Emerging Issues:

Foreign Ownership, Control, and Influence (FOCI)

November 30| 1:00 – 2:00 pm

Presented by:

Marc Violante, WPI

Webinar Etiquette

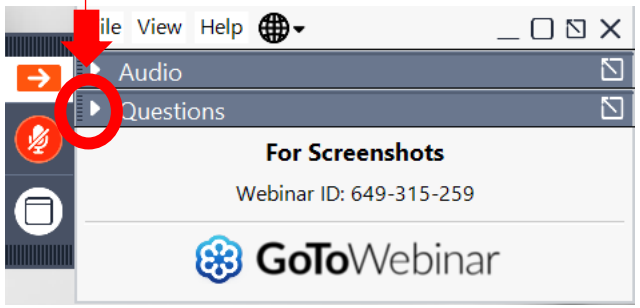
PLEASE

- § 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!

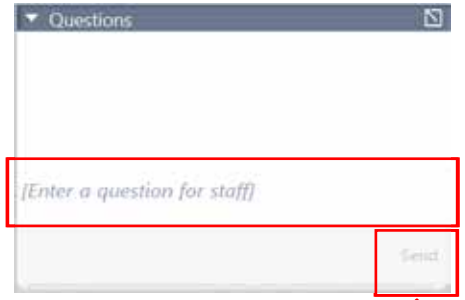
OPENING THE QUESTIONS BOX

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

NCMA WISCONSIN

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

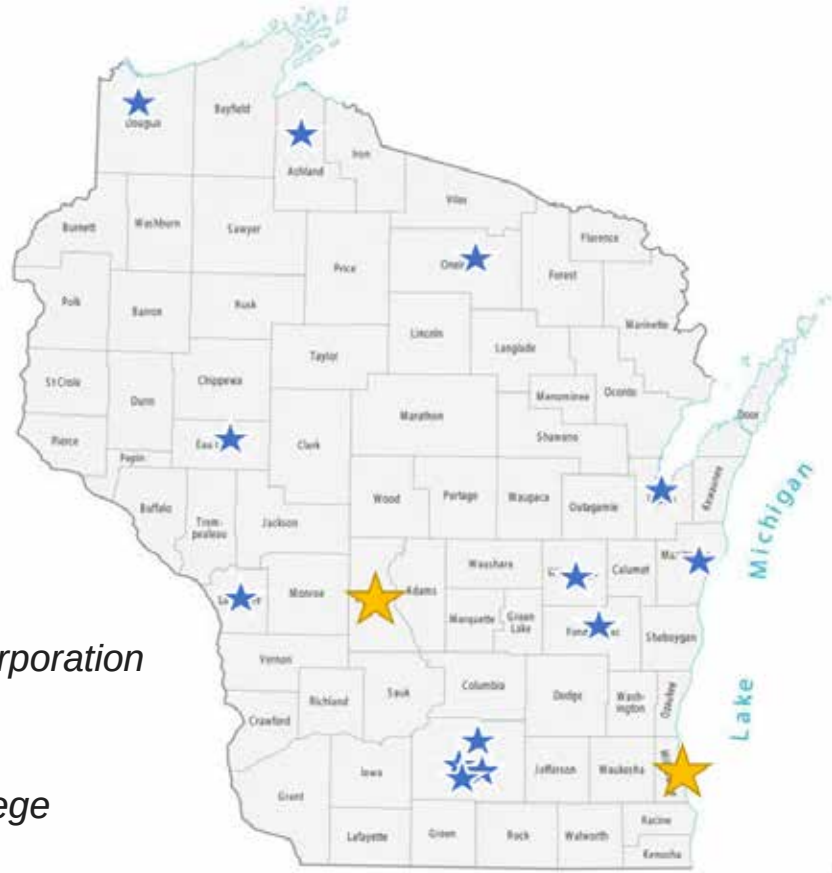
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, 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

