

## Security and the Federal Government

# Meeting security standards where it counts most

### The state of security

Innovations in information technology continue to drastically change the way information is created, stored, managed, distributed, and archived. However, threats to information security from people seeking to intercept or corrupt valuable information and disrupt the flow of business are also on the rise. The magnitude of destruction caused by cyber-criminals is hard to overstate – privacy, property, assets of all kinds, are at stake. And, no one is as sensitive to these threats as the U.S. Federal Government and its agencies.

### Common Criteria Certification

Common Criteria Certification is now required to ensure that IT systems and devices utilized by the federal government for national security are indeed secure. This process provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. Product testing is conducted by third-party laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP).

### Front and center with security

At Xerox, security issues have always been front and center. As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure. And now, with Common Criteria Certification, Xerox customers have an extra measure of confidence that their information is absolutely safe.



### The Challenge:

Federal government policy requires that all networked devices used in national security systems meet 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 security claims are objectively verified.

### The Solution:

Common Criteria Certification, administered by the National Information Assurance Partnership (NIAP). This is a rigorous process that includes the testing of devices against security requirements by accredited, third-party laboratories.

### The Xerox Advantage:

In addition to delivering exceptionally well-architected and highly productive devices into the office environment, Xerox has received Common Criteria Certification for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55. As part of the certification process, the security of the embedded fax function of these devices was also validated. *No other multifunction device manufacturer has obtained third-party assurance that fax and network lines are separated.*



## Commitment to Security and the Common Criteria

Xerox offers a variety of solutions that maximize productivity and security.

**Embedded Fax** – Prevents unauthorized access to the device via the fax subsystem because it is internally separated from network functions. *No other multifunction device manufacturer has obtained third party assurance that fax and network lines are separated.*

**Image Overwrite** – Electronically eradicates data processed to the hard disk during print, scan, or e-mail operations by repeatedly overwriting the data.

**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.

**Removable Disk Drive Accessory** – The removable hard drive may be taken out and stored for maximum security.

**Network Authentication** – Restricts access to scan, e-mail, and network 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 for specific IP addresses to control communications with specific network clients.

### Achieving Common Criteria Certification

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** – During normal operation, a multifunction device temporarily stores image data on the hard drive. The image overwrite function eradicates customer data by repeatedly overwriting the disk surface with specific patterns of data. At the end of the procedure it reads a portion of the overwritten area – typically 10% – to make sure that only the last pattern written can be read. This ensures 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 eradicates data once a job is completed or when invoked at any time by the system administrator.

#### Authentication and Security Management –

Only system administrators 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.

