Cybertrack Written Discovery Requests

For: [insert organization name]

To: [Insert Local Government Team primary point(s) of contact]
From: [Insert Assessment Team primary point(s) of contact]
Request Date: [Insert request date]
Response Due Date: [Insert response due date]

Table of Contents

About Cybertrack

With sponsorship from the Indiana Office of Technology (IOT), Purdue University and Indiana University have partnered to develop Indiana's local government cybersecurity assessment program. The project is designed to put local governments in contact with top tier cybersecurity experts, and provide them **practical, prioritized advice about doable, powerful cybersecurity fundamentals.** Our goal is to make Indiana more secure in the short term and shape our collective cybersecurity strategy and policy for the long term.

The primary deliverable of each assessment is a report, which will include evaluations of organizational cybersecurity fundamentals and safeguards, actionable recommendations, and explanations thereof. The recommendations will emphasize individual local government's cybersecurity strategies, with a particular focus on short-term priorities.

Organizations' responses to the questions and requests in this document are central to supporting these outcomes.

To learn more, visit http://cybertrack.org/. [site is not yet active]

Instructions

Please provide your organization's written responses to this questionnaire. The following instructions apply to all the questions and requests posed in this document. Additional background information or guidance specific to a numbered section appears under the header for that section. If you have questions, please contact your Cybertrack Assessment Team.

A. **You are answering on behalf of your organization.** Do your best to provide a single response, based on your facts, regardless of whether opinions or views of the facts might differ among colleagues.

B. **Can I provide documentation to answer these questions?** Yes, you may answer questions by providing supporting documentation. In your written response, please indicate the title and/or filename of the document(s) you provide, and provide some context (*e.g.*, URL, section, page number) and explanation of how the documentation supports your answer.

C. **How long and detailed do the responses need to be?** Most questions can be answered adequately in just a few sentences.
   a. Please be specific (*e.g.*, when referring to a person, include first name, last name, and role/title; when referring to technical resources, include major version numbers).
   b. Responses of "unknown", "not applicable", or "to be determined" are appropriate when factually accurate.
   c. You are free to provide as much information as you wish. Additional detail will help the assessment team in evaluating your responses and tailoring its recommendations.
   d. If relevant information does exist but cannot be provided, please provide a written statement explaining the nature of the information and reason for exclusion.

D. **Who needs to be involved?** In many cases, a single individual will not be able to respond to all requests without collaborating or consulting with others. We provide many definitions in-line, but have assumed that at least one person involved in responding will have preexisting knowledge of basic IT concepts. Consider engaging with senior leadership, technology personnel, your organization's independent contractors (*e.g.*, technology service providers), and others who may be able to help you accurately and efficiently respond.

E. **Can I be honest?** Yes, the more complete you are with your answers, the more your organization has to gain. Our immediate goal is to provide you meaningful, prioritized, doable advice to help you protect your organization. We're also trying to build a broad, general understanding of cybersecurity capabilities and needs across the wide variety of Indiana's local government entities, so resources can be channeled to where they're most needed. The security-specific information you provide during the assessment will be protected and will not be shared with the State government or other third parties. Anonymized and aggregated assessment information will be reported publicly and to the State; individual local governments will not be identified in this reporting without express permission.

1 Cybersecurity Programmatics Questions

The questions in this section are derived from the Trusted CI Framework. The Framework is a minimum standard for cybersecurity programs. Unlike other cybersecurity frameworks, the Trusted CI Framework is focused entirely on organizational cybersecurity fundamentals, aka "programmatics." It consists of 16 "Musts," organized under four pillars: Mission Alignment, Governance, Resources, and Controls. Each Must represents a foundational requirement for a competent cybersecurity program.

The following questions are designed to gather information about your organization's implementation of a carefully selected subset of these Musts. Each question begins with an overview of one Trusted CI Framework Must, and goes on to ask specific questions about your organization's cybersecurity program that are connected to that Must.

Must 5: Leadership

Organizations must involve leadership in cybersecurity decision making.
"Organizational leadership includes the senior executives and other decision makers responsible for an organization. These are the people ultimately responsible for the organization who make final decisions regarding the highest priorities."

