State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Superior Office Svc., Inc.
208 Leon Sullivan Way
Chas. WV 25301

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/25/2007	NET 30	OUR TRUCK	Dest.	N/A

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	3	LS		015-15	$5888.00 mo.	$211,968.00 36 mo. Total

MULTIFUNCTIONAL DIGITAL IMAGING SYSTEM

TO PROVIDE 36 MONTH LEASE/RENTAL, FOR 3 RICOH MODEL MP 1100 OR EQUAL DIGITAL MULTIFUNCTIONAL IMAGING SYSTEM WITH MONTHLY MAINTENANCE, UNLIMITED SERVICE CALLS, ALL PARTS, LABOR AND TONER TO BE INCLUDED, EXCEPT PAPER.

THE MODEL/BRAND/SPECIFICATIONS NAMED HEREIN ESTABLISH THE ACCEPTABLE LEVEL OF QUALITY ONLY AND ARE NOT INTENDED TO REFLECT A PREFERENCE OR FAVOR ANY PARTICULAR BRAND OR VENDOR. VENDORS WHO ARE BIDDING ALTERNATES SHOULD SO STATE AND INCLUDE PERTINENT LITERATURE AND SPECIFICATIONS. FAILURE TO PROVIDE INFORMATION FOR ANY ALTERNATES MAY BE GROUNDS FOR REJECTION OF THE BID. THE STATE RESERVES THE RIGHT TO WAIVE MINOR IRREGULARITIES IN BIDS OR SPECIFICATIONS IN ACCORDANCE WITH SECTION 148-1-4(F) OF THE WEST VIRGINIA LEGISLATIVE RULES AND REGULATIONS.

MANUFACTURER: CANON ..... MODEL #: IR7105 .....

METER CLICKS SHALL BE COUNTED AS 1 COPY REGARDLESS OF COPY SIZE. OVERAGE CHARGES SHALL BE PER COPY ABOVE 600,000 COPIES PER MONTH FOR ALL THREE MACHINES COMBINED.

MONTHLY CHARGES SHALL INCLUDE ALL THREE MACHINES FOR LEASE/RENTAL, MAINTENANCE AND OVERAGE CHARGES.

A CHANGE ORDER TO ESTABLISH START DATE WILL BE GENERATED AFTER INSTALLATION AND ACCEPTANCE OF

RECEIVED
2007 MAY 16 A 10:30
PURCHASING DIVISION
STATE OF WV

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE Doug Farmer TELEPHONE 304-414-7250 DATE 5-16-07

TITLE Branch MGR. FEIN 550465039 ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Superior Office Sup., Inc.
208 Leon Sullivan Way
Chas., WV 25301

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/25/2007	Net 30	Our Truck	Dest.	N/A

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

MACHINES BY DOH.

SEE ATTACHED

VENDOR PREFERENCE CERTIFICATE

CERTIFICATION AND APPLICATION* IS HEREBY MADE FOR PREFERENCE IN ACCORDANCE WITH WEST VIRGINIA CODE, 5A-3-37 (DOES NOT APPLY TO CONSTRUCTION CONTRACTS).

A. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:

(✓) BIDDER IS AN INDIVIDUAL RESIDENT VENDOR AND HAS RESIDED CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR

(✓) BIDDER IS A PARTNERSHIP, ASSOCIATION OR CORPORATION RESIDENT VENDOR AND HAS MAINTAINED ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR 80% OF THE OWNERSHIP INTEREST OF BIDDER IS HELD BY ANOTHER INDIVIDUAL, PARTNERSHIP, ASSOCIATION OR CORPORATION RESIDENT VENDOR WHO HAS MAINTAINED ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR

( ) BIDDER IS A CORPORATION NONRESIDENT VENDOR WHICH HAS AN AFFILIATE OR SUBSIDIARY WHICH EMPLOYS A MINIMUM OF ONE HUNDRED STATE RESIDENTS AND WHICH HAS MAINTAINED ITS HEAQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA CONTINUOUSLY FOR THE FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE [signature] TELEPHONE 304-414-7250 DATE 5-16-07

TITLE Branch Mgr FEIN 550465039 ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	3

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B	FREIGHT TERMS
04/25/2007				

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

CERTIFICATION.

B. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:

(✓) BIDDER IS A RESIDENT VENDOR WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST 75% OF THE EMPLOYEES WORKING ON THE PROJECT BEING BID ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID;
OR
( ) BIDDER IS A NONRESIDENT VENDOR EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS OR IS A NONRESIDENT VENDOR WITH AN AFFILIATE OR SUBSIDIARY WHICH MAINTAINS ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST 75% OF THE EMPLOYEES OR BIDDERS' AFFILIATE'S OR SUBSIDIARY'S EMPLOYEES ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID.

BIDDER UNDERSTANDS IF THE SECRETARY OF TAX & REVENUE DETERMINES THAT A BIDDER RECEIVING PREFERENCE HAS FAILED TO CONTINUE TO MEET THE REQUIREMENTS FOR SUCH PREFERENCE, THE SECRETARY MAY ORDER THE DIRECTOR OF PURCHASING TO: (A) RESCIND THE CONTRACT OR PURCHASE ORDER ISSUED; OR (B) ASSESS A PENALTY AGAINST SUCH BIDDER IN AN AMOUNT NOT TO EXCEED 5% OF THE BID AMOUNT AND THAT SUCH PENALTY WILL BE PAID TO THE CONTRACTING AGENCY OR DEDUCTED FROM ANY UNPAID BALANCE ON THE CONTRACT OR PURCHASE ORDER.

BY SUBMISSION OF THIS CERTIFICATE, BIDDER AGREES TO

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	4

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Superior Office Suc., Inc.
208 Leon Sullivan Way
Chas., WV 25301

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/25/2007	Net 30	Our Truck	Dest.	N/A

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

DISCLOSE ANY REASONABLY REQUESTED INFORMATION TO THE PURCHASING DIVISION AND AUTHORIZES THE DEPARTMENT OF TAX AND REVENUE TO DISCLOSE TO THE DIRECTOR OF PURCHASING APPROPRIATE INFORMATION VERIFYING THAT BIDDER HAS PAID THE REQUIRED BUSINESS TAXES, PROVIDED THAT SUCH INFORMATION DOES NOT CONTAIN THE AMOUNTS OF TAXES PAID NOR ANY OTHER INFORMATION DEEMED BY THE TAX COMMISSIONER TO BE CONFIDENTIAL.

UNDER PENALTY OF LAW FOR FALSE SWEARING (WEST VIRGINIA CODE 61-5-3), BIDDER HEREBY CERTIFIES THAT THIS CERTIFICATE IS TRUE AND ACCURATE IN ALL RESPECTS; AND THAT IF A CONTRACT IS ISSUED TO BIDDER AND IF ANYTHING CONTAINED WITHIN THIS CERTIFICATE CHANGES DURING THE TERM OF THE CONTRACT, BIDDER WILL NOTIFY THE PURCHASING DIVISION IN WRITING IMMEDIATELY.

BIDDER: Superior Office Suc., Inc. Doug Facemire

DATE: 5-16-07

SIGNED: Doug Facemire

TITLE: Branch Mgr.

* CHECK ANY COMBINATION OF PREFERENCE CONSIDERATION(S) IN EITHER "A" OR "B", OR BOTH "A" AND "B" WHICH YOU ARE ENTITLED TO RECEIVE. YOU MAY REQUEST UP TO THE MAXIMUM 5% PREFERENCE FOR BOTH "A" AND "B".
(REV. 12/00)

NOTICE

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
Doug Facemire	304-414-7250	5-16-07

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
Branch Mgr	55-0465039	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	5

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
SUPERIOR OFFICE SUC., INC.
208 LEON SULLIVAN WAY
CHAS., WV 25301

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/25/2007	NET 30	OUR TRUCK	Dest.	N/A

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

A SIGNED BID MUST BE SUBMITTED TO:

DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
BUILDING 15
2019 WASHINGTON STREET, EAST
CHARLESTON, WV 25305-0130

THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:

SEALED BID

BUYER: 33

RFQ. NO.: 5770015

BID OPENING DATE AND TIME

PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:

304-414-7051

CONTACT PERSON (PLEASE PRINT CLEARLY):

DOUG FACEMYRE

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
[signature]	304-414-7250	5-16-07

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
BRANCH MGR	550465039	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
5770015	6

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN JOHNSTON
304-558-2402

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Superior Office Svc., Inc.
208 Leon Sullivan Way
Chas., WV 25301

SHIP TO
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION
BUILDING 5, ROOM A050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV
25305-0430 304-558-0408

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/25/2007	NET 30	OUR TRUCK	Dest.	N/A

BID OPENING DATE: 05/16/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
	****** THIS IS THE END OF RFQ 5770015 ****** TOTAL:					$211,968.00

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE [signature] TELEPHONE 304-525-7250 DATE 5-16-07

TITLE Branch MGR FEIN 550465039 ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

SPECIFICATIONS

- MACHINE TYPE: CONSOLE

- RESOLUTION: 1200dpi

- DOCUMENT FEEDER: RADF FOR 100 SHEETS UP TO 11 X 17 ORIGINALS

- DUPLEX: UNLIMITED (5.5 X 11 TO 11 X 17)

- MAXIMUM COPY SIZE: 11 X 17 (LEDGER)

- MINIMUM COPY SIZE: 5.5 X 8.5

- COPY SPEED : 105cpm, LETTER SIZE

- MAGNIFICATION REDUCTION / ENLARGEMENT 25%TO 400% INCREMENTS OF 1%

- MINIMUM PAPER CAPACITY SUPPLY : 7,000 SHEETS OF 20-WT. OR GREATER. VARIOUS SIZES 5.5 X 8.5 TO 11 X 17
(NOTE) : HALF OF THE PAPER CAPACITY SUPPLY TO ACCOMMODATE 11 X 17, 20-WT AT ONE TIME.
(ALSO NOTE) LARGE SIZE CAPACITY PAPER TRAYS WILL BE NECESSARY.

- MULTIPLE COPIES : 1 TO 9999

- PAPER WEIGHTS : 17-LB TO 110-WT

- AUTO PAPER TRAY SWITCHING

- MULTI-BYPASS TRAY: 500 SHEETS OF 8.5 X 11 TO 11 X 17

- SECURITY FEATURES: USER AUTHENTICATION, DATA OVERWRITE SECURITY
- SYSTEM, ENCYPTED ADDRESS BOOK , UNAUTHORIZED COPY CONTROL (RPCS DRIVER)

- POWER REQUIREMENTS : 208 – 240V, 50 /60 Hz 20A

FINISHER

- RECEIVING PAPER TRAY : SORTER / STACKER 3000 SHEET CAPACITY

- STAPLER: 100 SHEET CAPACITY OF LETTER SIZE.

