Executive Summary

When purchasing information and communication technology (ICT) products, including print devices and cartridges, companies and organizations can take various steps to ensure that these technologies are as protected as possible from threats like malicious tainting leading to cybersecurity breaches and corruption through methods like counterfeiting of components and completed goods. One important step is seeking out products that have received ISO 20243 certification. This certification is based on The Open Group’s Open Trusted Technology Provider™ Standard OTTP-S (also known as the ISO 20243 standard), a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software commercial-off-the-shelf (COTS) ICT products across the supply chain and product lifecycle.

Procuring ISO 20243-certified technology has only grown in importance in recent years, given the increased sophistication of cyberattacks, the global nature of printer and cartridge manufacturing and supply chains, and the expansion of work to less-secure home environments. Fortunately, the ISO standard can give organizations greater peace of mind that their products are genuine and high-quality with minimized risk from infiltration and data breaches. Keypoint Intelligence’s review of the print landscape determined that HP is currently the only manufacturer offering

*The Open Group is a global consortium that leads the development of open, vendor-neutral technology standards and certifications. The Open Group has a diverse membership of more than 800 organizations including customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries.
both ISO-certified enterprise/managed print devices and associated cartridges—translating into a comprehensive print system with this designation. The HP print systems with ISO 20243 certification include:

- **HP managed-enterprise printer line** and its **Original HP toner and ink cartridges** (as part of HP Wolf enterprise endpoint security for print)
- **HP DesignJet and PageWide XL large format printer product lines and their Original HP cartridges**

In addition, all of HP’s Original HP toner and ink cartridges for SMB, mid-market, micro-business, and consumer environments have ISO 20243 certification—making all HP Original Cartridges for small format printers ISO certified. HP has also earned ISO 20243 certification for scan technology products, including HP network scanners for document workflows, ScanJet Enterprise, and Digital Sender Flow.

**Key Findings**

- The international ISO 20243 standard was created to help assure product integrity and supply chain security throughout the product lifecycle.
- Application of ISO 20243 to print systems (i.e., printers plus associated ink or toner cartridges) helps guarantee components like micro-controller chips on print cartridges remain untainted and sensitive data in and around these components stays protected.
- HP is unique in that it **has obtained ISO 20243 certification** for the supply chain of its enterprise/managed small format print devices, large format print devices, and all Original HP print cartridges.
  - **HP’s ISO 20243-certified printers** include its LaserJet, Laser, and PageWide small format devices as well as its DesignJet and PageWide XL enterprise large format print devices.
  - **HP’s ISO 20243-certified cartridges** include Original HP print cartridges associated with the ISO 20243-certified printers as well as Original HP print cartridges for small-business small format printers (OfficeJet Pro and LaserJet Pro models) and micro-business printers (DeskJet, OfficeJet, LaserJet, and Laser models).
Recommendations for IT Decision Makers Purchasing Print

- Understand product security and integrity issues can arise at any point during the product lifecycle, including the design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases.

- When looking for print technology, assess the various security features and certifications of products under consideration, including ISO 20243 certification.

- Stay up to date on the evolution of security and supply chain trends and standards at the national and international level to make the best product procurement choices possible from a security and product-integrity perspective.

Introduction

Security, no doubt, is a top priority of many companies and organizations—federal, state, and local government entities included. One aspect of this overarching priority is ensuring that the products and technologies being used are secured from malicious tampering and alteration throughout their entire development and existence. Indeed, lifecycle security is a set of protections to help guarantee that products are safe from tampering or counterfeit through their lifecycle, from conception through disposal.

While product lifecycle security, including supply chain security, is often discussed in the context of products like computing devices and software, it has immense relevance to many different kinds of technology, including those that move across multiple countries in their fabrication and supply chain. In this white paper, we will discuss the mounting importance of ensuring print devices and cartridges are safeguarded from illicit access and misrepresentation throughout their full lifecycles.

What Is ISO 20243 Certification?