Must 5 Q1

Which leaders, if any, in your organization are involved in cybersecurity decision making? Provide the names, roles, and titles, and generally describe the types of decisions each is involved in making.

Must 7: Cybersecurity Lead

Organizations must establish a lead role with responsibility to advise and provide services to the organization on cybersecurity matters.
"[The cybersecurity lead] ensures the program educates and advises decision makers on cybersecurity matters, including risk identification and mitigation, and policy development. The [cybersecurity lead] also provides leadership for services like incident response coordination, and cybersecurity control selection and monitoring."

Must 7 Q1

Has your organization established a cybersecurity lead role? (E.g., Chief Information Security Officer, Information Security Officer, Cybersecurity Lead.)

☐ Yes
☐ No

If yes, what is the title of that role, and to whom does that role report?

Must 7 Q2

Does your cybersecurity lead role have regular meetings (e.g., weekly, monthly, quarterly) with the organization’s senior-most leaders dedicated to cybersecurity?

☐ Yes
☐ No

If so, please describe the nature and frequency of these meetings. If not, please describe any barriers.

Must 9: Policy

Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity policies.

“‘Policy’ refers to documented normative statements adopted by an organization to govern human behavior.”

Must 9 Q1

Does your organization have a cybersecurity plan, master cybersecurity policy, or other document that governs your entire cybersecurity program?

☐ Yes
☐ No

If so, please provide documentation if possible. If not, describe any barriers to establishing cybersecurity policies.

Must 12: Cybersecurity Budget

Organizations must establish and maintain a cybersecurity budget.

"A cybersecurity budget is a financial plan that commits specific resources for the organization's cybersecurity efforts over a designated period of time."

Must 12 Q1

Does your organization have a cybersecurity budget? This may take the form of a line-item in a larger budget, or may be a stand-alone budget.

□ Yes
□ No

If so, please provide documentation if you are able. If not, please describe any barriers to implementing this Must.

Must 12 Q2

If applicable, what percentage of your total organizational budget is dedicated to cybersecurity?

Must 12 Q3

Has the percentage of your organizational budget allotted to cybersecurity increased, decreased, or remained the same since 2020? Please list any items that have made significant contributions to budget changes.

Must 13: Personnel

Organizations must allocate personnel resources to cybersecurity.

"Personnel resources are commitments made by an organization to assign human effort to particular activities on behalf of the organization. Personnel resources allocated to cybersecurity include both full-time cybersecurity employees and employees with partial cybersecurity responsibilities."

Must 13 Q1

Does your organization formally allocate personnel effort to cybersecurity?

☐ Yes
☐ No

If so, how much employee time (including partially allocated employees) is allocated to cybersecurity in terms of full-time equivalents (FTEs)? If not, describe any barriers to implementing this Must.

Must 13 Q2

Does your organization make use of cybersecurity contractors (*i.e.,* third parties hired to do specific cybersecurity work?)

☐ Yes
☐ No

Must 15: Baseline Control Set

Organizations must adopt and use a baseline control set.

"A baseline control set is a predetermined set of controls used as a default when selecting security controls for information assets." Examples: CIS Controls, NIST Cybersecurity Framework Core, NIST SP 800-171, FISMA Moderate Controls Baseline. "Adoption" of a baseline control set means committing to use a particular baseline control set or sets as the default when selecting controls, not that you have implemented every control on the baseline control set.

Must 15 Q1

Has your organization adopted a baseline control set for cybersecurity (CIS, NIST Cybersecurity Framework, etc.)?

☐ Yes
☐ No

If so, which baseline control set or sets has your organization adopted? If not, describe any barriers to implementing this Must.

2 Cybersecurity Controls Questions

The questions in this section are derived primarily from Implementation Group 1 of the Center for Information Security (CIS) Controls v8.[1]

The CIS Controls "are a relatively short list of high-priority, highly effective defensive actions that provide a 'must-do, do-first' starting point for every enterprise seeking to improve their cyber defense."[2] They are 1) highly prioritized; 2) updated frequently; 3) described in sufficient detail for organizations to implement them; and 4) developed by a collaborative and open process informed by a diverse group of cybersecurity practitioners. They map readily to the controls in many other cybersecurity standards (*e.g.,* NIST CSF, NIST 800-53, SOC 2). Each Control is broken down into "Safeguards" that describe specific actions that enterprises should take to implement the Control.