- STAPLER POSITION : 1 – ANY CORNER & 2 – SIDE MARGIN

AUTOMATIC DOCUMENT FEEDER

- ACCEPTABLE ORIGINALS : STATEMENT)9 X 11) TO 11 X 17 (LEDGER)

- SCANNING SPEED : AT LEAST 80-CPM ON LETTER SIZE ORIGINALS.

- CAPACITY : 100 PAGES, ALL ACCEPTABLES SIZES, OF 20-LB, PAPER.

- PAPER WEIGHTS: 13-LB TO 110-LB, INDEX.

- HDD : 100GB STORAGE.

PRINTER MODULE

- MAXIMUM SPEED / RESOLUTION : 105, 1200 dpi

- MEMORY : 512MB RAM MINIMUM.

- PRINTER LANGUAGES : PLC5e, PLC6, RPCS (STANDARD)

- INTERFACE : ETHERNET R145-45 : 100 BASE – TX/ 10BASE-T, USB 2.0

- DRIVERS : STANDARD : PCL5e, PCL6, RPCS

- MIB SUPPORT : STANDARD : MBI-II, HOST RESOURCE, PRINTER MIB

- NETWORK SUPPORT: WINDOWS 9x/ME/NT 4.0/2000/XP/SERVER 2003; NOVELL NETWARE 3,12,3.2, 4.1, 4.11, 5.0 UNIX SUIN SOLARIS 2, 6, 7, 8, 9; HP-U 10.X11X; SCO OPEN SERVER 5.0.6; REDHAT LINUX 6.X/7.X8.X; IBM AIX V4.3, 5LVS. 1; MAC OS 8.6- 9.2. (OSX CLASSIC) MAC OS 10.1 OR LATER.

- NETWORK PROTOCOL: TCP/IP, IPX/SPX, SMB, ETHERTALK (AUTO SWITCHING)

SCANNER MODULE

- SCAN SPEED: 80 IMAGES PER MINUTE OF LETTER SIZE, AT 200dpi OR GREATER

- IMAGING; OPTIONAL RESOLUTION: 100-600 dpi OUTPUT FORMAT; TIFF (MULTI/SINGLE), JPEG, PDF, (MULTI/SINGLE) , HIGH-COMPRESSION PDF

- SPECIAL FEATURES: SCAN TO E-mail , SCAN TO FOLDER, SIMULTANEOUS SCAN- TO – E-mail, LDAP SUPPORT.

STANDARD UTILITIES: WEB BASE, CLIENT AND ADMINISTRATIVE APPLICATION.

EVALUATION AND AWARD SHALL BE BASED ON A 36 MONTH LEASE TOTAL COST INCLUDING THE MONTHLY LEASE RATE, MONTHLY MAINTENANCE RATE AND ESTIMATED OVERAGE OF 2000 COPIES PER MACHINE PER MONTH. AGENCY ESTIMATED COPY VOLUME IS 200,000 PER COPIER, PER MONTH. METER READINGS ARE TO BE COMBINED ON ALL THREE COPIERS FOR A TOTAL OF 600,000 COPIES PER MONTH.

BID SCHEDULE FOR 36 MONTH LEASE

ESTIMATED USAGE - 600,000 COPIES PER MONTH

QUANTITY

3	MONTHLY COPIER LEASE CHARGE PER MACHINE	$ 862.66 EA.
3	*MONTHLY MAINTENANCE CHARGE PER MACHINE	$ 1100.00 EA.

MONTHLY COPY ALLOWANCE 600,000 COPIES PER MONTH.

EXCESS COPY CHARGE $ .008 EA.

*MAINTENANCE SHALL INCLUDE ALL PARTS, LABOR, AND SUPPLIES EXCEPT PAPER.

SERVICE

SUCCESSFUL VENDOR MUST HAVE A MINIMUM OF TWO FACTORY TRAINED TECHNICIANS. PROOF OF CERTIFICATION REQUIRED PRIOR TO AWARD.

LOCATION OF SERVICE FACILITY AND PHONE NUMBER

208 LEON Sullivan Way Chas., WV 25301
304-414-7250

RESPONSE TIME TO SERVICE CALL (STATED IN HOURS)

1-4 Hours on Site

AGENCY EXPECTS SERVICE TECH'S REPLY TO SERVICE CALLS WITHIN 4-HOURS BY PHONE, AND WITHIN 8 HOURS IN PERSON OF INITIAL SERVICE CALL. IF PARTS ARE NEEDED TO BE ORDERED THAT ARE NOT IN THE POSSESSION OF THE LOCAL VENDER OR SERVICE TECH'S POSSESSION THE COMPANY OR SERVICE TECH WILL BE REQUIRED TO ARRANGE FOR THE PART OR PARTS TO BE DELIVERED DIRECTLY TO OUR AGENCY, WHEN THE PART OR PARTS ARE RECEIVED AT OUR LOCATION WE WILL IN TURN CALL THE COMPANY OR TECH. WE EXPECT A TECH WITHIN 4 HOURS TO INSTALL SAID PART OR PARTS.

DELIVERY

EQUIPMENT MUST BE DELIVERED, INSTALLED AND IN GOOD WORKING ORDER IN THE BASEMENT OF BUILDING #5, ROOM A-011 IN THE STATE CAPITOL COMPLEX.

CONTACT - BILL PERRY 304-558-9254

DEPARTMENT OF TRANSPORTATION
DIVISION OF HIGHWAYS
OFFICE SERVICES DIVISION, BLDG., #5, A-050
1900 KANAWHA BOULEVARD, EAST
CHARLESTON, WV 25304-0430

RFQ No. 5770015

AFFIDAVIT

West Virginia Code §5A-3-10a states:
No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owned is an amount greater than one thousand dollars in the aggregate

DEFINITIONS:
"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions. "Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities. "Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

EXCEPTION:
The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

LICENSING:
Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agencies or political subdivision. Furthermore, the vendor must provide all necessary releases to obtain information to enable the Director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

CONFIDENTIALITY:
The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures and rules. Vendors should visit **www.state.wv.us/admin/purchase/privacy** for the Notice of Agency Confidentiality Policies.

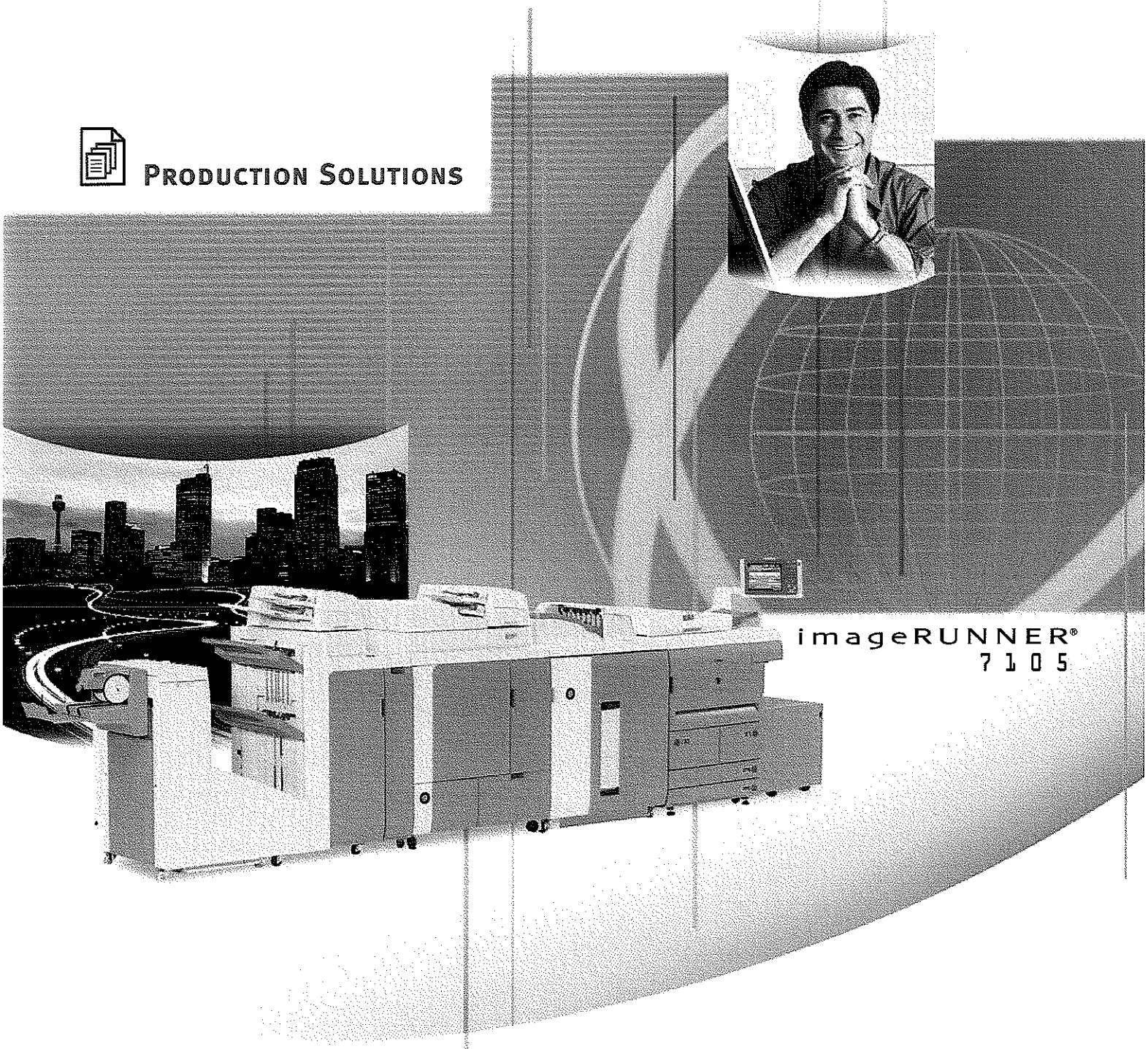
Under penalty of law for false swearing (West Virginia Code, §61-5-3), it is hereby certified that the vendor acknowledges the information in this said affidavit and are in compliance with the requirements as stated.

Vendor's Name: Superior Office Service, Inc.

Authorized Signature: [signature] Date: 5-16-07

Canon

PRODUCTION SOLUTIONS



imageRUNNER® 7105

meap POWERED BY

Challenge Your Document Production Standards

The Canon imageRUNNER 7105 is perfectly suited for central reproduction departments, print-for-pay establishments, print-on-demand applications, and large corporate offices where high-speed document production is required. To maximize versatility, the system is designed to meet professional publishing needs with available in-line perfect bookbinding, saddle-stitched booklet finishing, hole-punching, tab-feeding, and high-capacity stacking.

You can also leverage your imageRUNNER device investment further by using part of the system's vast memory as an on-site document storage and print-on-demand solution, while retaining complete control over device access and data protection with the latest identity management and security measures.

