Canon

CYBERSECURITY WHITE PAPER

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

Version 1.0
March 2023

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 dealer 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)** is one such tool that is consistently 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 files 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. The **"Requirement Compatibility Chart"** in the Appendix describes the requirements in further detail plus how those requirements relate to the functions of Canon devices. The chart also provides 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

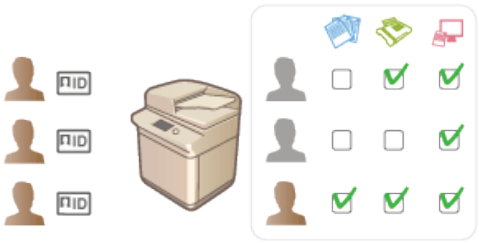
- **User Authentication/Access Control**
  Canon devices provide administrators with various authentication options for ensuring that only authorized users can use the machine and its functions (such as the print, copy, scan, and send functions).

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

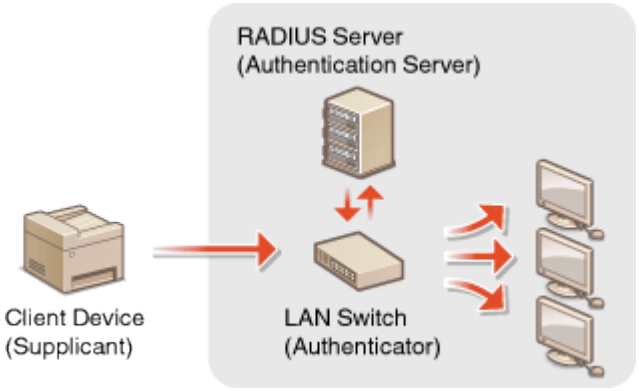
You can configure the firewall settings of a Canon device to prevent unauthorized access by third parties, as well as network attacks and intrusions, by only allowing communication with devices that have a specific IP address.

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.

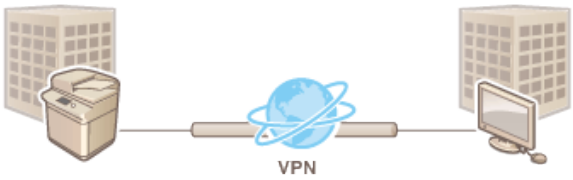
TPM (Trusted Platform Module)
Canon devices include a TPM chip for securely managing confidential information. The encryption key protected by the TPM chip encrypts the following confidential information in Canon device:

- 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.

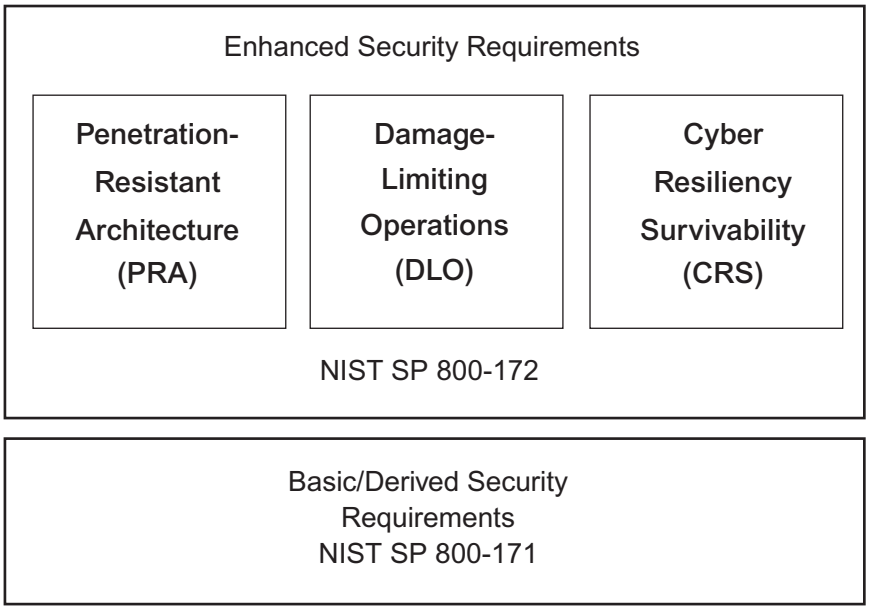
The countermeasures perform the following:

- 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

The “Requirement Compatibility Chart” in the Appendix describes how you can utilize/configure/operate the functions of Canon devices to respond to eachrequirement in the guidelines. The chart also provides examples of measures that organizations should implement to respond to the requirements in the guidelines. For details, see “Requirement Compatibility Chart” in the Appendix.

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.

5 Appendix

Reference

- NIST CSF
  https://www.nist.gov/cyberframework
- NIST SP 800-171 Revision 2
  https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-172
  https://csrc.nist.gov/publications/detail/sp/800-172/final

5.1 NIST SP 800-171 Requirement Compatibility Chart

This table is provided in support of “Guidance for Canon Printer and Multifunction Device Functionality in Support of NIST SP 800-171 and NIST SP 800-172”, version 1.00, March 2023.
Use this table when configuring the settings to respond to each requirement in the guideline.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
Family	ID	Requirement				
3.1 ACCESS CONTROL Basic (Basic Security Requirements)	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	This requirement states that you must limit access to appropriate users and the processes/devices that act on behalf of those users. You can use the functions of the machine to enforce various access restrictions.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Manage users of the machine with user account management. The following operations are required for performing user account management: • Creating user accounts • Assigning privileges according to an access control policy • Managing passwords - Changing the default password - Setting a password policy • Deleting unnecessary accounts
	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	This requirement states that you must limit the functions available to users with access privileges by user attribute. You can use the functions of the machine to limit the functions available to users by user role.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Manage users of the machine with user account management. The following operations are required for performing user account management: • Creating user accounts • Assigning privileges according to an access control policy • Managing passwords - Changing the default password - Setting a password policy • Deleting unnecessary accounts
	3.1.3	Control the flow of CUI (Controlled Unclassified Information) in accordance with approved authorizations.	This requirement states that you must control the traffic flow of CUI (Controlled Unclassified Information) between systems. The machine supports the actions of your organization to meet this requirement by providing traffic flow control functions such as a firewall and proxy functionality. You must appropriately configure the functions such as the firewall according to the CUI control flow policy defined by your organization.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses. **Proxy Settings** When viewing websites, the machine connects to outside networks via a proxy server. Using a proxy server improves the security of viewing websites.	Configure <Firewall Settings>. Enable <Proxy Settings>.	Use the firewall and proxy settings to construct an appropriate traffic flow control environment in order to implement the information flow control that is approved by your organization. Configure the appropriate network settings for the machine.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	This requirement states that you must separate the duties of the individuals that belong to your organization. Your organization is mostly responsible for this requirement. You must define and separate the duties. The machine supports the actions of your organization to meet this requirement by providing the following functions: • Default roles such as administrator and general user roles • Creation of custom roles with custom function usage restrictions For example, you can configure and use custom roles according to the duties defined in your organization, in order to achieve appropriate separation of duties for using the functions of the machine.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Separate the duties of individuals and define an access control policy according to those duties. Assign privileges according to the access control policy for the accounts of users who use the machine.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	This requirement states that you must apply the principle of least privilege to the users of systems according to their duties. The machine provides the following roles: • The general user role that can use basic functions such as printing and copying • The administrator role that has special privileges for changing administrator settings The machine also provides functions for creation of custom roles with custom function usage restrictions.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Apply the principle of least privilege and define an access control policy that assigns the minimum required access permissions. Assign privileges according to the access control policy for the accounts of users who use the machine.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	This requirement states that privileged users must use non-privileged accounts when using nonsecurity functions. Your organization is mostly responsible for this requirement. Individuals (privileged users) that belong to your organization must switch accounts according to the function they use. The machine provides the administrator role for privileged accounts and the general user role for non-privileged accounts. You can meet this requirement by ensuring that users switch accounts according to the functions they will use.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Limit the use of privileged accounts and define an access control policy ensuring that non-privileged accounts are used for accessing nonsecurity functions. To meet this requirement, create non-privileged accounts for accessing nonsecurity functions. 1. Assign privileges to the accounts of users according to the access control policy. 2. Ensure that users use a non-privileged account when using nonsecurity functions.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	This requirement states that you must retain a record such as a log to enable audits when a non-privileged user executes a privileged function. The machine provides functions for: • Controlling the function execution of privileged and non-privileged users by role • Retaining an audit log of privileged function operations, such as administrator setting changes	**Audit Log Function** You can use logs to check/analyze how the machine is used.	Enable the audit log function.	Limit the use of privileged accounts and define an access control policy ensuring that non-privileged accounts are used for accessing nonsecurity functions. Assign privileges according to the access control policy for the accounts of users who use the machine. Use the audit log to audit the usage status of the machine to ensure that the machine is being appropriately used according to the access control policy.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.8	Limit unsuccessful logon attempts.	This requirement states that you must limit the number of login attempts. For example, you must lock out the user after a certain number of unsuccessful login attempts. The machine provides a function for locking the account when user authentication fails. You can also set the number of failed login attempts that can occur before the account is locked, and the amount of time that must pass after lockout before login attempts can be received again.	**Lockout Function** You can configure lockout settings to limit the number of continuous login attempts. When the machine detects the set number of failed login attempts, the system temporarily locks the account.	Enable <Lockout Settings>.	Define a policy for limiting failed login attempts, such as a failed login count for lockout and an interval time until logins are received again after a lockout occurs. Configure appropriate lockout settings for the machine to limit login attempts.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.9	Provide privacy and security notices consistent with applicable CUI (Controlled Unclassified Information) rules.	This requirement states that you must provide notifications regarding privacy and security to system users according to the applicable CUI (Controlled Unclassified Information) rules. Your organization is mostly responsible for this requirement, rather than the machine.	N/A	N/A	Provide privacy and security notifications consistent with applicable CUI (Controlled Unclassified Information) rules and make sure that users see the notifications when accessing information systems.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	This requirement states that when a period of inactivity exceeds the specified time, you must set the system to: • Lock the session. • Hide the system screen using a pattern image such as a screensaver or fixed image. The machine enables you to set the length of the period of inactivity until the Auto Reset function locks the session. And then, the machine displays a fixed screen when an auto reset occurs.	**Auto Reset Function** When the user performs no operations on the touch panel display for a certain period of time, the machine performs an auto reset to automatically log the user out. After logging the user out, the machine displays the authentication screen.	Configure <Auto Reset Time>.	Enable session locking using a screensaver or similar function. Configure the auto reset time according to the policy.
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.11	Terminate (automatically) a user session after a defined condition.	This requirement states that when a period of inactivity exceeds the specified time, your system must terminate the user session automatically. The machine provides a function for terminating the session by forcibly logging the user off when a period of inactivity exceeds the specified time. The machine also requests login authentication again when starting a new session after a session has been terminated (when using the machine again).	**Auto Reset Function** When the user performs no operations on the touch panel display for a certain period of time, the machine performs an auto reset to automatically log the user out. The machine also automatically terminates the session when the user performs no operations on the Remote UI for a certain period of time. When starting a new session, the machine requests user authentication again.	Configure <Auto Reset Time>.	Decide how long the period of inactivity should be before locking the session. Configure the auto reset time according to the policy.
	3.1.12	Monitor and control remote access sessions.	This requirement states that you must monitor remote access. The machine provides a function for retaining a log of remote access such as Remote UI operations.	**Audit Log Function** You can use logs to check/analyze how the machine is used.	Enable the audit log function.	Use the audit log to audit the usage status of the machine to ensure that the machine is being appropriately used according to the access control policy.
	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	This requirement states that you must employ session protection (confidentiality protection) mechanisms for remote access sessions. The machine provides a function for encrypting the data on the communication route when a user accesses the machine remotely, such as with Remote UI operations. This function employs a cryptographic module that is compliant with the FIPS 140 standard.	**TLS Encrypted Communication** You can use TLS encrypted communication to prevent actions such as eavesdropping, tampering, and spoofing when accessing the machine from a computer or other device to exchange data. You can also set the machine to limit communication to that using an algorithm compliant with the FIPS 140-2 standard. **IPSec Communication** While TLS only encrypts data used on a specific application, such as a Web browser or an e-mail application, IPSec encrypts data at the IP packet level. This enables IPSec to offer a more versatile security system than TLS.	Configure <TLS Settings>. Enable <Use TLS> in the settings of each function/application. Also set the machine to verify the server certificate, depending on the environment. Enable <Use IPSec>. Enable <Format Encryption Method to FIPS 140-2>.	When remotely accessing a system, use a session protection function that employs an encryption mechanism such as TLS or IPSec. Configure the appropriate network settings for the machine to protect network communications.
	3.1.14	Route remote access via managed access control points.	This requirement states that you must route remote access via managed access points. Your organization is mostly responsible for this requirement. The machine supports the actions of your organization to meet this requirement by providing a firewall function for limiting the networks that can access the machine.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses.	Configure <Firewall Settings>.	Establish remote access routing via a managed access point. Configure the appropriate network settings for the machine.
	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	This requirement states that you must authorize remote access and use of privileged commands and security-related information (such as audit logs). You can limit functions by user role and use the user authentication function of the machine according to an access control policy defined by your organization to limit the privileged functions that can be executed via remote access and limit access to security-related information to specific users. For example, you can control the machine to allow only a specific IT administrator to use privileged functions that affect the machine, such as changing administrator settings from the Remote UI and viewing audit logs.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	Assign privileges according to the access control policy for the accounts of users who use the machine. The administrator must manage the important settings of the machine, such as user management and security settings.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.16	Authorize wireless access prior to allowing such connections.	This requirement states that you must appropriately manage the devices (such as smartphones and tablets) that perform wireless access within your organization. Your organization is mostly responsible for this requirement, rather than the machine. You must define and implement device management guidelines, such as: • Device type and setting requirements based on a BYOD (Bring Your Own Device) policy • Authentication requirements for wireless connections The machine provides the following functions for supporting the operation of management guidelines: • IEEE 802.1X authentication for authenticating the devices that connect to the machine via wireless LAN • Enabling/disabling the wireless direct connection itself	**IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client. **Wireless LAN** You can wirelessly connect the machine to a computer or mobile device via a wireless LAN router (access point). The settings required to use this function must be configured by an administrator. The machine also supports connecting to network environments that have adopted IEEE 802.1X authentication.	Enable <IEEE 802.1X Settings>. Configure <Wireless LAN Settings>. Disable <Direct Connection Settings>.	Allow wireless access before allowing wireless connections, according to the access control policy. You can also adopt IEEE 802.1X authentication to allow network connections only to client devices authorized by an authentication server. Configure the appropriate network settings for the machine. Disable the direct connection settings for wireless LAN.
	3.1.17	Protect wireless access using authentication and encryption.	This requirement states that you must protect wireless access to a system using authentication and encryption functions. The machine provides the following functions to protect wireless access: • Device authentication via IEEE 802.1X or a PSK (pre-shared key) • Data encryption You can use IEEE 802.1X authentication to secure wireless connections.	**IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client. **Wireless LAN** You can wirelessly connect the machine to a computer or mobile device via a wireless LAN router (access point). The settings required to use this function must be configured by an administrator. The machine also supports connecting to network environments that have adopted IEEE 802.1X authentication.	Enable <IEEE 802.1X Settings>. Configure <Wireless LAN Settings>. Disable <Direct Connection Settings>.	Protect wireless access using authentication and encryption, according to the access control policy. You can also adopt IEEE 802.1X authentication to allow network connections only to client devices authorized by an authentication server. Configure the appropriate network settings for the machine. Select a secure algorithm for the data encryption method.
	3.1.18	Control connection of mobile devices.	This requirement states that you must appropriately manage mobile devices used in your organization (devices which are connected to a system in your organization). This requirement applies to the obligations of your organization, and does not apply to the machine. For example, you must define mobile device usage guidelines and manage mobile devices using the methods indicated below: • EMM (Enterprise Mobility Management)/MDM management • Mobile device identification • Management of software inside mobile devices • Mobile device virus checking • Mobile device configuration management	N/A	N/A	Manage the mobile devices used in your organization according to an access control policy and control connections.
	3.1.19	Encrypt CUI (Controlled Unclassified Information) on mobile devices and mobile computing platforms.	This requirement states that you must use encryption to protect the CUI (Controlled Unclassified Information) saved on mobile devices. This requirement only applies to mobile devices, and not the machine, as it is not a mobile device.	N/A	N/A	Manage the mobile devices used in your organization according to an access control policy and control connections. You need to perform encryption on the entire mobile device or at the container level, in order to protect the confidentiality and integrity of CUI (Controlled Unclassified Information).