Implementation Group 1 (IG1)[3] is a set of 56 Safeguards that "represents a minimum standard of information security for all enterprises"[4] and helps all organizations deal with the most common types of attacks we see in real life. The following questions are designed to gather information about your organization's implementation of a carefully selected subset of IG1 Safeguards.[5]

The following requests begin with CIS IG1 Safeguard's title and official description. Key terms found throughout this Cybersecurity Controls Questions section are defined in the table below. Additionally, many individual Safeguards have a similar table to provide clarifying definitions.

[1] https://www.cisecurity.org/controls/v8.

[2] https://www.cisecurity.org/controls/cis-controls-faq.

[3] https://www.cisecurity.org/controls/implementation-groups/ig1.

[4] https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene.

[5] A few questions in this section also address Safeguards from Implementation Groups 2 and 3 or IG1 Safeguards that have closely related content. These are indicated by purple text (*e.g.*, the first question about Safeguard 7.1(IG1), also addresses Safeguard 8.2 (IG2 & 3)).

Key Terms and Definitions for Cybersecurity Controls Section[6]

Key Term(s)	***Definition***
Enterprise assets	Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments. [CIS v8]
Encryption	Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data. [NIST]
End-user devices	Information technology (IT) assets used among members of an enterprise during work,off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations. [CIS v8]
Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/ virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. [CIS v8]
Non-computing/Internet of Things (IoT) devices	Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets. [CIS v8]
Servers	A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.[CIS v8]
Sensitive data *e.g.* business critical data	A descriptor of information whose loss, misuse, or unauthorized access or modification could adversely affect security. [NIST] or affect the enterprise's ability to conduct business.

[6] Key term definitions were derived from the following three resources, with the definition source included in brackets:

- [CIS v8] → CIS Controls v8 document glossary.
- [cisecurity.org] → https://www.cisecurity.org/cybersecurity-terms-definitions.
- [NIST] → https://csrc.nist.gov/glossary.

CIS Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

“Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise’s network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.”

Key Term(s)	***Definition***
MDM (Mobile Device Management)	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.. [NIST]
network address *i.e.,* Internet Protocol (IP) Address	A unique identifying number that every device connected to the internet possesses. IP addresses allow information to be sent between devices. [cisecurity.org] *Example*: 12.34.56.78
hardware address *i.e.,* MAC Address	A hardware address that uniquely identifies each component of an [ethernet] network. [NIST] *Example*: aa:bb:cc:00:11:22

CIS 1.1 Q1

Has your organization established and maintained an accurate, detailed, and up-to-date inventory of all enterprise assets?

□ Yes
□ No

If yes, describe the process, including what types of enterprise assets and/or software are covered. If no, please describe the barriers to implementing this Safeguard.

CIS 1.1 Q2

From the following list, please specify which details are included in the inventory records:

□ the network address (IP address)
□ hardware address (MAC address)
□ OS/firmware version
□ machine name
□ enterprise asset owner
□ department for each asset
□ whether the asset has been approved to connect to the network

If you did not check all of the above, please describe why the unchecked items are not recorded.

CIS 1.1 Q3

Does your organization review and update documentation for your asset inventory?

□ Yes
□ No

If yes, describe the asset inventory review and update process, and frequency of the updates. If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 2.2: Ensure Authorized Software is Currently Supported

“Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise’s mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.”

Key Term(s)	*Definition*
unsupported software ***e.g.* end-of-life (EOL) software**	Software that no longer receives vendor support for patches and feature upgrades. (p.38) [CIS]
mitigating controls	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities [NIST]
residual risk	Portion of risk remaining after security measures have been applied. *and/or* Risk that remains after risk responses have been documented and performed [NIST]

CIS 2.2 Q1

Does your organization have a process to identify unsupported/end-of-life software for enterprise assets on your network?

□ Yes
□ No

If yes, please please describe the typical action that is taken to mitigate the risk. If no, please describe the barriers to implementing this Safeguard.

CIS 2.2 Q2

Does your organization have unsupported/end of life enterprise asset(s) accessible from the internet (*i.e.,* able to be connected to from outside of your enterprise network)?