Companies and organizations can obtain ISO 20243 certification to recognize and promote the product lifecycle security of information and communication technology (ICT) products. This certification is based on The Open Group's Open Trusted Technology Provider™ Standard (also known as the ISO 20243 standard)—a set of guidelines, requirements, and recommendations (for example, guidance around security labeling techniques) that address specific threats to the integrity of hardware and software commercial-off-the-shelf (COTS) ICT products. ISO 20243 is
designed to address threats related to maliciously tainted and counterfeit goods, and it covers the full breadth of the product lifecycle, from technology development to supply chain. Within these categories, it addresses every phase and activity of the product's lifecycle, including design, sourcing, build, fulfillment, distribution, sustainment, and disposal. The idea is all these stages must adhere to security best practices, as it only takes one weak link in the product lifecycle chain for security to be compromised.

**Product Lifecycle Categories and Activities**

![Diagram of product lifecycle categories and activities](image)

- **Information technology** – Open Trusted Technology Provider Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations (2018)
The following graphic gives an example of how different constituents in COTS ICT product supply chains would ideally interact. In some cases, one or more constituent types may not have a role to play.

**Ideal Interactions Between Different Constituents in COTS ICT Product Supply Chains**


Obtaining the ISO 20243 standard is quite an involved process, with documentation requirements in areas like risk management, physical security, access controls, employee and supplier security and integrity, and business partner security. For a full list of security attributes covered and associated documentation required, see the “ISO 20243 OTTP-S Assessment Documentation Scope” table in the Appendix.

The ISO 20243 standard is relatively new, with the first version having been published in 2013 (though it was based on years of development with stakeholders like the US Department of
Defense and the National Aeronautics and Space Administration). This was followed by the 2014 publication of the second version, which was approved by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in 2015. The standard is clearly well regarded by governmental bodies and authorities. In fact, the US National Institute of Standards and Technology (NIST) cybersecurity framework is aligned to related organizational practices in the standard. The ISO 20243 OTTP-S standard has also been:


- Mentioned in testimony and a hearing delivered to the US Congress regarding supply chain risk and cybersecurity issues.

- Part of the National Defense Authorization Act for Fiscal Year 2016 (Section 888), requiring the US Secretary of Defense to conduct an assessment of the application of the standard (or a similar standard) when procuring secure information technology and cybersecurity systems as well as to provide a related briefing to the Committee on Armed Services of the Senate and the House of Representatives.

A related affirmation of product lifecycle security’s importance was US President Joe Biden’s May 2021 executive order to improve the nation’s cybersecurity and protect federal government networks, including a call to improve software supply chain security. Shortly after the signing of this executive order, the Information Technology Industry Council (ITI), a global advocate for technology public policies and industry standards, published a position paper on Standards and Guidelines to Enhance Software Supply Chain Security. This document encourages NIST to leverage and align with existing international standards for software integrity chains and provenance, including ISO-IEC 20243:2018. More specifically, the US government intends to:

- **Establish baseline security standards** for developing software sold to the government, including requiring developers to make greater visibility into their software and making security data publicly available.

- **Stand up a public-private process** to develop new and innovative approaches to secure software development and use the power of federal procurement to incentivize the market.

- **Create a pilot program** for an ENERGY STAR-type of label so the government and public at large can quickly determine whether software was developed securely.
Why Is ISO 20243 Certification Important for Enterprise/Managed Print Systems?

Print systems are the technology needed to print documents, including the print device itself and marking supplies like ink and toner cartridges. Increasingly, these technologies are targets for criminals to gain access to sensitive data, use as a basis for counterfeit versions, and (implicitly or explicitly) do harm to the manufacturers, sellers, and acquirers of these products. This is being driven by the growing sophistication of cybersecurity attacks, the shifting nature of print device and cartridge development and manufacturing, and the expansion of work environments to more and oftentimes less-secure locations.