MAIN UNIT

Type:	Digital Multifunctional Imaging System
Imaging System:	Laser Dry Electrostatic Transfer
Developing System:	Dry Monocomponent Toner Projection
Main Unit CPU:	Dual Canon Custom Processors
Interface Connection:	10/100Base-TX (RJ-45), USB 2.0 High Speed
Image Server Memory:	Standard 1GB RAM + 40GB HDD
Max. Mail Boxes Supported:	100 (Max. Page Capacity: Approximately 20,000 pages)
Max. Copy Reservation:	20 Jobs
Acceptable Originals:	Sheets, Books, 3-Dimensional Objects up to 4.4 lb.
Max. Original Size:	11" x 17"
Max. Copy Size:	11" x 17"
Min. Copy Size:	3-15/16" x 5-7/8" (Stack Bypass)
Scanning Resolution:	600 x 600 dpi
Copy Resolution:	1200 x 600 dpi (Interpolated)
Halftone:	256-Level Grayscale
Exposure Control:	Automatic or Manual (Text, Photo, or Text/Photo)
Copy Speed:	105 cpm (Letter) 53 cpm (11" x 17")
First-Copy Time:	2.8 Seconds (From Platen)
Warm-Up Time:	6 Minutes or Less
Multiple Copies:	1 – 9,999
Duplexing:	Standard Automatic Trayless Duplexing
Magnification	
From Glass:	25% - 400% (In 1% increments)
From Feeder:	25% - 200% (In 1% increments)
Preset Reduction:	25%, 50%, 64%, 73%, 78%
Preset Enlargement:	121%, 129%, 200%, 400%
Standard Paper Supply:	Dual Front-Loading Drawers (1,500 Sheets each)
	Dual Front-Loading Cassettes (550 Sheets each)
	50-Sheet Stack Bypass
Optional Paper Supply:	3,500-Sheet Paper Deck-W1/X1
Paper Capacity:	Standard: 4,150 Sheets Maximum: 7,650 Sheets
Acceptable Paper Weight:	17 lb. Bond to 110 lb. Index (All Sources)
Power Consumption:	2.15kW
Plug:	NEMA 6-15R
Photoconductor Yield:	6 Million Impressions
Toner Yield:	47,000 Images @ 6% Coverage

Duplex Automatic Document Feeder

Tray Capacity:	100 Sheets
Scanning Speed:	85 Sheets Per Minute (Letter)
Acceptable Original Sizes:	Statement to 11" x 17"
Acceptable Size Originals:	Same Width
Acceptable Paper Weight:	13 lb. Bond to 80 lb. Cover

OPTIONAL ACCESSORIES

Paper Deck-W1/Paper Deck-X1

Paper Capacity:	3,500 Sheets
Number of Drawers:	1
Acceptable Paper Weight:	17 lb. Bond to 110 lb. Index
Acceptable Paper Size	
Paper Deck-W1:	Letter
Paper Deck-X1:	Letter-R, Letter, Legal, 11" x 17"

Perfect Binder-A1*

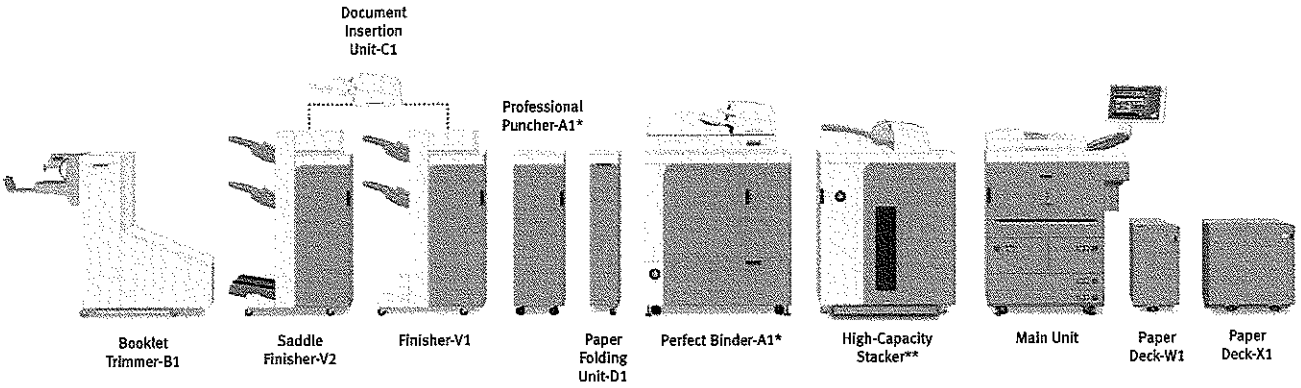
Bind Method:	Perfect Binding
Cutting Method:	Stack Rotation 3-Direction, or 1-Direction (for Open Edge) Cut
Finished Book Size: (After 3-Direction Cutting)	
Width:	7-1/8" to 11-1/4"
Length:	5-5/8" to 8-1/4"
Book Thickness:	10 to 200 Sheets Using 17 to 24 lb. Bond 10 to 150 Sheets Using 24 to 28 lb. Bond 10 Sheets Using 28 lb. Bond to 110 lb. Index
Cover Source Location:	Stack Bypass, Paper Drawers, Paper Deck (Imageable) Document Insertion Unit (For Pre-Printed Covers)
Stacker Tray Capacity:	3.94" (100mm) (Equivalent to 10 100-page Books with 17 lb. Bond)
Glue Supplies & Yield:	Glue-A1 (33 lb./15kg): Estimated Yield: 5,000 Sets of 100 Sheet Books (20 lb. Bond) Glue-A2 (11 lb./5kg): Estimated Yield: 1,650 Sets of 100 Sheet Books (20 lb. Bond)
Glue Warm-Up Time:	380 Seconds or Less
Glue Unit Capacity:	Bind Approximately 180 100-page Books Using 20 lb. Bond Paper
Trim Range	
Width:	7mm – 27mm
Length:	7mm – 39mm Adjustable in 1mm increments
Trimmer Waste Capacity:	Space for 3-Sided Cuttings From Approximately 15 100-page Books

Document Insertion Unit (Standard With Perfect Binder-A1)

Acceptable Media:	Covers and Inserts
Number of Trays:	2
Tray Capacity	
Upper Tray:	200 Sheets (20 lb. Bond)
Lower Tray:	200 Sheets (20 lb. Bond)
Acceptable Paper Weight:	17 lb. Bond to 158 lb. Index
Acceptable Paper Sizes	
Upper Tray:	Letter, Letter-R, Executive
Lower Tray:	11" x 17", Legal, Letter, Letter-R, Executive

Finisher-V1/Saddle Finisher-V2

Number of Trays:	2/3
Tray Capacity	
Top Tray:	3,000 Sheets
Lower Tray:	2,000 Sheets
Saddle-Stitch Tray:	30 Booklets or Limitless
Acceptable Paper Weight	
Finisher-V1:	17 lb. Bond to 110 lb. Index
Saddle Finisher-V2:	17 lb. Bond to 110 lb. Index
Acceptable Paper Size:	11" x 17", Legal, Letter, Letter-R, Statement-R, Executive
Staple Positions:	Corner Stapling, Double Stapling
Max. Stapling Capacity:	100 Sheets (Letter, Executive) 50 Sheets (11" x 17", Legal, Letter-R)
Type of Staple:	Staple-N1 (5,000 x 3)



Saddle-Stitching (Saddle Finisher-V2 Only)

Acceptable Paper Size:	11" x 17", Legal, Letter-R
Folding Mode:	V-Folding Standard
Stapling Capacity:	20 Sheets (80 Pages)
Type of Staple:	Staple-P1 (5,000 x 2)

Professional Puncher-A1* (For Finisher-V1/Saddle Finisher-V2)

Type:	External In-Line Punch Unit
Hole-Punching Method:	Press Punch Unit
Acceptable Punch Paper Weight:	20 lb. Bond to 110 lb. Index
Acceptable Punch Paper Size:	Letter
Punch Speed:	Up to 105 ppm (Depending on speed of main unit)
Punch Patterns (Optional):	Plastic Comb (19-Hole) Twin Loop (32-Hole) Twin Loop (21-Hole) Color Coil (44-Hole) Velo Bind (11-Hole) Loose-leaf Bind (3-Hole) Proclick (32-Hole)

Puncher Unit-V1 (For Finisher-V1/Saddle Finisher-V2)

Type:	Internal Punch Unit
Hole-Punching Method:	Press Punch System
Acceptable Punch Paper Weight:	17 lb. Bond to 110 lb. Index
Acceptable Punch Paper Size	
Two Holes:	Legal, Letter-R
Three Holes:	11" x 17", Letter
Punch Speed:	Up to 105 ppm (Depending on speed of main unit)

Document Insertion Unit-C1 (For Finisher-V1/Saddle Finisher-V2)

Number of Trays:	2
Capacity	
Upper Tray:	200 Sheets
Lower Tray:	200 Sheets
Acceptable Paper Weight:	17 lb. Bond to 158 lb. Index
Acceptable Paper Size	
Upper Tray:	Letter, Letter-R, Executive
Lower Tray:	11" x 17", Legal, Letter, Letter-R, Executive

Paper Folding Unit-D1 (For Finisher-V1/Saddle Finisher-V2)

Folding Method:	Roller Pressure Folding
Folding Type:	Z-Fold
Acceptable Paper Weight:	17 lb. Bond to 20 lb. Bond
Acceptable Paper Size:	11" x 17"

Booklet Trimmer-B1 (For Saddle Finisher-V2)

Margin Trimming:	Open-End Only
Trim Thickness:	40 Sheets
Waste Tray Capacity:	1,500 Sheets of Trimmed Strip
Acceptable Paper Weight:	17 lb. Bond to 110 lb. Index
Output Tray Capacity:	30 Booklets

CONNECTIVITY OPTIONS

Universal Send Kit-E1

Sending Method:	E-mail, I-fax, File Server (IPX, FTP, SMB), User Inbox
Address Book Capacity:	1,800 Destinations
File Format:	Standard: TIFF, PDF Optional: PDF (OCR)
Sending Size:	Statement to 11" x 17"
Scan Density:	200/300/400/600 dpi

