NIST Cybersecurity White Paper
NIST CSWP 51 ipd

Developing a Transit Cybersecurity Framework Community Profile

Project Update

Initial Public Draft

CheeYee Tang
Smart Connected Systems Division
Communications Technology Laboratory

Eileen Division
Alex Alshtein
Matt Hardison
Christina Sames
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.51.ipd

August 20, 2025

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

How to Cite this NIST Technical Series Publication:
Tang C, Division E, Alshtein A, Hardison M, Sames C (2025) Developing a Transit Cybersecurity Framework Community Profile Project Update. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 35 ipd.
https://doi.org/10.6028/NIST.CSWP.51.ipd.

Author ORCID iDs
CheeYee Tang: 0009-0000-2847-1443
Eileen Division: 0009-0004-3152-3776
Alex Alshtein: 0009-0009-9071-160X
Matt Hardison: 0009-0002-7422-8131
Christina Sames: 0009-0003-1817-8333

Contact Information
transit-nccoe@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Public Comment Period
August 20, 2025 – September 19, 2025

Submit Comments
transit-nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/cswp/51/developing-a-transit-cybersecurity-framework/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Transit agencies face rising cybersecurity risks that can impact the delivery of safe and reliable transit services. This white paper outlines the preliminary content of a Transit Cybersecurity Framework (CSF) Community Profile that is intended to provide a mission-prioritized approach to identifying practical cybersecurity outcomes tailored to the sector's cybersecurity challenges and priorities. It offers an update on the progress made to date, a preview of the priorities that the community shared that informs the Profile, and a general description of the essential features of a draft Profile. It is designed to engage public and private sector stakeholders in the transit community to inform a draft Transit CSF 2.0 Community Profile, set to publish later this year.

Keywords

Bus, commuter rail, cybersecurity, Cybersecurity Framework (CSF), public transportation, rail, risk management, subway, transit.

Audience

This cybersecurity white paper is primarily intended for cybersecurity professionals, executives, and management teams of public and private organizations that own or operate public transportation services. The audience also includes affiliated entities, such as county governments responsible for overseeing transit operations, federal agencies with oversight of transit operations, and transit industry associations.

Note to Reviewers

NIST aims to tailor the CSF to meet the unique needs of transit owners and operators, resulting in a Transit CSF Community Profile (hereafter, the Community Profile). To date, NIST has engaged with a broad cross-section of stakeholders in the transit sector and has begun developing this Community Profile content. This white paper presents preliminary content for public review and comment ahead of publishing a draft Community Profile.

NIST requests input on the unique technical challenges of securing the transit sector, transit community priorities, and the set of standards, guidelines, and practices that address the needs of securing the transit ecosystem. NIST welcomes your suggestions in these areas in addition to comments on the content within this white paper.

***Editor's Note**: Italicized text within a section provides additional context for the content in that section of the Community Profile and requests for targeted feedback.*

Table of Contents

List of Tables

List of Figures

1. Introduction

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 introduced the concept of a *Community Profile*. A Community Profile is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. It is typically developed for a particular sector, subsector, technology, threat type, or other use case, and can be used by an organization as the basis for its own Organizational Target Profile [1].

The National Institute of Standards and Technology is currently developing a Transit Community Profile to provide a voluntary, risk-based approach for managing cybersecurity activities, reducing cybersecurity risks, and improving the cybersecurity posture of the transit community.

The transit community, for the purposes of the Community Profile, includes public and private owners and operators of public transportation services. They operate a diverse mix of equipment and services that can include bus and rail (i.e., light rail, subway, and commuter rail), and also includes affiliated entities, such as county governments responsible for overseeing transit operations. However, it does not include national rail passenger or freight rail services.

The Community Profile will suggest prioritization of cybersecurity outcomes to meet specific strategic business/mission focus areas for the transit community and identify relevant and actionable security practices that can be implemented in support of those areas. It is intended to complement, not replace, any existing cybersecurity programs, guidelines, or policy that transit operators may already have in place.

