

Setting new standards for security in the office

Announcing Common
Criteria Certification for
the Xerox WorkCentre
M35/M45/M55 and
WorkCentre Pro 35/45/55

June 2004



Table of Contents

1. Security requirements and the marketplace	1
2. Establishing a Common Criteria	2
3. Xerox commitment to security	4
4. Conclusions	6



1 Security requirements and the marketplace

Innovations in information technology have rapidly increased over the last several years, fueling the pace and productivity of business across all sectors and industries. Great strides have been made in the way information is created, stored, managed, distributed, and archived. However, this innovation has also created opportunities for those seeking to intercept or corrupt valuable information and disrupt the flow of business. The magnitude of destruction that can be wrought by cyber-criminals is truly hard to overstate—privacy, property, assets of all kinds, are at stake.

In response to these threats, Xerox has taken an industry-leading role by developing and implementing information security technology for nearly a decade. This paper will explore the dynamic state of evolving security regulations and the efforts of Xerox to meet and exceed its customers' security needs. It will also highlight Xerox's most recent achievement—Common Criteria Certification of the WorkCentre M35/M45/M55 and WorkCentre Pro 34/45/55.

Responding to the federal government

Given the highly sensitive nature of data handled by the federal government, whether pertaining to national security or Social Security, it must be protected. Recent geopolitical events have emphasized the importance of information security and strengthened the resolve of the United States Federal Government, as well as individual state and local governments, to protect information systems and their networks.

Other events, ranging from corporate financial scandals to initiatives designed to protect individual privacy rights, have also fostered the creation of information security legislation. The Health Insurance Portability and Accountability Act (HIPAA) in health care, Gramm-Leach-Bliley (GLBA) in the financial sector, and the Federal Information Security Management Act of 2002 (FISMA) are just a few examples of many new security regulations being issued to oversee the way that information is shared, stored, and protected.

With so many regulatory and compliance measures to respond to, Xerox has looked to federal government requirements, among others, as guidelines. By developing solutions that comply with the most stringent security standards, Xerox is in a position to offer highly secure solutions to all of its customers in all business sectors. Whether customers are seeking compliance with HIPAA or are concerned with the Sarbanes-Oxley Act, they can be assured that their information is being protected with the same rigor as national security matters.

2

Establishing a Common Criteria

Common Criteria Certification provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality, and availability for systems and data, accountability at the individual level, and assurance that all goals are met. Common Criteria Certification is a requirement of hardware and software devices used by federal government on national security systems.

The history of Common Criteria

The Common Criteria is a descendant of the US Department of Defense Trusted Security Evaluation Criteria (TCSEC) originally in the 1970's. TCSEC was informally known as the "Orange Book." Several years later Germany issued their own version, the Green Book, as did the British and the Canadians. A consolidated European standard for security evaluations, known as ITSEC, soon followed. The United States joined the Europeans to develop the first version of the international Common Criteria in 1994. The current version of the Common Criteria, 2.1, was issued in August, 1999.

The Common Criteria is also known as ISO 15408. The international community has embraced the Common Criteria through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The National Information Assurance Partnership (NIAP) was formed to administer a security evaluation program in the United States that utilizes the Common Criteria as the standard for evaluation.

Achieving Common Criteria Certification

Common Criteria Certification is a rigorous process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluation of products against security requirements. Products are tested against functional security requirements based on predefined Evaluations Assurance Levels (EALs). Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 were tested against and met EAL 2.

For health care, financial services and other industries, the need for security is no less important. Whether they are protecting their customers' privacy, or intellectual and financial assets, assurance that networks, hard drives and phone lines are safe and secure from hackers, viruses and other malicious activities is critical. Common Criteria Certification, while not a requirement outside the federal government, can provide independent validation and assurance of all security claims.

For years, Xerox has held a leadership position in delivering exceptionally well-architected and highly productive devices for the office environment. Now Xerox can add Common Criteria Certification for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 to its long list of customer advantages for the office.



