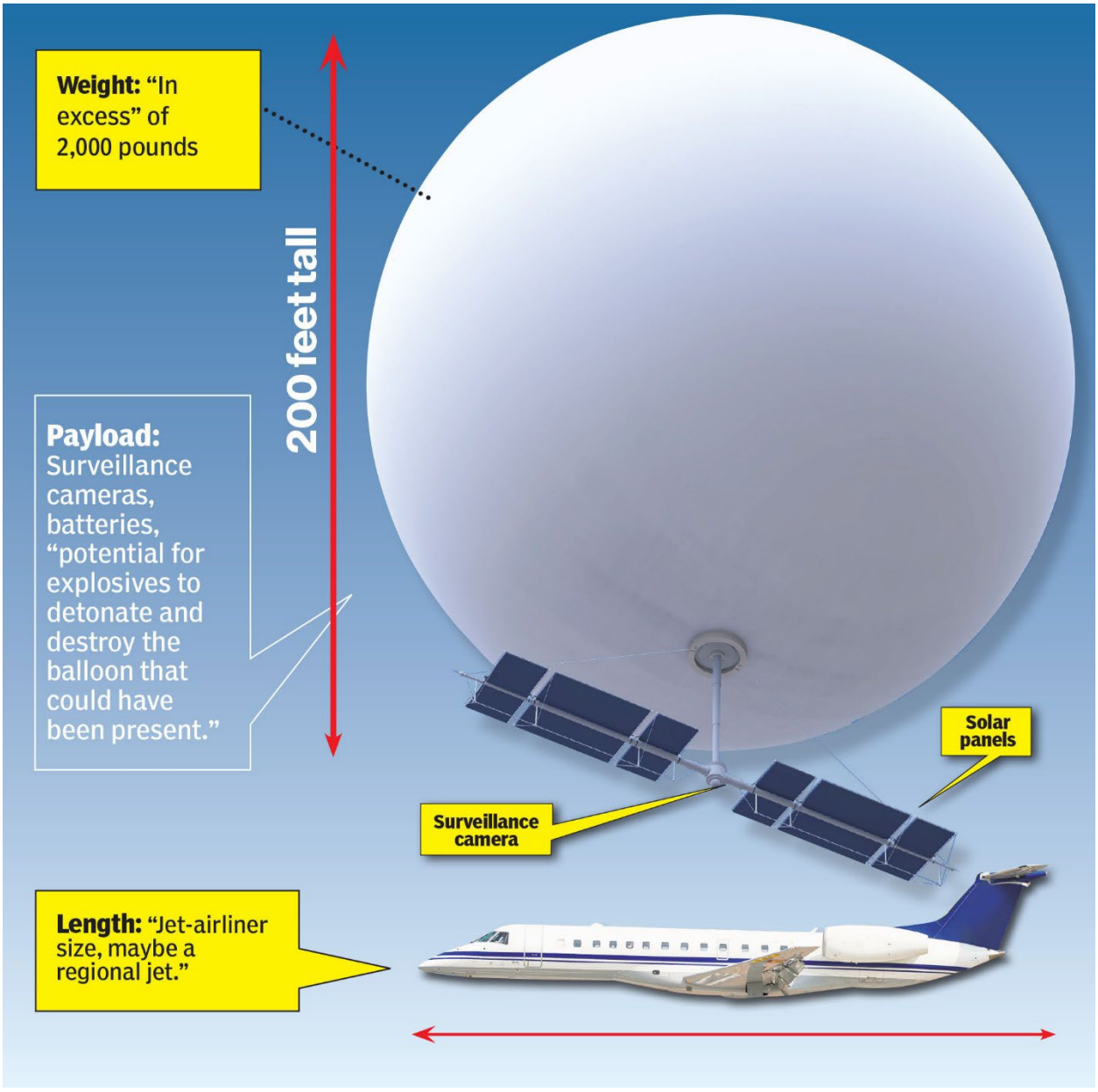
Dangerous Chinese Microelectronics don't always come with Balloons



2023 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Team Introductions

Area	First Name	Last Name	Email	Organization
Private Sector	Joseph	Cawley	Joseph.Cawley@Lanops.Com	Lanops
Private Sector	Thomas	Gardner	Thomas.Gardner@Hp.Com	HP Federal
Private Sector	Sarah	Ireland	Sireland@Securecommunitynetwork.Org	Secure Community Network Inc
Private Sector	King-In	Marshall	King-In.Marshall@Ballaerospace.Com	Ball Aerospace
Private Sector	Emily	Robertson	Emily.Robertson@Lcra.Org	Lower Colorado River Authority
Private Sector	Thomas	Watson	Thomas.Watson@Rtx.Com	Raytheon Tech
Private Sector	Rick	Randall	Rrandall@Mitre.Org	The MITRE Corporation
Government	Vincent	S		DHS I&A (The Office of Intelligence & Analysis)
Government	Daniel	M		DHS HSI (Homeland Security Investigations)
Government	Matthew	D		U.S. Air Force
Champion	Glenn	B		U.S. Navy

We deeply appreciate our subject matter experts that were a valuable resource for the development of this paper. Thank you for making such a valuable contribution to our team.

First Name	Last Name	Title	Organization
Carlos	Cuellar	Principal Failure Analysis Engineer/Team Lead	RTX Failure Analysis and Component test Laboratory
Diganta	Das	Dr - Research Associate Mechanical Engineering	University of Maryland Center for Advanced Lifecycle Engineering
Fred	Schipp	Electronics Engineer	Naval Surface Warfare Center
Henry	Livingston	Retired Technical Director and Engineering Fellow	BAE Systems Retired
Luigi	Aranda	Sr. Manager Failure Analysis Lab	RTX Failure Analysis and Component test Laboratory
Michael A.	Ach	Branch Chief – Enforcement Division	U.S. Customs and Border Protection Electronics Center of Excellence and Expertise
Sam	Jensen	Principal Electrical Engineer Component Testing	RTX Failure Analysis and Component test Laboratory
Sonny L.	Kilmer	Senior Industry Liaison, Intellectual Property Rights Center	Homeland Security Investigations
Brent	Rogan	Special Agent - Counter Proliferation Investigations	Homeland Security Investigations
Yolanda	Benetiz	Assistant Center Director	U.S. Customs and Border Protection Electronics Center of Excellence and Expertise

Homeland Security

Impact of counterfeit Chinese microelectronics on the supply chain gap analysis

Index

DISCLAIMER STATEMENT: *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.*

1.0 Target Audience

Companies that seek to better understand the Chinese counterfeit microelectronic threat, how this can be mitigated, and what resources are available to these companies

2.0 Objectives and Scope

The main aim of this document is to familiarize the reader with counterfeit microelectronics and potential ways to minimize risk of introduction, and those that would help remediate it.