The Transit Community Profile will offer a variety of potential benefits, including but not limited to:

- Describe a shared taxonomy to support communication about cybersecurity risk management for transit owners/operators
- Consolidate transit cybersecurity requirements, recommendations, and guidelines from multiple industry stakeholders under one framework
- Develop common target outcomes that transit owners and operators can use to support strategic planning efforts and cybersecurity assessments
- Provide scalable and achievable cybersecurity recommendations and guidelines for transit owners/operators of all sizes

2. Transit Stakeholder Engagement

Developing a Community Profile involves active participation and collaboration from community stakeholders. The National Institute of Standards and Technology engaged with representatives from key national transit organizations and federal agencies (listed below) to identify a cross section of small, medium, and large transit operators to take part in a series of Community Profile working sessions.

- American Public Transportation Association (APTA) members
- Community Transportation Association of America members
- U.S. Department of Homeland Security Transportation Security Administration (TSA)
- U.S. Department of Transportation (DOT) Office of Sector Cyber Coordination
- U.S. DOT Federal Railroad Administration
- U.S. DOT Federal Transit Administration (FTA)

During these working sessions, transit operators took part in facilitated discussions and tailored activities designed to gather and consolidate information and perspectives on their unique cybersecurity challenges, mission priorities, organizational capabilities and resources, and general insights and expertise to inform the Community Profile. A breakdown of working session topics is shown in Figure 1.

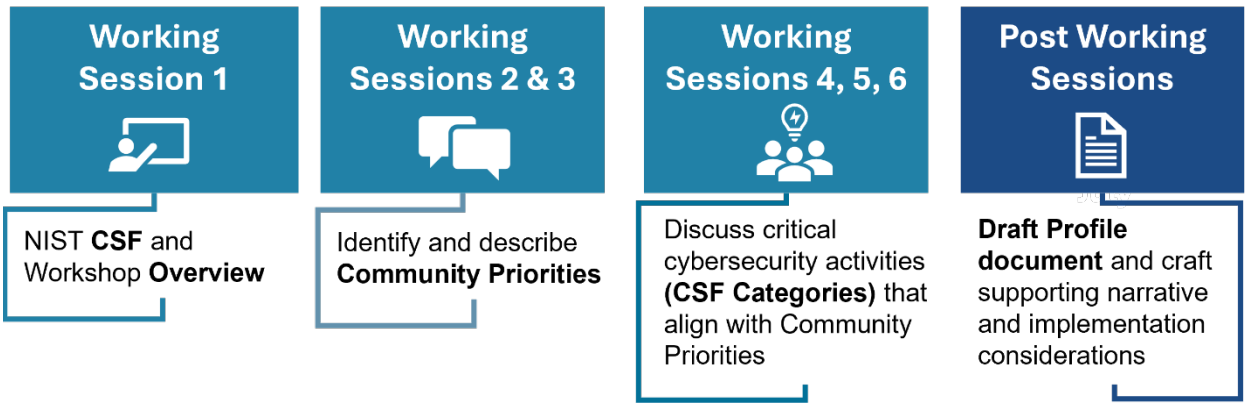

Figure 1: Overview of Community Profile Working Sessions

From these discussions, transit community participants:

- Identified high-level Community Priorities based on importance/criticality to the transit community and its operations
- Discussed ranked cybersecurity outcomes that enable each transit Community Priority
- Shared their expertise, challenges, perspectives, and expectations to enrich the Community Profile and ensure it addresses the specific threats and vulnerabilities unique to the transit sector

- Shared key transit-specific cybersecurity resources and guidance, including APTA's Cybersecurity Resources and TSA's Surface Transportation Cybersecurity Toolkit to inform Profile guidance

3. Challenges to Securing Transit Systems

Transit owners and operators manage a complex network of business and operational systems in service to their mission. Examples can include:

- Rail signaling and train control systems
- Bus fueling, battery-electric charging, and charge management systems
- Scheduling and dispatching
- Facility management systems
- Emergency communications systems
- Control and communication systems
- Ticketing systems
- Command centers
- Revenue collection systems, including back office and fare payment systems
- Public information systems, such as station-based electronic signage and web and mobile applications/systems

Traditionally, many of these systems relied on direct connections for communications. Today, communication between and among these systems is digital and network-based, including through extensive use of wireless connectivity. This dependence on digital technology and interconnections to sustain daily operations has widened the cyber attack surface for transit agencies. Operators must now manage the cybersecurity risk of their IT and OT systems while meeting increasingly demanding safety and operating requirements.

Several aspects of the transit sector make it uniquely challenging to protect and requires a more tailored approach to prioritize and apply cybersecurity risk management measures. These include:

- **Safety-critical control systems**. Safety-critical control systems—such as signaling and train control for rail, and steering, acceleration, and brake control for buses—are governed by standards which may not fully account for cybersecurity risk. Cybersecurity risk mitigations for these systems must be carefully implemented to ensure they meet safety and industry standards without triggering the need for safety recertification.
- **Legacy systems**. Most transit agencies simultaneously manage both modern and legacy IT and OT infrastructure and systems. Legacy systems and assets in the transit sector have long lifecycles measured in decades, not years, and may not be able to accommodate modern cybersecurity controls (e.g., multifactor authentication, advanced encryption). Retrofitting these systems for cybersecurity purposes can be cost-prohibitive and disruptive, and compensating cybersecurity controls may be needed to meet the security outcomes.

- **Communication systems**. Communication systems (e.g., wireless, wired, radio) are the backbone of public transit operations, supporting coordination between buses, vehicles, trains, control centers, and infrastructure. They facilitate real-time updates, signaling, dispatching, and monitoring. Any disruption or compromise in these systems can lead to operational failures, delays, or even accidents, impacting the safety and reliability of transit systems.
- **Vendor supply chain**. Rail and bus transportation systems and components are supplied by a large variety of domestic and global suppliers. Likewise, transit agencies rely heavily on vendor services and contractors to install, manage, and maintain their IT and OT systems and infrastructure. Cybersecurity supply chain risk management must be part of an organization-wide risk management strategy.
- **Distributed and mobile operations**. Transit operations and their support systems are geographically dispersed with mobile assets. Rail operators, for example, manage systems and sensors that encompass the rail network and associated facilities. Likewise, bus operators support moving assets, garages, and maintenance facilities deployed across a metropolitan region.
- **Physical security concerns**. Transit assets and infrastructure are both accessible to and used by the public. Many of the supporting systems are also distributed across a broad region, making physical security more challenging and exposing certain elements, such as telecommunications systems or wayside equipment, to potential unauthorized physical and logical access by malicious actors.
- **Safety-centric culture**. A transit operator's top responsibility is safety. Cybersecurity knowledge and awareness in many agencies is still maturing. The American Public Transportation Association, federal agencies, suppliers, and the operating agencies themselves have worked to develop and organize resources to advance cybersecurity awareness and protections specific to transit operations. Cybersecurity measures and training must continue to integrate into an agency's overall safety framework to improve effectiveness.

4. Community Profile Structure

The Transit CSF Community Profile will be built around the six Functions of the CSF 2.0: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER. Each Function consists of Categories that are a group of related cybersecurity outcomes that collectively make up each CSF Function. Each Category is decomposed into Subcategories that define more specific technical and management activities.

Figure 2 provides a representation of how cybersecurity outcomes are prioritized by the workshop participants. The stars in Figure 2 represent the degree of importance of CSF 2.0 outcomes in the context of the Community Profile [2].