November 30, 2023

WPI OFFICE LOCATIONS

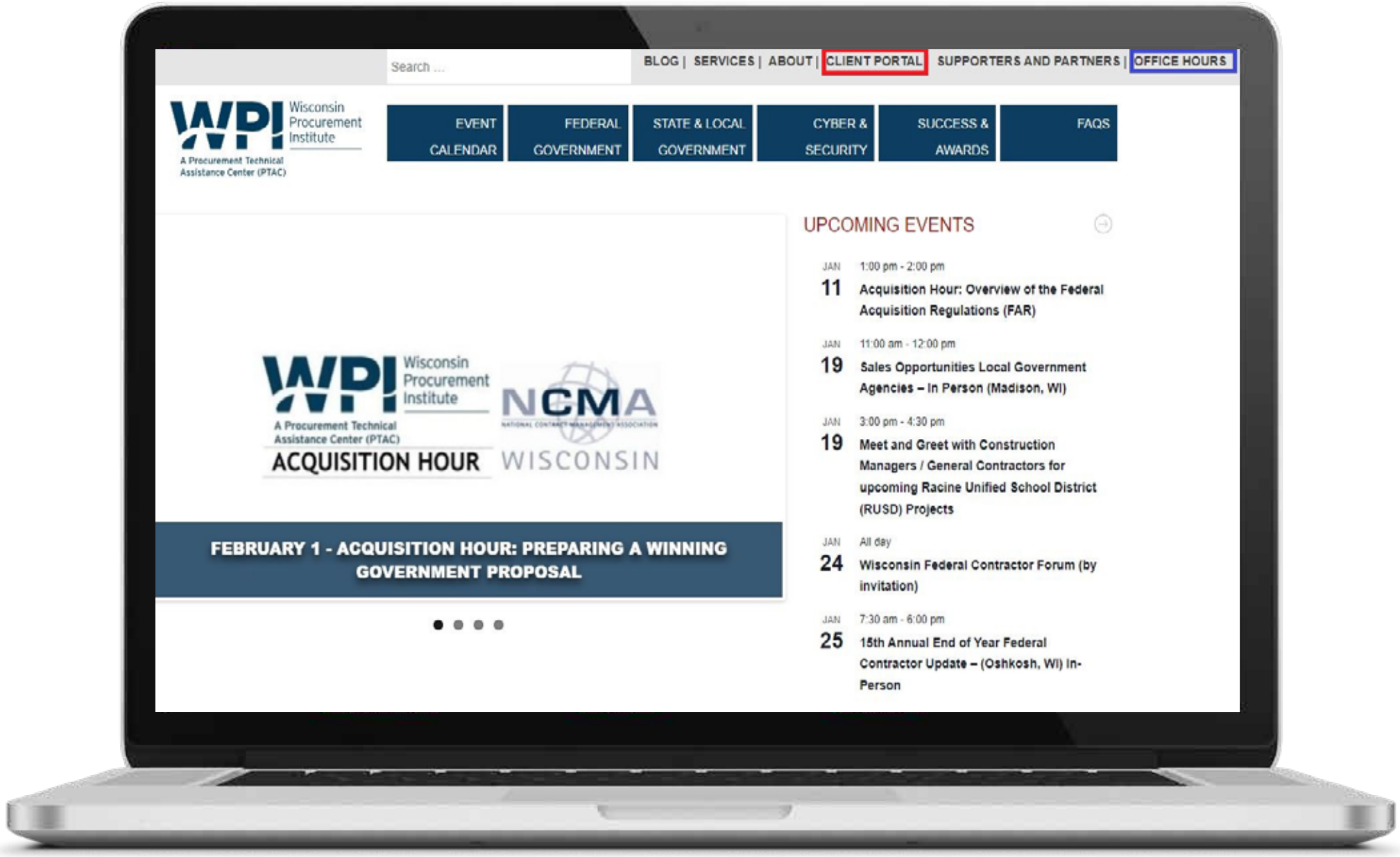
- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **CAMP DOUGLAS**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

November 30, 2023

NCMA WISCONSIN



WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

Foreign Ownership, Control, and Influence (FOCI)

Marc N. Violante

Wisconsin Procurement Institute

November 30, 2023

Today’s webinar

- First and foremost, FOCI can negatively impact our National Security.
- Additionally, FOCI can impact a company’s ability to qualify for a Facility Clearance and in some instances contract award.
- FOCI is not just a single item or a one-time action.
- FOCI is central to being a DoD contractor
- This webinar will provide an overview of these key ideas, requirements, and resources.

What if the world isn't as it seems?

