National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Xerox Corporation

Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems

Report Number: CCEVS-VR-06-0021

Dated: 6 April 2006

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jean Hung

The MITRE Corporation

Jandria Alexander

The Aerospace Corporation

Common Criteria Testing Laboratory

Computer Sciences Corporation

Annapolis Junction, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Xerox Corporation Image Overwrite Security for a line of copiers and multifunction systems. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC), and was completed during March 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by CSC. The evaluation determined the product to be **Part 2 extended and Part 3 augmented,** and to meet the requirements of **EAL2 augmented with ALC_FLR.2**. The product is not conformant with any published Protection Profiles.

The TOE is a multi-function device (hereafter referred to as a MFD) that copies, prints, scans to e-mail, scans to a network repository, and analog faxes from either the platen or the print driver (the latter referred to as LanFax). The MFD contains an internal hard disk drive (referred to as Network Controller HDD). Standard security functions include SSL, IPSec, SNMPv3, a host-based firewall, and an internal audit log. Additionally, the TOE can be configured to filter inbound network traffic based on source IP address and/or destination network protocol/port. Finally, the TOE also maintains an audit log. Users may be authenticated to the network or locally at the device.

The evaluated configuration also includes the Image Overwrite Security accessory, the embedded fax accessory, and in the WorkCentre Pro models, the Network Scanning accessory, all consumer options. The Overwrite Security accessory causes any temporary image files created during a print, network scan, scan-to-email, and LanFax job to be overwritten when those files are no longer needed or "on demand" by the system administrator. Copy and embedded fax jobs do not get written to the HDD. The overwrite algorithm conforms to DoDD 5200.28-M. The Network Scanning option utilizes the inherent TOE SSL support to secure the filing of scanned documents on a remote SSL-enabled server. The Embedded Fax accessory provides local analog fax capability over PSTN connections and also enables LanFax jobs.

The TOE includes security functions implemented at the TOE interfaces, as follows:

- Image Overwrite (TSF_IOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSec)
- Network Management Security (TSF_NET_MGMT)
- FAX Flow Security (TSF_FAX_FLOW)

- Security Management (TSF_FMT)

A Strength of Function claim of SOF-basic is made for all models of WorkCentre®/WorkCentre® Pro.

The Security Target (ST) for WorkCentre®/WorkCentre® Pro models is contained within the document Xerox WorkCentre®/WorkCentre® Pro 232/238/245/255/265/275 Multifunction systems Security Target Version 1.0, Revision 1.12, March 23, 2006.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1~~Table 1~~ provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems
Protection Profile	None
Security Target	*Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction SystemsVersion 1.0, Revision 1.12, March 23, 2006*
Evaluation Technical Report	*Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target Version 1.0, Version 1.0, March 13, 2006*
Conformance Result	Part 2 extended conformant, Part 3 conformant, EAL 2
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	Computer Sciences Corporation
Validators	Jean Hung of The MITRE Corporation and Jandria Alexander of The Aerospace Corporation

3. SECURITY POLICY

The Xerox product line identified enforces the following security policies:

3.1 Image Overwrite Policy

The WorkCentre®/WorkCentre® Pro models implement an image overwrite security function (Immediate Image Overwrite (IIO)) that causes temporary image files created during a print, network scan, scan-to-email, or LanFax job to be overwritten automatically at the completion of the job. The "On-Demand" Image Overwrite (ODIO) function can be manually invoked by the system administrator. Both IIO and ODIO use a three pass overwrite procedure as described in DODD 5800.28-M. [Copy and analog fax jobs initiated from the platen do not create files on the Network Controller HDD so no overwrite is needed for these job types.]

Once invoked, ODIO cancels all copy, print, network scan, scan-to-email, LanFax, or analog fax, jobs, halts the printer interface, and overwrites the contents of the sectors used for temporary image files on the internal hard disk drive. The entire machine then reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

3.2 Identification and Authentication Policy

The WorkCentre®/WorkCentre® Pro models can authenticate users to a remote network authentication server. Supported authentication services include Kerberos (Solaris), Kerberos (Windows 2000), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000). The system prevents unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax) unless the user is properly authenticated. To access a network service, the user is required to provide a user name and password which is then validated by the remote authentication server.

