Threats to Electronics

Protecting Intellectual Property and Our Nation

This presentation contains information associated with United States Persons (USPER) as defined by Executive Order 12333 and Department of Defense Manual 5240.01. Such information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates USPER information (USPI) in accordance with all applicable laws, directives, and policies. Questions about the handling of this information should be referred to DCSA North Region CI.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Presented by Michelle Yoworski
Counterintelligence Special Agent
DCSA Eastern Region

Agenda

- Background
- Move to Zero Trust
- The Threat Actors
- How Are Electronics Facilities Targeted?
- Protecting Your Intellectual Property (IP)

Critical Importance of Electronics to DoD

As of May 2020, there are 12 DoD Priorities:

Microelectronics

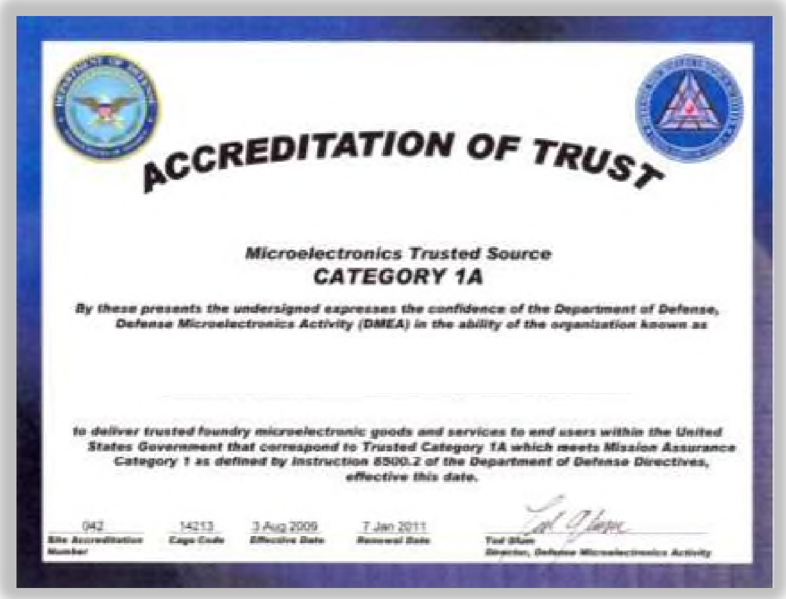
- Operation Warp Speed
- Microelectronics
- Hypersonics
- Autonomy
- Cyber
- 5G Communications
- Space
- Quantum Science
- Fully-Networked Command, Control, & Communications
- Biotechnology
- Artificial Intelligence
- Directed Energy

Trusted Foundry

- The Defense Microelectronics Activity (DMEA) is the program manager for the DoD Trusted Foundry program.
- Trusted – is the confidence in one’s ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, And distribute national security critical components (i.e. electronics).

From Trusted Foundry to Zero Trust

- The Trusted Foundry model no longer meets our needs.
- “Outdated and cannot provide us with access to the most advanced manufacturing capabilities.”
- Businesses could not make a business case for following the Trusted Foundry model.



ACCREDITATION OF TRUST

Microelectronics Trusted Source
CATEGORY 1A

By these presents the undersigned expresses the confidence of the Department of Defense, Defense Microelectronics Activity (DMEA) in the ability of the organization known as

to deliver trusted foundry microelectronic goods and services to end users within the United States Government that correspond to Trusted Category 1A which meets Mission Assurance Category 1 as defined by instruction 8500.2 of the Department of Defense Directives, effective this date.

042	14213	3 Aug 2009	7 Jan 2011	
Site Accreditation Number	Cage Code	Effective Date	Renewal Date	Ted Glum Director, Defense Microelectronics Activity

Zero Trust … Now What?

- Zero Trust assumes nothing is safe and everything must be tested and validated.
- More work is needed to ensure Zero Trust does not significantly increase costs to production, yet counters threats like:
  - Malicious insertion
  - Fraudulent products
  - IP theft
  - Quality and reliability features
- Zero Trust is in the initial stages of implementation and will face many continuous challenges.

Who Targets the Electronics Industrial Base?

- Anyone looking to gain a military or commercial advantage or to nullify ours:
  - Acquire U.S. technology
  - Reverse engineering
  - Seeking talent

- State-sponsored actors modernizing their militaries.
- Non-state actors seeking profit by violating export regulation.
- Trusted insiders targeted by state actors, or seeking profit of their own and contact non-state and state actors.

The China Threat - Background

- Chinese leaders recognize their initial success as the world's low-cost factory was going to run its course.
- To avoid the "middle income trap" China needed high-end manufacturing jobs, but lacked the manufacturing capacity.
- Closing the high-technology gap became a national priority with multiple initiatives to close that gap with the West.

The China Threat - State Sponsored Initiatives

- Five Year Plans (FYP) key themes:
    - Update from low-tech to high-tech
    - Reduce dependence on foreign technology
    - Promote Chinese technology globally
- 13th FYP - To improve manufacturing of advanced electronics.
- 14th FYP - Seeks technology breakthroughs.
- Made in China 2025 - Improve domestic integrated circuits (IC) manufacturing capabilities.