3.0 Executive Summary

This study on Chinese Counterfeit Microelectronics covered a broad area impacting many markets. Our team consisted of professionals in profit and non-profit industry, the intelligence community, homeland security, defense and academia. The format covers the common research questions of Who, What, why, When, Where, and How. The paper identifies some common best practices and recommendations to mitigate the problem. Because of the unclassified nature of the study, it does not go into counterfeit practices in the intelligence community or specific government activities, but the best practices and recommendations would apply for those cases as well. Further study on this subject is recommended at the classified level, especially since the damage to national security is highest there.

Who? Outside of intelligence actors the who is the Chinese small electronics business and the Chinese criminal element. Why? They are motivated by profit. Like most people in this world, they are just trying to make ends meet and put food on the table. They have little understanding of the concept of intellectual property and even those that do lack the ethical framework necessary not to sell to a buyer that is demanding their products or goods.

What? They are often taking recyclable or discarded electronics and stripping off the valuable components and chips. They will modify the serial number or nameplate data or just start with a blank.

Where? Most of the counterfeit activity occurs in the industrial cities or near the international shipping ports. When? This is a continuous ongoing activity motivated by profit and a market demand for hard to get or cheap products.
How? The use of cheap labor, available supplies or electronic waste, lack of environmental regulations or controls and government and police willing to look the other way allows this market to flourish. As economic cooperation with China deteriorates the problem grows worse.

Mitigation? The best mitigation is an in-depth knowledge of your supply chain. This includes not just first tier, but second and third tier as well. Supply Chain Risk Management (SCRM) practices should follow practices described by the DHS SCRM Task Force. This is similar to the Cyber Risk Management Framework as described in the NIST 800 series documents. Study the potential risks and invest in knowing your suppliers. Buy only from Original Equipment Manufacturers (OEM) or their designated and approved channel partners. If force to buy from eBay or non-approved vendor, because of lack of part availability, consider independent testing of the parts before system use.

This study is an overview of the problem. More study is required within the IC to mitigate the use of counterfeit microelectronics in intelligence activities.

.

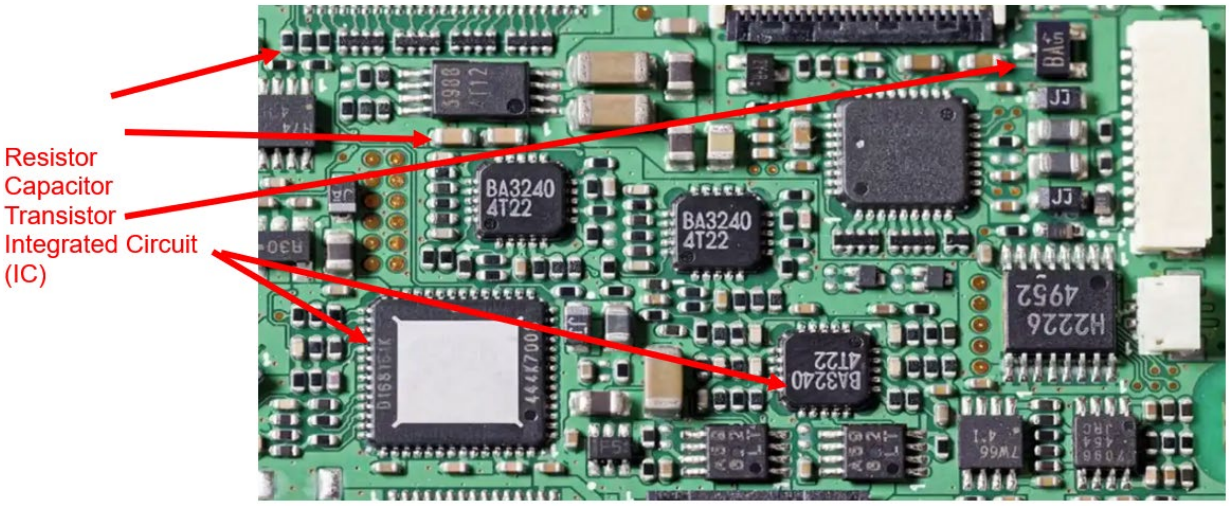
4.0 What is counterfeit microelectronics, an overview

The Oxford Learners online dictionary defines microelectronics as:
"using or relating to very small electronic circuits".

(https://www.oxfordlearnersdictionaries.com/us/definition/english/microelectronic)

For the purpose of this paper microelectronics will include objects ranging from discrete components (resistors, diodes, inductors, connectors, etc.) to active components (transistors, diodes, and integrated circuits) to finalized products such as routers, switches, LRU (line replaceable unit). See the figure below for a representative LRU with common microelectronics referenced. Counterfeit microelectronics are microelectronics that are intentionally misrepresented and "often have inferior specifications and/or quality, they may represent a hazard if incorporated into critical systems such as aircraft navigation, life support, military equipment, or space vehicles."

(SOURCE: https://en.wikipedia.org/wiki/Counterfeit_electronic_components)



Assuring that Microelectronics are both reliable and secure is critical for U.S. national and economic security. In today's global electronics supply chain, hardware and software vulnerabilities are increasingly prevalent, and a whole-of-government and industry solution is needed to ensure a long-term supply of microelectronics enabling our domestic capabilities.