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.1 ACCESS CONTROL Derived (Derived Security Requirements)	3.1.20	Verify and control/limit connections to and use of external systems.	This requirement states that you must verify, control, and limit connections to external systems (such as external cloud services) outside your organization. Your organization is mostly responsible for this requirement. You must define and implement a policy regarding the use of external systems. The machine supports the actions of your organization to meet this requirement by providing an IP filter function for controlling access to the machine from external systems.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses. **Proxy Settings** When viewing websites, the machine connects to outside networks via a proxy server. Using a proxy server improves the security of viewing websites.	Configure <Firewall Settings>. Enable <Proxy Settings>.	1. Set conditions regarding the use of external information systems according to the security policy and procedures of your organization. 2. Control and limit connections to external information systems. Configure firewall settings and proxy settings that are appropriate for the machine.
	3.1.21	Limit use of portable storage devices on external systems.	This requirement states that you must control the usage of portable storage (such as external hard disk drives or USB flash drives) managed by your organization on external systems. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must define and implement a policy regarding the use of external systems so that portable storage is allowed in external systems only when administrator authorization is obtained.	N/A	N/A	1. Set conditions regarding the use of external information systems according to the security policy and procedures of your organization. 2. Control and limit connections to external information systems. Limit the use of portable storage devices on external systems.
	3.1.22	Control CUI (Controlled Unclassified Information) posted or processed on publicly accessible systems.	This requirement states that you must control the CUI (Controlled Unclassified Information) posted to systems disclosed to the public or processed on such systems. Your organization is mostly responsible for this requirement, rather than the machine. For example, in order to control the CUI posted to/processed on public systems, you must: • Manage the employees that are able to post CUI (Controlled Unclassified Information) to public systems such as websites. • Conduct a review before posting.	N/A	N/A	Manage and control the information posted to or processed on systems that are publicly accessible.
3.2 AWARENESS AND TRAINING Basic (Basic Security Requirements)	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	This requirement states that you must provide training on security awareness to employees at your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must disseminate security warnings (such as instructing employees not to open attachments or links in suspicious e-mail) by means of training and posters in the company.	N/A	N/A	Conduct security training to disseminate security warnings (such as instructing employees not to open attachments or links in suspicious e-mail). Decide the frequency for conducting security training.
	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	This requirement states that you must conduct appropriate security training for the employees of your organization according to their role (such as software developer, system developer, or network administrator). Your organization is mostly responsible for this requirement, rather than the machine.	N/A	N/A	Conduct appropriate security training for the employees of your organization according to their role (such as software developer, system developer, or network administrator). Decide the frequency for conducting security training.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.2 AWARENESS AND TRAINING Derived (Derived Security Requirements)	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	This requirement states that you must provide security training on insider threats and reporting those threats. Your organization is mostly responsible for this requirement, rather than the machine.	N/A	N/A	Implement security training regarding insider threats and their reporting. More specifically, disseminate information about high-risk actions that may indicate potential insider threats, upon deciding a method for reporting. Potential indicators and possible precursors of insider threats include the following behaviors: • Inordinate, long-term job dissatisfaction • Attempts to gain access to information not required for job performance • Unexplained access to financial resources • Bullying or sexual harassment of fellow employees • Workplace violence • Other serious violations of organizational policies, procedures, directives, rules, or practices
3.3 AUDIT AND ACCOUNTABILITY Basic (Basic Security Requirements)	3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	This requirement states that you must record audit logs in order to monitor inappropriate system activity. The machine provides an audit log function for recording the various types of operations performed on the machine.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	Decide the events that must be audited. Also decide the frequency for auditing the events. Identify additional information that is required for auditing, as required. Decide values such as thresholds that determine the inappropriate state of the events subject to auditing. Build an audit team. Configure the audit log function and appropriately audit the machine.
	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	This requirement states that you must ensure that the actions and events caused by specific users are uniquely traceable. The machine provides an audit log function for recording the various types of operations performed on the machine. Audit logs enable you to trace events at the user level, as they record user IDs and time stamps for each audit event.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	Decide the events that must be audited. Also decide the frequency for auditing the events. Identify additional information that is required for auditing, as required. Decide values such as thresholds that determine the inappropriate state of the events subject to auditing. Build an audit team. Configure the audit log function and appropriately audit the machine.
3.3 AUDIT AND ACCOUNTABILITY Derived (Derived Security Requirements)	3.3.3	Review and update logged events.	This requirement states that you must review and change the events subject to auditing according to the situation. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must review the audit logs when an incident occurs. If you decide that tracking is difficult using only the items currently recorded to the audit log, you must add items to be recorded in order to track similar incidents more effectively in the future. The machine supports the actions of your organization to meet this requirement by providing a function for changing the items to be recorded in audit logs.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	Periodically review the events for auditing and reconsider the items for auditing as required, to ensure that the appropriate events are audited. Configure the audit log function and appropriately audit the machine.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
Family	ID	Requirement				
3.3 AUDIT AND ACCOUNTABILITY Derived (Derived Security Requirements)	3.3.4	Alert in the event of an audit logging process failure.	This requirement states that you must set systems to issue an alert when audit log recording fails. The machine provides a function for issuing an alert on the control panel when an error occurs with the audit log function.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	Configure the systems of your organization to issue an alert in the case of audit logging process failure, and define and implement responses for alerts. For example, configure the system to alert the person assigned by your organization when the audit process of the system fails, who must then cancel the alert (recover the audit process). Configure the audit log function and appropriately audit the machine. If an error regarding the audit log function appears on the control panel of the machine or Remote UI, you should: 1. Display the log management screen of the Remote UI. 2. Check the error and resolve it. For details on how to resolve errors, see the online manual for the machine.
	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	This requirement states that you must respond to suspicious activity by reviewing and analyzing audit logs and making reports. Your organization is mostly responsible for this requirement. You must review and analyze the audit logs of systems and implement an appropriate incident response. The machine supports the actions of your organization to meet this requirement by providing an audit log function for recording the various types of operations performed on the machine.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	1. Identify signs of problems in the systems of your organization by reviewing, analyzing, and surveying audit logs. 2. Build an audit team that responds to suspicious activity. Configure the audit log function and appropriately audit the machine.
3.3 AUDIT AND ACCOUNTABILITY Derived (Derived Security Requirements)	3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	This requirement states that you must reduce the size of audit logs (eliminate information that does not relate to incident tracking) and create reports so that you can smoothly conduct audit log analysis and reporting. Your organization is mostly responsible for this requirement. You must extract the required information from audit logs to create reports. The machine supports the actions of your organization to meet this requirement by providing an audit log function for recording the various types of operations performed on the machine. You can retrieve audit logs from the machine and use those logs as a base to simplify the process of audit log analysis and reporting.	**Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Enable the audit log function.	Build an audit team that retrieves information from the audit log, simplifies that information, and creates reports. Configure the audit log function and appropriately audit the machine.
	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	This requirement states that you must synchronize system clocks with a trusted information source (NTP server) in order to record correct time stamps in audit logs. The machine enables you to use an NTP server for time synchronization, and the synchronized time is also used for the time stamps of audit logs.	**SNTP Settings** SNTP is a protocol for adjusting clocks in devices based on the standard of a time server on a network. By referencing a trusted NTP server, you can maintain the precision of time stamps.	Configure <SNTP Settings>.	Decide the settings such as the time server and polling interval that the systems of your organization will reference, and ensure that the systems can correctly synchronize the time and generate time stamps. Configure the NTP server address and polling interval on the machine.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.3 AUDIT AND ACCOUNTABILITY Derived (Derived Security Requirements)	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	This requirement states that you must protect audit logs from unauthorized access, tampering, and deletion. The user authentication function of the machine enables you to limit the users that can perform operations on audit logs. The machine also encrypts audit logs using the storage data encryption function and saves them inside the machine. It is difficult to directly access the storage to modify or delete audit logs. In addition, you can output audit log files to make backups and restore logs even if they are deleted.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result **Storage Data Encryption** The storage of the machine contains files in the Advanced Box and Mail Box, registered information in the Address Book, undeleted job data, and password information. By encrypting this data, you can prevent the information from being accessed without authorization.	Configure <User Management>. Enable the audit log function.	Decide the administrator of the audit function. Configure the user management function of the machine so that only the administrator of the audit function can access the audit log function. You do not need to configure the function for encrypting the storage data of the machine.
	3.3.9	Limit management of audit logging functionality to a subset of privileged users.	This requirement states that you must limit the management of the audit log function to a subset of privileged users. The user authentication of the machine enables you to limit the users that can access the audit log function. For example, configure the machine so that only the administrator can access the audit log function.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Configure <User Management>. Enable the audit log function.	Decide the administrator of the audit function, and configure user management functionality so that only the administrator of the audit function has audit-related privileges, such as accessing the audit log function.
3.4 CONFIGURATION MANAGEMENT Basic (Basic Security Requirements)	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	This requirement states that you must manage the system configurations of your organization (such as operating system versions and installed applications). Your organization is mostly responsible for this requirement. You must manage and regulate system configurations upon defining baseline configurations for your organization systems. The machine supports the actions of your organization to meet this requirement by providing a function for displaying the device configuration such as the version and optional product of the machine on the Counter/Device Information screen.	**Counter/Device Information** You can check the device configurations, which include the serial number, IP address, version, and optional product. You can also check information on the version of the security chip used in the encryption of data in storage.	Display <Check Device Configuration>.	Build, document, and manage baseline configurations based on the system component information of the machine. Periodically review the baseline configurations, and update them when system changes are made. When building the baseline configurations, you can use the device information view function of the machine to obtain information on the system components.
	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	This requirement states that you must manage the security settings of the systems in your organization. Your organization is mostly responsible for this requirement. You must apply and regulate security settings upon defining a security settings baseline (security policy) for the systems in your organization. The machine supports the actions of your organization to meet this requirement by providing the following functions: • A security policy function that allows you to easily configure security settings • A batch setting function using setting files that are obtained with the import/export function	**Security Policy** The Security Policy function of the machine enables you to apply/manage all the settings related to information security. You can import/export the security policy settings of the machine. You can apply the same policy to multiple devices to manage all the devices in your organization using the same settings.	Configure <Security Policy Settings>.	Define device security settings according to the security policy of your organization. Apply the defined security settings to all of the devices used in your organization. You can use the Security Policy function of the machine to apply a security policy. Example security policy settings include a wireless connection policy, communication operational policy, and authentication operational policy. You can import/export a configured security policy, which enables you to set the same security policy for multiple devices.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
Family	ID	Requirement				
3.4 CONFIGURATION MANAGEMENT Derived (Derived Security Requirements)	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	This requirement states that you must track, review, approve/decline, and audit changes made to the systems of your organization. Your organization is mostly responsible for this requirement. When changing the systems in your organization (such as changing the version of an operating system), you must: 1. Review the changes to be made. 2. Approve/decline the changes. 3. Implement the approved changes. To support the actions of your organization to meet this requirement, Canon provides notifications that indicate the new functions and changes added to the machine by firmware updates (User's Guide (Notification of New and Enhanced Functions)).	N/A	N/A	When making changes to the system of the machine, follow the procedure below: 1. Review the changes to be made. 2. Approve/decline the changes. 3. Implement the approved changes. System changes include the following: • Changes to baseline configurations • Changes to configuration settings • Unscheduled and unapproved changes • Changes for fixing vulnerabilities For example, when reviewing firmware updates, you can check changes provided by firmware updates in the User's Guide (Notification of New and Enhanced Functions). 1. Review the changes to be made. 2. Approve/decline the changes. 3. Update the firmware. 4. Reflect the changes to baseline configurations. You can use the approved auto firmware update function, but you must track the changes and reflect them in the baseline configurations.
	3.4.4	Analyze the security impact of changes prior to implementation.	This requirement states that you must analyze the security impact before making changes to the systems of your organization. Your organization is mostly responsible for this requirement, rather than the machine.	N/A	N/A	When making changes to the system of a device, follow the procedure below: 1. Review the changes to be made. 2. Approve/decline the changes. 3. Implement the approved changes. System changes include the following: • Changes to baseline configurations • Changes to configuration settings • Unscheduled and unapproved changes • Changes for fixing vulnerabilities
	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	This requirement states that you must define the person that implements changes (such as changing or updating hardware configurations) to the systems of your organization, and document and implement access restrictions. Your organization is mostly responsible for this requirement. You must define and specify the person with the privileges to access hardware and software to make physical and logical changes, and also document regulations concerning access restrictions. Access restriction methods include entry management, password-based user authentication, and automated updates. The machine supports the actions of your organization to meet this requirement by providing a function for applying access restrictions based on user roles.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Access Management System** You can assign the functions available for each privilege level (role) and create new roles.	Configure <User Management>. Enable <Use ACCESS MANAGEMENT SYSTEM>.	1. Define and specify the person with the privileges to access hardware and software to make physical and logical changes. 2. Document access restriction regulations. Example access restriction methods include entry management and password-based user authentication. Alternatively, you can automate system updates to limit user access to the update function. For example, you can assign a device administrator and create a device administrator account. By configuring the machine to allow only a device administrator to access device settings, you can ensure that only the assigned administrator can change the device configuration.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.4 CONFIGURATION MANAGEMENT Derived (Derived Security Requirements)	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	This requirement states that the systems of your organization must only provide essential capabilities (the principle of least functionality). Your organization is mostly responsible for this requirement. You must regulate the configurations and functions of the systems in your organization according to the baseline configurations and security policy that were deliberated upon and defined. You must also define the baseline configurations and security policy based on the principle of least functionality, so that unnecessary hardware or software is not installed and unnecessary functions are not enabled. The machine supports the actions of your organization to meet this requirement by providing a batch setting function. With this function, you can easily apply the security policy defined by your organization by importing/exporting batch setting files.	**Security Policy** The Security Policy function of the machine enables you to apply/manage all the settings related to information security. Security policy settings enable you to configure settings such as [USB Policy], [Port Usage Policy], and [Printing Policy] to ensure that unnecessary functions are not enabled. You can import/export the security policy settings of the machine. You can apply the same policy to multiple devices to manage all the devices in your organization using the same settings.	Configure <Security Policy Settings>.	Identify functions not required for the operation of the machine according to baseline configurations and security policy, and limit/disable those functions. The functions to limit/disable include applications, protocols, and ports that are enabled by default. The Security Policy function of the machine enables you to limit all the functions related to information security. For example, you can limit the ports of unused printing protocols (such as port number 515 for LPD and port number 21 for FTP) using this function.