To authenticate the system administrator, the WorkCentre®/WorkCentre® Pro models utilize a simple authentication function accessible through the front panel or web interface. The system administrator must authenticate by entering an 8 to 12 digit PIN prior to being granted access to the tools menu and system administrator functions. The system administrator must change the default PIN after installation is complete. While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered. The authentication mechanism has a PIN space of 12**3 to 12**12.

System administrators may also authenticate through a Web user interface that requires the user to enter a PIN and enter "admin" into the username field. The username prompt provided by the web server is not used, but is provided for historical reasons. The only valid string is "admin", which is hard coded into the web server and cannot be changed. Additional users cannot be added. The TOE does not associate user attribute or privileges based on username.

3.3 Security Management

The WorkCentre®/WorkCentre® Pro models utilize the front panel software module security mechanisms to allow only authenticated system administrators the capability to invoke or abort the ODIO function, enable or disable the IIO function, enable or disable embedded fax, and change the system administrator PIN. Additionally, the TOE utilizes the web server authentication mechanism to allow only authenticated system administrators the capability to configure SSL, IPSec, and/or SNMPv3, to manage IP filtering rules, to download the audit log, to configure network authentication, or to manually invoke "On Demand" Image Overwrite.

The WorkCentre®/WorkCentre® Pro models restrict the ability to manage administrative functions to the system administrator.

3.4 Cryptographic Support

The WorkCentre®/WorkCentre® Pro models utilize data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-186, SSLv3, SNMPv3.

3.5 Auditing Policy

The WorkCentre®/WorkCentre® Pro models generate logs that track events/actions (e.g. print/scan/LanFax job submission) to logged in users, and each log entry contains a timestamp. The audit logs are only available to system administrators and can be securely downloaded via the Web interface for viewing and analysis.

3.6 Information Flow Control Policy

The WorkCentre®/WorkCentre® Pro models implement a static, host-based firewall that limits network access to the device. The system administrator can control access based on source IP address and/or protocol/port. Access rules can be administered via a secure interface provided by the Web UI.

3.7 Fax-Network Separation

The WorkCentre®/WorkCentre® Pro models have an architecture that provides separation between the optional FAX processing board and the network controller. This architecture ensures that a malicious user cannot access network resources from the telephone line via the system's optional FAX modem.

4. ASSUMPTIONS

4.1 Usage Assumptions

The system is expected to be used in what has traditionally been known as "a relatively benign environment." That is, all the information on the system is at the same level of sensitivity, and all users are authorized for that level of information (although they do not necessarily have access to all the data). There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains. The system administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the system administration documentation. Procedures exist for granting system administrator(s) access to the TSF. The administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

4.2 Environmental Assumptions

It is presumed that the TOE has been delivered, installed, and configured in accordance with documented procedures, which includes installation and setup by an authorized Xerox technician.

In addition, it is assumed that the TOE will be located within facilities providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE and the TOE serial port. There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.

5. ARCHITECTURAL INFORMATION

5.1 Description

The TOE is a multi-function device (MFD) that copies and prints, with scan to e-mail, network scan, and FAX options. The TOE includes the Image Overwrite Security accessory. This accessory forces any temporary image files created during a print, network scan, scan to email, or LanFax job to be overwritten when those files are no longer needed. An additional package (optional in the evaluation) is the network scanning package. Table 1 lists the Evaluated Models and Capabilities. (X – included in all con figurations; O – product options ordered separately).