5.0 Who is doing it, why, and where

The "who" will focus on the Chinese entrepreneur and commercial side of counterfeiting and smuggling, and why China has been the main source for this counterfeiting to the US. It will not focus on "state-sponsored" counterfeiting.

5.1 Why do they do it

Different actors do it for different reasons we cover the breakout in the following:

5.1.1 The demand side

There is a market for counterfeit goods in the US. In 2022, the counterfeit electronics risk organization ERAI, Inc. reported 768 suspect counterfeit and nonconforming parts, fewer than the record 1,282 parts reported in 2011 but a 35 percent increase over the previous year that may represent a return to pre-Covid levels of demand.

Source: https://www.erai.com/erai_blog/3181/2022_annual_report

The market takes advantage of buyers that have not put in place supply chain measures and are desperate to find a particular part. Buyers may be seeking out-of-production parts because of lack of parts lifecycle planning. However, while 32.5 percent of parts reported to ERAI in 2022 were identified as "obsolete" or "not for new design", 62.2 percent were classified as "active" parts, suggesting that it is not only the search for out-of-production parts that drives demand. Low-cost products sought by unscrupulous brokers or buyers in order to pad margin or meet a requirement. Sometimes "lowest price/Least Cost" drives towards counterfeit and sometimes it is the simple convenience to an organizational buyer of purchasing a part online without having to submit a supplier for supply chain review.

5.1.2 The supply side

Cultural and enforcement: Counterfeit and pirated goods from China, together with transshipped good from China to Hong Kong, accounted for 75 percent of the value of counterfeit and pirated goods seized by US Customs and Border Protection in 2021, according to the Office of the US Trade Representative. The Chinese have no problem counterfeiting culturally, ethically, or morally. It's just another form of doing business….and making money! The concept of intellectual property is unknown or discarded in many cases. There are multiple links and players, all of whom have one common motive … money. Going after the money is the key to disrupting these practices.

A common method for counterfeiting electronic parts begins with the acquisition of legitimate discarded parts from piles of electronic waste. Some of these junk parts have been recently discarded, and others are decades old, meaning that some of these

components, from the very moment they're acquired, are destined to fail should they find themselves in modern equipment.

A variety of techniques, including surface sanding, acid washes, river washes and exposure to open flames, are then used to conceal the true origin of the part. Following the concealment process, the parts are often relabeled as a better or matching grade using lasers and digital printing techniques, before being packaged and sold to brokers across the globe.

Another method of counterfeiting electronic parts follows the same process of supply chain introduction; however, the parts, instead of being acquired from a pile of waste, are manufactured as blanks in a factory before being marked, packaged and sold.

5.2 The actors

5.2.1 Individual mom-and-Pop shops

These are usually vendors seeking to profit from suppliers in a tight spot and through an adversary who's created a cloned part that's home to a cyber backdoor. "There is more incentive than ever to profit off of counterfeit components just by advertising that you have them available within the supply chain when no one else does," This is usually just for pure profit motives, sometimes shell companies/presences are set up and then gone before the fraud is detected. Sometimes it is a straight rip-off other times they do actually deliver the fraudulent goods to extend the fraud.

5.2.2 Criminal actors

Like the mom-and-Pop shops are in it for the money, the difference is that they go beyond a simple theft to more malicious attacks. For them it is not only making money on the part but giving them the ability to leverage that part to compromise the larger system that it is part of increasing the payout.

5.3 Where is it done?

There are multiple locations but the focus for this paper will be China.

5.3.1 Physical locations:

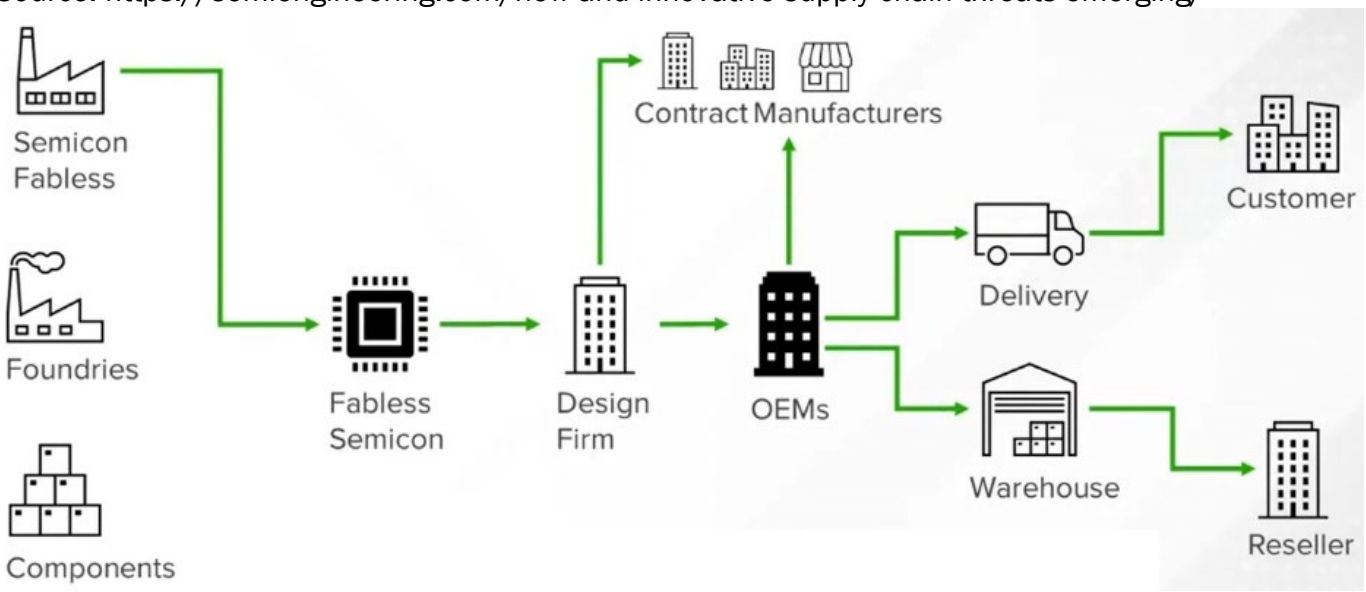
Foreign: The same regional centers that produce valid microelectronics are natural areas for counterfeit production because of access to feedstock, transportation infrastructure for import and export, and workers that may have experience in the electronics industry.
Major centers are: Beijing, Shandong, Fujian, Hong Kong, Shenzhen)
Domestic: Remarking of feedstock does not only take place overseas. Genuine chips can be imported to the US and remarked domestically or misrepresented.
Chinese personnel have come to the US to establish a local footprint for distribution.
a lot of blank chips come in and are marked in the US according to customer needs.
If chips are not marked, they cannot be considered counterfeit.