In a famous commencement speech given in 2005 by David Foster Wallace, he tells a quick story about two young fish swimming along together. They come across an older fish who calls out to them, "Morning, boys. How's the water?" The two young fish keep on swimming, as it were, and after a bit one looks at the other, puzzled, and says, "What the hell is water?"

https://www.psychologytoday.com/us/blog/stop-avoiding-stuff/202211/what-if-the-world-isn-t-it-seems

FOCI

~ “FOCI isn’t always a person in a trench-coat at the end of a dark alley”

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

China manipulates markets

- State Control
  - Laws, policies and regulations
    - Favor Chinese corporations > disadvantage to foreign corporations
- Licensing Process
  - Extensive and complex
    - Discriminates against foreign investors
    - Process is unclear, arduous
    - Requires companies to disclose sensitive information

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/

Raw materials and manufacturing

- Monetary impact of Chinese cyber espionage
  - Between - $20 Billion and $30 Billion annually
- Critical Minerals
  - US, Australia, Canada – 5 of 37 minerals
  - China (BRI) – 14 of 37 minerals
- Manufacturing Capacity
  - China 25% of world's manufacturing
  - ½ Dual use (military/commercial)

Life is about managing risks

- Being able to manage risks requires
- Awareness
  - Walking
  - Driving
  - Lifestyle
  - Financial
- Being able to manage risks related to FOCI also requires awareness
  - Of the landscape
  - Tools
  - Mechanisms
  - Being able to look past what is being presented

The issue

What if the normal rules of business – trust, relationships and purpose have been thrown by the wayside – not acknowledged or honored?

What if different rules are in play?

- Rules that may include:
  - Steal
  - Cheat
  - Co-opt

- - to access and obtain important and critical technology instead of developing it independently
- In general, associated risks that may be looked to avoid
  - Financial, time, effort, success v. failure, resource usage

Who is calling – Who sent the email?

Picture of book cover: Authentication From Passwords to Public Key, Richard E. Smith, Addison Wesley, 2002

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

Risk

- -- is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:
  (i) the adverse impacts that would arise if the circumstance or event occurs; and
  (ii) the likelihood of occurrence.
- Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Special Publication 800-30 Guide for Conducting Risk Assessments; page 6

Linkedin – issues or no issues?

- Is it reasonable to view the use of Linkedin as creating risk?
- Can the use of Linkedin lead to loss of a job and serious criminal charges?

Elicitation – some techniques

- Assumed Knowledge
- Bracketing
- Can you top this?
- Confidential Bait
- Criticism
- Deliberate False Statements/Denial of the Obvious
- Feigned Ignorance
- Flattery
- Others

https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view

One technique - Elicitation

- Elicitation is a technique used to collect information that is not readily available and do so without raising suspicion that specific facts are being sought.
- Elicitation is not rare –
  - "It is not uncommon for people to discover information about a person without letting on the purpose.
  - **For example**, have you ever planned a surprise party for someone and needed to know their schedule, wish list, food likes and dislikes or other information without that person finding out you were collecting the information or for what purpose?
  - The problem is when a skilled elicitor is able to obtain valuable information from you, which you did not intend to share because you did not recognize and divert the elicitation.

https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view

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

Take and Replace

- Huawei
- GE Turbine blades
- **China rushes to swap Western tech with domestic options as U.S. cracks down**
  - https://www.reuters.com/technology/china-rushes-swap-western-tech-with-domestic-options-us-cracks-down-2023-10-26/
- Take and Replace –
  - Adversary takes the technology, duplicates it, uses the “taken” tech and replaces the original.
  - One goal, take over supply for that industry

In another case – also GE

- Xiaoqing Zheng, 59, of Niskayuna, New York, was convicted of conspiracy to commit economic espionage, following a four-week jury trial that ended on March 31, 2022. According to court documents, Zheng was employed at GE Power in Schenectady, New York, as an engineer specializing in turbine sealing technology. He worked at GE from 2008 until the summer of 2018. The trial evidence demonstrated that Zheng and others in China conspired to steal GE's trade secrets surrounding GE's ground-based and aviation-based turbine technologies, knowing or intending to benefit the PRC and one or more foreign instrumentalities, including China-based companies and universities that research, develop, and manufacture parts for turbines.

https://www.justice.gov/opa/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage

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/

Risk management processes

(i) framing risk;

(ii) assessing risk;