□ Yes
□ No

If yes, please please describe the business function of these enterprise asset(s) . If no, please describe the barriers to implementing this Safeguard.

CIS 2.2 Q3

Does your organization document and maintain a software list that records authorized/unauthorized software?

□ Yes
□ No
□ N/A

If yes, describe any review and update process, including the frequency and what events trigger that process. If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 2.3: Address Unauthorized Software

"Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently."

Key Term(s)	***Definition***
Unauthorized software	Software connected to an enterprise's infrastructure which is not needed or not approved for business purposes, and may pose unnecessary security risks. (p. 11) [CIS v8]

CIS 2.3 Q1

Does your organization identify and remove unauthorized software on your assets?

☐ Yes
☐ No

If yes, please describe your method of unauthorized software identification and removal. If no, please describe the barriers to implementing this Safeguard.

CIS 2.3 Q2

Does your organization document exceptions to software installed on devices that would otherwise be considered unauthorized software?

☐ Yes
☐ No

CIS Safeguard 3.3: Configure Data Access Control Lists

“Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.”

Key Term(s)	*Definition*
access control lists	A list of entities, together with their access rights, that are authorized to have access to a resource. [NIST]
need to know	Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties. [NIST]

CIS 3.3 Q1

Does your organization identify groups and users that should and should not have access to specific data assets?

□ Yes
□ No

CIS 3.3 Q2

Does your organization adjust file system permissions based on who should have access to specific data assets?

□ Yes
□ No

CIS 3.3 Q3

Does your organization adjust network access control lists based on who should have access to specific data assets?

□ Yes
□ No

CIS Safeguard 3.4: Enforce Data Retention

“Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum timelines.”

CIS 3.4 Q1

Does your organization have an enterprise data management process?

□ Yes
□ No

If yes, please describe the data retention process and whether it addresses minimum and maximum timelines of data retention.

CIS Safeguard 3.10: Encrypt Sensitive Data in Transit (IG2 & IG3)

"Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH)."

Key Term(s)	***Definition***
data in transit	Data in transit, also called data in motion, is data that is actively moving from one location to another. This can be across the internet, within a private network, or from one device to another.[7] The adoption of data encryption [in transit] can provide mitigation against data compromise. (p. 14) [CIS v8]

CIS 3.10 Q1

Does your organization encrypt all sensitive data when it is sent over the network (*i.e.,* data in transit)?

□ Yes
□ No

If no, please describe the barriers to implementing this Safeguard.

[7] https://www.quest-technology-group.com/academy/what-is-data-in-transit-vs-data-at-rest.

CIS Safeguard 3.11: Encrypt Sensitive Data at Rest (IG2 & IG3)

"Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data."

Key Term(s)	*Definition*
application-layer encryption *i.e.* client-side encryption	Encryption of [network traffic] that sends and receives data for particular applications such as DNS, HTTP, and SMTP. [NIST] Client-side encryption is the cryptographic technique of encrypting data on the sender's side, before it is transmitted to a destination.
data at rest	Data at rest is data that is not actively moving. It is data stored on a hard drive or storage device.[8] The adoption of data encryption [at rest] can provide mitigation against data compromise. (p. 14) [CIS v8]

CIS 3.11 Q1

From the following list, please specify which *enterprise-owned* devices use encryption for data at rest. This includes local disk encryption (*e.g.,* Bitlocker, Apple Filevault, Linux Unified Key Setup (LUKS)?

- ☐ Servers
- ☐ Databases
- ☐ User end-point device - Laptop (Safeguard 3.6, IG1)
- ☐ User end-point device - Desktops (Safeguard 3.6, IG1)
- ☐ Mobile devices (*e.g.* phones, tablets) (Safeguard 3.6, IG1)

If you did not check all of the above, please describe why the unchecked asset types do not have data at rest or local disk encryption enabled.

[8] https://www.quest-technology-group.com/academy/what-is-data-in-transit-vs-data-at-rest.

CIS 3.11 Q2

Does your organization use encryption for data at rest on enterprise assets that store "sensitive data"?

□ Yes
□ No

If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 4.1: Establish and Maintain a Secure Configuration Process

"Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."