5.3.2 Virtual locations:

The spread of global marketplace and auction sites, including those based in China with lax counterfeiting policies, has made it easier for unwary or unscrupulous buyers to access counterfeit microelectronic components.
Examples of out-of-production chips on online auction and marketplace sites.
AliExpress and Tencent on USTR counterfeit list
A US person who pled guilty to trafficking in fraudulent and counterfeit Cisco networking equipment in June 2023 ran at least 19 companies as well as 15 Amazon storefronts and at least 10 eBay storefronts, Justice.

5.4 A typical counterfeit network would look like this.

Source: https://semiengineering.com/new-and-innovative-supply-chain-threats-emerging/



5.4.1 And include:

1. Raw material suppliers
2. Freight agents smuggling controlled components “in” the manufacturer
3. The manufactures who make the actual make product
4. The printers who make the packaging
5. The China based traders who link overseas buyers with the manufacturers
6. The international traders who manage the global trade and distribution
7. The logistics agents who get the goods out of China to the end market
8. The corrupt Government or local officials who allow the manufacture and export to go ahead unmolested
9. The end market wholesale buyer

10. Distribution in the end market
11. Commercial seller
12. The end buyer/final customer
13. Money laundering service providers
14. Mislabeled products

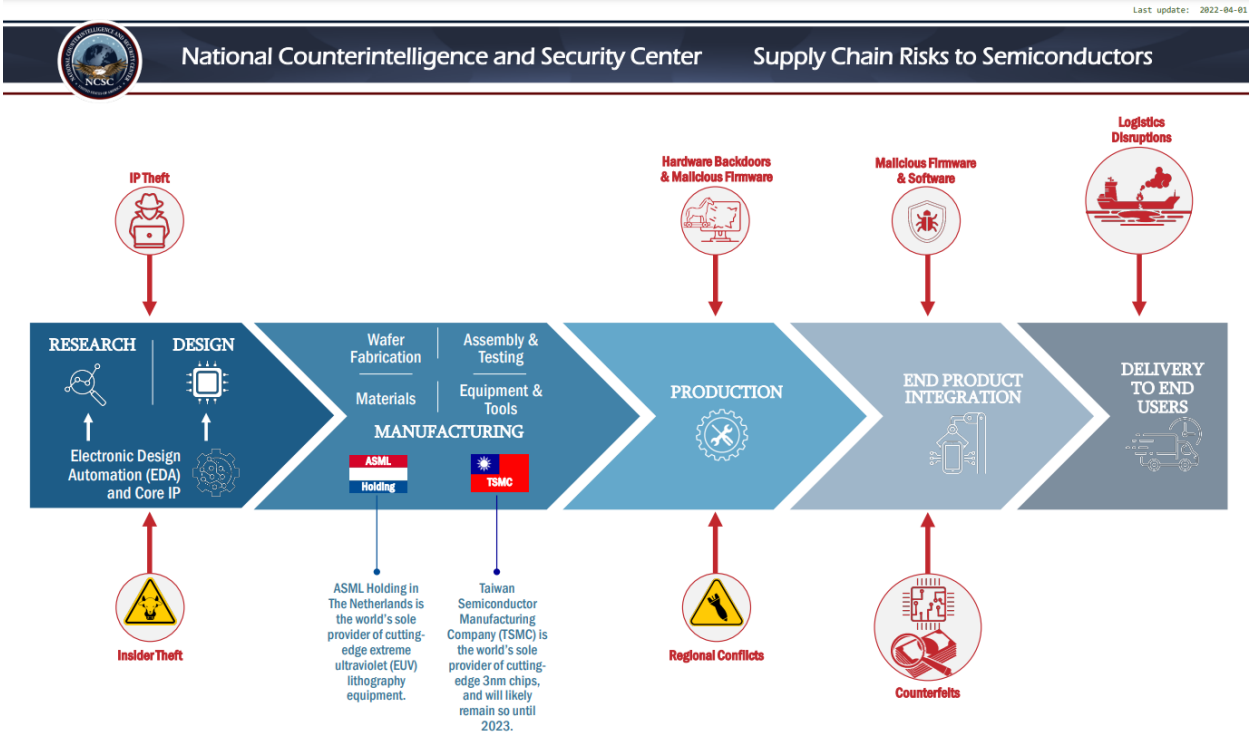
Examples:

https://www.justice.gov/usao-ndtx/pr/texas-man-who-lied-about-origin-chinese-made-products-sentenced-4-years-prison-ordered

https://www.justice.gov/usao-edny/pr/aventura-technologies-inc-and-its-senior-management-charged-fraud-money-laundering-and

6.0 How does it get into the supply chain

There are gaps in cooperation between private industry and government that facilitate Chinese counterfeit microelectronics That is the part of the supply chain we will focus on.



Source: https://www.dni.gov/files/NCSC/documents/supplychain/semiconductor-supply-chain-2022-39E2C6B0-.pdf

The COVID-19 pandemic greatly expanded and magnified vulnerabilities already present in the microelectronic supply chain. The loss of control due to off-shoring needed to be remediated especial for critical business and defense sectors.

Over the last decade as China's and Asia's share of the electronic supply chain steadily grew to over 90% very little was done at a local level to effectively counter the fraud, it was just too widespread and of minimal impact to most civilian applications.

The Global shortage of semiconductors during Covid highlighted the U.S.'s over dependence on Asian markets to reliably support our electronic infrastructure leaving U.S. industry Highly vulnerable.