Table 1: Models and capabilities

	Print	Copy[1]	Network Scan	Embedded Fax[1]	Scan 2 email
WorkCentre 232	x	x	n/a	o	x
WorkCentre 238	x	x	n/a	o	x
WorkCentre 245	x	x	n/a	o	x
WorkCentre 255	x	x	n/a	o	x
WorkCentre 265	x	x	n/a	o	x
WorkCentre 275	x	x	n/a	o	x
WorkCentre Pro 232	x	x	o	o	x
WorkCentre Pro 238	x	x	o	o	x
WorkCentre Pro 245	x	x	o	o	x
WorkCentre Pro 255	x	x	o	o	x
WorkCentre Pro 265	x	x	o	o	x
WorkCentre Pro 275	x	x	o	o	x

[1] Copy and embedded FAX jobs are not spooled to the HDD.

The MFD stores temporary image data created during a print, network scan or scan to email, and LanFAX job on an internal hard disk drive (HDD). This temporary image data consists of the

original data submitted and additional files created during a job. Copy and local FAX jobs do not get written to the HDD.

In the base evaluated configuration, the TOE, with the Image Overwrite Security accessory, provides an image overwrite function to enhance the security of the MFD. This function overwrites temporary document image data as described in DoD Standard 5200.28-M either at the completion of each print, network scan, scan to email, or LanFAX job, or *on demand* of the MFD system administrator. A system administrator may use the *on demand* image overwrite security option to clear sensitive information from the HDD when the MFD is, for example, decommissioned.

The TOE configuration, with respect to the WorkCentre Pro models, adds Xerox's Network Scanning Accessory. This accessory allows documents to be scanned at the device with the resulting image being stored on a remote server/repository. The connection between the device and the remote server is secured when the TOE's SSL support is enabled; the transfer of the data is through an HTTPS connection.

All models of the TOE have the optional Embedded FAX accessory added. This accessory permits the TOE to function as a local Fax connected to the PSTN.

All models of the TOE support both auditing and network security. The system administrator can enable and configure the network security support. The network security support is based on SSL. When SSL support is enabled on the device, the following network security features can be enabled/configured: HTTPS support (for both the device's Web UI and secure network scan data transfer); system administrator download of the device's audit log; IPSec support for lpr and port 9100 print jobs; secure network device management through SNMPv3, and specification of IP filtering rules.

5.2 Physical Scope and Boundary

The TOE is a Multi-Function Device, shown in Figure 1, which performs printer, copier, scanner, LanFax, embedded analog FAX (optional), and email functions. The physical scope and boundary of the TOE consists of the Xerox WorkCentre or WorkCentre Pro devices and include installed Xerox accessories. For this evaluation, all models of the TOE will include the Image Overwrite Security accessory and the embedded FAX accessory. In the WorkCentre Pro models the Network Scanning accessory (a software component) is included in the configuration.

Figure 1: Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275

*** Also shown are an optional paper feeder and finisher.**

The TOE physical boundary also consists of the Administrative and User Guidance provided on CDs with the device, as well as, the Secure Operation guidance provided to consumers through the Xerox web site (www.xerox.com/security). Table 2 lists the Evaluated Software/Firmware version.

Table 2 Software Version Numbers

Software/Firmware Item	WorkCentre	WorkCentre + PostScript	WorkCentre Pro
System Software	**12.027.24.015**	**14.027.24.015**	**13.027.24.015**
Network Controller Software	**040.010.01121**	**040.010.11121**	**040.010.51121**
UI Software	**012.27.059**	**012.27.059**	**012.27.059**
IOT Software	**61.30.00**	**61.30.00**	**61.30.00**
SIP Software	**12.27.56**	**12.27.56**	**12.27.56**
DADH Software (Options)			
• Normal Mode	**14.00.00**	**14.00.00**	**14.00.00**
• Quiet Mode	**15.12.00**	**15.12.00**	**15.12.00**
FAX Software	**02.27.011**	**02.27.011**	**02.27.011**
Finisher Software (Options)			
• 1K LCSS	**01.27.00**	**01.27.00**	**01.27.00**
• 2K LCSS	**03.10.00**	**03.10.00**	**03.10.00**
• HCSS	**13.36.00**	**13.36.00**	**13.36.00**
• HCSS with BookletMaker	**23.20.00**	**23.20.00**	**23.20.00**

