# Cyber AI Profile COI Working Sessions: Usability of the Profile

**May 12, 2026**

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Agenda

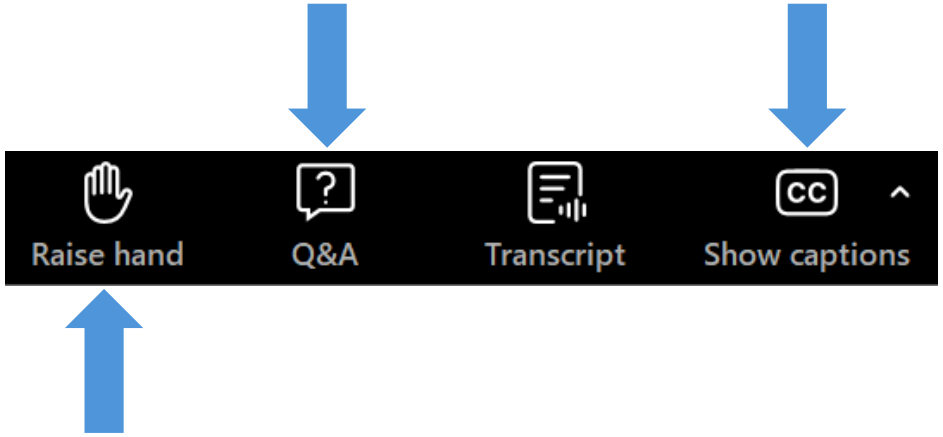
- Cyber AI Profile Project Overview
- Today's Plan
- Incorporating Roles Discussion
- Addressing Supply Chain Discussion
- AI Bill of Materials Discussion
- Profile Delivery Formats Discussion
- Open Discussion
- Close-out

# Engagement

## Via Zoom:

We would love to hear from you!

- Submit questions during Q&A
- Raise your virtual hand to be unmuted to speak (remember to unmute on your end, too!)
- Enable captioning




## Via Slido:

Please use Slido to participate throughout the session. Scan the QR code or go to Slido.com and enter the access code to access the polls as they are opened.

**Slido.com**
**#CyberAI_Spring2026-3**

# Cyber AI Profile Project Overview

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Cybersecurity, Privacy, and AI

The diverse use and rapid proliferation of Artificial Intelligence (AI) promises unique value for industry, consumers, and broader society, but like many technologies, to recognize these benefits to the greatest potential, new risks from these advancements in AI must be managed.

In NIST's Applied Cybersecurity Division (ACD), our key concern is how advancements in the broad adoption of AI may impact current cybersecurity and privacy risks and risk management approaches.

https://www.nist.gov/itl/applied-cybersecurity/cybersecurity-privacy-and-ai

# The Case for a Cyber AI Profile

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

**Purpose:**

Support cybersecurity programs as they manage the impacts of advancements in AI to their organization

## Areas of focus:

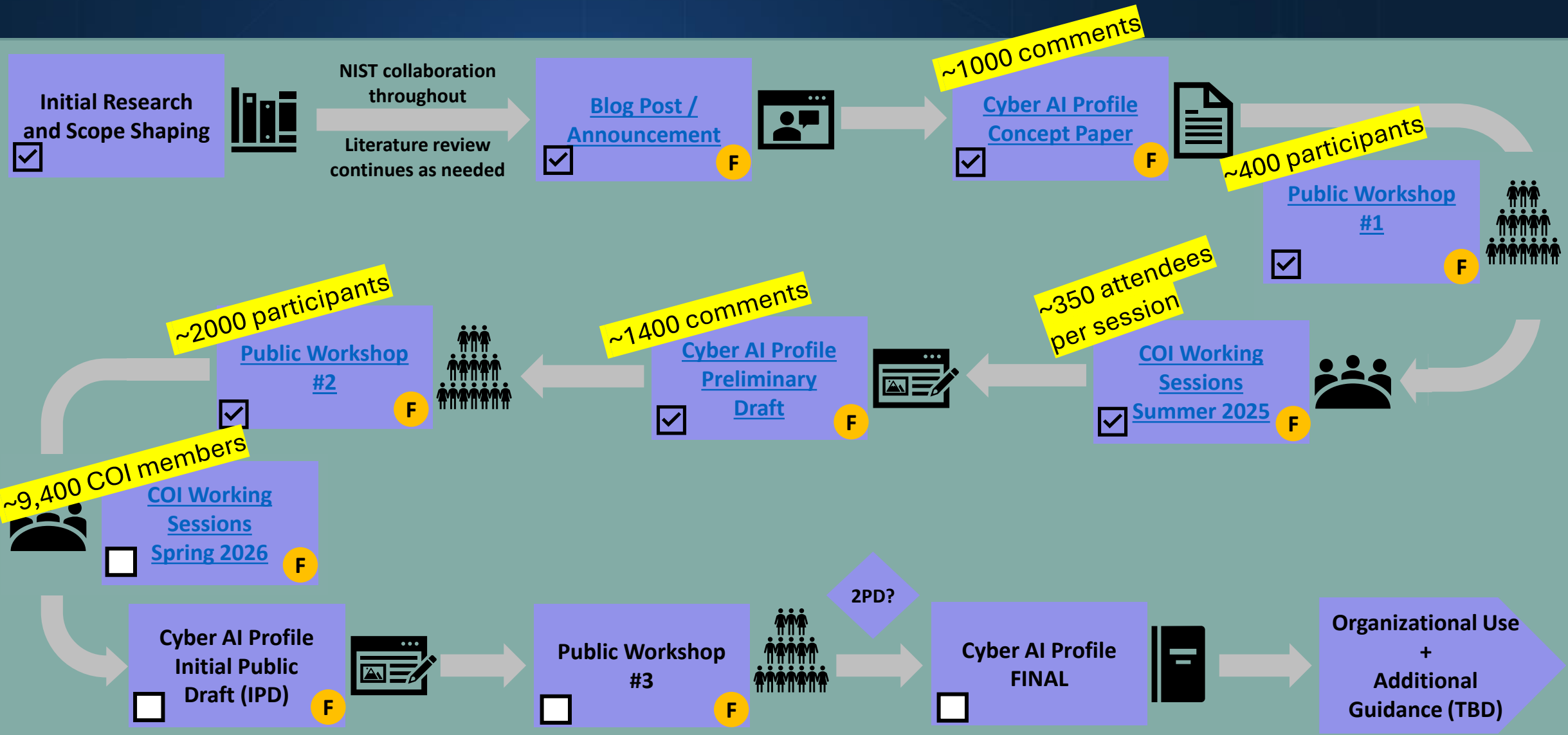
- Cybersecurity risks that arise from the use of AI by organizations, including securing AI systems, components, and machine learning infrastructures, and minimizing data leakage.
- Determining how to defend against AI-enabled attacks.
- Assisting organizations in the use of AI with their cyber defense activities and using AI to improve privacy protections.

## Outcomes:

- Establishes a shared understanding of AI-related cybersecurity terminology and considerations
- Fosters collaboration and communication across the AI and cybersecurity communities
- Enables organizations to measure their current practices, understand the available references, and identify gaps to update Organizational Profiles and roadmaps

# Cyber AI Profile Roadmap

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE




F Opportunities for COI/public stakeholder feedback (NOTE: Internal NIST collaboration occurs throughout)

# Overall Outcomes of COI Engagement

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

### Concept Paper

- Confirmed the need for guidelines
- Agreed the NIST CSF was the right starting point
- Identified key challenges

### Workshop #1

- Validated direction of the Profile
- Identified critical topics
- Proposed priorities and resources

### Summer 2025 COI Working Sessions

- Refined cybersecurity priorities for each Focus Area

### Workshop #2

- Continued refining Profile direction and content
- Shared insights regarding implementation

### Preliminary Draft Comments

- Informed continued build out of Profile
- Raised areas for further engagement with the COI

Workshop #1 Blog Post

Workshop #2 Blog Post

# Additional Resources

**Cyber AI Profile**

- NIST Cybersecurity, Privacy, and AI Program
- Blog post:  Managing Cybersecurity and Privacy Risks in the Age of Artificial Intelligence: Launching a New Program at NIST | NIST
- NCCoE Project Page: Cyber AI Profile
- Cybersecurity and AI Workshop Concept Paper (posted in advance of the April 3, 2025, workshop)
- April 2025 Cyber AI Profile Workshop recording
- Blog post:  Reflections from the First Cyber AI Profile Workshop
- Blog post: Reflections from the Second Cyber AI Profile Workshop
- Cyber AI Profile COI Working Sessions Introduction Video

**NIST Cybersecurity Framework**

- NIST CSF
- NIST CSF FAQs
- NIST CSF 2.0 Informative References
- NIST CSF Events

**NIST Resources for Applying NIST Frameworks**

- Resources for Applying NIST Frameworks

**Community Profiles**

- Examples of Community Profiles
- Creating Community Profiles FAQs

Cyber AI Profile Project Page

# Today's Plan

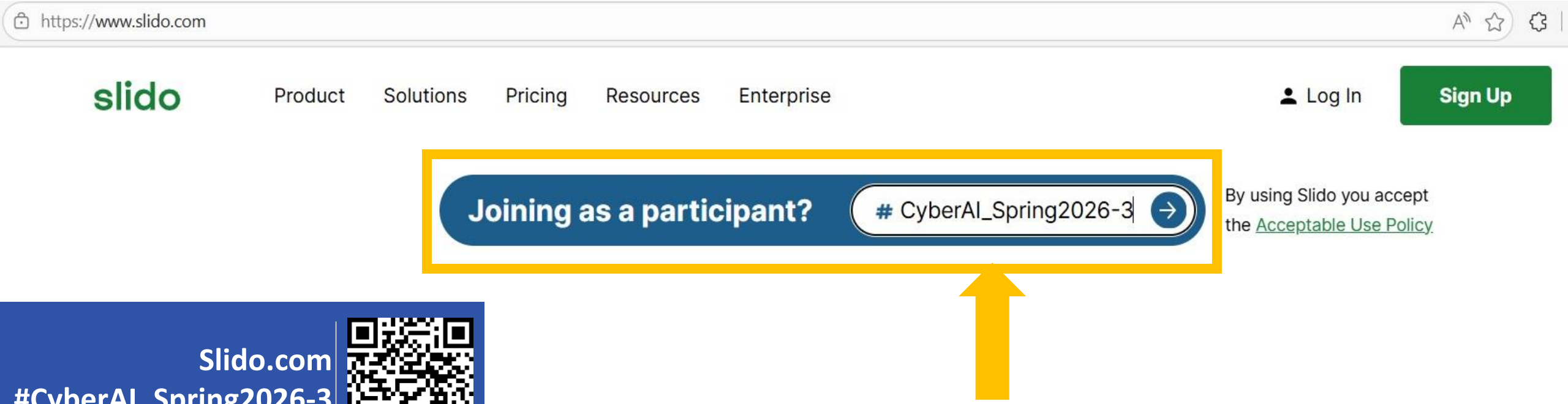
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# How You Contribute Today

- **Please raise your virtual hand or type in the chat to contribute**
- Members of the press, please identify yourself and your organization
- Be respectful of others
- Please don’t be shy – we would love to hear from everyone!
- **Please remain on mute when not speaking**
- **We will use Slido to facilitate some of our discussions**

# Using Slido

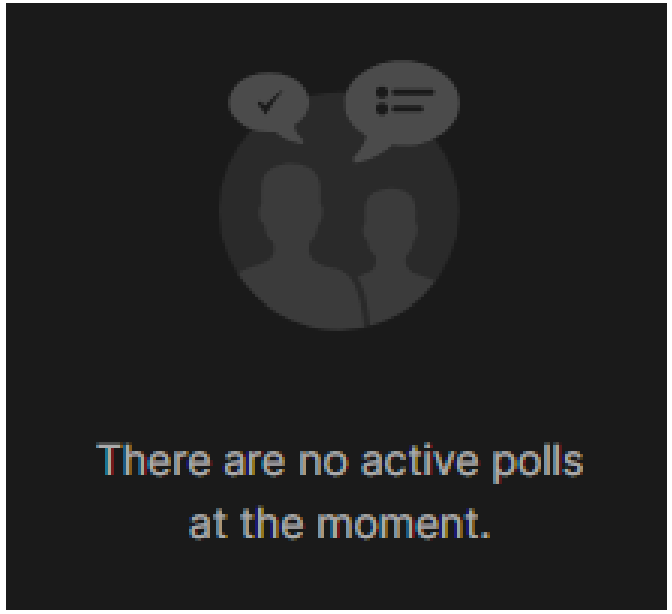
- We will be using Slido to facilitate some of our discussions
- Options to join via QR code or URL + event code
- Works on mobile phone and computer
- Responses are anonymous



