NTCIP

S

National Transportation Communications for ITS Protocol

Results of the NTCIP Task Force on Interoperability and Security

November 2025

ACKNOWLEDGEMENTS

This document was prepared by the NTCIP Task Force on Interoperability and Security, a temporary group established by the Joint Committee on the NTCIP. The Joint Committee on the NTCIP is organized under a Memorandum of Understanding among the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA). The Joint Committee on the NTCIP consists of six representatives from each of the standards development organizations, and provides guidance for NTCIP development.

The following individuals were members of the NTCIP Task Force on Interoperability and Security:

- John Thai (Co-Chair)
- Tom Stiles (Co-Chair), Swarco McCain
- Luke Aldrich, Skyline Products
- Shaun Alford, Yunex
- James Barnhart, Skyline Products
- Matt Barron, Cubic
- Ralph Boaz, Pillar Consulting
- Wolfgang Buckel, Yunex
- Patrick Chan, ConSysTec
- Meadow Cho, Saesol Tech
- Anthony Cox, Advanced Traffic
- Doug Crawford, Q-Free
- Ray Deer, Oriux
- Jonathan Grant, Yunex
- Brian Griggs, Econolite
- Craig Hinners, NoTraffic
- Woody Kim, Saesol Tech
- AJ Lahiri, ConSysTec
- Matt Luker, Utah DOT
- Patrick Marnell, Q-Free
- Michael Mullen, Caltrans
- Siva Narla, ITE
- Whitney Nottage, Q-Free
- Tony Pallissery, Yunex
- Frank Provenzano
- Robert Rausch, TransCore
- Avery Rhodes, Advanced Traffic
- Michael Robinson, Caltrans
- Mark Simpson, Swarco McCain
- Shane Johnson, Econolite
- Douglas Tarico, Econolite
- Shea Tomsin, Econolite
- Paul Tykodi, Massachusetts DOT
- Ken Vaughn, Trevilon
- Donald Wang, Western Systems
- Robert White, Nashville DOT
- Wuping Xin, Caliper

Purpose

The purpose of this document is to propose to the National Transportation Communications for ITS Protocol (NTCIP) Joint Committee (JC) a course of action to expedite the deployment of secure center-to-field communications for actuated signal controllers (ASCs). Concerns have been expressed by key stakeholders (primarily traffic controller manufacturers) that the *Recommended Standard NTCIP 1202 v04* will further delay deployment of secure communications required to protect the Intelligent Transportation Systems (ITS) architecture.

Background

Providing secure communications was determined to be the highest priority in updating 1200 series NTCIP standards by the Infrastructure Standards Security Assessment (ISSA) working group. The final report of the ISSA project, NTCIP 9014, outlines a plan to transition all NTCIP device standards based on SNMPv1 communications to SNMPv3. SNMPv3 provides authentication and encryption to protect communications, addressing security limitations inherent in SNMPv1. The NTCIP working groups have been addressing security inadequacies in the existing SNMPv1-based standards as each 1200 series document is updated. The NTCIP 1202 working group voted and recommended to the NTCIP Joint Committee that SNMPv3 be specified as the protocol for managing ASC devices and providing secure communications for the NTCIP 1202 v04 standard.

At the NTCIP Joint Committee (JC) Meeting held in Salt Lake City, UT from April 28th through May 1st, 2025, the manufacturer community voiced concerns regarding lead time to put to market full implementation of NTCIP 1202 v04 Recommended Standard (RS) due to extensive development effort required by adoption of ISO standardization (ISO 26048-1) and security and data management/transfer using the SNMPv3 mechanism as specified in NTCIP 1202 v04 RS. Specifically, concerns focused on the level of effort needed by device manufacturers and system integrators to implement the new standard due to the significant redesign and restructuring of the underlying NTCIP 1201/1103 data structures. The updated data structures would significantly impact the operations of the devices' embedded software, requiring major rework of logic code in addition to the changes specific to NTCIP communications. The following are two examples:

- The deprecation of the NTCIP 1201 MIB objects includes a change to the software schedule. The changes in table sizes and types of tables and objects require refactoring and/or substantially rewriting the scheduling functionality in the device software. For a device to communicate with both NTCIP 1202 v03 based managers (e.g., central software system) and NTCIP 1202 v04 based managers, the device software would require two different implementations of the scheduler parameters.