The China Threat - State Sponsored Initiatives

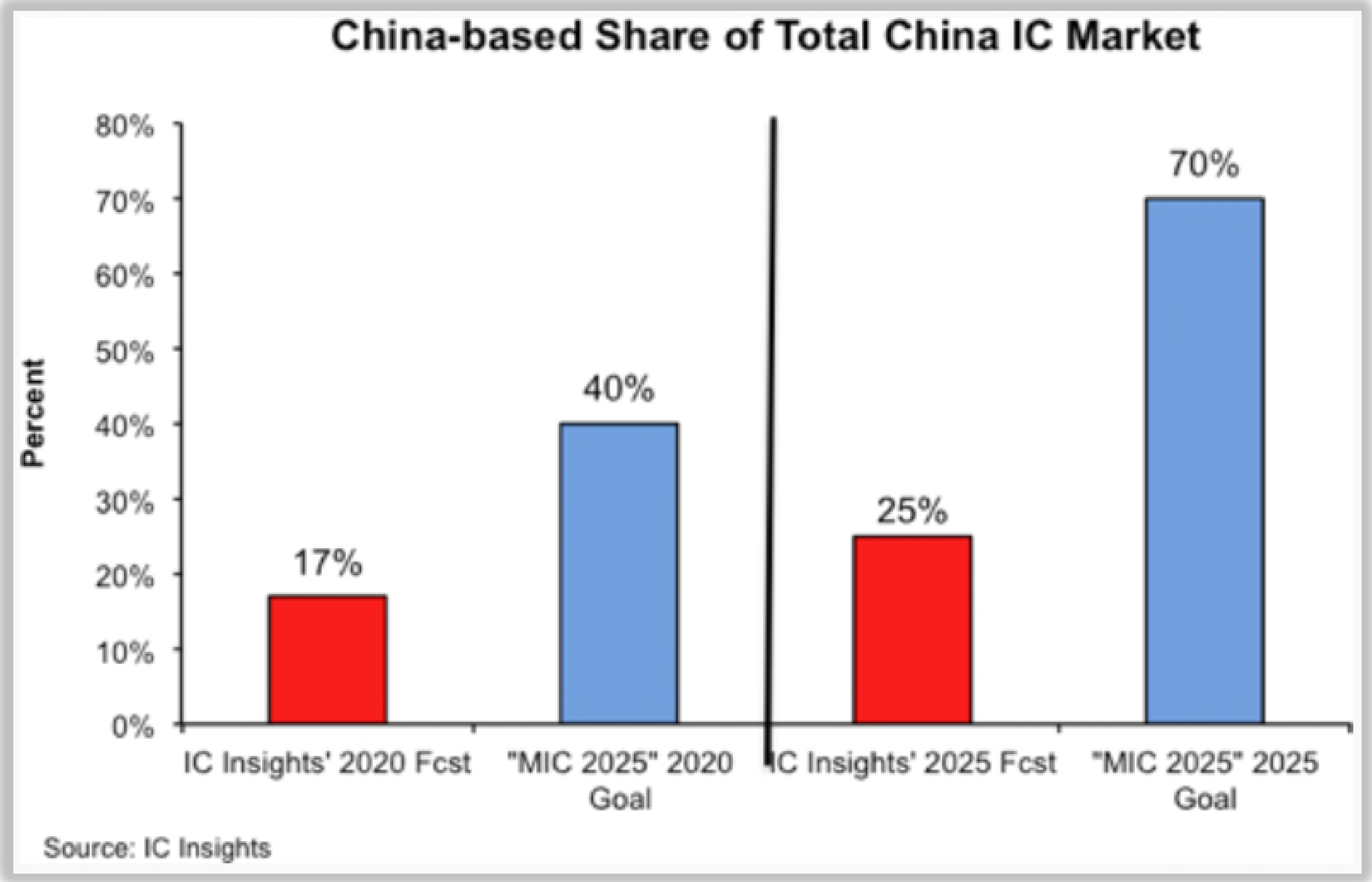
- National Integrated Circuit Fund (NICF):
  - Chinese government fund to develop domestic IC self-sufficiency
  - NCIF’s goal is to meet country’s local chip demand by 2030
  - $22 billion raised in 2014
  - $29 billion raised in 2019
- 2017 Chinese laws compel every Chinese citizen, company, and organization to assist in national security and intelligence work.
  - International businesses operating in China or through Chinese businesses/intermediaries are also indirectly affected by mandate.

The China Threat - Microelectronics is Key

Microelectronics

- Operation Warp Speed
- Microelectronics
- Hypersonics
- Autonomy
- Cyber
- 5G Communications
- Space
- Quantum Science
- Fully-Networked Command, Control, & Communications
- Biotechnology
- Artificial Intelligence
- Directed Energy

The China Threat - How Are They Doing?



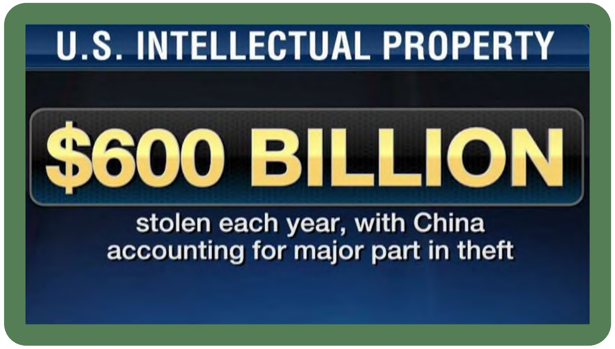
Source: IC Insights

How Are Electronics Facilities Targeted?

- Common successful methods of targeting electronics facilities include:
  - IP Theft
  - Foreign Investment
  - Mergers, Acquisitions, Joint Ventures (JVs)
  - Supply Chain Vulnerabilities
  - Export Violations
  - Cyber
  - Trusted Insiders

Intellectual Property (IP) Theft

- IP theft by foreign countries costs our nation millions of jobs and between $225-$600 billion a year.
- Adversaries use many methods to fulfill their technology gaps like abusing relationships, gaining access to Trusted Foundries, and IP theft.
- Third-party intellectual property (3PIP) can save time and money, but with more than 60% of 3PIP occurring overseas…
    - Lack of visibility = increased risk
    - Can foreign 3PIP be trusted?
    - Risk of malicious insertion



U.S. INTELLECTUAL PROPERTY

$600 BILLION

stolen each year, with China accounting for major part in theft

IP Theft: Case Study #1

- In 2018, two naturalized U.S. citizens in California were charged with illegally obtaining dual-use electronic data from a U.S. company that manufactured specialized Monolithic Microwave Integrated Circuits (MMICs) and sending that data to China.
  - (USPER) Yi-Chi Shih
  - (USPER) Kiet Ahn Mai
- Shih accessed the victim company's computer systems via its web portal after Mai posed as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States.
- After gaining access, they illegally obtained IP for export.