Key Term(s)	*Definition*
secure configuration process *i.e.,* Configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. [NIST]

CIS 4.1 Q1

Has your organization established and maintained a secure configuration process for enterprise assets and software?

□ Yes
□ No

If yes, describe the process, including what types of enterprise assets and/or software are covered. If no, please describe the barriers to implementing this Safeguard.

CIS 4.1 Q2

Does your organization review and update documentation for your secure configuration process?

□ Yes
□ No

If yes, describe the review and update process. Please also include what events trigger that process.

CIS Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

"Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."

Key Term(s)	***Definition***
secure configuration process *i.e.,* Configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. [NIST]

CIS 4.2 Q1

Does your organization have a secure configuration process for network devices?

□ Yes
□ No

If yes, please describe this configuration process.

CIS 4.2 Q2

Does your organization document secure configuration processes for network infrastructure?

□ Yes
□ No
□ N/A

If yes, describe any review and update process, including the frequency and what events trigger that process.

CIS Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets

"Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes."

CIS 4.3 Q1

Does your organization configure automatic session locking on enterprise assets?

□ Yes
□ No

If yes, what is the timeframe at which a session is locked for user devices and for servers? If no, please describe any barriers to implementing this Safeguard.

CIS Safeguard 4.6: Securely Manage Enterprise Assets and Software

"Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential."

Key Term(s)	*Definition*
infrastructure-as-code *i.e.*virtual servers	The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools. [NIST]
secure protocol *i.e.,* secure communication protocol	A communication protocol that provides the appropriate confidentiality, source authentication, and integrity protection. [NIST]

CIS 4.6 Q1

In the instances where your organization's end-point assets and software are managed over the network (*i.e.,* not physically interacting with the device), does your organization only use secure protocols to do so?

☐ Yes
☐ No

If no, please describe any barriers to implementing this aspect of the Safeguard: managing end-points and software over the network.

CIS 4.6 Q2

In the instances where your organization is accessing administrative interfaces over the network (*i.e.,* not physically interacting with the device), does your organization only use secure protocols to do so?

☐ Yes
☐ No

If no, please describe any barriers to implementing this aspect of the Safeguard: accessing administrative interfaces over the network.

CIS 4.6 Q3

Does your organization develop and implement any virtual servers (*e.g.* VMWare ESXi, Citrix)?

☐ Yes
☐ No

If yes, please describe how you manage code version control and describe your secure coding practices. Please also include any barriers to implementing these.

CIS Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software

"Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable."

Key Term(s)	***Definition***
vendor account	Accounts for: Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization. [NIST]

CIS 4.7 Q1

Where default accounts exist on your organization's assets and software, does your organization disable and/or change the default password for the default accounts?

☐ Yes
☐ No

If no, please describe any barriers to implementing this Safeguard.

CIS 4.7 Q2

Please describe whether and how your organization manages vendor accounts and vendor access, both local and remotely accessible, on your organization's assets.

CIS Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

"Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use from the user's primary, non-privileged account."

Key Term(s)	***Definition***
dedicated administrator account	Dedicated accounts with escalated privileges and used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts. [CIS v8]

CIS 5.4 Q1

Does your organization, including users who have privileged accounts, use only unprivileged accounts when performing general computing activities?

□ Yes
□ No

If no, please indicate which enterprise assets use administrative accounts to perform daily operations, and describe why.

CIS Safeguard 6.4: Require MFA for Remote Network Access

"Require MFA for remote network access."

Key Term(s)	*Definition*
MFA *i.e.,* Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (*e.g.*, password/personal identification number [PIN]); (ii) something you have (*e.g.*, cryptographic identification device, token); or (iii) something you are (*e.g.*, biometric). [NIST]
remote network access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. [NIST]

CIS 6.4 Q1

Does your organization require MFA authentication for remote network access?

□ Yes
□ No

If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 6.5: Require MFA for Administrative Access

"Require MFA for all administrative access accounts, where supported, [and] on all enterprise assets, whether managed on-site or through a third-party provider."

Key Term(s)	*Definition*
third-party provider *i.e.,* Third-Party Relationships	Relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. [NIST]

CIS 6.5 Q1

Does your organization require MFA authentication for all administrative access accounts on enterprise assets owned by you?

□ Yes
□ No

If no, please describe the barriers to implementing MFA for administrative access on your enterprise assets.