As for cybersecurity attacks, many examples of advanced malicious tampering and information extraction have been documented in the media in recent years. A cybersecurity breach involved hackers breaking into US-based SolarWinds’ IT_resource_management_software, adding malicious code, and then gaining access to confidential company information after SolarWinds unknowingly sent out the bad code to customers (as part of software updates). With many of today’s print devices and cartridges containing micro-controller chips (to enhance performance and functionality), there’s also the risk that these components can be improperly manipulated or counterfeited.

Print devices and marking supplies are also frequently manufactured and distributed across multiple countries and sites, increasing the possibility of an infiltration opportunity in the supply chain. Indeed, while globalization has made these products more affordable to produce as well as acquire, the potential associated risks (from both an upstream and downstream perspective) cannot be ignored.

And with more people now working from home, fueled by the COVID-19 pandemic and subsequent office closures (which to a large extent has persisted, despite many office re-openings), the number of environments in which print technology can be threatened has only increased. Now, it is essential that not only in-office printers and cartridges are protected from breaches but also the kinds of products that are being used for home-based working. It appears that many IT decision makers within companies and organizations are aware of this reality, according to primary research from Keypoint Intelligence, an independent market research and product testing firm focused on the print and document technology industries.
What are the biggest security risks for your company with an increase in remote workforce? (Select up to 2.)

- Less secure home-based devices accessing company data: 48%
- Company data leaving the corporate firewall: 48%
- Vulnerable Virtual Private Network (VPN) technology: 33%
- Lack of security training/education amongst staff: 32%
- Outdated policies for company resources and/or tools: 23%
- Not applicable: 4%
- Not sure: 3%
- Other: 1%

N = 234 respondents who believe the pandemic will increase the number of home workers at their company

IT Decision Maker Office Survey – US (Keypoint Intelligence, November 2020)

What Are Benefits of Using ISO 20243-Certified Enterprise/Managed Print Systems?

There are several benefits of using print devices and cartridges that are ISO 20243 certified, including:

- Reducing the risk of technology quality issues
- Minimizing the chance of information security and data privacy breaches
- Having peace of mind that print security issues have been minimized
Reducing the Risk of Technology Quality Issues

As mentioned above, the ISO 20243 certification is based on guidelines and requirements designed to limit the risk of product tampering and counterfeit*. This is clearly a big problem, as evidenced by the approximately 6.6 million illegal counterfeit printer cartridges that have been removed from market through the HP Anti-Counterfeit and Fraud (ACF) Program (in partnership with local law enforcement) in the last eight years. This is equivalent to about 800,000 cartridges a year; if components of counterfeit HP print cartridges are included in the tally, the HP ACF Program assisted local law enforcement in seizing 5.6 billion counterfeit items between 2013 and 2021.

Efforts to lessen these risks are synonymous with protecting the quality of products, including print devices and cartridges. Indeed, using original equipment manufacturer (OEM) products that adhere to the ISO 20243 requirements and recommendations is a significant step in ensuring product quality is premium as well as protected throughout the supply chain.

OEM printers and cartridges are built for optimum print quality and reliability, with components like HP cartridge chips that make various adjustments (across different jobs, media, and cartridge life periods) to guarantee excellent output quality, consistency, and accuracy. As another example, each HP cartridge is designed to work with specific HP printers, limiting the chance the cartridge will cause damage to the printer or reduce its longevity. Minimizing issues around print quality and device longevity are key in maintaining productivity within one's organization, satisfying customers, and saving money.

*This includes (as just one of many examples) requirements for the secure transmission and handling of products and components during delivery.

Minimizing Chance of Information Security and Data Privacy Breaches

Acquiring technology conforming to best practices for product lifecycle security also helps limit the chance that a malicious party can gain access to the data within that product. For example, one of the ISO 20243 requirements is for manufacturers to use one or more up-to-date malware detection tools to ensure components from suppliers as well as components or products delivered to customers or integrators do not contain malware.

Indeed, the inclusion of malware in a product's software code can result in sensitive data within that product or connected to that product (e.g., through a network, the Internet) to be obtained...
and misused by a third party—potentially resulting in a loss of compliance, a loss of customer trust, and/or financial penalties for companies or organizations using these technologies. By working with manufacturers that adhere to the ISO 20234 guidelines around malware avoidance as well as other protections to maintain information security and data privacy, organizations can reduce the threat of a potential data breach.