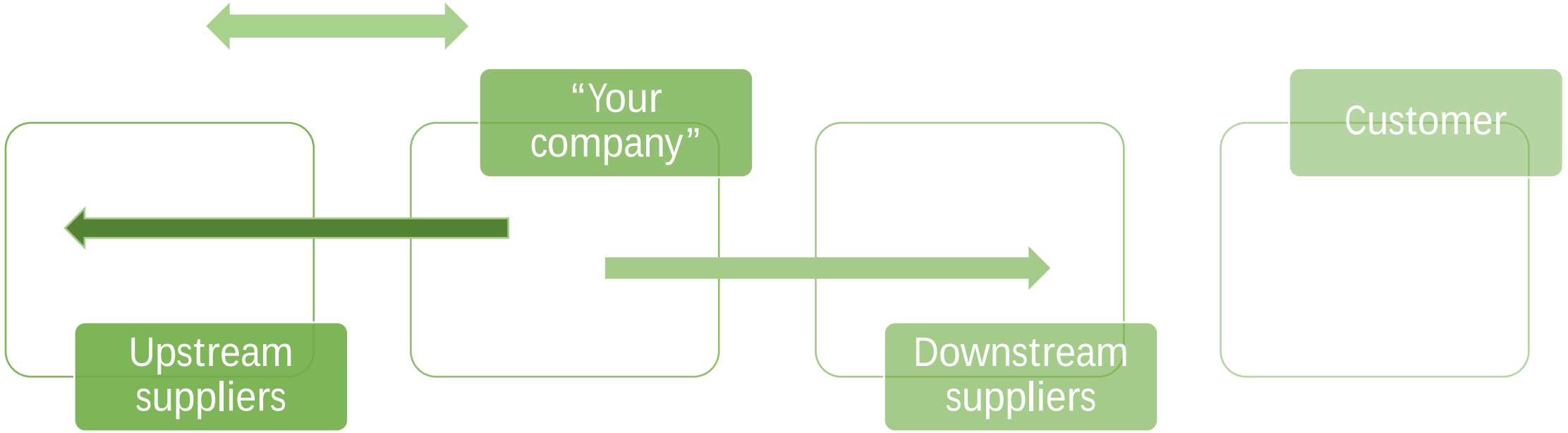
(iii) responding to risk; and

(iv) monitoring risk.

Special Publication 800-30 Guide for Conducting Risk Assessments; page 4

Key Idea – Supply Chain – Not company

Performance Chain



Insiders can be threats too

Disgruntled former VP hacks company, disrupts PPE supply, earns jail term

The sabotage of electronic records led to delays in shipping critical PPE during the COVID-19 pandemic.

- Dobbins set about disrupting Stradis' electronic records by creating a secondary user account and both editing over 115,000 records and deleting over 2,300 entries.
- Dobbins' actions did not just cause the company's operations to grind to a screeching halt in March; issues continued for months after as Stradis sought to repair the damage.

https://www.zdnet.com/article/disgruntled-former-vp-hacks-company-disrupts-ppe-supply-earns-jail-term

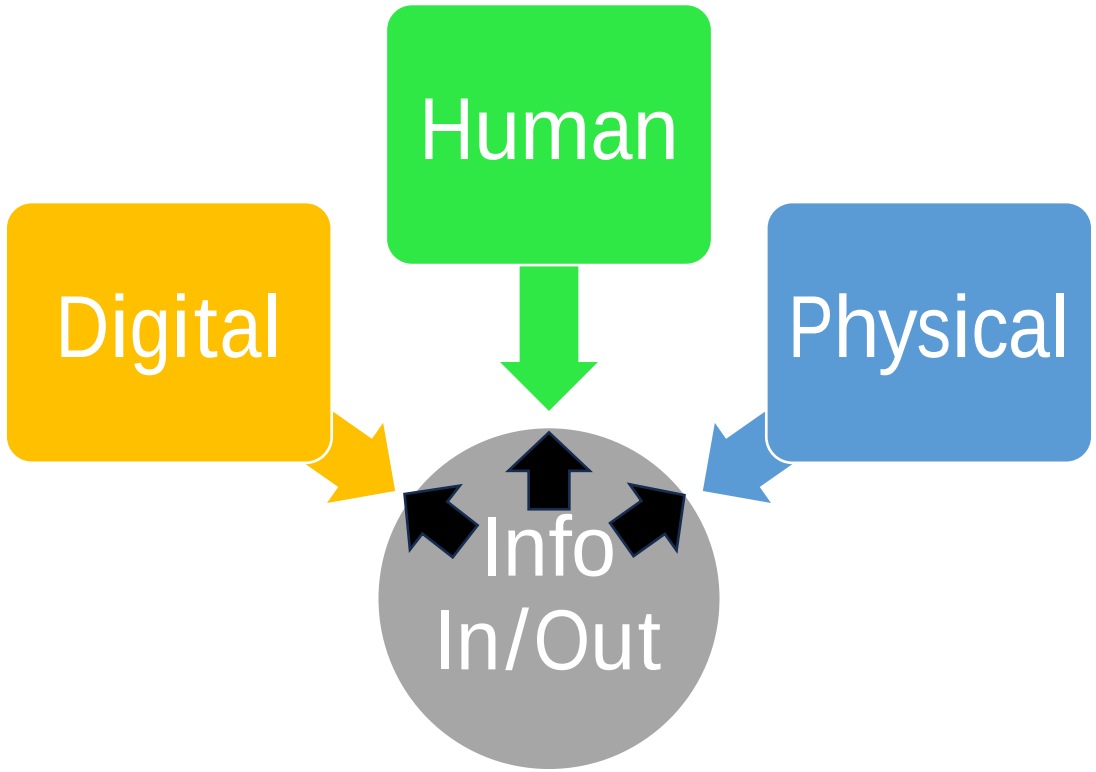
Focus on the spirit & intent – not the words!

