LANIER

Security Solutions

SOLUTION

Leadership in information security

Comprehensive and reliable solutions to protect sensitive information

Version 14

Don't underestimate the risks and costs of information theft

Information is your most valuable asset. By "information" we mean classified, confidential, or otherwise sensitive documents, anything from embassy floor plans to personnel reviews. The unauthorized collection of proprietary information, "economic espionage," accounts for losses in the range of $53 billion to $59 billion annually.[1] Whether generated within a government, business or private setting, there is the urgent need to implement effective strategies to protect information assets.

While digital technology has transformed business practices by enabling nearly instantaneous data exchange, it has brought with it some new challenges in terms of security. Specifically, those intent on undermining your interests can quickly and easily intercept information when it's in digital form. This risk can expose you to a diminished competitive advantage, possible litigation or eroding stockholder trust. Listed below are a few high-risk sectors:

High Risk Sectors	Information at Risk
Federal Government	National Security, Military and Trade Secrets
Financial	Mergers and Acquisitions, Stock Transactions
Pharmaceutical	Clinical Trials, Patent Applications, Quarterly Financial Results
General Office	Customer Lists, Executive Compensation, Restructuring Plans
High-tech	New Product Design (R&D), Intellectual Property
Laboratories	Test Methods, Research Reports
Law Firms	Briefs, Depositions, Contracts
Accounting	Audit Data, Financial Reports
Medical/Hospitals	Billing, Medical Records

Leadership in Information Security

Lanier, a leading provider of high-performance office technology, including color and black & white multifunctional products, printers, facsimile systems, scanners, duplicators and wide format systems — is dedicated to helping you address unique and varied security challenges as they emerge. By providing customized security options for our customers Lanier has developed a comprehensive suite of security solutions. These security solutions protect printed and electronic data content against opportunistic or targeted threats, both internal and external.

Assessing your vulnerabilities, establishing security objectives, and taking appropriate countermeasures will minimize the risk of potentially serious security breaches, and at the same time enable you to meet rigorous security compliance requirements.

[1] According to a study released in 2002 by the American Society of Industrial Security, U.S. Chamber of Commerce, and PricewaterhouseCoopers in a survey of Fortune 1000 corporations and 600 small to mid-sized U.S. companies.

This guide details Lanier Security Solutions that were designed to best meet your objectives when securing digital office systems. This multi-layered approach will effectively close the door on those that wish to exploit vulnerabilities. In fact, whether your Lanier systems are networked or non-networked, these fully integrated, cost-efficient solutions will guard against prevalent security breaches, without disruption to normal (authorized) document workflow.

Lanier Security Solutions Guide

Risk Level ▶	**LOW**			**HIGH**
Security Layer	**1**	**2**	**3**	**4**
Security Objective…	• Restrict Unauthorized Device Access • Control Device Output…	Plus… • Secure Network Devices • Secure Network Print Data • Destroy Latent Data…	Plus… • Physically Secure Data/Ports • Encrypt Web Communications • Authenticate Users…	Plus… • Monitor and Control Resources • Audit All Device Activity
Lanier Security Solutions	• User Codes • Locked Print • RAM-based Security	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • HDD Encryption • Data Encryption • DataOverwrite-Security System • Web Image Monitor • Web SmartDevice-Monitor	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • Data Encryption • DataOverwrite-Security System • Removable Hard Drive • Network Port Security • HDD Encryption • 128-bit Encryption over SSL/HTTPS • NT Authentication • Web Image Monitor • Web SmartDevice-Monitor	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • Data Encryption • DataOverwrite-Security System • Removable Hard Drive • Network Port Security • 128-bit Encryption over SSL/HTTPS • NT Authentication • Print Copy & Control • Web Image Monitor • Web SmartDevice-Monitor • HDD Encryption • IPv6 • Kerberos • Enhanced Locked Print • Print Copy Scan (PCS) Director • Card Authentication Package

Restrict Unauthorized Device Access

User Codes

User Codes (standard in most Lanier systems) enable system administrators to manage and track the use of Lanier digital output devices. A User Code can be assigned to an individual based on which function(s) they have permission to access. This level of control enables you to monitor system usage (e.g., generate print counter reports by function and User Code).

Control Device Output

Locked Print

Locked Print (available through Lanier's advanced print drivers) maintains confidentiality by suspending document printing until the authorized user (author/creator) enters the correct PIN (Personal Identification Number) from the device control panel. This eliminates the possibility of anyone viewing or removing a document from the paper tray. (Locked Print requires a hard drive that may be optional, depending on model.)

Locked Print Password Encryption

As a new feature the password used for locked printing can be encrypted to protect against wiretapping.

Enhanced Locked Print

Enhanced Locked Print lets you capture all the benefits of shared, centralized MFPs without compromising document security. Users store, release and manage confidential documents with the security of user ID and password authorization. It's a fast and simple solution for protecting your organization's confidential and proprietary data.

