Canon

VERSION 1.0 | UPDATED MAY 2024

NIST CYBERSECURITY WHITE PAPER FOR LAW FIRMS

Guidance for Canon Printer/Multifunction Device Functionality in Support of NIST SP 800-171 and NIST SP 800-172

Who should read this white paper?

Security administrators of organizations that handle sensitive information and the administrators in charge of the configuration and maintenance of Canon devices should read this paper.

This white paper describes how Canon devices (Canon printers/multifunction printers) can support users in protecting and managing sensitive information and how these devices can assist customers in their efforts to implement the NIST Cybersecurity Framework.

For those models herein referred to as “Canon devices,” see the following URL:
https://oip.manual.canon/USRMA-7492-zz-CSPS-enUS/

Canon Inc. and Canon U.S.A. may update the list of Canon devices and terms of this white paper from time to time, and so you should review the updates prior to implementing any recommended changes.

NOTE: *Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality and performance; you may want to test these settings in your environment. The authors and publishers of this content are not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the products and suggestions discussed in this white paper. Canon U.S.A. does not make any warranties concerning the accuracy or completeness of the opinions, data, and other information contained in this content and, as such, assumes no liability for any errors, omissions, or inaccuracies therein, or for an individual’s or organization’s reliance on such opinions, data, or other information.*

This white paper covers the following cybersecurity guidelines:

- NIST SP 800-171 **(National Institute of Standards & Technology Special Paper 800-171) “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”** sets security requirements for protecting Controlled Unclassified Information (CUI). Controlled Unclassified Information is defined as **data that “requires safeguarding or dissemination controls”** and includes more than 100 categories encompassing health information, student records, personnel records, research data, and more developed for government agencies.

- NIST SP 800-172 **(National Institute of Standards & Technology Special Paper 800-172) “Enhanced Security Requirements for Protecting Controlled Unclassified Information”** is a supplement to NIST SP 800-171 and focuses on enhanced security controls to build resilience against Advanced Persistent Threats (APTs). Advanced Persistent Threats are defined as those cyberattacks designed to gain access to an organizational network for a prolonged period of time to steal data. These guidelines define additional requirements for non-federal systems that manage, process, and store CUI.

Which security controls are covered in these NIST guidelines?

To meet the NIST guidelines established in NIST SP 800-171 and SP 800-172, a company or product must be compliant in 110 security controls across the following 14 categories:

- Access Control
- Audit & Accountability
- Awareness & Training
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System & Communications Protection
- System & Information Integrity

What is NIST?

The National Institute of Standards and Technology (NIST) is a non-regulatory U.S. government agency responsible for developing metrics, standards, and technology that fosters innovation and economic competitiveness within the science and technology fields. NIST is also responsible for producing standards and guidelines that help federal agencies meet Federal Information Security Management Act (FISMA) requirements. Finally, NIST helps organizations by promoting data security and cybersecurity best practices to protect their information and information systems through cost-effective programs.

What is the NIST Cybersecurity Framework?

The NIST CSF (Cybersecurity Framework) helps organizations manage cybersecurity risk by providing a common language and systematic methodology that complements existing risk management processes. This *Framework for Improving Critical Infrastructure Cybersecurity* is outcome-driven so that educational organizations can scale their activities based on what is economically or organizationally viable for their security environments and cybersecurity maturity.

What is Zero Trust Security?

Rooted in “never trust, always verify,” Zero Trust security is a strategic approach that requires users to continuously authenticate and validate at every stage of a digital transaction. Zero Trust security can be applied to software applications, endpoints such as multifunction printers, laptops, and other iOT devices as well as network infrastructure. Zero Trust processes are incorporated in effective cybersecurity models such as the NIST CSF.

What is the significance of NIST SP 800-171 and NIST SP 800-172?

The requirements in these two documents help any organization that processes, stores, and/or transmits CUI to identify best practices for protecting information such as legal documents, health records, financial information, and more. These requirements can also help legal organizations identify contractors that can offer security features to help users safeguard CUI. This has become the benchmark for all types of organizations seeking to implement cybersecurity best practices.

For more information about Canon devices, contact your Canon authorized representative.