Some contributing factors that enable counterfeit parts:

- Dynamic inter-layered supply chains
- No chain of custody
- Least cost
- Lack of parts for parts for past end-of-life equipment
- Assumption of like “New “quality or equivalent
- Lack of or no testing
- Concern over self-reporting.

7.0 The impact to the government and private sector

What Happens When a Counterfeit Part Enters the Supply Chain?
The impact of counterfeiting usually falls into one of three categories:

7.1 Non-functional parts – These parts result in immediate problems when they do not function as expected. Since counterfeiters are usually profit motivated it is unlikely the parts have been tested and any nonfunctional devices will go straight to the end user. If the end user has bought additional components as spares there may be a significant time between receiving and realizing the parts are nonfunctional. For safety critical systems, this may result in those safety critical systems being down when they are needed most.

7.2 Functional substandard parts – These can expose a company to liability because the components work as expected, but they may be refurbished or substandard, and can quickly deteriorate after the end user begins using them. Some consequences of functional substandard parts.

- Premature system failures also known as reduction in Mean Time Between Failures (MTBF)

- Loss of credibility with customers MTBF reduction

- Increased costs due to:
    - Additional root cause analysis
    - Increased rework and repair
    - Increased scrap
    - Excessive inventories requiring additional storage and tracking

- Longer-than-necessary lead times when spares are depleted earlier than anticipated due to MTBF reduction.

- Quality and reliability failures - quality issues resulting from product defects or inadequacies that can lead to system vulnerabilities or degraded life-cycle performance.

- Loss of access - occurs when the DoD has limited or no access to a particular component. 'Constant vigilance'

7.3 This paper focuses primarily on for profit, remarked, counterfeit microelectronics and does not directly address clones and Trojans.

Most of the mitigations listed will reduce the risk of exposure to clones and trojan microelectronics as well. Clones and Trojans identify two different types of counterfeits and there is a difference between them. Clones attempt to mimic the device they are replacing commonly using a more advanced microelectronic and programming it to mimic the original device behavior. Trojan devices will also mimic the anticipated functional behavior but have a trigger or backdoor to allow an adversary to introduce malware.

7.4 Some examples:

7.4.1 Servers

"Now, with it often taking as long as two years to obtain some components from approved sources, electronics manufacturers find themselves facing fewer options. The most common counterfeits are not malicious, Martin said, and might simply have had their serial numbers altered to disguise that they're not suited for military purposes."

Source: https://www.legacycomponents.com/component/content/article/26-news/50-counterfeit-components-market-on-the-rise?Itemid=1259

7.4.2 Buildings and equipment

"Officials say that between approximately December 2017 and December 2020, Montenes bribed a procurement officer at a DOE laboratory in Virginia to enter into contracts for electronic components that MSHT would supply to the lab. The payments ranged $500 to $7,200, which Montenes mailed from Long Island the procurement officer in Virginia. During the bribery scheme, the procurement officer, whom officials call "Co-conspirator 1," awarded contracts worth more than $969,000 to MSHT, which represented 95% of all of MSHT's sales to the DOE's Virginia laboratory.

Some of the electronic components sold by MSHT to DOE, based on Montenes's bribes, went on to fail and cause a fire, officials said. This resulted in approximately $1.8 million in repairs and other costs to DOE."

Source https://libn.com/2023/05/03/li-business-owner-pleads-guilty-in-scheme-to-obtain-1m-in-federal-contracts/

7.4.3 Aircraft

"In the case of the June 2020 death of Air Force pilot 1st Lt. David Schmitz, the lack of transparency may have proved deadly. Schmitz died after his parachute didn't deploy from his malfunctioning ejection seat, which the Air Force Research Laboratory said may have had up to 10 counterfeit and faulty transistors and semiconductor chips."

Source: https://www.military.com/daily-news/2021/06/19/air-force-knew-it-had-ejection-seat-problem-didnt-speed-fix-then-pilot-died.html#:~:text=There%20was%20no%20shortage%20of%20missteps%2C%20accidents%20and,cable%20arrest%20while%20landing%20with%20his%20busted%20gear.

While the lab said the parts were "suspect," it noted more analysis would be required to determine if they were truly counterfeit.

7.4.4 Security Electronics

China has to altered its label practices at the behest of the U.S. customer:

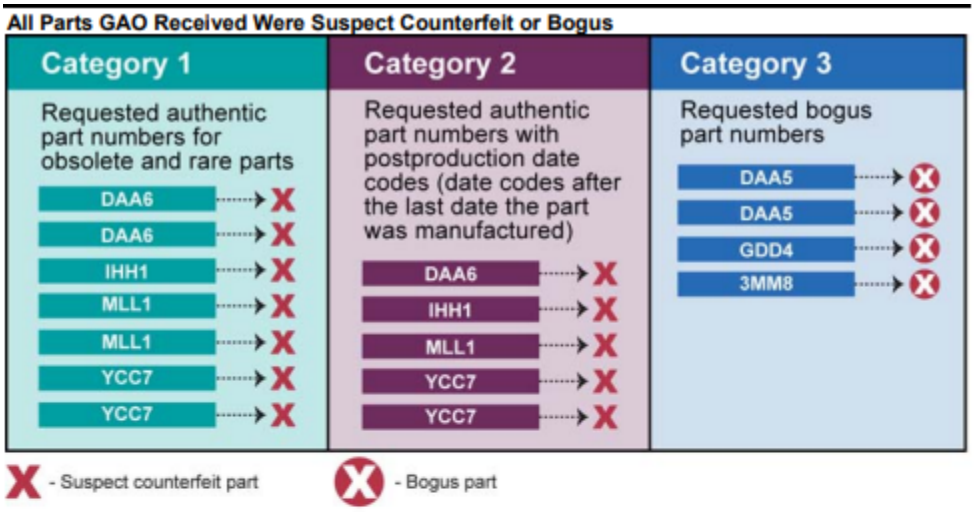
A NY-based surveillance and security company knowingly sold Chinese-made products, with known vulnerabilities, to U.S. government and Department of Defense components by passing the products off as American-made. The company worked with Chinese manufactures to conceal the Chinese origin by not printing the manufacturer's initials on the circuit boards. By marketing the products as American-made the company was able to charge a premium for security conscious customers. (USA v Aventura Technologies, Inc)