IP Theft: Case Study #1

- The MMICs were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese MMIC manufacturer on the Department of Commerce Entity List since 2014.
  - Shih was the president of CGTC.
  - MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures, and radar applications.
- Mai used his California-based company to pose as a legitimate domestic customer to purchase MMICs.
- In addition to seeking the MMICs, the two men also sought the company's proprietary design services.

IP Theft: Case Study #1

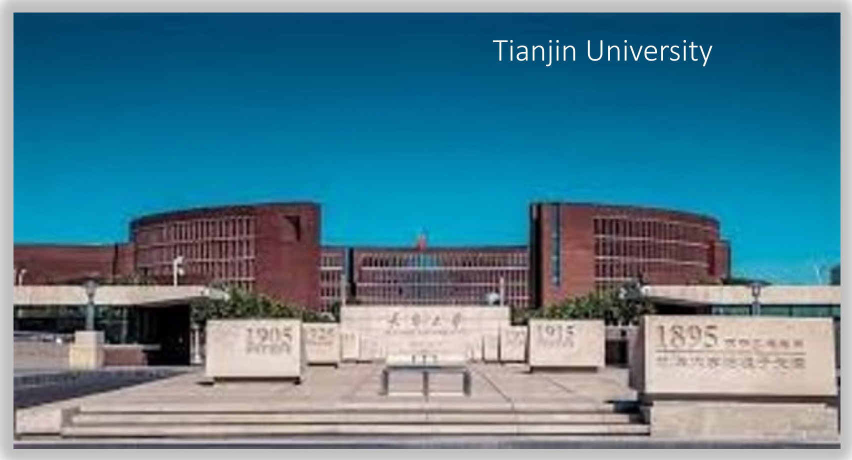
- In July 2019, a federal jury found Shih guilty of illegally shipping semiconductors with military applications to China.
- Additionally, Shih was found guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency, and conspiracy to gain unauthorized access to a protected computer to obtain information.
- Shih was an electrical engineer and also an adjunct professor at a Southern California university.
- Mai pleaded guilty in December 2018 to one felony count of smuggling and is awaiting sentencing.

IP Theft: Case Study #2

- In June 2020, Chinese national Hao Zhang was found guilty of economic espionage, theft of trade secrets, and conspiring to commit both offenses.
- From 2010 to 2015, Zhang stole trade secrets from (USPER) Avago and (USPER) Skyworks.
- California-based Avago was the leading U.S. company selling Film Bulk Acoustic Resonators (FBAR); and Massachusetts-based Skyworks was developing its own Bulk Acoustic Wave Technology.

IP Theft: Case Study #2

- Zhang conspired with another Chinese national, Wei Pang, who he met at a university in Southern California while working on a DARPA-funded FBAR cell phone technology.
- While Zhang worked at Avago and Pang at Skyworks, the two shared trade secrets. They also started a business in China to compete with the two U.S. companies.
- In 2009, at the direction of Tianjin University, they formed Novana, and relocated to the Cayman Islands.


Tianjin University

IP Theft: Case Study #2

- Zhang and Pang took Avago’s FBAR process that had taken over 20 years to develop.
- Zhang’s company and Tianjin University also took the information to compete unfairly in the cell phone RF Filters market.
- In June 2020, Zhang, Pang and four others were found guilty of economic espionage and theft of trade secrets.

Foreign Investment

- "The Chinese government directs Chinese firms to invest in and acquire U.S. companies and assets in order to obtain cutting-edge technologies and IP, fostering technology transfer in strategic industries."
- "Between 2013 and 2016, China-based firms leveraged state funding to attempt to acquire or invest in at least 27 U.S. semiconductor firms totaling more than $37 billion."

~ The U.S.-China Economic and Security Review Commission report, May 2019

Foreign Investment: Case Study

- UK firm Imagination Technologies provides an example of how Chinese entities may target struggling companies in order to acquire access to prioritized technologies.
- Imagination's stock fell 70% in 2016 after (USPER) Apple announced it would stop using Imagination's licensed graphics processing unit (GPU) technology.
- September 2017, the entire company was sold to Cayman Island-based, Canyon Bridge, funded by China's central government.

Foreign Investment: Case Study

- Canyon Bridge Capital Partners purchased Imagination for $744 million USD.
- In April 2020, China Reform attempted to place hand-picked members of a Chinese state-owned asset manager to Imagination’s board of directors.
- Imagination’s owners defended the move stating it would be helpful in plans to expand in China.
- The push for the new board members was dropped after pushback from the UK government.

Mergers, Acquisitions, & Joint Venture Threats

- Joint Ventures (JVs) can provide a starting point for foreign entities to target U.S. technology both in the U.S. and overseas.
- In return for having potentially lucrative access to China's huge domestic market, China often forces foreign firms to share valuable IP as a condition for entering into a JV.
- Commercial competitors worldwide can make JVs in any country a potential risk.
- Foreign investment and joint venture risk also extends to your customers or subcontracts.

This risk increases significantly in a country that is a strategic competitor!

Mergers, Acquisitions, & JVs: Best Practices

- Be diligent in evaluating investors and JV partners.
- Be aware that promises to protect your IP may not be honored.
- Ask uncomfortable questions about ownership, controlling interests, and ultimate sources of funding.
- Share information with each other and partner with your government contacts.

DCSA is ready to assist!