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

Hid for two years!

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

Information Flows / Channel / Sharing



- 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?

Potential Tactics

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

“threat avenues”

- Transactional
- Human
- Cyber

Valley of Death

- 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?

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.fbi.gov/video-repository/made-in-america-092019.mp4/view

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

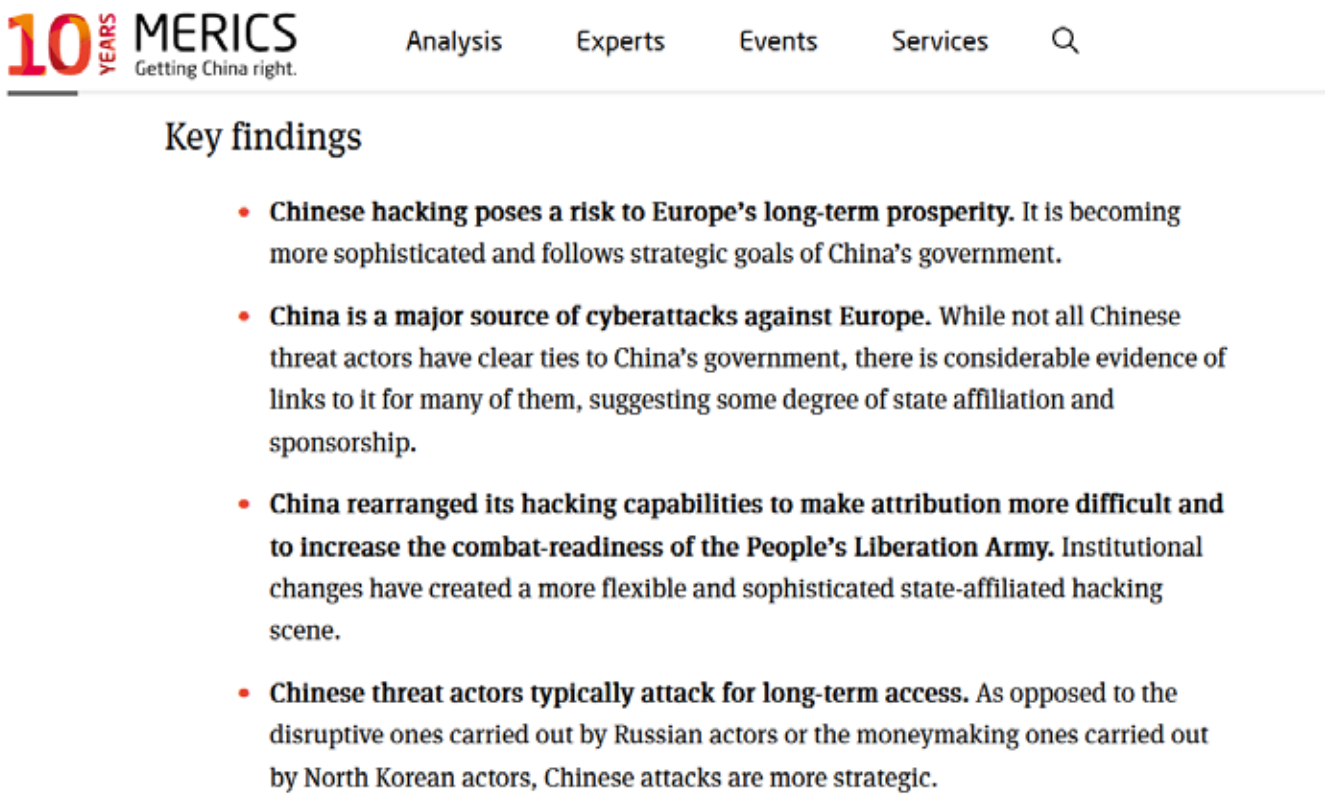
- "They've pioneered an expansive approach to stealing innovation through a wide range of actors,"
- Wray told the audience that China is targeting everything from agricultural techniques to medical devices in its efforts to get ahead economically. While this is sometimes done legally, such as through 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

