

# Manufacturing Supply Chain Traceability – Traceability Chain MVP Introductory Webinar

National Cybersecurity Center of Excellence

Wednesday, June 7<sup>th</sup>, 2023



*This meeting is being recorded*

# DISCLAIMERS

- **Presentation:**

- Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

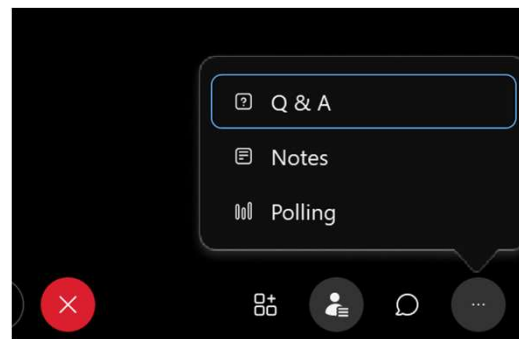
- **Recording:**

- *Recording Note: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcast or otherwise made publicly available by NIST. By registering for — or attending — this event, you acknowledge and consent to being recorded.*

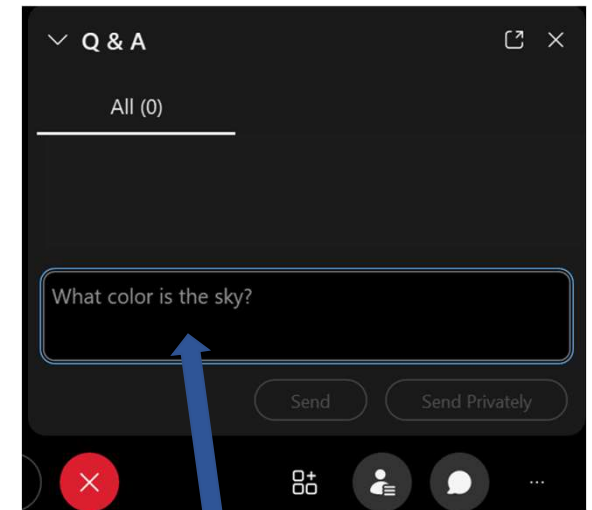
# AUDIENCE ENGAGEMENT

Please use the Q&A window to enter your questions.

We will do our best to answer all questions during the Q&A and will post responses to those we didn't have time to cover



1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.



2. Type your question in the text box and click Send

# INTRODUCTION

- Michael Pease, [michael.pease@nist.gov](mailto:michael.pease@nist.gov)
  - National Institute of Standards and Technology Smart Connected System Division
- Steve Granata, [sgranata@mitre.org](mailto:sgranata@mitre.org)
  - The MITRE Corporation
- Harvey Reed, [hreed@mitre.org](mailto:hreed@mitre.org)
  - The MITRE Corporation

# WHO WE ARE

A solution-driven, collaborative hub addressing complex cybersecurity problems



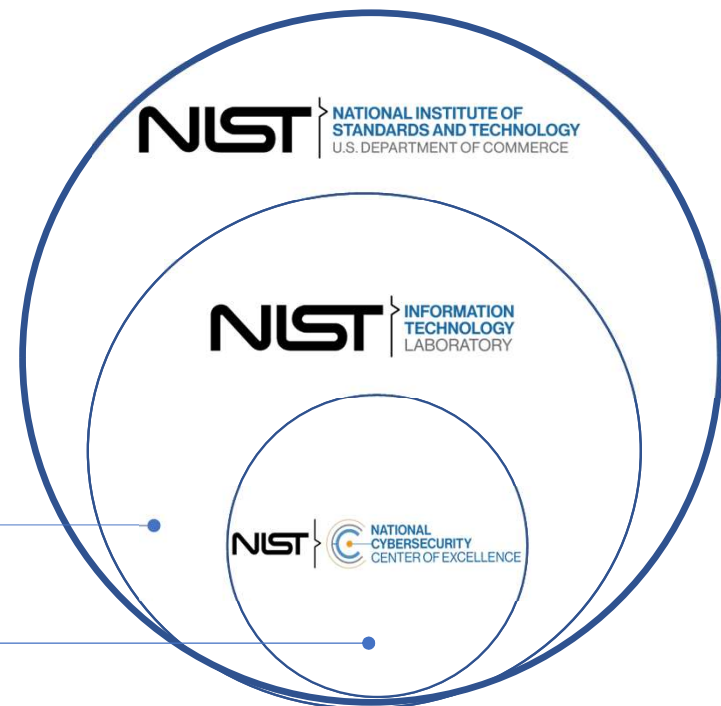
# Who We Are

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

NIST is a **non-regulatory** agency. Our guidance is **voluntary**.