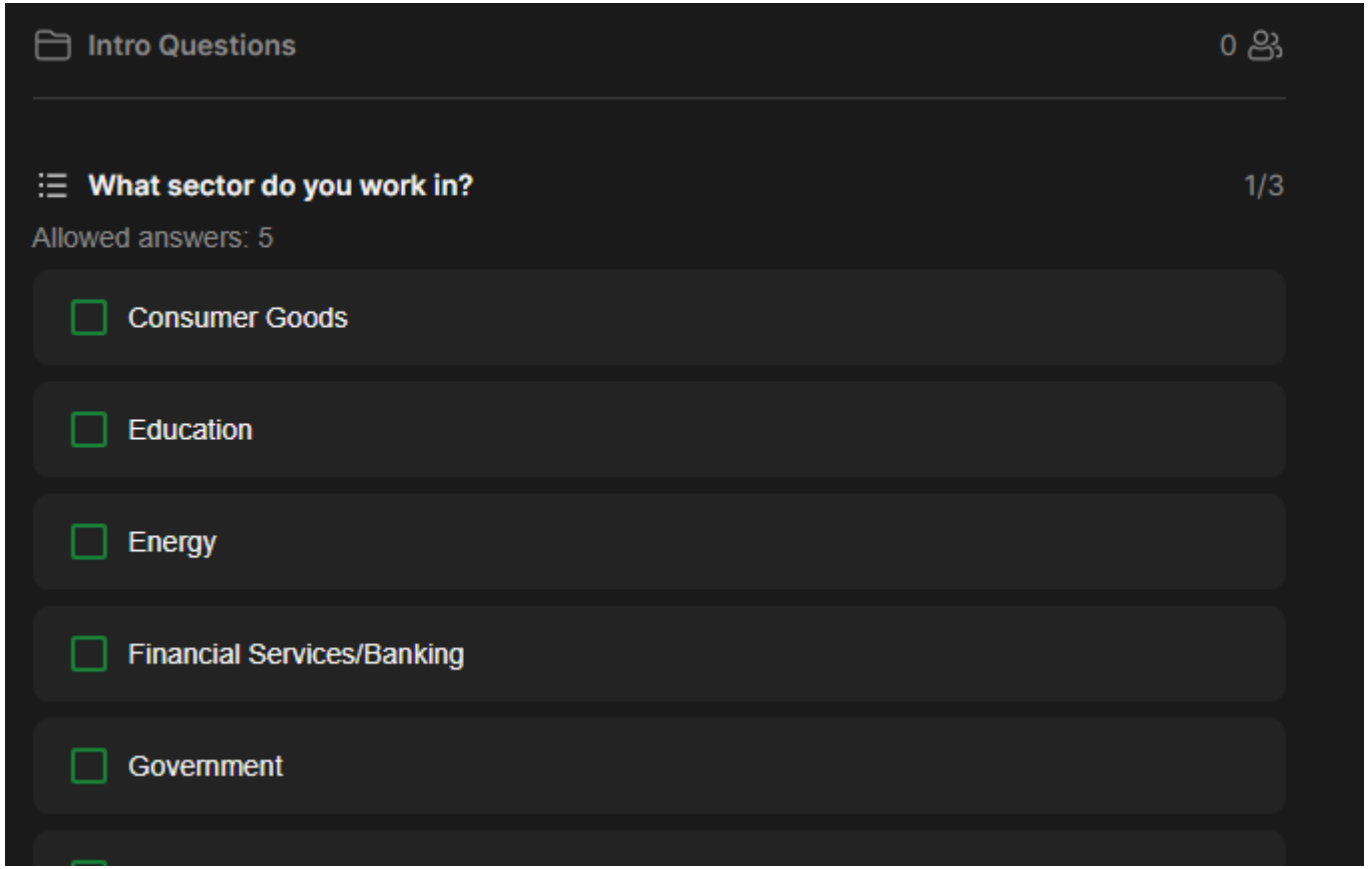

**Slido.com**
**#CyberAI_Spring2026-3**

# Slido Screens

## No Active Polls




## Active Polls

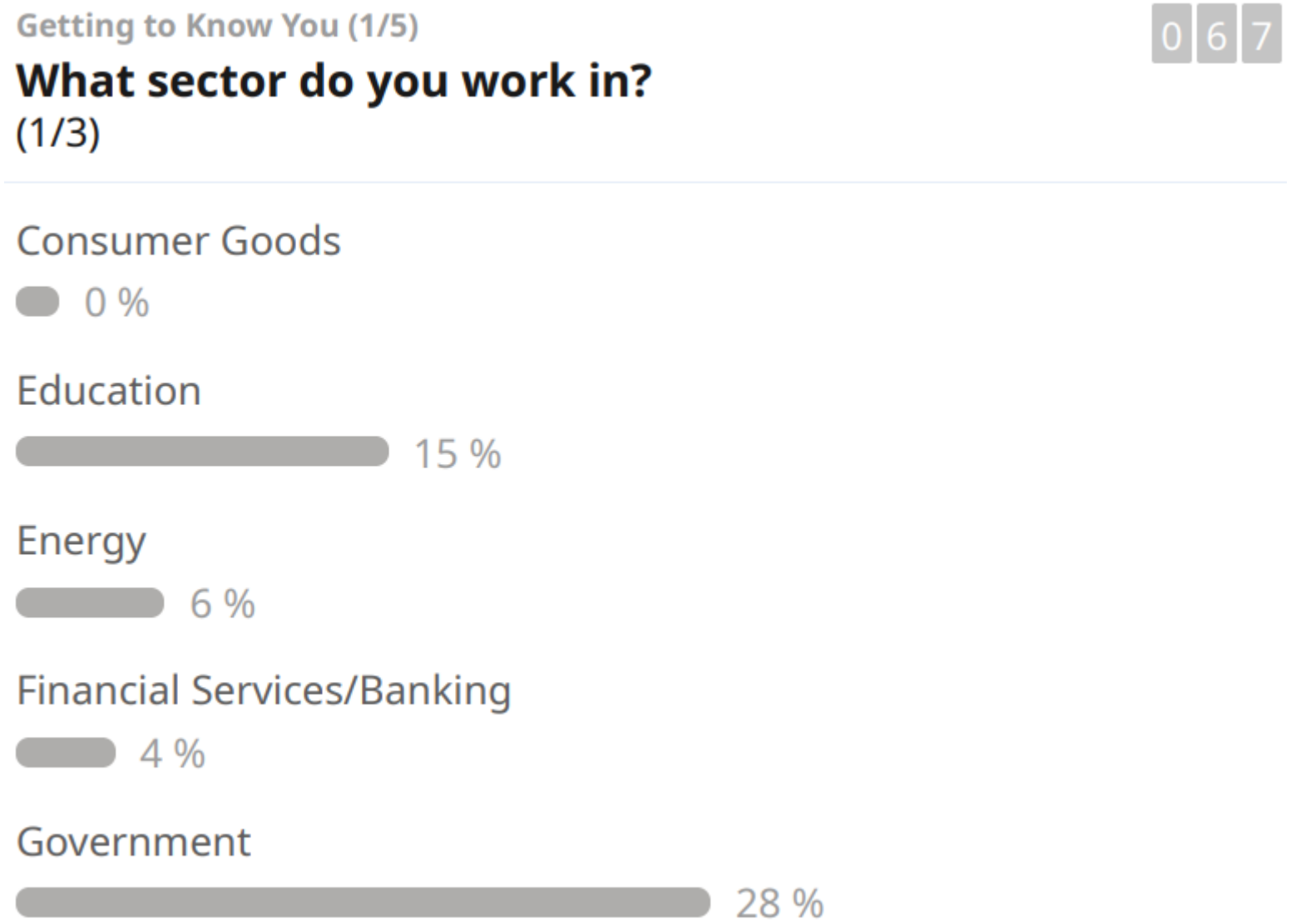


# Slido: Getting to Know You

- What sector do you work in?
- Which NIST Frameworks does your organization use?
- Which Cyber AI Profile materials have you read?
- If you are already using the Preliminary Draft of the Cyber AI Profile, how are you using it?
- Did you have an opportunity to provide feedback on the Cyber AI Profile Preliminary Draft during the public comment period?