**Peace of Mind**

By using ISO 20243-certified enterprise/managed print systems, companies and organizations can have peace of mind that their print equipment is reasonably protected against tampering, misrepresentation (e.g., in terms of brand, OEM status), and cyberattacks. They can know that the product conforms to a large number of guidelines and requirements within three key areas:

- **Product development/engineering**: These requirements address the software/firmware/hardware design process, configuration management, a well-defined development/engineering method process and practices, quality and test management, and product sustainment management.

- **Secure development/engineering**: These requirements cover threat analysis and mitigation, run-time protection techniques, vulnerability analysis and response, product patching and remediation, secure engineering practices, and monitoring and assessing the impact of changes in the threat landscape.

- **Supply chain security**: These requirements deal with risk management, physical security, access controls, employee and supplier security and integrity, business partner security, supply chain security training, information systems security, trusted technology components, secure transmission and handling, open source handling, counterfeit mitigation, and malware detection.

While one can never be 100% sure their organization and products won’t experience a security breach, making smart procurement decisions based on standards like ISO 20243 is a great way to increase one’s level of confidence and protection.
Which Enterprise/Managed Print Systems Have ISO 20243 Certification?

Keypoint Intelligence, the independent market research and product testing firm mentioned above, conducted a review of the leading printer manufacturers in the market to see which have ISO 20243-certified print devices, OEM print cartridges, and print systems (printers plus same-OEM ink or toner cartridges). This research revealed that HP is the only OEM offering ISO 20243-certified print systems (for its enterprise/managed printers and associated cartridges), though Lexmark has obtained ISO 20243 certification for its laser print devices only (the associated Lexmark toner cartridges do not have this certification).

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>ISO 20243-Certified Print Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canon Group</td>
<td>None</td>
</tr>
<tr>
<td>Fujifilm</td>
<td>None</td>
</tr>
<tr>
<td>HP Inc.</td>
<td>HP managed-enterprise printers such as HP Color Laser M555dn, HP Color LaserJet Managed Flow MFP E876660z, PageWide Enterprise Color 586Z, the DesignJet T1700, ScanJet Enterprise 8500 FN2, and the associated HP cartridges</td>
</tr>
<tr>
<td>Konica Minolta Group</td>
<td>None</td>
</tr>
<tr>
<td>Kyocera Group</td>
<td>None</td>
</tr>
<tr>
<td>Lexmark</td>
<td>Laser print devices only (no cartridges are ISO 20243-certified)</td>
</tr>
<tr>
<td>Ricoh Group</td>
<td>None</td>
</tr>
<tr>
<td>Sharp</td>
<td>None</td>
</tr>
<tr>
<td>Toshiba</td>
<td>None</td>
</tr>
<tr>
<td>Xerox</td>
<td>None</td>
</tr>
</tbody>
</table>

Keypoint Intelligence research and IDC market share data from Q2 2021

HP also obtained ISO 20243 certification for enterprise-class large format HP DesignJet and HP PageWide XL printing devices and their Original HP print cartridges as well as for HP ScanJet Enterprise and Digital Sender Flow network scanners. HP printers outside the enterprise class are produced with a mindful approach to supply chain, following the [HP Standard 10-04 for Information Protection and Security for Suppliers/Partners](https://www.hp.com/en-us/support/article/c04638552). This comprehensive approach
to supply chain security practices across these diverse HP print devices, cartridges, and print systems shows HP's commitment to mitigating threats of malicious tampering and counterfeits.

The fact that HP has obtained ISO 20243 certification for its HP managed-enterprise printers and all cartridges aligns with its overall emphasis on and commitment to printer security. In fact, the company boasts a variety of other security certifications, recognitions, and product features—including:

- **Buyers Lab (BLI) Security Validation from Keypoint Intelligence** for Device Penetration and Firmware Resilience for HP FutureSmart Enterprise Firmware v4, which is used on all HP managed-enterprise devices.