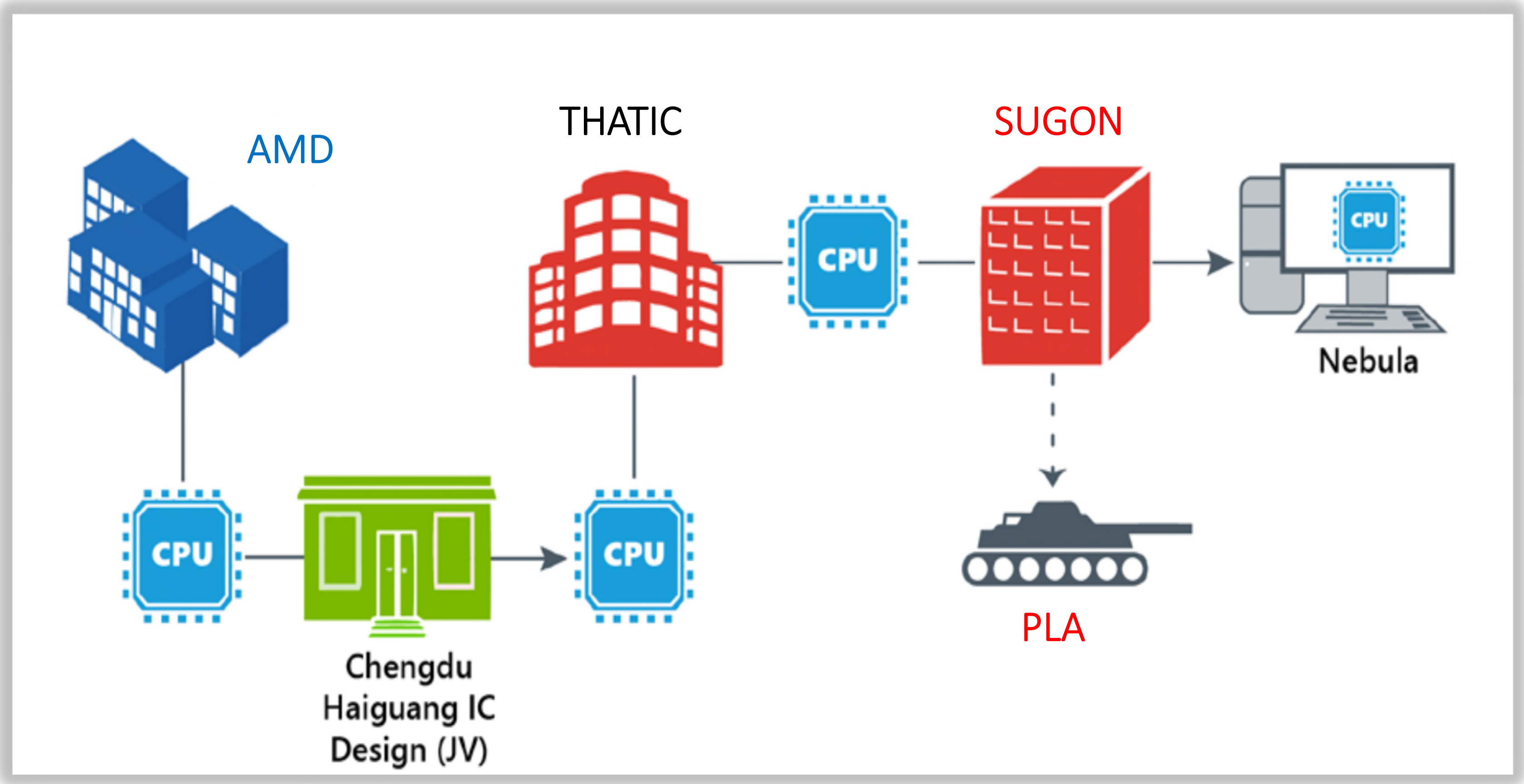
Mergers, Acquisitions, & JVs: Case Study

- In 2016, (USPER) AMD created two JVs with Tianjin Haiguang Advanced Technology Investment Co Ltd (THATIC).
- One of these companies, Chengdu Haiguang IC Design (Chengdu) is 70% owned by THATIC and 30% owned by AMD.
- AMD provided THATIC the technology license for AMD's x86 central processing unit (CPU) chip designs.
- In 2019, China-based Sugon revealed its next-generation supercomputer Nebula, which used over 300 AMD x86 CPUs that were made in China.

Mergers, Acquisitions, & JVs: Case Study

- Sugon, itself a shareholder in THATIC, gained access to AMD’s chip designs.
- In June 2019 the US Bureau of Industry and Security labeled Sugon a risk to national security due to its role in developing exascale high performance computing and acknowledgment of military end users of its technology.
- AMD’s technology licensing with THATIC helped enable THATIC to domestically produce CPUs using AMD technology, thus providing Sugon access to the technology.

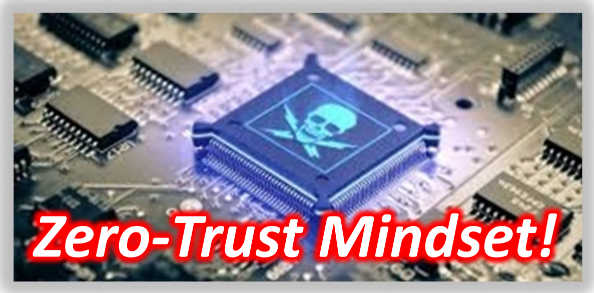
Mergers, Acquisitions, & JVs: Case Study



Supply Chain Vulnerabilities

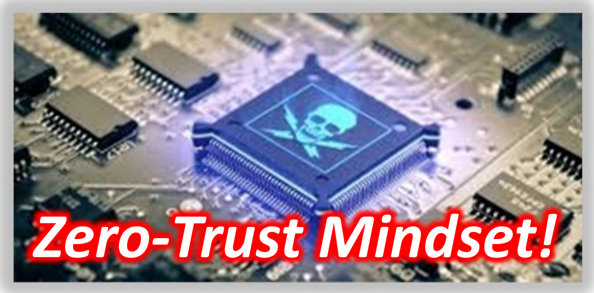
- A 2012 Government Accountability Office (GAO) report highlighted China's failure to crack down on microelectronics counterfeits and clones.
- GAO set up a fictitious company to solicit parts.
- Out of 396 responding vendors, 334 were from China.
- GAO bought 16 different parts from 13 Chinese suppliers…

All were counterfeit!