SOURCE: nist.gov

Contents

1 Preface: NIST CSF for Law Firms

As the frequency and breadth of cyberattacks grows, every organization must prioritize:

- Management and protection of important information within their systems
- Implementation of measures to counter cybersecurity risks (such as unauthorized access and disclosure of confidential data)

To help do this, legal entities—including law firms, corporate law offices, and government bodies as well as businesses in every industry—can turn to established frameworks for guidance. The **National Institute of Standards and Technology Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)** was developed by the U.S. Department of Commerce to be used across industries. This framework provides tools and a methodology for evaluating products, managing cybersecurity risk, and identifying measures to protect data at rest and in transit. The NIST CSF may be especially relevant in the legal space for the following reasons:

The NIST Cybersecurity Framework (CSF) lays out a roadmap for identifying cybersecurity risks, helping to detect a security breach, responding to a cybersecurity incident, and restoring access to information that may have been compromised. It is used by businesses of all sizes, and many organizations may ask that their third-party vendors also adopt the framework to mitigate risk to sensitive shared information.

The NIST CSF provides law firms and corporations with a security playbook designed to identify potential security weaknesses and a methodical process to allocate resources where they are most needed while simplifying the compliance and security audit processes. **Employing this valuable tool may help protect IT systems and assist in meeting the demands of privacy and data security regulations.**

As legal entities grapple with compliance and regulatory requirements in hybrid and remote working environments, establishing a process of continuous evaluation and improvement for internal and external data management is more important than ever.

Canon strives to assist corporations and law firms to gain a better understanding of how Canon devices can help support their cybersecurity initiatives. **Canon device features can support specific NIST guidelines (NIST SP 800-171 and SP 800-172) focused on helping to protect confidential case file information and other forms of Controlled Unclassified Information (CUI) for government-level organizations and associated businesses.**

This white paper outlines how certain features of Canon devices can help support legal organizations in meeting rigorous standards with detailed information about recommended settings for standard and optional features. **"Additional Compatibility Charts"** in the Appendix describe the requirements in further detail plus how those requirements relate to the functions of Canon devices. The charts also provide examples of measures you can implement at your organization.

2 Cybersecurity Measures of Canon Devices

Printers/multifunction devices connect to the network of systems at organizations and handle important information such as document data. Therefore, printers/multifunction devices require the same security measures as other information devices. Canon devices provide functions for responding to the five elements required for cybersecurity, which are “Identify,” “Protect,” “Detect,” “Respond,” and “Recover.” These five elements are defined as framework core functions in the NIST CSF. By comprehensively implementing measures for these five functions, you can not only protect your organization from cybersecurity risks, but also swiftly discover them and recover from them. As cyber attacks have become more sophisticated, the importance of the “Detect,” “Respond,” and “Recover” functions has increased, and Canon devices have enhanced the measures they provide for those functions.

The next section uses the five framework core functions of the NIST CSF to describe the security functions provided by Canon devices that are effective for cybersecurity measures.

The Five Framework Core Functions

Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

2.1 Identify/Protect

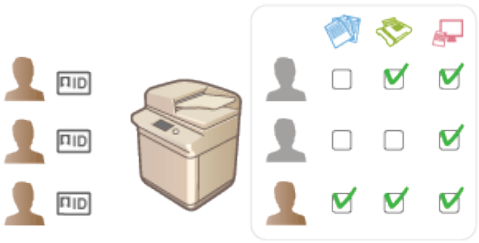
- **User Authentication/Access Control**
  Canon devices provide administrators with various authentication options for ensuring that only authorized users can use the machine and its functions (such as the print, copy, scan, and send functions).

Log-in Service (User Authentication)

The log-in service (User Authentication) performs personal authentication based on the information registered for each user, enabling you to limit the users who can access the Canon device. You can additionally specify an Active Directory or LDAP server on the network as an authentication server to utilize the existing user information registered on the server. Canon devices also support user authentication using IC cards, which you can use with a PIN to achieve multifactor authentication.

ACCESS MANAGEMENT SYSTEM

You can assign the functions available for each privilege level (role) and create new roles. This enables you to perform more detailed user management, such as “prohibit user A from making copies” or “allow user B to use all machine functions.”



Advanced Box Authentication Management

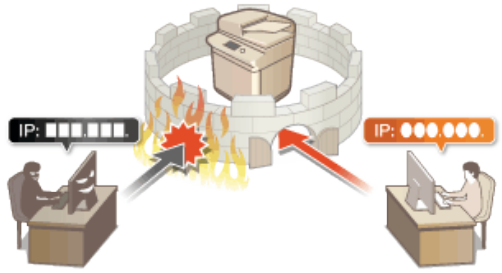
The storage of Canon devices contains a shared space called the “Advanced Box.” You can disclose the Advanced Box on the same network as a Canon device using the SMB or WebDAV protocol. You can prevent unauthorized access by setting Canon devices to perform authentication when you disclose the Advanced Box.