	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	This requirement states that you must restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services used in the systems of your organization. Your organization is mostly responsible for this requirement. You must regulate the systems in your organization according to a security policy (defining the allowed ports, protocols, and services) that was deliberated and defined. The machine supports the actions of your organization to meet this requirement by providing a security policy function for restricting the functions of the machine according to a security policy defined by your organization.	**Security Policy** The Security Policy function of the machine enables you to apply/manage all the settings related to information security. Security policy settings enable you to configure settings such as [USB Policy], [Port Usage Policy], and [Printing Policy] to ensure that unnecessary functions are not enabled. You can import/export the security policy settings of the machine. You can apply the same policy to multiple devices to manage all the devices in your organization using the same settings.	Configure <Security Policy Settings>.	Identify functions not required or not secure for the operation of the machine according to baseline configurations and security policy, and limit/disable those functions. The Security Policy function of the machine enables you to limit all the functions related to information security. For example, you can limit the ports of unused printing protocols (such as port number 515 for LPD and port number 21 for FTP) using this function.
	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	This requirement states that you must apply a deny-by-exception (blacklisting) policy and permit-by-exception (whitelisting) policy to limit the software that is used in the systems of your organization. The machine provides the following functions for whitelisting: • System verification functions (used during startup and operation) • Signature verification function (used when installing firmware and applications)	**Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Apply blacklisting policy or whitelisting policy to limit the software which is used in the systems of your organization. The Verify System at Startup function and the Protect Runtime System function enable you to restrict the systems used on the machine.
	3.4.9	Control and monitor user-installed software.	This requirement states that you must control and monitor the new software installed on the systems of your organization. The machine provides MEAP (Multifunctional Embedded Application Platform) as a platform for extending or optimizing the various functions of the machine, such as "communication", "authentication", and "output" functions. You can install and check the usage status of MEAP applications using SMS (Service Management Service) from the Remote UI. In addition, the user authentication function enables you to limit the users that can manage applications, and the audit log function enables you to record/monitor installation events.	**MEAP Application Management** You can display SMS in the Remote UI to manage applications. **Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result	Manage applications using [Service Management Service] in the Remote UI. Enable the audit log function.	1. Define a policy regarding the software components to install on the machine but not defined in the baseline configurations. 2. Confirm that the policy is complied with. A policy includes rules such as restrictions on application sources and the authorization of installation. You can display SMS in the Remote UI to manage applications. The machine records installation events in an audit log, and you can monitor the audit log to check compliance with the policy regarding the applications that can be installed.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
Family	ID	Requirement				
3.5 IDENTIFICATION AND AUTHENTICATION Basic (Basic Security Requirements)	3.5.1	Identify system users, processes acting on behalf of users, and devices.	This requirement states that you must identify the users and devices that access the systems of your organization. You must assign identifiers so that users and devices can be uniquely identified. The machine provides various authentication functions including the following: • User authentication for accessing the control panel and Remote UI • Access control at the communication protocol level • Access control for using the Advanced Box You can also use an authentication server to identify/authenticate the devices that can access the machine via an IEEE 802.1X-authenticated network.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. **Network Authentication Management** You can set an authentication function for the communication protocols (such as IPP and SNMP) of the machine. **Advanced Box Authentication Management** You can prevent unauthorized access by setting the machine to perform authentication when the Advanced Box is disclosed externally. **IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client.	Configure <User Management>. Enable <Use Authentication> in <IPP Print Settings>. Disable <Use SNMPv1> in<SNMP Settings>. Configure <Use SNMPv3>. Configure <Authentication Management> in <Advanced Box Settings>. Enable <IEEE 802.1X Settings>.	Enable the users and devices that access the system to be uniquely identified. For example, you can assign users IDs to identify users and use MAC addresses and IP addresses to identify devices. The machine enables you to identify users using the IC cards or user accounts requested when performing authentication to access the machine. For device identification, you can adopt IEEE 802.1X authentication to allow network connections only with client devices identified/authorized by an authentication server. You can also identify devices by checking information such as the IP addresses of the devices that accessed the machine, which are recorded in audit logs.
	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	This requirement states that you must require authentication for network access to the systems of your organization. The machine provides various user authentication functions including the following: • User authentication for accessing the control panel and Remote UI • Access control at the communication protocol level • Access control for using the Advanced Box The user authentication of the machine enables you to use password authentication to identify users, and you can set the machine to request users to change their password from the default password. You can also use an authentication server to identify/authenticate the devices that can access the machine via an IEEE 802.1X-authenticated network.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. If the administrator password has not been changed from the default password, a message prompting you to set a new password appears. **Network Authentication Management** You can set an authentication function for the communication protocols (such as IPP and SNMP) of the machine. **Advanced Box Authentication Management** You can prevent unauthorized access by setting the machine to perform authentication when the Advanced Box is open to external access. **IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client.	Configure <User Management>. Enable <Use Authentication> in <IPP Print Settings>. Disable <Use SNMPv1> in<SNMP Settings>. Configure <Use SNMPv3>. Configure <Authentication Management> in <Advanced Box Settings>. Enable <IEEE 802.1X Settings>.	Authenticate the users and devices that access the systems of your organization. The machine enables you to set authentication for accessing the machine via the control panel and Remote UI. In addition, you can set an authentication function for the protocols that have one (such as IPP and SNMP). You can also adopt IEEE 802.1X authentication to allow network connections only with client devices identified/authorized by an authentication server.
3.5 IDENTIFICATION AND AUTHENTICATION Derived (Derived Security Requirements)	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	This requirement states that you must use multifactor authentication for network access to the systems of your organization and for local access to privileged accounts. You can set the machine to require multifactor authentication by using both IC card authentication and PIN authentication when a user accesses the control panel.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. You can set IC card authentication as one of the methods for multifactor authentication.	Configure <User Management>.	Set multifactor authentication for access to the systems of your organization. Enable IC card authentication and PIN authentication for the administrator in the user management settings of the machine. Also implement multifactor authentication for information terminals at the systems of your organization and set the authentication domain of the machine according to that configuration. The machine enables you to set Active Directory or an LDAP server as the authentication server.
	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	This requirement states that you must adopt replay-resistant authentication mechanisms for network access to the systems of your organization. The machine enables you to use TLS communication to protect the communication route for access to the Remote UI, and this provides the machine with resistance to replay attacks.	**TLS Encrypted Communication** TLS encrypted communication adopts replay-resistant authentication mechanisms. Therefore, you can use TLS encrypted communication to enable the machine to withstand replay attacks when the machine is accessed from a computer or other device to exchange data.	Configure <TLS Settings>. Enable <Use TLS> in the settings of each function/application. Also set the machine to verify the server certificate, depending on the environment.	Adopt replay-resistant authentication mechanisms for network access. You can enable the TLS function of the machine to increase resistance against replay attacks when the machine is accessed from the Remote UI. To use TLS, you must specify a key and certificate (server certificate) required for encryption.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.5 IDENTIFICATION AND AUTHENTICATION Derived (Derived Security Requirements)	3.5.5	Prevent reuse of identifiers for a defined period.	This requirement states that you must prevent the reuse of the login accounts of systems in your organization for a specified period. You must define and implement user account management guidelines to ensure that identifiers are not reused for the period specified in the guidelines, and disseminate this information to employees.	N/A	N/A	Define/manage user account management guidelines and specify a period during which accounts cannot be reused. Prohibit accounts from being reused for the specified period, according to the user account management guidelines. For example, if the user name is used for the account name, the account of a person joining your organization would be the same as that of a person with the same name who has left your organization. This corresponds to account reuse and is prohibited during the period specified in the policy.
	3.5.6	Disable identifiers after a defined period of inactivity.	This requirement states that you must disable login accounts for the systems of your organization that have been inactive for a specified period. The machine enables the automatic deletion of accounts of users that have not logged in for a certain period of time.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. The machine can automatically delete the accounts of users that have not logged in for a certain period of time.	Configure [Delete users that have not logged in for the specified period] in [Authentication Management] from the Remote UI.	Define/manage user account management guidelines and specify an inactivity period after which the machine automatically deletes accounts. Delete any accounts for which the specified period has elapsed. The machine provides a function for automatically deleting the accounts of users that have not logged in for a certain period of time, and you can enable that function to automatically delete such accounts.
	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	This requirement states that you must enforce a minimum password complexity and length when setting/changing the password of a login account for the systems of your organization, according to the policy defined by your organization. The machine enables you to set a minimum password length and complexity* in order to improve the reliability of passwords. * You can require the use of numbers, lowercase/uppercase letters, or symbols.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. You can set the minimum number of characters required when registering a password and whether to require the use of characters, numbers, or symbols in passwords.	Configure the following settings in <Password Settings>: • <Minimum Length Settings> • <Use at Least 1 Uppercase Character> • <Use at Least 1 Lowercase Character> • <Use at Least 1 Digit> • <Use at Least 1 Symbol>	Define a policy for setting passwords. A policy includes rules for the minimum number of characters and password complexity (combination of numbers, letters, and symbols). Configure the machine to request the users of systems to set a password that complies with the policy. The machine provides a function for setting a password policy, and you can enable the function to force users to comply with a policy.
	3.5.8	Prohibit password reuse for a specified number of generations.	This requirement states that you must prevent the reuse of passwords for the specified number of generations for the login accounts of systems in your organization. You must state that passwords must not be reused for the specified number of generations in the password management guidelines, and disseminate this information to the employees of your organization.	N/A	N/A	Define/manage password management guidelines and specify the minimum number of password generations (password change history) until the use of the same password is allowed. Prohibit the use of the same password if the number of password generations has not reached the specified number of times. For example, if the minimum number of password generations is set to three, the same password as any of the previous three generations cannot be set as the new password. The same password as the first generation can be used for the fifth generation.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.5 IDENTIFICATION AND AUTHENTICATION Derived (Derived Security Requirements)	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	This requirement states that you must change the default password for the login accounts of systems in your organization. The machine provides a function that prompts the administrator to change their password when they log in for the first time.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. If the administrator password has not been changed from the default password, a message prompting you to set a new password appears.	Configure <User Management>.	Change the default password used to log in for the first time. The machine displays a warning that prompts the administrator to change their password when they log in for the first time.
	3.5.10	Store and transmit only cryptographically-protected passwords.	This requirement states that you must protect the passwords for the login accounts of systems in your organization. The machine stores the user passwords used for user authentication after hashing or encryption. The machine also provides the following functions: • Encrypting the storage of the machine • Encrypting communication routes using TLS	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. The machine stores the passwords used for user authentication after hashing or encryption. **Storage Data Encryption** The storage of the machine contains files in the Advanced Box and Mail Box, registered information in the Address Book, undeleted job data, and password information. By encrypting this data, you can prevent the information from being accessed without authorization. **TLS Encrypted Communication** You can use TLS encrypted communication to prevent actions such as eavesdropping, tampering, and spoofing when accessing the machine from a computer or other device to exchange data.	Configure <User Management>. Configure <TLS Settings>. Enable <Use TLS> in the settings of each function/application. Also set the machine to verify the server certificate, depending on the environment.	Protect the login accounts of systems in your organization by encrypting the passwords. The machine stores passwords after hashing or encryption. You can enable TLS to protect the passwords in the communication route, which is used for logging in to the machine from the Remote UI.
	3.5.11	Obscure feedback of authentication information.	This requirement states that you must obscure the passwords of the login accounts of systems in your organization by displaying them as asterisks or by other means to prevent shoulder surfing when users enter passwords. The machine provides a function for masking the entered characters when entering a password to prevent others from seeing the characters.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation. The machine provides a function for masking entered characters when entering a password.	N/A	Implement measures for obscuring authentication information, such as masking entered characters when entering a password. The machine does not need to be configured to do so.
3.6 INCIDENT RESPONSE Basic (Basic Security Requirements)	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	This requirement states that you must establish an incident response system at your organization. Your organization is mostly responsible for this requirement, rather than the machine. You must create an incident response team such as a CSIRT (Computer Security Incident Response Team).	N/A	N/A	Define and establish an incident response system.
	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	This requirement is related to incident response. It states that you must track the cause of, document, and report incidents to authorities both inside and outside your organization, in particular. Your organization is mostly responsible for this requirement, rather than the machine. The CSIRT in your organization must investigate/respond to incidents and report the result, which you must then document. You must also report the investigation results both inside and outside your organization.	N/A	N/A	Define and establish incident response processes, including tracking the cause of, documenting, and reporting incidents to authorities both inside and outside your organization, in particular.
3.6 INCIDENT RESPONSE Derived (Derived Security Requirements)	3.6.3	Test the organizational incident response capability.	This requirement is related to incident response. It states that you must test the incident response capability of your organization, in particular. Your organization is mostly responsible for this requirement, rather than the machine.	N/A	N/A	Conduct testing of incident response training.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.7 MAINTENANCE Basic (Basic Security Requirements)	3.7.1	Perform maintenance on organizational systems.	This requirement states that you must conduct maintenance on systems in your organization. Your organization is mostly responsible for this requirement. You must conduct maintenance on the systems in your organization according to a maintenance plan. The machine supports the actions of your organization to meet this requirement by providing a function for backing up and restoring data when replacing the storage.	**Backing Up/Restoring Data** You can back up the data saved on the machine to external storage or an SMB server. By backing the data up in advance, you can restore the data in case anything happens to it.	Perform the data backup/restore process from [Data Management] in the Remote UI.	Conduct maintenance on the machine according to a maintenance plan. Maintenance includes the following: • Regular planned maintenance • Irregular maintenance • Reconfiguration as required • Damage repairs The machine provides a data backup function to use when replacing the storage, and you can back up the data when performing maintenance and restore the data after maintenance is complete.