Supply Chain Vulnerabilities

- The Senate Armed Services Committee looked at the DoD supply chain over two years from 2009-2010 and found 1,800 cases of counterfeit electronics involving over one million parts.
- Over 100 cases were tracked through the supply chain with 70% attribution back to China.
- Some commonalities found included counterfeit parts changing hands multiple times, with independent and unvetted distributors often being the source.



Supply Chain Vulnerabilities

- Potential supply chain weaknesses include:
  - Counterfeits and Clones
  - Malicious Insertion
  - Tampering
  - Fraudulent Products
- Ongoing problem:
  - In 2017, the DoD estimated that up to 15% of all spare and replacement parts for its weapons, vehicles, and other equipment are counterfeit.
  - Counterfeit microchips, integrated circuits in particular, have turned up in replacement parts in various U.S. Government equipment.

Supply Chain Vulnerabilities: Case Studies #1

- From 2007–2009, Florida company (USPER) Vision Tech sold counterfeit ICs from suppliers in China and Hong Kong.
  - Sold to U.S. Navy and defense contractors as Original Equipment Manufacturer (OEM) parts
  - The company told clients the parts were from suppliers in Europe
  - Instructed employees to use large erasers to remove debris and discoloration
- In October 2011, an administrator was sentenced to 38 months in prison.
- CEO pleaded not guilty, but passed away in May 2011.
- First federal prosecution in a case involving the trafficking of counterfeit integrated circuits.

Supply Chain Vulnerabilities: Case Studies #2

- From 2007 – 2012 a Massachusetts man imported and sold thousands of Chinese and Hong Kong originated counterfeit ICs to U.S. semiconductor companies and the U.S. Navy.
- The U.S. Navy ICs were for use in nuclear submarines.
- He claimed the ICs were new and manufactured in Europe.
- Testing revealed the ICs were resurfaced changing the date code and affixing counterfeit marks.
- This was the second successful conviction in U.S. history on charges of trafficking counterfeit military goods.

"I have to buy China and risk fake parts to compete … it's my whole biz."

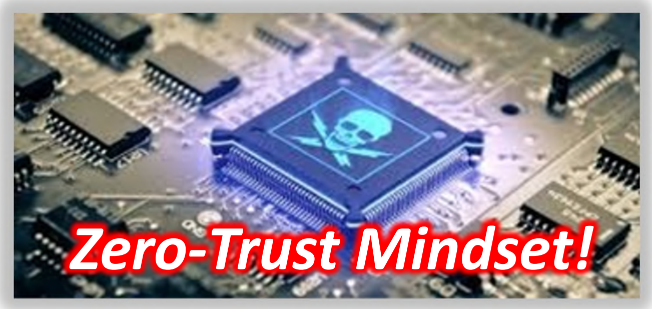
Supply Chain Vulnerabilities: Case Studies #3

- From 2007 – 2009 (USPER) Mustafa Abdul Aljaff used at least 8 fraudulent companies and various websites to sell Chinese and Hong Kong counterfeit parts to 420 buyers.
- The parts had counterfeit trademarks and military grade markings from legitimate semiconductor manufacturers.
- Some of the counterfeit items were purchased from Vision Tech.

"I stole since I could. I became convinced that I was smarter than everyone else, and that my superior intelligence entitled me to anything I could get away with. The sheer complexity of the fraud I orchestrated was its own form of intoxication, and I believed that I would never get caught."
~ Abdul Aljaff

Supply Chain Vulnerabilities: Case Studies #4

- From 2012 – 2015 Chinese company, HK Potential, trafficked counterfeit semiconductors.
- In October 2014 and March 2015 Chinese national Jiang Guanghou Yan sold 45 counterfeit (USPER) Intel microprocessors to an undercover agent, believing the parts would be used on a U.S. Navy submarine contract.
- Yan offered the agent $37,000 each for 22 stolen (USPER) Xilinx military grade semiconductors to illegally export to China and provided fake components to be substituted for the real semiconductors.



Supply Chain Vulnerabilities: Best Practices

- 2012 The National Defense Authorization Act (NDAA)
  - Strengthened import inspections
  - U.S. Government partnership with industry
- Committee on Armed Services recommends:
  - Information sharing on counterfeit materials via the Government Industry Data Exchange Program
  - Reporting and regulations (60 days)
- National Intellectual Property Rights Coordination Center
  - Operation Chain Reaction

Supply Chain Vulnerabilities: Best Practices

- Thoroughly vet foreign-owned or controlled entities
- Create scalable environments for design assurance
- Maintain obscuration and marking methods for electronic components
- Verify and validate tools yet to be developed

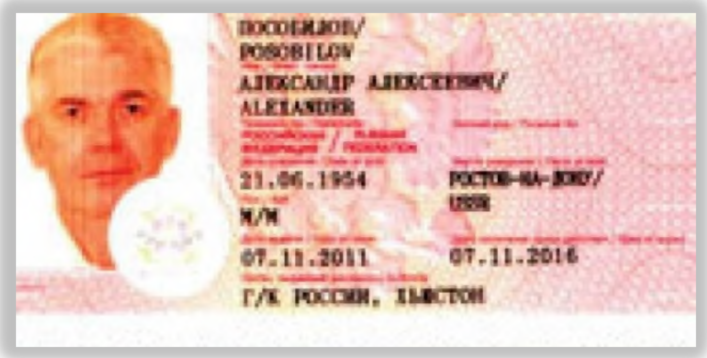
Your flexibility and input as the DoD moves to Zero Trust is invaluable to making this transition a successful and secure one.