- Users can safely send documents to printers where they are securely held until released by the authorized user.
- Documents cannot be picked up at the printer by another user, protecting information confidentiality.
- Documents stored at the printer are encrypted (information cannot be compromised if hard drive is stolen).
- Enhanced Locked Print is installed to the Multifunctional-printing device either via embedded firmware (SD Card) or remotely via Web Interface.
- Administrators and users can configure Enhanced Locked Print through a simple web browser-based interface.

RAM-based Security

Select Lanier MFP systems use RAM (Random Access Memory) for document processing tasks as a copier, not a hard disk drive. Though a hard drive is available as an option, there is a security benefit to the base configuration in that jobs processed though RAM are volatile (i.e., when the system is turned off, data is immediately erased). Without a means to permanently store data, such as a hard drive, the security threat is eliminated. As such, these MFP systems can be proposed for low-volume environments where information security is the top priority.

Secure Network Devices

SmartDeviceMonitor (for Admin*)

SmartDeviceMonitor is utility software bundled with all Lanier printers, print-enabled MFPs and the Printer/Scanner Kit option. This versatile software suite simplifies all aspects of installation, monitoring and management of Lanier network output systems, while supporting key security features.

- **Change Community Name**
  To address SNMP (Simple Network Management Protocol) vulnerability, the system administrator can change the Community Name of Lanier hardware devices from "Public" to another more secure name. If this security measure is taken, the Community Name (for the software) must have the identical name as the connected Lanier output device.
- **Restrict User Access**
  System administrators can control user privileges through the User Management Tool. This activates a menu for review of the peripherals authorized for use by User Code and User Name. All Lanier supported peripherals on the network are listed, and a simple click on the device, accesses a menu that restricts or enables access to the device for individual users.

Web Image Monitor

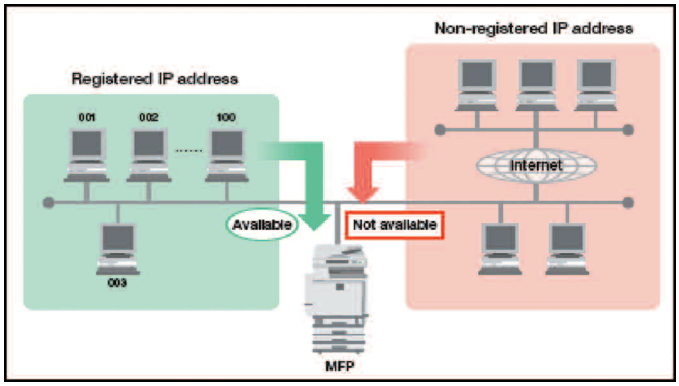
Web Image Monitor is an integrated Web-based utility for device management.

- **Set IP Address Range (IP Filtering)**
  System administrators can restrict authorized connections to the print controller from those hosts whose IP addresses fall into a particular IP range. Commands or jobs sent from non-authorized IP addresses are ignored by the print controller.
- **Network Port Security**
  The system administrator can enable or disable IP ports, thus controlling the different network services provided by the print controller to an individual user.

*Note: SmartDeviceMonitor for Admin resides on the client desktop and allows users to determine the status and availability of Lanier networked peripherals. Once installed, an icon is placed on each user's desktop in the Windows Taskbar, which shows system status at a glance.

IP (Internet Protocol) Address Filtering

In a LAN, an IP Address is each networked computer's unique hardware number. Just like your street address with a house or apartment number, these addresses help route e-mails and attachments, forward faxes to the proper recipient, and send print data to networked output devices from originating PCs. The ability of Lanier devices to block/restrict a particular end-user or set of end-users based on IP addresses improves the management of PCs and users, helps to balance output volumes among multiple devices, and enhances network security by limiting access to files stored in devices.

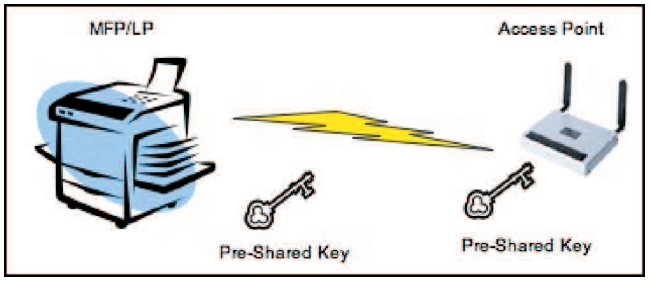


Job Logs/Access Logs

A complete listing of every job executed by the device is stored in memory. This list may be viewed via Web SmartDeviceMonitor to track and trace device usage by job and/or user. When used in conjunction with external user authentication modes, it will be possible to determine which specific users may be abusing a device. It is also possible to determine which device was used and by whom in tracing an unauthorized transmission.

WPA Support (Wi-Fi Protect Access)

Used in conjunction with the IEEE 802.11a/b/g Wireless LAN option, WPA is a security specification that addresses vulnerabilities in wireless communications. It provides a high level of assurance to enterprises, small businesses, and even home-based users that data will remain protected by allowing only authorized users to access their networks. "Personal" and "Enterprise" authentication and encryption features block intruders with wirelessly-enabled laptops from tapping into wireless networks in any environment, preventing the interception of data streams and passwords, or from using the wireless connection as an entry point into the customer data network.