Information Technology Laboratory

Applied Cybersecurity Division





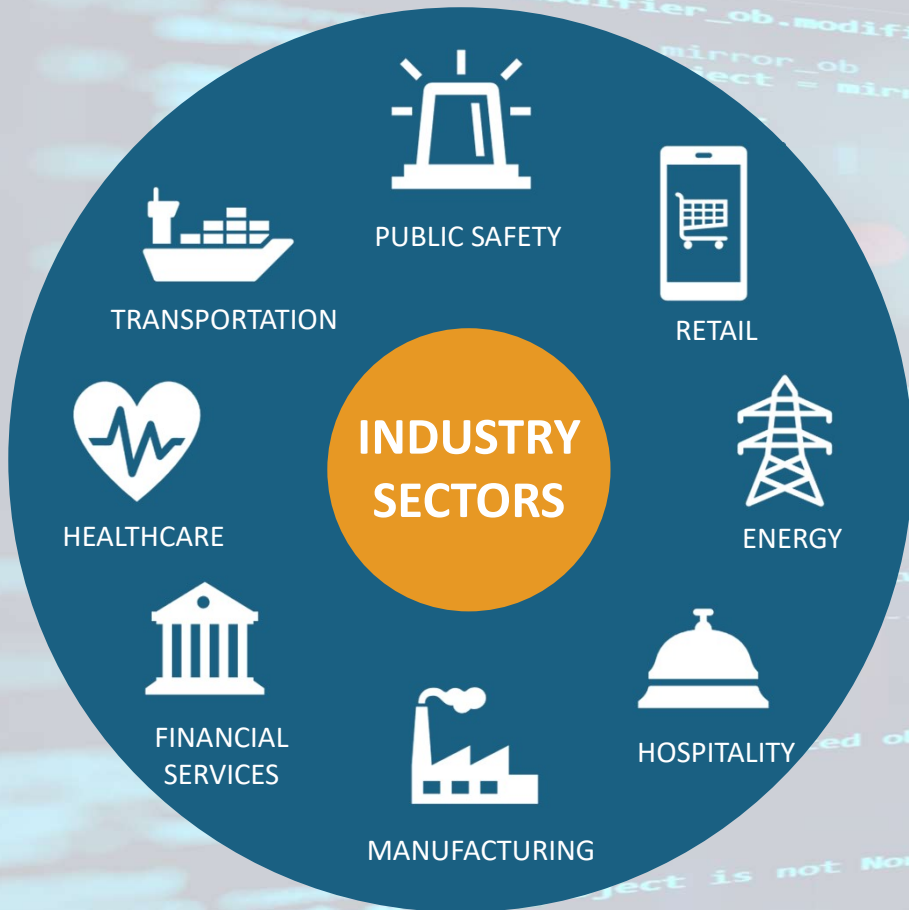


# What We Do

We collaborate to develop modular, repeatable applied cybersecurity architectures using:

- ➔ Existing Standards
- ➔ Existing guidance
- ➔ Commercially available technologies

# Guidance Created With Industry, For Industry



SECURITY GUIDANCE    OUR APPROACH    NEWS & INSIGHTS    GET INVOLVED

**By Technology**

- 5G Cybersecurity
- Applied Cryptography
- Artificial Intelligence
- Critical Cybersecurity Hygiene
- Data Classification
- Data Security
- DevSecOps
- Hybrid Satellite Networks
- Internet of Things (IoT)
- IPv6
- Mobile Device Security
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

**By Sector**

- Consumer Data Protection
- Energy
- Financial Services
- Healthcare
- Manufacturing
- Public Safety/First Responder
- Water/Wastewater

**By Status**

- Defining Scope
- Seeking Collaborators
- Preparing Draft
- Soliciting Comments
- Reviewing Comments
- Finalized Guidance
- Archived