Canon Multi-PDL Printer Kit-H1

Processor:	Dual Canon Custom Processors
Memory:	1 GB – Shared
Storage:	40 GB – Shared
PDL Support:	PCL 5e, PCL 6, PostScript® 3 Emulation, UFR II
Resolution:	1200 x 1200 dpi: UFR II, PostScript 3 Emulation 2400 x 600 dpi: PCL 5e, PCL 6
Interface Connections	
Standard:	10/100Base-TX (RJ-45), USB 2.0 High Speed
Network OS:	Windows® 98/Me/2000/XP Windows NT® 4.0 Windows Server 2003 (TCP/IP) Solaris 1.1x, 2.5x or Later Macintosh® OS 8.0 or Later (PPD) Novell® NetWare® v3.2, 4.1, 4.11, 4.2, 5, 5.1, 6, 6.5 (IPX/SPX)

imagePASS-S1 Print Controller

Type:	External Stand-Alone Controller
Processor:	Intel® Celeron® D 2.8GHz
Memory:	256MB
Storage:	80GB HDD
PDL Support:	Adobe® PostScript 3, PCL 5e, PCL 6
Resolution:	1200 x 1200 dpi: PostScript 3 2400 x 600 dpi: PCL 5e, PCL 6
Interface Connections:	Standard: 10Base-T/100Base-TX/1000Base-T (RJ-45) (RJ-45), USB 2.0 High Speed
Network OS:	Windows 98/Me/2000/XP Windows Server 2003 (TCP/IP) Solaris 8 or Later Sun OS 4.1.3 or Later Macintosh OS 9.2, OSX (10.2.4) or Later Novell NetWare 4.2, 5.1, 6.5 (IPX/SPX)

Other Accessories

- Cassette-AB1
- Tab Feeding Attachment-A1
- Document Tray-L1
- Braille Label Kit-A1
- Control Card Reader-D1
- Control Card Sets
- Universal Send PDF Enhancement Kit-C1
- Web Access Software-C1
- Remote Operator's Software Kit-A1
- Security Expansion Board-F1
- Expansion Bus-D1
- imageRUNNER Security Kit-A2
- Voice Guidance Kit-A2
- Secure Watermark Kit-A1
- Barcode Printing Kit-A1
- Finisher Option Power Supply Unit-R1
- Stacker Dolly-A1**
- Perfect Binder-A1
- Punch Tools
- ADF Access Handle-A1
- Hot Folder for imagePASS-S1
- Impose for imagePASS-S1
- High Capacity Stacker**

*The Professional Puncher-A1 cannot be installed simultaneously with the Perfect Binder-A1 and/or Puncher-V1.

**Check with your Authorized Canon Dealer for availability.

NOTE: Some accessories require additional equipment or may be prerequisites for other options. Check with your local Authorized Canon Dealer for details. Actual product appearance may differ from pictures shown.

Device Dimensions and Power Requirements Chart

Product/Accessory Name	Dimensions (H x W x D)	Weight	Power
Main Unit	58" x 47-7/8" x 30-7/8" (1474mm x 1216mm x 783mm)	617 lb. (280kg)	208V, 60Hz, 12A
Paper Deck-W1	22-1/2" x 12-3/4" x 23" (570mm x 323mm x 583mm)	90.4 lb. (41kg)	Directly From Main Unit
Paper Deck-X1	22-5/8" x 23-3/8" x 24-1/2" (574.5mm x 593mm x 621mm)	101 lb. (46kg)	
High-Capacity Stacker	50-4/5" x 33-9/10" x 30-1/5" (1290mm x 860mm x 765mm)	440 lb. (200kg)	120V, 10A
Perfect Binder-A1	53-1/2" x 36-1/4" x 31-1/8" (1360mm x 920mm x 791mm)	696 lb. (316kg)	208V, 15A
Finisher-V1	46-1/2" x 31-1/2" x 31-1/4" (1180mm x 800mm x 792mm)	278 lb. (126kg)	Directly From Main Unit* or 208V, 60Hz, 12A**
Saddle Finisher-V2	46-1/2" x 31-1/2" x 31-1/4" (1180mm x 800mm x 792mm)	392 lb. (178kg)	
Document Insertion Unit-C1	8-3/8" x 24-5/8" x 26-1/4" (213mm x 625mm x 667mm)	37.5 lb. (17kg)	From Finisher-V1 or Saddle Finisher-V2
Paper Folding Unit-D1	41" x 7-1/8" x 31" (1040mm x 179mm x 786mm)	97 lb. (44kg)	
Booklet Trimmer-B1	41" x 62-1/10" x 30-2/5" (1040mm x 1575mm x 770mm)	335 lb. (152kg)	
Professional Puncher-A1	38-1/2" x 12" x 28-1/2" (978mm x 305mm x 723mm)	170 lb. (77kg)	

** When Finisher is equipped with Paper Folding Unit-D1 and/or Document Insertion Unit-C1.*

*** When Finisher is equipped with Professional Puncher-A1, Booklet Trimmer-B1, High-Capacity Stacker, and/or Perfect Binder-A1.*

Canon

imageANYWARE

1-800-OK-CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042

0806-7105SS-PDF-TM

PRINTED ON RECYCLED PAPER IN THE U.S.A.

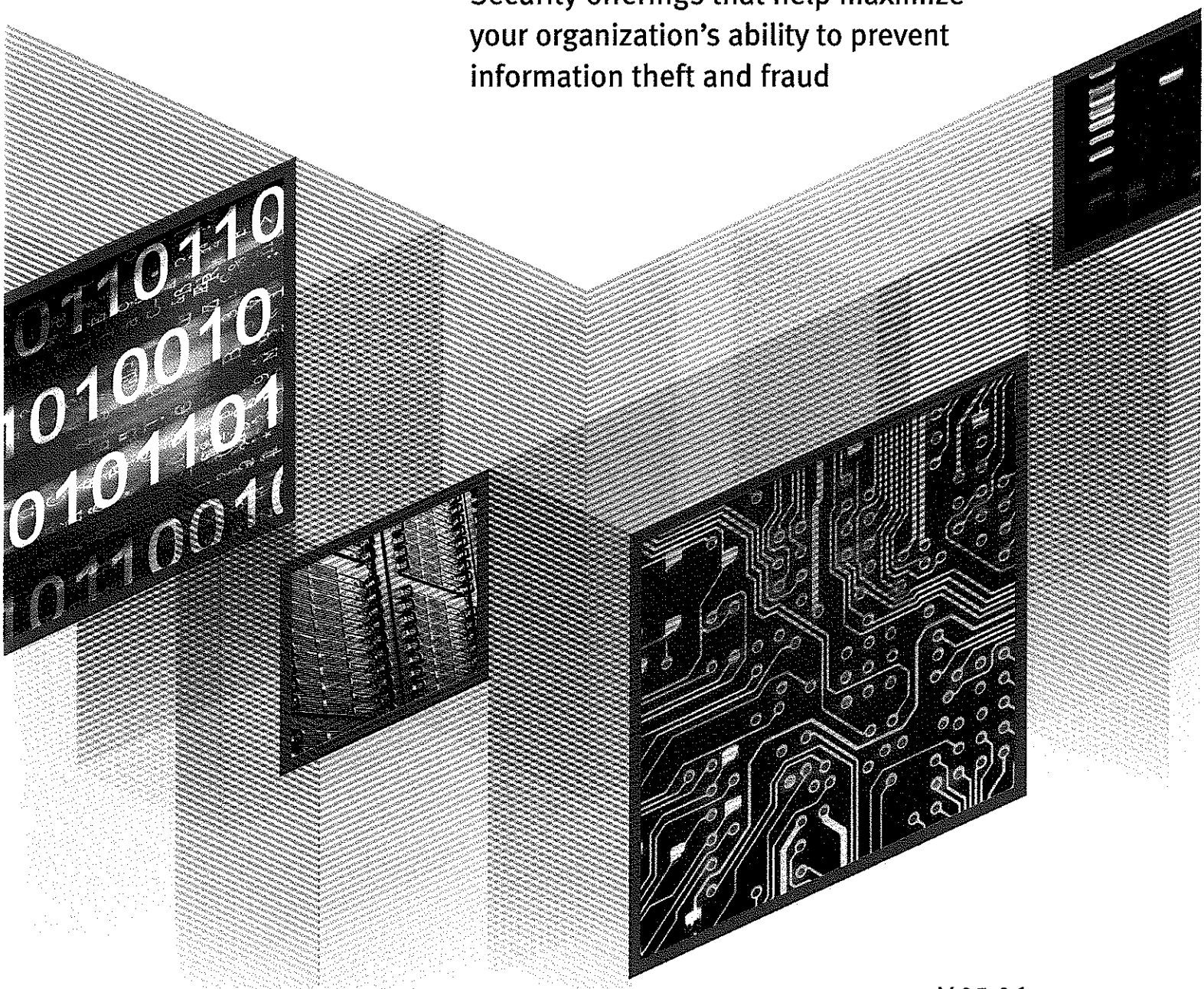
Canon

Canon Security Solutions

for the

imageRUNNER® Series imagePlatform Devices

Security offerings that help maximize your organization's ability to prevent information theft and fraud



V.05.06

The information contained in this document pertains to Canon's imagePlatform architected devices, known as the imageRUNNER line of digital multifunctional products. The information in this document is exclusive of imageRUNNER Segment One devices.

Your business produces, analyzes and processes information daily. Information is a company's most valuable asset and also the most vulnerable one. Information can be shaped into multiple forms: bits and bytes for network transfer and storage, printed documents, or materials for presentation. Because information can be presented in multiple ways and is found in various locations, it is extremely vulnerable to attacks including data corruption, theft, piracy, and destruction.

Most of today's enterprises have built a strong perimeter of firewalls, intrusion prevention systems, and anti-virus software to protect their digital assets. Attention is given to servers, network equipment, and user workstations, but networked printers and multifunctional digital copier devices have been largely ignored when it comes to security. With the advent of the MultiFunctional Printer (MFP), more and more functionalities have been integrated into one system, including scanning, copying, faxing, printing, and even Web access. These devices have become new targets for attackers, as they act as "information hubs," where data from various business units, departments, and users is processed, stored, and produced.

The value of this system to an intruder could be much higher than any other single system on the network. As networked printers and multifunctional systems complete the transformation from output terminal to true network node, businesses and IT professionals need to be just as concerned with data residing on – and passing through – MFP hard drives as they are with PC and network security.

Thus, corporate IT and security departments must include MFP devices as critical assets that require protection from internal and external threats. However, the knowledge needed to protect an MFP is much different than that needed to secure other types of network devices, such as file servers, databases, or routers. Many MFP devices run operating systems and offer hard disk drives to temporarily or permanently store data.

If information theft or virus insertion is the goal, it is easier and faster to penetrate a single MFP shared by an entire department than to target scores of individual computers. Internal security breaches of intellectual property and confidential information can be as damaging to your business as the theft of hard goods from the warehouse.

Once perceived as necessary only for government and military applications, security is now a growing requirement in the private sector as well. Consider the volumes of customer data and revenue forecasts that could be stolen from a company's sales/marketing database or the evidentiary information gathered by the legal department for a pending lawsuit or patent application. Imagine the impact on individual futures and careers should educational records be compromised or the financial impact of a competitor intercepting engineering designs and confidential product launch strategies.