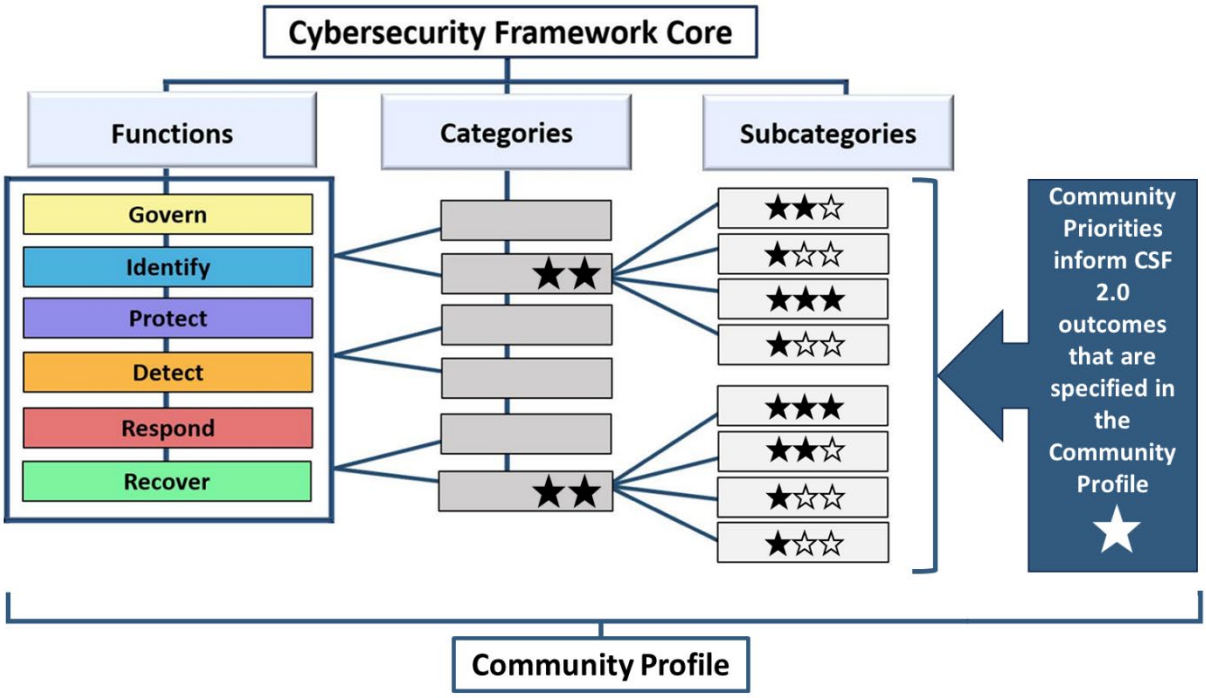

Figure 2: Representation of Community Profiles Using the CSF 2.0 Core

Additional information about, and examples of, Community Profiles are available online at the NCCoE Resources for Applying NIST Frameworks. The Transit CSF Community Profile will be included in this resource library once it is published.

5. The Role of Community Priorities in Profile Development

Identifying Community Priorities is an important part of the Community Profile-building process. Community Priorities reflect the fundamental purpose and operation of the community and can provide the context for identifying and managing applicable cybersecurity risk management measures. They serve to inform the CSF 2.0 outcomes and their relative importance within the community.

Consistent with this approach to Profile development, participants identified eight notional Community Priorities for the transit sector. Those Priorities were further consolidated in the working sessions into four Strategic Focus Areas. Those Focus Areas and some of the challenges identified are included in Table 1.