- **BLI 2021-2022 PaceSetter Award in Document Imaging Security for the Office** from Keypoint Intelligence for its strong ecosystem of security products and services for business purchasers, including its self-healing firmware and in-memory breach detection for HP business-class MFPs and printers, endpoint security services, and dealer and customer security awareness campaigns.

- HP Wolf enterprise endpoint security for print encompassing hardware security, endpoint security software, and security services across company sizes, work environments (e.g., home and office), and devices (e.g., printers and PCs). See [hp.com/go/printersthatprotect](http://hp.com/go/printersthatprotect) and [hp.com/wolf](http://hp.com/wolf).

- **Original HP Office Class cartridge security** with only original HP components; a secure, unalterable chip; tamper-resistant packaging; holographic security labels (that include an identifier tracked through the HP supply chain); and communication and authentication between the printer that is designed and manufactured to be secure. See [hp.com/go/suppliesthatprotect](http://hp.com/go/suppliesthatprotect).

- **Certificate for HP chips** in Original HP managed-enterprise printer cartridges meeting requirements for EAL 5+ international standard common criteria for computer security certification.

- **Bug Bounty program** to identify and remediate potential risks in office-class print cartridges.

- **Dynamic Security** allowing customers to authenticate Original HP Cartridges. See [hp.com/learn/DS](http://hp.com/learn/DS).

- **Breadth of managed-enterprise devices** with fleet security management, whitelisting, run-time intrusion detection; HP Connection Inspector; and HP Sure Start BIOS protection.
Our Take

Product and data security are especially crucial in today’s world of connected and networked devices and technology. When it comes to print devices and associated cartridges, these products are not immune to security breaches, data leaks, and corruption through counterfeit and tampering. In theory, these actions can occur at any point along the product lifecycle when appropriate measures aren’t in place to protect the technology from malicious third parties. The good news is that a set of guidelines is in place, in the form of the ISO 20243 standard and certification program, to help manufacturers minimize the risk of product security breaches and tampering. Companies and organizations in the market for print devices and cartridges are advised to strongly consider products that have obtained this certification.

Appendix

<table>
<thead>
<tr>
<th>Device and Cartridge Scope of ISO 20243 Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Printer Hardware</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>HP managed-enterprise printers and MFPs</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HP DesignJet and PageWide XL large format printers and MFPs</td>
</tr>
<tr>
<td>HP ScanJet Enterprise and Digital Sender Flow network scanners</td>
</tr>
</tbody>
</table>
## ISO 20243 OTTP-S Assessment Documentation Scope

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Evidence Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Management</strong></td>
<td>• Supply chain risk/business continuity planning policy documents</td>
</tr>
<tr>
<td></td>
<td>• Training and mitigation plan</td>
</tr>
<tr>
<td></td>
<td>• Evidence of risk management plan being followed (e.g., component qualification report, snapshot of risk management tools)</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>• Physical security management policy</td>
</tr>
<tr>
<td></td>
<td>• Evidence of procedures in above policy (e.g., pictures of cages, locked doors, CCTV video)</td>
</tr>
<tr>
<td><strong>Access Controls</strong></td>
<td>• Security controls: access control policies and procedures documents</td>
</tr>
<tr>
<td></td>
<td>• Evidence of procedures (e.g., supplier premises logs, access logs, CCTV, video of implementation of personal searches or badging)</td>
</tr>
<tr>
<td><strong>Employee and Supplier Security and Integrity</strong></td>
<td>• HR identity check process</td>
</tr>
<tr>
<td></td>
<td>• Evidence that the identity is verified by the organization</td>
</tr>
<tr>
<td><strong>Business Partner Security</strong></td>
<td>• Supplier and customer communication process</td>
</tr>
<tr>
<td><strong>Supply Chain Security Training</strong></td>
<td>• Training materials, training certificates, computer-based training</td>
</tr>
<tr>
<td><strong>Information Systems Security</strong></td>
<td>• List of the types of supply chain data that are protected and of associated security controls</td>
</tr>
<tr>
<td><strong>Trusted Technology Components</strong></td>
<td>• Quality assurance process with example component quality conformance report</td>
</tr>
<tr>
<td></td>
<td>• Policy on use of authentic components or policy to prevent the use of counterfeit components</td>
</tr>
<tr>
<td><strong>Secure Transmission and Handling</strong></td>
<td>• Security controls and secure transmission and handling procedures</td>
</tr>
<tr>
<td></td>
<td>• Evidence of conformance (photos reflecting CCTV use, secure packaging, security tape, shipping logs, use of encryption)</td>
</tr>
<tr>
<td><strong>Open Source Handling</strong></td>
<td>• Records of component lineage derivation for the open source components (security and integrity checking)</td>
</tr>
<tr>
<td></td>
<td>• Open Source product support policy</td>
</tr>
<tr>
<td><strong>Counterfeit Mitigation</strong></td>
<td>• Counterfeit review and response policy</td>
</tr>
<tr>
<td></td>
<td>• Scrap handling procedures</td>
</tr>
<tr>
<td><strong>Malware Detection</strong></td>
<td>• Acceptance procedures requiring the use of malware detection tools</td>
</tr>
<tr>
<td></td>
<td>• Demonstration of records showing application of malware detection tools before final packaging and delivery</td>
</tr>
</tbody>
</table>
Functions of Original HP Cartridge Chips