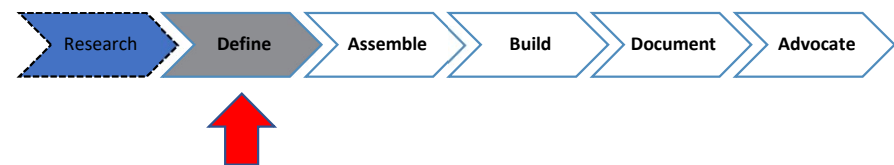
# Current Project

Draft Project Description

Comments being reviewed and adjudicated, Jun 2023

The screenshot shows a webpage from the National Cybersecurity Center of Excellence (NCCoE) at NIST. The page title is "Manufacturing Supply Chain Traceability Using Blockchain Related Technologies". The header includes the NIST logo and navigation links: "SECURITY GUIDANCE", "OUR APPROACH", "NEWS & INSIGHTS", "GET INVOLVED", and a "SEARCH" button. The main content area features a large, stylized graphic of a glowing orange cube on a dark blue background with glowing lines. Below the graphic, there is a paragraph of text: "Presently, end operating environments within critical infrastructure sectors have limited ability to obtain trusted pedigree and provenance information for the components supporting their operational environments. Insufficient traceability information for critical components reduces effectiveness of risk-based evaluations of security, safety, sustainability, and other compliance needs within end operating environments, including reduced ability to detect vectors of adversarial attack."

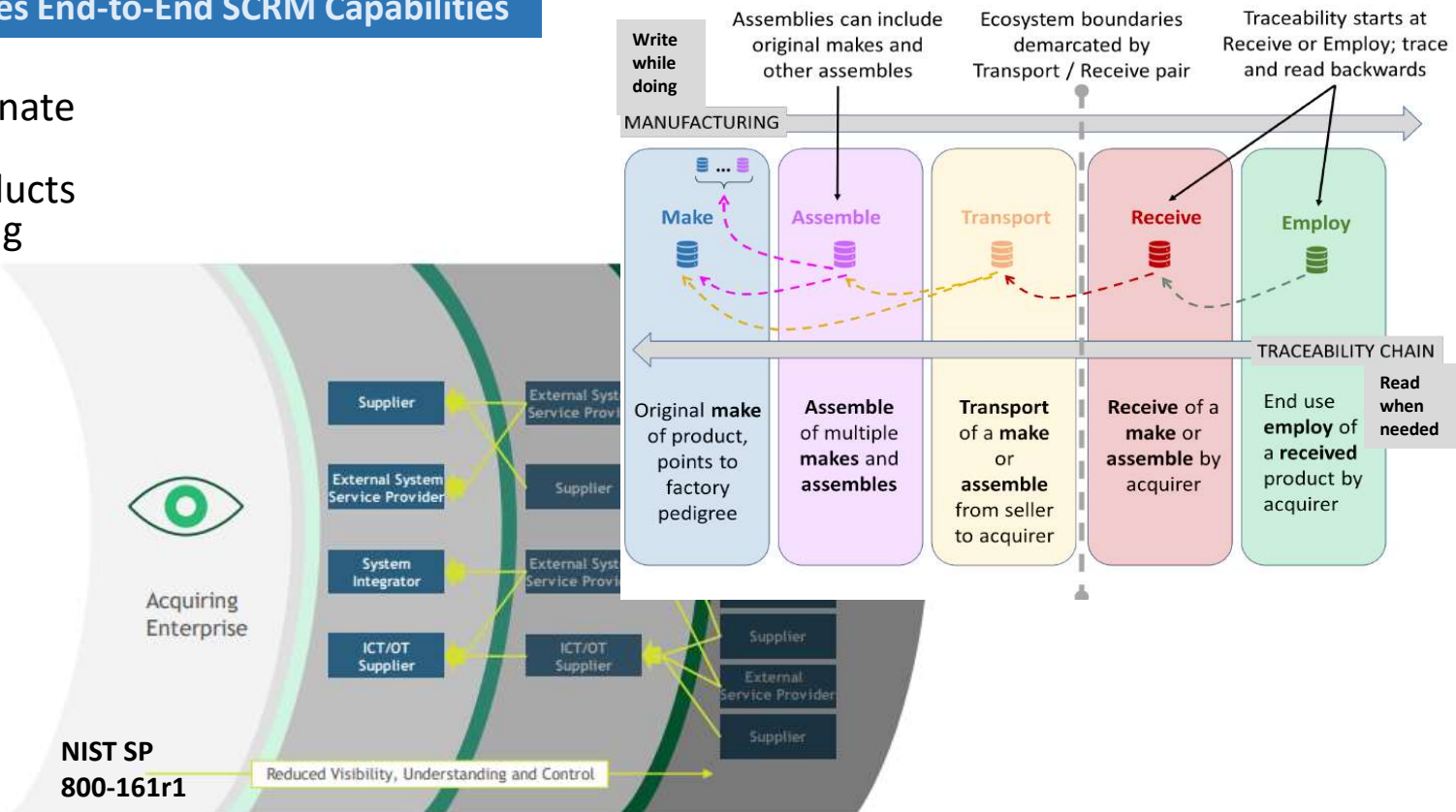
[Manufacturing Supply Chain Traceability Using Blockchain-Related Technologies | NCCoE \(nist.gov\)](https://www.nist.gov/nccoe/manufacturing-supply-chain-traceability-using-blockchain-related-technologies)