A Texas-based company defrauded the U.S. government by claiming their security electronics were manufactured in the United States when they were really made in China. The company, which claimed to be "a USA Manufacturing Company" would purchase products from China and remove labels indicating the true country of origin and replace them with labels indicating that the products were made in Texas. Company employees even requested that the Chinese manufacturer stop labeling the items and the packaging with Chinese characters. The company sold security cameras, solar powered light towers, digital video recorders, and other electronics to DHS and other government agencies. (USA v Suhaib Allababidi)

Please Note **Legally only the OEM (Original Equipment Manufacturer) can state if a product is counterfeit.**

7.4.5 Fraud Test

The willingness of the market to supply counterfeit parts was tested by the GAO By deliberately requesting non-existing parts.



Source: GAO analysis of independent laboratory test results.

Note: Part numbers shown have been altered from the part numbers used for purchasing.

Specifically, all 12 of the parts received after GAO requested rare part numbers or postproduction date codes were suspect counterfeit, according to the testing lab. Multiple authentication tests, ranging from inspection with electron microscopes to X-ray analysis, revealed that the parts had been re-marked to display the part numbers and manufacturer logos of authentic parts. Other features were found to be deficient from military standards, such as the metallic composition of certain pieces. For the parts requested using postproduction date codes, the vendors also altered date markings to represent the parts as newer than when they were last manufactured, as verified by the parts' makers. Finally, after submitting requests for bogus parts using invalid part numbers, GAO purchased four parts from four vendors, which shows their willingness to supply parts that do not technically exist.

United States Government Accountability Office

8.0 Are there any preventative measures

Face to Face is the most important thing for selecting partners. Its Supplier verification, plain and simple. Trust but verify.

Buyers can reduce the risk of introducing counterfeit microelectronics in their supply chain by purchasing from trusted sources: authorized distributors or original component manufacturers. Most counterfeit components enter the supply chain from independent distributors.

Need to limit the minimum threshold for small business, not just the department of defense based on what does the supplier need to do?

Following are some steps to help control your overseas supply chain:

Order from OEM whenever possible.

When OEM is not feasible check with OEM to determine who their authorized distributors are. Commonly this can be done by searching the OEM's website or contacting their regional sales office.

OTHER methods that can be used before physical inspection to minimize risk

While parts lifecycle planning should be included in every product, buyers may still have to seek out-of-production parts. In these cases, buyers can reduce risk by seeking out brokers and independent distributors that test their components, are part of public and private reporting networks, and adhere to commercial anti-counterfeiting standards.
Buyers can seek out brokers that utilize testing laboratories and other means to verify the authenticity of products.

Accreditations or membership in professional organizations such as ERAI—which are primarily independent distributors—or the Electronic Components Industry Association (ECIA) or registration with government databases such as GIDEP can indicate.

Purchase from sources that utilize mitigation resources such as AS6496 Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution

Not searching out counterfeit parts on eBay or storefronts that appear to be drop-shippers.

Testing is the last defense and indicates a failure somewhere earlier in the supply chain. You have to have a good risk management process.

Initial Screening Technique	What it can determine
Paperwork Inspection (if any exists).	If a verifiable paper chain of ownership exists, it can bolster the likelihood parts are genuine.
Gross and Fine Visual Inspection	Can identify bent leads, package cracks, etc. that may indicate that the parts were pulled from recycled systems.
Re-mark/Resurface Solvent Testing.	Can identify a re-marked device, but counterfeiters are becoming increasingly adept at re-marking.
Standard X-Ray	Can determine if a die is present in the package and if it is the correct shape.
X-Ray Fluorescence	Can determine if there are any foreign elements present on the package or leads.
Device Decapsulation	Can verify die manufacturer and die part number marking, but is a destructive test and can only be performed on a sample basis.

9.0 Are there any compensating controls or mitigation

Aircraft example

"For about half the summer, 18 newly completed F-35 fighter jets sat outside Air Force Plant, a Lockheed Martin-operated facility in Fort Worth, Texas.

Instead of flying to military bases around the world, the F-35s were parked while U.S. Defense Department officials tried to untangle the supply chain mess that had stuck them there.

In August, the Pentagon had halted delivery of the aircraft after Honeywell, the maker of a key engine component in the F-35, told Lockheed it had new concerns about the provenance of one part. Specifically, the subcontractor had learned a magnet in the component had been made for years using raw materials sourced in China — a violation of federal procurement rules.

The Defense Department ultimately decided the Chinese alloy didn't endanger or compromise the F-35, and it granted a waiver in early October for deliveries to resume."

Source https://www.defensenews.com/pentagon/2022/12/06/fake-parts-a-pentagon-supply-chain-problem-hiding-in-plain-sight/

10.0 What should you do when it is discovered

10.1 Government efforts

10.1.1 DoD Microelectronics Guidance

OUSD (R&E) is developing and updating guidance to support program use of evidence-based microelectronics assurance to manage microelectronics risk that is commensurate with their program requirements. OUSD (R&E) engaged with the microelectronics suppliers and DoD users in multiple forums including working groups, conferences, and industry groups. OUSD (R&E) is coordinating with the CHIPS program office and has worked with the American National Standards Institute (ANSI) to host two workshops with USG, standards bodies, and industry to identify appropriate considerations and criteria for assurance of microelectronics. The Trusted and Assured Microelectronics (T&AM) Program is making investments to develop and demonstrate tools, techniques, and technology to equip programs to implement microelectronics assurance.

10.1.2 National Security Agency releases Field Programmable Gate Array Documentation

Field Programmable Gate Array (FPGA) are used in DoD systems and are also commonly used in the commercial sector. The National Security Agency (NSA) has released a total of nine Cybersecurity Technical Reports for FPGAs to help establish assurance for field-programmable gate array (FPGA) devices and to protect them from adversarial influence.

These documents can be found at: https://www.nsa.gov/Press-Room/DoD-Microelectronics-Guidance/.