802.1X Wired Authentication

802.1X provides Network-port based authentication for point-to-point communication between network devices and a LAN port. By providing a point-to-point connection to a LAN port, communication will terminate if the authentication fails.

Data Encryption

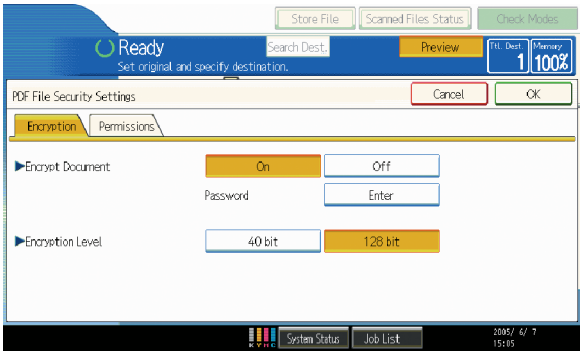
As mission critical data traverses the network it is possible for the knowledgeable hacker to intercept raw data streams, files, and passwords. The advent of wireless network technology, while increasing the convenience of surfing and printing for millions, also leaves networks vulnerable to attack from intruders armed with wireless laptops via any access points within range. Without protection, intelligible information can easily be stolen, or modified/falsified and re-inserted back into the network. Lanier devices are equipped with the following encryption capabilities to reduce these risks.

Address Book Encryption

Address Book Encryption protects contact information by encrypting the data stored in a system's address book. Even if the HDD is physically removed from the unit, the data cannot be read. This function eliminates the danger of a company's or department's entire population of employees, customers, or vendors being targeted for malicious e-mail messages or PC virus contamination. Further, since address book data usually corresponds to user names and passwords used elsewhere on the network, protecting printer/MFP address book data increases overall network security.

Encrypted PDF Transmission

Adobe's PDF file format has become the universal standard for creating documents that can easily be opened and shared by any user on any platform. Adobe provides the Acrobat® Reader® application as a free download across the Web. A PDF file is essentially a snapshot of a document. It is unchangeable (although files are editable with the full Adobe Acrobat application) and therefore attractive to document owners that wish to share, but restrict alterations, to approved documents. Part of the attraction of the PDF format is that file sizes are drastically reduced versus those of the native application, making them easier and faster to e-mail.



While Adobe offers a number of security-related features within the Acrobat application to lock and password-protect documents, there is nothing to prevent the files from being intercepted in a decipherable form while traveling over the network. That's where Lanier's Encrypted PDF Transmission function adds value, scrambling and encrypting the data that would otherwise be a very transparent document during transmission. Users may choose between 40-bit and 128-bit encryption, and set recipient rights to allow changes to or extract content from the document. (See also PDF Password Encryption.)

Hard Drive (HDD) Encryption

This function can encrypt the system's hard drive to protect against data theft. Even if the hard drive stolen, data will not be disclosed. The encryption methodology used is Advanced Encryption Standard (AES) to 256 bits.

Driver Encryption Key

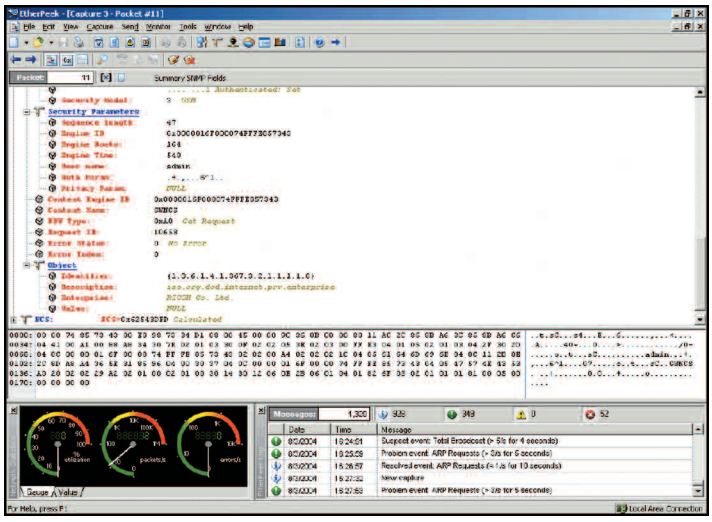
Lanier devices offer this feature that scrambles user authentication passwords when using the PCL or RPCS drivers so others cannot access the system fraudulently using a stolen user's password.

PDF Password Encryption

This function corrects a vulnerability in Encrypted PDF Transmission in that the window for entering the user password displays the password in clear text. This function encrypts passwords up to 32 characters for more secure PDF transmission and storage. The assignment of a group password for both the destination machine and connected PCs is done via DeskTopBinder Lite.

SNMP v3 Encrypted Communication

Simple Network Management Protocol version 3 (SNMP v3) is a network management standard widely used in TCP/IP environments. SNMP provides a method of managing network hosts such as printers, scanners, workstation or server computers, and groups bridges and hubs together into a "community" from a centrally-located computer running network management software. It allows administrators, for example, to make changes to device settings via SmartDeviceMonitor from a networked PC with encrypted communications to maintain a secure environment.