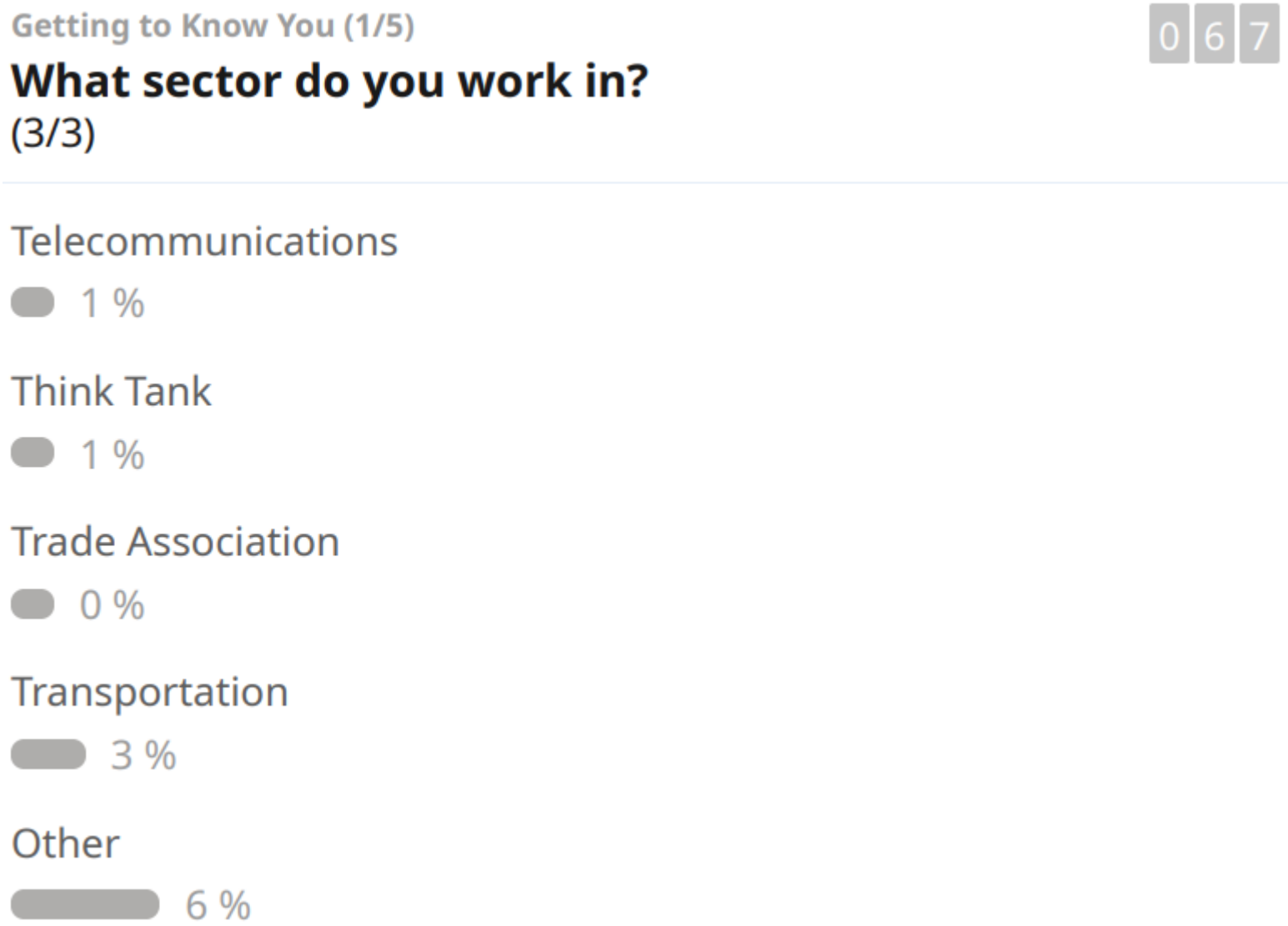
**Slido.com**
**#CyberAI_Spring2026-3**

# Slido: Getting to Know You

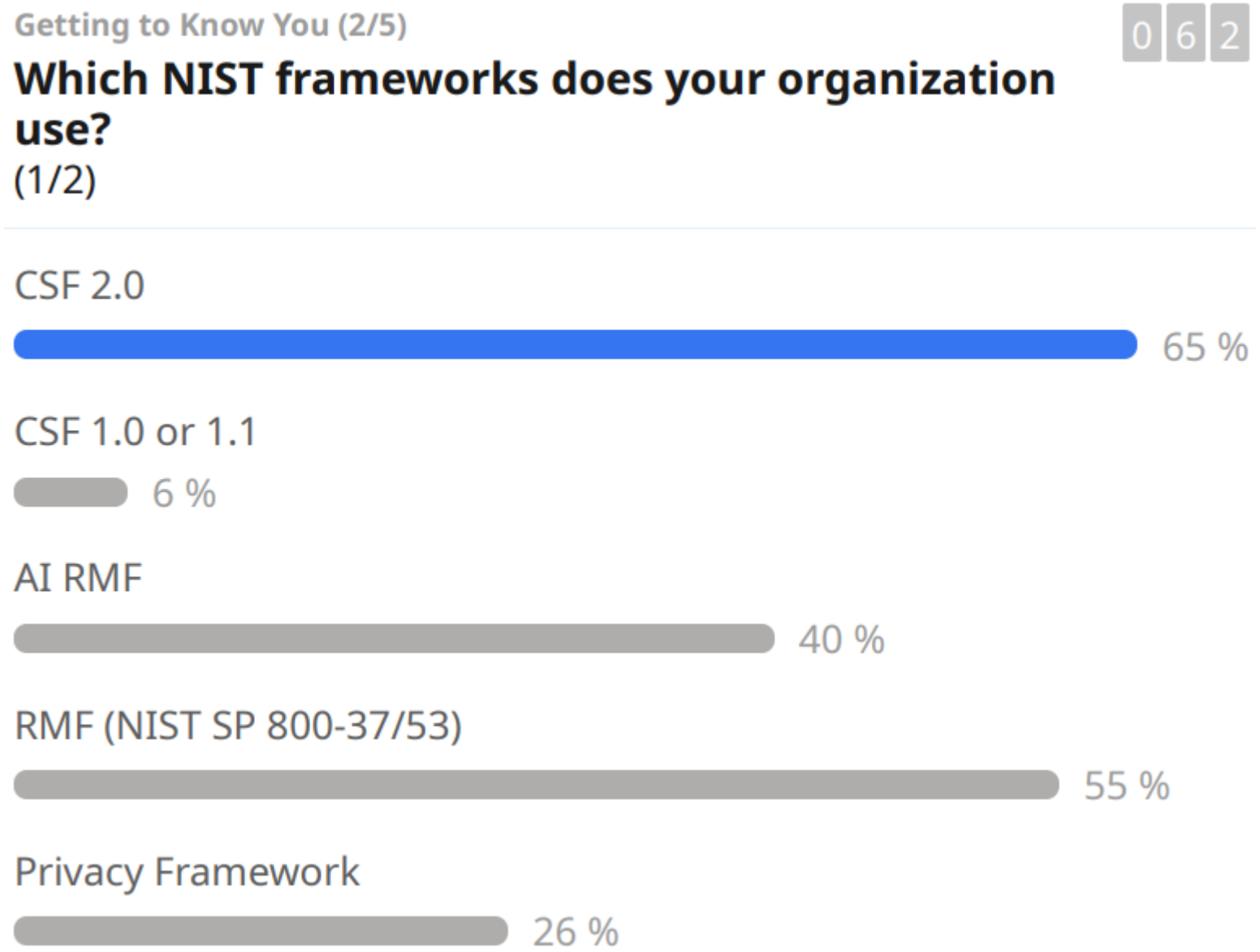


# Slido: Getting to Know You

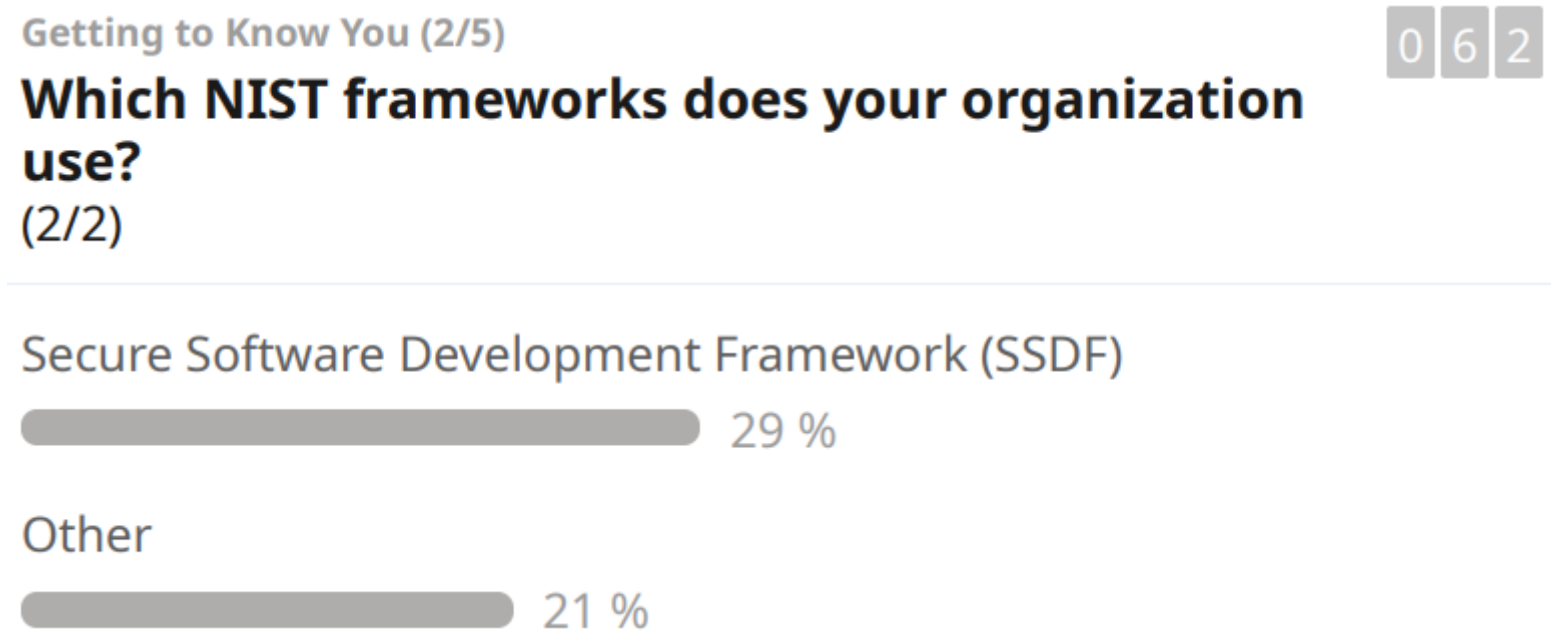
# Slido: Getting to Know You



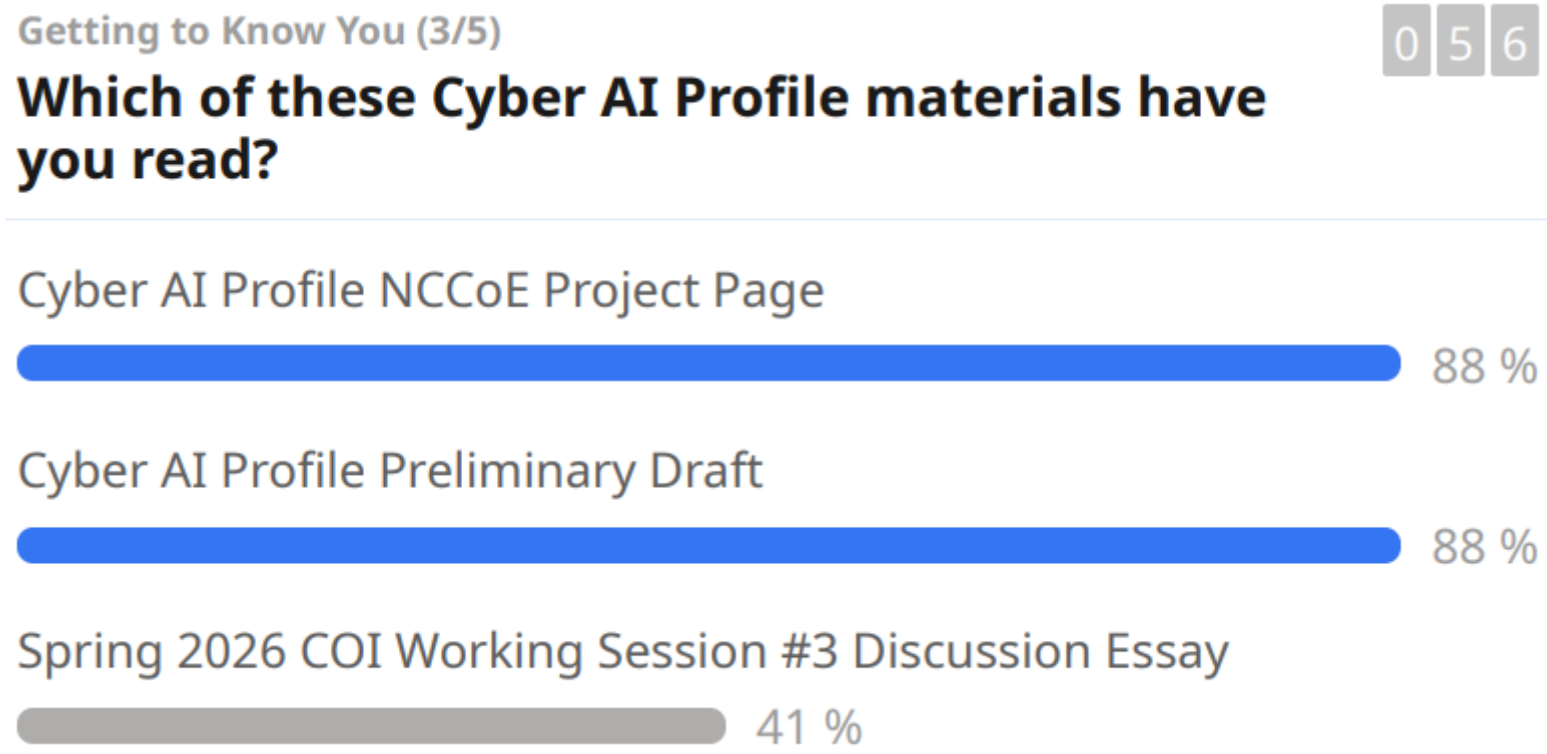
# Slido: Getting to Know You



# Slido: Getting to Know You



# Slido: Getting to Know You



# Slido: Getting to Know You

Getting to Know You (4/5)

0 1 2

**If you are already using the Preliminary Draft of the Cyber AI Profile, how are you using it?**
(1/2)

- Reviewing the profile through the lens of enterprise AI cybersecurity workflows, operational usability, human oversight, and implementation considerations for AI-enabled cyber defense and resilience systems.
- Not yet
- Using it on the Enterprise Grade Customers
- Taking notes for how our AI processes are to be augmented and adopted into our current environment
- As guidance for our GRC programs.
- No, frameworks consensus. Privacy acts in place and some cloud etc..
- Updating the know-how based on latest developments in standards
- Not yet
- Not yet
- As a baseline to guide internal IT operations.

# Slido: Getting to Know You

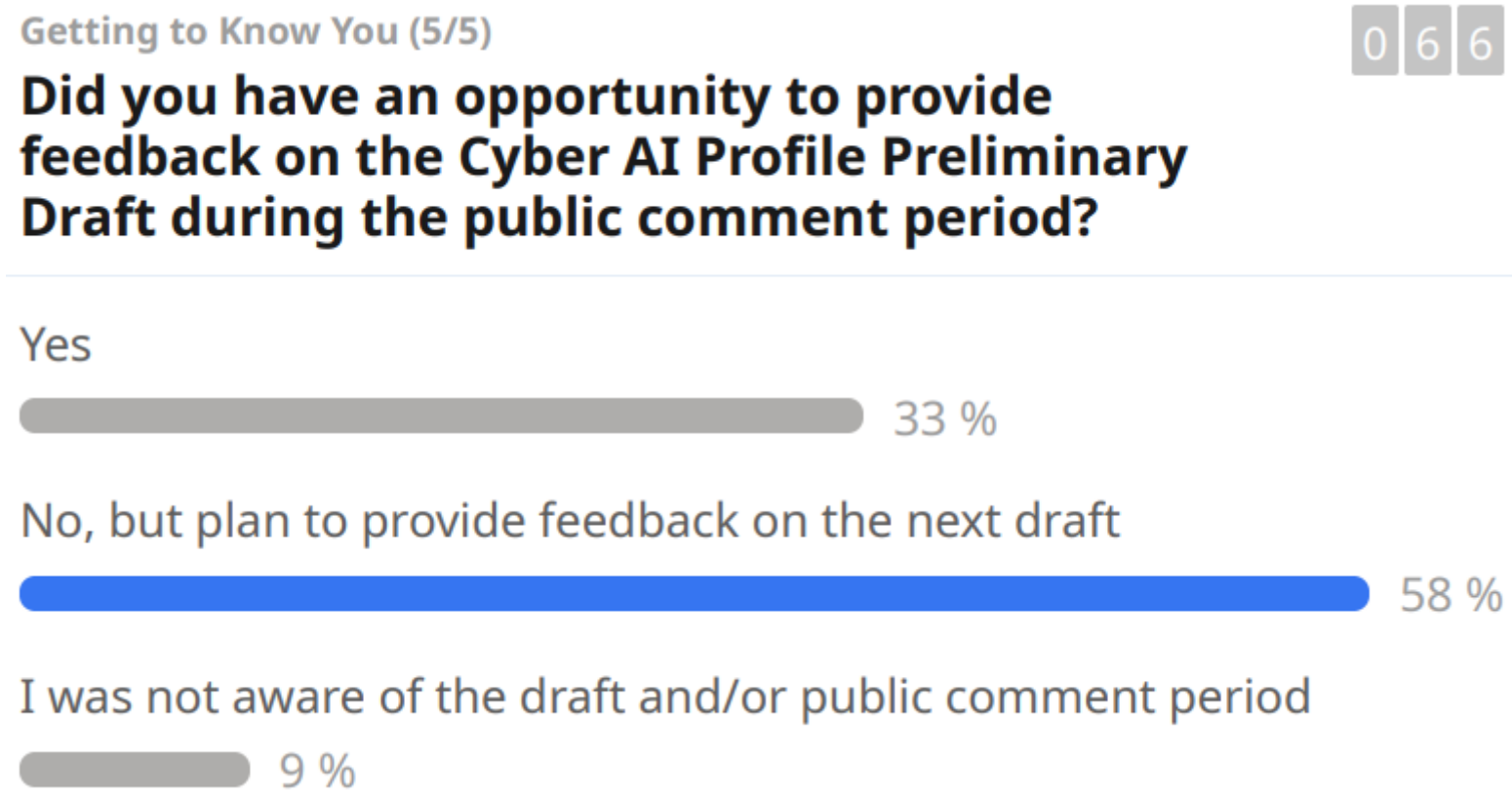
Getting to Know You (4/5)

0 1 2

**If you are already using the Preliminary Draft of the Cyber AI Profile, how are you using it?**
(2/2)

- N/A
- Continuously improving

# Slido: Getting to Know You



# General Discussion Plan

- Summary of feedback on the topics (roles, supply chain, and delivery formats)
- Review proposed options
- Facilitated discussion
- How we plan to use this feedback

# Today's Focus: Usability of the Profile

- Incorporating and supporting roles, including drawing out content related to Supply Chain and AIBOMs
- Discussion delivery formats for the final Cyber AI Profile

Discussion Essay #3

Cyber AI Profile Draft

# Incorporating Roles

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Roles: Summary of Feedback

**Feedback on the Preliminary Draft indicated a need to provide revisions to address the unique roles and responsibilities of AI developers, deployers, and consumers and included requests to:**

Include new AI-specific roles and responsibilities in CSF Considerations

Highlight the differentiating responsibilities of developers, deployers, and end-users

# NIST AI RMF: AI Actors

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

**Adopt representative list derived from NIST AI RMF:**

## AI Developers

Provide the **initial infrastructure of AI systems**

Responsible **for model building and interpretation tasks**, including the creation, selection, calibration, training, and/or testing of models or algorithm

**Examples:**
machine learning experts, data scientists, developers

## AI Deployers

Responsible for **contextual decisions** relating to how the AI system is used **to assure deployment of the system into production**.
Includes piloting the system, checking compatibility with legacy systems, ensuring regulatory compliance, managing organizational change, and evaluating user experience

**Examples:**
system integrators, software developers, end users, operators and practitioners, evaluators

## AI Governance

Retains **management, fiduciary, and legal authority and responsibility** in which an AI system is designed, developed, and/or deployed

**Examples:**
organizational management, senior leadership, Board of Directors

## End Users

**Use the system** for specific purposes within organizational restrictions **and can range in competency** from AI experts to first time technology end users

**Examples:**
individuals, groups

# Roles: Proposed Options

**Option 1:**

**Differentiate unique aspects of AI roles within an organization in Section 1.3 to highlight the shared responsibilities across the 3 Focus Areas:**

- Sets the Audience scope early in the Cyber AI Profile
- Effective communication with leadership

NIST's preferred option

**Option 2:**

**Include specific roles, based on the AI actors and actor tasks discussed in the Cyber AI Profile's Sample Focus Area Considerations as referenceable elements to augment new AI-specific personnel**

- Helps organization's identify roles and responsibilities directly in the Sample Focus Area considerations
- Enables organizations to develop own responsibility matrices
- Portability of the CSF Sample Considerations

# Roles: Option 1

**Option: Create a shared responsibility matrix across the 3 Focus Areas**

- E.g., Section 1.3 (Audience)
- Focus on shared AI roles
- NIST AI RMF AI roles as the standard

***Section 1.3 modifications is provided as an example**

**1.3. Audience**

The Cyber AI Profile is intended for any organization that:

- AI Users and Consumers: Use AI technologies, including stand-alone AI systems (such as chatbots and document summarizers) and AI-enabled capabilities embedded in other systems (such as AI used to analyze and balance demand across a power grid), regardless of whether those technologies are purchased or internally developed;
- AI Developers and Deployers and Users of 3rd Party AI Providers: Seek to understand and take advantage of the cybersecurity capabilities that AI can provide, such as AI-driven analytics within cybersecurity tools;
- AI Developers and Deployers: Would like to better understand and defend against AI-enabled cyber-attacks (e.g., against adversaries using AI to generate convincing malicious emails)

This Cyber AI Profile can be used by organizations to identify and communicate cybersecurity expectations regarding AI with internal and external stakeholders. The Profile can also be used by organizational leadership to generate priorities tailored to the operational aspects of the organization.

