CNC Federal
More than Business as Usual

xerox

Compliance with common security requirements

Xerox has a dedicated commitment to keeping information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Below is a selection of Xerox TAA Compliant products and a few of the commonly required security features and options available with each.

Xerox TAA Compliant Products

Xerox Product	TAA Configurations	IPv6/IPsec	IP Filtering	SNMP v3 Encryption	Disk Image Overwrite
Color Printers					
Phaser® 6280	YN	IPv6	X	X	X
Phaser 6360	YN / YDN /YDT / YDX	IPv6	X	X	X
Phaser 7400	YN / YDN /YDT / YDX		X	X	X
Phaser 7500	YDN /YDT / YDX	IPv6	X	X	X
Phaser 7760	YN / YDN /YDT / YDX		X	X	X
Phaser 8560	YN / YDN /YDT / YDX	IPv6	X	X	X
Black-and-White Printers					
Phaser 3600	B / DN / N		X	X	
Phaser 4510	YB /YN / YDT /YDX	IPv6	X	X	X
Phaser 5550	YN / YDN / YDT	IPv6	X	X	X
Color Multifunction Printers					
Phaser 8560MFP	YD	IPsec	X	X	X
Black-and-White Multifunction Printers					
WorkCentre® 4118	X				
WorkCentre M20i	All		X		
WorkCentre 4250/4260	S / X / XF / SM / XM / XFM	IPv6	X	X	X
Fax Machines					
FaxCentre® 2218	FC2218				

TAA compliant configurations denote that the country of origin for the specified configuration of that printer, MFP or fax machine complies with the requirements of the US Trade Agreements Act (TAA).

IPv6: Internet Protocol version 6 (IPv6) is the next-generation Internet Layer protocol for internetworks and the Internet. IPv6 has been implemented on all major operating systems in use in commercial, business, and home consumer environments. Network security is integrated into the design of the IPv6 architecture. The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

IPsec: Internet Protocol Security (IPsec) secures Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. IPsec can be used for protecting any application traffic across the internet.

IP Filtering Feature: Internet Protocol (IP) Filtering provides a system administrator with a means of restricting access to the system to a specific set of IP addresses. This provides a first level of defense against unauthorized use of the system. Computers whose IP addresses are outside of the allowed set are not permitted to print.

SNMP v3 Encryption: Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices. SNMPv3 is the current standard version of SNMP as of 2004. SNMPv3 provides important security features:

- Message integrity to ensure that a packet has not been tampered with in transit.
- Authentication to verify that the message is from a valid source.
- Encryption of packets to prevent snooping by an unauthorized source.

Disk Image Overwrite: The Image Overwrite security option electronically shreds information stored on the hard disk of devices as part of routine job processing. Electronic erasure can be performed automatically at job completion or on demand. The Xerox Image Overwrite security process implements a three-pass algorithm originally specified by the U.S. Department of Defense.

For more information, go to www.xerox.com/security.