“Here to stay” – Chinese state-affiliated hacking for strategic goals



10 YEARS MERICS Getting China right.

Analysis Experts Events Services

Key findings

- **Chinese hacking poses a risk to Europe’s long-term prosperity.** It is becoming more sophisticated and follows strategic goals of China’s government.
- **China is a major source of cyberattacks against Europe.** While not all Chinese threat actors have clear ties to China’s government, there is considerable evidence of links to it for many of them, suggesting some degree of state affiliation and sponsorship.
- **China rearranged its hacking capabilities to make attribution more difficult and to increase the combat-readiness of the People’s Liberation Army.** Institutional changes have created a more flexible and sophisticated state-affiliated hacking scene.
- **Chinese threat actors typically attack for long-term access.** As opposed to the disruptive ones carried out by Russian actors or the moneymaking ones carried out by North Korean actors, Chinese attacks are more strategic.

https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals - November 22, 2023

Awareness and good procedures are needed

5-Year-Long Cyber Espionage Campaign Hid in Google Play

OceanLotus targeted Android devices in the so-called PhantomLance campaign.

A targeted cyber-spying mission waged by a notorious hacking team out of Vietnam preyed mainly on Android users in Southeast Asia and evaded detection in Google Play, APKpure, and other app markets for five years.

Researchers at Kaspersky today revealed details of their study of the attack campaign they call PhantomLance, which they believe is the handiwork of OceanLotus. While Kaspersky has a policy of not tying attack groups with specific nation-states, OceanLotus long has been believed to be a Vietnamese advanced persistent threat (APT) group. PhantomLance — which targets Android — has managed to stay alive by changing up its malware along the way to evade detection.

https://www.darkreading.com/endpoint/5-year-long-cyber-espionage-campaign-hid-in-google-play/d/d-id/1337676?

Increased domestic manufacturing

- **China rushes to swap Western tech with domestic options as U.S. cracks down**
  - Beijing has increased spending on domestic tech since late 2022
  - Telecoms and banks likely next to be pushed to use more Chinese products
  - Replacing Western tech due to geopolitics and cyberattack fears
  - Foreign firms still dominant in banking-related software

https://www.reuters.com/technology/china-rushes-swap-western-tech-with-domestic-options-us-cracks-down-2023-10-26/

Something to watch (possible driver)

02/07/2019

Evolving Made in China 2025

China's industrial policy in the quest for global tech leadership

Four years ago, China launched its ambitious industrial strategy Made in China 2025 and caused considerable irritation around the world. The blueprint for China's path to becoming an industrial superpower has changed the way foreign companies, business associations, and governments view the country. They increasingly perceive the People's Republic more as a systemic rival than a partner. Made in China 2025 has recently disappeared from official rhetoric of the Chinese leadership. But Beijing's aims remain unchanged and its industrial policy is already being implemented: it wants Chinese companies to become global leaders in ten core industries by 2025. And it aims to be a global technological superpower by 2049.

https://www.merics.org/en/papers-on-china/evolving-made-in-china-2025

Example 2: Elemental Servers

- In another alarming example, China appears to have infiltrated high levels of the U.S. government through its strategic acquisitions, corporate purchases, and component suppliers.
- An American server company, Elemental, uses a third-party firm (Super Micro) to assemble its servers. Super Micro is one of the world's greatest suppliers of motherboards, which are assembled by Chinese contractors. At the behest of the Chinese government, those Chinese contractors inserted a small microchip that was not part of the server's motherboard design.
- Alarm! Elemental's servers are used in DOD data centers and the onboard networks of U.S. Navy warships.

Billion-Dollar Secrets Stolen

- When scientist Hongjin Tan resigned from the Oklahoma petroleum company he'd worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.
- But Tan told a colleague a different story over dinner.
- That conversation prompted Tan's employer to ask him to leave the firm immediately—and then his employer made a call to the FBI tip line to report a possible crime. The resulting investigation led to Tan's guilty plea and 24-month prison sentence for stealing proprietary information that belonged to his company.
- *Tan's theft of a trade secret—one worth an estimated $1 billion—is an example of what the FBI says is a systematic campaign by the Chinese government to gain economic advantage by stealing the innovative work of U.S. companies and facilities.*

FBI agents said he began accessing these sensitive files around the time he applied to China's Thousand Talents Program. U.S. intelligence agencies have found that, through this program, China provides financial incentives and other privileges to participants who are willing to send back the research and technology knowledge they can access while working in the United States.