***Editor's Note**: The list of challenges beside each Community Priority below is not exhaustive; NIST is interested in feedback on technology-specific cybersecurity challenges that are top of mind for your transit operations and how they align with your organization's mission. Suggest challenges that should be considered, removed, or consolidated in the Profile. Which challenge(s) stands out or resonates the most with respect to your operating environment?*

Table 1 Notional Transit Community Priorities

Strategic Focus Area	Community Priority	Cybersecurity Challenges Identified
Transit Operations and Ridership	Deliver Reliable "On Time" Service	Increasing operational efficiencies and redundancies, providing and restoring services during disruptions, maintaining disaster recovery and business continuity capabilities, and continuously improving services.
	Deliver Safe and Secure Transit Services	Identifying cybersecurity risks that can jeopardize services and staff/rider safety, continually monitoring systems for anomalous activity, enabling incident recovery execution, adhering to safety regulations, identifying high value assets/crown jewels, maintaining resilience through documented and tested business continuity and disaster recovery plans.
Protection and Management of Transit Assets	Protect Data	Complying with state and federal data protection regulations, protecting sensitive information such as system security information and staff and rider personal data, and securing financial transactions and systems (e.g., fare payment systems or accounting/payroll systems).
	Protect IT and OT Systems and Assets	Achieving regulatory compliance, discovering and documenting asset inventories, protecting legacy systems, securing communication systems, and providing physical security to OT assets and remote sites/systems, monitoring and detecting malicious behavior, securing access to information systems,

Strategic Focus Area	Community Priority	Cybersecurity Challenges Identified
		identifying critical assets and infrastructure, leveraging modern cybersecurity protections, and achieving economies of scale.
Stakeholder Coordination	Foster Collaboration Among Stakeholders	Aligning cybersecurity objectives with internal stakeholder needs to manage shared security risks, identifying and codifying (e.g., through Memorandum of Understanding) roles and responsibilities with internal and external partners/vendors/suppliers in order to support cyber incident response and recovery.
	Secure the Transit Supply Chain	Managing the supply chain of key IT/OT components and supporting infrastructure (e.g., factoring in equipment replacement lead times for system components as part of business continuity/disaster recovery plans), managing relationships with as well as risks of third-party vendors, suppliers, and managed service providers, and integrating cybersecurity requirements into acquisitions.
Organizational Development	Engage in Continuous Improvement and Innovation of Transit Operations	Evaluating the security risk of emerging technologies, applying modern cybersecurity controls to legacy assets, and applying lessons learned from cyber audits/events/incidents/exercises to continually improve a cybersecurity program.
	Cultivate a Cyber Aware Workforce	Hiring, training, and retaining qualified cyber talent, incorporating cybersecurity into enterprise risk management, providing tools to recognize and report on cyber risks, providing role-based training and encouraging staff accountability for cybersecurity, executing and measuring the effectiveness of training and cyber awareness campaigns, and instituting cybersecurity governance and management.

6. Community Profile Mapping

The foundation of the transit Community Profile is the CSF 2.0 Profile mapping, which is typically presented as a table or set of tables. The mapping is organized around the CSF 2.0 Core to identify and prioritize cybersecurity outcomes that are most relevant to the transit sector. It is supplemented with recommendations, considerations, and guidelines that agencies and operators can leverage and adapt for their own environment.

In the mapping table, each CSF 2.0 Subcategory appears as its own row. An example of this is shown in Figure 3. Each row is labeled to show its importance to one or more of the four Strategic Focus Areas, using the following designations:

- Elevated (E): These Subcategories are deemed the most critical for supporting a Focus Area, based on input from the CSF Profile working sessions.
- Supporting (–): These Subcategories are important for the transit sector's cybersecurity posture but are not as critical relative to the Elevated Subcategories.

The National Cybersecurity Center of Excellence (NCCoE) team of transit sector and cybersecurity subject matter experts analyzed the outputs from the CSF Profile working sessions and Category prioritization activities and used them to inform CSF Subcategory designations. The designations of "Elevated" and "Supporting" are relative to the Profile and may vary for different transit agencies. Each transit operator should consider its own goals and priorities when consulting this Profile and adjust how it applies the guidelines accordingly.

Only Subcategories designated as "Elevated" will include an explanation of their importance to a particular Community Priority, as well as voluntary guidelines and informative references.