The government has enacted several pieces of legislation – such as Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, and the Patriot Act – which are intended to protect confidential information. These regulations require organizations to constantly examine their networks and information workflows to make certain that they remain in compliance for records retention/destruction and threats against fraud. In addition, the organization must maintain the privacy of personal, financial, medical, and insurance data.

Government Legislation

The following table summarizes common information security items applicable to MFP devices, as required by current government regulations:

	Requirements	Threats	Potential Mitigation
Sarbanes-Oxley (SOX)	• Section 302 requires executives to certify the accuracy of corporate financial reports. • Section 404 requires executives and auditors to confirm the effectiveness of internal controls for financial reporting. • Section 409 requires any material changes in the financial state of the issuer to be communicated quickly and with supporting data to the public.	Unauthorized access to, or modification of, data; data fraud; data deletion; data availability	User authentication; access controls; encryption (storage and transmission); logging and auditing
Gramm-Leach-Bliley (GLBA)	GLBA has new privacy laws that regulate actions regarding confidential personal information that is collected. Data should be encrypted when in storage. Data in paper form needs to be secured and disposed of properly. Data should only be accessed on a need-to-know basis.	Unauthorized access to, or modification of, data; data fraud; data deletion	User authentication; access controls; encryption (storage and transmission); logging and auditing
Health Insurance Portability & Accountability Act (HIPAA)	Section 164. 312, Technical Safeguards, requires technical policies and procedures for access control on systems that maintain electronic protected health information (EPHI) to be implemented. Also, integrity controls and encryption should be implemented for data in transmission. Audit controls and person/entity authentication mechanisms should be established.	Unauthorized access to, or modification of, data; data fraud; data deletion; audit control	User authentication; access controls; encryption (storage and transmission); logging and auditing
California Information Practice Act CA SB 1386	Organizations must ensure that data privacy is protected and disclose any computer security breaches.	Unauthorized access to, or modification of, data; data fraud; data deletion; audit control	User authentication; access controls; encryption (storage and transmission); logging and auditing
Federal Information Security Management Act (FISMA)	• Sec. 3544 (a)(1)(A)(i) & Sec. 3547: The application should be protected against unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. • Sec. 3544. (a)(1)(A)(ii): Same requirements as the last section, but applies to a contractor of an agency or other organization on behalf of the agency. • Sec. 3544 (b): The application must be able to ensure the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets.	Unauthorized access to, or modification of, data; data fraud; data deletion; data availability	User authentication; access controls; encryption (storage and transmission); logging and auditing

From the summarized table, it is obvious that the mitigation mechanisms are all similar in implementation. More specifically, they are as follows:

1. User Authentication

Every user should establish his or her identity before accessing any resource. Authentication is the method used to verify that the user is who he or she claims to be. The most common authentication mechanisms include passwords, smartcards, and two-factor authentication, such as a combination of a password and card access.

2. Access Control

Every user's identity is associated with a role and privileges. These decide what the user can access and what actions the user can perform on a given resource. Access controls help protect resources from unauthorized access, modification, and deletion. Role-based access controls (RBAC) are the most common implementation of access controls.

3. Encryption

The confidentiality and integrity of data must be protected while it is in storage and during network transmission. Protection of data during transmission is commonly achieved through the use of encryption, including Secure Socket Layer (SSL), IPSEC, and algorithms such as 3DES, AES and RSA.

4. Logging and Auditing

Audit trails help system owners and auditors confirm that the implemented security mechanisms, such as authentication and access controls, network systems, and application logs, are implemented to serve this purpose.

To better understand the security features offered on Canon's imageRUNNER® Series devices, it is first useful to review the goals of information security: to keep data confidential, to maintain data integrity, and to make data available to legitimate users. Any product that hopes to provide security must achieve these three goals.

1. Confidentiality

Corporate data may contain information about the organization that should be kept confidential. The goal of confidentiality is to prevent the disclosure of data to unauthorized individuals.

2. Integrity

In addition to keeping data confidential, it must be kept accurate. Integrity assures that data is not altered, either accidentally or with malicious intent.

3. Availability

Confidentiality and integrity must be achieved while still making data accessible to legitimate users. Controls should be in place to prevent attackers from denying legitimate users access to data and resources.

CANON SECURITY SOLUTIONS

To help you meet your corporate security goals, Canon imageRUNNER devices may be equipped with a number of defense solutions that meet the highest standards for data confidentiality, integrity, and availability. From secure printing and document storage to sophisticated identity and device access management, you can trust Canon to deliver solutions that authenticate, encrypt, and preserve data and user histories. Canon's leading-edge security strategy maximizes your organization's ability to prevent information theft and fraud, while ensuring availability for authorized users.

- **System Architecture**

  Before a system is even deployed on a network, it should be properly secured to ensure that it will not introduce new vulnerabilities into the environment or become an easy target. The system should be easy to maintain as new threats emerge and the network evolves. The imageRUNNER device security functionality is implemented early in the design phase and was built as an integral part of the system.

- **Data Protection**

  Because data may be transmitted and often stored outside the realm of access controls, the confidentiality and integrity of data must be further protected with the use of encryption while it is in storage and during network transmission. The imageRUNNER device provides SSL for data in transmission and 3DES encryption for data in storage. Canon's Security Kit option provides the ability to encrypt and overwrite information as well as conceal Job Log data.

- **Authentication**

  On the network, the first step of protecting confidentiality and integrity is to ensure that users are who they say they are before they are allowed to access any data or resources. This is accomplished through the process of authentication. The imageRUNNER device provides various authentication mechanisms, including Department ID Management, Simple Device Log-in (SDL), and Single Sign-On (SSO) authentication. Canon's MEAP development platform allows for the creation of customized authentication applications. For example, end-users can utilize their company's smart card as a way to authenticate at the device.

- **Access Control**

  Once a user's identity is confirmed, that identity can be checked against access controls to determine the user's role and privileges as the next step in protecting information. The role and privileges decide what the user can access and what actions can be performed on a given resource. These access controls protect resources from unauthorized access, modification, and deletion. The imageRUNNER device includes various access controls, such as MAC/IP address filters, control cards, and digital watermarking.

- **Hard-Copy/Fax-Based Controls and Logging/Auditing**

  These features are also available on every imageRUNNER device.

These defense solutions are summarized in the table on the following page and are described in detail throughout the remainder of this document.

Summary of Canon Security Solutions and Protection to Meet Regulatory Compliance

Protection	Canon Security Solution
System Architecture	• imagePlatform controller architecture • UNIX-based proprietary operating system • Multifunctional Embedded Application Platform (MEAP®) • Controlled access to ports and services • Device Information Delivery Function (DIDF)
Data Protection	• Hard disk drive directory information is stored separately • Temporary and permanent data is written to random, non-contiguous locations on the hard disk drive • Security Kit option: -Hard Drive Data Encryption, 3DES -Hard Drive Data Overwrite -Job Log Conceal • Hard Disk Drive format • Removable Hard Disk Drive Kit option • Mail Box Backup capability • SSL • PDF Encryption option
Authentication	• Department ID Management • Control Card/Control Reader System Access option • Simple Device Log-In (SDL) • Single Sign-On (SSO) • System Administrator control
User/Network Access Controls	• MAC/IP Address Filter • Department ID Management • Control Card/Control Reader System Access option • Simple Device Log-In (SDL) • Single Sign-On (SSO) • System Administrator control • DIDF
Hard-Copy Controls	• Secured Print • Digital Watermark • Secure Watermark • Confidential Print
Fax-Based Controls	• Separation of fax and network functions • Job Forwarding • Memory Lock
Logging and Auditing	• Job Log Conceal (Security Kit option)

System Architecture

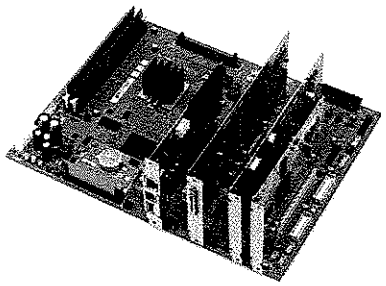
You Take Your Security Needs Seriously. Canon Does Too.

imagePlatform Controller and Operating System

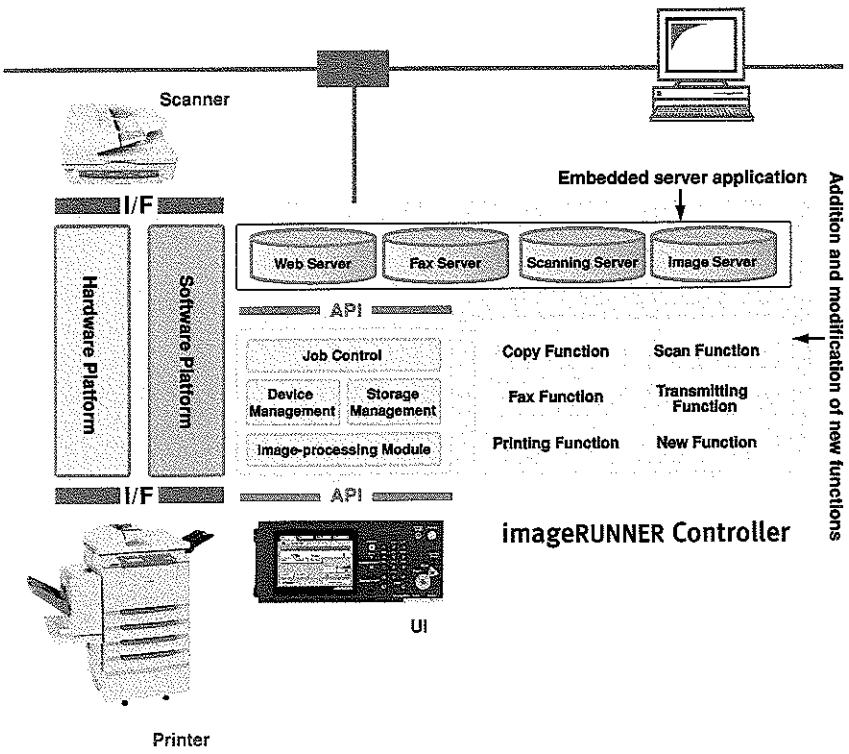
A corporate network will never be secure if the individual systems on the network are not protected against attack before they are deployed, and more importantly, maintained at that same level of security throughout their lifecycles.

Security starts here, with Canon's performance-driven common controller imagePlatform architecture. Canon's imagePlatform controller technology is the brains inside every imageRUNNER device. Its standardized foundation speeds the development and deployment of product enhancements and new functionalities across the entire product line, helping to reduce costs while increasing productivity.

Canon's imagePlatform controller architecture uses a UNIX-like, real-time operating system with source code expressly designed for Canon to run embedded applications for imageRUNNER device control. While powerful and adaptable by Canon, it is essentially a closed and proprietary operating system which is not widely distributed and, as such, is not a common target for hackers or viruses.