Common Criteria Certification for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 was completed by Computer Science Corporation, an accredited Common Criteria Testing Laboratory. The security functions certified include:

- Image Overwrite
- Authentication
- Security Management
- Data Flow Security

Image Overwrite – During normal operation, a multifunction device temporarily stores image data on the hard drive. The image overwrite function eradicates customer data by overwriting the disk surface following operation and insures that no normal read process can discover the original customer data. The overwrite mechanism complies with the 3-pass process specified in the U.S. Department of Defense Directive 5200.28-M. The image overwrite function overwrites data once a job is completed or when invoked at any time by the system administrator.

Authentication and Security Management –

Only users who are assigned as the system administrator and authenticated via a personal identification number can access the security settings of the device. Network authentication further restricts access to scan, e-mail, and fax features by validating network user names and passwords prior to the use of these features.

Data Flow Security – The secure embedded fax ensures that malicious users cannot access network resources from the telephone line via the device's fax modem because the fax subsystem is internally separated from network functions. Additionally, faxes can be automatically routed to a password protected fax mailbox or stored at the device until an authorized user releases them for printing.

About NIAP

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems, and appropriate metrics for evaluating those products and systems.

The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure.

For more information, visit www.niap.nist.gov.

3 Xerox commitment to security

Decision makers across industries and within both private and public sectors are facing the arduous task of integrating and complying with new security regulations while facing increased levels of accountability. What's more, they're under constant pressure to protect intellectual and financial assets from assaults, viruses, worms, and other forms of cyber-sabotage. In the office environment, decision makers have had to simply trust that their vendors' security statements were true, with little or no ability, or opportunity, to validate security claims when making purchase decisions.

At Xerox, security issues are front and center. As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Customers have responded by looking to Xerox as a trusted provider of secure solutions with many standard and optional security features. And now, with Common Criteria Certification, Xerox customers can be completely confident that their information is safe.

Xerox Security Goals

Xerox comprehends and supports Common Criteria security objectives as well as security regulations relating to health care, finance, pharmaceuticals and other industries. Xerox has identified five key security goals:

- | | | | | |
|---|--|---|--|--|
| ▼ | ▼ | ▼ | ▼ | ▼ |
| Integrity | Confidentiality | Availability | Accountability | Assurance |
| <ul style="list-style-type: none">• No unauthorized alteration of data• System performs as intended, free from unauthorized manipulation | <ul style="list-style-type: none">• No unauthorized disclosure of data during processing, transmission, or storage | <ul style="list-style-type: none">• Systems work properly• No denial of service for authorized users• Protection against unauthorized use of the system | <ul style="list-style-type: none">• Actions of an entity can be traced directly to that entity | <ul style="list-style-type: none">• Confidence that integrity, confidentiality, availability, and accountability goals have been met |

The solution that maximizes productivity and security

In the networked office environment, digital multifunction devices print, copy, scan, e-mail, and fax. Hand in hand with this broad range of functionality is an equally broad range of security issues. Security breaches can be as inadvertent as picking up someone else's job from the printer tray to malicious viral infections, hacking, and data theft.

It's important to note that in some environments, such as the federal government, it has been a matter of policy not to allow multifunction devices to be simultaneously connected to the fax and the network. While this mandate protects the network from hackers who might try to access it via the fax, it disables the fax capability of the device altogether. Now with Common Criteria Certification, Xerox is the only multifunction device manufacturer to receive third-party validation that the fax and network lines are separate and secure. This assurance means that users of Xerox multifunction devices can "turn the fax back on."

Xerox can also provide security solutions that restrict access, track usage, and protect all confidential data that travels through the CopyCentre digital copiers, WorkCentre copier-printers, and WorkCentre Pro advanced multifunction systems.