To complement this Cyber AI Profile and support the adoption of the AI Risk Management Framework, NIST is developing a series of *Control Overlays for Securing AI Systems (COSAiS)* using the NIST Special Publication (SP) 800-53 controls. Control overlays enable organizations and communities of interest to tailor the controls (or control baselines) for their specific context and needs. COSAiS w additional implementation-fo idelines and assist users an AI systems ma e unique ris use cases:

- Adapting & Using Ge
- Using & Fine-Tuning
- Using Agentic AI: Sin Multi-Agent

Learn more about the Contro Project, Slack space, and how to join the Slack channel at: https://csrc.nist.gov/projects/cosais
Questions and comments can be directed to overlays-securing-ai@list.nist.gov.

**Describe unique and shared AI roles and responsibilities under Section 1.3, Audience**

# Roles: Option 2 (NIST's Preferred Option)

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

**Option: Create a separate element dedicated to AI Roles**

- E.g., Section 2.4 (CSF Considerations)
- Focus on relevant use cases
- NIST AI RMF AI roles as the standard

***Section 2.4 is provided as an example**

| CSF 2.0 Core: GOVERN | General Considerations | Focus Area Proposed Priorities & Considerations | | |
|---|---|---|---|---|
| | | Secure | Defend | Thwart |
| **GOVERN (GV)** | The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored | | | |
| **Organizational Context (GV.OC)** | The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood | | | |
| **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management | **General Considerations:** No general considerations identified—see Focus Area Considerations.<br><br>**Example Informative References:** NIST SP 800-53, Rev 5: PM-11<br><br>**Roles:** AI Governance, End Users, ... | **Proposed Priority: 3**<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain<br><br>**Roles:** AI Developers, AI Deployers | **Proposed Priority: 3**<br><br>**Sample Opportunities:** Standard cybersecurity practices apply.<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** ENISA Threat Landscape 2025; DASF 50; ATLAS AML.M0020; OWASP AI Exchange: AI Security Overview; https://arxiv.org/pdf/2311.05232; NIST AI 100-2e2025<br><br>**Roles:** AI Developers, AI Deployers | **Proposed Priority: 3**<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** AI-specific Example Informative References pending additional inputs.<br><br>**Roles:** End-Users |

SAMPLE TEXT PROVIDED FOR DISCUSSION PURPOSES ONLY

# Roles: Proposed Options

**Option 1:**

**Differentiate unique aspects of AI roles within an organization in Section 1.3 to highlight the shared responsibilities across the 3 Focus Areas:**

- Sets the Audience scope early in the Cyber AI Profile
- Effective communication with leadership

**Slido.com**
**#CyberAI_Spring2026-3**

**NIST's preferred option**

**Option 2**

**Include specific roles, based on the AI actors and actor tasks discussed in the Cyber AI Profile's Sample Focus Area Considerations as referenceable elements to augment new AI-specific personnel**

- Helps organization's identify roles and responsibilities directly in the Sample Focus Area considerations
- Enables organizations to develop own responsibility matrices
- Portability of the CSF Sample Considerations

# Roles: Proposed Options

**What is your preferred option for handling roles in the Profile?** 0 4 0

Option 1: Differentiate unique aspects of AI roles within an organization in Section 1.3 to highlight the shared responsibilities across the 3 Focus Areas

15 %

Option 2: Include specific roles, based on the AI actors and actor tasks discussed in the Cyber AI Profile's Sample Focus Area Considerations as referenceable elements to augment new AI-specific personnel (NIST's preferred option)

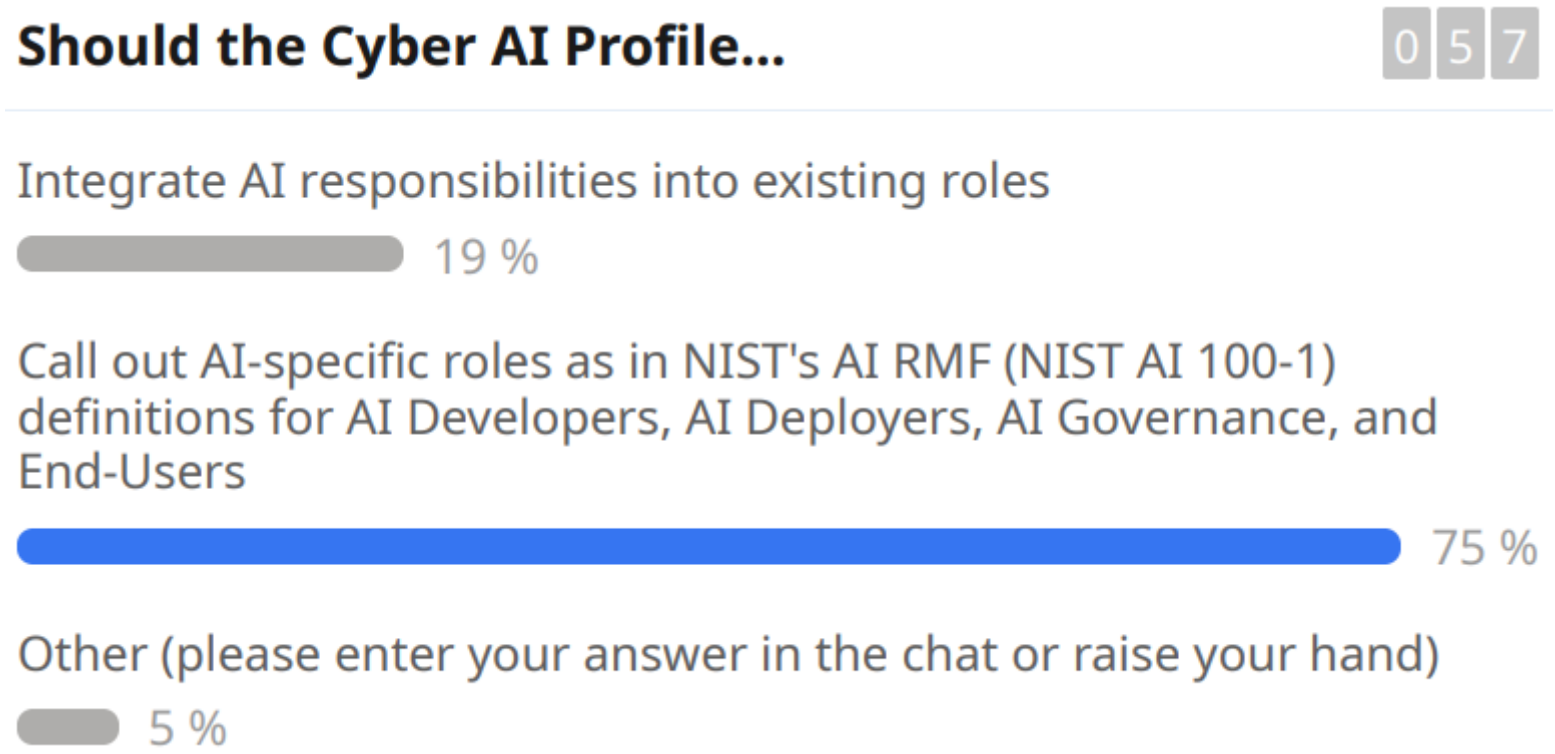
85 %

# Roles: Questions for Discussion

- Should the Cyber AI Profile:
  - Integrate AI responsibilities into existing roles
  - Call out AI-specific roles as in NIST's AI RMF (NIST AI 100-1) definitions for AI Developers, AI Deployers, AI Governance, and End-Users
  - Other?

Slido.com
#CyberAI_Spring2026-3

# Roles: Questions for Discussion



# Addressing Supply Chain

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Supply Chain: Summary of Feedback

**Feedback on the Preliminary Draft indicated a need to provide revisions to address the criticality of the Supply Chain of AI and include requests to:**

- Provide richer citations and informative references to existing standards and specifications
- Highlight that data is a critical piece of AI's supply chain
- Elevate prioritizations within CSF Considerations where Supply Chain is addressed
- Provide illustrative case studies and examples of Supply Chain attack vectors as referenceable materials

# Supply Chain: Proposed Options

NIST's preferred option

**Option 1:**

**Create a separate section dedicated to AI Supply Chain to address relevant use cases and highlight its importance in the CSF Sample Considerations**

- Improves visibility and transparency
- Calls out specific components of AI systems
- Strengthens procurement decisions for models, data, and 3rd

**Option 2:**

**Elevate visibility of supply chain in CSF Sample Considerations**

- Highlights the criticality of supply chain directly in line with relevant CSF Subcategories
- NOTE: Prioritizations may be removed in future Cyber AI Profile document

# Supply Chain: Option 1 (NIST's Preferred Option)

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

**Option 1: Create a separate section dedicated to Supply Chain**

- E.g., Appendix item
- Focus on AI data
- Supply Chain as a standalone topic

**Table of Contents**



**List of Tables**



***Appendix E is provided as an example**

**Describe Supply Chain and its importance under a new Appendix item**

# Supply Chain: Option 2 (GV.SC Example)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## Option 2: Elevate visibility of the Supply Chain of AI

- E.g., Section 2.4 (CSF Considerations)
- Focus on relevant use cases
- Higher prioritization where supply chain is explicitly discussed

***GV-SC-01 from Section 2.4 is provided as an example**

| CSF 2.0 Core: GOVERN | General Considerations | Focus Area Proposed Priorities & Considerations: Secure | Defend | Thwart |
|---|---|---|---|---|
| **GOVERN (GV)** | The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored | | | |
| **Cybersecurity Supply Chain Risk Management (GV.SC)** | Cyber supply chain risk management processes are identified, established, managed, monitored, and im | | | |
| **GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders** | **General Considerations:** Organizations need to understand the origins of AI components (e.g., microservices, containers, libraries, data, hardware software), the new vulnerabilities they may introduce, and their potential impacts to cybersecurity.<br><br>**Example Informative References:** NIST SP 800-53, Rev 5: PM-30; SR02; SR-03; Reflections from the First Cyber AI Profile Workshop<br><br>SAMPLE TEXT PROVIDED FOR DISCUSSION PURPOSES ONLY | **Proposed Priority: 1**<br><br>**Sample Focus Area Considerations:** With AI, data provenance should be weighted just as heavily as software and hardware origin. All data input (both training and inference input) is an aspect of the supply chain for AI. With RL, data comes from the environment it is trained in. Take special care that the environmental conditions of the model are aligned with supply chain risk.<br><br>**Example Informative References:** DASF 22, 23, 32, 45, 51, 53; ATLAS AML.M0023; OWASP AI Exchange: General Governance Controls; | **Proposed Priority: 1**<br><br>**Sample Focus Area Considerations:** The integrity of training and input data (part of the data supply chain) should be verified to detect and prevent data poisoning and tempering. In some organizations, RL can be used to detect malicious activity on a network. For example, a model that uses online learning is constantly improving from day-today activity. A malicious actor could work out how to trigger the alarm system in the model, while keeping the network intact and operating normally. Overtime, the model may "learn" that this behavior is creating false alarms and cease to alert operators when this behavior happens in the future. Protecting against this requires careful consideration of how the model is trained (i.e., do not allow online training or validate datasets). | **Proposed Priority: 1**<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply. (Rationale) Suppliers and third parties with access to internal data, systems, and software may be the target of AI-enabled cyber attacks.<br><br>**Example Informative References:** NIST SP 800-161 Rev. 1; AI 100-2e2025 |

# Supply Chain: Option 2 (ID.AM Example)

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## Option 2: Elevate visibility of the Supply Chain of AI

- E.g., Section 2.4 (CSF Considerations)
- Focus on relevant use cases and sub-categories

| | | | | |
|---|---|---|---|---|
| **IDENTIFY (ID)** | The organization's current cybersecurity risks are understood | | | |
| **Asset Management (ID.AM)** | Assets (e.g., data, hardware, software, systems, facilities, services, people) 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 | | | |
| **ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained** | **General Considerations: No general considerations identified - see Focus Area Considerations.**<br><br>**Example Informative References:**<br><br>**NIST SP 800-53, Rev 5: AC-04; CA-03; CA-09; PL-02; PL-08; PM-07** | **Proposed Priority: 1**<br><br>**Sample Focus Area Considerations:** **Address Supply Chain Considerations first.**<br><br>Categorize traffic into four distinct groups: internal human generated traffic, internal computer-generated network traffic (such as from cron jobs or automated processes), internal AI based traffic (AI tools searching the web or utilizing organizational resources), and external traffic.<br><br>Note that external traffic is difficult to categorize as human or bot generated. However, there is value in tracking network traffic surrounding model registries and dataset sources, to better detect attempted supply chain attacks.<br><br>**Example Informative References:** DASF 5, 7, 10-11, 13, 16, 18-19, 24, 28, 30-32, 41, 44, 48, 52, 56, 58-60, 62; OWASP AI Exchange: Controls to Limit the Effects of Unwanted Behavior; OWASP Conventional Runtime Controls; OWASP AI Exchange: General Governance Controls; OWASP AI Exchange: Model Access Control; OWASP LLM Top Ten: LLM03 Supply Chain; ENISA Threat Landscape 2025 | **Proposed Priority: 2**<br><br>**Sample Focus Area Considerations:** **Address Supply Chain Considerations first.**<br><br>Maintain representations of AI data flows, including the paths for inference requests, training data pipelines to enforce defense boundaries and detect anomalies.<br><br>**Example Informative References:**<br><br>DASF 38; ENISA Threat Landscape 2025; AI 100-2e2025 | **Proposed Priority: 2**<br><br>**Sample Focus Area Considerations:** **Address Supply Chain Considerations first.**<br><br>Standard cybersecurity practices apply. Understanding the network facilitates a clearer understanding of normal and abnormal traffic that can indicate a security event is occurring.<br><br>**Example Informative References:**<br><br>NIST SP 800-172 Configuration Management 3.4.1e-3.4.3e; ATT&CK M1015; ATT&CK M1028; AI 100-2e2025 |

