

August 27, 2009

# Bogus Computer Shipments

## Security Intelligence Advisory



### Recommended Actions

1. Integrate supply chain into your security program.
2. Match all received equipment, including serial numbers, against packing slips and purchase orders.
3. Contact your computer equipment supplier and establish controls for ordering and receiving.
4. Help the purchasing department control rogue acquisition of all sensitive equipment.
5. Establish a centralized place for each facility that acts as a control point to receive packages.
6. Establish a reporting process for handling strange activities, packages and shipments.

### Technolytics

4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I [www.technolytics.com](http://www.technolytics.com)

technolytics

The Federal Bureau of Investigations (FBI) is currently investigating the unexpected delivery of laptops to several states, including West Virginia Governor Joe Manchin's office. In early August, Governor Manchin's office received five computers in Hewlett-Packard (HP) packages. An internal investigation concluded that no one from the state had ordered them. Authorities are working with HP trying to obtain tracking documents that clearly define the path from manufacturer, to order, to point of distribution, to point of sale and delivery. The concerns prompted the isolation of the computer equipment. The laptops were not turned on or connected to a network. It is unclear at this point if forensic analysis has been completed on the computer equipment that is in question, or if there were any malicious capabilities accompanying the computer equipment. Introduction of unauthorized or compromised computer or networking equipment could wreak havoc on any network. As you may recall, last year Technolytics issued a Security Intelligence Advisory about counterfeit computer networking equipment and microprocessors which pose a very similar threat. One thing is for sure, if this was an act of cyber espionage, it was creative and well planned and also expensive.



### HP Response

"HP is aware that fraudulent state government orders recently have been placed for small amounts of HP equipment," company officials said in the statement. "HP took prompt corrective action to address the fraudulent orders and is working with law enforcement personnel on a criminal investigation."

### Analysis

It is not clear if this shipment was a deliberate act of cyber espionage or not. It is possible this was simply been an accidental mis-shipment, or a mistake made on another contract. However if it was a form espionage, this type of tactic as an espionage program is expensive and therefore thought to be restricted to high value targets. HP has multiple contracts to supply computers to various state agencies so the arrival of HP computers would not be out of the norm. However receiving a shipment that is not expected is what creates the concern. The discipline around end-to-end supply chain security is currently minimal in many organizations. When you couple this with the fact that rogue acquisition of equipment always has been a problem for organizations of all sizes — using this technique as a vector to target and compromise computer systems is very troubling. The supply chain must be fully integrated into an organization's security program to minimize this and other potential security risks. In addition, end-to-end supply chain processes must be established with security designed into the process, and not added as an after thought.