# TRACEABILITY SHIFT IN PERSPECTIVE

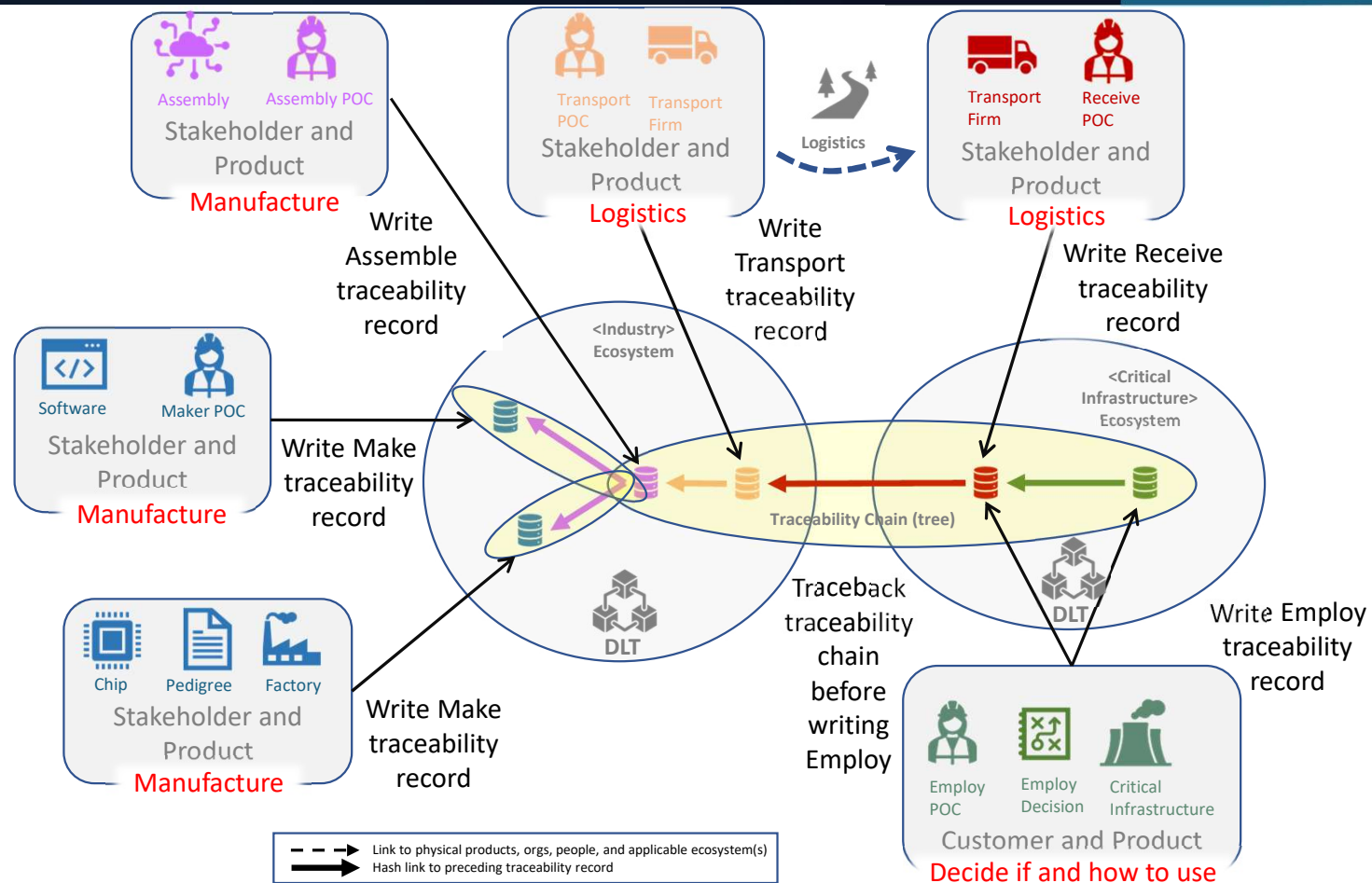
## Traceability Fundamentally Enables End-to-End SCRM Capabilities