https://www.fbi.gov/news/stories/scientist-sentenced-for-theft-of-trade-secrets-052720

Economic Espionage – possible indicators

KNOW THE SIGNS

- Working odd hours without authorization
- Taking proprietary information home without authorization
- Unnecessarily copying material
- Disregarding company policies on personal software and hardware
- Accessing restricted websites
- Downloading confidential material
- Conducting unauthorized research

PERSONAL BEHAVIORS

- Unexplained short trips to foreign countries
- Engaging in suspicious personal contacts with competitors, business partners or unauthorized individuals
- Buying items they normally cannot afford
- Overwhelmed by life crises or career disappointments
- Showing concern about being investigated

COMMON FACTORS

- Financial need
- Greed
- Unhappiness in the workplace
- Different allegiances to another company or country
- Drug/Alcohol abuse
- Vulnerability to blackmail
- Job offers from other organizations

https://www.fbi.gov/file-repository/economic-espionage-508.pdf/view

Insider Threat

- **The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy (FBI)**

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

- **Economic Espionage: How to Spot a Possible Insider Threat (FBI, May 2012)**

This article talks about the threat of corporate insiders stealing secrets, focusing on foreign economic espionage. It includes cases examples and potential warning signs.

- **Combating the Insider Threat (DHS National Cybersecurity and Communications Integration Center, May 2014)**

This document includes characteristics of insiders at risk of becoming a threat, behavioral indicators of malicious threat activity, behavioral prediction theories, countermeasures and deterrence methods, and training suggestions.

- **National Counterintelligence and Security Center Insider Threat Webpage**

This webpage contains link to relevant documents and websites.

Filed under: Frontpage Feature

https://www.dsac.gov/topics/insider-threat

Good videos

Economic Espionage

- **FBI Launches Nationwide Awareness Campaign**

- The Company Man: Protecting America' Secrets
  https://www.fbi.gov/news/stories/economic-espionage
- Made in America
  - https://www.fbi.gov/video-repository/made-in-america-092019.mp4/view
- GAME OF PAWNS - The Glen Duffie Shriver Story
  - https://www.youtube.com/watch?v=TEYRLDvJaxo&feature=youtu.be

Resource - video

- **WORLD EXCLUSIVE: Chinese spy spills secrets to expose Communist espionage | 60 Minutes Australia**
  - https://www.youtube.com/watch?v=zdR-I35Ladk

Targeted Venture Capital

- Targeted venture capital allows Chinese firms to access valuable U.S. technology and IP, including technologies with potential dual-use applications.
- Heavily regulated Chinese companies are some of the largest *targeted venture capital* investors.
- Even before the start of the COVID-19 pandemic, Chinese private equity and venture capital investments have become more targeted.
- Chinese regulations on outbound capital encourage this capital to target specific sectors, like U.S. technology start-up companies.
- There is more U.S. venture capital activity in China than there is Chinese capital activity in the U.S.

DAU course slide

Example: Apple

- In 2016, Apple signed an agreement with the Chinese government to invest about $275B in China over a five-year period. This deal was taken after Chinese regulators began targeting the iPhone and Apple's sales began to falter.
- Apple signed a **Memorandum of Understanding** with the Chinese government committing Apple to sign more deals with Chinese software companies, using more Chinese-made components, and collaborating with Chinese universities on research and development, among other things.
- In return, the Chinese government agreed not to choke off Apple's access to the vast Chinese consumer market.

Key Tactics

- Leveraging partnerships and joint ventures to gain intellectual property and force “tech transfers.”
- Combining cyber campaigns with embedded personnel to collect sensitive information from research and development (R&D) and technology firms.
- Using private equity firms and shell companies to obscure Chinese state involvement.
- Paying premiums for U.S. acquisitions (market distortions) and targeting distressed U.S. companies through bankruptcy procedures.
- Manipulating deals to reduce the U.S. company’s market value prior to acquisition.
- **Note**: Early-stage technology is vulnerable to these tactics due to the desire for quick funding and guaranteed exits to get that foreign capital and the capital options, and the ability and need of China to gain access to that technology.

