

## Snapshots of the Cyber Supply Chain Survey Tool

Below is the Cyber supply chain survey tool front page where general information is provided. Note that we are still in phase one where the site is only available to federal employees only.

### Cybersecurity Risk Analytics and Measurement CRA



#### Cyber Supply Chain Survey Tool

OMB Control #0693-0043

Expiration Date: 06/30/2025

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995 unless the information collection has a currently valid OMB Control Number. The approved OMB Control Number for this information collection is 0693-0043. Without this approval, we could not conduct this survey/information collection. Public reporting for this information collection is estimated to be approximately 40 minutes/hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. All responses to this information collection are voluntary. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the National Institute of Standards and Technology (NIST) at: 100 Bureau Drive, Gaithersburg, MD, 20899, Attn: Hung Trinh, or [cyberriskanalytics@nist.gov](mailto:cyberriskanalytics@nist.gov).

[Additional Informed Consent Information](#)

+ expand all

#### Purpose and Scope

#### Audience

#### Survey Tool Overview

#### Preparation

#### Survey Results

Click on the button below to download the user guide, then follow this [link to the survey tool](#).

[Download](#)

#### PROJECT LINKS

##### Overview

##### News & Updates

##### Publications

#### ADDITIONAL PAGES

##### Terminology

#### CONTACTS

##### CRA team

[cyberriskanalytics@nist.gov](mailto:cyberriskanalytics@nist.gov)

##### Hung Trinh

[hung.trinh@nist.gov](mailto:hung.trinh@nist.gov)

##### Katherine Schroeder

[Katherine.Schroeder@nist.gov](mailto:Katherine.Schroeder@nist.gov)

#### GROUP

[Security Engineering and Risk Management](#)

#### TOPICS

**Security and Privacy:** [risk management](#), [security measurement](#)

#### RELATED PROJECTS

The expandable sections can be viewed through this link

<https://cms.csrc.nist.gov/preview/projects/cybersecurity-risk-analytics/cscs-tool>

The link from the front page has a link to the [Cyber supply chain survey page](#) where the survey questionnaire is located. They are divided into six expandable sections.

## Cybersecurity Risk Analytics and Measurement CRA



Print this page

### Cyber Supply Chain Survey

✓ The Cyber Supply Chain Survey Tool is a resource designed for research and education purposes to help organizations manage cybersecurity risks in their supply chain. Users can gain insights into their processes and capabilities for addressing cyber supply chain issues by answering a series of questions. The tool collects general contextual data on the organization and generates an output analysis based on the responses. It also directs users to relevant standards and guides for further information. This survey is anonymous, and no personal identifiers are collected. The organization's name is not required. However, it is important to note that this survey is only for federal participants. You may choose to participate voluntarily, and by doing so, you acknowledge that you are a federal employee.

Expand all

► Respondent Profile

► I. Identify

► II. Protect

► III. Detect

► IV. Respond

► V. Recover

Submit

## Expanded Respondent profile section

Expand all

### ▼ Respondent Profile

#### How large is your organization

- ☐ Small Organization (fewer than 100 employees)
- ☐ Small-Medium Organization (100-999 employees)
- ☐ Medium-sized Organization (1,000-9,999 employees)
- ☐ Large Organization (10,000 employees or more)

#### Are you a parent or subsidiary organization?

- ☐ Parent Organization
- ☐ Subsidiary Organization

#### Are your networks/IT systems

- ☐ Primarily managed by your parent organization
- ☐ Primarily managed by your own unit

What is your organization's North American Industry Classification System (NAICS) Code?

What most accurately describes your job title / professional role? (NICE 2017 Framework)

- None - ▼

Which business roles are the people from your organization who contributed to this questionnaire responsible for? Select all that apply.

- ☐ All Source-Collection Manager
- ☐ All Source-Collection Requirements Manager
- ☐ All-Source Analyst
- ☐ Authorizing Official/Designating Representative
- ☐ Communications Security (COMSEC) Manager
- ☐ Cyber Crime Investigator and Law Enforcement /Counterintelligence Forensics Analyst
- ☐ Cyber Defense Analyst
- ☐ Cyber Defense Forensics Analyst and Law Enforcement /Counterintelligence Forensics Analyst
- ☐ Cyber Defense Incident Responder
- ☐ Cyber Defense Infrastructure Support Specialist

## Expanded Identity section

Expand all

► Respondent Profile

▼ I. Identify

▼ A. Asset Management

1. Do you have an accounting or inventory of assets related to protected data? (Assets include: network devices, servers, desktops, registers, operating systems, database software, and applications.)

☐ Yes

☐ No

☐ Not Applicable

2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?

☐ Yes

☐ No

☐ Not Applicable

2.1 Does this program specify security standards for each class of data?

☐ Yes, for ALL classes of data

☐ Yes, for SOME classes of data

☐ No, not for any class of data

☐ Not Applicable

3. Do you have a process for regularly and frequently identifying vulnerabilities associated with assets related to protected data?

