CRITICAL MANUFACTURING SECTOR: Introduction to the Gray Market

This fact sheet informs readers of the continued rise of the gray market and how gray market components can affect national critical infrastructure. This document will also introduce what a gray market is, common types of gray market components, and why they are problematic from a national security standpoint.

WHAT IS THE GRAY MARKET?

There are three forms of markets – white market, gray market, and black market – all of which pose significant risks since they could compromise the information of the buyer, purchaser, and those who will be affected using these materials. The gray market, or middle market, is an unofficial market providing access to sellers and buyers through unauthorized channels, those not affiliated with the brand or original component manufacturers (OCM). The gray market process is also known as "parallel imports."

WHAT ARE GRAY MARKET MATERIALS? WHAT CAUSES THE GRAY MARKET?

Gray market materials are products or components that are sold legally but outside the brand's permission and authorized distribution channels. **Authorized channels and manufacturers are those associated with the brand or OCM. Any channels with no connection to the brand or OCM are considered unauthorized distribution channels.** Gray market stock may include obsolete or allocated parts and branded products diverted into this market and cannot be supported through its original sanctioned brand, which may cause issues with warranties and technical support. Additionally, gray market materials can be advertised as new and authentic but instead, they are used, refurbished, or even counterfeit.

Common gray market materials include:

- Electronic components (USB memory drives, smart home/alarm systems, microchips [e.g., integrated circuits])
- IT, security, and networking hardware
- Construction materials and other raw metals (e.g., aluminum and particularly steel, manufactured to make nuts, bolts, screws, beams, and other materials)

Gray market materials can be put into circulation by:

- Brands themselves when they are selling old stock.
- Third parties down the line of distribution (e.g., retailers or distributors selling off old stock).
- Outside companies selling lower-priced, but still operational, knockoffs of common products.

WHY ARE GRAY MARKET MATERIALS PROBLEMATIC?

Gray market materials can enter the supply chain at numerous points, which makes tracing their origin and original supplier difficult. Components and materials purchased and sold within this secondhand market can create unacceptable and dangerous risks for everyone involved.

Risks of gray market components include:

- **Liability and safety concerns:** Considering the greater chance of sourcing refurbished, defective, or even obsolete or counterfeit components, gray market materials raise the risk of an accident or failure due to the quality or reliability of the component.
- **Mislabeled components:** Some products listed on the gray market may be mislabeled accidentally or intentionally. Without the ability to trace or test for its originality, it becomes impossible to know if the component is genuine or not.
- **Invalid warranties:** Often, gray market products have no valid warranty or service agreements. Many manufacturers invalidate warranties on parts that don't go through the properly authorized channels.

HOW DOES THE GRAY MARKET AFFECT THE CRITICAL MANUFACTURING SECTOR?

Supply chain security is vital in providing traceable, genuine, and warranted products and services. It is imperative to ensure that vendors and suppliers meet regulatory requirements.[1] When a supply chain incident occurs, everyone suffers—buyers, suppliers, and consumers. Gray market materials in critical manufacturing endanger the continued operation and functionality of critical infrastructure. Critical manufacturing owners and operators should know gray market material and component risks, as they pose a much higher threat. Various concerns present themselves when dealing with gray market materials and components in a critical manufacturing setting.

- **Cybersecurity Concerns:** Plugging in components into a facility network can introduce malware, spyware, or other harmful programs.
- **Production Concerns:** The use of gray market parts can introduce flaws or imperfections in end products (e.g., a gray market bolt can fail causing an airplane engine to malfunction).
- **Reputation Concerns:** Failure due to the use of gray market materials can irreparably damage a company or brand, especially if that failure results in injury or loss of life.
- **National Security Concerns:** A component or final product made with gray market materials can be passed between critical infrastructure sectors, leading to increased national risk.

HOW TO AVOID GRAY MARKET MATERIALS

The most trusted way to avoid gray market materials and obtain genuine products is to **purchase directly from authorized manufacturers or authorized distributors, those connected to the brand or OCM.** Avoiding gray market materials altogether is the safest and best option. Staying up to date on authorized product information specs (e.g., serial numbers, specific stock-keeping unit [SKU] numbers, and authorized construction materials) is one way that critical manufacturing owners and operators can reduce the risk of using suspected gray market materials.

To avoid the dangers of gray market materials, it is fundamental to:

- Purchase directly from authorized manufacturers or authorized distributors.
- Research and create relationships with trustworthy suppliers.
- Acquire serial numbers of components.
- Report questionable suppliers or distributors to the organization's procurement office and official manufacturers and distributors.

RELEVANT CASE STUDY EXAMPLE

The Senate Armed Services Committee (SASC) launched an investigation into counterfeit electronic parts in the Department of Defense's supply chain from 2009–2011. Many of these parts came from various resale points in the U.S., U.K., and Canada. Investigators pointed to China as a source for the counterfeit electronics. The investigation uncovered suspected counterfeit parts on mission computers for Missile Defense Agency (MDA) missiles and thermal weapons sights delivered to the Army and on military planes. There were 1,800 identified cases of counterfeiting and less than 1 million total suspected parts. Subsequently, SASC staff were barred from China. All materials, components, and electronic parts must be vetted to ensure they are products of authorized/franchised distributors and suppliers within the supply chain. This vetting and authentication process provides the highest confidence in authenticity and the lowest risk in procuring wayward gray market materials and counterfeits.[2]

FOR MORE INFORMATION ON THE CRITICAL MANUFACTURING SECTOR

Contact the Critical Manufacturing Sector Management Team at CriticalManufacturingSector@cisa.dhs.gov or learn more at cisa.gov/critical-manufacturing-sector.

[1] Supply chain regulatory requirements include, but are not limited to, international trade regulations; environmental, social, and governance (ESG) standards; product safety and quality regulations; data privacy and security regulations; and anti-corruption and bribery regulations.
[2] Abesamis, C. and Leblanc, M. (2015) NASA Counterfeit Parts Awareness and Inspection [PowerPoint slides 23 and 24]. Retrieved from PDF version copy of the NASA Counterfeits Parts Awareness and Inspection.