Software/Firmware Item	WorkCentre	WorkCentre + PostScript	WorkCentre Pro
Scanner Software (Options)			
• 232/238/245/255 PPM[1] Models	**17.05.00**	**17.05.00**	**17.05.00**
• 265/275 PPM[1] Models	**04.09.00**	**04.09.00**	**04.09.00**

5.3 Logical Scope and Boundary

The TOE logical boundary composed of two distinct security approaches: the architecture of the TOE, and the security functions provided by the TOE.

Architecturally, the TSF cannot be bypassed, corrupted, or otherwise compromised. Whereas the TOE is an MFD and not a general purpose computer, there are no untrusted subjects, or processes, contained therein, and the TSF functions in its own domain (Security Architecture – TSF_ARCH). While not a TSF in the classic sense of the term, the functionality that would be associated with TSF_ARCH is present and represented by the security functional requirements (SFRs) FPT_RVM.1 and FPT_SEP.1 based strictly on the TOE definition and architecture.

The following security functions are controlled by the TOE:

- Image Overwrite (TSF_IOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSec)
- Network Management Security (TSF_NET_MGMT)
- FAX Flow Security (TSF_FAX_FLOW)
- Security Management (TSF_FMT)

6. DOCUMENTATION

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence[1], covering:

- Configuration Management Documentation,
- Functional Specification,
- High-level Design,
- Correspondence Evidence,
- Installation, Generation, and Startup Procedures,
- Delivery Procedures, Secure Installation and Operation Guidelines,
- Strength of Function Analysis,
- Test Coverage Analysis Evidence,
- Vulnerability Analysis Report,
- Administrator Guide,
- User Guide,
- Configuration Management,
- Test Documentation to include Test Plans, Procedures, and Test Results
- Security Target

[1] A complete list of the documentation used during the evaluation is included in Section 3.5 of the *Evaluation Technical Report for a Target of Evaluation*, Version 1.0, March 13, 2006.

7. IT PRODUCT TESTING

7.1 Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results demonstrate accurate correspondence between the tests identified and the functional specification, and that the developer's testing is adequate to satisfy the requirements of EAL2.

The developer tested each of the security functions; their tests were largely focused on verification of the security functional requirements claimed in the ST. This includes user data protection, image overwrite, authentication and security management requirements, etc.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. They also verified that the test documentation showed results that were consistent with the expected results for each test script.

7.2 Evaluator Testing

The evaluator performed independent testing of a subset of the TOE Security Functions. The test cases devised by the evaluation team demonstrate that the TOE meets the security functional requirements in the Security Target and that the security functions operate as described in the design evidence. The evaluation team used information provided in the development evidence to determine which interfaces to stimulate to produce the desired effects.

The independent testing focused on five areas

- TOE Verification
- Image Overwrite
- Authentication
- Security Management
- Cryptographic Support and User Data Protection

7.2.1 Vulnerability Testing

The purpose of vulnerability testing is to determine the existence and exploitability of flaws or weaknesses in the MFD. The evaluator ran a nikto scan against the TOE to determine if any obvious vulnerabilities with default or sample web server files are revealed. The nikto command completed successfully and no obvious vulnerabilities are revealed.

The evaluators tested the ability of the TOE to block unauthorized access to the Audit Log, and to block unauthorized access via the NetBios connection (i.e., attempt to access the net controller filesystem through NetBios); to protect the System Administrator's password from capturing when SSL is enabled; as well as immunity to a number of known attack scenarios (e.g., Postscript file enumeration , Postscript denial of service, TRACE cross-site scripting, resource flooding SYN flood, malicious Jetdirect, buffer overflow, etc.)

8. EVALUATED CONFIGURATION

Evaluated TOE: Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems.