➤ Network Authentication/Access Control

Actions of malicious third parties, such as eavesdropping, tampering, and spoofing during communication may cause unexpected damage to authorized users. Canon devices provide various measures for increasing network security to protect important data and information.

Firewall Settings

You can configure the firewall settings of a Canon device to prevent unauthorized access by third parties, as well as network attacks and intrusions, by only allowing communication with devices that have a specific IP address.

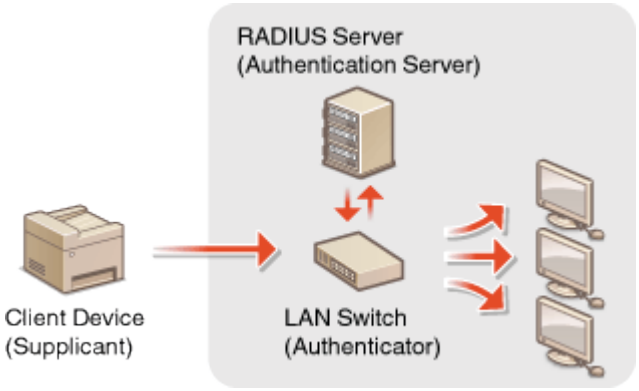


Proxy Settings

You can configure the proxy settings to enable a Canon device to connect to outside networks via a proxy server when viewing websites. The proxy server function improves security when viewing websites.

IEEE 802.1X Authentication

Canon devices can connect to networks that have adopted IEEE 802.1X as a client. By adopting IEEE 802.1X, you can block communication requests from unauthorized devices.



➤ Data Security

Canon devices use industry-standard algorithms to securely protect data that's saved to the internal storage and data that's sent via a network. The function for encrypting data on storage and networks uses an encryption module that complies with FIPS 140.*

Storage Data Encryption

The storage of Canon devices contains files in the Advanced Box and Mail Box, registered information in the Address Book, undeleted job data, and password information. Canon devices encrypt the above data to prevent the information from being accessed without authorization.

* FIPS (Federal Information Processing Standards) 140: Computer security standards defined by the United States government that specify requirements for cryptography modules.

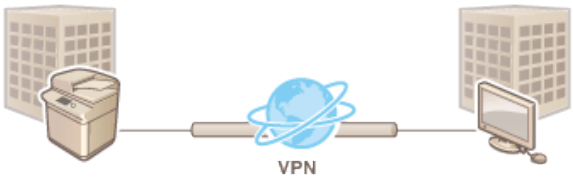
TPM (Trusted Platform Module)
Canon devices include a TPM chip for securely managing confidential information. The encryption key protected by the TPM chip encrypts the following confidential information in Canon device:

- Passwords
- Public key pairs for TLS communication
- User certificates

The TPM enables you to prevent the leak of confidential information due to physical analysis or unauthorized access to the Canon device.

TLS Encrypted Communication (Network Data Encryption)
You can use TLS encrypted communication to prevent actions such as eavesdropping, tampering, and spoofing when accessing the printer/multifunction device from a computer or other device to exchange data.

IPSec Communication (Network Data Encryption)
While TLS only encrypts data used on a specific application, such as a Web browser or an email application, IPSec encrypts the whole (or payloads of) IP packets. This enables IPSec to offer a more versatile security system than TLS.



In addition, Canon devices enable you to protect document data by setting conditions for limiting the use of the following functions:

- those that may lead to information leaks regardless of user's intention
- those that may be abused by a user with malicious intent

Forced Hold Printing
The administrator can change the settings to store documents in Canon devices without printing them in order to avoid cases such as:

- Users leaving printed materials on the machine, which are then taken away by another person
- Accidental leaks of information
- Misprints

Stored document data is associated with users and groups to help prevent unauthorized printing.

Restricting the Use of Memory Media

Although memory media such as USB drives provide convenience, they can also be a source of information leakage if they're not properly managed. You can prohibit the use of memory media so that a user cannot save scanned documents on memory media or print data saved on memory media.

2.2 Detect/Respond/Recover

➤ **Security Monitoring**

Cybersecurity measures are required to monitor system operation, and detect, track, and respond to events that may affect systems or the organization. Canon devices provide a log function for monitoring the use of the device. You can use logs to check/analyze how the device is used.

Audit Log Function

You can use the audit log function to monitor security events. For example, you can perform the following auditing:

- Monitoring the user authentication log for unauthorized access (or attempted access) to the device
- Monitoring the device usage logs for unauthorized printing, sending, or changing of administrator settings

By linking with a SIEM* system, you can also collect/analyze logs and send notifications on security incidents.