DAU Course Slide

Example: Key Tactic

- A123 Systems was an American company founded in 2001 by three Americans—one of Chinese descent—and they specialized in the new, faster-recharging lithium-ion battery system. For the next several years, the company received several grants, contracts, and tax credits totaling hundreds of millions of dollars to develop its lithium-ion battery technology for plug-in hybrid electric vehicles and build the facilities to manufacture and build them.
- In December 2009, the company formed a joint venture with Shanghai Automotive Industry Corporation, the largest automaker in China. This was the first joint venture between a Chinese automaker and a non-Chinese battery supplier. In 2010, the company formed a joint venture with Shanghai Automotive Industry Corporation to manufacture its batteries in China in early 2010.
- After a product recall in 2012 resulted in about a $55M loss, Chinese automotive components manufacturer Wanxiang Group agreed to invest up to $465M to acquire as much as 80% of A123 Systems in August 2012. However, they withheld their funding which eventually resulted in A123 Systems filing for bankruptcy.
- In January 2013, Wanxiang America purchased the preponderance of A123 Systems' assets out of bankruptcy for $256.6M—far less than their original $465M investment agreement—and organized A123 Systems, LLC.

DAU Course slide

Targeted Tech

- **Emerging Technologies**: 5G, artificial intelligence, biotechnology, future “high value” technology, machine learning, quantum computing, robotics, semiconductors, unmanned systems/drone technology
- **Traditional Industries**: aerospace and defense, information communications technology, manufacturing, mining and energy, real estate, utilities

DAU Course slide

Small Business - example

- **Emerging Technology**: Lithium-ion batteries for electric vehicles, smartphones
- **U.S. Government Funding Provided**
- Small Business Innovation Research (SBIR) funding
- Awarded contract with U.S. private consortium and U.S. government
- Developed at U.S. government-funded research facility
- **Adversarial Capital Used**: Formed joint venture for production in a strategic adversarial country
- **Result**
- Joint venture escaped proper review
- Foreign relationship did not cause U.S. government funding program scrutiny

DAU Course slide

Large Business - example

- A large public electric motor company received heavy Small Business Innovation Research (SBIR) funding at its start.
- In later years, it received a strategic investment from a large Chinese state-owned enterprise.
- This investor first gained access to a board seat with the company.
- They then gained access to some of the technology and technical details that were shared with the board.
- This technology was so cutting edge that it was not yet on any export control list.
- The sharing of that technology through the board then was *not* controlled through export controls. As a result, China gained access to this technology data.

DAU Course slide

Related Laws/Programs

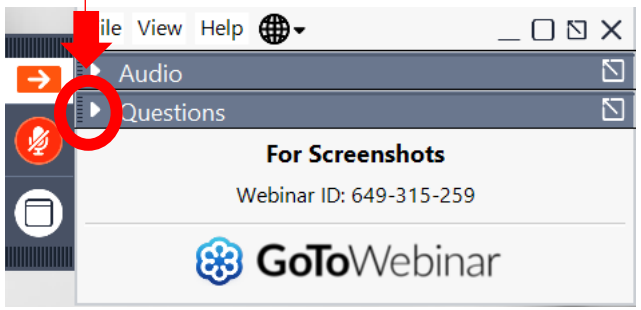
- The Committee on Foreign Investment in the United States (CFIUS)
- The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)
- Some association to the Defense Production Act
- Required filings
  - involving investments by foreign persons in certain U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies.
  - Impact national security
  - Foreign control key element

https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance

QUESTIONS?

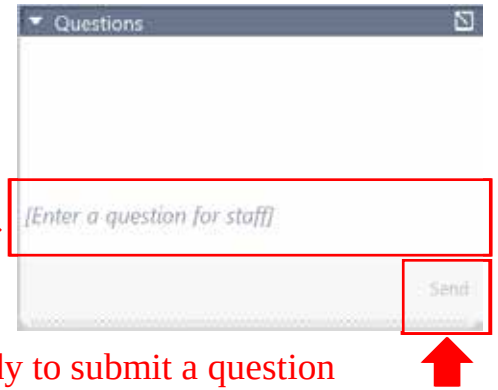
OPENING THE QUESTIONS BOX

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

- November 29
  Service Contracts with Federal Agencies
- December 12
  The HUBZone Program – Certification Benefits and Regulations
- December 13
  Analyzing and Responding to Federal Construction Solicitations
- January 10
  Mastering Federal Construction Contract Performance

…More information and registrations at wispro.org/events

Registration Now Open

The Contracting Academy

Developing and Growing Government Contractors

December 5-7, 2023

MarketplaceWisconsin.com

November 30, 2023

Registration Now Open

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

WPI Wisconsin Procurement Institute APEX ACCELERATORS

Announcing 2024

Evening FAR Sessions

January 30 – March 19

Wispro.org/Events

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

November 30, 2023

SURVEY

Wisconsin Procurement Institute

November 30, 2023

NCMA WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

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