SAMPLE TEXT PROVIDED FOR DISCUSSION PURPOSES ONLY

***ID.AM-03 from Section 2.4 is provided as an example**

# Supply Chain: Proposed Options

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

**NIST's preferred option**

**Option 1:**

**Create a separate section dedicated to AI Supply Chain to address relevant use cases and highlight its importance in the CSF Sample Considerations**

- Improves visibility and transparency
- Calls out specific components of AI systems
- Strengthens procurement decisions for models, data, and 3rd

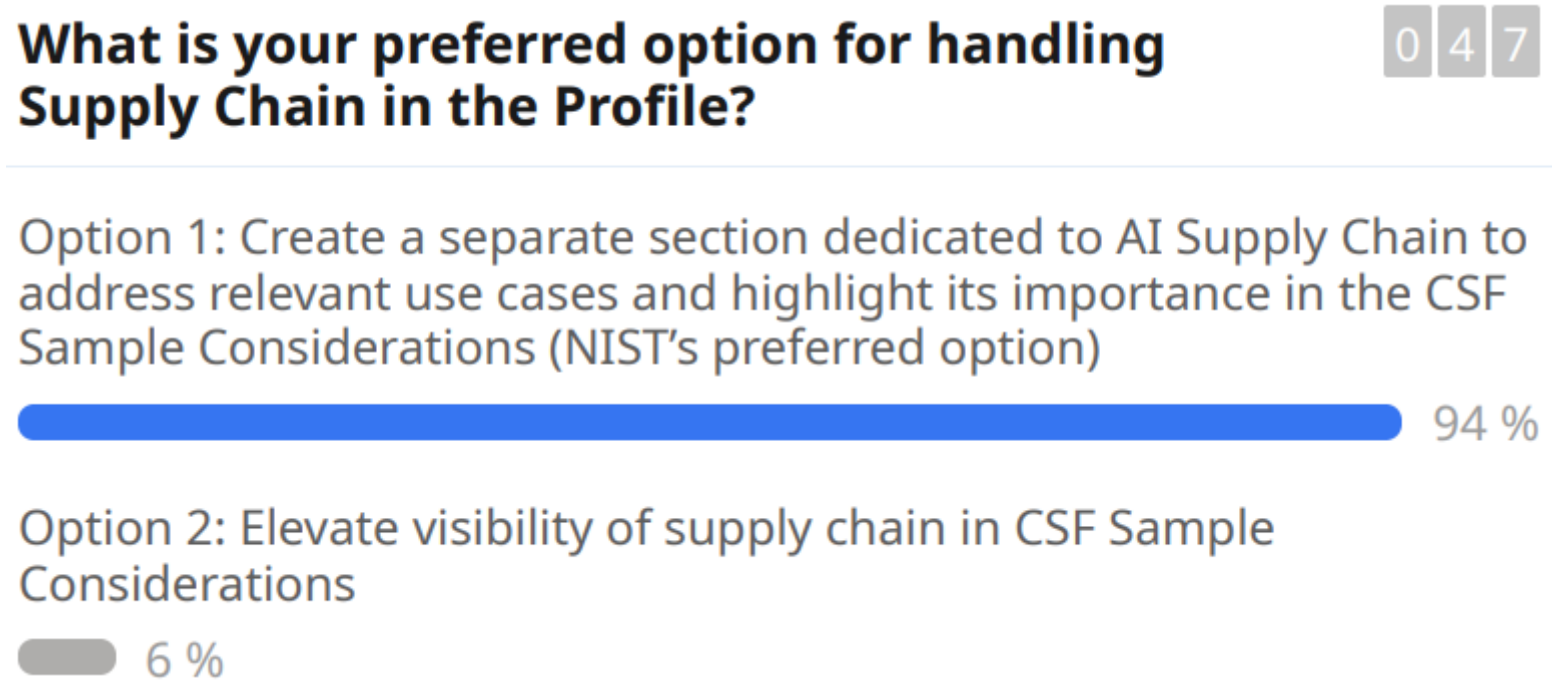
**Option 2:**

**Elevate visibility of supply chain in CSF Sample Considerations**

- Highlights the criticality of supply chain directly in line with relevant CSF Subcategories
- NOTE: Prioritizations may be removed in future Cyber AI Profile document

**Slido.com**
**#CyberAI_Spring2026-3**

# Supply Chain: Proposed Options



# Supply Chain: Questions for Discussion

- How should accountability be spread across the supply chain:
  - How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?
  - Are there other parties which share responsibility?

Slido.com
#CyberAI_Spring2026-3

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

0 2 8

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(1/11)

- While it seems most appropriate that developers and deployers should be engaged in post acquisition activities related to supply chain integrity, deployers and developers often view procurement as responsible. However procurement often does little after acquisition. So it would be beneficial to specifically assign responsibility
- Line of responsibility should be an integrated whole during the time of deployment and testing phase.
- organizations are using role-based governance, risk-tiering, contractual allocation, human oversight assignments, technical documentation, logging, and post-deployment monitoring to make responsibility auditable.
- The Responsibility Matrix • Developers

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

0 2 8

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(2/11)

(Providers): Accountable for "Secure-by-Design." They must ensure data integrity, bias mitigation, and provide an AI-BOM (Bill of Materials) for transparency. • Deployers (Operators): Accountable for "Secure-in-Context." They manage the integration, set the "Human-in-the-Loop" guardrails, and are responsible for the specific data fed into the system. • Users (Consumers): Accountable for "Compliant Usage." They must follow operational guidelines and are responsible for the final application of the AI's output.

- Sharing information based on: 1. Experience, trial& error mistakes 2. Smoothly running executions from the beginning to

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

0 2 8

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(3/11)

the end of the task and delivery 3. Major hitches, related to security and safety issues.

- Organizations are handling AI responsibility through existing roles — security, legal, procurement, IT, app owners, and business owners — rather than through clean AI-specific
- What many organizations are doing now is defining AI responsibility as a shared effort across developers, deployers, and users instead of placing ownership on a single team. Developers handle secure and trustworthy design, deployers focus on operational security, monitoring, and compliance, while users are expected to use AI responsibly and validate outputs. The more mature programs are aligning this structure

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

0 2 8

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(4/11)

with the National Institute of Standards and Technology AI RMF and National Institute of Standards and Technology by embedding AI governance into existing cybersecurity, risk, privacy, and compliance processes rather than creating separate frameworks. The key is establishing clear accountability, oversight, and continuous monitoring from the beginning of the AI lifecycle.

- AI policies, ongoing training and continuous monitoring
- AI Governance committees and defining roles and responsibilities for all staff.
- Organizations should define clear lifecycle accountability across AI developers, deployers, and users,

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

0 2 8

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(5/11)

covering design intent, data quality, validation, monitoring, incident response, and operational impact.

- You'll need to communicate accountability rests with leadership. Developers, deployers, and users have accountability but without leadership accountability/responsibility, it'll be hard to drive action.

- AI accountability should be treated as a shared responsibility across the full AI supply chain, but it should not be diluted or pushed entirely to one party. Each participant should be accountable for the risks they create, control, introduce, accept, or are best positioned to manage. Developers and model providers are responsible for designing, testing,

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(6/11)

documenting, and securing the AI system, including clearly explaining model limitations, data use, training practices, security controls, and material changes to the model or service. Deployers, such as the organization implementing the AI system, remain accountable for how the AI is used in the business environment. This includes approving the use case, determining whether sensitive or regulated data may be used, ensuring appropriate access controls and human oversight, monitoring system behavior, and formally accepting any

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(7/11)

residual risk. Even when a vendor provides the AI capability, the deploying organization still owns the business decision to use it and the operational impact it may create. End users also have responsibility, but they should not be the only line of defense. Users must follow acceptable use policies, avoid entering prohibited data, validate AI outputs before relying on them, and report issues such as inaccurate, inappropriate, or unexpected results. However, the organization must design governance and technical controls that do not depend solely on perfect user behavior.

- There is still need to have accountabilty for these roles in

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(8/11)

traditional sense and to incorporate AI accordingly. AI is still a (software) tool that woud be subject to controls, cyber security and due diligence etc as in software development life cycles.

- Assessing who holds ultimate responsibility and accountability? Developers create the product, deployers implement the product, and users will use whatever product has been purchased. Transparency in the workflows will help assess who holds liability in the event of harm.
- Data responsibility has to move away from the organization and toward the source. Data provenance and data inventories play a mutually supportive role in understanding the nature of the

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(9/11)

data and metadata, as well as the requirements that travel with them (e.g. use agreements, consent). Data accountability flows upstream to developers/sources, while organizational impact accountability flows to leadership.

- Hospitals are struggling to do any of this with BAAs and risk shifting with third party AI vendors
- Contracts, Documents of Understanding or other agreements, RACI, Cyber Insurance,
- 1. Contracts 2. AI Use Policies 3. Data sheets and model guides 4. RACI charts (ad hoc perhaps...)
- They are still crafting lines that incorporate AI demands. However, older framework are still in use
- Who is responsible accountable and informed We

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(10/11)

have to share responsibilities including third parties

- The pattern that is emerging is "shared but structured accountability" across the AI lifecycle.
- Working with finance teams to stop allowing credit card purchases of AI subscriptions requiring enterprise agreements/contracts. Holding developers/deployers to the same standards as traditional developers, educating users on safe AI use, understanding where enterprise agreements exist, what data can and cannot be introduced into AI systems.
- RACI
- The developer of the system architecture

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (1/2)

028

**How are organizations today establishing the lines of responsibility among developers, deployers, and users in the context of AI systems?**
(11/11)

should be responsible for this.

- Simply add responsibility to the role but NIST should provide examples or best practices
- IT governance policies
- Block all, allow only trusted or approved post security review
- It seems like the wild west at the moment. We are even seeing others start to develop using AI coding like CFOs.

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

024

## Are there other parties which share responsibility?

(1/7)

- Governance, RM, System Authorization
- Supply Chain vendors and personnel.
- the party with control over a risk decision should carry responsibility for that decision, and the party accepting residual risk should be named, documented, and auditable.
- Yes, several "hidden" parties are critical to the chain:

• Data Providers: Responsible for the legal lineage and ethical sourcing of training datasets. • Infrastructure/Cloud Providers: Accountable for the physical and logical security of the hardware where the AI

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

024

## Are there other parties which share responsibility?

(2/7)

resides. • Open-Source Curators: Responsible for the integrity of public repositories to prevent "poisoning" or malicious code injection. • Third-Party Auditors: Independent entities accountable for verifying compliance and safety benchmarks.

- 1. The umbrella organisation(s) "overlooking" developers, deployers, and users of the AI-system(s) in use and under scrutiny.

2. Feedback to organisations like NIST, IEEE to look into the technical details.

- Responsibility should be shared among all interested parties.
- Vendors/ Suppliers
- In practice, responsibility extends well beyond developers, deployers, and users. The organizations building mature AI

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

024

## Are there other parties which share responsibility?

(3/7)

governance programs are also involving: -Executive leadership for risk acceptance, governance direction, and strategic oversight. -Cybersecurity and GRC teams for AI risk assessments, controls, monitoring, and compliance alignment. -Legal and privacy teams to address regulatory, contractual, intellectual property, and data protection concerns. -Data owners and business units to ensure data quality, appropriate use cases, and business accountability. -Third-party vendors and providers since many AI capabilities rely on external models, APIs, or cloud platforms.

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

0 2 4

## Are there other parties which share responsibility?

(4/7)

-Audit and compliance teams for independent validation and continuous assurance. -Human oversight reviewers/leaders who validate critical AI-driven decisions and reduce operational or ethical risks.

- Everyone is responsible for AI within an organization.
- The orgs IT/InfoSec teams.
- Yes. Shared responsibility also includes data owners, model vendors, cloud providers, regulators, auditors, cybersecurity teams, legal, risk, and business owners.
- Leadership
- Other parties also share accountability, including cloud providers, system integrators, data owners, procurement, legal, privacy, compliance, and security GRC. These groups help ensure that contracts, data protections, access controls, monitoring,

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

0 2 4

## Are there other parties which share responsibility?

(5/7)

audit rights, incident response, and regulatory expectations are properly addressed. AI accountability should follow the full lifecycle of the system: from design and development to deployment, use, monitoring, and retirement.

- This article tries to delineate more on accountability and judgement, not just human in loop simply for review https://www.techpolicy.press/ai-efficiency-can-undermine-accountability-even-with-humans-in-the-loop/
- Organizations who collaborate with developers and implement technologies should also be held responsible--this includes those software programs that may not originate within the organization,

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

024

## Are there other parties which share responsibility?

(6/7)

however use SAAS integrated into an operating system where users will be required to incorporate into their day-to-day operations (e.g. Microsoft incorporating CoPilot).

