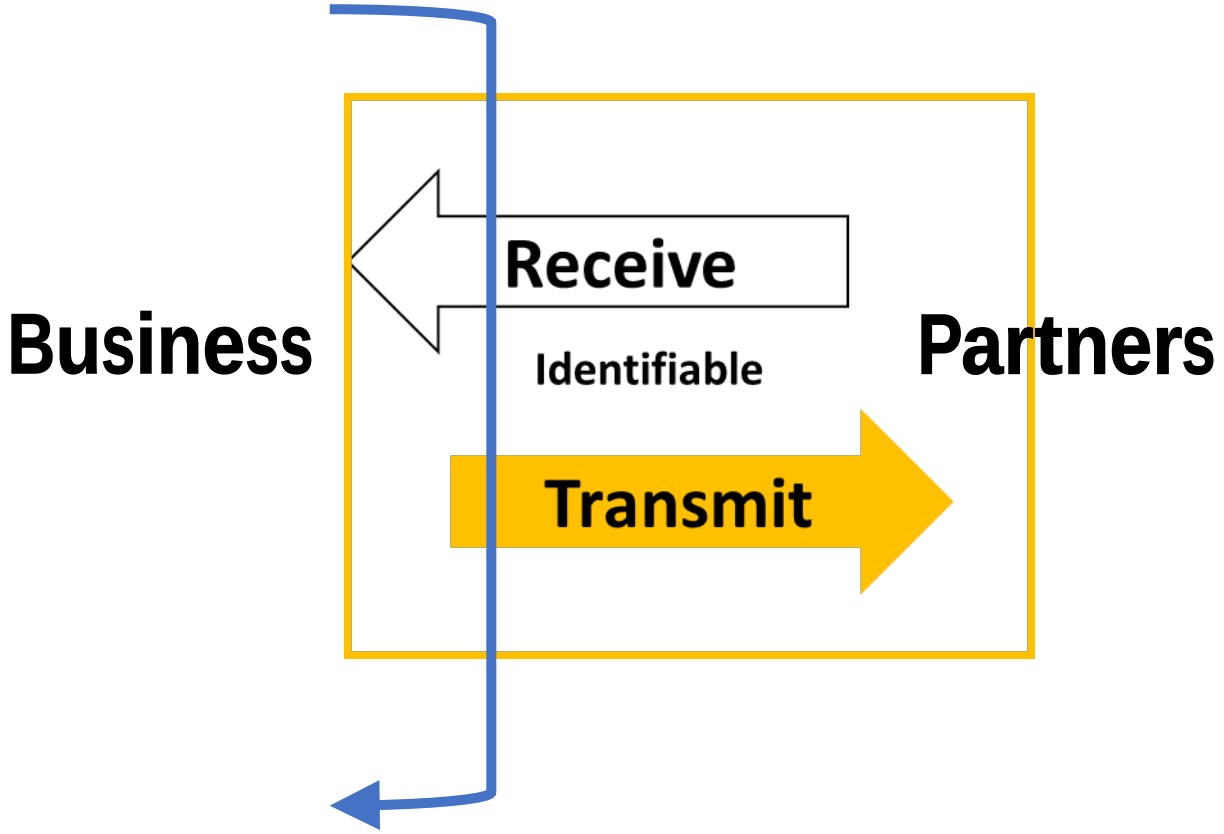
Ørequired to destroy all documents, including all reproductions, duplications, or copies thereof as may have been further distributed by the Contractor.

ØDestruction 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!

Develop Data Exchange Agreement

- Requirements – specifications
- Usage agreement
- Eligibility
- Protocols
- Software – encryption
- Identity – authorization
  - URL, Credentials, MAC



Federal Contract Information (FCI)

- *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
- The Contractor *shall* apply the following basic *safeguarding* requirements and procedures – these are the 15 requirements
  - If these apply to the company currently in possession of the FCI, it seems reasonable that any recipient should also be compliant with these 15 requirements.