10.2 Civilian efforts

10.2.1 If you are a producer of Chips

a) Copywrite the Chip.
b) Register the copywrite (If you don't do this second step it will be difficult to enforce)
- Create - (https://iprr.cbp.gov/s/)
- CPBS Search (https://iprs.cbp.gov/s/)

10.2.2 If you manufacture an item that uses microchips.

You have to select what standards and guidelines you will use to source chips, perhaps develop a risk scoring methodology with input from senior management.

Try to buy from only OEM-approved distributors. Know the chain of custody and what their "Due Diligence is". Do they monitor subcontractors or use 3rd parties?

Reference NIST 800 series framework for risk-based modifications Mitigate or accept https://csrc.nist.gov/projects/risk-management/about-rmf

Make sure that any design changes are reviewed and understood in advance.

Perform Random sample testing.

Transfer Risk to the Extent Possible
Require a Certificate of Insurance and writing “hold harmless” or indemnification provisions into contracts. Make sure that any issues are addressed in US courts.

Be sure to check Aftermarket entries – like firmware driver updates

Source https://www.travelers.com/resources/business-industries/technology/defending-your-supply-chain-from-counterfeit-electronic-parts

10.2.3 End Users

The End user had no real chance of catching the counterfeit until it fails.
For simple devices it is just a minor inconvenience but for critical infrastructure it is much more impactful, and there will likely be both financial and reputational loss in addition to possible legal repercussions.

The best an end user can do is to build high availability systems combined with a solid backup and recovery plan. But all of that inflates the total cost of the system that is passed along to the consumer.

For example, instead of just 1 server you would have 2 or more servers that are load balanced so that in the event of the failure of one server the application would seamlessly continue on the other with no loss of data.

Event will usually be a P1/S1 (Priority 1/Severity 1) And follow the usually response (Remediation followed by Root Cause analysis) until that point they won’t really know what happened. Then will have to check the rest of the environment for similar components and replace them.

Impact/Urgency	1 – Critical	2 – High	3 – Medium	4 – Low
1 – Extensive	Priority 1	Priority 2	Priority 2	Priority 3
2 – Significant	Priority 2	Priority 2	Priority 3	Priority 4
3 – Moderate	Priority 2	Priority 3	Priority 4	Priority 4
4 – Minor	Priority 3	Priority 4	Priority 4	Priority 4

Source https://ut.service-now.com/sp?id=kb_article&number=KB0011708

When an event is declared the incident response team will take over and drive to the restoration of services.

Figure 2-1. Communications with Outside Parties

Source: https://csrc.nist.gov/files/pubs/sp/800/61/r2/final/docs/draft-sp800-61rev2.pdf

Finally, a Root Cause Analysis will be performed.

NIST SP 800-30 Rev. 1 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-39 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

https://blog.rsisecurity.com/what-is-a-root-cause-analysis-report/

11.0 Key Findings

What are best practices?

Unfortunately, it falls to vendors to secure shipments of goods and components. There's no centralized entity or system capable of dealing with counterfeit products, and government agencies and law enforcement aren't up to the task.

For example, China is one of the world's largest manufacturers and is also the world's largest source of counterfeit goods, despite new crackdowns by government authorities. Since there's no central policing authority to monitor the shipment of goods, it's up to each country to do the best it can to eliminate phony products from imports and exports. Another challenge is the quality of exported goods. Factory seconds are often passed off as quality goods. In the Chinese wholesale market, for example, Grade-A goods may be manufactured by factories licensed to make authentic branded products, while lesser-grade goods may be diverted as factory seconds or manufactured in the same factories using lower-grade materials. When low-grade units are passed off as quality products, even those managing the supply chain are unaware of when goods are phony.

Brokers: Brokers are affordable acquisition and quality control entity that can reduce the risk of counterfeit microelectronics for any sized company. Brokers can scale their pricing for any business, making them a fiscally responsible solution. Brokers are responsible for vetting the vendors, stress/failure testing the microelectronics, and distributing them to the customer. If issues arise with the microelectronic after acquisition, Brokers are usually willing to help the customer rectify the issue, reducing the risk and financial impact of counterfeits that make it into the production cycle. While not infallible, Brokers are a risk mitigation measure that provides a level of confidence and insurance to the customer that typically lacks the requisite expertise and financial resources to independently acquire and test microelectronics.

Proper Disposal of E-Waste: Approximately 70% of worldwide E-waste collates in China. Proper disposal of E-Waste for any sized company helps mitigate the threat of counterfeit microelectronics returning to the US supply chain. Proper disposal of E-waste comes in many form that can be relatively inexpensive. Certified electronic recyclers can properly dispose of E-waste, including removal and destruction of microelectronics. When deciding which recycler to use, ask how they dispose of microelectronics to ensure that process is included in the service. Physical destruction is the best method of combating counterfeit microelectronics as it prevents refurbishment. This can typically be conducted by the onsite IT or a contractor.

Distributed Ledger is great control for known suppliers only but usefulness depends on how it is constructed and the particular product it is going into.

What makes distributed ledger technology ideal for authenticating goods shipments is that it is unhackable. The data is encrypted, and to access it authenticated users must be verified by each node to create a consensus of veracity. For goods in the supply chain, the

advantage of using a distributed ledger system is that it enables end-to-end validation so goods can be authenticated at any point

Once trusted suppliers have been verified a distributed ledger is a best practice for authenticating shipments and secure communication. Distributed ledger is a traceability and coordination control between the supplier and company that allows a limited number of known parties to protect their physical and financial transactions. A company can verify the parties involved, quantity, and unique identifier of goods when using distributed ledger. This can further be improved with the use of an RFID card that can be inserted into a shipment for traceability. The distributed ledger is a premium quality control measure and largely prevents tampering throughout the acquisition process.