CIS 6.5 Q2

Does your organization require MFA authentication for all administrative access accounts on enterprise assets or services (*e.g.,* cloud services) that leverage a third-party provider?

☐ Yes
☐ No

If no, please describe the barriers to implementing MFA administrative access on third-party resources leveraged by your organization.

CIS Safeguard 7.1: Establish and Maintain a Vulnerability Management Process

"Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."

Key Term(s)	*Definition*
vulnerability management	Continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information. (p. 26) [CIS v8]
risk-based	Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch. (p. 26) [CIS v8
remediation	The act of mitigating a vulnerability or a threat. [NIST]

CIS 7.1 Q1

Has your organization established a vulnerability management process?

□ Yes
□ No

If yes, describe the process, including (1) what types of enterprise assets and/or software are covered, (2) your risk-based remediation strategy (Safeguard 7.2, IG2 & IG3)**, and (3) how you remediate detected vulnerabilities** (Safeguard 7.7, IG2 & IG3)**. If no, please describe the barriers to implementing this Safeguard.**

CIS 7.1 Q4

Does your organization document a vulnerability management process?

□ Yes
□ No
□ N/A

If yes, describe any review and update process, including the frequency and what events trigger that process. If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 7.3: Automated Operating System Patch Management

"Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis."

CIS 7.3 Q1

Does your organization configure automatic updates for operating systems?

□ Yes
□ No

If yes, describe the automated update process, and frequency of the updates. If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 8.1: Establish and Maintain an Audit Log Management Process

"Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard"

Key Term(s)	*Definition*
audit log	Unlike system logs, which are native logs to systems, typically provide system-level events that show various system process start/end times, crashes, etc.. Audit logs typically include user-level events—when a user logged in, accessed a file, etc. (p. 29) [CIS v8]
network traffic flow logs	Logs recording network communications that are carried over wired or wireless networks between hosts. [NIST]
log aggregation	The consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event.[NIST] or to collect multiple log sources into one central log repository
log correlation	Finding relationships between two or more log entries. [NIST]

CIS 8.1 Q1

Has your organization established an audit log management process?

☐ Yes
☐ No

If yes, select from the following list which audit log activities are included in the audit log management:

☐ Enable enterprise asset logs locally on the server and/or service (Safeguard 8.2, IG1)

☐ Collect network traffic flow logs from network devices (e.g. routers, switches) (Safeguard 13.6, IG2 & IG3)

☐ Collect enterprise asset logs in a central log server or log aggregation service

(Safeguard 8.2, IG1)

- □ Conduct analysis of enterprise asset logs for pre-determined activities (*e.g.* system security alerts, access events) (Safeguard 8.2, IG1)
- □ Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. (Safeguard 8.11, IG2 & IG3)
- □ Implement event alerting across enterprise assets as a result of log correlation and analysis (Safeguard 13.1, IG1)
- □ Share cyber threat alerts and indicators, and related information, with external organizations like IN-ISAC, MS-ISAC (Safeguard 13.1, IG1)
- □ Configure detailed audit logging for enterprise assets containing sensitive data. (*e.g.* event source, date, username, timestamp, source addresses, destination addresses) (Safeguard 8.5, IG2 & IG3)

If no, please describe the barriers to implementing this Safeguard.

CIS 8.1 Q2

Does your organization document the audit log management process?

□ Yes
□ No
□ N/A

If yes, describe any review and update process, including the frequency and what events trigger that process. If no, please describe the barriers to implementing this Safeguard.

CIS Safeguard 10.1: Deploy and Maintain Anti-Malware Software

“Deploy and maintain anti-malware software on all enterprise assets.”

Key Term(s)	*Definition*
anti-malware software *i.e.,* antivirus software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. [NIST] Anti-virus: software that can prevent, detect, and/or remove malware. [cisecurity.org]

CIS 10.1 Q1

From the following list, please specify which enterprise assets have anti-malware protection deployed:

☐ User end-point devices (*e.g.* workstations, laptops)
☐ Mobile devices (*e.g.* phones, tablets)
☐ Servers
☐ Email service

If you did not check all of the above, please describe why the unchecked enterprise asset types do not have anti-malware protection.