Earlier versions (v1 and v2) of SNMP were used to configure and monitor remote devices. The latest version, SNMP v3, offers enhancements to user authentication and data encryption that deliver greater security features to protect customer data and network assets. When activated, SNMP v3 prevents unauthorized users from seeing either the password and/or the actual content of the file in readable text form, protecting valuable information.

Kerberos

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by implementing secret-key cryptography. Many internet protocols do not provide any security for their passwords. Hackers employ programs called "sniffers" to extract passwords to gain access to networks. Sending an unencrypted password over a network is risky and can open the network to attack. Kerberos authentication helps to limit the risks caused by unencrypted passwords and keep networks more secure.

IPsec Communication

IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment. Organizations that require high levels of security have networks with IPsec for data protection. These organizations require printing using IPsec.

S/MIME for Scan to E-mail

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME (Multipurpose Internet Mail Extensions). MIME is an Internet Standard that extends the format of e-mail to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets.

This function is used to encrypt confidential data transmitted by Scan to E-mail for data protection against wiretapping.

Secure Network Print Data

Data Encryption via IPP

Another effective way to achieve data security is through encryption. Using Lanier's SmartDeviceMonitor for Client utility, print data can be encrypted by means of Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP), thus securing data between workstations and network printers/MFPs. (TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.) This means that any attempt to tap print data will fail, i.e., the intercepted data is indecipherable. Please see the included product specification charts for model support.

Destroy Latent Data

Lanier DataOverwriteSecurity System (DOSS):

To further thwart data loss, an organization's information security measures should incorporate technology that destroys latent digital images on the MFP's hard drive. Lanier's DataOverwriteSecurity System achieves that goal as it destroys temporary data stored on the MFP's hard drive by writing over the latent image with random sequences of "1's" and "0's."

- Lanier's three-pass random data overwrite process makes any effort to access and reconstruct stored print/copy files virtually impossible.
- Operates in conjunction with the Removable Hard Drive Security Systems, providing a multi-layered approach to securing sensitive documents.
- A simple display panel icon provides visual feedback regarding the overwrite process, e.g., completed or in-process.
- Conforms to National Security Agency (NSA) recommended methods of managing classified information.
- **Assists in compliance with HIPAA, GLBA and FERPA requirements.**
- DOSS Type A, B, C, D, F, H and I are ISO 15408 Certified to an EAL of 3.

Security Acts Compliance Requirements

By employing Lanier's DataOverwriteSecurity or Removable Hard Drive Systems, companies involved in the collection and dissemination of medical records, e.g., hospitals, healthcare organizations, and human resources protect patient privacy. Specifically, data regarding an individual's medical condition cannot be retrieved or stolen, thus assisting with necessary HIPAA-compliance requirements. **HIPAA (Health Insurance Portability and Accountability Act)** is a law designed to protect working Americans and their families from discrimination based on pre-existing medical conditions. In addition, Lanier's DOSS and RHD options also assists in compliance with financial privacy **(Gramm-Leach-Bliley Act)** and student privacy **(Family Education Rights Privacy Act)**.

Physically Secure Data/Ports

Removable Hard Drive Security (RHD) Systems

Convenient and easy to use, Lanier's Removable Hard Drive Systems interface with a digital system's standard hard drive. This solution secures the system's internal hard drive within an external rigid housing using a key lock system. A numbered labeling system ensures the Removable Hard Drive is easy to identify while in storage or when being replaced in the system. Also provided is a cushioned static-free case to protect the Removable Hard Drive while in transit or storage.

To provide even more security and flexibility when dealing with both classified and non-classified documents, an optional additional Removable Hard Drive is available. This allows Lanier digital systems to handle two separate interchangeable Removable Hard Drives; one RHD for classified documents and the other RHD for unclassified documents. After the classified documents have been copied or printed, the classified drive can be removed and placed in a secure location and the unclassified drive can be reinserted for unclassified copying or printing.

- The Removable Hard Drive is placed in a strategically accessible area for easy authorized removal and storage.
- Maximizes security by allowing the physical separation of data from the input/output device, preventing access to remnant data.
- Removable Hard Drive-enabled Lanier systems operate seamlessly with the device's robust copy, print and scan features.
- Operates in conjunction with Lanier's DataOverwriteSecurity System, providing a multi-layered approach to securing sensitive documents.
- All functions are available (copy, print, scan, fax and Document Server*) when the Removable Hard Drive is installed.

***Document Server**, a capability of select Lanier output systems that stores jobs (scan, print, fax, or copy) on the system's hard drive, also supports Secure Document Release.

Network Port Security

Typically, network-enabled systems are shipped to the customer with all the network ports "open," making the addition of these systems to different networks as easy as possible. Although making the network-enabled systems easy to install, opened unused network ports pose a security risk.