Sources:

[1] Supplychainbrain.com; 24 August 2021; Counterfeit Goods Are Everywhere. This Technology Sweeps Them from Supply Chains; https://www.supplychainbrain.com/blogs/1-think-tank/post/33575-combatting-supply-chain-counterfeiting-with-technology

[1] Harvard Business Review; 1 June 2020; Building a Transparent Supply Chain; https://hbr.org/2020/05/building-a-transparent-supply-chain

[1] Harvard Business Review; 1 June 2020; Building a Transparent Supply Chain; https://hbr.org/2020/05/building-a-transparent-supply-chain

12.0 Forecast

Things get transshipped, China will do it through other countries.

Deny China the equipment to manufacture chips

We need to handle e-waste disposal better

US needs to start its own manufacturing (The CHIPS and Science Act)
CHIPS Act, P.L. 117-167. Texas, Arizona, Ohio and Oregon are likely candidates.

Source:
govinfo.gov/content/pkg/PLAW-117publ167/html/PLAW-117publ167.htm

Source:
https://www.cnbc.com/2022/03/23/inside-asml-the-company-advanced-chipmakers-use-for-euv-lithography.html

13. ANALYTIC DELIVERABLE DISSEMINATION PLAN

Office of the Director of National Intelligence

FBI, including the Domestic Security Alliance Council

Intelligence Community Analytic Outreach Coordinators

Department of Homeland Security Headquarters and Components, including Component Intelligence Offices

DHS Association Partners, including but not limited to BENS, ASIS, ISMA, etc.

Previous participants in the AEP and IC Analyst-Private Sector Program

US Council of competitiveness. Deborah wince smith

House and Senate appropriation committee

house select committee on intelligence Senate

FBI InfraGard

National Counterintelligence and Security Center

National Intellectual Property Rights Coordination Center

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.

14. List of References

When Your Smart ID Card Reader Comes with Malware
https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/

Cyberattack can steal data via cooling fan vibrations
https://techxplore.com/news/2020-04-cyberattack-cooling-fan-vibrations.html

A Hauppauge computer equipment distributor pleaded guilty in federal court
https://libn.com/2023/05/03/li-business-owner-pleads-guilty-in-scheme-to-obtain-1m-in-federal-contracts/

DAU - Counterfeit Parts
https://www.dau.edu/acquipedia/pages/ArticleContent.aspx?itemid=451

DARPA Joins Public-Private Partnership to Address Challenges Facing Microelectronics Advancement
https://www.darpa.mil/news-events/2021-12-22

REIMAGINING THE GLOBAL SUPPLY CHAIN POST COVID-19
https://www.siemensgovt.com/assets/documents/gated-content/P2P-Supply-Chain-Report.pdf

A chlorate candle, or an oxygen candle
https://en.wikipedia.org/wiki/Chemical_oxygen_generator

Semiconductor industry association
https://www.semiconductors.org/

Detecting Counterfeit ICs
https://www.electronicdesign.com/technologies/test-measurement/article/21185936/saelig-detecting-counterfeit-ics

Texas Man Who Lied About Origin of Chinese-Made Products
https://www.justice.gov/usao-ndtx/pr/texas-man-who-lied-about-origin-chinese-made-products-sentenced-4-years-prison-ordered
USTR Releases 2022 Review of Notorious Markets for Counterfeiting and Piracy
https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/ustr-releases-2022-review-notorious-markets-counterfeiting-and-piracy

15. List of Resources

Computer Security Incident Handling Guide
https://media.licdn.com/dms/document/D4E1FAQFqHtS4Awm7QQ/feedshare-document-pdf-analyzed/0/1683416169704?e=1684368000&v=beta&t=EL8CMeXDiZGpO32TP-y_SoghRiWP1L-cbW7Q3cqgox0

Supply chain risk management
https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

Security and Privacy Controls for Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Securing the Microelectronics Supply Chain
https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1300/PEA1394-1/RAND_PEA1394-1.pdf

How to Trademark your product
https://www.uspto.gov/trademarks

How to apply, update, or record trademark with CBP
https://help.cbp.gov/s/article/Article-270?language=en_US

How to check, change or update your recording with CPB
https://iprs.cbp.gov/s/

Trusted Foundry Program Accredited Suppliers
https://www.dmea.osd.mil/otherdocs/accreditedsuppliers.pdf

Counterfeit Integrated Circuits: Threats, Detection, and Avoidance
https://ches.iacr.org/2018/slides/ches2018-tutorial1-slides.pdf

National Intellectual Property Rights Coordination Center
https://www.iprcenter.gov/

16. Glossary

Term	Description
BIS	Bureau of Industry and Security.
Capacitor	A Device that stores electrical energy.
Clones	Making a duplicate copy that appears identical.
Copyright	Copyright is a type of intellectual property that protects original works.
Copywrite Registration	It puts others on notice that your work is protected by a copyright and that you are the owner.
Counterfeit	Something being passed off as something it is not.
Cyber Backdoor	An unpublished way to get around normal security measures and gain high level access.
Electronic Waste	Also known as e-waste, it consists of discarded electrical components or devices.
ERAI	The Counterfeit Electronics Risk Organization.
Functional Substandard Part	A Part that works but may not be up to spec and fail sooner than a genuine one.
Integrated Circuit (IC)	An integrated circuit also referred to as a chip is a set of electronic circuits set on one small flat piece of semiconductor material.
Microelectronics	The design and manufacture of very small electronic components.
Misrepresented	False or misleading representation of an item.
Mitigation	The reduction of impact in the event of a failure.
Mom-And-Pop Shops	Small, family-owned or independent business, lacking the rigor of larger companies.
Nonconforming Parts,	Counterfeit products tend to have cheap and unoriginal substitutes in place of authentic ones.
Non-Functional Parts	A component that simply does not work. For example, a chip may have 4 CPU's but only 3 actually work.
OEM	Original Equipment Manufacturers - Companies that design and make parts.
Remarking	Also known as relabeling, it is basically marking the chip to appear as something else.
Resistor	A component that implements electrical resistance as a circuit element.
Risk Acknowledgement	Understanding and accepting a Risk as nonmaterial.
Transistor	Used to amplify or switch electrical signals and power.
Trojan	Malware that misleads users by disguising itself as a standard program.

For additional terms please reference:
https://csrc.nist.gov/glossary