➤ **Cyber Resilience**

Cyber resilience is the act of preparing to detect attacks and swiftly restore systems to their original state to minimize the damage of a cyber attack.

Cyber resilience requires measures from three perspectives:

- Detecting cyber attacks
- Responding to detected cyber attacks
- Restoring systems from the damage of cyber attacks

Canon devices provide functions for these cyber resilience measures.

* SIEM (Security Information and Event Management): A system for detecting security incidents by collecting, managing, and analyzing the logs of software and devices in systems.

Verify System at Startup/Protect Runtime System

As a solution for verifying system integrity, Canon devices provide the following functions:

- The Verify System at Startup function that verifies the system during startup
- The Protect Runtime System function that monitors software changes at runtime to prevent unauthorized changes

These functions enable you to constantly monitor the system for the intrusion of malicious code. The Protect Runtime System function incorporates McAfee Embedded Control technology as a countermeasure for malware. This technology uses an allow list (whitelist) to perform the following:

- Allowing only trusted applications to run in the system
- Preventing unauthorized system changes

Preventing Firmware/Application Tampering

Canon devices verify digital signatures when the firmware is updated or an application is installed. This function enables you to prevent unauthorized programs from being installed on the devices.

Backing Up/Restoring Data

This function enables administrators to back up and restore the data and settings of Canon devices.

The functions introduced in this white paper are only a sample of the security measures provided by Canon devices. Canon devices have various other security functions that you can flexibly customize according to your environment. For details, see the Canon website.

3 Functionality in Support of Cyber Security Guidelines

This section describes how the cybersecurity measures of Canon devices respond to the security requirements defined in cybersecurity guidelines. This white paper covers the following cybersecurity guidelines:

- NIST SP 800-171
- NIST SP 800-172

3.1 Cyber Security Guidelines

3.1.1 NIST SP 800-171

NIST SP 800-171 adopts the recommended requirements for non-federal information systems that share important information, from the following regulations:

- FIPS (Federal Information Processing Standards) PUB 200, “Minimum Security Requirements for Federal Information and Information Systems”
- NIST SP 800-53, “Security and Privacy Controls for Information Systems and Organizations”

These regulations define the requirements regarding the processing, saving, and transferring of important information. (The information systems of United States government agencies are obligated to comply with the above regulations.) Therefore, complying with NIST SP 800-171 enables you to maintain a protection level equivalent to information systems at government agencies for system elements that process, save, or transfer important information. Organizations that conduct business with government bodies such as the United States Department of Defense and Japanese Ministry of Defense must comply with NIST SP 800-171.

NIST SP 800-171 defines 110 security requirements for protecting important information, which are categorized into 14 families. Each family includes requirements related to the general security topics of that family. Security requirements are divided into “Basic Security Requirements” and “Derived Security Requirements.” Derived Security Requirements supplement the Basic Security Requirements and required for responding to the Basic Security Requirements.

Secruity Requirement Family

Family	Description
ACCESS CONTROL	Limiting the users and devices that can access systems
AWARENESS AND TRAINING	Providing the members of the organization with education and training on security
AUDIT AND ACCOUNTABILITY	Auditing systems, tracking audit information, and maintaining accountability
CONFIGURATION MANAGEMENT	Establishing and managing system configuration standards
IDENTIFICATION AND AUTHENTICATION	Identifying and authenticating the users and devices that use systems
INCIDENT RESPONSE	Tracking and reporting incidents
MAINTENANCE	Performing system maintenance
MEDIA PROTECTION	Protecting important information on media and limiting access to important information
PERSONAL SECURITY	Screening the individuals that can access systems
PHYSICAL PROTECTION	Limiting physical access to systems
RISK ASSESSMENT	Assessing the risks faced by systems
SECURITY ASSESSMENT	Assessing the security management measures of the organization
SYSTEM AND COMMUNICATIONS PROTECTION	Monitoring, controlling, and protecting the communication at system boundaries
SYSTEM AND INFORMATION INTEGRITY	Ensuring the integrity of systems and information

3.1.2 NIST SP 800-171

NIST SP 800-172 has been created as a supplement to NIST SP 800-171. NIST SP 800-172 defines enhanced security requirements to help protect important information from APTs (Advanced Persistent Threat). APT is an advanced type of targeted attack. The standard was published in February 2021.