Controlled Unclassified Information (CUI)

- CUI –
  - DoD Instruction 5200.48 Controlled Unclassified Information
    - see: https://www.dodcui.mil/
  - Required training CDSU
  - Lawful Government Purpose
  - Determination if there are other information categories included
  - Handled / Shared in accordance with applicable requirements
    - Email – encrypted
    - Recipient has completed DoD Basic Assessment with score in SPRS
  - May include – JCP and/or ITAR

Distribution Statements – required warning

- All printed and electronic technical information, including technical information in a digital form, that is determined to contain export-controlled technical information, will be marked as shown in Figure 3.

DoDI 5230.24, January 10, 2023

Figure 3. Export-Control Warning

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Section 2751 of Title 22, United States Code) or the Export Control Reform Act of 2018 (Chapter 58 Sections 4801-4852 of Title 50, United States Code). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25 and DoD Instruction 2040.02.

https://www.dodcui.mil/Policy/ - 5230.24; page 20

Joint Certification Program (JCP)

- Managed by DLA
- Requires enhanced JCP certification
  - Training review
  - SPRS – cyber
  - Registration
  - Identification of Data Custodian & alternatives
  - Computer ID – MAC address
- May include CUI and/or ITAR

DoD Directive 5230.25

The JCP was 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 DODD 5230.25, "Withholding of Unclassified Technical Data and Technology from Public Disclosure," and Canadian Technical Data Control Regulations.

DoDD 5230.25, November 6, 1984

E5. ENCLOSURE 5
NOTICE TO ACCOMPANY THE DISSEMINATION OF EXPORT-CONTROLLED TECHNICAL DATA

E5.1.8. A copy of this notice shall be provided with any partial or complete reproduction of these data that are provided to qualified U.S. contractors.

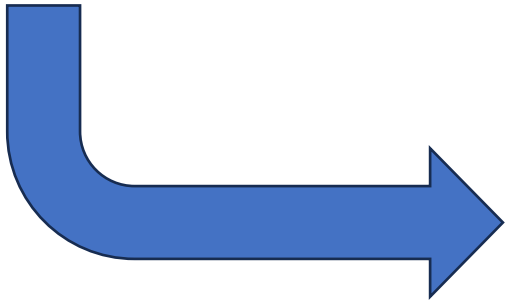
https://www.dla.mil/Logistics-Operations/Services/JCP/
5230.25 - Withholding of Unclassified Technical Data From Public Disclosure; page 21

References matter – DoDD 5230.25, 11/6/84

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



E1. 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
(o) Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018

Penalties

- E5.1.2. Under 22 U.S.C. 2778 the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of $100,000, or both. Under 50 U.S.C., Appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000, or five times the value of the exports, whichever is greater; or for an individual, imprisonment of up to 10 years, or a fine of up to $250,000, or both.

- E5.1.3. In accordance with your certification that establishes you as a "qualified U.S. contractor," unauthorized dissemination of this information is prohibited and may result in disqualification as a qualified U.S. contractor, and may be considered in determining your eligibility for future contracts with the Department of Defense.

DoDD 5230.25, November 6, 1984, enclosure 5

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

Foreign Ownership, Control or Influence (FOCI)

- Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it's the policy of the U.S. Government to allow foreign investment consistent with the national security interest of the United States.
- A company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/

Adversarial landscape

- China* -- (BRI - ~140 countries)
- China currently represents the biggest threat and competitor to the United States in terms of global economic influence.
- Russia may pose a bigger military threat since it possesses weapons of mass destruction, but its economy is about the size of Texas, so they don’t pose as great an economic threat.
- Iran poses a different type of threat, but nowhere near the size of China.
- North Korea
- Venezuela

THREATS

FBI Opens a Case on Chinese Activity 'Every 10 Hours,' Intel Chiefs Say

China leads a pack of threats to the United States, they tell lawmakers.

BY PATRICK TUCKER
TECHNOLOGY EDITOR

APRIL 14, 2021 05:00 PM

The threat from China, multi-faceted and severe, is foremost in a pack that includes Russian actions in Ukraine, Iranian nuclear efforts, and North Korea's existing nukes, U.S. intelligence leaders told the Senate Intelligence Committee on Wednesday.