- **Traceability records** illuminate the physical and/or digital flow of materials and products in a supply chain, informing product **provenance**.
- **Pedigree** supporting information captured in traceability records and reflects product quality in terms of:
  - Original producer authenticity
  - Adherence to specifications and standards



# TRACEABILITY CHAIN RECORDING SUPPLY CHAIN TRANSACTIONS

- **Actors** create the traceability chain one transaction at a time
- **Ecosystems** are consortiums based on common interests e.g.: DLT implementation, traceability data types, and industry sector or sub-sector(s) standards
- **DLT** are permission based and enables confidentiality and integrity, and permanence of records beyond the lifecycle of a company.



# TRACEABILITY RECORD DATA FIELDS

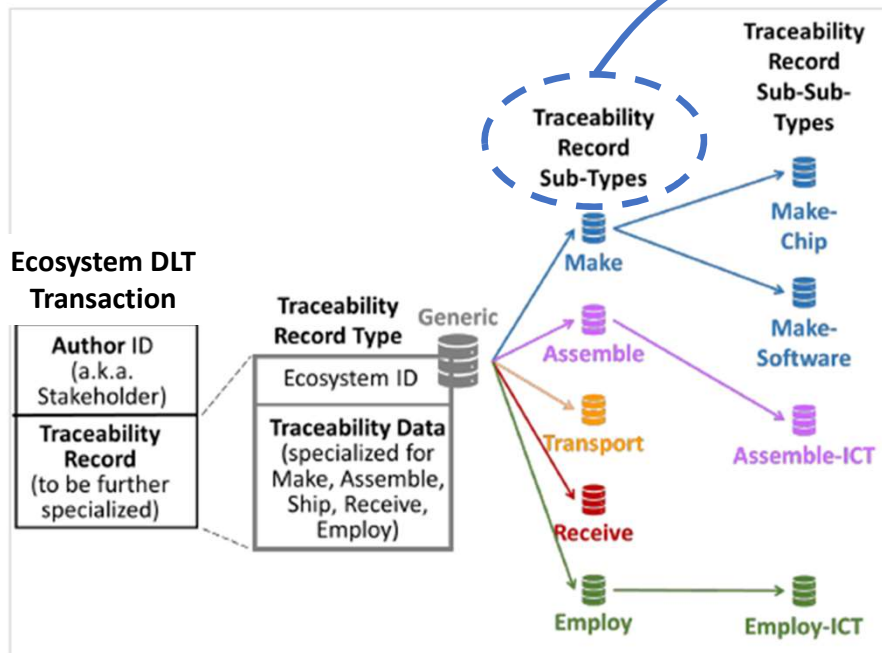


Figure 13: Traceability Data Types

463

Table 1: Traceability Record Sub-type Data Fields

Traceability Record Types	Data Fields	Notes
Top level (generic)	<ul style="list-style-type: none"> <li>Blockchain user address</li> <li>Traceability Record (see below sub-types)</li> </ul>	The blockchain user address is a public key, derived from the user private key; the user is the relevant stakeholder and an individual (not organization). Decentralized identity standards orgs are working the complex issues regarding organizational identity.
Make Sub-type	<ul style="list-style-type: none"> <li>Ecosystem ID (origination)</li> <li>Factory ID (organization)</li> <li>Product ID</li> <li>Maker POC</li> <li>Pedigree Statement</li> </ul>	Factory is in (origination) ecosystem
Assemble Sub-type	<ul style="list-style-type: none"> <li>Ecosystem ID (origination)</li> <li>Assembly ID</li> <li>Assemble POC</li> <li>For each product included in the assembly                             <ul style="list-style-type: none"> <li>Hash-link to Make traceability record</li> <li>Product ID in Make traceability record</li> </ul> </li> </ul>	Assemble can refer to assemble / make records in the same ecosystem, and/or receive records from prior ecosystems Assemble traceability records are the branching nodes in the traceability chain/tree
Transport Sub-type	<ul style="list-style-type: none"> <li>Ecosystem ID (origination)</li> <li>Factory ID (origination)</li> <li>Transport POC</li> <li>Transport Firm</li> <li>Ecosystem ID (destination)</li> <li>Consuming ID (destination organization)</li> <li>Hash-link to Assemble or Make traceability record</li> <li>Product ID (assemble or simple make)</li> </ul>	Transport record is in origination ecosystem
Receive	<ul style="list-style-type: none"> <li>Ecosystem ID (origination)</li> <li>Ecosystem ID (destination)</li> <li>Transport Firm</li> <li>Receive POC</li> <li>Hash link to transport record</li> <li>Product ID (assemble or simple make)</li> <li>Consuming ID (destination organization)</li> </ul>	Receive record is in destination ecosystem
Employ	<ul style="list-style-type: none"> <li>Ecosystem ID (final use in critical infrastructure, or equivalent)</li> <li>Critical Infrastructure (or equivalent) ID</li> <li>Employ POC</li> <li>Hash link to receive record</li> <li>Product ID (assemble or simple make)</li> <li>Link to employ decision</li> </ul>	The employ decision is the document which summarizes the decision to use the product, and where in the critical infrastructure (or equivalent) the product is used.