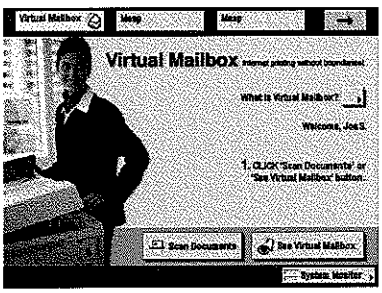
Canon's imagePlatform controller architecture is at the heart of every imageRUNNER device.



Multifunctional Embedded Application Platform (MEAP®)

Canon's MEAP architecture is based on the JAVA development platform. It provides a feature-rich environment to create applications that enable dynamic information flows to be embedded within imageRUNNER devices. The MEAP architecture allows customers to develop and install robust applications, including user authentication and device security.

Canon restricts access to the MEAP development platform and SDK, making the platform only available to approved developers. Furthermore, application integrity is assured by Canon, as all applications are encrypted and embedded with a digital signature and license. If the application is modified, the attached signature code will not match the original application and, as a result, will not run. In addition, a special key is required that prevents the application code from being accessed. Therefore, it is virtually impossible for anyone to alter a MEAP application or write a rogue application for an imageRUNNER device.



MEAP Application: Virtual Mailbox

Controlled Access to Ports and Services

At Canon, we understand that organizations have varied needs and security standards for remote user access and remote administration. That's why Canon has provided multiple options for accessing the imageRUNNER device across the network. Canon also understands that every open port and enabled service provides another potential path of attack on the system. For this reason, System Administrators have been provided with the ability to choose the remote access methods they want to use and have the option to disable the rest. The imageRUNNER device has been set up to support only the necessary protocols used for transferring data, which are restricted using a network application. Unauthorized access from the outside is blocked through IP-address-based connection restrictions. Network protocols, such as IPP, FTP, SNTP, SNMP, RAW, LPD, and others, can also be switched on or off at the administrator's discretion. Disabling unneeded services, protocols, and ports assists in hardening the device and securing the network by reducing potential intrusion points.

Wherever possible, Canon has implemented communication protocols in ways that reduce risk. For example, FTP (File Transfer Protocol) is commonly used in many multifunction devices to transfer, copy, and delete files, as well as connect to a remote computer. However, when implemented in the imagePlatform architecture, the FTP function is limited to printing only, thereby preventing unauthorized access to files stored on the imageRUNNER device's hard disk drive via FTP.

Device Information Delivery Function (DIDF)

Device Information Delivery Function (DIDF) allows the administrator to easily manage and maintain imageRUNNER devices over a network and ensure that these devices are configured in accordance with the company's security policy. The administrator sets one imageRUNNER device as the reference machine and the management data can be distributed and registered automatically to other specified imageRUNNER devices on the network. Data that can be managed includes the Address Book, Forwarding Settings, Favorites Keys, Department ID, and settings entered on the Additional Functions.

Data Protection

Hard Drive Data Protection

The imageRUNNER device has the ability to process image data for printing, scanning, faxing, and copying, which creates efficiency in your workflows. It is important to understand how data stored on the imageRUNNER device is protected.

Most multifunction products store image data on resident hard disk drives, just like the kind found on a personal computer. That data may be scanned images, incoming faxes, spooled print jobs stored temporarily, or files saved in local Mail Boxes for long-term archival and future print-on-demand needs. In addition, just like a PC, the file data remains accessible until that disk sector is overwritten. Without a security strategy in place, documents could be accessed from the unit's hard drive via a networked PC and reprinted. Consider the implications if the unit's hard drive were replaced or stolen, or if the imageRUNNER device were returned, redeployed, or disposed of before the data on the hard drive was removed – where is your data now? And how is your data being protected?

All data, both temporary and permanent, sent to a Canon imageRUNNER device is written in random, non-contiguous locations on the hard disk drive. Data stored on the hard disk drive of a black-and-white imageRUNNER device is compressed using the JBIG file format, and data stored on the hard drive of a color-enabled or business color imageRUNNER device is compressed using a proprietary JPEG format. Compressed data may only be read by an imageRUNNER device using a proprietary JBIG or JPEG format integral to the operating system, thus making stored data highly secure. The hard disk drive directory information for Business Color imageRUNNER devices is also stored on a separate system board, making file reconstruction infeasible in the event of hard disk drive removal. With Canon's Business Color imageRUNNER devices, directory information is located in SRAM on a controller board; on Canon's black-and-white imageRUNNER devices, directory information is located on the Hard Disk Drive and is transmitted to DRAM on the controller board at the time the device is powered on.

Volatility

Canon's controller for imageRUNNER devices consists of RAM and Hard Disk Drive for memory storage. Random Access memory (RAM) is short-term, volatile memory. Once the power is turned off, all information stored is erased and no longer stored in the device. Canon's imageRUNNER devices utilize volatile memory to store image data during the printing and copying process. When the imageRUNNER device is powered off, volatile memory is erased.

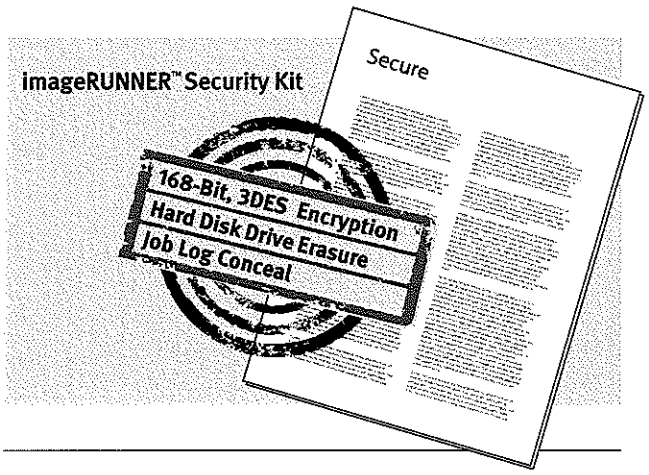
Canon's imageRUNNER devices utilize Hard Disk Drive memory to store system control data and user preference settings as well as system software, application software, driver software and customer data files. Hard Disk Drive memory supports long-term and short-term memory. Image data is temporarily stored on the hard drive for copy, print, fax, and scan functions and is erased after the transaction has been completed. Image data may also be permanently stored on the hard drive through the imageRUNNER device's Mail Box function. When image data is permanently stored on the hard disk drive, this date is retained even if the imageRUNNER device is powered off.

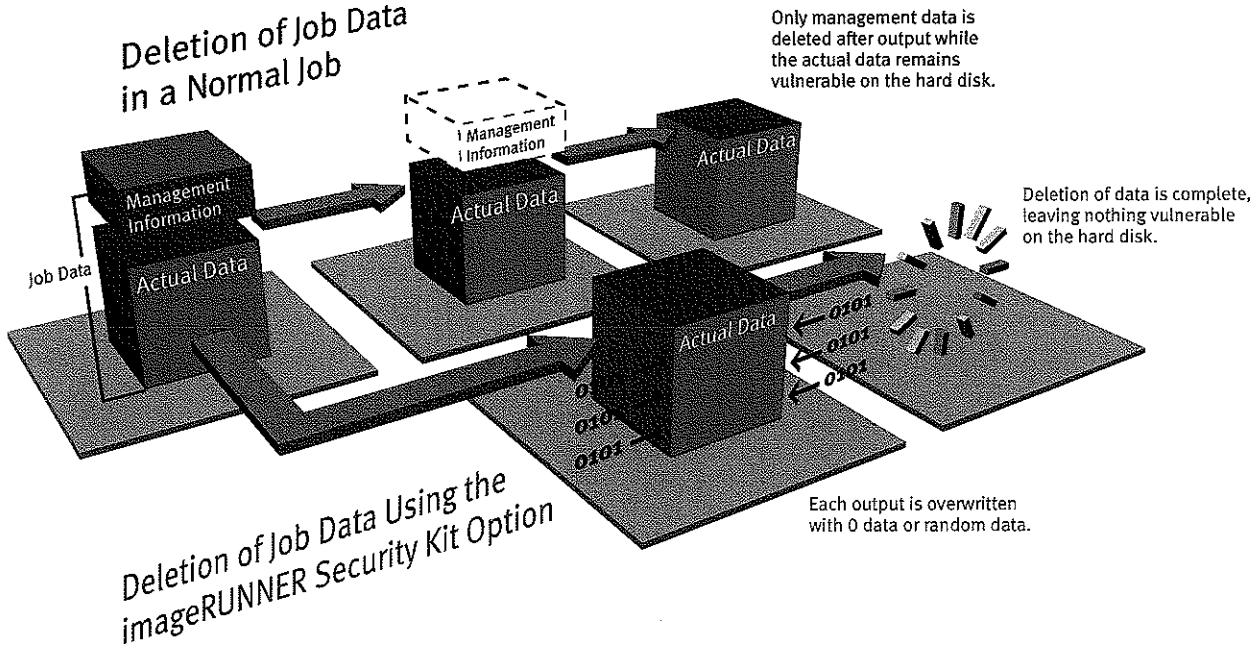
imageRUNNER Security Kit Option

Canon offers an optional imageRUNNER Security Kit to protect hard disk drive content. The centerpiece of Canon's data protection initiative, the Security Kit is a piece of software containing a set of utilities that allows you to encrypt all user data prior to storage on the hard disk and initiate the overwriting of the hard disk to completely erase previously stored data. When activated, the Security Kit delivers peace of mind for those in charge of managing sensitive information.

The Security Kit Includes:

- 168-Bit, 3DES Encryption
- Hard Disk Drive Overwrite Function
- Job Log Conceal





• 168-Bit, 3DES Data Encryption

Encryption on the hard drive is achieved by using a multi-step process to mitigate any risk of unauthorized disclosure. First, the imageRUNNER device uses mathematical algorithms to scramble bits of data. The data is then encrypted using 168-bit, 3DES encryption, making the intelligible reconstruction of files infeasible in the event the disk is removed. A secret key is created in the imageRUNNER device, which is stored in a separate system board. This secret key is used to encrypt all image data before writing to the HDD, providing protection for both temporary and permanent data such as documents stored in Mail Boxes. Finally, the data is stored in non-contiguous locations on the imageRUNNER device's hard drive.

• Hard Disk Drive Overwrite Function

On most systems that contain a hard drive, once a file is deleted or removed from temporary memory, it is still accessible until it is overwritten. An attacker with the right tools can easily reconstruct files that have been deleted or have passed through a temporary storage area on the system. For an MFP device, the risk is the same. Each document that is copied, scanned, printed, or faxed creates some amount of data in temporary storage. With Canon's Hard Disk Drive Overwrite function, the data created for each copy, print, scan, and fax job is overwritten and erased immediately after the job is completed; therefore, no trace of the information remains on the hard disk. Choose one of three erasure methods depending on the sensitivity of your documents and applications: overwrite once with null data, overwrite once with random data, and overwrite with random data three times for maximum security protection.