- Usually not willing to take risk and cyber insurance costs increase and attack surface increased
- a. Data providers/brokers b. Infrastructure and cloud providers c. Third party evaluators/auditors d. Regulators/Int'l standards bodies e. Affected (Harmed) people and their representatives (regulators/lawyers) f. Insurers
- Vendors as third parties
- Mostly have to share with developers and some third party users
- Yes! Beyond developers, deployers, and users, responsibility

# Supply Chain: Questions for Discussion

Supply Chain: Questions for Open Discussion (2/2)

0 2 4

## Are there other parties which share responsibility?

(7/7)

is also shared by model providers, CSPs, data suppliers, tool/plugin developers, auditors/regulators, and governance bodies overseeing AI use

- Procurement/Finance, Executive Management
- The system integrador and the deployer.
- Yes
- There must be 100% accountability when data loss occurs

# Break – 5 Minutes

Discussion Essay #3

Cyber AI Profile Draft

*Resume in 5 minutes*

# Incorporating AI Bill of Materials (AIBOM)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# AIBOM: Summary of Feedback

**Feedback on the Preliminary Draft indicated a need to provide revisions to address incorporating AIBOMs and include requests to:**

- Include new AIBOM definitions in context of SBOMs, Model Cards, and Data Cards
- Provide a minimum set of elements that for an AIBOM
- Utilize AIBOM references throughout the CSF Sample Considerations
- Remove (future) mentions of AIBOM to remain agnostic to specification and focus on outcomes of those materials

# AIBOM: Proposed Options

**Option 1:**

**Remove mentions of AIBOM from Cyber AI Profile**

- Remains agnostic to provenance and lineage mechanism
- Cyber AI Profile can be more broadly adopted
- Focuses Cyber AI Profile on the outcomes of provenance and attestation mechanisms

NIST's preferred option

**Option 2:**

**Reference AIBOM throughout Cyber AI Profile Sample Considerations and develop a minimum set of elements of an AIBOM**

- Enhance transparency of AI asset provenance and attestation in context of existing mechanisms (SBOM, Model and Data Cards)
- Clear, interoperable, target while AIBOM-development matures
- Identify initial minimum set of AIBOM elements

# AIBOM: Option 1

**Option 1: Do not include AIBOM references in CSF Sample Considerations**

- Reference mature SBOM, Model and Data Card mechanisms
- Focus on outcomes

***GV.SC—03 is provided as a Sample Consideration**

| CSF 2.0 Core: GOVERN | General Considerations | Focus Area P | | |
|---|---|---|---|---|
| | | Secure | | |
| **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes | **General Considerations:** No general considerations identified - see Focus Area Considerations.<br><br>**Example Informative References:** NIST SP 800-53, Rev 5: AC-01; AT-01; AU-01; CA-01; CM-01; CP-01; IA-01; IR-01; MA-01; MP-01; PE-01; PL-01; PM-01; PS RA-01; SA-01; SC-01; PM-09; PM-18; PM-3 02; SR-03; RA-03; RA | **Proposed Priority:** 1<br><br>**Sample Focus Area Considerations:** While the cybersecurity practices for managing supply chain risks remain the same when considering AI software, consider | **Proposed Priority:** 2<br><br>**Sample Focus Area Considerations:** Integrate AI-related risk considerations in cybersecurity supply chain risk management to prevent compromised models and lities.<br><br>025;<br><br>2025 | **Proposed Priority:** 3<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** NIST SP 800-161 Rev. 1 |
| **GV.SC-04:** Suppliers are known and prioritized by criticality | **General Considerati** general considerati see Focus Area Consi<br><br>**Example Informative References:** NIST SP 800-53, Rev 5: RA-09; SA-09; SR-06 | **Considerations:** Standard cybersecurity practices apply. (Rationale) AI-based services create a higher reliance on | **Considerations:** Rank AI models used for cybersecurity defenses according to potential adverse impacts if compromised so | **Proposed Priority:** 3<br><br>**Sample Focus Area Considerations:** Standard cybersecurity practices apply. |

**Introduce no changes to the Sample Considerations in referencing AIBOM and instead focus on outcomes of inventory and attestation mechanisms**

# AIBOM: Option 2 (NIST's Preferred Option)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## Option 2: Create a minimum set of elements of an AIBOM

- Better observability of supply chain considerations
- Focus on a minimum set of elements
- Frame within context of existing SBOM and Model/Data Card formats

**Appendix E. AI Bill of Materials (AIBOM) Elements**

| | |
|---|---|
| AIBOM record metadata | Unique AIBOM identifier, version, date created, date last updated, organization or tool that produced it |
| AI system identification | System/application name, short description, business purpose or use case, environment such as development, test, or production |
| System owner and maintainer | Business owner, technical owner, maintainer, and contact information |
| Model Card:<br>Model inventory | Each model used in the system, including model name, version, supplier or source, model type, and role in the system |
| Data Card:<br>Data inventory | Key datasets or data sources used to train, fine-tune, validate, test, ground, or operate the system, including dataset name, source, version, and purpose |
| Software dependencies | Major libraries, frameworks, packages, container images, and orchestration/runtime components with names and versions |
| External services and APIs | Third-party AI services, APIs, foundation model providers, plugins, or retrieval services the system depends on |
| Provenance | Where each major component came from, such as repository, registry, vendor, internal team, or service provider |
| Component relationships | How components connect, such as which dataset trained which model, which application calls which model, and which model depends on which service |
| Licensing and usage rights | Applicable licenses, contractual restrictions, and authorized usage conditions for models, data, and software |
| Integrity identifiers | Hashes, signatures, image digests, or other identifiers that help confirm the exact component version |
| Deployment context | Where the AI component runs or is hosted, such as cloud provider, service region, platform, or on-premises environment |

***Appendix E is provided as a notional, non-exhaustive example**

**Provide an element list of an AIBOM and its purpose under Appendix item**

# AIBOM: Proposed Options

**Option 1:**

**Remove mentions of AIBOM from Cyber AI Profile**

- Remains agnostic to provenance and lineage mechanism
- Cyber AI Profile can be more broadly adopted
- Focuses Cyber AI Profile on the outcomes of provenance and attestation mechanisms

NIST's preferred option

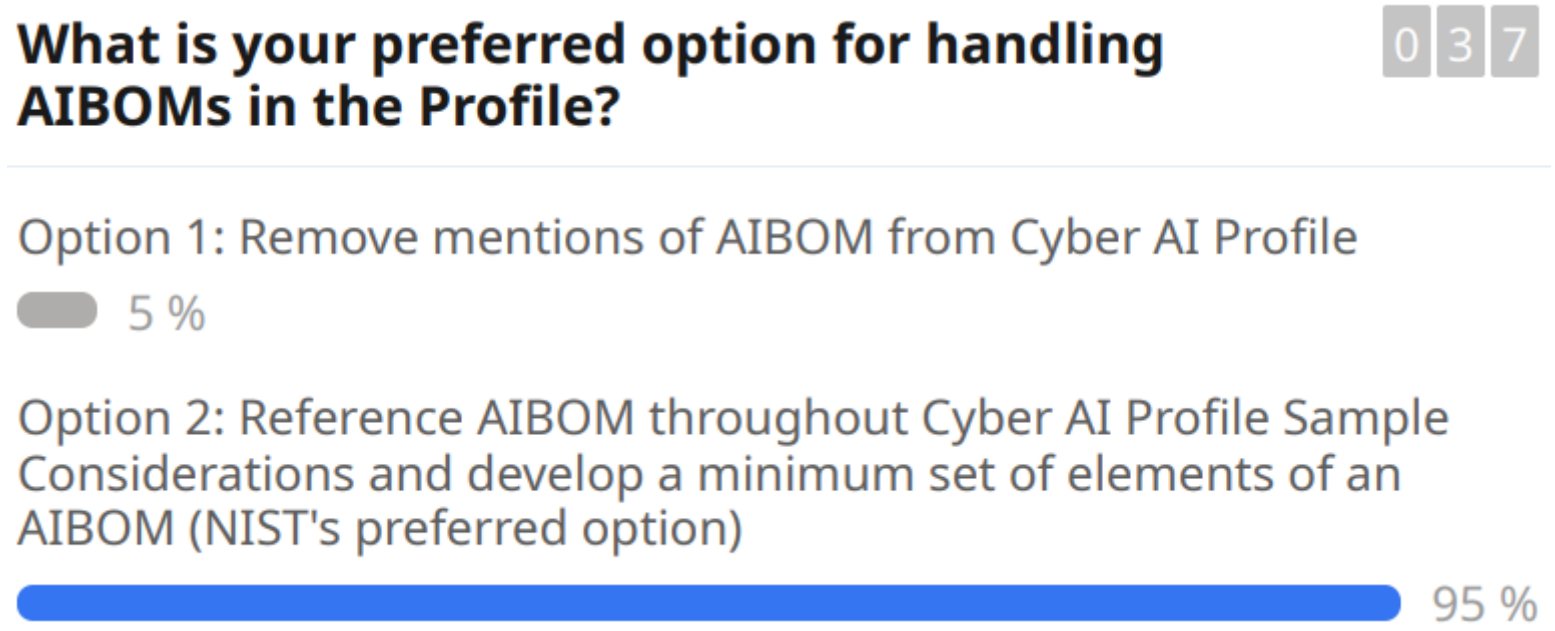
**Option 2:**

**Reference AIBOM throughout Cyber AI Profile Sample Considerations and develop a minimum set of elements of an AIBOM**

- Enhance transparency of AI asset provenance and attestation in context of existing mechanisms (SBOM, Model and Data Cards)
- Clear, interoperable, target while AIBOM-development matures
- Identify initial minimum set of AIBOM elements

**Slido.com**
**#CyberAI_Spring2026-3**

# AIBOM: Proposed Options



# AIBOM: Questions for Discussion

What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?

Slido.com
#CyberAI_Spring2026-3

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(1/10)

0 2 0

- Togaf
- Itsm
- Map frameworks it's or Itil, cobit, etc.. Governance, oversight, processes, roles, rasci, level, SD, etc..
- Operational and assurance elements beyond SBOMs, Model Cards, and Data Cards, such as runtime dependencies, agent/tool permissions, retrieval provenance, human oversight points, behavioral constraints, drift thresholds, assurance status, and operational risk tradeoffs including compute and cost impacts.
- Workbook
- Engineering level 1 document vendor proposed architectural components per sheet finally providing topographical conceptual view diagram etc..
- Cobit 5
- Architectural Integration

# AIBOM: Questions for Discussion

## What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?

0 2 0

(2/10)

Elements, Input Guardrails, System Prompts,

- Include last assessment or evaluation date ((to ensure that the AI component(s)) are still secure or not compromised
- agentic AI system needs to broadly included.
- AI tax
- AI-specific supply chain dependencies,
- Well articulated roles and responsibilities at each stage, including the data used and control of outcomes
- The minimum AIBOM should only include the connective tissue not already covered by SBOMs, model cards, or data cards: how the AI components are assembled, which model/data/prompt/RAG/tool/API dependencies influence behavior, where the system runs, who approved the deployment, how integrity is verified, and how changes are tracked over time.

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(3/10)

0 2 0

- At a minimum, I'd expect an AIBOM to include: -Model lineage and provenance — where the model originated, fine-tuning history, inherited dependencies, and upstream providers. -AI-specific supply chain dependencies — external APIs, foundation models, plugins, orchestration frameworks, vector databases, agents, and connected tools. -Intended use and operational boundaries — approved use cases, prohibited uses, risk tier/classification, and human oversight requirements. -Runtime behavior and autonomy levels — whether the AI can make decisions, execute actions, call external systems, or operate agentically. -Security and safety controls — guardrails, prompt injection protections, monitoring capabilities, abuse prevention, and fail-safe mechanisms. -Risk exposure indicators — known limitations, adversarial

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(4/10)

0 2 0

testing results, toxicity/bias concerns, hallucination risk, and model drift considerations. Data governance mapping sensitive data exposure potential, retention behavior, data residency, and downstream data sharing implications. -Accountability and ownership responsible business owner, model steward, security approver, and escalation contacts. -Lifecycle and change management retraining frequency, update cadence, version tracking, rollback capabilities, and decommissioning procedures.

- From my perspective the real value of an AIBOM is creating a centralized operational and governance view of AI risk that connects software, models, data, autonomy, and accountability into a single artifact rather than treating them separately.
- Source of training data

# AIBOM: Questions for Discussion

## What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?

0 2 0

(5/10)

- Information about APIs / MCP Model Context Protocol
- -Potential Side Effects- Unintended Outcomes
- model integrity (cryptographic verification), AI service dependencies, LLM-specific components, Execution environment
- What AI is being used, by whom, for what purpose, against what data, with what level of autonomy, through which vendors and connectors, under which controls, and what changes would require re-approval?
- At a minimum, I'd expect an AIBOM to include: -Model lineage and provenance — where the model originated, fine-tuning history,

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(6/10)

0 2 0

inherited dependencies, and upstream providers. -AI-specific supply chain dependencies — external APIs, foundation models, plugins, orchestration frameworks, vector databases, agents, and connected tools. -Intended use and operational boundaries — approved use cases, prohibited uses, risk tier/classification, and human oversight requirements. -Runtime behavior and autonomy levels — whether the AI can make decisions, execute actions, call external systems, or operate agentically. -Security and safety controls — guardrails, prompt injection protections, monitoring capabilities, abuse prevention, and fail-safe mechanisms. -Risk exposure indicators — known limitations, adversarial testing results, toxicity/bias concerns, hallucination risk, and model drift considerations.

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(7/10)

0 2 0

Data governance mapping sensitive data exposure potential, retention behavior, data residency, and downstream data sharing implications. -Accountability and ownership responsible business owner, model steward, security approver, and escalation contacts. - Lifecycle and change management retraining frequency, update cadence, version tracking, rollback capabilities, and decommissioning procedures.

- - Inference Environment Constraints (e.g., specific quantization levels) - Risk Mitigation Model or/and Metric
- Industry denotes the elements and attributes global touch points different laws different processes etc., touch point millions rtc
- AI SBOM (cyan track — NTIA / CISA / EO 14028 / SPDX / CycloneDX) Six domains: Component Identity → Dependencies

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(8/10)

0 2 0

→ Integrity & Provenance → Licensing → Vulnerability Linkage → AI-Specific Extensions (model artifacts, dataset packages, ONNX format, inference runtime) AI MBOM (green track — CISA / EU AI Act / NIST AI RMF / ISO 42001) Six domains: Model Identity → Training Data Provenance → Training & Fine-Tuning → Evaluation & Safety → Governance & Risk → Deployment & Lifecycle

- Vendor name, technology name, version number, repos where the technology resides, location where technology is deployed, intended use and any unique identifiers (YAML, fingerprint indictors, hashes etc.)
- Human oversight and auditing performed and tracked for accountability and cost savings ~ value for the customer and savings for the producer. I think this

# AIBOM: Questions for Discussion

**What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?**
(9/10)

0 2 0

topic will get bigger as AI takes over human effort, in the meantime - human auditing should be produced and accountability for gaps justified

- A minimum AIBOM should include AI operational and governance elements not captured by SBOMs, Model Cards, or Data Cards, such as model lineage and orchestration dependencies, agent/tool permissions, runtime behavioral constraints, drift and retraining triggers, assurance and validation status, human oversight points, safety boundary mappings, and provenance of external retrieval or decision influencing sources.
- Establishing clearly defined roles and responsibilities at every level might be worth taking into consideration. A role can change as the process evolves,

# AIBOM: Questions for Discussion

## What should be within a minimum set of AIBOM elements that is not already encompassed by SBOMs, Model and Data Cards?

0 2 0

(10/10)

and ensuring the process of the evolution of change management is transparent as well in order to create a paper trail for accountability.