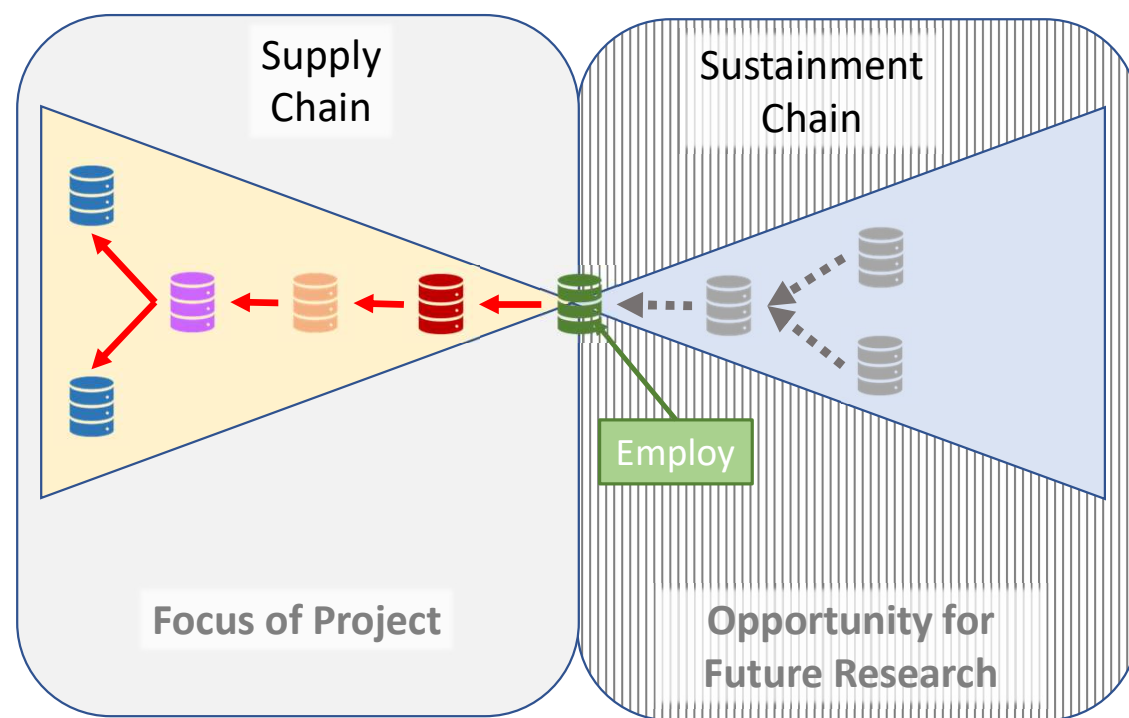
453



# TRACEABILITY CHAIN PROJECT IS A STARTING POINT

Traceability Fundamentally Enables End-to-End SCRM Capabilities

- Focus on end user tracing back through the supply chain
- Traceability Chain project is a starting point for supporting future research, e.g.:
  1. Sustainment chain integration
  2. Specialized traceability transaction types
  3. Evaluate how traceability chain enables supply chain decision support



# HIGH LEVEL ARCHITECTURE

- Loosely-coupled ecosystems
  - Independent DLTs
  - Secure API (write and query)
- Single identity and access management for MVP
- Dashboard
  - Monitoring MVP
  - Data Collection
  - Scenario Execution