CIS 10.1 Q2

If there are asset types that *do* have malware protection but are not included in the list above, please list them here.

CIS Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates

“Configure automatic updates for anti-malware signature files on all enterprise assets.”

Key Term(s)	*Definition*
Anti-malware signature files *i.e.,* signature	A set of characteristics of known malware instances that can be used to identify known malware and some new variants of known malware. [NIST]

CIS 10.2 Q1

Does your organization configure automatic updates for anti-malware signature files?

□ Yes
□ No

If yes, please list which of the asset types from the previous question (CIS Safeguard 10.1) are configured for automatic anti-malware signature updates.

CIS Safeguard 11.1: Establish and Maintain a Data Recovery Process

"Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."

Key Term(s)	*Definition*
Data recovery process	Ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state. (p. 36) [CIS v8]

CIS 11.1 Q1

Has your organization established a data recovery process?

□ Yes
□ No

If yes, please select which activities you include in your data recovery process:

□ Identify the scope of data recovery
□ Recovery prioritization
□ Security of backup data
□ Test data recovery procedures

CIS 11.1 Q2

Does your organization document your data recovery process?

☐ Yes
☐ No
☐ N/A

If yes, describe any review and update process, including the frequency and what events trigger that process.

CIS Safeguard 13.3: Deploy a Network Intrusion Detection Solution (IG2 & IG3)

"Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service"

Key Term(s)	*Definition*
Network Intrusion Detection System (NIDS)	Software that [observes and records network traffic] and network traffic analysis to identify suspicious activity and record relevant information. [NIST]
cloud service provider (CSP)	A pool of virtual resources—developed from hardware owned and managed by a third-party company—that is automatically provisioned and allocated among multiple clients through a self-service interface.[9]

CIS 13.3 Q1

Has your organization deployed a network intrusion detection solution or equivalent (*e.g.*, Zeek, Suricata, 3rd network intrusion detection services) ?

☐ Yes
☐ No

If yes, describe the network intrusion detection solution, including (1) if the solution is deployed locally (*e.g.,* on-premises) or via remote infrastructure (*e.g.,* "the cloud"). If no, please describe the barriers to implementing this Safeguard.

[9] https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud.

CIS Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

“Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.”

Key Term(s)	*Definition*
security incident	An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See cyber incident. [NIST]

CIS 17.3 Q1

Does your organization have an enterprise process for the workforce to report security incidents?

□ Yes
□ No

If yes, please describe the enterprise process for the workforce to report security incidents.

CIS 17.3 Q2

From the following list, please select which activities are specified in your process for reporting security incidents:

□ reporting timeframe
□ personnel to report to
□ mechanism for reporting
□ the minimum information to be reported

CIS 17.3 Q3

Do you conduct training for your workforce on how to report security incidents?

□ Yes
□ No

CIS Safeguard 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

"Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum."

Key Term(s)	*Definition*
incident response (IR) exercise *i.e.* table top exercise	Exercises [that] are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making [NIST]

CIS 17.7 Q1

Does your organization conduct routine incident response exercises and scenarios (*e.g.,* tabletop exercises) for key personnel involved in the incident response process?

□ Yes
□ No

If yes, describe the exercise planning process and the frequency of the exercises. If no, please describe the barriers to implementing this Safeguard.

3 Wrap-up Questions

The questions in this section are designed to give the assessment team a greater understanding of your organization's engagement with this questionnaire, and give you an opportunity to share additional relevant information about your cybersecurity environment..

Wrap-Up Q1: Participants

Provide a listing of all people who participated or were consulted in providing your responses. Include full names and titles/roles.

Wrap-Up Q2: Strengths and Capabilities

Does your organization have any cybersecurity strengths or capabilities, whether discussed in responses to prior questions or not, that you want to highlight? If so, please describe.

Wrap-Up Q3: Weaknesses and Challenges

Does your organization have any cybersecurity weaknesses or challenges, whether discussed in responses to prior questions or not, that you want to highlight? If so, please describe.

Wrap-Up Q4: Incidents

Has your organization experienced an impactful cybersecurity incident in the last 3 years? If so, please describe.

Wrap-Up Q5: Anything Else?

Is there anything else you want to share with the Assessment Team? If so, please use this response to describe.