To provide enhanced network security, Administrators can disable a specific protocol such as SNMP or FTP using Web Image Monitor or SmartDeviceMonitor. This prevents the theft of user names and passwords, as well as eliminating outside threats including destruction/falsification of stored data, Denial of Service (DoS) attacks and viruses from entering the network via an unused printer or MFP port.

Encrypt Data Communication

128-bit Encryption over SSL

GlobalScan and DocumentMall both support 128-bit encryption over SSL (Secure Sockets Layer). SSL technology works by using a private key to encrypt data that's scanned from the Lanier MFP to the GlobalScan or DocumentMall server, creating a secure connection. Any URL (Uniform Resource Locator) that requires an SSL connection, such as GlobalScan and Document Mall, will start with https:, with "s" standing for "secure."

GlobalScan is a Web-based Content and Document Management Solution that enables select Lanier systems to perform network scanning functions, specifically, scan to e-mail or folder, as well as perform OCR, fax and document management functions via optional plug-ins. This powerful, yet easy-to-use, paper document capture and distribution system integrates seamlessly with your existing mail infrastructure to significantly boost workgroup productivity by combining scanning functionality within an accessible copier platform. **GlobalScan's enhanced security features include:** Secure LDAP, Secure SMTP, Kerberos Authentication and Password Protected PDF.

Authenticate Users

Prevent Unauthorized System Usage:

Authentication is an MFP security feature that restricts unauthorized users, or a group of users, from accessing system functions or changing machine settings. This important capability enables the system administrator to employ "Access Limitation Management," helping to protect your MFP installed base from unapproved usage or tampering.

DocumentMall, a low cost, low risk host application provides secure Internet access to your documents from anywhere in the world, 24 hours a day, 7 days a week, enabling easy sharing and collaboration across disperse geographic boundaries.

- **User Authentication** enables you to restrict machine access so that only those with a valid user name and password can access MFP functions.
- **Windows Authentication** verifies the identity of the MFP user by comparing login credentials (user name/password) against the database of authorized users on the Windows Network Server, thus granting or denying access to MFP functions.
- **LDAP Authentication** validates a user against the LDAP (Light-weight Directory Access Protocol) server, so only those with a valid user name/password can access your global address book, i.e., search and select e-mail addresses stored on the LDAP Server.
- **Administrator Authentication** – A registered administrator manages system settings and user access to MFP functions. Up to four Administrators can share the administrative tasks, enabling the workload to be spread and limit unauthorized operation by a single administrator, though the same individual can assume all roles. In addition, a separate Supervisor can be established for setting or changing the administrator passwords.
- **Basic Authentication** – Authenticates a user utilizing the user name/password registered locally in the MFP's Address Book. No one without a valid user name/password can access the machine.
- **User Code Authentication** – Utilizes Lanier's standard User Code system to authenticate the user. The MFP operator simply enters their User Code, which is compared to the registered data in the MFP's address book. No one without a valid User Code can access the machine.

  Basic Authentication and User Code Authentication can be utilized in non-Windows and/or non-networked office environments.
- **US Department of Defense Common Access Card (CAC) Authentication** – The Common Access Card (CAC) is a US DoD specialized ID card-based authentication system design to make Lanier MFP's compliant with the Homeland Security Presidential Directive -12 (HSPD-12). This Directive requires that all federal employees and contractors enhance security efficiently by reducing identity fraud through increased protection of personal privacy. The only customers for Lanier's CAC Authentication Solution is the U.S. Department of Defense (DoD) [US Army, Navy Air Force, Marines, Coast Guard and affiliated agencies]

Monitor and Control Resources

Print Copy Scan (PCS) Director

Print Copy Scan (PCS) Director is a comprehensive print management solution, which enables customers to analyze, understand and ultimately save on the costs associated with printing and photocopying. This solution can be implemented to silently monitor printing activity, limit the number of prints and copies a user can make, as well as enforce "rules based" printing methodologies to reduce Total Cost of Ownership.

Print Copy Scan (PCS) Director identifies and controls the cost of printing across the entire enterprise.

Audit All Device Activity

Lanier Print and Copy Control v3 for Equitrac Office and Express

Lanier Print and Copy Control enables customers to better control user access and track copy/print information via software embedded onto the hard disk drives of select Lanier output systems. Advantages include:

Secure Authentication Options

Protect sensitive data and prevent unauthorized use with the authentication method that fits your business.

- Ultimate simplicity and security. Employees access MFPs using their company ID badges and optional card readers that install in minutes. Lanier PCC accepts MIFARE®, Legic®, HID® Prox (125 KHz) and magnetic stripe cards.
- Convenient customized access. Easily track all document output using secure PIN access — by user, project or even workgroup.
- Instant company-wide access. Users simply input their existing network IDs and passwords to "unlock" MFPs.

User Friendly and Secure

- Convenient, secure printing. Follow-You™ document production lets you output documents from any network MFP so you can avoid busy or unavailable machines, or send multiple documents and print them as needed in different departments, floors or buildings.
- Timed control. Administrators can schedule automatic deletion of jobs from the server after a preset time limit.
- Strengthened security. Jobs reside on a secure server — not on system hard drives. Plus, fewer documents sit unattended in output bins since they're held until released by user.