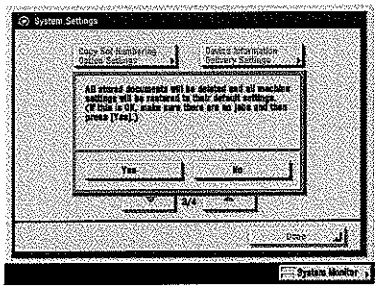
Overwriting prevents information to be retrieved by data, disk, or file recovery utilities. Overwriting is resistant to keystroke recovery attempts executed from standard input devices and from data hacker tools. The overwriting process includes not only the logical storage location of a file, but also includes all addressable locations. The security goal of overwriting is to replace written data with random data.

• Job Log Conceal Function

The same job history screen that offers traceability can also be concealed from unauthorized users to hide the list of completed jobs, aiding in regulatory compliance.

Hard Disk Drive Format

There may come a time when your imageRUNNER device will be redeployed, either within your organization or to another company, such as at the end of a lease. Best practices always recommend that systems be completely wiped before they leave the organization or even before they are redeployed within. The Hard Disk Drive Format feature, which is standard with all black-and-white imageRUNNER devices, completely erases all data stored on the hard disk, including files, job logs, Address Books, and user mode settings, in a single operation. This ensures that the imageRUNNER device's hard drive is wiped clean before being returned off lease, redeployed elsewhere in the organization, or disposed of, and eliminates concerns of violating your company's security policies.



Use the Hard Disk Drive Format administration's screen to initialize all data settings.

Removable Hard Disk Drive Kit Option

For an even greater level of security, the Removable Hard Disk Drive Kit Option allows for the physical removal of the disk from the main unit. This option provides another layer of data security for government agencies and corporate enterprises that need to ensure that data stored on the hard disk is physically secured when the unit is not in use. The Removable Hard Disk Drive Kit Option includes a case and key, allowing the hard drive to be easily removed for secure storage and easily replaced when needed. This option will be available in the second half of 2006.

Secure Socket Layer (SSL) Encryption

Many organizations are quite diligent about protecting data as it is transferred between PCs and servers or from one PC to another. However, when it comes to transmitting that same data to and from the MFP device, it is almost always sent in clear text. As a result, it may be possible to capture all the data as it is sent to the printer via the network. Canon can help mitigate this dilemma by providing Secure Socket Layer (SSL) encryption support for some transmissions to and from the imageRUNNER device. SSL can be applied for scan-to-email and Internet-fax (I-fax).

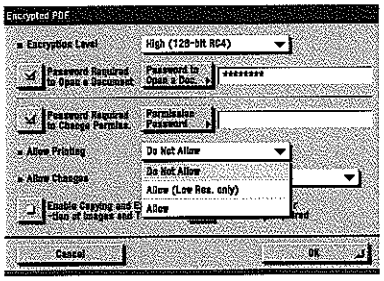
Scan and Send with SSL

Your imageRUNNER device is a communications hub, capable of connecting your business with high-speed information distribution capabilities through Canon's Universal Send™ technology. By leveraging the power of your existing data network infrastructure, you can scan and send TIFF, PDF, and JPEG files to any network destination—e-mail addresses, network servers, file folders, and Internet fax numbers. Even though scanned data is just passing through your MFP, data streams can be intercepted as they travel to their intended destinations. Fortunately, Canon offers several methods to shield files against falsification and theft.

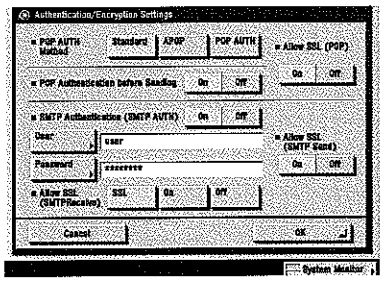
In addition to MAC and IP Address Filters, Canon imageRUNNER devices utilize SSL technology to encrypt the content of e-mails and I-faxes when sending to authorized destinations. SSL for scan and send provides transport layer security to ensure documents scanned on an imageRUNNER device are safely transmitted to the recipient.

PDF Encryption

In addition to SSL encryption for sending scanned documents, the imageRUNNER device also uses Adobe® standards to allow users to scan and send documents as encrypted PDF files. This is performed directly at an imageRUNNER device equipped with Universal Send, without the need for additional software. This provides a second layer of security beyond SSL encryption, and helps to ensure that documents are still secured once they reach their destination. By requiring a password to open the document or to print, change, or extract data, PDF Encryption gives businesses increased control over documents, even after they leave your hands. For even greater protection, the password itself can be encrypted to further restrict unauthorized users from viewing documents. Users may select either 40-bit or 128-bit encryption.



PDF Encryption Screen

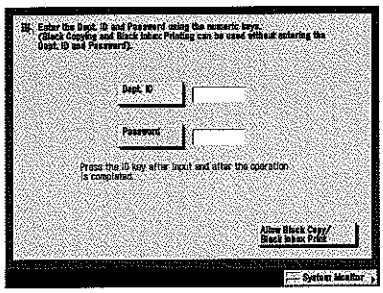


SSL/Authentication Setting (E-mail/I-fax)

Authentication

Authentication is the First Step Toward Regulatory Compliance

The proper identification and authentication of every user attempting to access a networked device is critical toward implementing a viable security system. Firms must have controls to restrict physical and virtual access to sensitive information. Depending on the size of your organization and the nature of your documents, Canon offers a number of user identity and tracking tools, ranging from basic to complex, ensuring that only authorized individuals can access system functions and data stored on your imageRUNNER device.



Department ID Management Screen

Department ID Management

On the more basic end of the scale, Department ID Management allows administrators to configure the imageRUNNER device with valid IDs and passwords for users. This embedded capability restricts system access and/or limits volumes to users, based on their assigned seven-digit ID and seven-digit password. Most imageRUNNER devices support up to 1,000 accounts and track usage by individual, department, or job. This gives administrators the ability to identify users, track job histories, limit volumes, and restrict access to system functions by individual. By registering a Department ID and password for each user, access to the device is limited to those who enter the correct Department ID and password.

Control Card/Card Reader System Option

The Control Card/Card Reader System option requires the use of intelligent cards that must be inserted in the system before granting access to functions. The card reader performs Department ID Management automatically. The optional Control Card/Card Reader system manages populations of up to 300 departments or users.

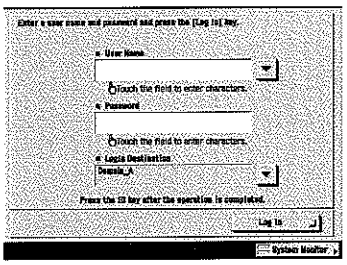
Authentication (Cont.)

Simple Device Log-In (SDL) Authentication

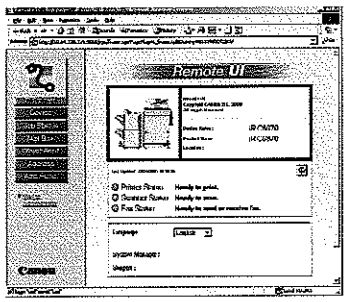
SDL is an enhanced version of Department ID Management that grants system access only after verifying an additional personal ID and password. When a user logs on to an imageRUNNER device via SDL, his/her e-mail address is automatically entered into the "From" field of any message sent from the machine. This provides not only authentication, but also non-repudiation. If data is sent from the imageRUNNER device, it can be traced back to the sender with a high degree of confidence.

Single Sign-On (SSO) Authentication

SSO is both easy to administrate and use for those in environments utilizing Active Directory. Enterprises with multiple MFPs and/or locations can use SSO to allow employees to access any imageRUNNER device on the network using the same ID and password as they use for their PCs and other networked data-sharing privileges. By utilizing SSO, the system administrator can track which users are logging onto each specific imageRUNNER device and the functions they are performing.



Single Sign-On Log-In Authentication Screen



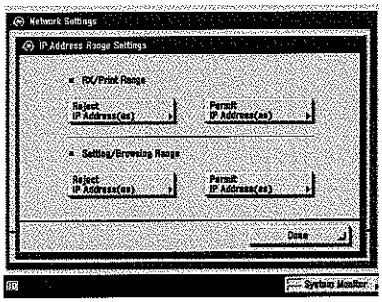
Canon's Remote User Interface Utility

System Administrator Control

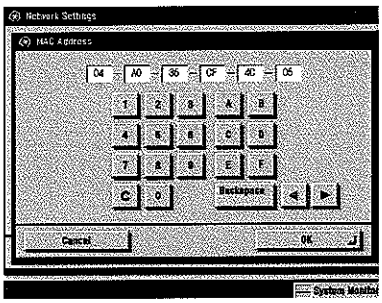
The System Administrator maintains complete remote control over device settings and end-user accessibility through the use of passwords. This can be accomplished at the device or remotely through Canon's Remote User Interface (RUI) utility, which allows device management and configuration from the desktop. Remote UI supports SSL encryption to protect data in transmission.

User-Based Access Controls

Once a user is authenticated, a secure system should determine what data and resources the user is allowed to access. Canon has applied the defense-in-depth principal to the imageRUNNER device so that even after access is granted to properly authenticated users, these people are limited in the actions they can undertake.



IP Address Range Settings Screen



MAC Address Settings Screen

Administrators can restrict access to individual functions by user, depending on network credentials. They can also limit which computers may communicate with the imageRUNNER device by enabling port filtering. In addition to preventing use of the system altogether, user-based access controls can be used to limit access to specific features and data stored on the imageRUNNER device.

Password Protection for Mail Boxes

Most imageRUNNER devices offer hard disk drives with a portion of capacity reserved for digital document storage in Mail Boxes. With the ability to store thousands of pages and files for archival, print-on-demand, or collaborative projects, Canon imageRUNNER devices serve as local document libraries as well as output devices. Documents created throughout the day can then be printed and collected in a single trip to the device to maintain privacy and efficiency. Documents intended for specific recipients remain under control with password protection. Administrators retain control of storage limitations to guard against access to files stored in unlocked Mail Boxes. Documents are stored on the internal hard disk drive until deleted, though administrators can also limit storage time of documents stored in Mail Boxes.

Network-Based Access Controls

In addition to user-based access controls, the imageRUNNER device also provides network-based access controls that can block specific systems and IP addresses from connecting to the device.

USB Block

USB Block allows the System Administrator to protect the imageRUNNER device against unauthorized access. This function may be set to permit or prevent the use of USB Device/Host Interface. System Administrators can use this function when connecting the device to a computer via a USB cable or when connecting a USB device to the imageRUNNER system. When the "Use USB Device" and "Use USB Host" modes are set to "off," USB Connections between the imageRUNNER device and a computer as well as the imageRUNNER device and a USB device are prohibited, preventing unauthorized access.