Some of the security features enabled by Xerox include:

Embedded Fax – Prevents unauthorized access to the device via the fax subsystem because it is internally separated from network functions. This eliminates a significant vulnerability; computers hackers cannot access the network and sensitive data via the fax line. No other multifunction device manufacturer has obtained third party assurance that fax and network lines are separated. (Available on Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55.)

Image Overwrite – Electronically eradicates customer data by repeatedly overwriting the disk surface with specific patterns of data. At the end of the procedure the device reads a portion of the overwritten area – typically 10% – to make sure that only the last pattern written can be read. This insures that no normal read process can discover the original customer data. Image Overwrite can be set to occur automatically at job completion or can be invoked by the system administrator as needed.

Device Access Password Protection – Administrative set-up screens and remote network settings cannot be viewed or altered without a personal identification number (PIN). This controls access to all device functions.

Secure Print – Holds jobs until the job owner enters a PIN to release them for printing to prevent unauthorized viewing. Secure Print prevents documents from ending up in unauthorized hands.

Removable Disk Drive Accessory – The removable hard drive may be taken out and stored for maximum security. This feature may be ideal for the most sensitive data. (Available on CopyCentre C65/C75/C90 and WorkCentre Pro 65/75/90.)

Network Authentication – Restricts access to scan, e-mail, and networked fax features by validating network user names and passwords prior to use of these features.

IP Address Restriction - Administrative set-up screens allow access to be restricted or granted for specific IP addresses to control communications with specific network clients.

Xerox Business Partners

Meeting the latest security demands often requires a joint effort between Xerox and its business partners. Xerox Business Partners are recognized industry leaders who, like Xerox, have developed exceptional capabilities and a loyal following of customers. Combining Xerox office technology with innovative, application-specific software developed by Xerox Business Partners and validated by Xerox allows customers to achieve higher levels of security.

Examples of Xerox Business Partner solutions that contribute to a secure office environment include the following:

- **Discovery, tracking, reporting, and assessment solutions**
 - Control Systems Xtrak
 - Equitrac Office
 - Pharos Blueprint and Uniprint
- **Secure fax solutions**
 - Omtool Genifax
 - Captaris RightFax
- **Secure e-mail solutions**
 - Omtool Genidocs
 - Captaris RightFax
- **Secure printing solutions**
 - Equitrac Office
 - Pharos Uniprint
 - Control Systems Xtrak
- **Encrypted distribution**
 - Omtool Genidocs
 - Captaris RightFax SecureDocs
- **Secure digital signature**
 - Omtool Genidocs

4

Conclusions

“Turning the fax back on”

Xerox digital multifunction devices are well-architected, highly productive solutions that offer superior reliability and performance. However, due to security concerns, the fax capability was frequently not utilized by customers concerned with potential security breaches. Customers simply didn't take full advantage of the features that the WorkCentre and WorkCentre Pro had to offer. Now with the Common Criteria Certification, the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 offer safe and secure faxing that has been tested and validated against federal government standards, allowing customers to maximize their equipment investment and productivity. Customers can now 'turn the fax back on' with confidence that their network is secure.

Simplifying the purchase decision

Regardless of industry or business environment, all sectors have an increasing need for secure information systems. Threats from hackers, viruses and other malicious sources will continue for the foreseeable future. In the ongoing battle to protect data and information networks, the best defense is an offensive course of action. Xerox has a proven track record in developing and implementing technologies that protect information whether it is being printed, copied, faxed, e-mailed, or archived. Now, Common Criteria Certification, the most rigorous validation process and the only one recognized by the federal government, provides Xerox customers with an even higher level of confidence that their data is safe. Combining this proven level of security with Xerox benchmark productivity, reliability, and service makes Xerox multifunction devices the superior choice for any demanding office environment.



Future certifications

Xerox will continue to seek Common Criteria evaluation and certifications for its products.

Call today. For more information about Xerox office workflow solutions, call **1-800-ASK-XEROX** or visit us at **www.xerox.com/office**.



XEROX
Worldwide Partner