	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	This requirement states that you must manage and protect the items that are used for maintenance on systems in your organization, such as maintenance tools. This requirement mainly applies to the obligations of your organization, but because maintenance of the machine is performed by a service representative, you must manage and protect the maintenance tools. Canon conducts training on maintenance and manages the tools used for maintenance.	N/A	N/A	Supervise the maintenance personnel and manage/protect the maintenance tools.
	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI (Controlled Unclassified Information).	This requirement states that you must sanitize (disable or delete) the CUI (Controlled Unclassified Information) in systems for off-site maintenance of the system in your organization. When providing a system to an external organization for maintenance, you must sanitize CUI by deleting data or removing storage so that the CUI on the system cannot be accessed. The machine supports the actions of your organization to meet this requirement by providing a function for completely erasing the data on the machine.	**Initialize All Data/Settings** You can restore all of the machine settings to the factory default values. All of the data that remains on the storage is overwritten with 0 (null) data or another value, which prevents the leakage of sensitive data when replacing or disposing of the storage.	Perform <Initialize All Data/Settings>.	When a third party performs maintenance on the machine, sanitize the CUI (Controlled Unclassified Information) on the storage. One method of sanitization is to completely erase the data on the storage. You can use the data/setting initialization function of the machine to erase the data.
3.7 MAINTENANCE Derived (Derived Security Requirements)	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	This requirement states that when you use portable media in maintenance on systems in your organization, you must perform virus checks on that media. This requirement mainly applies to the obligations of your organization, but maintenance of the machine is performed by a service representative. The service representative follows the security policy of your organization (for example, using USB flash drives that have been checked for viruses).	N/A	N/A	Perform virus checks on the portable media used for maintenance.
	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	This requirement states that when conducting remote maintenance via a network on the systems of your organization, you must: 1. Implement access control using multifactor authentication. 2. Immediately terminate the session when remote maintenance is complete. This requirement does not apply to the machine because it does not have a remote maintenance function.	N/A	N/A	When performing remote maintenance via a network, use multifactor authentication to perform access control. Terminate the session immediately after remote maintenance is complete.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.7 MAINTENANCE Derived (Derived Security Requirements)	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	This requirement states that you must supervise the activities of maintenance personnel when conducting maintenance on systems in your organization. Your organization is mostly responsible for this requirement. You must supervise maintenance personnel that perform on-site work to ensure that they do not perform unauthorized actions. When temporarily providing the maintenance personnel of an external organization with an account such as a visitor account, your organization is also responsible for user account management.	N/A	N/A	When performing maintenance on the machine, approve the personnel who can access the machine. Supervise the maintenance of the machine.
3.8 MEDIA PROTECTION Basic (Basic Security Requirements)	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI (Controlled Unclassified Information), both paper and digital.	This requirement states that you must protect media (portable media including both paper and digital data) containing CUI (Controlled Unclassified Information) handled by your organization. Your organization is mostly responsible for this requirement. You must protect portable media containing CUI handled by your organization by storing the media in a location where entry management or other such restrictions are implemented. The machine supports the actions of your organization to meet this requirement by providing the following functions to prevent printed materials containing CUI from being taken away by third parties without authorization: • The forced hold printing function • The function for limiting the use of portable media	**Forced Hold Printing** The device administrator can configure the storage of documents in the machine without printing in order to avoid cases such as: • Users leaving printed materials on the machine, which are then taken away by another person • Accidental leakage of information • Misprints **Restricting the Use of Memory Media** Although memory media such as USB flash drives provide convenience, they can also be a source of information leakage if they are 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.	Enable <Forced Hold>. Select <Off> for <Use Scan Function> or <Use Print Function> in <Memory Media Settings>.	Protect the portable media containing CUI (Controlled Unclassified Information) handled by your organization. For example, place printed materials containing CUI in a location where access is restricted by entry management or in a storage area that can be locked. The machine supports the protection of CUI by providing the forced hold printing function and the function for limiting the use of memory media. By setting forced hold printing, you can prevent third parties from taking away printed materials. To limit the use of portable media, configure memory media settings.
	3.8.2	Limit access to CUI (Controlled Unclassified Information) on system media to authorized users	This requirement states that you must control access to the media (portable media including both paper and digital data) containing CUI (Controlled Unclassified Information) handled by your organization. Your organization is mostly responsible for this requirement. You must protect media containing CUI handled by your organization by storing the media in a location only accessible by authorized users. You must also keep a record of media taken out of the location using a method such as keeping a ledger.	N/A	N/A	Limit access to the portable media containing CUI (Controlled Unclassified Information) handled by your organization. For example, place devices in a location where access is restricted by entry management or in a storage area that can be locked in order to allow only approved users to access the devices. Implement a check out and return process for accessing media, and keep a record of the media that is checked out.
	3.8.3	Sanitize or destroy system media containing CUI (Controlled Unclassified Information) before disposal or release for reuse.	This requirement states that you must appropriately sanitize or destroy the following items before disposal or release for reuse: • Media (portable media including both paper and digital data) containing CUI (Controlled Unclassified Information) • Recordable media (internal storage) inside system devices The machine provides a function for completely erasing the data on the internal storage and you can use that function before disposing of or reusing the machine.	**Initialize All Data/Settings** You can restore all of the machine settings to the factory default values. All of the data that remains on the storage is overwritten with 0 (null) data or another value, which prevents the leakage of sensitive data when replacing or disposing of the storage.	Perform <Initialize All Data/Settings>.	Erase the information on the internal storage when disposing of or reusing the machine. You can use the Initialize All Data/Settings function of the machine to erase the data.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
Family	ID	Requirement				
3.8 MEDIA PROTECTION Derived (Derived Security Requirements)	3.8.4	Mark media with necessary CUI (Controlled Unclassified Information) markings and distribution limitations.	This requirement states that you must clearly mark media (portable media including both paper and digital data) containing CUI (Controlled Unclassified Information) handled by your organization. Your organization is mostly responsible for this requirement, rather than the machine. The machine supports the actions of your organization to meet this requirement by providing the watermark and secure watermark functions for adding watermarks on printed materials to indicate that the materials contain CUI.	**Watermark** When printing/copying, you can add a watermark such as "TOP SECRET" to the output. **Secure Watermark** You can configure the machine to always embed invisible text such as "DO NOT MAKE COPIES" or "TOP SECRET" in the background of printed or copied documents. The embedded text becomes visible when the documents are copied, alerting users to unauthorized duplication or the risk of information leakage.	Configure <Watermark> or <Secure Watermark Settings>.	If the machine handles information (such as printed materials) that contains CUI (Controlled Unclassified Information), indicate that the printed materials contain CUI. For example, clearly specify the users that can view the information by indicating the level of confidentiality on printed materials. You can use the watermark or secure watermark function to print a watermark indicating that printed materials contain CUI (for example, with a level of confidentiality) on output paper, or embed a secure watermark.
	3.8.5	Control access to media containing CUI (Controlled Unclassified Information) and maintain accountability for media during transport outside of controlled areas.	This requirement states that you must perform access control and maintain accountability for taking media (portable media including both paper and digital data) containing CUI (Controlled Unclassified Information) handled by your organization outside the organization. Your organization is mostly responsible for this requirement, rather than the machine. One of the methods for maintaining accountability when taking things outside your organization is to perform encryption on the data in media and detect any tampering. You can also limit the people allowed to transport media, and retrieve a precise record by tracking the transport route, to prevent/detect loss, destruction, and tampering of data.	N/A	N/A	Protect the confidentiality and integrity of CUI (Controlled Unclassified Information) when taking the device or the internal storage of the device away from the installation/storage location. You can protect the confidentiality and integrity of information by encrypting media and limiting the people who can transport media, as well as tracking and recording the transport route.
	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI (Controlled Unclassified Information) stored on digital media during transport unless otherwise protected by alternative physical safeguards	This requirement states that you must maintain the confidentiality of media (portable media including digital data) containing CUI (Controlled Unclassified Information) handled by your organization when that media is taken outside your organization. Your organization is mostly responsible for this requirement, rather than the machine. You must ensure that data is encrypted before media containing CUI is taken out of your organization.	N/A	N/A	Protect the confidentiality and integrity of CUI (Controlled Unclassified Information) when taking the device or portable media away from the installation/storage location.
	3.8.7	Control the use of removable media on system components.	This requirement states that you must manage removable media (such as external hard disk drives) containing CUI (Controlled Unclassified Information) handled by your organization. Your organization is mostly responsible for this requirement, rather than the machine. You must implement the following management, for example: • Perform a virus check when removable media is connected to a system in your organization. • Manage (minimize) the amount of removable media. • Ensure traceability when media is taken out (until the media is correctly disposed of or reused). The machine supports the actions of your organization to meet this requirement by providing functions for limiting the use of portable media on the machine.	**Restricting the Use of Memory Media** Although memory media such as USB flash drives provide convenience, they can also be a source of information leakage if they are 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.	Select <Off> for <Use Scan Function> or <Use Print Function> in <Memory Media Settings>.	Perform management on the removable media containing CUI (Controlled Unclassified Information). For example, restrict or prohibit the use of removable media handled by your organization. When using removable media, you must: • Confirm that no malicious code is contained on the media. • Ensure traceability when the media is taken out of your organization. • Perform tracking until the media is correctly disposed of or reused. Configure memory media settings to restrict the use of portable media on the machine.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.8 MEDIA PROTECTION Derived (Derived Security Requirements)	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	This requirement states that you must prohibit the use of portable storage devices containing CUI (Controlled Unclassified Information) handled by your organization when you cannot identify their owner. Your organization is mostly responsible for this requirement, rather than the machine. You must prohibit the use of portable storage devices whose owner (such as an individual, organization or project) cannot be identified, to avoid risks. The machine supports the actions of your organization to meet this requirement by providing functions for limiting the use of portable media on the machine.	**Restricting the Use of Memory Media** Although memory media such as USB flash drives provide convenience, they can also be a source of information leakage if they are 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.	Select <Off> for <Use Scan Function> or <Use Print Function> in <Memory Media Settings>.	Prohibit the use of portable storage devices containing CUI (Controlled Unclassified Information) handled by your organization when you cannot identify their owner. For example, mandate the affixing of labels that indicate the owner (such as an individual, organization or project) of the portable storage devices handled by your organization, and prohibit the use of devices without labels. Configure memory media settings to restrict the use of portable media on the machine.
	3.8.9	Protect the confidentiality of backup CUI (Controlled Unclassified Information) at storage locations.	This requirement states that you must also ensure the confidentiality of CUI (Controlled Unclassified Information) saved by your organization for backup purposes. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must encrypt CUI and save it to an external hard disk drive as a backup, then protect that hard disk drive using physical access control (such as entry management). The machine supports the actions of your organization to meet this requirement by providing a function for encrypting the backup data.	**Backing Up/Restoring Data** You can back up the data saved on the machine to external storage or an SMB server. By backing the data up in advance, you can restore the data in case anything happens to it. You can enter a password when backing up data to encrypt the data that is saved.	Perform the data backup/restore process from [Data Management] in the Remote UI. Configure [Encrypt Backup Data].	Protect the confidentiality of backup data when making backups of the CUI (Controlled Unclassified Information) handled with the machine. For example: 1. Encrypt the hard disk drives where backup data is stored. 2. Place them in a location where access is restricted by entry management or in a storage area that can be locked in order to allow only approved users to access the devices. You can use the data backup/restore function of the machine to back up data to external storage or an SMB server. You can also encrypt the backup data.
3.9 PERSONNEL SECURITY Basic (Basic Security Requirements)	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI (Controlled Unclassified Information).	This requirement states that you must screen individuals when authorizing access to your organizational systems that contains CUI (Controlled Unclassified Information). Your organization is mostly responsible for this requirement, rather than the machine. You must screen individuals. Screening involves, for example, conducting background checks and drug tests, and performing screening that reflects appropriate laws, policies, regulations, and standards, according to the access level required for each rank.	N/A	N/A	When your organization handles CUI (Controlled Unclassified Information), screen the individuals that handle the CUI. Screening involves procedures such as background checks and drug tests, and performing screening that reflects appropriate laws, policies, regulations, and standards, according to the access level required for each rank.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.9 PERSONNEL SECURITY Basic (Basic Security Requirements)	3.9.2	Ensure that organizational systems containing CUI (Controlled Unclassified Information) are protected during and after personnel actions such as terminations and transfers.	This requirement states that you must ensure that CUI (Controlled Unclassified Information) and the systems of your organization that include CUI continue to be protected during and after personnel changes such as terminations and transfers. Your organization is mostly responsible for this requirement, rather than the machine. You must implement measures such as the following to protect CUI from the people that leave your organization: • Retrieve all IT devices belonging to your organization (for example, laptops, mobile phones, and storage devices) from a person that leaves your organization. • Retrieve all ID cards, access cards, and keys belonging to your organization from a person that leaves your organization. • Conduct exit interviews to reconfirm that employees have the obligation to not discuss CUI after leaving the company. You must also implement the following measures: • Erase the data on all devices used by a person that leaves your organization, before reusing those devices. • Delete all accounts authorized to access CUI that were used by a person that leaves your organization. • Disable or close the employee accounts used by a person that leaves your organization. • Restrict access to physical spaces that use CUI.	N/A	N/A	Implement measures to prevent users who leave your organization (due to a termination or transfer) from accessing the CUI (Controlled Unclassified Information) in devices. For example, you must: 1. Request a terminated or transferred user to return items such as the IT devices and ID cards that were lent to the person. 2. Confirm constraints regarding confidential information such as CUI. You must erase the information on IT devices that were lent to the person and disable their accounts.
3.10 PHYSICAL PROTECTION Basic (Basic Security Requirements)	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	This requirement states that you must limit physical access to systems and equipment of your organization to authorized individuals. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must limit the people who can physically access the system using entry management.	N/A	N/A	Install/place devices in an environment that can only be physically accessed by authorized individuals. An example environment that only authorized individuals can access has the following features: • It is physically isolated from other locations by locking or another method. • Access is controlled with the credentials in a badge, ID card, or smart card. Because the location where the devices are installed/placed is likely to be a room, room access control, or entry management, is probably an effective measure. However, also consider the effectiveness of access control over the whole site or building, according to your environment.
	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	This requirement states that you must protect and monitor the system infrastructure (such as power facilities, power cables, and network cables) of your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must protect and monitor IT infrastructure using entry management and security cameras.	N/A	N/A	Protect and monitor the physical infrastructure systems of your organization. Infrastructure systems can include the following: • Power facilities and power cables for supporting the power infrastructure • Network cables, hubs, and routers for supporting the network infrastructure • Entry management systems and security cameras for supporting the installation environment