Export Violations

- At a fraction of the cost of high-end electronic research and development, adversaries will falsify documents, use front companies, insert multiple transshipment points and transshippers to obfuscate the ultimate destination and end-use of export controlled electronics.
- In a globalized supply chain, it takes time and resources to properly vet purchase orders to ensure you do not become a victim of efforts to commit export violations.

Export Violations: Case Study #1

- In 2004 (USPER) Alexander Posobilov joined (USPER) Arc Electronics.
- From 2008 – 2012 Posobilov managed a team at Arc Electronics, working to acquire cutting-edge electronics from U.S. manufacturers for illegal export to Russian military and intelligence agencies.
- Posobilov and accomplices lied about the destinations of the purchases, sending approximately $50 million of electronics to Russia and the Russian Ministry of Defense.



ПОСОБИЛОВ/
POSOBILOV
АЛЕКСАНДР АЛЕКСЕЕВИЧ/
ALEXANDER
РОССИЙСКАЯ / RUSSIAN
ФЕДЕРАЦИЯ / FEDERATION
21.06.1954
РОСТОВ-НА-ДОНУ/
USSR
М/M
07.11.2011
07.11.2016
Г/К РОССИИ, ХЬЮСТОН

Export Violations: Case Study #1

- Posobilov and accomplices hired Russian-speaking salespeople to lie to vendors and falsify export records.
- Seven of Arc Electronics' top ten clients were specially authorized to procure military parts by the Russian Ministry of Defense.
- Arc's Russian customers included a research unit for the FSB, Russia's internal security agency, and entities building air and missile defense systems.
- Eight former employees either pled guilty or were convicted in the illegal export scheme.

Export Violations: Case Study #2

- U.S.-Russian dual citizen (USPER) Alexey Barysheff, a Brooklyn resident, and two Russian nationals based in Denver were arrested in October 2016 for operating U.S.-based front companies to illegally send export controlled ME components to Russia.
- Brooklyn-based front companies (USPER) BKLN Spectra, Inc. and (USPER) UIP Techno Corp. were established in 2015 to facilitate the purchase and illegal export of ME components to Russian entities.
- The electronic components acquired from U.S. vendors included digital-to-analog converters and ICs frequently used in radar and surveillance systems, missile guidance, and satellites.

Export Violations: Case Study #2

- To evade export restrictions, they concealed they were exporters, falsified shipping and export control records, and shipped the components to Russia via Finland.
- Barysheff pleaded guilty to submitting false export information, and was sentenced to time served in October 2017.
- The Russian nationals pleaded guilty to conspiracy to violate IEEPA and were sentenced to time served and were ordered removed from the United States on May 2, 2017.

Cyber Threats

- After years of news reports of successful cyber infiltrations and attacks targeting U.S. companies, the U.S. public and private sectors are exercising increased vigilance in the cyber domain.
- Increased awareness and implementation of more robust cyber defenses does not necessarily guarantee cyber safety.
- It’s becoming more and more difficult to detect attacks targeting Electronic Design Automation (EDA) tools.

Cyber Threats: Best Practices

Just to name a few:

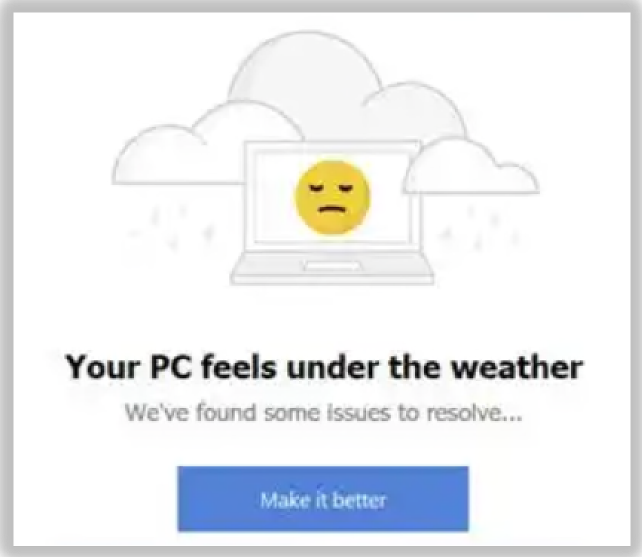
- Phishing training and awareness
- Patching vulnerabilities (zero-day)
- Multi-factor authentication
- Access controls, user account audits, reduce privileges
- Review Bring Your Own Device (BYOD) policies
- Application Whitelisting (AWL)
- Segment networks
- Lock down unused ports, turn off unused services
- Strong password policies
- Secure remote access, limit access
- Monitor and respond
- Data loss prevention

Cyber Threats: Case Study #1

- In 2017, hackers compromised a popular computer cleanup tool, CCleaner, developed by British company Piriform.
- Piriform’s servers and CCleaner‘s software updates were tainted with a malware backdoor, creating a digital supply chain vulnerability.
- Over 2.2 million corrupted versions were downloaded, with official releases containing malware.
- Czech cybersecurity company Avast then acquired CCleaner along with its corrupted servers.

Cyber Threats: Case Study #1

- Hackers used stolen credentials to log into a remote desktop account on a developer computer, and moved laterally, working after office hours.
- Of the successful downloads, 40 companies were specifically targeted with ShadowPad malware, resulting in 11 companies being infiltrated.
- The malware was linked to Chinese-speaking creators, and some communicated to South Korean and Russian organizations.
- CCleaner was targeted again in 2019 and its internal network compromised.