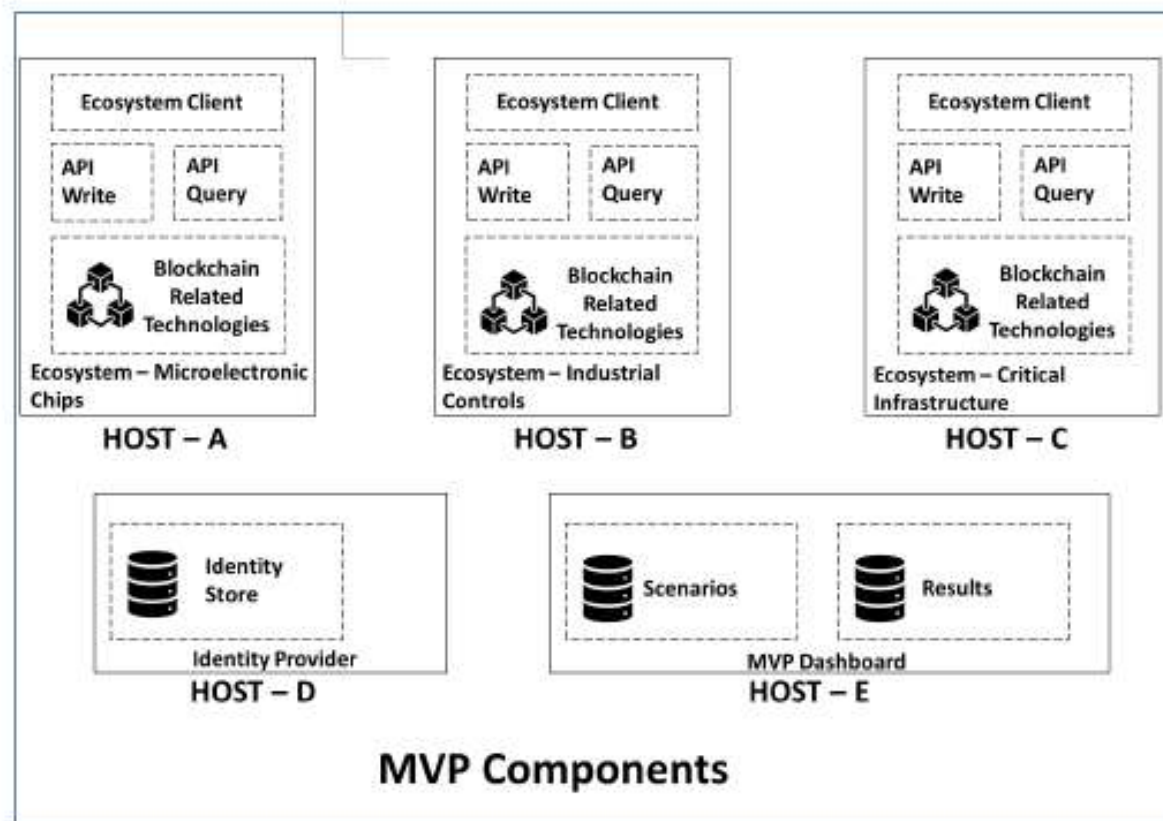


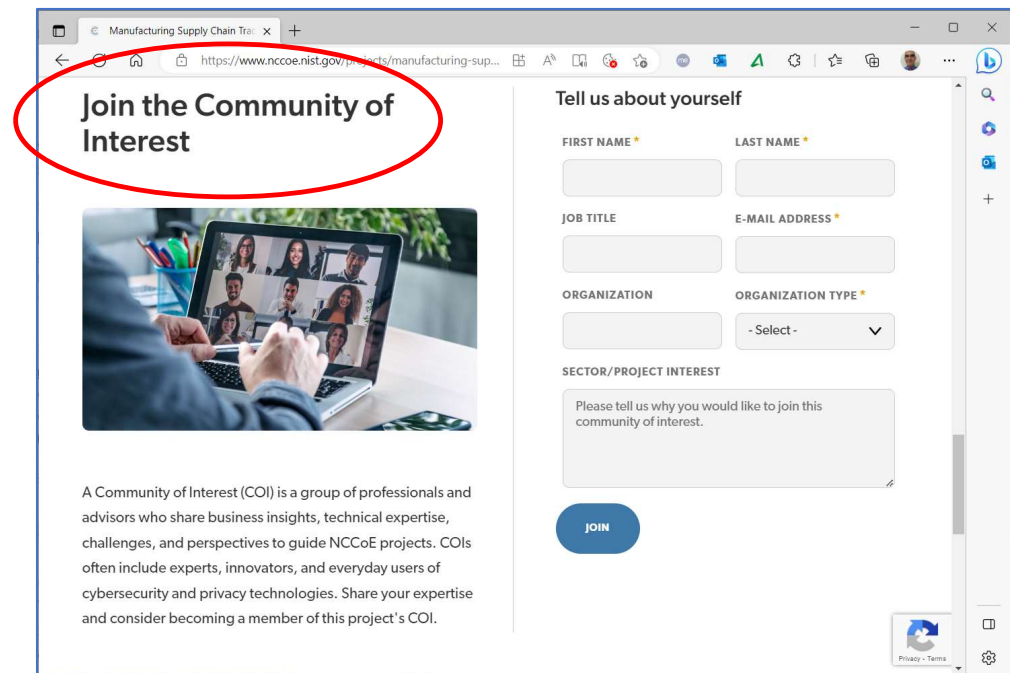
Figure 5: Component and Server Architecture