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.10 PHYSICAL PROTECTION Derived (Derived Security Requirements)	3.10.3	Escort visitors and monitor visitor activity.	This requirement states that you must escort and monitor visitors and guests to your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must monitor the activities of visitors by requesting visitors wear badges and ensuring that employees accompany visitors.	N/A	N/A	Constantly escort visitors and monitor visitor activity within the facility. Also maintain a record of visitor activities using a visitor log or other means. You must also consider the following measures: • Establishing a procedure for escorting visitors • Adopting a method for identifying visitors, such as badges or name cards
	3.10.4	Maintain audit logs of physical access.	This requirement states that you must maintain an audit log of physical access to systems and entry to facilities at your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must automatically record entry into a room using ID cards in an audit log, or record the entry/exit of visitors to the facility at a reception desk.	N/A	N/A	Appropriately manage audit logs regarding physical access. Audit logs regarding physical access include logs on access to facilities such as sites, buildings, and rooms, and logs regarding visitors.
	3.10.5	Control and manage physical access devices.	This requirement states that you must manage hardware tokens (such as ID cards) used for physical access to systems and entry to facilities at your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must manage the access privileges of ID cards for each individual that the cards are granted to.	N/A	N/A	Appropriately manage the devices (such as hardware tokens and ID cards) used for physical access control. You must also consider the following measures to perform appropriate management: • Establishing a life cycle flow from issuing to disposal/expiration • Handling exceptions, such as the lending or losing of devices
	3.10.6	Enforce safeguarding measures for CUI (Controlled Unclassified Information) at alternate work sites.	This requirement states that you must protect the CUI (Controlled Unclassified Information) in the alternate work sites of your organization (such as working from home or satellite offices). Your organization is mostly responsible for this requirement, rather than the machine. For example, you must implement the following measures according to policies and organization rules: • Adopting a patch management function, antivirus software, and hard disk encryption in laptop computers that are taken outside your organization • Adopting a secure communication method such as a VPN for access to systems in your organization	N/A	N/A	Implement appropriate access control for physical access to alternate work sites (such as working from home or satellite offices). Measures of an equivalent level to those used at regular work sites are required at alternate work sites.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.11 RISK ASSESSMENT Basic (Basic Security Requirements)	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI (Controlled Unclassified Information).	This requirement states that you must conduct periodic assessments on risks to the organizational operations, organizational assets, and individuals regarding CUI (Controlled Unclassified Information). Your organization is mostly responsible for this requirement, rather than the machine. The risk assessment referred to here is general business risk assessment, and differs from "3.12 SECURITY ASSESSMENT". For example, you must periodically conduct an assessment of the following risks that might lead to critical incidents: • Poorly designed and executed business processes • Inadvertent actions of people, such as disclosure or modification of information • Intentional actions of people, such as insider threat and fraud • Failure of systems to perform as intended • External events, such as natural disasters, public infrastructure and supply chain failures	N/A	N/A	Conduct periodic risk assessments (risk evaluations) on work and assets. You must also consider the following measures in risk assessments: • Evaluating the possibility and scope of damage caused by unauthorized access, use, disclosure, interruption/disruption, change, or destruction to information systems and the information that those information systems process, save, or transfer • Recording the results of the risk assessment and sharing the review and results with stakeholders • Swiftly conducting a risk assessment when there are major changes to the environment where information systems operate or when there are other changes to the situation that can impact the state of security
3.11 RISK ASSESSMENT Derived (Derived Security Requirements)	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	This requirement states that you must periodically conduct vulnerability scanning on systems in your organization. Your organization is mostly responsible for this requirement. For example, you must use a commercial vulnerability scanner to periodically evaluate vulnerabilities in applications and systems in your organization, including the machine.	N/A	N/A	Scan for vulnerabilities periodically and when new vulnerabilities are identified in related information systems/applications.
	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	This requirement states that you must respond to vulnerabilities on the systems of your organization. Your organization is mostly responsible for this requirement. For example, you must: 1. Use a commercial vulnerability scanner to detect/evaluate vulnerabilities in applications and systems in your organization, including the machine. 2. Apply patches to correct the vulnerabilities as required.	N/A	N/A	Remediate vulnerabilities identified in risk assessments. This may include the method for applying patches to information systems and the method for defining measures for avoiding vulnerabilities.
3.12 SECURITY ASSESSMENT Basic (Basic Security Requirements)	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	This requirement states that you must periodically assess the security controls in the systems of your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must conduct assessments (security assessments) on security controls as indicated below: • Periodically evaluate and document security controls. • Propose new controls or update existing controls. • Create plans for correcting (fixing) controls. • Document newly identified security risks.	N/A	N/A	Periodically assess the security controls in the systems of your organization.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.12 SECURITY ASSESSMENT Basic (Basic Security Requirements)	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	This requirement states that you must develop and implement action plans for handling the vulnerabilities in the systems of your organization. Your organization is mostly responsible for this requirement. For example, you must develop and implement an action plan for swiftly handling vulnerabilities that a vulnerability scanner finds in the systems of your organization, including the machine. Action plans include the following: • Specifying the person responsible for handling vulnerabilities • Defining the method and schedule for handling vulnerabilities • Defining the method for evaluating and measuring the results of handling the vulnerabilities	N/A	N/A	Fix flaws in the systems of your organization and develop and implement an action plan for reducing/eliminating vulnerabilities.
3.12 SECURITY ASSESSMENT Basic (Basic Security Requirements)	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	This requirement states that you must periodically check the controls in order to assess the validity of security controls in the systems of your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must: 1. Periodically check whether an inventory of the hardware, software, and firmware in the systems of your organization is managed in accordance with the security controls defined by your organization. 2. Make improvements as required. 3. Report the results to your superiors.	N/A	N/A	Check security controls and improve them as necessary, to ensure the continued effectiveness of the controls.
	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	This requirement states that you must develop a system security plan that describes the methods for implementing the security requirements. Your organization is mostly responsible for this requirement, rather than the machine. You must develop a system security plan based on NIST SP 800-18, for example.	N/A	N/A	Develop, document, and periodically update the system security plan. The system security plan should indicate the following: • System boundaries • The system operating environment • How the security requirements are implemented • Relationships with other systems
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Basic (Basic Security Requirements)	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	This requirement states that you must monitor, control, and protect communications at the system boundaries of your organization. The machine provides a firewall function. You can use the firewall function to monitor, control, and protect the communications (communication data sent and received by the machine) that pass the boundary of the machine. The machine also provides a function for using a proxy server. You can use the proxy server function to monitor, control, and protect the communications that pass the boundary of the systems in your organization.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses. **Proxy Settings** When viewing websites, the machine connects to outside networks via a proxy server. Using a proxy server improves the security of viewing websites.	Configure <Firewall Settings>. Enable <Proxy Settings>.	Monitor, manage, and protect communications at the major internal boundaries and external boundaries of the systems in your organization. 1. Define the major internal boundaries and external boundaries of the systems in your organization. 2. Monitor, manage, and protect communications at the defined boundaries with measures such as a proxy server. The machine provides a firewall function and function for using a proxy server. Enable and implement the functions of the machine according to the security control policy that you must implement for the systems of your organization.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Basic (Basic Security Requirements)	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	This requirement states that you must employ security-oriented architecture design, software development techniques, and system engineering principles in the IT infrastructure development of your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must conduct system development in a manner that incorporates applicable methods in NIST SP 800-160 (System Security Engineering).	N/A	N/A	Employ security-oriented architecture design, software development techniques, and system engineering principles when newly developing or upgrading the IT systems of your organization.
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Derived (Derived Security Requirements)	3.13.3	Separate user functionality from system management functionality.	This requirement states that you must separate the user functions and system management functions of the systems in your organization. The machine separates functions for system administrators (such as changing administrator settings) and functions for general users (such as printing and scanning). You can also use the user authentication function to perform access control by identifying general users and privileged users (administrators) that can use the functions of the machine for system administrators.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation.	Configure <User Management>.	Separate the user functions and system management functions of the systems in your organization. The machine separates functions for administrators (such as changing administrator settings) and functions for users (such as printing, scanning, and sending). Enable and implement the administrator functions of the machine according to the security control policy that you must implement for the systems of your organization.
	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	This requirement states that you must prevent information leaks via the shared system resources such as storage in the systems of your organization. The machine provides the forced hold printing function and Advanced Box authentication management function to prevent the unauthorized transfer and unintended transfer of information in the storage.	**Forced Hold Printing** The device administrator can configure the storage of documents in the machine without printing in order to avoid cases such as: • Users leaving printed materials on the machine, which are then taken away by another person • Accidental leakage of information • Misprints **Advanced Box Authentication Management** You can prevent unauthorized access by setting the machine to perform authentication when you disclose the Advanced Box.	Enable <Forced Hold>. Configure <Authentication Management> in <Advanced Box Settings>.	Prevent information leaks via the shared system resources such as storage in the systems of your organization. The machine enables you to use the forced hold printing function and Advanced Box authentication management function to prevent information leaks via the shared system resources such as storage in the systems of your organization. Configure the above functions according to the security control policy that you must implement for the systems of your organization.
	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	This requirement states that you must use subnetworks to ensure that the systems of your organization that are accessible externally are separated from internal networks. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must build a demilitarized zone (DMZ) between internal networks and external networks such as the Internet.	N/A	N/A	Build subnetworks that are physically or logically separated from internal networks, and place the system components for external access on those subnetworks.
	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	This requirement states that you must deny network traffic by default and allow network traffic by exception (whitelist) when controlling the network systems of your organization. The machine provides a firewall function that enables you to refuse all traffic and only allow the required traffic by exception (whitelisting) according to a security policy of your organization.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses.	Configure <Firewall Settings>.	Configure the firewall settings for the external boundaries and internal boundaries of the systems in your organization, according to a policy of "Deny network communications traffic by default and allow network communications traffic by exception". Follow the same policy for configuring the firewall function of the machine.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Derived (Derived Security Requirements)	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	This requirement states that you must disable split tunneling when your organization uses a VPN. Your organization is mostly responsible for this requirement, rather than the machine. You must: • Disable split tunneling in the settings of remote devices (such as laptop computers, smartphones, and tablets) that connect from outside via a VPN. • Detect the split tunneling of remote devices (or the setting that allows split tunneling) and prohibit connection if a device is using split tunneling.	N/A	N/A	Prevent remote devices from simultaneously establishing non-remote connections with the systems of your organization and communicating via some other connection to resources in external networks (such as split tunneling).
	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI (Controlled Unclassified Information) during transmission unless otherwise protected by alternative physical safeguards.	This requirement states that you must protect the data transmitted by systems in your organization (implement measures for preventing information leaks). The machine uses an encryption module that has received FIPS 140 certification. You can set the machine to use an algorithm that complies with FIPS 140-2 to encrypt the data during transmission. The machine also provides the TLS function and IPSec function to encrypt data during transmission.	**TLS Encrypted Communication** You can use TLS encrypted communication to prevent actions such as eavesdropping, tampering, and spoofing when accessing the machine from a computer or other device to exchange data. You can also set the machine to limit communications to those using an algorithm compliant with the FIPS 140-2 standard. **IPSec Communication** While TLS only encrypts data used on a specific application, such as a Web browser or an e-mail application, IPSec encrypts data at the IP packet level. This enables IPSec to offer a more versatile security system than TLS.	Configure <TLS Settings>. Enable <Use TLS> in the settings of each function/application. Also set the machine to verify the server certificate, depending on the environment. Enable <Use IPSec>. Enable <Format Encryption Method to FIPS 140-2>.	Implement encryption mechanisms to prevent unauthorized disclosure of CUI (Controlled Unclassified Information) during transmission. The machine provides the TLS function and the IPSec function to encrypt data during transmission. The TLS function enables you to select the encryption algorithm. Select an encryption algorithm that complies with FIPS 140-2.
	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	This requirement states that the communication sessions in the systems of your organization must terminate the network connection when a communication session is terminated or inactive for the specified period of inactivity. The machine provides a function that automatically terminates the network connection when a communication session is terminated or inactive for the specified period of inactivity.	The machine automatically terminates the network connection when a communication session is terminated or inactive for the specified period of inactivity. For example, the machine automatically terminates the session when the user performs no operations on the Remote UI for a certain period of time.	N/A	Configure the systems to terminate network sessions at the end of the network sessions or after a defined period of inactivity. The machine does not require you to configure settings regarding the timeout of network sessions.
	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	This requirement states that you must manage the encryption keys (cryptographic keys) of the systems in your organization. Your organization is mostly responsible for this requirement. You must manage and operate the encryption keys used for the encryption of CUI (Controlled Unclassified Information), according to the laws, executive orders, policies, directives, regulations, and standards that your organization must follow. The machine enables you to protect keys with TPM when the machine performs key management, such as generation and protection of encryption keys.	**TPM** You can securely store the encryption key (TPM key) in the TPM chip. The encryption key encrypts the following confidential information in the machine: • Passwords • Public key pairs for TLS communication • User certificates This enables you to prevent important information in the machine from leaking.	Configure <TPM Settings>.	Generate, discard, and manage encryption keys according to the security control policy that you must implement for the systems of your organization. Enable the TPM settings of the machine to manage encryption keys.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Derived (Derived Security Requirements)	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI (Controlled Unclassified Information).	This requirement states that you must use FIPS-validated products for protecting CUI (Controlled Unclassified Information) with encryption in the systems of your organization. The machine uses FIPS-validated products in TLS/IPSec encrypted communication and storage encryption.	**FIPS 140-2 Approved Algorithm** You can limit the encryption method of TLS communication to an algorithm that is compliant with the FIPS 140-2 standard. You do not need to configure the machine because the storage encryption function and IPSec function always operate with an algorithm compliant with the FIPS 140-2 standard.	Enable <Format Encryption Method to FIPS 140-2>.	You must use an encryption module compliant with the FIPS standard. Configure the machine so that an algorithm compliant with the FIPS 140-2 standard is used.
	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	This requirement states that you must prohibit device activation via remote access and notify users of device usage when using collaborative computing devices such as teleconferencing systems used by your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must: • Disable any functions for remotely enabling the camera or microphone. • Employ a tool for warning the user when the camera or microphone is enabled by the other party (such as an indicator light or a popup display).	N/A	N/A	Prohibit device activation via remote access and notify users of device usage when using collaborative computing devices such as teleconferencing systems used by your organization.
	3.13.13	Control and monitor the use of mobile code.	This requirement states that you must monitor the use of mobile code (such as JavaScript, ActiveX, and Flash) in the systems of your organization. The machine provides functions for controlling the mobile code executed in the Web Access function of the machine, such as JavaScript settings, and a function for controlling the use of the Web Access function itself.	**Web Access** You can use JavaScript as mobile code that operates in the Web Access function. You can also control the use of JavaScript.	Configure <Use JavaScript> in <Web Access>.	Monitor the use of mobile code (such as JavaScript, ActiveX, and Flash) in the systems of your organization. When enabling the Web Access function of the machine, control the use of mobile code using the JavaScript setting.
	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	This requirement states that you must manage and monitor VoIP used in the systems of your organization. Your organization is mostly responsible for this requirement, rather than the machine. The machine enables you to use a VoIP gateway in the IP Fax function.	N/A	N/A	Manage and monitor the use of VoIP.
	3.13.15	Protect the authenticity of communications sessions.	This requirement states that you must protect the authenticity of communication sessions established/used by the systems of your organization. The machine protects communication sessions with communication route encryption using TLS. The machine also decides the session ID at random to counter session ID attacks, such as session fixation attacks.	**TLS Encrypted Communication** You can use TLS encrypted communication to prevent actions such as eavesdropping, tampering, and spoofing when accessing the machine from a computer or other device to exchange data.	Configure <TLS Settings>. Enable <Use TLS> in the settings of each function/application. Also set the machine to verify the server certificate, depending on the environment.	Protect against threats such as man-in-the-middle attacks, session hijackings, and tampering with the communication sessions in the systems of your organization. The machine can increase resistance to these threats by encrypting the communication route using TLS. Therefore, enable TLS communication in the machine.
	3.13.16	Protect the confidentiality of CUI (Controlled Unclassified Information) at rest.	This requirement states that you must protect the confidentiality of the CUI (Controlled Unclassified Information) in the systems of your organization. The machine provides a storage encryption function for protecting the confidentiality of the data in the machine.	**Storage Data Encryption** The storage of the machine contains files in the Advanced Box and Mail Box, registered information in the Address Book, undeleted job data, and password information. By encrypting this data, you can prevent the information from being accessed without authorization.	N/A	Protect the confidentiality of the CUI (Controlled Unclassified Information) in the systems of your organization. The machine automatically encrypts the data in the storage using the storage data encryption function.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
				Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.14 SYSTEM AND INFORMATION INTEGRITY Basic (Basic Security Requirements)	3.14.1	Identify, report, and correct system flaws in a timely manner.	This requirement states that you must identify, report, and correct known vulnerabilities in the systems of your organization. Your organization is mostly responsible for this requirement. You must: 1. Gather/identify information on vulnerabilities in the systems of your organization. 2. Report to the person who is responsible for information security. 3. Swiftly correct vulnerabilities that have an impact on the systems. When Canon releases information regarding device vulnerabilities, swiftly report to the person in charge of information security at your organization and update the firmware as required. The machine provides functions for manually and periodically updating the firmware. These functions enable you to apply firmware updates that fix newly identified vulnerabilities.	N/A	N/A	Gather information on vulnerabilities affecting the devices and software that make up the systems of your organization and enact appropriate countermeasures. The machine provides functions for manually and automatically updating the firmware. Use these functions to update the firmware. Periodically access the Canon website to check for updated information on vulnerabilities.
	3.14.2	Provide protection from malicious code at designated locations within organizational systems.	This requirement states that you must protect the systems of your organization from malicious code (malware). The machine provides the following functions for detecting malware: • System verification functions (used during startup and operation) • Signature verification function (used when installing firmware and applications)	**Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Protect the systems of your organization from malicious code. The machine verifies digital signatures when a user installs a MEAP application or updates the firmware, to ensure that only legitimate software is installed. The machine provides the Protect Runtime System and Verify System at Startup functions for protecting the software embedded in the machine. Enable these functions.
	3.14.3	Monitor system security alerts and advisories and take action in response.	This requirement states that you must monitor and appropriately respond to warnings and advice from external organizations regarding the security of the systems in your organization. Your organization is mostly responsible for this requirement, rather than the machine. For example, you must: 1. Order a CSIRT in your organization to monitor warnings or advice from external organizations such as US-CERT. 2. Apply patches to fix vulnerabilities in your systems according to those warnings or advice, as required.	N/A	N/A	Receive outside information on vulnerabilities affecting the devices and software that make up the systems of your organization and enact appropriate countermeasures. You must receive vulnerability information from trusted external organizations such as US-CERT and JPCERT.
3.14 SYSTEM AND INFORMATION INTEGRITY Derived (Derived Security Requirements)	3.14.4	Update malicious code protection mechanisms when new releases are available.	This requirement states that you must swiftly update the malware detection function of systems in your organization. Your organization is mostly responsible for this requirement. For example, you must configure the antivirus software used in your organization to automatically update definition files and the detection engine. The machine provides system verification functions (used during startup and operation) for detecting malware.	**Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Swiftly update the systems of your organization when updates are available for the mechanisms that protect the systems from malicious code. For example, when the definition file of antivirus software has been updated, you must swiftly apply the update. The protection mechanism of the machine does not require that you update the virus definition file separately. Conduct firmware updates to ensure that the firmware is always the latest version.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.14 SYSTEM AND INFORMATION INTEGRITY Derived (Derived Security Requirements)	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	This requirement states that you must perform periodic scanning and real-time scanning of the systems and files in your organization. Your organization is mostly responsible for this requirement. For example, you must configure antivirus software to periodically scan the systems of your organization and conduct virus scans every time portable media such as a USB flash drive is used. The machine provides system verification functions (used during startup and operation) for detecting malware. These functions detect malware using a whitelisting method. The machine also provides a signature verification function (used when installing firmware and applications) to prevent the unauthorized installation or execution of malware.	**Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Perform periodic scans of the systems in your organization and real-time scans of files from external sources (portable media such as USB flash drives) as files are downloaded, opened, or executed. The machine performs digital signature verification, system verification at startup, and runtime system protection to scan software during installation, startup, and at runtime. Enable the Protect Runtime System and Verify System at Startup functions.
	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	This requirement states that you must monitor the systems in your organization to detect signs of attacks and potential threats. Your organization is mostly responsible for this requirement. You must use measures such as SIEM and IDS (Intrusion Detection System)/IPS (Intrusion Prevention System) to detect/monitor indicators of threats and counter them as required. The machine supports the actions of your organization to meet this requirement by providing the following functions: • Firewall Settings • Verify System at Startup • Protect Runtime System • Signature validation when installing firmware and MEAP applications • Audit Log settings These functions record the history and logs of problems (such as when unauthorized communication is blocked or tampering is detected). You can analyze the history and logs to detect indicators of attacks on the machine.	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses. You can check the latest 100 communications blocked by the firewall in the IP Address Block Log. You can export the history of blocked communications from the Remote UI in CSV format. **Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation. **Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following: • Operation date/time • User name • Type of operation • Type of function • Operation result You can use Syslog Send to send information to a SIEM (Security Information and Event Management) system. By linking with a SIEM system, you can manage various information that is analyzed from real-time alert information.	Configure <Firewall Settings>. Check <IP Address Block Log>. Enable <Verify System at Startup>. Enable <Protect Runtime System>. Enable the audit log function.	Monitor the systems of your organization including network traffic to detect attacks and indicators of potential attacks. You can retrieve the following logs: • History of communication blocked by the firewall • Results of digital signature verification during installation • Results of system verification at startup • Results of runtime system protection By analyzing these logs, you may be able to detect attacks or indicators of attacks.
	3.14.7	Identify unauthorized use of organizational systems.	This requirement states that you must identify unauthorized usage of the systems in your organization. Your organization is mostly responsible for this requirement, rather than the machine. You must use measures such as IDS (Intrusion Detection System)/IPS (Intrusion Prevention System), antivirus software, and SIEM to monitor the usage status of systems at your organization and identify (specify) unauthorized use. The machine supports the actions of your organization to meet this requirement by providing the following functions: • Firewall Settings • Verify System at Startup • Protect Runtime System • Signature validation when installing firmware and MEAP applications	**Firewall** A firewall is a system that prevents unauthorized access, attacks, and intrusions into the local area network from outside networks. In your network environment, you can block access from outside parties thought to be dangerous by limiting communication from specific external IP addresses. You can check the latest 100 communications blocked by the firewall in the IP Address Block Log. You can export the history of blocked communications from the Remote UI in the CSV format. **Verify System at Startup** This function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation. **Audit Log Function** You can use logs to check/analyze how the machine is used. Logs record information including the following:	Configure <Firewall Settings>. Check <IP Address Block Log>. Enable <Verify System at Startup>. Enable <Protect Runtime System>. Enable the audit log function.	Identify the unauthorized or unapproved use of the systems in your organization. You can retrieve the following logs: • History of communication blocked by the firewall • Results of digital signature verification during installation • Results of system verification at startup • Results of runtime system protection By analyzing these logs, you may be able to detect unauthorized use of the systems in your organization.

