Hewlett Packard Enterprise



# HPE Cybersecurity Business Practices

## Supplier Summit August 2016

Hewlett Packard Enterprise (HPE) is actively engaged with all levels of its supply chain, design tools/systems, and manufacturing environment to protect against the introduction of counterfeit electronic parts and/or malicious software/malware. This involves multiple approaches as no single method provides sufficient coverage. HPE requires that all suppliers of products and services to HPE demonstrate the same level of concern as reflected in their business practices. A single vulnerability anywhere in the supply chain could prove disastrous for both HPE and the end-user customer.

### The changing security landscape

No longer is the threat that of a lone hacker working for the thrill of penetrating corporate or government networks. Cybercrime has become big business as criminals, to hacktivists, to nation states work to steal information to either enrich themselves or further their cause.

The security landscape evolves on a daily basis. Customers are requiring that HPE products and services be guaranteed free of counterfeit parts and malicious software/malware. The inability to comply with cybersecurity requirements can be a lockout when bidding on government and commercial contracts.

### Expectations of suppliers to HPE

A cyber risk management plan, which should be part of every supplier's document library, allows the supplier to evaluate the completeness of their cybersecurity defense plan. This plan provides a framework as to how risk is mitigated, transferred, avoided, or accepted. In some cases, this framework will need to be done in consultation with HPE.

HPE supports a sensible, risk-based approach to managing cybersecurity throughout the supply chain and at all tiers (supplier, sub-supplier, etc.). Suppliers should take a comprehensive approach to maintain security including the establishment of a robust cybersecurity framework. The framework should incorporate processes to identify, prevent, detect, respond to, and recover from technology-based attacks.

Suppliers of products and services to HPE (at any tier) are expected to partner with HPE in preventing the proliferation of counterfeit parts and/or malicious software/malware. Based, in part, on ever-evolving government and industry policies, standards, and best practices (DFARS, NIST, ISO, etc.), HPE has crafted a series of standards and self-assessment tools. The standards can be found on the **HPE Supplier Portal**. The self-assessment tools, in a spreadsheet format, allow the supplier to quickly identify areas where their cybersecurity practices need attention. Suppliers will be contacted when it is time to complete their self-assessments. Onsite follow-ups will be scheduled with suppliers as needed.

## HPE Supply Chain Risk Management Practices & Controls

| Design | Sourcing | Build | Fulfillment | Distribution | Sustainment & operations | Disposal |
|---|---|---|---|---|---|---|

**Prevent, monitor, detect, analyze, avoid, and report incidents of suspect and confirmed counterfeit and malicious taint**

| Component suppliers | | | | Factory access controls | | | | Physical security requirements | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Suppliers & subs HPE approved | AVL approved vendor list | HPE SBC & supplier code of conduct | Investigate allegations of breach & counterfeit | Security guards | Employee background checks | Electronic badge access control | CCTV monitoring | Alarms & motion detection systems | Restricted high value parts area | Gated entry points | Segregated secure customer furnished equipment area |
| **HPE Direct Relationship** | | | | **Factory security protocol** | | | | **Secure facilities** | | | |

**Proof points for DFARS compliance**

- Trusted suppliers used for sourcing
- Approved vendor list
- Factory Malware Scanning
- Quality & Procurement Management System with industry standard and best practice implementation
- Advanced detection capabilities in select parts
- Continuous process improvement
- C-TPAT tier III certification
- GIDEP program monitoring and reporting
- Risk-based security audits performed
- Material control processes including quarantine, purge, and end of life
- Training on counterfeit identification, detection and avoidance
- Component traceability for HPE and suppliers
- Change control processes
- Inspection and testing of electronic parts
- Monitor for incidents of suspect counterfeit, counterfeit, and taint

In order to facilitate full compliance with HPE standards, all requirements on suppliers MUST be flowed down to all subsequent tiers. Where it is not contractually possible for a sub-supplier to provide confidential information to the next higher tier, the sub-supplier must provide a signed statement attesting to their compliance with the particular standard. This allows HPE to assure customers of complete traceability of the components and software used in the design process, in the manufacturing shop floor production equipment, and in the product itself.

## More information

The HPE cybersecurity standards can be found on the **HPE Supplier Portal**.

Once logged into the HPE Supplier Portal, click **<Supplier Handbook, Restricted Access>**. Scroll down to find standard HX-00014-03, HPE Standard 14-03 Product Cybersecurity Standard for Suppliers. Other HPE cybersecurity standards can be found below HX-00014-03.

Any questions regarding HPE's cybersecurity position or expectations should be addressed to the HPE procurement team or to Scott A. Stephens, EG Product Cybersecurity Manager, at **scott.a.stephens@hpe.com**.

The self-assessment tools will be sent to the supplier contacts. The message will contain information regarding the requested return date and whom to contact with questions or concerns.

Learn more at
**h20168.www2.hpe.com/supplierextranet/index.do**

**Sign up for updates**

Hewlett Packard Enterprise



4AA6-6553ENN, July 2016