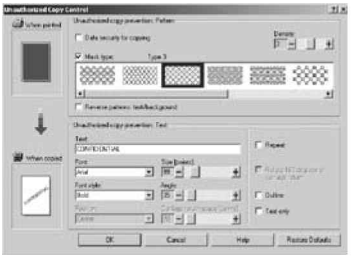
Unauthorized Copy Control

Lanier's innovative RPCS print driver supports a unique feature that no other manufacturer offers, Unauthorized Copy Control. What this feature does is embed patterns and text under printed text, eliminating the risk of unauthorized copying of sensitive documents.

This new functionality is ideal for smaller businesses that primarily use the system for fax, copy and print output, for instance, companies that copy personnel reports, compensation plans, medical records, financial reports, etc.

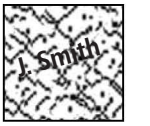
Unauthorized Copy Control consists of two functions:

1. Mask Type for Copying[2] is a standard RPCS feature that embeds a masking pattern and message within the original printout. If copies are made, either on the Lanier or competitive digital systems, the embedded message appears; the author's name, for instance, would help identify the originator.



Lanier RPCS Printer Driver

Masked Type for Copying



Data Security for Copying

2. Select Data Security for Copying[1] in the RPCS driver and all copy output that is made on a MFP equipped with the Copy Data Security Unit will be grayed out, leaving only a 0.16" (4mm) margin of masking pattern.

Notes:

[1] Requires optional Copy Data Security Unit. Not supported on some Fax-enabled configurations. Scanner feature must be deactivated on some Scan-enabled configurations. Copy reduction ratio less than 50% will be deactivated.

[2] Some digital MFPs may not detect masking patterns.

General Office *Commercial Facsimile Security Features*

Standalone Commercial Fax

Restricted Access

Restricted Access allows you to keep close track of machine usage and deters passers-by from using the machine. Authorized users must enter a code before they can use the machine. Furthermore, this function can be linked to the Night Timer feature so that Restricted Access is turned on/off at certain hours, preventing after-hours access.

Server Domain Authentication

When security and user tracking are an issue for IT Managers, Server Domain Authentication is standard on the LF416e and LF515e. Authentication limits access to the fax systems increasing security by monitoring machine usage. Machine access is given only to users with a Windows domain controller account. Server Authentication will limit access to the fax system not only for scan to e-mail, but also for standard faxing, IP faxing and LAN faxing.

Security PIN Code Protection

To prevent exposure of a PIN Code or Personal ID, any character after a certain position in the destination's dial number will be concealed both in the display and Communications Report.

Closed Network

With Closed Networks, the ID codes of the communicating machines are checked. If they are not identical, the communication is terminated, thus preventing possibly confidential documents from being transmitted intentionally or accidentally to the wrong location(s), i.e., outside the network. (Note: Closed Network requires all fax systems be Lanier systems with closed network capability.)

Confidential Transmission/Reception

This feature enables the user to transmit/receive to a mailbox that is passcode-protected. Messages are only printed after the recipient enters the proper passcode, providing an enhanced level of security when communicating between machines.

Memory Lock

When Memory Lock is enabled, documents from all senders (or specific senders) are retained in memory. When the Memory Lock ID is entered from the control panel, the documents print, another form of security that prevents documents from sitting on a receive tray for passers-by to read.

Networked Commercial Fax

ITU-T Sub-address Routing

Using a Sub-address, appended to a fax number, makes it possible to route a fax directly to the recipient's PC, via their e-mail address. When received to a PC, confidentiality is maintained, i.e., only the recipient can view the message.

IP-fax

Lanier Facsimile Systems, with NIC FAX Unit installed, support secure T.38 real-time IP-fax over a corporate Intranet, not only bypassing costly phone lines, but also operating securely behind the firewall.

Lanier Security Solutions Compatibility Chart

	Commercial Facsimile Security Features							
	Closed Network	Confidential Transmission/Reception	IP Fax	ITU-IT Sub-address Routing	Memory Lock	Restricted Access	Security PIN Code Protection	Server Domain Authentication
Super G3 Facsimile								
LF225m		■				■		
LF215m		■						
LF312	■	■			■	■	■	
LF412	■	■			■	■	■	
LF412e	■	■	■	■	■	■	■	■
LF510	■	■			■	■		
LF515e	■	■	■	■	■	■		■

ISO 27001 Information Security Statement

Lanier recognizes the importance of helping to protect the information assets of our business, our valued customers, our business partners, and our employees. We are therefore committed to develop, implement, and continually improve an Information Security Management System (ISMS) that identifies and protects the information assets of our business operations. In order to best satisfy our commitment to information security, Lanier has chosen ISO 27001 Certification.

ISO 27001:2005 is an international standard setting out the requirements for an Information Security Management System. It is designed to identify, manage, and minimize a wide range of threats to which information is regularly subjected. The Standard requires that processes and procedures are scripted to develop, identify and minimize or eliminate security risks that may affect information systems. All 'assets' (asset = anything of importance to Lanier) within scope are identified and protected using the evaluation criteria of 'Confidentiality, Integrity and Availability'… The 'Confidentiality' of all assets is assured. The 'Integrity', or accuracy, of our assets is safeguarded. And, the 'Availability', or accessibility, of our assets and systems to those who require them, is assured.