NIST SP 800-171 rev2 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
			• Audit Log settings These functions record the history and logs of problems (such as when unauthorized communication is blocked or tampering is detected). You can analyze the history and logs to identify (detect) unauthorized usage of the machine.	• Operation date/time • User name • Type of operation • Type of function • Operation result You can use Syslog Send to send information to a SIEM (Security Information and Event Management) system. By linking with a SIEM system, you can manage various information that is analyzed from real-time alert information.		

5.2 NIST SP 800-172 Requirement Compatibility Chart

This table is provided in support of “Guidance for Canon Printer and Multifunction Device Functionality in Support of NIST SP 800-171 and NIST SP 800-172”, version 1.00, March 2023.
Use this table when configuring the settings to respond to each requirement in the guideline.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.1 ACCESS CONTROL Enhanced Security Requirements	3.1.1e	Employ dual authorization to execute critical or sensitive system and organizational operations.	This requirement states that you must use dual authorization when operating a "critical or sensitive system". You must identify/define "critical or sensitive systems" in advance. Normally, "critical or sensitive systems" refer to systems such as the financial systems of banks and the control systems of infrastructure. You must also employ dual authorization. It requires the approval of two authorized individuals to execute certain commands, actions, or functions on a "critical or sensitive system", as defined by your organization, including the machine. For example, when your organization updates a "critical or sensitive system", you must ensure that the update is only allowed upon obtaining authorization from the main administrator and a sub administrator. You must also require dual authorization when using the privileged commands of a "critical or sensitive system".	N/A	N/A	Identify/define what constitutes a "critical or sensitive system" in advance. You must employ dual authorization. It requires the approval of two authorized individuals to execute certain commands, actions, or functions on a "critical or sensitive system". Therefore, determine whether you have any "critical or sensitive systems", and if you do, require dual authorization when using the functions of those systems.
	3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	This requirement states that you must limit access to the systems of your organization to only the devices and systems managed by your organization. Your organization is mostly responsible for this requirement. You must manage the devices in your organization so that devices infected with malware or other compromised devices cannot access the systems in your organization. In addition, you can adopt technical measures such as a device authentication function that requests authentication when a device accesses a system. For the device authentication of the machine, you can use RADIUS authentication.	**IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client. When a device is connected to a network that has adopted IEEE 802.1X and starts communication, the network first verifies the device. The network checks the device by querying the RADIUS server to authenticate the device. The LAN switch (access point) blocks communication requests from the device until the device is authenticated.	Enable <IEEE 802.1X Settings>.	Investigate a method for determining whether the entities that access systems (including the machine) are system components of your organization. Also, investigate a method for verifying that the machine is a system component of your organization when the machine accesses a system. For example, you can perform device authentication, limit devices by MAC address or IP address, or require RADIUS authentication. For the machine, you can use RADIUS authentication.
	3.1.3e	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	This requirement states that you must use a secure information transfer method defined by your organization to control the flow of information between security domains on the systems of your organization. Your organization is mostly responsible for this requirement. First, you must distinguish between domains that include CUI (Controlled Unclassified Information) and domains that do not include CUI. This includes the domain of the machine. Next, you must define the method used for transferring information between domains that include CUI and domains that do not include CUI. For example, you can use a firewall to separate domains that include CUI and domains that do not include CUI. You can control the flow of information (CUI) between domains using a site-to-site VPN via a corporate WAN. You can also separate domains by setting a file server for retaining CUI and implementing appropriate access control to that file server.	N/A	N/A	Define a secure method for transferring information in your organization. Also, distinguish between domains that include CUI and domains that do not include CUI. Then, control the flow of information to/from the domains that include CUI using a secure method for transferring information. Examples of secure methods for transferring information include VPNs and firewalls.
3.2 AWARENESS AND TRAINING Enhanced Security Requirements	3.2.1e	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	This requirement states that you must provide employees of your organization with training on advanced persistent threats (APTs). Your organization is mostly responsible for this requirement. An APT is a type of targeted attack, which involves an advanced and prolonged attack. APTs are often conducted systematically. As with regular targeted attacks, APTs are often triggered by employees carelessly accessing suspicious e-mail or websites. For example, you must provide employees with training that describes specific examples of APTs and instructs employees not to open suspicious e-mail or websites in all systems including the machine. Because the threat of APTs is evolving on a daily basis, you must update the content of the training when the APT trends change or new attack methods surface. Alternatively, you must periodically review and update the content of the training.	N/A	N/A	Provide employees with training on APTs. In the training, describe specific examples of APTs and instruct employees not to open suspicious e-mail or access suspicious websites that may cause exposure to APTs. Also periodically review and update the content of the training at the frequency defined by your organization or when APT trends change or new attack methods surface. Additionally, define the frequency for conducting training and the frequency for reviewing the content of the training.
	3.2.2e	Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	This requirement states that you must provide the employees of your organization with role-based practical training and provide your employees and their superiors with feedback on the training results. Your organization is mostly responsible for this requirement. For example, create threat scenarios that suppose APTs on systems including the machine, and provide scenario-based security training to employees. In the practical training, conduct actual targeted attacks on target employees via a method such as e-mail so that employees can experience an incident response, such as what to do when they open a suspicious e-mail. Also evaluate the response of each employee and share feedback with the employees and their superiors.	N/A	N/A	Create a threat scenario for an APT and conduct training for building awareness according to that scenario, for example via drills that send a fake suspicious e-mail to employees. After conducting training, evaluate the response of each employee and share feedback with the employees and their superiors.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.4 CONFIGURATION MANAGEMENT Enhanced Security Requirements	3.4.1e	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	This requirement states that you must perform configuration management on the devices managed by your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. First, you must define the baseline configuration of components (hardware, software, and firmware) that make up the devices and systems in your organization. Then, gather the configurations of devices and systems in your organization, and manage them in a trusted repository. You must build a baseline configuration comprising the components that you can obtain (download) from trusted sources. The machine supports the actions of your organization to meet this requirement by providing the following functionality: • Automatically updating firmware periodically • Displaying device information • Displaying information on installed applications	**Scheduled Firmware Updates** You can configure the Scheduled Update function to set the machine to periodically check for new firmware and automatically update the firmware. **MEAP Application Management** You can display SMS in the Remote UI to manage applications.	Configure <Scheduled Update Settings>. Manage applications using [Service Management Service] in the Remote UI.	Build, document, and manage baseline configurations based on the system component information of devices. You must manage baseline configurations in a trusted repository. You must also periodically review baseline configurations. Before changes are made to baseline configurations, you must: 1. Analyze the impact that those changes will have on security. 2. Authorize the changes. When building the system components of devices, obtain (download) them from a trusted source. For example, when installing firmware and applications to the machine, use official Canon firmware and applications. Do not download software from third parties of an uncertain origin. When building the baseline configurations, you can use the device information view function of the machine to obtain information on the system components.
	3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	This requirement is related to configuration management on the devices that are managed by your organization. It states that you must automatically correct (rectify) the components of devices that differ from the defined baseline configuration. For example, build systems (adopt tools) that can detect when devices and systems differ from the baseline configuration in a repository that gathers and manages the configurations of devices in your organization. When a device or system that differs from the baseline configuration is detected, you must: • Manually or automatically delete unnecessary components • Apply update patches • Change settings Alternatively, you must isolate devices with a configuration that differs from the baseline configuration to prevent any potential impact from affecting other devices (for example, by spreading malware). The machine provides the Verify System at Startup function and the Protect Runtime System function to automatically detect and disable unauthorized components. These functions enable you to automatically isolate (disable) unauthorized components of the machine so that they do not affect other systems in your organization.	**Verify System at Startup** The Verify System at Startup function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Use an automated mechanism to detect deviation from the baseline configuration, such as incorrectly configured system components and unauthorized system components. For example, build a system for automatically gathering and managing information on the system components in your organization. That system should be in a repository that gathers and manages the device configurations in your organization. Then, compare the collected information on device system components with the baseline configuration in the repository of your organization so that you can detect deviation from the baseline configuration. In addition, you must define the security response to these detected deviations. For example, the security response should include the following: • Automatically deleting unnecessary system components • Requesting a system administrator to delete unnecessary system components Isolate devices that are detected as deviating from the baseline configuration so that they do not affect other systems in your organization. The Verify System at Startup function and the Protect Runtime System function of the machine enable you to automatically detect and isolate (disable) unauthorized components of the machine.
	3.4.3e	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	This requirement is related to configuration management on the devices that are managed by your organization. It states that you must use automated management tools in particular to maintain system components in an appropriate state. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you can use an automated tool to gather and manage component information in a repository. The information should include the components of the devices that are managed by your organization, such as the version number of their operating system. When a vulnerability is discovered in a component, you should: 1. Refer to the component information in the repository. 2. Schedule to apply the latest patch to the devices that contain the vulnerable component. The machine supports the actions of your organization to meet this requirement by providing a function for automatically updating firmware periodically.	**Scheduled Firmware Updates** You can configure the Scheduled Update function to set the machine to periodically check for new firmware and automatically update the firmware.	Configure <Scheduled Update Settings>.	Use an automated mechanism to maintain the appropriate states of system component configurations in your organization. You must ensure that system components are updated, complete, accurate, and available for immediate use. For example, build a system for automatically gathering and managing information on the system components in your organization. That system should be in a repository that gathers and manages the device configurations in your organization. When a vulnerability is discovered in a component, you should: 1. Refer to the component information in the repository. 2. Schedule to apply the latest patch to the devices that contain the vulnerable component. You can use the Scheduled Update function of the machine to automatically update the firmware of the machine.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.5 IDENTIFICATION AND AUTHENTICATION Enhanced Security Requirements	3.5.1e	Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	This requirement states that you must identify and authenticate systems in your organization when the system connects to a network, using replay-resistant bidirectional authentication. First, you must define the systems that this requirement applies to. Then, you must authenticate the defined systems using a replay-resistant authentication method such as TLS server/client authentication when connecting to a network. You must also manage the encryption keys used for authentication via a secure method such as TPM (Trusted Platform Module) or TEE (Trusted Execution Environment). If your organization has defined the machine as a system to which this requirement applies, you can control the machine using IEEE 802.1X authentication. This allows the machine to connect to a network only when replay-resistant bidirectional authentication has verified the machine. The machine also includes a TPM to securely manage the information used in authentication.	**IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client. **TPM** You can safely store the encryption key (TPM key) in the TPM chip. The encryption key encrypts the following confidential information in the machine: • Passwords • Public key pairs for TLS communication • User certificates Encryption keys enable you to prevent important information in the machine from leaking.	Enable <IEEE 802.1X Settings>. Configure <TPM Settings>.	For the network connection, adopt replay-resistant bidirectional authentication in the systems and system components defined by your organization. For example, you can use TLS as bidirectional authentication that is replay resistant. Also, you must protect the encryption keys used for authentication in secure storage. You can set the IEEE 802.1X authentication function of the machine. It allows the machine to connect to the network of your organization only when bidirectional authentication has verified the machine. To use this function, you must build an authentication network that supports IEEE 802.1X. You can also set the TPM function of the machine to securely manage the information used in IEEE 802.1X authentication.
	3.5.2e	Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	This requirement states that you must perform automated password management using a mechanism such as a password manager. This requirement applies to the systems and system components that do not support multifactor authentication or complex account management (such as separate system accounts for each user and logging). For example, you can use a password manager to automatically perform generation, rotation, management, and storage of separate strong passwords for users and device accounts. A router has a single administrator account, but an organization usually has multiple network administrators. This means that multiple administrators often share accounts (passwords), which can cause problems with access management and accountability. A password manager uses technology such as automatic password rotation (in this example, for a router password). It grants specific users temporary access to a device by checking out a temporary password and then checking in that password to terminate access. The password manager also records a log of these processes. In addition, the password manager strongly protects the passwords that it manages. You do not need to prepare a separate tool such as a password manager for the machine because the machine includes user account management and access control functions. The machine also records the operations that each logged-in user performs on the machine.	**Personal Authentication Management** You can manage the users of the machine with an authentication application (login service) to maintain a higher level of security and enable efficient machine operation.	Configure <User Management>.	Conduct password management if user authentication functions such as multifactor authentication and complex account management are not available for the systems in your organization. The password management should be automated by a password manager that meets the following conditions: • Automatically performs generation, rotation, management, and storage of separate strong passwords for users and device accounts • Strongly protects and manages the passwords You do not need to prepare a separate tool such as a password manager for the machine because the machine includes user account management and access control functions.
	3.5.3e	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	This requirement states that you must manually or automatically prohibit system components from connecting to the systems of your organization unless they are: • Known • Authenticated • In a properly configured state • In a trusted profile Because the machine supports IEEE 802.1X, you can use IEEE 802.1X authentication to ensure that the machine can connect to the network of your organization only when the machine is authenticated. Furthermore, you can use IEEE 802.1X to ensure that only authenticated devices can connect to the machine via a network. The machine also provides the Verify System at Startup function and the Protect Runtime System function to verify that the system components of the machine are appropriately configured.	**IEEE 802.1X Support** The machine can connect to networks that have adopted IEEE 802.1X authentication as a client. **Verify System at Startup** The Verify System at Startup function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <IEEE 802.1X Settings>. Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Manually or automatically prohibit system components from connecting to the systems of your organization unless they are: • Known • Authenticated • In a properly configured state • In a trusted profile You can set the IEEE 802.1X authentication function of the machine to allow the machine to connect to the network of your organization only when the machine is authenticated. You can also use IEEE 802.1X to enable only authenticated devices to connect to the machine via a network. To enable the IEEE 802.1X authentication function, you must build an authentication network that supports IEEE 802.1X. You must define the devices managed by your organization, including the machine, and configure an authentication server (RADIUS server) to allow only the managed devices to access a network. The Verify System at Startup function and the Protect Runtime System function of the machine enable you to verify that the system components of the machine are appropriately configured.
3.6 INCIDENT RESPONSE Enhanced Security Requirements	3.6.1e	Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].	This requirement states that you must establish an SOC (Security Operation Center) and maintain and operate the SOC for the period defined by your organization. Your organization is mostly responsible for this requirement. You must operate an SOC to continuously (for the period defined by your organization) monitor the systems and networks in your organization, including the machine. The SOC continuously monitors and analyzes the logs of the systems and networks in your organization, in order to detect signs of security incidents in your organization. The log analysis of the SOC also supports the duties of a CSIRT when an incident occurs. Your organization may have a unique SOC, or use the SOC service of an external vendor.	N/A	N/A	Establish an SOC (Security Operation Center) that continuously monitors the systems and networks in your organization and detects incidents. Also specify the period of monitoring, for example: 24 hours a day, 365 days a year. The SOC continuously monitors and analyzes the logs of the systems and networks in your organization. The log analysis of the SOC also supports the duties of a CSIRT (Computer Security Incident Response Team) when an incident occurs.
	3.6.2e	Establish and maintain a cyber incident response team that can be deployed by the organization within [Assignment: organization-defined time period].	This requirement states that you must establish a CSIRT (Computer Security Incident Response Team) that can be deployed within the period defined by your organization, and maintain the team. Your organization is mostly responsible for this requirement. You must establish a CSIRT that is permanent or can be deployed within the defined period. The CSIRT is a team of experts that assess, document, and respond to cyber incidents in your organization. The team swiftly recovers the systems (including the machine) in your organization from incidents, and implements the necessary controls to avoid future incidents.	N/A	N/A	Establish a CSIRT (Computer Security Incident Response Team) that can be deployed within the period defined by your organization. The CSIRT is a team of experts that assess, document, and respond to cyber incidents in your organization. The team swiftly recovers the systems in your organization from incidents, and implements the necessary controls to avoid future incidents.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.9 PERSONNEL SECURITY Enhanced Security Requirements	3.9.1e	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	This requirement states that you must conduct enhanced personnel screenings defined by your organization of employees with access to systems that include CUI. You must also continuously rescreen those employees at the frequency defined by your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must conduct background screening that is defined by your organization for the purpose of protecting the security of CUI, in addition to the regular personnel screenings. The screening activities reflect applicable laws, executive orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.	N/A	N/A	Conduct enhanced personnel screenings defined by your organization of employees with access to systems that include CUI. Rescreen employees that have already been screened, at the frequency defined by your organization, to confirm that the employees meet the required personnel screening standards. Personnel screenings include, for example, background screening for the purpose of protecting the security of CUI, in addition to the regular personnel screenings. The screening activities reflect applicable laws, executive orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.