# NEXT STEPS

1. Finalize adjudication of comments received during the comment period
2. Release FRN based on Project Description
3. Please join the community of interest

[Manufacturing Supply Chain Traceability Using Blockchain-Related Technologies | NCCoE \(nist.gov\)](https://www.nccoe.nist.gov/projects/manufacturing-supply-chain-traceability-using-blockchain-related-technologies)

Scroll down...



**Join the Community of Interest**

**Tell us about yourself**

FIRST NAME \*  LAST NAME \*

JOB TITLE  E-MAIL ADDRESS \*

ORGANIZATION  ORGANIZATION TYPE \*

SECTOR/PROJECT INTEREST

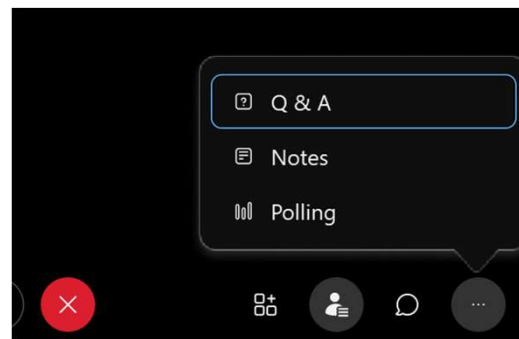
Please tell us why you would like to join this community of interest.

A Community of Interest (COI) is a group of professionals and advisors who share business insights, technical expertise, challenges, and perspectives to guide NCCoE projects. COIs often include experts, innovators, and everyday users of cybersecurity and privacy technologies. Share your expertise and consider becoming a member of this project's COI.

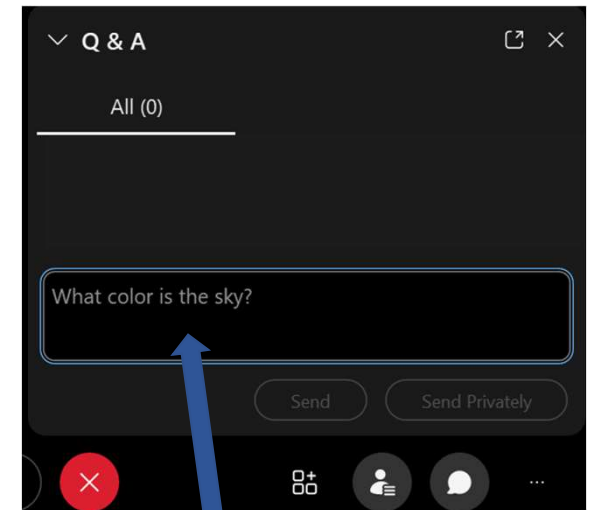
# AUDIENCE ENGAGEMENT

Please use the Q&A window to enter your questions.

We will do our best to answer all questions during the Q&A and will post responses to those we didn't have time to cover



1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.



2. Type your question in the text box and click Send





Michael Pease, [michael.pease@nist.gov](mailto:michael.pease@nist.gov)

National Institute of Standards and Technology Smart Connected System Division

Steve Granata, [sgranata@mitre.org](mailto:sgranata@mitre.org)

The MITRE Corporation

Harvey Reed, [hreed@mitre.org](mailto:hreed@mitre.org)

The MITRE Corporation



[nccoe.nist.gov](http://nccoe.nist.gov)



[@NISTcyber](https://twitter.com/NISTcyber)