Note: The ISO 27001 International Standard sets out the requirements for Information Security Management Systems. It is supplemented by ISO/IEC 17799:2005 (Information Technology — Security techniques — Code of practice for information security management). The code of practice is a reference document which defines best practices for information security management, and is a direct outgrowth of the earlier British Standard BS 7799; in fact, the terms BS 7799 and ISO 17799 often are used interchangeably. The ISO 27001 Standard was published in 2005.

Lanier ISO 15408 Certification Statement

Security for customer networks, information and intellectual property is a main priority for Lanier. Keeping this in mind, Lanier is pleased to offer ISO 15408 Certification to support our customers' information security needs.

ISO 15408, also known as NIAP/Common Criteria Certification, is an international standard developed for IT security systems. Through this standard, security features and functions can be identified, tested, and then verified by an independent third-party testing organization. The certification provides vendors with government-recognized verification that their security claims are accurate.

Customers benefit from this certification by using it as a proof source for their information assurance/security plans. These information assurance/security plans are used to document that information is handled securely. Examples of how ISO 15408 certification can be useful is for Gramm Leach Bliley Act, HIPAA and US Government Security compliance requirements that require documented information security plans.

ISO 15408 Product Certifications

Lanier stands as an industry leader with a dynamic product line that is constantly being improved to meet our customers changing requirements. ISO 15408 Certification for Lanier products is a continuous process with ongoing certification updates and efforts. Therefore, the latest certification information may not be listed on this website. Please contact your Lanier sales professional for the most up-to-date information regarding ISO 15408 and ISO 27001 Certifications.

Lanier Security Solutions Compatibility Charts

	Network Protection			Device Access										Data Encryption										Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option
Color Multifunction																														
GX3000S	■	■				■																				■		■		
GX3000SF	■	■	■			■																				■		■		
GX3050SFN	■	■	■			■																				■				
SP C220S	■	■	■																							■				
SP C231SF/C232SF	■	■	■																					■		■				
LD215cg	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■					■	■		■		■		
LD520CL	■	■	■	■	■	■	■	■		■	■		■	■		■		■		■					■	■		■	■	■
LD520C/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD525C	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD420c	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■		
LD425c/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■		
LD430c	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■		
LD528C/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD533C/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD435c/LD445c	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■					■	■	■			■		
LD540C/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD550C/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LC425/LC430			■	■	■	■**	■	■				■	■	■				■					■***	■	■			■		
LC435/LC440			■	■	■	■**	■	■				■	■	■				■					■***	■	■			■		
LD160c*	■	■	■		■	■	■	■					■	■	■	■	■	■					■	■	■					
LC155*	■	■	■	■	■	■	■	■					■	■	■		■	■					■	■	■					
LD260c/LD275c	■	■	■	■		■	■	■		■		■	■	■	■		■	■	■	■	■	■	■	■	■				■	■
LD365C/LD375C	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
Pro C550EX/ C700EX****	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
Pro C900s	■	■	■	■	■	■	■	■					■	■	■		■		■	■			■							

** With the LD160c and LC155, these security features are only available when configured with Next Generation Architecture controller.*

*** With these products, only IP Address Filtering is available. MAC filtering is not available on these products.*

**** With the EFI versions, the DataOverwriteSecurity System feature is called Secure Erase.*

***** Note: The Pro C550EX/Pro C700EX and Fiery controllers have separate security features. The security features listed above are for the mainframe GW controller only. If the mainframe is configured with the Fiery, the Fiery's security features take precedence.*

	Network Protection			Device Access										Data Encryption										Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option
Color Multifunction (continued)																														
LD130C/LD130CSR/ LD140C/LD140CSR	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■					
LD630C/LD635C	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■					■
LD645C/LD655C	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■					■
LD620C/LD625C	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■				■	■

	Network Protection			Device Access									Data Encryption									Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option
Black & White Multifunction																													
AC016		■			■																				■				
AC017		■			■																				■				
AC122L		■	■		■																				■				
AC116n	■	■	■																						■				
AC230n		■	■		■																				■				
SP 3400SF/ SP 3410SF	■	■	■	■	■		■																■		■				
LP131SFL/LP131SF/ LP136SF	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■
LD015/F/SPF		■	■		■																				■				
LD016/F/SPF	■	■	■*	■*		■*		■*	■**				■*	■*	■*	■*	■*	■*								■			■	
LD117/F/SPF	■	■	■*	■*	■*	■*	■*	■*	■**	■*	■*		■*	■*	■*	■*	■*	■*	■*	■*	■*	■*	■*	■*	■*	■				
LD115		■	■		■																				■				
LD116		■	■		■																				■				
LD316/SPF	■	■	■*	■*		■*		■*	■**				■	■†	■*	■*	■*	■*										■		
LD118/d		■	■		■																				■				
LD120/d		■	■		■																				■				
LD320d/dSPF	■	■	■*	■*		■*		■*	■**				■	■†	■*	■*	■*	■*								■			■	
LD035/SP	■	■	■		■	■	■						■					■						■	■	■				
LD528SP/LD533SP	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
LD325/SP	■	■	■	■	■	■	■		■			■	■	■		■		■					■	■	■	■				
LD330/SP	■	■	■	■	■	■	■		■			■	■	■		■		■					■	■	■	■		■		
LD225/P/SP/ SPF/SPi	■	■	■	■	■	■	■	■					■	■	■	■	■	■					■	■	■	■		■		
LD230/P/SP/ SPF/SPi	■	■	■	■	■	■	■	■					■	■	■	■	■	■					■	■	■	■		■		
LD425B/LD425/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■	■	■	■	■	■			■	■
LD335/SP	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■