	3.9.2e	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	This requirement states that if adverse information develops or is obtained about employees with access to CUI, you must protect CUI from those employees. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must immediately take actions to protect the CUI while the adverse information is resolved, if there is a case that meets both of the following conditions: • Adverse information develops or is obtained about employees that have access to CUI. • There is doubt about whether those employees should have continued access to systems containing CUI.	N/A	N/A	If adverse information develops or is obtained about employees with access to CUI, you must protect CUI from those employees. For example, you must protect the CUI by stopping the access privileges of employees while the adverse information is being resolved, if there is a case that meets both of the following conditions: • Adverse information develops or is obtained about employees that have access to CUI. • There is doubt about whether those employees should have continued access to systems containing CUI.
3.11 RISK ASSESSMENT Enhanced Security Requirements	3.11.1e	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	This requirement states that you must utilize threat intelligence as part of the risk assessments of your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. You must consider and adopt threat intelligence to use for risk assessment.	N/A	N/A	Consider using a threat intelligence service in order to obtain threat intelligence. Based on the obtained threat intelligence, build a system for: • Defining system security requirements • Developing the system and security architectures • Selecting security solutions • Monitoring (including threat hunting) • Performing recovery
	3.11.2e	Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.	This requirement states that you must conduct threat hunting on the systems defined by your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, actively and assertively detect, track, and respond to threats via the following measures: • Analyzing audit logs for the systems defined by your organization at the frequency defined by your organization • Utilizing threat intelligence and honeypots	N/A	N/A	Conduct cyber threat hunting activities in order to check the systems defined by your organization for traces of intrusion. More specifically, actively and assertively detect, track, and respond to threats by analyzing audit logs and utilizing threat intelligence and honeypots. Also, define the indicators for conducting cyber threat hunting activities, or the frequency for conducting cyber threat hunting.
	3.11.3e	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.	This requirement states that you must use advanced automation and analysis functions for supporting the CSIRT and SOC of your organization to predict and identify risks. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. The CSIRT and SOC analyze an enormous amount of system logs and network logs. To help them efficiently predict and identify the risks to systems in your organization, utilize an AI data analysis tool from an external vendor.	N/A	N/A	Employ advanced automation and analytics capabilities for identifying and predicting risks to systems including the machine. For example, implement the following solutions: • Automated workflow operations • Automated threat discovery and response
	3.11.4e	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	This requirement states that you must document or reference the following information in a system security plan: • The security solution selected by the organization • The rationale for the security solution • Risk determination Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must refer to NIST SP 800-18 to formulate a system security plan that includes the above information.	N/A	N/A	Formulate a system security plan that includes the following information: • The security solution selected by the organization • The rationale for the security solution • Risk determination For example, document the following information and enable it to be referenced from the system security plan: • The contract for adopting the security solution • The system configuration • Threat analysis results • Risk determination results
	3.11.5e	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	This requirement states that you must conduct an effectiveness evaluation of security solutions at the frequency defined by your organization, based on threat intelligence. The security solutions should respond to the risks that the systems of your organization may face. Your organization is mostly responsible for this requirement. For example, you must periodically assess the security solution for protecting the systems of your organization based on threat intelligence, and change the security solution as required.	N/A	N/A	Measure the effect of the adopted security solution. Periodically conduct this measurement at a defined frequency, because new methods of attack and new vulnerabilities may be discovered as time goes by.
	3.11.6e	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	This requirement states that you must assess, respond to, and monitor supply chain risks associated with the systems of your organization and their components. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must reference standards such as NIST SP 800-161 to manage supply chain risks.	N/A	N/A	Identify and monitor supply chain risks. If changes occur in a supply chain, conduct another risk assessment.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.11 RISK ASSESSMENT Enhanced Security Requirements	3.11.7e	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency].	This requirement states that you must develop and update a risk management plan for supply chain risks associated with the systems of your organization and their components. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must reference standards such as NIST SP 800-161 to develop a plan for managing supply chain risks and update the plan at the timing defined by your organization.	N/A	N/A	Define a frequency for updating the plan for managing supply chain risks, and maintain the plan.
3.12 SECURITY ASSESSMENT Enhanced Security Requirements	3.12.1e	Conduct penetration testing [Assignment: organization-defined frequency], leveraging automated scanning tools and ad hoc tests using subject matter experts.	This requirement states that you must conduct penetration tests on the systems and solutions of your organization, at the frequency defined by your organization. Your organization is mostly responsible for this requirement. For example, you must conduct penetration tests to assess the vulnerabilities of systems and solutions in your organization, including the machine, at the frequency defined by your organization. You can carry out penetration tests using an automated vulnerability scanner or internal/external security expert (penetration tester).	N/A	N/A	Conduct penetration tests on the systems of your organization at the frequency defined by your organization. Penetration tests enable you to identify the weaknesses and vulnerabilities of the systems in your organization to assist you in making improvements to the security strategy of your organization. You can conduct penetration tests via: • An automated vulnerability scan tool • A security expert (penetration tester) in your organization • A trusted third party organization
3.13 SYSTEM AND COMMUNICATIONS PROTECTION Enhanced Security Requirements	3.13.1e	Create diversity in [Assignment: organization-defined system components] to reduce the extent of malicious code propagation.	This requirement states that you must create diversity in system components defined by your organization to reduce the extent of malicious code propagation. You must define the system components that this requirement applies to in advance. Methods for creating diversity include the following: • Using antivirus software from multiple software vendors • Adopting multiple operating systems • Using ASLR (Address Space Layout Randomization) The machine provides an ASLR function for supporting the actions of your organization to meet this requirement. The ASLR function enables you to reduce the propagation of malicious code. The machine also allows you to generate diversity because multiple operating systems are installed on the machine.	**ASLR** Address Space Layout Randomization	N/A	Diversify the system components defined by your organization to prevent the propagation of malicious code. Even if an attack has worked on a certain system component, you can reduce the success rate of the same attack on the other system components. This can be achieved by creating diversity in your system components. For example, you can adopt security products (such as antivirus software) from various companies in the systems of your organization in order to diversify your system components. Even if an attack that utilizes a vulnerability in the security products of a particular company succeeds, the impact of that attack will be limited to those system components. The possibility of the attack affecting system components that are protected by the products of other companies will be reduced. The machine provides an Address Space Layout Randomization (ASLR) function for creating diversity. By creating diversity, even if an attack has worked on a certain system component, you can reduce the success rate of the same attack on the other system components. The machine also allows you to generate diversity because multiple operating systems are installed on the machine.
	3.13.2e	Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [Assignment: organization-defined changes and frequency of changes by system and system component].	This requirement states that you must perform randomization on the attack interfaces (attack surfaces) of the systems and system components in your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you must change the IP addresses and DNS names of systems that are disclosed externally on a random basis to make it more difficult for attackers to continuously mount attacks.	N/A	N/A	Adopt random elements defined by your organization in systems that may become attack interfaces. You can incorporate random elements to hinder the prediction of attack interfaces. The random elements can also affect the planning and execution of attacks. For example, if you select time as an element to randomize, you can take the following measures: • Changing the IP address and DNS name of the machine at random times of day • Randomly shortening the period that credentials are valid Other measures include the following: • Changing the browser and search engine at random times of day • Rotating the roles and responsibilities of employees at your organization
	3.13.3e	Employ [Assignment: organization-defined technical and procedural means] to confuse and mislead adversaries.	This requirement states that you must use technical and procedural means to confuse and mislead attackers. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, you can use honeypots to provide attackers with fake targets and false information in order to confuse and mislead attackers.	N/A	N/A	Adopt technical and procedural elements defined by your organization in the systems of your organization to confuse and mislead attackers. By adopting technical and procedural elements, you can: • Delay attacks • Reduce the affected scope of attacks • Prevent information leaks For example, take the following measures: • Set up a honeypot in the systems of your organization to lead attackers to a fake target. • Intentionally embed false information in the data handled by your organization to mislead attackers.
	3.13.4e	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	This requirement states that you must protect CUI on the systems and system components of your organization via either or both of the following measures: • One or more physical isolation techniques defined by your organization • One or more logical isolation techniques defined by your organization Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. You must define physical and/or logical isolation methods for protecting systems. Examples of logical isolation methods include CUI data tags, DRM, and VLAN. Examples of physical isolation methods include the installation of CUI data servers in rooms subject to entry management (where they are not connected to a network).	N/A	N/A	Adopt the physical/logical isolation techniques defined by your organization in the systems or system components of your organization to protect information including CUI. By adopting isolation techniques, you can implement additional security measures for system components that handle CUI, and limit the information flow of CUI. Examples of logical isolation techniques include the following: • Tagging CUI data • Using DRM to monitor and limit the flow of CUI • Isolating CUI on hosts using virtual machines or VLAN Examples of physical isolation techniques include the installation of CUI data servers in rooms subject to entry management (where they are not connected to a network).
	3.13.5e	Distribute and relocate the following system functions or resources [Assignment: organization-defined frequency]: [Assignment: organization-defined system functions or resources].	This requirement states that you must distribute the locations of processing activities or storage sites defined by your organization, and reallocate them periodically. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, periodically change IP addresses, DNS names, and the network topology, and perform fragmentation.	N/A	N/A	Distribute the locations of processing activities or storage sites defined by your organization, and reallocate them at the frequency defined by your organization. By distributing and reallocating the locations of processing activities and storage sites, you can make it more difficult for attackers to set a target. You can also minimize the range affected by breaching. For example, you can periodically change IP addresses, DNS names, and the network topology to hinder the targeting of an attacker. You can also prevent breaches from affecting all data by adopting fragmentation to distribute data processing.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
3.14 SYSTEM AND INFORMATION INTEGRITY Enhanced Security Requirements	3.14.1e	Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	This requirement states that you must use RoT (Root of Trust) mechanisms or digital signatures to verify the integrity of software which you define as security critical or essential. You must define the software of the systems in your organization that is security critical or essential in advance. Secure boot is one example of a method for verifying the integrity of the software that is security critical or essential in the systems of your organization. The machine provides the Verify System at Startup function to verify the integrity of firmware and applications at startup using digital signature verification based on RoT mechanisms. The machine also provides the Protect Runtime System function to prevent unauthorized modification to programs or the execution of unauthorized programs using RoT-based software while the machine is running. Furthermore, the machine verifies digital signatures when a user installs a MEAP application or updates the firmware, to ensure that only legitimate software is installed.	**Verify System at Startup** The Verify System at Startup function verifies the integrity of the firmware, system, and MEAP applications in the machine at startup. **Protect Runtime System** The Protect Runtime System function can improve system reliability by preventing unauthorized modification to programs and the execution of unauthorized programs while the machine is in operation.	Enable <Verify System at Startup>. Enable <Protect Runtime System>.	Verify the integrity of software that is defined as security critical or essential by your organization, using RoT-based mechanisms or digital signatures. First, you must define the software of the systems in your organization that is security critical. Next, you must investigate a method for verifying the integrity of the defined software. The machine verifies digital signatures when a user installs a MEAP application or updates the firmware, to ensure that only legitimate software is installed. The machine also provides the Protect Runtime System and Verify System at Startup functions for protecting the software embedded in the machine. Enable these functions.
	3.14.2e	Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.	This requirement states that you must continuously monitor the systems and system components of your organization for abnormal or suspicious behavior. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, use a commercial UEBA (User and Entity Behavior Analytics) tool to monitor abnormal or suspicious behavior in the systems of your organization via AI or machine learning.	N/A	N/A	Continuously monitor the systems and system components of your organization for abnormal or suspicious behavior. First, you must identify the target systems and system components in your organization to monitor. Next, you must investigate a method for monitoring the behavior of each target.
	3.14.3e	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	This requirement states that you must ensure that the systems and system components defined by your organization are included in the scope of the specified enhanced security requirements. Alternatively, you must ensure that those systems and system components are segregated in purpose-specific networks. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. For example, check whether the functions and settings of the systems in your organization meet the enhanced security requirements of NIST SP 800-172. For systems that do not meet the requirements of NIST SP 800-172, check whether the systems are isolated or separated from the Internet to make those systems more difficult to attack.	N/A	N/A	Ensure that the systems and system components defined by your organization are included in the scope of the specified enhanced security requirements. Alternatively, you can ensure that those systems and system components are segregated in purpose-specific networks. You can perform network isolation using technologies such as encryption, authentication, and access control.
	3.14.4e	Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].	This requirement states that you must refresh the systems and system components defined by your organization from a known trusted state, at the frequency defined by your organization. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. First, you must define the systems and system components that this requirement applies to and define the frequency for refreshing. Then, for example, you must reimage (update or restore) the target systems and system components on a repository at the frequency defined by your organization. The reimaging of system components includes the reinstallation of firmware, operating systems, and applications from a known, trusted source. You must also periodically verify the reliability and integrity of the repository. This enables you to suppress the impact of and spread of attacks from the APT. The machine supports the actions of your organization to meet this requirement by providing a function for automatically updating firmware periodically.	**Scheduled Firmware Updates** You can configure the Scheduled Update function to set the machine to periodically check for new firmware and automatically update the firmware.	Configure <Scheduled Update Settings>.	Refresh the systems and system components defined by your organization, at the frequency defined by your organization, from a known trusted state. First, you must identify the target systems and system components in your organization. Next, determine a suitable frequency for refreshing the targets. The machine provides a function for periodically updating the firmware, which enables you to automate firmware updates.
	3.14.5e	Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.	This requirement states that you must check the persistent storage locations in your organization at a frequency defined by your organization, and delete any unnecessary CUI. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. First, you must define the frequency for checking persistent storage. Then, for example, check the CUI stored on persistent storage such as hard disk drives at the frequency defined by your organization, and delete unnecessary CUI that is not used. You can protect the following CUI by storing it in offline storage to protect it from the threat of unauthorized access through a network: • Information that you do not currently use but may use in the future • Information that you are obliged to retain	N/A	N/A	Check the persistent storage locations in your organization at a frequency defined by your organization, and delete any unnecessary CUI. You must determine the frequency for checking each target storage location.
	3.14.6e	Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.	This requirement states that you must use threat indicator information and effective mitigations obtained from external organizations defined by your organization to perform intrusion detection and threat hunting. Your organization is mostly responsible for this requirement. The requirement does not apply to the machine. You must define the external organizations (such as JPCERT, US-CERT, and CERT/CC) to use as sources for threat information (including threat details and countermeasures/mitigations) in advance. Then, for example, you must: 1. Obtain information regarding threats from JPCERT. 2. Request that your SOC (Security Operation Center) utilize the obtained information to perform intrusion detection and threat hunting in the systems of your organization.	N/A	N/A	Use threat indicator information and effective mitigations obtained from external organizations defined by your organization to perform intrusion detection and threat hunting.
3.14 SYSTEM AND INFORMATION INTEGRITY Enhanced Security Requirements	3.14.7e	Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques].	This requirement states that you must verify the correctness of software defined as security critical or essential by your organization using verification methods and techniques defined by your organization. You must implement the following in advance: 1. Define the software that is security critical or essential. 2. Define a method for verifying that the defined software is correct. If the software defined as security critical or essential is developed in-house, you must use a verification method defined by your organization to verify that the in-house software is correct. If the software is developed by an external vendor, this requirement applies to that vendor. However, as mentioned in the discussion found in NIST SP 800-172, it normally takes time to verify the correctness of software, so verification is not performed on most commercial operating systems and applications. Verification may only be performed on extremely limited applications, such as the verification of encryption protocols.	**FIPS 140-2 Compliance** The encryption algorithm of the machine complies with the FIPS 140-2 Level 2 standard for information processing that is formulated by the federal government of the United States. The machine can use this encryption technology for TLS encrypted communication, IPSec communication, and storage data encryption functions. **Common Criteria (ISO/IEC 15408) Certification** This machine is compliant with IEEE Std 2600^{TM}-2008 (IEEE 2600), an international standard concerning information security for multifunctional peripherals and printers. Furthermore, the machine has received third-party evaluation to confirm that its security functions comply with IEEE 2600, and has achieved Common Criteria (ISO/IEC 15408) certification.	N/A	Verify the correctness of software defined as security critical or essential by your organization using verification methods and techniques defined by your organization. For the machine, you can verify the correctness of components by confirming the following information: • The cryptographic module in the machine is compliant with FIPS 140. • The machine itself has achieved Common Criteria (ISO/IEC 15408) certification. The machine employs a cryptographic module that is compliant with the FIPS 140 standard, and the machine itself has achieved Common Criteria (ISO/IEC 15408) certification that complies with IEEE 2600.