***Editor's Note**: NIST welcomes feedback on which CSF 2.0 Categories and Subcategories should be designated as "Elevated," and invites input from the community about areas that are particularly challenging to implement or where cybersecurity risk management guidance is needed. NIST also encourages suggestions for existing standards, guidelines, and best practices to include in the Community Profile.*

NIST CSF 2.0 Subcategory	Transit Operations and Ridership	Protection and Management of Assets	Stakeholder Coordination	Organizational Development	Subcategory Rationale and Guidelines
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	**E**	—	—	**E**	**Transit Operations and Ridership:** Cybersecurity is an enterprise risk that senior leaders should consider alongside others, such as financial and reputational risk. A transit operator's mission and vision inform and help prioritize cybersecurity risk management decisions related to safe and reliable transit services, and the need for, or use of, new technologies. **Organizational Development:** Staff in all parts of a transit agency should understand the risk a cybersecurity incident/event can cause to transit operations and its importance in critical infrastructure. Understanding the transit agency's mission helps identify and prioritize the groups or functional areas where cybersecurity training and awareness would be most beneficial, including groups that administer technology or handle sensitive information both inside and outside of IT (e.g., OT/SCADA, garages, vehicles) and business groups such as senior management, safety, security, human resources, legal, and procurement/contracts. **Recommendations/Considerations/Guidelines:** • Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, and other organizations. (NIST 800-53r5 PM-11) • Review the agency's mission, vision, and strategic plan/roadmap. Determine if major projects (e.g., system build out, renovation, integration with partners) are being undertaken in the next 1-5 years and to what extent they involve technology and influence cybersecurity risk. (APTA SS-ECS-RP-004-23) • Envision cybersecurity as a contributor to concrete, visible, positive progress for the agency and its mission. (APTA SS-ECS-RP-004-23)

Figure 3: Sample CSF 2.0 Transit Community Profile

7. Applying the Transit CSF Community Profile

Transit agencies and operators can adapt and use the Community Profile to establish or improve their cybersecurity risk governance process, practices, and activities and align with other risk management priorities. When applying the Community Profile, transit agencies and operators should consider the unique needs of their operating environment (e.g., applicable local laws, policies, standards), risks, challenges, threats, and other influencing factors adapting it for their use.

To apply the Community Profile, transit agencies and operators may use the following activities:

- Use as a baseline to develop an agency's own CSF Organizational Target Profile.
- Conduct a gap analysis to determine a transit operator's cybersecurity posture relative to the Community Profile. Address gaps by prioritizing outcomes based on impact and relative importance to cybersecurity and how those gaps advance a transit operator's mission.
- Map the transit operator's applicable policies, standards, and other implementation resources where available (these may be used in addition to or instead of the references provided for each Subcategory).
- Integrate CSF cybersecurity outcomes into existing and emerging corporate-wide risk governance programs.
- Tie key cybersecurity outcomes to budget/resource allocations for cybersecurity within the transit agency.
- Use the Community Profile as a tool to aid cybersecurity risk management and strategic communications, both internally and externally.

8. Next steps

The National Institute of Standards and Technology invites feedback on the concepts outlined in this white paper through September 19, 2025. Comments can be sent to transit-nccoe@nist.gov. Comments received will be considered during the development of the draft Transit Community Profile. While the Profile will provide additional details and content, NIST encourages input on this approach at this stage, as well as on specific topics identified in this white paper (e.g., the **Editor's Note**).

To help you stay informed and engaged with activities related to this Profile effort, NIST has established the Transit CSF Community Profile page on the NCCoE website located at https://www.nccoe.nist.gov/projects/transit-cybersecurity-framework-csf-community-profile. This site provides status updates on the Profile and offers an opportunity to join the Transit Profile Community of Interest.

References

[1] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[2] Pascoe C, Snyder JN, Scarfone KA (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd