Question Category	
Preliminary	Questions that examine basic c
Identity and Access Management (IAM)	Questions that examine identity
Device Configuration & Security	deployment of devices across t
Security controls to maintain CIA	organizational assets and data.
Organizational Governance & Training	ensure security policies are imp
Vulnerability Management (VM)	Questions that examine an orga
Supply Chain Risk Management (SCRM)	vendor security.
Incident Response (IR)	Questions that examine an orga

categories for organizations to complete as they navigate through the
fundamental cybersecurity practices that are expected to be the found

Description
yber hygiene
and access management polices and procedures.
he organization.
lemented and understood.
anization's VM policies and procedures.
anization's IR policies and procedures.

ReadySetCyber questionnaire. These questions assess
lations of any information security program, and help to

QID	Questions	Definitions
1	Are you a small business?	Small businesses are those with less than 100 employees
	Do you employ others than yourself?	Include anyone who has access to your data or devices, paid or unpaid.
	Is your work password different from your personal password?	
	Is your work password a strong password?	Strong passwords are longer than 8 characters, a combination of numbers, letters, and characters, with at least one capital and lower case letter
	Do you have multi-factor authentication enabled on your work computers and systems?	Multi-Factor Authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.
	Do you regularly back up your important work data?	
	What methods do you backup your data?	
	Is automatic backup enabled?	
	Can you quickly access your backed up data?	
	What type of devices do you use for work?	

Which of the following security features do you have enabled? (See list provided)	
Do you use a combination of a firewall and antivirus on your work computers?	Firewall and antivirus are security features that are built into Windows and macOS, and can be found in your computer's settings. You can also choose to buy these products from a third party.
Do you disable services not required for business purposes?	
Do you stay current on software updates?	
Do you download apps and software from official and/or reputable sources?	

Possible Responses	CISA Resources
Yes No	Cyber Guidance for Small Businesses
Yes No	Cyber Essentials Webinar
Yes No	Article: Choosing and Protecting Passwo
Yes No	Video: Secure Our World – Keep Your Ac
Yes No	Video: Secure Our World – Make Your A
Yes No	CISA Publication: Data Backup Options
An external hard drive, a USB stick or flash drive A network-connected hard drive (such as a NAS drive) A cloud drive A combination of the above	
Yes No	Cyber Essentials Toolkit: Your Data
Yes No	Cyber Essentials Toolkit: Your Data
Laptop computer Desktop computer Mobile devices (phone, tablet, PDA) A combination of the above	CISA Publication: The Risks of Portable D

Screen to auto-lock after a period of inactivity PIN code, passcode, fingerprint, face ID (or other biometric) to access your device Find my device (for Apple devices) Play protect (for Android devices)	Video: Are your mobile settings leaving y
Yes No	Article: Understanding Anti-virus softwa
Yes No	Article: Network Security
Yes No	Video: Secure Our World – Stay Safe by
Always Sometimes Never	Fact Sheet: Securing the Software Suppl

Recommendation Description
CISA has Cyber Guidance for Small Businesses, which is great place for any organization to start their cybersecurity journey.
Include anyone who has access to your data or devices, paid or unpaid. To prevent a security incident in one of your accounts from affecting all of your accounts, it's important to use unique passwords. Check out this article to learn more.
A great first step to securing user accounts is to learn how to choose strong passwords. Watch this short video from CISA to learn more.
As this short video will explain, a password is not enough. CISA strongly recommends that individuals and organizations implement multi-factor authentication to keep your accounts and data safe.
To ensure the availabilty of your data, it's important to make regular backups. This guidline from CISA outlines some options for how to backup your data.
Establish regular automated backups and redundancies of key systems. Employ a backup solution that automatically and continuously backs up your business-critical data and system configurations. Regular backups protect against ransomware and malware attacks. Use on-site and remote backup methods to protect vulnerable information.
Prioritize backups (based off of the importance of the information) and have a schedule of what to bring back online when so that your business can still function during a cyberattack. Test your backup strategy before you need to use it to make sure you have full read-back verification, a method of preventing errors when information is relayed or repeated in a different form in order to confirm its accuracy.
Keep your organization safe by ensuring you have policies and procedures to prevent unauthorized devices from connecting to your network. This article outlines the risks posed by portable devices.

To keep your information secure, it's important to ensure your devices have security features enabled. You should set your screen to auto-lock after a period of inactivity, and unlocking the device should require a PIN, Password, or Biometrics (such as a face ID or fingerprint).
Read this article to learn more about how Anti-virus software can identify and block many viruses before they can infect your computer.
Disabling services that you aren't using is one step you can take to keep your data safe. This article about home network security explains why and provides some other simple recommendations.
Many software updates are created to fix security risks, so it's important to keep your software up to date. Watch this short video to learn more.
This might mean only downloading from an official app store such as Apple App Store or Google Play, or researching the brand or checking its reviews first. For more details, read the Securing the Software Supply Chain Fact Sheet.

What is your organization's name?		Text Field
Are you a small business?	*A small business is a corporation, partnership, or sole proprietorship with fewer employees and typically lower average annual revenue than larger businesses in the same industry.*	Yes No
Does your business employ anyone else other than you?	*Include anyone who has access to your data or devices, paid or unpaid.*	Yes No
		Chemical Sector Commercial Facilities Sector Communications Sector Critical Manufacturing Sector Dams Sector Defense Industrial Base Sector Emergency Services Sector Energy Sector Financial Services Sector

Critical Infrastructure Sector	*Please note if your organization is part of one of the sixteen Critical Infrastructure Sectors, as defined here: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors*	Food and Agriculture Sector Government Facilities Sector Healthcare and Public Health Sector Information Technology Sector Nuclear Reactors, Materials, and Waste Sector Transportation Systems Sector Water and Wastewater Systems Not part of a Critical Infrastructure Sector
Critical Infrastructure Sub Sector	*If applicable, please note your sub sector*	Text Field
Organization Website		Text Field
Contact Name		Text Field
Contact Email		Text Field

Confirm Contact Email		Text Field
Headquarters Address		Address fields (Street or PO Box, Number, City, State, ZIP Code)
What Cybersecurity Services are currently in use at your organization?		Text Field
Is your organization an existing recipient of CISA cybersecurity services or recipient of CISA services in the past?		Text Field
What is the greatest cybersecurity challenge facing your organization?		Text Field
Would you like to take the basic questionnaire or the more in-depth assessment?	*The basic questionnaire covers cybersecurity best practices for users. The more advanced assessment alights to the Cross-Sector Cybersecurity Performance Goals.*	Basic Advanced

Questions	Possible Responses
Does your organization have security controls in place that appropriately identify, authenticate, and authorize users? (Category Question)	Yes No
Do your systems require a minimum password length of 15 characters (including OT systems, where technically feasible)? (2.B)	Yes No
Do you log all unsuccessful login attempts and provide security teams with alerts if a certain number of unsuccessful logins occur over a short period of time? (2.G)	Yes No
Do you change default passwords on all your IT and OT assets to the maximum extent possible, and implement compensating security controls wherever it is not? (2.A)	Yes No

Do you use MFA for access to all IT/OT assets, using the strongest available method possible? (2.H)	Yes No
Do you ensure all user and administrator or super-user accounts are kept separate and privileges are re-evaluated on a recurring basis? (2.E)	Yes No
Do you ensure all credentials, including those for service/machine accounts, are unique and separate across IT and OT networks? (2.C)	Yes No
Do you have an enforced process that ensures all departing employees return their physical security badges, tokens, etc. and have their accesses revoked on the day of their departure? (2.D)	Yes No

Definitions
Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, andphysical access control mechanisms.
Logs: A record of the events occurring within an organization's systems and networks.
Default Passwords: Factory default software configurations for embedded systems, devices, and appliances often include simple, publicly documented passwords. These systems usually do not provide a full operating system interface for user management, and the default passwords are typically identical (shared) among all systems from a vendor or within product lines. Default passwords are intended for initial testing, installation, and configuration operations, and many vendors recommend changing the default password before deploying the system in a production environment. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, andphysical access control mechanisms.

Multi-Factor Authentication (MFA): Multifactor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

Organizations should implement MFA for access to assets using the strongest available method for that asset). MFA options sorted by strength, high to low, are as follows:
1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI) based - see CISA guidance in"Resources");
2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used;
3. MFA via short message service (SMS) or voice only used when no other options are possible.

Phishing-Resistant MFA: As defined in OMB Memorandum 22-09, authentication processes designed to detect and prevent
disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic
acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange,
transmission, or reception of data or information.

Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices
that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.

Service acccount: "Non-human" (not specific to an individual user) account that is often used by an application or service to interact with the operating system

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange,
transmission, or reception of data or information.

Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices
that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.

Original CPG Question	Original CPG Responses
N/A	Implemented In Progress Scoped Not Started
Do your systems require a minimum password length of 15 characters (including OT systems, where technically feasible)?	Implemented In Progress Scoped Not Started
Do you log all unsuccessful login attempts and provide security teams with alerts if a certain number of unsuccessful logins occur over a short period of time?	Implemented In Progress Scoped Not Started
Do you change default passwords on all your IT and OT assets to the maximum extent possible, and implement compensating security controls wherever it is not?	Implemented In Progress Scoped Not Started

Do you use phishing-resistant MFA for critical systems?	Implemented In Progress Scoped Not Started
Do you ensure all user and administrator or super-user accounts are kept separate and privileges are re-evaluated on a recurring basis?	Implemented In Progress Scoped Not Started
Do you ensure all credentials are unique and separate?	Implemented In Progress Scoped Not Started
Do you have an enforced process that ensures all departing employees return their physical security badges, tokens, etc. and have their accesses revoked on the day of their departure?	Implemented In Progress Scoped Not Started

Associated CPGs	Level	CISA Resources
Category	N/A	Video: Strong Passv
2.B	3	Article: Choosing a
2.G	3	Logging Made Easy
2.A	4	Bad Practices

2.H	5	Video: Make Your A
2.E	3	Article: Defend Priv
2.C	4	Article: Choosing a
2.D	2	CISA Webinar: A Ho

Recommendation Description for Primary Resource	Secondary Resources
A great first step to securing user accounts is to learn how to choose strong passwords. Watch this short video from CISA to learn more.	Cyber Essentials Toolkit: Y
Not all passwords are created equal! This article explains how to choose and protect strong passwords.	John the Ripper Password
Logging is an important part of any organization's security posture. CISA has rolled out a new service that will make logging a breeze for your organization. Click the link to learn more!	Security Onion
It's important to change the default passwords on all of your assets. Check out this list of other common "Bad Practices" that might be making it easier for attackers to target your organization.	AllStar

Using Multi-Factor Authentication (or MFA) is a simple way to make your accounts much safer from criminals seeking to steal your information. Watch this video to learn more.	CISA MFA Resources
Users should only have the minimum privileges necessary to do their work. This article explains the importance of separating accounts and the principle of "least privilege."	Secureworks WhiskeySAM
Not all passwords are created equal! This article explains how to choose and protect strong passwords.	O365Spray
Employees who leave your organization should not have access to your organization's data. Watch this webinar to learn more about departing employees and other potential insider threats.	Insider Threat Mitigation (

Recommendation Description for 2nd Resource	Priority
CISA's Cyber Essentials Toolkit provides guidance on where to start when implementing cybersecurity best practices.	1
This offering is a password security auditing and password recovery tool available for many operating systems.	15
Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management.	21
AllStar is a GitHub application for enforcing security policies and permissions.	24

A password is not enough. CISA strongly recommends that individuals and organizations implement multi-factor authentication to keep your accounts and data safe. Check out CISA's MFA Resource page to learn more.	26
The WhiskeySAML tool automates the remote extraction of an ADFS signing certificate.	12
This tool is a username enumeration and password spraying tool aimed at Microsoft Office 365.	15
This guide will explain the threat that current and former employees can pose to your organization and offer to steps to mitigate the risk.	10

Questions	Possible Responses
Do you have device configuration policies and controls in place to manage the security, provisioning, and deployment of devices across the organization? (Category Question)	Yes No
Do you have administrative policies or automated processes that ensure all new hardware, firmware or software must be approved before being deployed? (2.Q)	Yes No
Are Microsoft Office macros, or similar embedded code, disabled by default on all devices? (2.N)	Yes No
Do you maintain a regularly updated inventory of all organizational assets with an IP address, and update this on a recurring basis? (1.A)	Yes No
Do you have policies and processes to prohibit the connection of unauthorized devices and media to IT and OT systems? (2.V)	Yes No
Do you maintain accurate documentation of network topology for all IT and OT networks? (2.P)	Yes No

Do you maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets? (2.O)	Yes No

Definitions	Original CPG Questions	Original Responses
Configuration: The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.	N/A	Implemented In Progress Scoped Not Started
	Do you have administrative policies or automated processes that ensure all new hardware, firmware or software must be approved before being deployed?	Implemented In Progress Scoped Not Started
Microsoft Office Macros: A macro in Access is a tool that automates tasks and adds functionality to forms, reports, and controls. For example, when a command button is added to a form, the button's OnClick event is associated with the macro.	Are Microsoft Office macros, or similar embedded code, disabled by default on all devices?	Implemented In Progress Scoped Not Started
Inventory: The formal listing or property record of personal property assigned to an organization.	Do you maintain a regularly updated inventory of all organizational assets with an IP address, and update this on a recurring basis?	Implemented In Progress Scoped Not Started
Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you have policies and processes to prohibit the connection of unauthorized devices and media to IT and OT systems?	Implemented In Progress Scoped Not Started
Network topology is used to describe the physical and logical structure of a network. It maps the way different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you maintain accurate documentation of network topology for all IT and OT networks?	Implemented In Progress Scoped Not Started

Baseline configurations: A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you maintain accurate documentation of baseline and current configurations of all critical IT and OT assets?	Implemented In Progress Scoped Not Started

Associated CPGs	Level	CISA Resources
Category	N/A	Securing Network Infrastructure
2.Q	5	Configuration and Change Mana
2.N	2	Article: Macro Security For Micr
1.A	5	Stuff Off Search
2.V	5	Article: The Risks of Portable De
2.P	4	CRR Resource Guide: Asset Inve

2.O	5	CRR Resource Guide: Configurat

Recommendation Description for Primary Resource	Secondary Resources
Check out this post on CISA's blog to get started securing network devices.	Cyber Essentials Toolkit: Your Syste
In order to keep your environment secure, you have to know what devices you have, how they're configured, and have a defined process for any changes you need to make. Read this guide to Configuration and Change Management to get started.	CIS Hardware and Software Asset T
Many types of malware rely on embedded code, such as Microsoft Office macros. To keep your organization safe, these macros should be disabled by default. Read this article to learn more.	How to Disable Macros
What do you know about your internet attack surface? To make sure you know what's accessible to attackers, check out CISA's Stuff Off Search.	Google Security Command Center
Keep your organization safe by ensuring you have policies and procedures to prevent unauthorized devices from connecting to your network. This article outlines the risks posed by portable devices.	Article: Protecting Portable Devices
To know what to protect, you need to know what you have. Check out this resource guide to creating an asset inventory.	Video: Create a Network Diagram

In order to keep your environment secure, you have to know what devices you have, how they're configured, and have a defined process for any changes you need to make. Read this guide to Configuration and Change Management to get started.	Microsoft Security Compliance Tool

Recommendation Description for 2nd Resource	Priority
CISA's Cyber Essentials Toolkit provides guidance on where to start when implementing cybersecurity best practices. Check out Chapter 3 to learn about securing your systems.	7
This tool is designed to help identify devices and applications. The spreadsheet can be used to track hardware, software, and sensitive information.	36
This white paper from the Center for Internet Security will walk you through the process of disabling macros by default in your organization.	8
This tool helps users strengthen their security posture by evaluating their security and data attack surface; providing asset	30
Read this blog from CISA to learn about how to protect your portable devices.	29
This video from Microsoft explains how to use Microsoft Vizio to create a network diagram	25

This toolset allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.	36

Original Question	Possible Responses
Do you have security controls and monitoring in place to protect the Confidentiality, Integrity, and Availability (CIA) of data? (Category Question)	Yes No
Are logs stored in a secure, centralized system, such as a security information and event management (SIEM) tool? (2.U)	Yes No
Do you collect and store logs for use for both detection and incident response activities? (2.T)	Yes No
Do you ensure all connections between IT and OT assets are denied by default unless explicitly allowed, and are required to pass through an intermediary system which is monitored and performs log collection? (2.F)	Yes No
Are sensitive data, including credentials, stored in a secure manner and only accessible to authenticated and authorized users? (2.L)	Yes No
Do you employ properly configured and up-to-date Transport Layer Security to protect data in transit whenever feasible? (2.K)	Yes No

Do you implement STARTTLS, SPF and DKIM, and DMARC on all organizational email infrastructure? (2.M)	Yes No
Do you maintain a regularly updated list of threats and their Tactics, Techniques, and Procedures (TTPs; for example, MITRE ATT&CK) relevant to your organization? (3.A)	Yes No

Definitions

The CIA triad is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure. The initials stand for the three principles on which information security rests:
- Confidentiality: Only authorized users and processes should be able to access or modify data
- Integrity: Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously
- Availability: Authorized users should be able to access data whenever they need to do so

Security information and event management (SIEM) tools: solutions which aggregate logs and allow users to create rules in order to detect, analyze, and respond to security threats.

Logs: A record of the events occurring within an organization's systems and networks.

Logs: A record of the events occurring within an organization's systems and networks.

Demilitarized Zone (DMZ): Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from intrusions.

Firewall: An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.

Transport Layer Security (TLS): An authentication and encryption protocol widely implemented in browsers and web
servers. HTTP traffic transmitted using TLS is known as HTTPS.

Encryption: Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes passive man-in-the-middle attacks more difficult.

SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) allow a sending domain to effectively "watermark" their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect.

When an email is received that doesn't pass an agency's posted SPF/DKIM rules, DMARC (Domain-based Message Authentication, Reporting & Conformance) tells a recipient what the domain owner would like done with the message.Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they wouldn't normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

TTPs - The behavior of a threat actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.

The MITRE ATT&CK framework is globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Original CPG Questions	Original Reponses	Associated CPGs
N/A	Implemented In Progress Scoped Not Started	Category
Are logs stored in a secure, centralized system, such as a security information and event management tool?	Implemented In Progress Scoped Not Started	2.U
Do you collect and store logs for use for both detection and incident response activities?	Implemented In Progress Scoped Not Started	2.T
Do you ensure all connections between IT and OT assets are denied by default unless explicitly allowed, and are required to pass through an intermediary system which is monitored and performs log collection?	Implemented In Progress Scoped Not Started	2.F
Are sensitive data, including credentials, stored in a secure manner and only accessible to authenticated and authorized users?	Implemented In Progress Scoped Not Started	2.L
Do you employ properly configured and up-to-date Transport Layer Security to protect data in transit whenever feasible?	Implemented In Progress Scoped Not Started	2.K

Do you implement STARTTLS, SPF, DKIM and DMARC on all organizational email infrastructure?	Implemented In Progress Scoped Not Started	2.M
Do you maintain a regularly updated list of threats and TTPs relevant to your organization?	Implemented In Progress Scoped Not Started	3.A

Level	CISA Resources	Recommendation Description for Primary Resource
N/A	Article: What is Cybe	If you're ready to start securing your network, check out this article with some cybersecurity basics.
5	Logging Made Easy (L	Logging is an important part of any organization's security posture. CISA has rolled out a new service that will make logging a breeze for your organization. Click the link to learn more!
5	Video: Introduction t	Watch this webinar to learn about incident response tools.
5	Layering Network Se	Check out this infographic to learn more about layering network security through segmentation.
5	Guide: Identity, Cred	To make sure that you are properly managing user identities and credentials, check out this guide.
5	CIS Guide: Encrypt Da	To protect data in transit, check out this Guide from the Center for Internet Security.

2	Insights: Enhance Em	A significant portion of attacks against organizations come via email. Download this guide to CISA's recommendations for enhancing email security to protect your organization.
5	CISA’s Alerts and Adv	CISA regularly publishes alerts and adviseries to keep organizations informed about existing and potential threats.

Secondary Resources	Recommendation Description for 2nd Resource	Priority
Cyber Essentials Tool	CISA's Cyber Essentials Toolkit provides guidance on where to start when implementing cybersecurity best practices. Check out Chapter 5 to learn about securing your data.	2
Video: Introduction t	Watch this webinar to learn about the importance of logging and how logs can be used in incident analysis and response.	27
Security Onion	Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management.	28
Network Segmentati	Visit Carnegie Mellon University's Software Engineering Institute Blog for an article on Network Segmentation concepts.	31
BitLocker for Microsc	This tool encrypts Microsoft Windows systems.	37
Cloudflare Universal	SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. Cloudflare allows any internet property to use SSL with the click of a button.	38

Perception Point	Perception Point Perception Point's Free Email Security Plan, protects organizations from any threat entering organization via email and other collaboration channels.	9
Microsoft Defender A	This tool protects and detects endpoint threats, including file-based and fileless malware. Built into Windows 10 and 11 and in versions of Windows Server.	32

Question	Possible Responses
Does your organization develop and practice information security governance across the organization and provide cybersecurity training for all employees? (Category Question)	Yes No
Does your organization have a named role/position/title identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities? (1.B)	Yes No
Are all employees and contractors provided with basic cybersecurity training on at least an annual basis? (2.I)	Yes No
Do you have training for OT cybersecurity? (2.J)	Yes No

Definitions	Original CPG Questions
Security governance: a process for overseeing the cybersecurity teams who are responsible for mitigating business risks. Security governance leaders make the decisions that allow risks to be prioritized so that security efforts are focused on business priorities rather than their own.	
	Does your organization have a named role/position/title identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities?
	Are all employees and contractors provided with basic cybersecurity training on at least an annual basis?
Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you have training for OT cybersecurity?

Original Responses	Associated CPGs	Level	CISA Resources
Implemented In Progress Scoped Not Started	Category	N/A	SAFECOM Governance
Implemented In Progress Scoped Not Started	1.B	3	Cyber Guidance for Be
Implemented In Progress Scoped Not Started	2.I	3	Recognize and Report
Implemented In Progress Scoped Not Started	2.J	3	OT Training Sign Up

Recommendation Description for Primary Resource	Secondary Resources	Recommendation Description for 2nd Resource
For guidance on the importance of establishing security governance within your organization, take a look at the resources on the SAFECOM Governance page.	Cybersecurity Workfo	This Guide helps professionals develop a training plan based on their current skill level and desired career opportunities.
To get started implementing a security culture at your organization, take a look at CISA's Guidance for Small Organizations.	CISA Cyber Essentials	CISA’s Cyber Essentials is a guide for leaders of small organizations to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
Did you know that CISA is on YouTube? Check out our channel for short educational videos like this one that you can use to train your employees and increase their security awareness.	Phishing Guidance fro	You can find plenty of documents providing basic cybersecurity guidance for your employees at cisa.gov, including this article detailing Anti-phishing guidance for your organizaiton.
Did you know that CISA provides virtual and in-person training sessions on a variety of topics? Visit CISA's training page to learn more.	Cybersecurity Workfo	This Guide helps professionals develop a training plan based on their current skill level and desired career opportunities.

Priority
5
14
11
20

Questions	Possible Responses
Does your organization have a process for Vulnerability Management? (Category Question)	Yes No
Do you keep track of known exploited vulnerabilities (listed in CISA's KEV Catalog) and ensure they are patched or mitigated in a timely fashion? (1.E)	Yes No
Do you maintain a public, easily discoverable method (such as a security.txt file) for security researchers to notify your security team of vulnerable, misconfigured, or otherwise exploitable assets? (4.B)	Yes No
Do you ensure that no exploitable services, such as Remote Desktop Protocol (RDP), are exposed on the public internet without appropriate compensating controls? (2.W)	Yes No
Do you ensure that no OT assets are on the public Internet, except where explicitly required for operation and protected by appropriate compensating controls? (2.X)	Yes No

Do third-parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of your cybersecurity defenses? (1.F)	Yes No

Definitions	Original CPG Questions
Vulnerability Management: the process of continuously identifying, evaluating, treating, and reporting the weaknesses in a system that could be exploited by a threat actor	
Known Exploitable Vulnerabilities (KEV) Catalog: A list of vulnerabilities that CISA has identified as being exploited, or that have been used by threat actors.	Do you keep track of known exploited vulnerabilities (listed in CISA's KEV Catalog) and ensure they are patched or mitigated in a timely fashion?
Vulnerability Disclosure Program: Gives security researchers clear guidelines for conducting vulnerability discovery activities and conveys CISA preferences for submitting discovered vulnerabilities to an organization. security.txt file: a proposed standard for websites' security information that is meant to allow security researchers to easily report security vulnerabilities: https://securitytxt.org/	Do you currently have a Vulnerability Disclosure Policy and/or run a bug bounty program? & Do you have a security.txt file on all public facing domains?
Remote Desktop Protocol (RDP): Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel. Network administrators use RDP to diagnose issues, login to servers, and to perform other remote actions. Remote users use RDP to log into the organization's network to access email and files. Compensating Controls - The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization.	Do you ensure that no exploitable services are exposed to the Internet without appropriate compensating controls?
Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms. Compensating Controls - The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization.	Do you ensure that no OT assets are on the public Internet, except where explicitly required for operation and protected by appropriate compensating controls?

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you regularly run third party tests such as penetration tests, incident simulations, tabletop exercises, etc.?

Original Responses	Associated CPGs	Level	CISA Resources
Implemented In Progress Scoped Not Started	Category	N/A	CRR Guide: Vulnerab
Implemented In Progress Scoped Not Started	1.E	4	Known Exploited Vu
Implemented In Progress Scoped Not Started	4.B, 4.C	5	CISA VDP
Implemented In Progress Scoped Not Started	2.W	3	Web Application Sca
Implemented In Progress Scoped Not Started	2.X	5	Cyber Hygiene Vuln

Implemented In Progress Scoped Not Started	1.F	5	Remote Penetration

Recommendation Description for Primary Resource	Secondary Resources	Recommendation Description for 2nd Resource	Priority
To get started with Vulnerability Management, download this comprehensive guide.	Video: Cloud Vulner	As organizations move more and more of their IT infrastructure to the cloud, it's important to ensure that your organization has vulnerability management in place in your virtual environment. Check out this vide from the 4th Annual National Cybersecurity Summit to learn more.	6
CISA keeps a database on Known Exploited Vulnerabilities on our website. Check it out here.	Blog: Understanding	Many software updates are created to fix security risks, so it's important to keep your software up to date, as this blog article will explain.	22
Visit https://securitytxt.org/ to learn about how you can create your owen security.txt file.	securitytxt.org	Visit https://securitytxt.org/ to learn about how you can create your owen security.txt file.	35
CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.	Binary Edge	This tool continuously collects and correlates data from internet accessible devices, allowing organizations to see what is their attack surface and what they are exposing to attackers.	19
Did you know that CISA offers several cyber hygiene services to help keep your organization safe? Visit the Vulnerability Scanning page today to take advantage of this free service.	Web Application Sc	CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.	19

This service tests perimeter defenses by mimicking the techniques adversaries use to gain unauthorized access to networks	Stakeholder Exercis	CISA offers a wide portfolio of downloadable Tabletop Exercise Packages (CTEPs) to serve as an off-the-shelf solution for a variety of stakeholders' exercise needs	33

Questions	Possible Responses	Definitions
Do you have a Supply Chain Risk Management process, or is risk management a consideration in your Supply Chain Management process? (Category Question)	Yes No	Supply Chain Risk Management (SCRM): A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain.
Do your procurement documents and contracts require vendors and service providers to inform you of security incidents within a certain time frame? (1.G)	Yes No	Procurement Documents: the paperwork detailing the contractual relationship between a customer and a supplier of goods or services
Do your procurement documents and contracts require vendors and service providers to inform you of security vulnerabilities within a certain time frame? (1.H)	Yes No	Procurement Documents: the paperwork detailing the contractual relationship between a customer and a supplier of goods or services
Do your procurements documents outline cybersecurity requirements and questions that are used to evaluate vendors such that, given two roughly equivalent options based on cost and functionality, the more secure option is preferred? (1.I)	Yes No	Procurement Documents: the paperwork detailing the contractual relationship between a customer and a supplier of goods or services

Original CPG Questions	Original Responses	Associated CPGs	Level
	Implemented In Progress Scoped Not Started	Category	N/A
Do your procurement documents and contracts require vendors and service providers to inform you of security incidents within a certain time frame?	Implemented In Progress Scoped Not Started	1.G	3
Do your procurement documents and contracts require vendors and service providers to inform you of security vulnerabilities within a certain time frame?	Implemented In Progress Scoped Not Started	1.H	3
o your procurement practices include cybersecurity requirements so that, given two roughly equivalent options based on cost and functionality, the more secure option is preferred?	Implemented In Progress Scoped Not Started	1.I	3

CISA Resources	Recommendation Description for Primary Resource	Secondary Resources
SCRM Webinar	Watch this webinar to learn about the importance of Supply Chain Risk Management and get started implementing SCRM in your organization.	Cyber Essentials: Supply Ch
Third Party Risk Mar	Download CISA's Third Party Risk Management template, so you can start making sure your third parties don't pose unnecessary risk to your organization	FedVTE course: Cyber Sup
A Resource Guide fo	The ICT SCRM Task Force's resource guide was created to provide a valuable starting point for you to develop and tailor an ICT SCRM plan that meets the needs of your organization.	Securing Small and Mediur
Video: Evaluating Ve	When choosing a vendor, it's important to keep security in mind. Watch this video to learn how to evaluate a vendor's trustworthiness.	OpenSSF: Scorecards

Recommendation Description for 2nd Resource	Priority
CISA's Cyber Essentials Toolkit provides guidance on where to start when implementing cybersecurity best practices. Check out this chapter to learn more about SCRM.	4
This free online course is available to the public and will explain how to get started with Supply Chain Risk Management	17
This handbook provides an overview of the highest supply chain risk categories commonly faced by ICT small and medium-sized businesses (SMBs).	17
Security Scorecards is a collection of security health metrics for open source, allowing users to evaluate the security practices of an open source package before use.	12

Questions	Possible Responses
Do you have an Incident Response and Recovery plan? (Category Question)	Yes No
Do you have up-to-date plans to recover and restore assets in case of a cybersecurity incident? (5.A)	Yes No
Do you have up-to-date cybersecurity incident plans for both IT and OT, and are these Incident Response plans drilled at least annually? (2.S)	Yes No
Do you have codified policies and procedures that specify to whom and how to report all confirmed cybersecurity incidents to the appropriate external authorities, within time frames directed by applicable regulatory guidance? (4.A)	Yes No
Do you back up all business critical systems at a regular cadence, no less than once per year, and are these backups stored separately from the source systems? (2.R)	Yes No

Definitions	Original CPG Questions
Incident Response Plan: A set of predetermined and documented procedures to detect and respond to a cyber incident.	
	Do you have up-to-date plans to recover and restore assets in case of a cybersecurity incident?
Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.	Do you have up-to-date and regularly exercised cybersecurity incident response plans for both IT and OT?
	Do you know where you can report incidents to CISA securely?
	Do you back up all systems necessary for operations at a regular cadence, no less than once per year?

Original Responses	Associated CPGs	Level	CISA Resources
Implemented In Progress Scoped Not Started	Category	N/A	Incident Response Plan Ba
Implemented In Progress Scoped Not Started	5.A	3	Incident Response Webina
Implemented In Progress Scoped Not Started	2.S	3	Tabletop Exercise Package
Implemented In Progress Scoped Not Started	4.A	3	CISA's Incident Reporting S
Implemented In Progress Scoped Not Started	2.R	5	Data Backup Options

Recommendation Description for Primary Resource	Secondary Resources
When incidents happen, your organization will recover faster if you already have a plan in place. Download this article to get started.	Planning Considerations for Cybe
To get started making an Incident Response plan, check out CISA's free on-demand webinar "Incident Response and Awareness Training"	CRR Supplemental Resource Gui
CISA offers a wide portfolio of downloadable Tabletop Exercise Packages (CTEPs) to serve as an off-the-shelf solution for a variety of stakeholders' exercise needs	Cybersecurity Tabletop Exercise
Save this link - The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA.	Federal Incident Notification Gui
To ensure the availabilty of your data, it's important to make regular backups. CISA has some backup options detailed here.	Windows Auto Backup

Recommendation Description for 2nd Resource	Priority
This guide provides recommendations on how to plan for and respond to cyber incidents.	3
The The Cyber Resilience Review Resource Guide for Incident Management has an Incident Reponse Plan Template that you can use to start drafting an IRP for your organization.	16
Check out this fact sheet for some tips on creating and running your own tabletop exercises.	18
This document provides guidance on incident reporting requirements.	13
This tool sets up automatic backups of Windows 10 and 11 operating systems.	34