8.1 Evaluation Tools

To perform functional and vulnerability testing activities, the evaluation team used the following equipment:

WCP - The Xerox WorkCentre Pro 238 was delivered and installed with all default parameters. The TOE is delivered and basic installation is provided by a factory authorized Xerox field engineer. According to the Xerox published Installation, Generation and Startup (IGS) Guidelines [XRA2_ADO_IGS], the TOE is configured by the consumer (System Administrator).

The Xerox field engineer delivered and installed the Xerox WorkCentre Pro 238 according to the guidelines he received from the factory. The CCEL then continued the installation in accordance with the IGS document [XRA2_ADO_IGS]. The IP address assigned to the network interface was 192.168.1.101.

WINXP - WINXP is a Windows XP Pro laptop used to interact with the WorkCentre Pro as the System Administrator via the WebUI. Additionally, WINXP has TeraTerm software installed to perform procedures that utilize the network controller serial port and "ngrep," a utility used to selectively capture network packets. The IP address assigned to the network interface was 192.168.1.201.

SUSE - SuSE is a Linux workstation with SuSE Pro 9.0 installed in its default configuration. SUSE was used to send SNMPv3 commands to the TOE. The IP address assigned to the network interface was 192.168.1.100.

WIN2K - WIN2K is a Windows 2000 Server used to provide DNS resolution services to the test components. The IP address assigned to the network interface was 192.168.1.1.

DEMETER - Demeter is a IBM T40 Thinkpad configured by the CCTL. The OS is Fedora Core 3 Linux installed with default parameters. The ethereal network scanning package was installed for use in developing network attack scripts. The IP address assigned to the network interface was 192.168.1.202.

Management Hub - The management hub is a CentreCOM 8 port Workgroup Hub. The TOE, SUSE, WINXP and WIN2K are connected via their respective Ethernet ports. Its purpose is to serve as a simple hub connecting the TOE and the client computers.

9. RESULTS OF THE EVALUATION[2]

The TOE was found to provide the capabilities defined by the Security Target, and to satisfy all the requirements of EAL2 augmented with ALC_FLR.2.

10. VALIDATOR COMMENTS

The Validator offers the following comments:

- The Validator did not attend testing for this product, but did carefully review all of the documentation provided by Xerox Corporation and Computer Sciences Corporation, in support of the evaluation.
- The cryptography used in this product has not been FIPS certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11. SECURITY TARGET

The ST, *Xerox WorkCentre®/WorkCentre®* Pro *232/238/245/255/265/275 Multifunction systems Security Target Version 1.0, Revision 1.12, March 23, 2006* is included here by reference.

[2] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. GLOSSARY

AUT	Authentication
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HDD	Hard Disk Drive
IIO	Immediate Image Overwrite
IP	Internet Protocol
IPSec	Internet Protocol Security
MFD	Multifunction Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary laboratory Assessment Program
ODIO	On-Demand Image Overwrite
PP	Protection Profile
PSTN	Publicly Switched Telephone Network
RSA	Rivest-Shamir-Adleman
SNMPv3	Simple Network Management Protocol , Version 3
SOF	Strength of Function

SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security : Introduction and general model, dated January 2004, version 2.2.

[6] Security Target, Xerox WorkCentre®/WorkCentre® *Pro* 232/238/245/255/265/275 Multifunction Systems Security Target Version 1.0, Revision 1.12, March 23, 2006.

[7] Common Criteria Testing Laboratory Penetration Test Plan and Report, Xerox WorkCentre®/WorkCentre® *Pro* 232/238/245/255/265/275 Multifunction Systems, March 13, 2006.

[8] CSC Common Criteria Laboratory Independent Test Plan and Report, Xerox WorkCentre®/WorkCentre® *Pro* 232/238/245/255/265/275 Multifunction Systems, March 13, 2006.

[9] Evaluation Technical Report for a Target of Evaluation, Xerox WorkCentre®/WorkCentre® Pro 232/238/245/255/265/275 Multifunction Systems Security Target Version 1.0, Version 1.0, March 13, 2006