Your PC feels under the weather

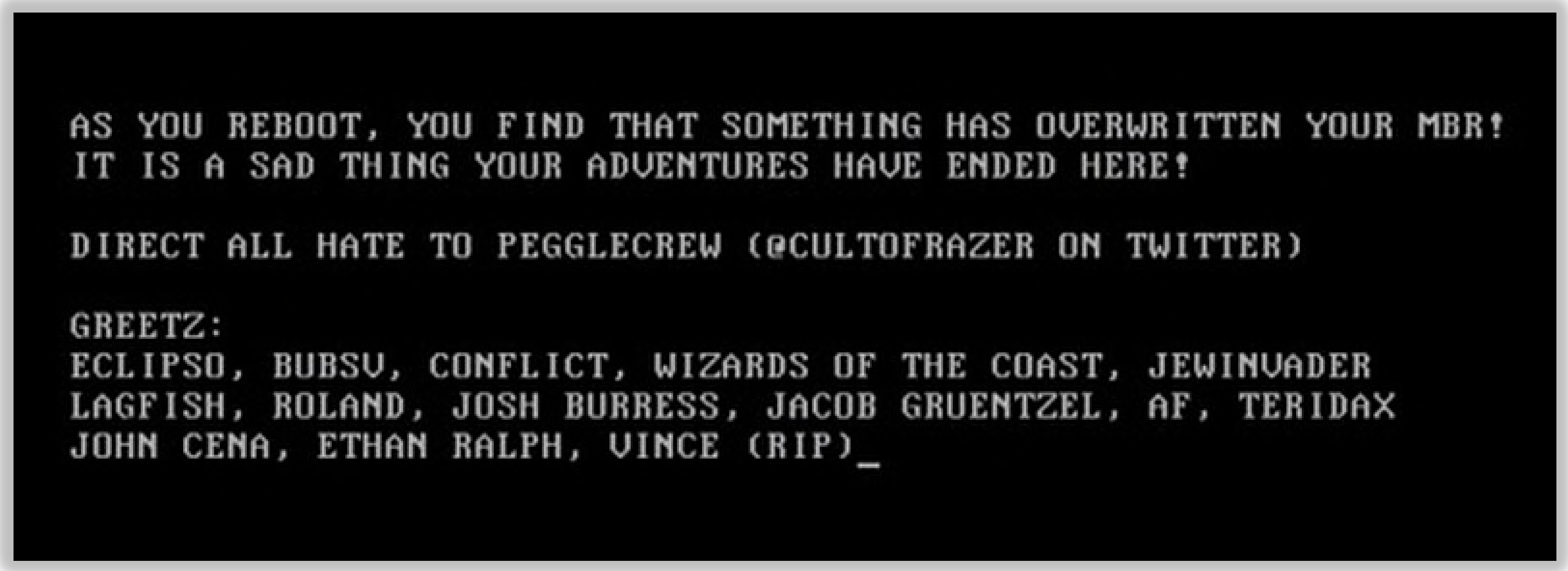
We've found some issues to resolve...

Cyber Threats: Case Study #2

- In 2011, (USPER) SourceForge detected an intrusion affecting their Concurrent Versions System (CVS), ViewVC, file release uploads, and interactive shell services.
- Attackers compromised the main server and inserted a backdoor into the software code.
- They then mirrored the compromised software to all software distribution sites so the compromised version was available for download.

Cyber Threats: Case Study #3

- In 2016, attackers compromised the website (USPER) FossHub. They injected malware into a download server, so downloads would contain a Trojan that would rewrite the user's Master Boot Record (MBR).



```
AS YOU REBOOT, YOU FIND THAT SOMETHING HAS OVERWRITTEN YOUR MBR!
IT IS A SAD THING YOUR ADVENTURES HAVE ENDED HERE!

DIRECT ALL HATE TO PEGGLECREW (@CULTOFRAZER ON TWITTER)

GREETZ:
ECLIPSO, BUBSV, CONFLICT, WIZARDS OF THE COAST, JEWINVADER
LAGFISH, ROLAND, JOSH BURRESS, JACOB GRUENTZEL, AF, TERIDAX
JOHN CENA, ETHAN RALPH, VINCE (RIP)_
```

Insider Threat

Definition:

- The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

The "insider threat" is the most damaging

Money

Compromise

Revenge

Ideology

Ego

Insider Threat: Best Practices

Personnel Security:

- Report foreign travel.
- Report and update foreign contacts and overseas relatives.

Defense Personnel and Security Research Center (PERSEREC) analysis of historical espionage cases revealed that spies with foreign relatives:

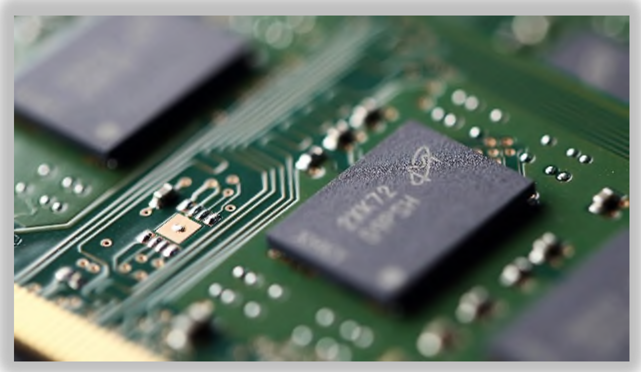
- Were more than twice as likely to have been recruited by foreign intelligence services.
- Were less likely to have failed in their espionage.
- Committed espionage for a greater length of time.