Destination Restriction Function

The following destination restriction functions are available with Canon's Universal Send Function: Address Book Registration Restriction, New Destination Instruction Restriction, and Address Book Access Restriction. Address Book Registration allows the System Administrator to restrict entries in the Address Book through the use of System Manager Settings. A password for Address Book Registration is set by the System Administrator and only that individual may register destinations in the Address Book, therefore restricting the list of "send" destinations to approved destinations only.

Data transmission to a new destination can be limited through the use of System Settings. This function prohibits transmissions to locations other than the destinations registered or permitted by the System Manager. Address Book Access Restriction restricts the imageRUNNER device to only display the destinations that are matched with the access numbers on the Address Book List by setting "System Settings/Address Book Restriction/Address Book Access Number Management (OFF/ON)" under the additional functions to "ON."

When you set the "Restrict New Address" to "ON," all the keys displayed in the new address under the "Send" feature are grayed out to prevent them from being selected.

IP Address Filter

The IP Address Filter on the imageRUNNER device performs a function common to many firewalls. Authorized IT personnel have the capability to permit or reject incoming packets from specific IP addresses. This allows you to restrict access to the imageRUNNER device for specific users or groups of users based on where they are on the network. For example, you could restart access to the finance department's imageRUNNER device in that department to help mitigate the risk of financial data being compromised. Likewise, you may not want your engineering department printing diagrams of your new product on an imageRUNNER device in an unsecured area. By blocking their IP addresses, you could force them to print to their imageRUNNER device in the secured engineering area.

Additionally, the imageRUNNER device also allows administrators to apply IP address filters for outbound connections as well. For example, for certain functions such as Remote Copy and Universal Send, administrators can block or restrict end-users from sending files to specific IP addresses. This can help minimize the risk of data falling into the wrong hands by being sent out of the company or to untrusted systems.

Media Access Control (MAC) Address Filter

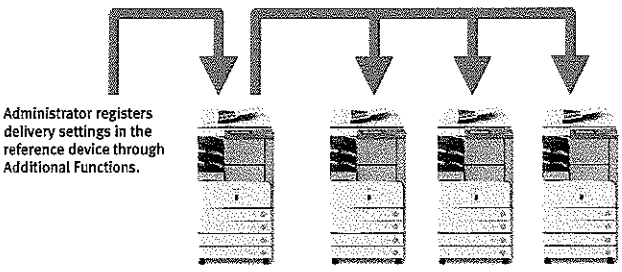
MAC address filtering is useful for smaller networks where administrators can manage controls for specific systems, regardless of the subnet to which they happen to be connected. For environments using Dynamic Host Configuration Protocol (DHCP) for IP address assignments, MAC address filtering can avoid issues that are caused when DHCP leases expire and a new IP address is issued to a system.

As with IP address filters, MAC address filters can be used to allow or deny access to specific addresses. Up to 100 MAC addresses can be registered and easily added, edited, or deleted from the UI. MAC address filters take a higher priority than the IP address filters, so necessary systems can be allowed or denied, even if the system's IP address would dictate otherwise. For example, a conference room may be on an IP address subnet that is denied access to the imageRUNNER device, but a trusted employee could have his/her laptop's MAC address added to the MAC address filters to enable access to the imageRUNNER device from that conference room as necessary.

Device Information Delivery Function (DIDF)

DIDF can be used to periodically broadcast security configuration settings from a single reference machine to hundreds of other imageRUNNER devices installed on the network for easy, consistent device management. DIDF ensures that all your imageRUNNER devices are identically configured and set up as intended, thus complying with your company's security policy.

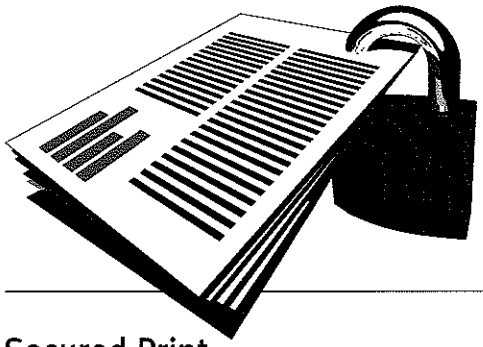
Device Information Delivery Function



Hard-Copy Controls

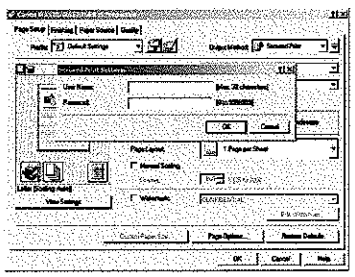
Despite all the difficulties of protecting information in its electronic soft-copy format, in many ways, that is a much easier task than protecting information in hard-copy format. For example, data in its electronic form can easily be encrypted when not in use and decrypted when needed. While network monitoring tools can watch for sensitive information leaving the network and block it or flag it for further investigation, hard-copy data cannot be protected in the same manner. It is very difficult to monitor the data that is leaving an organization in hardcopy format.

Canon imageRUNNER devices are equipped with a host of features and functions to minimize accidental disclosure of data to casual observers. From basic face-down output to secure printing, Canon protects your information with the following security technologies.

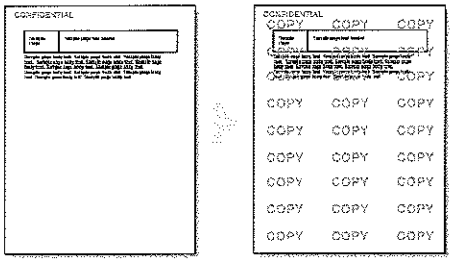


Secured Print

Secured Print is essentially a delayed, authenticated print feature that holds a print job in queue at the device until the user has authenticated at the imageRUNNER device. The imageRUNNER device requires the user to set a password in the print driver window when sending a print job from a connected PC. The imageRUNNER device will accept the job and hold the file in memory until the user arrives at the system and enters the correct password at the control panel. This ensures that the author is in close proximity when the document is printed.



Secured Print Screen



Document with embedded hidden text from the Secure Watermark

An unauthorized copy of a document with the Secure Watermark

Digital Watermarking

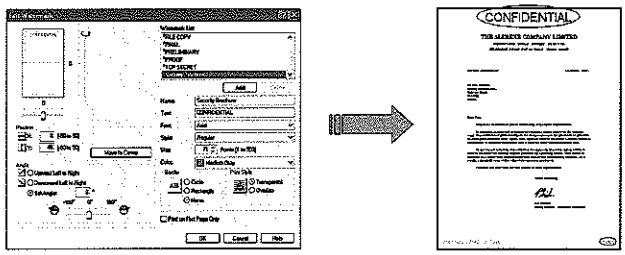
Used to embed the document's owner information in either its printed or digital form, this technology allows the owner to leave traces and prevent unauthorized copying of his or her document. Digital Watermarking works by inconspicuously embedding coded information in photographs and other works in digital form, much like the watermarks used in bank notes. The hidden watermark then becomes visible when the document is copied, which deters users from making unauthorized copies of sensitive or confidential documents.

Secure Watermark

Regain control over hard-copy document distribution and versioning with the optional Secure Watermark function. This enables the user to embed hidden text within the backgrounds of documents. The hidden watermark becomes visible only when the document is copied and deters users from reproducing sensitive or confidential documents.

Confidential Print

This feature places a five-digit serial number on all pages of every set when printing multiple copies of sensitive documents. This helps the document owner keep track of printed copies to ensure that when those copies are no longer needed, they can all be collected and accounted for before storage or destruction.



Canon's Fax Boards Have Firewall Protection

Many customers may be misinformed about the possibility of network penetration via the public switched telephone network (PSTN) used for voice and fax transmission. Select imageRUNNER devices may be equipped with a G3 fax board. To help prevent network penetration via the public switched telephone network, the imagePlatform architecture's firewall physically and logically separates the fax modem from network functions residing on the main controller board. The G3 fax board implementation connected to the public switched telephone network responds only to CCITT.T30 commands and does not support network communication protocols, preventing hackers from initiating a malicious network attack via the fax port on a Canon imageRUNNER device. Only G3 Fax protocol data can be exchanged; otherwise, the circuit is disconnected with a fax error code.

The imageRUNNER device's Fax Board does not come with a binary transfer function and, therefore, it is not possible to receive data files other than fax image files. In the very unlikely event that the fax board did receive a data file that "pretended" to be a fax image data file, the call would be disconnected and result in a fax code error.

Fax Forwarding

This function allows select imageRUNNER devices equipped with a fax board to forward inbound fax transmissions to specific recipients. This is done by setting predetermined conditions or storing faxes in a secure Memory Reception Inbox for later printing rather than permitting incoming messages to pile up in an open output tray.

Memory Lock

Documents received by select imageRUNNER devices equipped with a fax board may store incoming fax documents into a memory reception box until the recipient decides to print them.

Common Criteria Certification

Canon's Security Kit "B" Series has received Common Criteria Certification for government procurement.

Common Criteria

A product awarded Common Criteria Certification (CCC) means it has passed a rigorous government-sponsored inspection process for the safety and security of data entered, stored, displayed, or transmitted by networked devices. Also known as ISO 15408, Common Criteria Certification is a requirement for all hardware and software devices used by government agencies handling national security data. Although not mandatory in the private sector, systems that achieve CCC standards engender a higher level of confidence among IT professionals.

Conclusion

Awareness is the key to initiating your security process, while regulations are a means to enforce implementation of proper controls regarding data security. Security threats have emerged to target networked MFPs in the office. Your organization needs to implement a security solution that will protect your data from fraud, unauthorized access, modification, and deletion. Canon understands your security requirements and has developed a security solution that helps mitigate the risk to your data.

Even the most well conceived security plan is subject to some penetration threat through the variables of workflow, document distribution capability, and employee motivations. However, by utilizing the security features of a Canon imageRUNNER device, you can help to effectively align security with corporate goals, protect company assets, and try to achieve compliance with federal regulations.

From the imagePlatform controller architecture to digital watermarking, Canon keeps your data secure whether you are printing, scanning, e-mailing, faxing, or copying. Ask your Authorized Canon Dealer for more information about how imageRUNNER security solutions can achieve the confidentiality, data integrity, and availability of information across your organization.

Statements made in this document are the opinions of Canon U.S.A. None of these statements should be construed to customers or Canon U.S.A.'s dealers as legal advise, as Canon U.S.A does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, CASB 1386, FISMA, Check 21, or the US Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Canon

imageANYWARE

1-800-OK CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042

0059W472
0506-iRS-25M-DMC

PRINTED ON RECYCLED
PAPER IN THE U.S.A.