- a. Legal basis for traiing data b. Bias and Fairness performance across demographic groups/geographic locations c.Harm incident history d. Intended use/phohibited use e. Human oversight requirements f. Redress and Accountability
- End-to-end lineage and operational context, including model–data–infrastructure dependency mapping, lifecycle traceability (training to deployment to operation), runtime telemetry/usage signals, control/governance context (access, roles, safeguards), and provenance validation metadata, which are not fully captured by SBOMs, model cards, or data cards alone

# Profile Delivery Formats

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Current Delivery Format

Each table summarizes the general and Focus Area-Specific considerations for one CSF Function.

General Considerations

Individual columns for each Focus Area that provide proposed Profile content

**Table 1 Cyber AI Profile – GOVERN.**

| CSF 2.0 Core: GOVERN | General Considerations | Focus Area Proposed Priorities & Considerations | | |
|---|---|---|---|---|
| | | Secure | Defend | Thwart |
| **GOVERN (GV)** | The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored | | | |
| **Organizational Context (GV.OC)** | The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood | | | |
| **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management | **General Considerations:** No general considerations identified - see Focus Area Considerations.<br><br>**Example Informative References:**<br>NIST SP 800-53, Rev 5: PM-11 | **Proposed Priority:** 3<br><br>**Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** OWASP General Governance; OWASP Supply Chain | **Proposed Priority: 3**<br><br>**Focus Area Considerations:** AI defense should support the organizational mission by accelerating detection and filtering noise, but humans should stay in the loop when Generative AI (GAI) tools are being used due to AI hallucination.<br><br>**Example Informative References:** ENISA Threat Landscape 62; DASF v4 Model Management; DASF v4 LLM hallucinations; MITRE ATLAS mitigations AML.M0020, AML.M0021; OWASP AI Exchange, p. 7, section "Summary - How to address AI Security?" https://arxiv.org/pdf/2311.05232; | **Proposed Priority:** 3<br><br>**Focus Area Considerations:** Standard cybersecurity practices apply.<br><br>**Example Informative References:** AI-specific Example Informative References pending additional inputs. |

Descriptions of CSF Functions, Categories and Subcategories (color-coded to match CSF 2.0)

Proposed priority (1, 2 or 3)

Considerations

Informative References (where available) – blanks represent potential gaps in available standards and guidelines

# Profile Delivery Formats: Summary of Feedback

**Feedback on Cyber AI Profile delivery formats included a desire for:**

- A machine-readable format (CSV, JSON, XML)
- Customizable ways of viewing the Profile via sorting and filtering
- Easy mapping to Online Informative References Program and CPRT
- A format ingestible by LLMs

# Proposed Priorities: Potential Options

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST's preferred option

## Option 1

**No Change**

Retain the same table format as the Preliminary Draft PDF – all Profile elements (considerations, opportunities Informative References, etc.)

## Option 2

**Separate Worksheets for Focus Areas**

General Considerations and each Focus Area is provided in a separate worksheet in the same workbook

Each Profile element has its own column in each worksheet

## Option 3

**Expanded Profile Elements by Column**

All Profile elements are in one worksheet

Each Profile element for General Considerations and Focus Areas has its own column

## Option 4

**Hybrid of Options 2 & 3**

General Considerations and each Focus Area is in its own worksheet

Each Profile element (e.g., considerations, Informative References) has its own column

Additional sheet provides consolidated view of all Profile elements

## Option 5

**Expanded Profile Elements by Row**

All Profile elements are in one worksheet

Each Profile element for General Considerations and Focus Areas has its own row

# Profile Delivery Format: Option 1

Each table summarizes the general and Focus Area-Specific considerations for one CSF Function.

General Considerations

Individual columns for each Focus Area that provide proposed Profile content

Table 1 Cyber AI Profile – GOVERN.

| CSF 2.0 Core: GOVERN | General Considerations | Focus Area Proposed Priorities & Considerations | | |
|---|---|---|---|---|
| | | Secure | Defend | Thwart |
| **GOVERN (GV)** | The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored | | | |
| **Organizational Context (GV.OC)** | The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood | | | |
| **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management | **General Considerations:** No general considerations identified - see Focus Area Considerations.<br>**Example Informative References:** NIST SP 800-53, Rev 5: PM-11 | **Proposed Priority:** 3<br>**Focus Area Considerations:** Standard cybersecurity practices apply.<br>**Example Informative References:** OWASP General Governance; OWASP Supply Chain | **Proposed Priority: 3**<br>**Focus Area Considerations:** AI defense should support the organizational mission by accelerating detection and filtering noise, but humans should stay in the loop when Generative AI (GAI) tools are being used due to AI hallucination.<br>**Example Informative References:** ENISA Threat Landscape 62; DASF v4 Model Management; DASF v4 LLM hallucinations; MITRE ATLAS mitigations AML.M0020, AML.M0021; OWASP AI Exchange, p. 7, section "Summary - How to address AI Security?" https://arxiv.org/pdf/2311.05232; | **Proposed Priority:** 3<br>**Focus Area Considerations:** Standard cybersecurity practices apply.<br>**Example Informative References:** AI-specific Example Informative References pending additional inputs. |

Descriptions of CSF Functions, Categories and Subcategories (color-coded to match CSF 2.0)

Proposed priority (1, 2 or 3)

Considerations

Informative References (where available) – blanks represent potential gaps in available standards and guidelines

| Characteristics | Machine/ LLM) Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Same format as the Preliminary Draft PDF<br>• Everything in one sheet<br>• All information for one Focus Area / Subcategory combination in one cell | ✓ | ✗ | ✓ | ✗ | ✓ |

# Profile Delivery Format: Option 2 (1 of 2)

**Separate Worksheets for Focus Areas**

| | A | B | C | D |
|---|---|---|---|---|
| 1 | CSF 2.0 Subcategory | Secure Priority | Secure Considerations | Secure Informative References |
| 2 | **GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management | 3 | Standard cybersecurity practices apply. | OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain |
| 3 | : Internal and external ers are understood, and ds and expectations cybersecurity risk management are understood and considered | 3 | Standard cybersecurity practices apply. | DASF 13, 40, 51, 53; OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain; ENISA Threat Landscape 2025 |
| 4 | **GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are unde tood and managed | 3 | The legal framework regarding AI usage is evolving, particularly in areas like cybersecurity, privacy, fair use of copyrighted material, and AI training. | DASF 32, 40; OWASP AI Exchange: Controls to Limit the Effects of Unwanted Behavior; OWASP Conventional runtime controls; OWASP AI Exchange: General Governance Controls; OWASP AI Exchange: Model Access Control; OWASP |

General | Secure | Defend | Thwart | +

| Characteristics | Machine/ LLM Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Splits the Focus Areas into different sheets<br>• Splits Profile elements across columns<br>• Enables filtering and sorting | ✓ | ✓ | ✗ | ✓ | ✗ |

# Profile Delivery Format: Option 2 (2 of 2)

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | CSF 2.0 Subcategory | Defend Priority | Defend Opportunities | Defend Considerations | Defend Informative References |
| 2 | **GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity—including | 1 | AI capabilities can support compliance with legal, regulatory, and contractual requirements by analyzing and summarizing requirements, accelerating policy development, speeding up review processes, identifying and mapping similar concepts between documents, and even | Defensive AI tools handle logs and sensitive data in line with privacy obligations including consent, usage and aggregation controls and new AI specific laws.<br><br>AI audits are designed to demonstrate | DASF 44,50; ENISA Threat Landscape 2025 ; ATLAS AML.M0005 |
| 3 | | 2 | Standard cybersecurity practices apply. | Understanding the strengths and limitations of AI capabilities for cyber defense is important for meeting stakeholder expectations and to ensure the balance between the required human oversight and automation. | DASF 38,50;OWASP AI Exchange: AI Transparency; ENISA Threat Landscape 2025; ATLAS AML.M0003 |
| 4 | | 3 | Standard cybersecurity practices apply. | Standard cybersecurity practices apply. | ENISA Threat Landscape 2025; DASF 50; ATLAS AML.M0020; OWASP AI Exchange: AI Security Overview; https://arxiv.org/pdf/2311.05232; NIST AI 100-2e2025 |
| 5 | | | | | |

**Ability to sort by Profile elements – example shows Defend Focus Area sorted by priority level**

| Characteristics | Machine/ LLM Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Splits the Focus Areas into different sheets<br>• Splits Profile elements across columns<br>• Enables filtering and sorting | ✓ | ✓ | ✗ | ✓ | ✗ |

# Profile Delivery Format: Option 3

**Each Profile element for General Considerations and Focus Areas has its own column**

**General Considerations** (Considerations, Informative References)

**Secure** (Priority, Considerations, Informative References)

**Defend** (Priority, Opportunities, Considerations, Informative References)

**Thwart** (Priority, Considerations, Informative References)

| CSF 2.0 Subcategory | General Considerations | General Informative References | Secure Priority | Secure Considerations | Secure Informative References | Defend Priority | Defend Opportunities | Defend Considerations | Defend Informative References | Thwart Priority | Thwart Considerations | Thwart Informative References |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management | No general considerations identified—see Focus Area Considerations. | NIST SP 800-53, Rev 5: PM-11 | 3 | Standard cybersecurity practices apply. | OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain | 3 | Standard cybersecurity practices apply. | Standard cybersecurity practices apply. | ENISA Threat Landscape 2025; DASF 50; ATLAS AML.M0020; OWASP AI Exchange: AI Security Overview; https://arxiv.org/pdf/2311.05232; NIST AI 100-2e2025 | 3 | Standard cybersecurity practices apply. | AI-specific Example Informative References pending additional inputs. |
| **GV.OC-02**: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered | AI use introduces considerations from multiple aspects of organizational operations, including legal, technical, procurement/acquisitions, and governance teams. Collaboration across these areas is essential for addressing AI-related cybersecurity risks. Multidisciplinary approaches facilitate a comprehensive enterprise view. | NIST SP 800-53, Rev 5: PM-09; PM-18; PM-30; SR-03; SR-05; SR-06; SR-08; Reflections from the First Cyber AI Profile Workshop | 3 | Standard cybersecurity practices apply. | DASF 13, 40, 51, 53; OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain; ENISA Threat Landscape 2025 | 2 | Standard cybersecurity practices apply. | Understanding the strengths and limitations of AI capabilities for cyber defense is important for meeting stakeholder expectations and to ensure the balance between the required human oversight and automation. | DASF 38,50;OWASP AI Exchange: AI Transparency; ENISA Threat Landscape 2025; ATLAS AML.M0003 | 2 | Standard cybersecurity practices apply. | AI-specific Example Informative References pending additional inputs. |

| Characteristics | Machine/ LLM Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Keeps everything in one sheet<br>• Splits Focus Area elements across columns | ✓ | ✓ | ✓ | ✗ | ✓ |

# Profile Delivery Format: Option 4

**Each Profile element for General Considerations and Focus Areas has its own column**

**NIST's preferred option**

**Separate Worksheets for General Considerations and Focus Areas + Consolidated View**

General Considerations

Secure

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | CSF 2.0 Subcategory | General Considerations | General Informative References | Secure Priority | Secure Considerations | Secure Informative References |
| 2 | **GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management | No general considerations identified—see Focus Area Considerations. | NIST SP 800-53, Rev 5: PM-11 | 3 | Standard cybersecurity practices apply. | OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain |
| 3 | **GV.OC-02**: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered | AI use introduces considerations from multiple aspects of organizational operations, including legal, technical, procurement/acquisitions, and governance teams. Collaboration across these areas is essential for addressing AI-related cybersecurity risks. Multidisciplinary approaches facilitate a comprehensive enterprise view. | NIST SP 800-53, Rev 5: PM-09; PM-18; PM-30; SR-03; SR-05; SR-06; SR-08; Reflections from the First Cyber AI Profile Workshop | 3 | Standard cybersecurity practices apply. | DASF 13, 40, 51, 53; OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain; ENISA Threat Landscape 2025 |
| | **GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity—including | The AI legal, regulatory, and standards landscape is rapidly evolving and will impact the decisions organizations make regarding whether, when, and | NIST SP 800-53, Rev 5: AC-01; AT-01; AU-01; CA-01; CM-01; CP-01; IA-01; IR-01; MA-01; MP-01; PE-01; PL-01; PM-01; PS-01; PT-01; RA-01; SA-01; SC-01; SI-01; SR-01; PM-28; PT | 3 | The legal framework regarding AI usage is evolving, particularly in areas like cybersecurity, privacy, fair use of copyrighted material, and AI | DASF 32, 40; OWASP AI Exchange: Controls to Limit the Effects of Unwanted Behavior; OWASP Conventional runtime controls; OWASP AI Exchange: General Governance Controls; OWASP |

Consolidated | General | Secure | Defend | Thwart | +

| Characteristics | Machine/ LLM Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Splits the Focus Areas into different sheets<br>• Splits Profile elements across columns<br>• Enables filtering and sorting<br>• Consolidated sheet pulls from individual sheets to provide everything in one sheet | ✓ | ✓ | ✓ | ✓ | ✓ |

# Profile Delivery Format: Option 5

**Each Profile element for General Considerations and Focus Areas has its own row. This example shows two Subcategories.**