Insider Threat: Case Study #1

- In 2018, three Taiwanese nationals, a Taiwan semiconductor foundry, and a Chinese-owned company were charged with conspiracy to steal trade secrets from (USPER) Micron Technology.
  - United Microelectronics Corporation (UMC)
  - Fujian Jinhua Integrated Circuit, Co., Ltd. (Jinhua)
- Micron is a global leader in Dynamic Random Access Memory (DRAM).
- Micron was the only United States-based company that manufactures DRAM.
- Prior to this event, China did not possess DRAM technology.

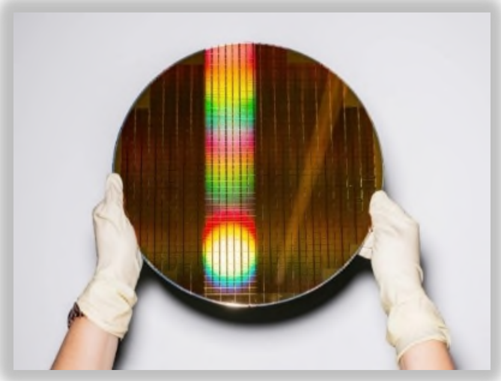
Insider Threat: Case Study #1

- In 2013, Zhengkun “Stephen” Chen was the General Manager/Chairman of a Micron acquisition.
- Chen became the president of Micron’s Taiwanese subsidiary that manufactured one of their DRAM chips.
- In 2015 Chen resigned and went to UMC, organizing a joint venture between UMC and Jinhua. Jinhua planned to mass produce UMC’s DRAM technology, and Chen eventually became president of Jinhua.



Insider Threat: Case Study #1

- Chen recruited numerous employees to leave the subsidiary and join Jinhua.
- Two recruited employees from Micron's Taiwan subsidiary, Jianting "J.T." He and Yungming "Kenny" Wang, downloaded over 900 confidential and I.P. files, and used external hard drives and cloud storage to transfer the DRAM files.
- On October 28, 2020, UMC pleaded guilty to criminal trade secret theft and was sentenced to pay a $60 million fine, in exchange for its agreement to cooperate with the government in the investigation and prosecution of Jinhua.



Insider Threat: Case Study #2

- In 2018, Chinese citizen, Xiaolang Zhang was indicted on theft of trade secrets for taking a confidential document including drawings of a circuit board designed for an autonomous vehicle being developed by Apple.
- Zhang resigned from his job saying he needed to return to China to take care of his sick mother.
- Apple immediately terminated Zhang's access and began a forensic analysis of his Apple devices and network activity.
- Days before resigning, Zhang's network activity increased notably, including while supposedly on vacation.

Insider Threat: Case Study #2

- His network activity included downloads to his wife's laptop of trade secret intellectual property.
- Apple subsequently learned Zhang went to work for China based X-Motors, a company focused on electric vehicles and autonomous vehicle technology.
- After Zhang purchased a last-minute round-trip plane ticket to China, he was arrested at the San Jose Airport.

Summary - What Can You Do?

Identify, prioritize, and commit to protecting your IP:

- **Know who you are doing business with**
  - Vet 3rd party vendors
  - Understand vendor’s security practices
  - Set minimum security standards
  - Ask questions before procuring products/services
- **Strengthen cyber security and hygiene**
  - Protect credentials by using two-factor authentication
  - Patch regularly
  - Beware of spear phishing
  - Social media privacy and security settings
- **Assume you have no privacy while traveling abroad**

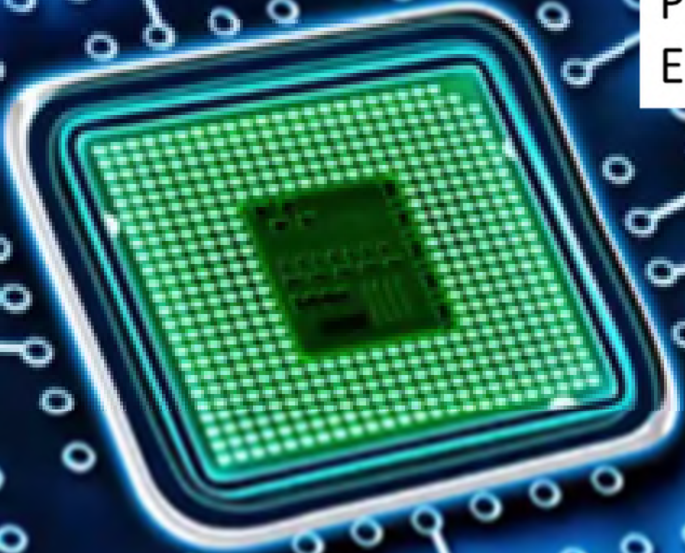
Summary - What Can You Do?

Identify, prioritize, and commit to protecting your IP:

- **Implement Insider Threat Programs**
  - Trusted insiders with access are often gravest threat
- **Institute an enterprise-wide security posture**
  - Socialize and practice policies twice a year
  - Include Acquisitions, Procurement, and Human Resources personnel in security plans
- **Maintain connectivity to the U.S. government**
  - Obtain current threat information and best security practices
  - Use all resources available to assist in protecting your IP and understanding the risk

Questions?

CI Special Agent Michelle Yoworski
Phone: 919-475-2021
Email: Michelle.l.Yoworski.civ@mail.mil



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

USPER Tracker

1. Mark Lewis (Director of Defense Research and Engineering for Modernization)
2. Dr. Lisa Porter
3. IC Insights
4. Investors Business Daily
5. Yi-Chi Shih
6. Kiet Ahn Mai
7. UCLA
8. Avago
9. Skyworks
10. Apple
11. AMD
12. Intel
13. Vision Tech
14. Mustafa Abdul Aljaff
15. Xilinx
16. Alexander Posobilov
17. Arc Electronics
18. Alexander Fishenko
19. Alexey Barysheff
20. BKLN Spectra
21. UIP Techno Corp.
22. SourceForge
23. FossHub
24. Micron Technology