☐ Yes, regularly and frequently

☐ Yes, but irregularly and infrequently

☐ No process

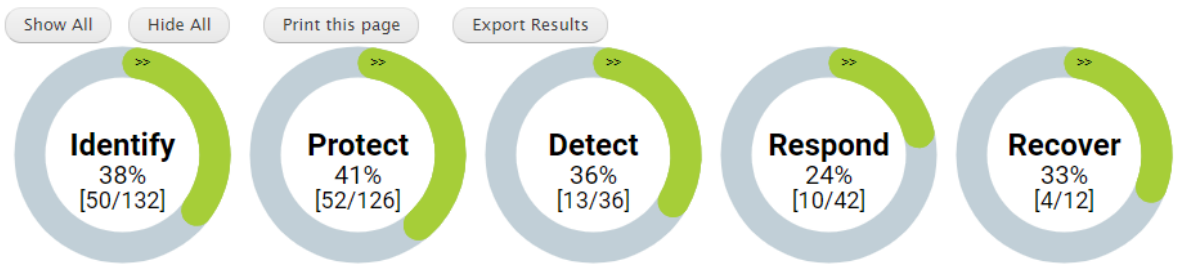
☐ Not Applicable

4. Is software versioning and patching history recorded for all applicable IT assets?

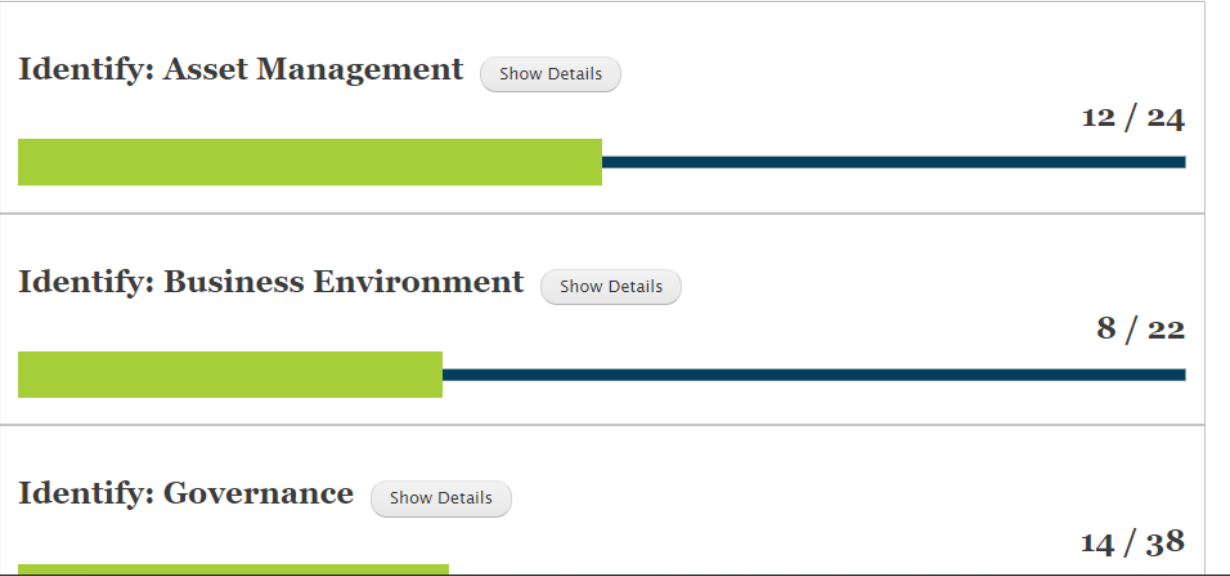
☐ Yes, for ALL applicable IT assets

☐ Yes, for SOME applicable IT assets

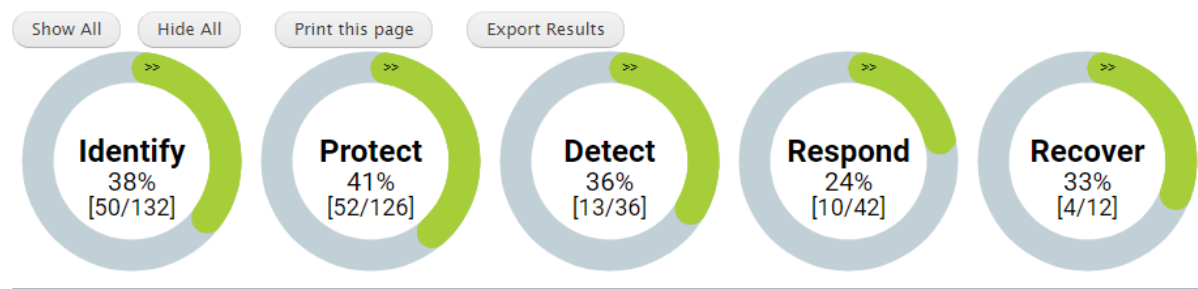
Sample analysis after the respondent submit the data.



Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.



Sample expanded sub-section under the Identity where links are provided to additional resources and references.



Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Identify: Asset Management

Show Details


12 / 24

Description	CSF Sub Category
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. <a href="#">Click for more info</a>	<a href="#">ID.AM-1</a> <a href="#">ID.AM-2</a> <a href="#">ID.AM-3</a> <a href="#">ID.AM-4</a> <a href="#">ID.AM-5</a>

The links from the assessment output directs the users to another tool maintained by ITL where resource mapping is continuously updated to all relevant guidance and standards.





Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

COMPUTER SECURITY  
RESOURCE CENTER  
CSRC

PROJECTSCYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT



Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

CPRT / Cybersecurity Framework v1.1 / ID / ID.AM / ID.AM-1

[Expand Entire Reference Dataset](#)

Export

IDENTIFY (ID)

The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device.  
> [Show all ID References](#)

Category	Subcategory	Reference Items 6
<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. > <a href="#">Show all ID.AM References</a>	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried > <a href="#">Show all ID.AM-1 References</a>	<b>CIS CSC:</b> 1 <b>COBIT 5:</b> BAI09.01, BAI09.02 <b>ISA 62443-2-1:2009:</b> 4.2.3.4 <b>ISA 62443-3-3:2013:</b> SR 7.8 <b>ISO/IEC 27001:2013:</b> A.8.1.1, A.8.1.2 <b>NIST SP 800-53 Rev. 4:</b> <a href="#">CM-8</a> , <a href="#">PM-5</a>