**Printer/Scanner Kit is required.* ***Printer/Scanner Kit and IEEE 802.11b required.*
†Printer/Scanner Kit or Fax Kit required.

	Network Protection			Device Access									Data Encryption									Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option
Black & White Multifunction (continued)																													
LD433B/LD433/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■	■	■	■	■	■			■	■
LD345/SP	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
LD255/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
LD265/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
LD275/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
LD260/LD270/ LD280	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
LD140SP/LD150SP	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			
LD040B/LD040/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
LD050B/LD050/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
LD360/LD370/ LD380/LD390	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD090	■	■	■		■	■																	■	■	■		■			
LD0105	■	■	■		■	■																	■	■	■		■			
Pro 906EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■
Pro 1106EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■
Pro 1356EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■
LD125	■[1]	■[1]	■[1]	■[1]		■[1]	■	■[1]	■[3]				■[1]	■[4]	■[1]	■[1]	■[1]	■[1]								■		■[1]	■	
LD125SPF	■	■	■	■		■	■	■	■[2]				■	■	■	■	■	■								■		■	■	
Pro 907EX/1107EX/ 1357EX	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
LD220F/LD220SPF	■	■	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[3]	■[1]	■[1]		■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■			■	■
SP 5200S/5210SF/ 5210SR	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■		■
SP 1200SF																										■				

[1]*Printer/Scanner Kit is required.* [2]*IEEE 802.11b required.* [3]*Printer/Scanner Kit and IEEE 802.11b required.*
[4]*Printer/Scanner Kit or Fax Kit required.*

	Network Protection			Device Access										Data Encryption										Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security
Color Printers																														
SP C220N/C221N/ C222DN	■	■	■																							■				
SP C231N/C232DN	■	■	■																							■				
SP C311N/C312DN	■	■	■																							■				
LP331cn	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■
LP331cn-KP HotSpot	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■
LP540C	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■
LP550C	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■
GX2500	■	■																								■				
GX3000*	■	■	■	■		■																				■		■		
GX e3300N*	■	■	■	■		■																				■		■		
GX3050N*	■	■	■	■		■																				■		■		
GX e3350N*	■	■	■	■		■																				■		■		
GX5050N*	■	■	■	■		■																				■		■		
GX e5550N*	■	■	■	■		■																				■				
GX7000	■	■																								■				
Pro C900	■	■	■	■	■	■	■	■					■	■	■		■		■	■			■							
LP137CN/LP142CN	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■	■				
SP C431DN-HS	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■					
SP C320DN	■	■	■	■		■	■	■	■	■	■		■	■				■		■	■	■	■	■		■				
GX e7700N	■	■	■	■		■																				■				
Pro C651EX/C751EX	■	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■		■		■					

GX3000/3050N/5050N does not use the same Web Image Monitor as the other Lanier printers. The browser is developed by Silex Technology and will be slightly different from the other models.

**The GX3000/GX e3300N/GX3050N/GX e3350N/GX5050N/GX e5550N support "IP address filtering" feature only.*
"Mac address filtering" is not supported.

Locked/Secure Print is only available if the Hard Disk is installed.

	Network Protection			Device Access										Data Encryption									Document Protection							
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security
Black & White Printers																													
SP 3300D/ SP 3300DN	■	■	■																						■				
LP131nL	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■
LP131n-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■
LP136n-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■
LP135n	■	■	■			■	■	■					■		■		■							■	■	■				
LP37N	■	■	■				■	■	■		■		■					■		■			■	■		■		■	■	■
SP 5100N	■	■	■			■	■	■					■		■		■									■				
LP150dn	■	■	■	■	■		■	■	■					■				■		■	■	■	■	■	■	■		■	■	■
LP235N	■	■	■	■	■	■			■																	■		■		
LP275hdn	■	■	■			■	■	■	■				■		■		■						■	■	■		■	■		
SP 5200DN	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■		■						■				
SP 5210DN	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■					
SP 1210N																										■				
SP 4310N	■	■	■		■		■	■	■		■		■	■			■	■		■	■		■	■		■		■	■	■

LANIER

SOLUTION

Security Solutions

Lanier Five Dedrick Place, West Caldwell, NJ 07006