Toner and ink cartridges contain micro-chips to communicate with the printer. Cartridges need to be able to communicate with the printers to provide beneficial functions, including:

- **Supplies level management** of ink or toner, which can be viewed like a gas gauge. This provides enough time to reorder supplies or (if an automatic supply fulfillment plan is used) for automatic supplies reordering. With some inkjet printers, if one continues to try to print when the ink is completely out, the printheads may be damaged—requiring replacement. The HP chip on the ink cartridge monitors and helps protect the printhead.

- Notice/Cartridge Compatibility/Electronic Keying (for color cartridges) to check for an inform or proper installation and cartridge compatibility to make sure that the correct cartridge is installed properly.

- **Authentication** informs the user that an Original HP cartridge has been installed as opposed to a third-party cartridge that is potentially masquerading as an Original HP one or was mistakenly ordered.

- **Consistent print quality:**
  - For laser toner printing, other cartridge components wear out over the life of the cartridge. The HP chip is used to make various adjustments to voltages applied to the various components—assuring that the cartridge will provide optimum print quality even as components inside the cartridges start to wear. Without such adjustments, print quality will deteriorate with use.
  - For inkjet printing, the HP chip includes technology packages with resources and recipes that make color maps to transform colors from the source to the different colors in the target image. This allows the cartridge to deliver optimal print quality over its life on different papers.
  - When improved ink formulas become available, these packages on the cartridge chip may be revised to optimize print quality. Original HP chips on HP Integrated Print Head (IPH) cartridges deliver consistent print quality with enhanced detail by communicating the ink drop weight/volume and estimated ink levels.
  - This produces sharp black text and vivid graphics, with reduced image grain and increased color gamut for photos and graphics with smooth gradations and accurate colors.

- **No personally identifiable information** is stored on the HP cartridge chip, so it can be confidently returned for recycling.
About Keypoint Intelligence

For 60 years, clients in the digital imaging industry have relied on Keypoint Intelligence for independent hands-on testing, lab data, and extensive market research to drive their product and sales success. Keypoint Intelligence has been recognized as the industry’s most trusted resource for unbiased information, analysis, and awards due to decades of analyst experience. Customers have harnessed this mission-critical knowledge for strategic decision-making, daily sales enablement, and operational excellence to improve business goals and increase bottom lines. With a central focus on clients, Keypoint Intelligence continues to evolve as the industry changes by expanding offerings and updating methods, while intimately understanding and serving manufacturers’, channels’, and their customers’ transformation in the digital printing and imaging sector.

For more information on Keypoint Intelligence, please call (973) 797-2100, visit www.keypointintelligence.com, or email info@keypointintelligence.com.