NIST SP 800-172 defines APT countermeasures via a multidimensional (defense-in-depth) protection strategy comprised of the three strategies described below (PRA, DLO, and CRS).

The requirements of NIST SP 800-172 are for implementing one or more PRA, DLO, or CRS strategies. NIST SP 800-171 is a basic cybersecurity guideline, while NIST SP 800-172 enables you to establish multidimensional (defense-in-depth) protection strategy. By responding to both of the guidelines, it is expected that you can minimize the impact of APTs when there is an unauthorized intrusion into a system in your organization.

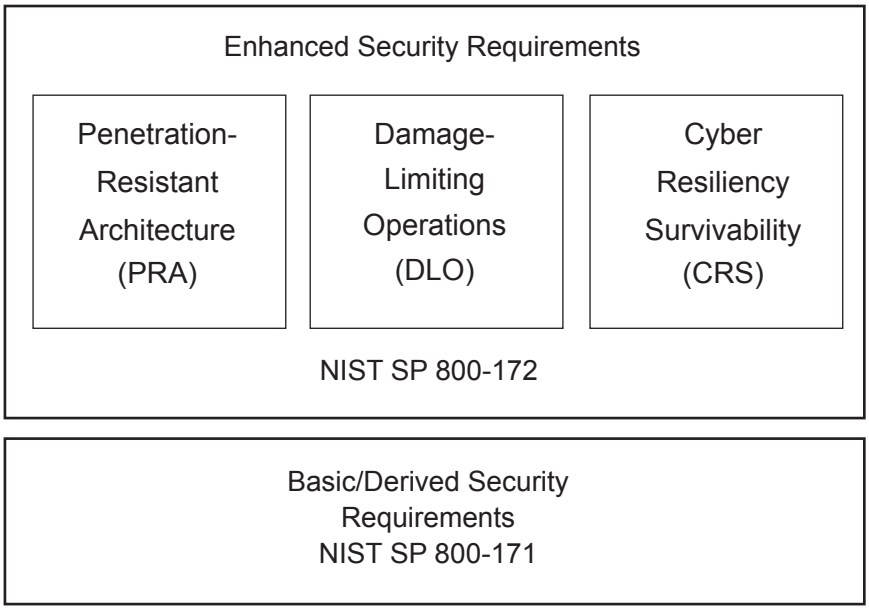
The countermeasures perform the following:

- Minimize the impact of (damages caused by) the intrusion
- Swiftly recover the system

PRA (Penetration-Resistant Architecture)
An architecture that uses technology and procedures to limit the opportunities for an adversary to compromise an organizational system and to achieve a persistent presence in the system.

DLO (Damage-Limiting Operations)
Procedural and operational measures that use system capabilities to maximize the ability of an organization to detect successful system compromises by an adversary and to limit the effects of such compromises (both detected and undetected).

CRS (Cyber Resiliency Survivability)
Designing systems, missions, and business functions to provide the capability to prepare for, withstand, recover from, and adapt to compromises of cyber resources to maximize mission or business operations.



NIST SP 800-172 is comprised of the same 14 families as NIST SP 800-171 and defines 35 security requirements.

3.2 Canon Printer/Multifunction Printer Functionality in Support of Cybersecurity Guidelines

This section describes how you should operate Canon devices and the kind of security measures that Canon devices provide for responding to cybersecurity guidelines. These guidelines define requirements for organizations that manage important information and do not define requirements for specific products and their functions. Therefore, in order to check how to respond to these guidelines, we extracted the requirements related to Canon devices from the requirements of each guideline. Then, we checked how the functions of Canon devices can be utilized to protect important information in response to the extracted requirements. We also checked the settings of devices required for correctly utilizing the functions of Canon devices.

The table below shows the functions that Canon devices provide to respond to the requirements in the guidelines. (For a description of each function, see Section 2.) The table below also provides recommended settings for appropriately utilizing each function. The “Requirement Compatibility Chart” in the Appendix provides details on the various settings and the functions that correspond to each guideline. Use the “Requirement Compatibility Chart” when configuring the settings.