"We have now over 2,000 investigations that tie back to the Chinese government," FBI Director Chris Wray said at the hearing. "On the economic espionage side alone, it's a 1,300 percent increase over the last several years. We're opening a new investigation on China every ten hours and I assure the committee it's not because our folks don't have anything to do with their time."

https://www.defenseone.com/threats/2021/04/fbi-opens-case-chinese-activity-every-10-hours-intel-chiefs-say/173376/

Look before you leap - the GE Engineer

- Court records show Chinese spies used LinkedIn to identify and initially contact Xu's target, former GE Aviation engineer David Zheng.
- He accepted an offer for a free trip to China in 2017 to present information about GE Aviation engines at the Nanjing University of Aeronautics and Astronautics, according to court records
- The FBI learned about Zheng's trip after he returned to Cincinnati and notified GE Aviation. The company fired Zheng.
- Court records show the Cincinnati-based investigation also provided key evidence in criminal cases in Arizona and Illinois.

https://www.wcpo.com/news/local-news/i-team/chinese-spy-sentenced-to-20-years-in-federal-prison-for-conspiracy-to-steal-ge-aviation-trade-secrets

NISPOM v. FOCI

- Pentagon contractors with access to classified information are regulated under the National Industry Security Program Operating Manual.
- The Pentagon's Defense Security Service has authority over most companies with facility security clearances.
- By law, NISPOM prohibits foreign ownership, control or influence over U.S. companies that hold clearances, but allows for the influence to be "mitigated" via proxy or special security agreements.
- "Each agreement generally requires the foreign-owned or controlled shareholder and the cleared company to implement certain corporate governance requirements to address U.S. national security concerns related to the protection of U.S. government classified information," said Fagan.

https://www.nationaldefensemagazine.org/articles/2015/5/12/defense-contractor-reinvents-itself-to-operate-under-foreign-ownership - May 12, 2015

Foreign Ownership

- **Defense Contractor ‘Reinvents Itself’ to Operate Under Foreign Ownership**
- At a time of heightened concern about attacks on U.S. computer networks, the federal government might be expected to frown on a foreign takeover of one its cybersecurity contractors.
- The $890 million acquisition last year of Maryland-based SafeNet by European digital security giant Gemalto was approved in January, although extraordinary actions had to be taken in order to allow the newly acquired company to remain a government contractor.
- “SafeNet had to reinvent itself to continue to sell to the government,” said Kirk Spring, president of SafeNet Assured Technologies in Abingdon, Maryland. The company provides data encryption hardware and software to military and intelligence agencies.

https://www.nationaldefensemagazine.org/articles/2015/5/12/defense-contractor-reinvents-itself-to-operate-under-foreign-ownership

FOCI – factors to be considered

- Record of economic and government espionage against U.S. targets
- Record of enforcement and/or engagement in unauthorized technology transfer
- The type and sensitivity of the information that shall be accessed
- The source, nature and extent of FOCI
- Record of compliance with pertinent U.S. laws, regulations and contracts
- The nature of any bilateral and multilateral security and information exchange agreements that may pertain
- Ownership or control, in whole or in part, by a foreign government

https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/

Potential Tactics

- Partner with firms to gain access
- Embed personnel
- Use Shell companies to hide
- -- Paying fair market value **is not** considered a tactic

Valley of Death – (possible pressure point)

- Typically, a term used by Venture Capital
- Gap between initial investment and sustaining revenue generation
- Companies need to be curious about the money
- May also apply to multi-year contract award
  - Award, multi-year effort requirement before delivery and payment
  - Company generally “is the bank” for the performance period
  - Does the company have the financial wherewithal?
  - Financial stress
    - Susceptible to investment – acquisition offers
    - Who really is providing the funds and what do they really want?