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | CSF 2.0 Subcategory | General | Secure | Defend | Thwart |
| 2 | **(Priority) GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management | None | 3 | 3 | 3 |
| 3 | **(Opportunities & Considerations) GV.OC-01** | No general considerations identified—see Focus Area Considerations. | Standard cybersecurity practices apply. | **Opportunities**: Standard cybersecurity practices apply.<br><br>**Focus Area Considerations**: Standard cybersecurity practices apply. | Standard cybersecurity practices apply. |
| 4 | **(Informative References) GV.OC-01** | NIST SP 800-53, Rev 5: PM-11 | OWASP AI Exchange: General Governance Controls; OWASP LLM Top Ten: LLM03 Supply Chain | ENISA Threat Landscape 2025; DASF 50; ATLAS AML.M0020; OWASP AI Exchange: AI Security Overview; https://arxiv.org/pdf/2311.05232; NIST AI 100-2e2025 | AI-specific Example Informative References pending additional inputs. |
| 5 | **(Priority) GV.OC-02**: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered | None | 3 | 2 | 2 |
| 6 | **(Opportunities & Considerations) GV.OC-02** | AI use introduces considerations from multiple aspects of organizational operations, including legal, technical, procurement/acquisitions, and governance teams. Collaboration across these areas is essential for addressing AI-related cybersecurity risks. Multidisciplinary | Standard cybersecurity practices apply. | **Opportunities**: Standard cybersecurity practices apply.<br><br>**Considerations**: Understanding the strengths and limitations of AI capabilities for cyber defense is important for meeting stakeholder expectations and to ensure | Standard cybersecurity practices apply. |

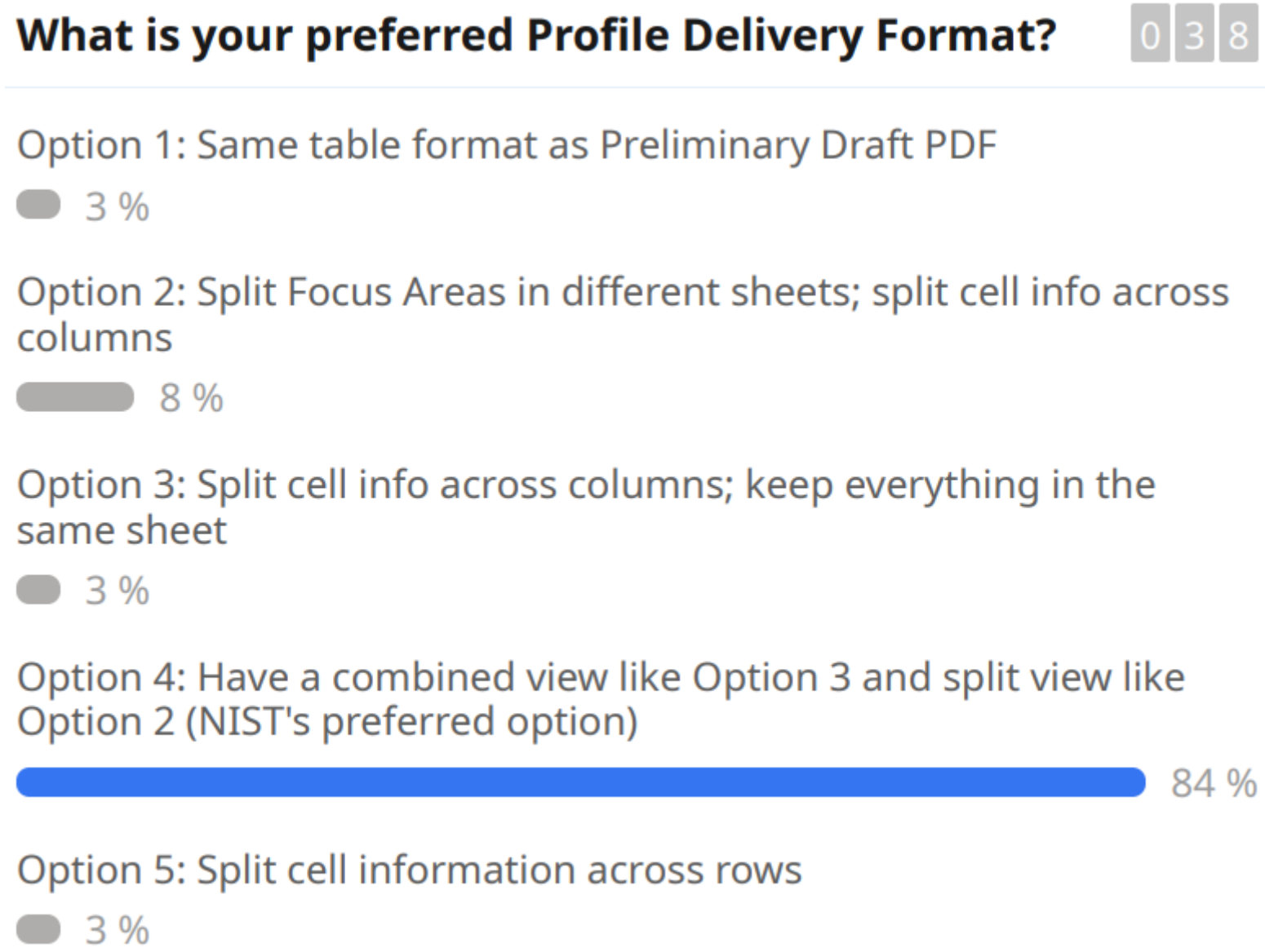
| Characteristics | Machine/ LLM Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything in one tab |
|---|---|---|---|---|---|
| • Keeps everything in one sheet<br>• Splits information across rows | ✓ | ✗ | ✓ | ✗ | ✓ |

# Profile Delivery Format Overview

| Option and Description | Machine (and LLM) Readable | Sort and Filter | Focus Areas Side by Side | Focus Areas Separate | Everything visible in one tab |
|---|---|---|---|---|---|
| Option 1 (same table format as Preliminary Draft PDF) | ✓ | ✗ | ✓ | ✗ | ✓ |
| Option 2 (split Focus Areas in different sheets; split cell info across columns) | ✓ | ✓ | ✗ | ✓ | ✗ |
| Option 3 (split cell info across columns; keep everything in the same sheet) | ✓ | ✓ | ✓ | ✗ | ✓ |
| Option 4 (have a combined view like option 3 and split view like option 2) **NIST's preferred option** | ✓ | ✓ | ✓ | ✓ | ✓ |
| Option 5 (split cell info across rows) | ✓ | ✗ | ✓ | ✗ | ✓ |

Slido.com
#CyberAI_Spring2026-3

# Profile Delivery Format Overview



# Profile Delivery Format: Questions for Open Discussion

- What else would you want to see in a Profile delivery format? Any additional functionalities?
- Is there another format which would work better? Other Excel Workbook formats could be emailed for reference.

Slido.com
#CyberAI_Spring2026-3

# Profile Delivery Format: Questions for Open Discussion

Profile Delivery Format: Questions for Open Discussion (1/2)

0 0 8

## What else would you want to see in a Profile delivery format? Any additional functionalities? (1/3)

- Version tracking and delta filtering at the tow and cell level will be very useful over time
- I'd want Profiles to go a bit further than just structure and formatting. Beyond the layout options, I'd look for: -Version control and change tracking so we can see how risk and controls evolve over time. -Clear risk prioritization so teams know what actually matters first -Role-based views (execs vs engineers vs auditors don't need the same lens) - APIs or integration hooks so it plugs into GRC tools, inventories, and monitoring systems -Built-in traceability back to frameworks. - Support for evidence and artifacts making it's audit-ready, not just descriptive
- Support both combined and split views, advanced

# Profile Delivery Format: Questions for Open Discussion





## What else would you want to see in a Profile delivery format? Any additional functionalities? (2/3)

filtering, machine readable export formats, cross profile mapping, version tracking, and operational metadata for automation and assurance use cases.

- Sap Signavio, etc, Lean IX and cx systems map end to end with process, people with filters, Ai joule, GRC controlled centrally, theirs party agentic is still grey...
- Historical reference information access would be useful, as in, being able to reference what the previous information was and have a link directly to it.
- Can we ensure that the workbook delivery format will maintain the property of every data element being labelled? That property is essential for converting the output into JSON, YAML, etc. As new properties are added in the future, it may not be easy to add them to the workbooks so that they are distinctly (row, column) labelled.

# Profile Delivery Format: Questions for Open Discussion

Profile Delivery Format: Questions for Open Discussion (1/2)

0 0 8

## What else would you want to see in a Profile delivery format? Any additional functionalities? (3/3)

- 1. role based filtered view as a default entry point 2. Harm-impact indicator 3. Regulatory mapping filter 4. Gap tracking functionality 5. Hyperlinked informative references 6. Version comparison view
- Option 4 works if it is clean structured data: stable IDs, consistent columns, version metadata, no merged cells, and reliable export to CSV/JSON/Markdown for GRC, RAG, and control mapping.

# Profile Delivery Format: Questions for Open Discussion



## Is there another format which would work better? Other Excel Workbook formats could be emailed for reference.

(1/2)

- Third-Party Risk (TPRM) Flags: A specific toggle for "Inherited Controls" versus "Customer-Managed Controls," which is vital for supply chain security and AI-SBOM discussions.
- Simplicity should be the guide word. The more approachable and universal the format, the wider the adoption.
- Excel is still useful for distribution and familiarity, but the better direction is treating it as just one view of a structured Profile not the actual architecture. Probably the real evolution is toward a “hybrid” and API-first, machine-readable profiles with multiple views layered on top.
- A hybrid workbook with both human readable and machine consumable formats would

# Profile Delivery Format: Questions for Open Discussion

Profile Delivery Format: Questions for Open Discussion (2/2)

0 0 6

**Is there another format which would work better? Other Excel Workbook formats could be emailed for reference.**
(2/2)

work best, especially if aligned for governance, assurance, and automation workflows.

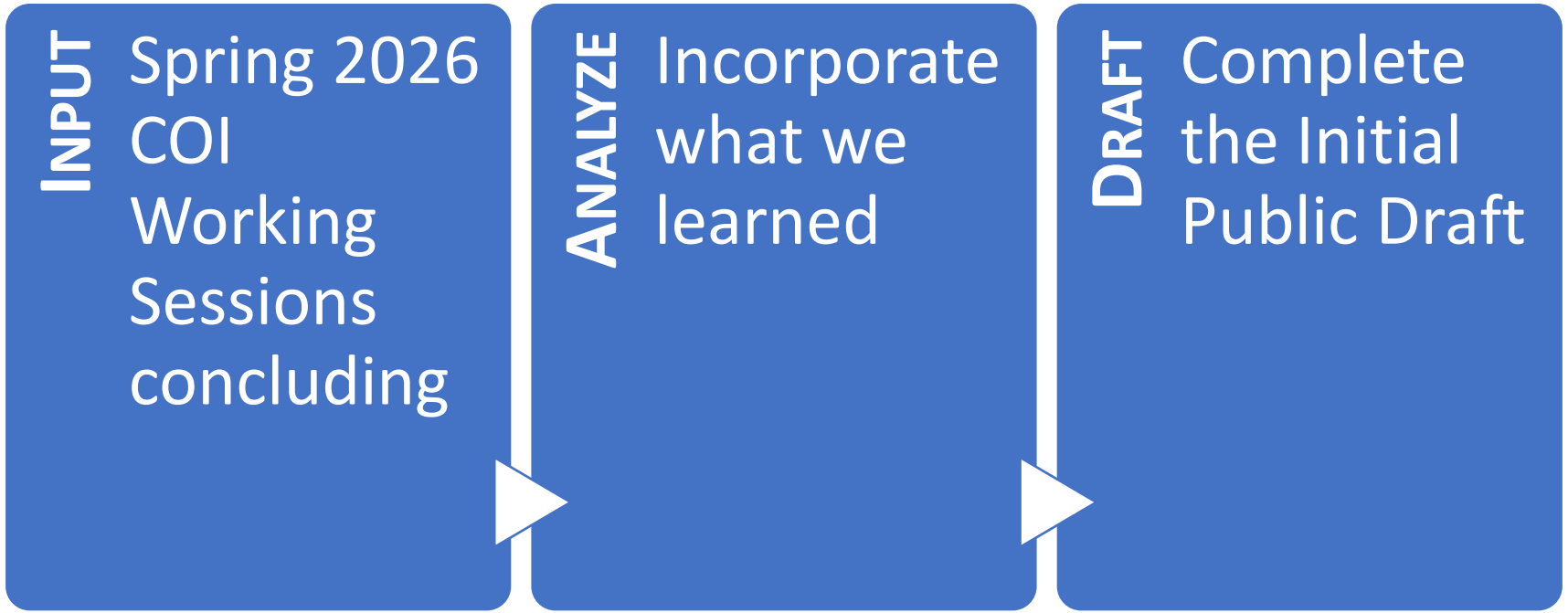
- Works. Unless to slow, need teams and Ai and Ml to speed up transformation and standards.
- a. JSON schema publication alongside the Excel workbook b. An interactive web-based interface, longer term c. A plain-language summary layer

# Open Discussion

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Close-out

# Working Sessions Next Steps




**If we missed your input today, please feel free to email us: CyberAIProfile@nist.gov! Please send your inputs by May 15, 2026.**

# Working Session Schedule

**April 28, 2026**

***Profile Elements***

**May 5, 2026**

***Extensions of Technical Content***

**May 12, 2026**

***Roles and Profile Delivery Formats***

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# We Appreciate Your Input

## THANK YOU

Your input is a critical part of this process!  Thank you for contributing to the development of the Cyber AI Profile!

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://www.nccoe.nist.gov/projects/cyber-ai-profile

CyberAIProfile@nist.gov

nccoe.nist.gov

@NISTcyber

# NIST AI and Cybersecurity Projects

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

| Topic | Learn More! |
|---|---|
| **AI Risk Management Framework (AI RMF)**<br>A framework to better manage risks to individuals, organizations, and society associated with artificial intelligence | |
| **Center for AI Standards and Innovation (CAISI)**<br>Facilitates testing and collaborative research related to harnessing and securing the potential of commercial AI systems | |
| **Adversarial Machine Learning**<br>Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (NIST AI 100-2 E2025) | |
| **Dioptra**<br>A software test platform for assessing the trustworthy characteristics of artificial intelligence systems | |
| **Secure Software Development Framework (SSDF) AI Profile**<br>Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile | |

| Topic | Learn More! |
|---|---|
| **PETs Test Bed**<br>Evaluating Differential Privacy Guarantees | |
| **DevSecOps**<br>Secure Software Development, Security, and Operations (DevSecOps) Practices | |
| **Agent Identities**<br>Digital Identity Guidelines, Revision 4 (NIST SP 800-63) | |
| **NCCoE Chatbot**<br>Secure, internal-use chatbot to assist with discovering and summarizing cybersecurity guidelines | |
| **COSAiS**<br>NIST SP 800-53 Control Overlays for Securing AI Systems (COSAiS) | |