Functions Corresponding to Guidelines and Recommended Settings

Function	Recommended Settings	Corresponding NIST SP 800-171/172 Family
User Authentication/ Access Control	Enable the user authentication function to manage the users that use Canon devices, and configure the settings for each user. Configure the Access Management System, password policy, and lockout settings appropriately. Configure authentication management if you are using the Advanced Box.	- Access Control - Audit and Accountability - Identification and Authentication - System and Communications Protection
Firewall Settings	Configure the firewall settings to manage communication with the devices.	- Access Control - System and Communications Protection
Proxy Settings	Configure the proxy settings.	- Access Control - System and Communications Protection

Function	Recommended Settings	Corresponding NIST SP 800-171/172 Family
TLS Settings	Configure the settings to enable the use of TLS encrypted communication. Configure the machine to verify the server certificate, depending on the environment. Register a server key/certificate that is issued by a trusted certificate authority. Then, set thekey/certificate as the key used for TLS encrypted communication to improve security. Configure the encryption method to comply with FIPS 140.	- Access Control - Identification and Authentication - System and Communications Protection
IPSec Settings	Configure the IPSec settings according to the environment.	- Access Control - System and Communications Protection
IEEE 802.1X Settings	Configure the IEEE 802.1X settings to adopt IEEE 802.1X.	- Access Control
Audit Log	Enable the audit log function. Configure Syslog settings to link with a SIEM system. Set the correct date and time on the Canon device. Configure the SNTP settings to synchronize the time of Canon device with a server.	- Access Control - Audit and Accountability - Incident Response
Restricting the Use of Memory Media	Configure the settings to restrict the use of memory media such as USB drives.	- Media Protection
Forced Hold Printing	Enable the function.	- System and Communications Protection
Storage Data Encryption	No configuration is necessary. This function is always enabled.	- Audit and Accountability - Identification and Authentication - System and Communications Protection
TPM (Trusted Platform Module)	Enable the function. Back up the TPM key onto a USB drive immediately after you enable the TPM setting.	- System and Communications Protection

Function	Recommended Settings	Corresponding NIST SP 800-171/172 Family
Verify System at Startup	Enable the function.	- Configuration Management - System and Information Integrity
Protect Runtime System	Enable the function.	- Configuration Management - System and Information Integrity
Preventing Firmware/ Application Tampering	No configuration is necessary; this function is always enabled.	- Configuration Management - System and Information Integrity

The guidelines state that you need to correctly operate and manage devices in systems. Canon devices provide the following functions to assist device management.

Device Management Functions

Function	Recommended Settings	Corresponding NIST SP 800-171/172 Family
Security Policy Settings	The Security Policy function enables you to apply/manage all the settings related to information security.	- Configuration Management
Device Information Display	The counter/device information enables you to check device configurations, which include the serial number, IP address, version, and optional products.	- Configuration Management
SMS (Service Management Service)	Canon devices provide MEAP (Multifunctional Embedded Application Platform) as a platform for extending or optimizing the various functions incorporated in the device. You can use SMS to install MEAP applications and check their status.	- Configuration Management
Scheduled Firmware Updates	Canon devices can periodically check for new firmware and automatically update the firmware.	- Configuration Management - System and Information Integrity

Function	Recommended Settings	Corresponding NIST SP 800-171/172 Family
Initialize All Data/Settings	When disposing or reusing the Canon device, you can completely erase the data saved to the device.	- Maintenance - System and Communications Protection
Backing Up/Restoring Data	You can back up or restore the data saved to the Canon device to perform maintenance.	- Maintenance

4 Summary

Canon devices provide various solutions for cybersecurity measures. By appropriately adopting these solutions, you can respond to the requirements for information devices in the security requirements defined by NIST SP 800-171 and NIST SP 800-172. Your organization is responsible for implementing the cybersecurity measures required by NIST SP 800-171 and NIST SP 800-172. Canon Inc. provides you with support for implementing your cybersecurity measures.

For your convenience, Canon has created an additional document “NIST Cybersecurity White Paper: Compatibility Charts for Law Firms, which describes how you can utilize/configure/operate the functions of Canon imageRUNNER ADVANCE DX and imagePRESS Lite devices to respond to each NIST SP 800-171 and NIST SP 800-172 requirement in the NIST Cybersecurity Framework guidelines.

Contact your Canon authorized representative to obtain a copy of detailed NIST SP 800-171 and NIST SP 800-172 Requirement Compatibility Charts for imageRUNNER ADVANCE DX and imagePRESS Lite devices.

5 Appendix

ABOUT NIST

- **NIST Overview**
  https://www.nist.gov/cybersecurity

- **NIST Cybersecurity Framework - Journey to CSF 2.0**
  https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

- **NIST FAQ**
  https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework

NIST SP 800-171 and SP 800-172

- *SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
  https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

- *SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*
  https://csrc.nist.gov/pubs/sp/800/172/final

1-844-50-CANON

usa.canon.com/business

02/25-0209-8292