NIST SP 800-172 Requirements			Relationship between the Requirements and Canon Printers/Multifunction Devices This column gives an overview of the requirements and describes the corresponding functions of Canon printers/multifunction devices. The term "the machine" refers to Canon printers/multifunction devices. Even if the machine is not directly related to a requirement, its functions are mentioned if those functions can support the actions required for your organization to meet cybersecurity guidelines.	Functionality of Canon Printers/Multifunction Devices		Response of Organization (Your Response) This column indicates the actions required by your organization in order to meet the requirement. The term "the machine" refers to Canon printers/multifunction devices. The actions described here are examples and other methods for meeting the requirements may exist.
Family	ID	Requirement		Related Functions This column indicates the functions of the Canon printers/multifunction devices related to the requirement. It includes functions that support the cybersecurity-related actions of your organization. "N/A" refers to requirements unrelated to the Canon printers/multifunction devices.	Corresponding Settings This column indicates the settings required for using the related functions.	
			The machine employs encryption modules that are compliant with the FIPS 140 standard as its critical encryption modules for security. These encryption modules are tested by third party testing organizations to verify their correctness, such as the implementation of the cryptographic algorithm, and are certified to comply with FIPS 140. Furthermore, the machine has received third-party evaluation to confirm that its security functions comply with IEEE 2600, a security standard for printers/multifunction devices, and has achieved Common Criteria (ISO/IEC 15408) certification.			

0323-VMLEGNISTWP-PDF-IH

Canon
usa.canon.com