Methods

- Invest in startup
  - Initial phase; prior to revenue generation
- Weaponize the supply chain
  - Identify and take advantage of vulnerabilities
- Use private equity firms and shell companies to hide intent, ownership

Example programs initiative - China

- Made in China 2025
  - Indigenous production by 2025
- Military-Civil Fusion (MCF)
- Belt and Road Initiative (BRI)
  - Expanding Global export and trade (140 countries)
- Layering of Laws
  - Laws that favor Chinese firms

China is targeting everything from agricultural techniques to medical devices

- "They've pioneered an expansive approach to stealing innovation through a wide range of actors,"
- Wray told the audience that China is targeting everything from agricultural techniques to medical devices in its efforts to get ahead economically. While this is sometimes done legally, such as through company acquisitions, China often takes illegal approaches, including cyber intrusions and corporate espionage.

"They've shown that they're willing to steal their way up the economic ladder at our expense."

FBI Director Christopher Wray

Just last month, a Harvard University professor was charged with lying about his contractual arrangement with China.

https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620
https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

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?

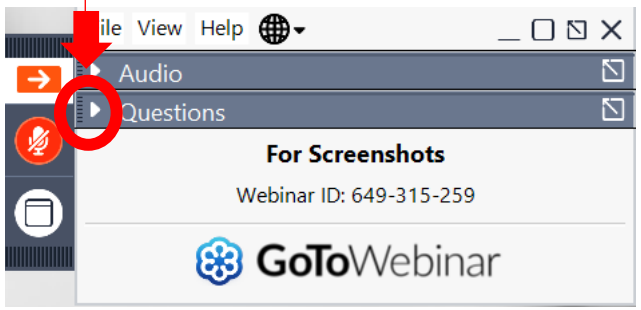
Incidents is there a plan – a process/procedure?

- 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?

QUESTIONS?

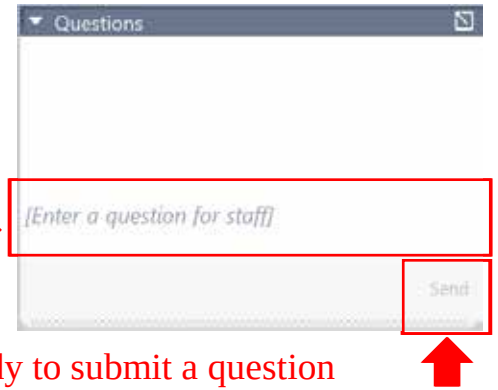
OPENING THE QUESTIONS BOX

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

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- February 7
  Federal Contracting: Contract Methods and Types of Contracts
- February 14
  Protecting Federal Contract Information (FCI): An Introduction to FAR 52.204-21
- February 28
  Protecting Federal Contract Information (FCI): An Introduction to FAR 52.204-21

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute APEX ACCELERATORS

NCMA WISCONSIN

EMERGING ISSUES LIVE WEBINAR SERIES

- February 1
  Sharing Sensitive Information (CUI, JCP, ITAR): Can I Just Send an Email or is more Required?

- February 15
  Analyzing and Understanding the DIBBS RFQ – Overlooked Requirements can Create Contract Compliance Issues

- February 29
  From SBIR/STTR to DPA Title III – An Overview of Federal Innovation Programs, Needs and Marketplace

- March 14
  Suggested Process for Creating a Federal Business Development Strategy

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute

NCMA WISCONSIN

11TH ANNUAL FAR EVENING WEBINAR & STUDY SESSIONS

- **January 30,** Session 1: Introduction and FAR Part 16
- **February 6,** Session 2: FAR Parts 1-4
- **February 13,** Session 3: FAR Parts 5-12
- **February 20,** Session 4: FAR Parts 13-18
- **February 27,** Session 5: FAR Parts 19-29
- **March 5,** Session 6: FAR Parts 30-33
- **March 12,** Session 7: FAR Parts 34-41
- **March 19,** Session 8: FAR Parts 42-53

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute

NCMA WISCONSIN

SURVEY

Wisconsin Procurement Institute

February 1, 2024

NCMA WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1.5 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

February 1, 2024