- The deprecation of existing NTCIP 1200 objects and replacing them with new, ISO-compliant objects with similar purposes requires re-working the software associated with those objects. In addition, every object changed requires some type of refactoring of the code and efforts associated with validation, review, and testing.

Many in the manufacturer community felt that there were more efficient methods to achieve cybersecurity and interoperability. At the JC Meeting, manufacturers shared different solutions to address concerns that could threaten long-term interoperability in the 1200 series standards. Recognizing that these concerns require further consideration, the *NTCIP Task Force on Interoperability and Security* was established at the Joint ATC and NTCIP JC meeting. The Task Force's primary objectives were to research alternative methods for expediting the implementation of a secure protocol while maintaining interoperability, and to deliver a white paper to the NTCIP Joint Committee for review and consideration. Additional details regarding the task force objectives and associated white paper are included below.

The following projects contributed to the development of Recommended Standard (RS) NTCIP 1202 v04. They are briefly described below to provide context for this proposal.

Infrastructure Standards Security Assessment (ISSA) Project (9/2019 - 8/2021)

ISSA was the first project to investigate the issue of securing NTCIP communications. NTCIP was originally built using SNMPv1, which allows for unverified user identification but does not provide any support for authentication or encryption. Due to this inherent limitation of SNMPv1, it was quickly determined that any solution would require a migration away from SNMPv1. This would result in a loss of backwards compatibility with prior versions of the NTCIP standards. At the start of the ISSA project, the NTCIP Base Standards Protocols and Profiles (BSP2) Working Group (WG) considered several alternative protocols, including:

- SNMPv3: the latest version of SNMP, which offered potentially the easiest migration path
- NETCONF: a protocol that many network device manufacturers migrated to after SNMP due to its ability to more easily handle proprietary extensions for configuration options
- RESTCONF: an alternative to NETCONF that offered a more API-centric interface
- REST APIs: which focus on APIs rather than object manipulation
- Data distribution technologies (e.g., MQTT, AQMP, DDS, etc.)

At the time, the group concluded that none of the other protocols offered a significant advantage over SNMPv3 and that migration to SNMPv3 would simplify the migration process due to its similar design to SNMPv1 (e.g., similar MIB, use of OIDs).

The main deliverable of the ISSA project was the report *NTCIP 9014v01 Infrastructure Standards Security Assessment (ISSA)*. The development of the NTCIP 9014 included:

- An assessment of the security needs for transportation field devices
- A detailed discussion of the proposed SNMPv3 communications stack
- An analysis of the changes that would be required to migrate from SNMPv1 to SNMPv3
- Documenting the way ahead to implement the changes, including the order in which standards would need to be updated and the coordination that would be required with ISO and IETF
- A detailed annex that identified the proposed changes for each object

The report was produced by the BSP2 WG and included the industry review and comment period required by the NTCIP Standards Development Process, as documented in NTCIP 8001.

International Standards Support (10/2022 - 6/20/25)

In addition to the ISSI project, the USDOT supported the necessary revisions to ISO and IETF standards to address the comments from the various NTCIP working groups. These resulted in the publication of RFC 9456, ISO 15784-2:2024, and ISO 26048-1:2025.

Infrastructure Standards Security Implementation (ISSI) Project (4/2023 - 6/20/25)

The NTCIP Infrastructure Standards Security Implementation Project (ISSI) was funded to implement the initial set of proposed changes as documented in NTCIP 9014 to enhance cybersecurity in NTCIP standards. The ISSI focused on:

- Revising the NTCIP foundational standards (i.e., NTCIP 1103, 2202, 2301, and 1201);
- Revising the highest priority device standards (i.e., NTCIP 1203 and 1204); and
- Starting revisions to the next tier of device standards (NTCIP 1209, 1211, and 1218).

NTCIP 1202, another high-priority standard, was omitted from this project due to other changes being made; instead, its migration to SNMPv3 was conducted under the separate NTCIP 1202 v04 project (see below).

While the update efforts focused on implementing the changes proposed in NTCIP 9014, detailed discussions of the standards often led to other refinements.

NTCIP 1202 v04 Actuated Signal Controllers (ASC) Development (8/2022 - 8/2025)

In August 2022, the NTCIP 1202 Working Group was tasked with developing NTCIP 1202 v04 with the primary objective of creating an NTCIP 1202 standard based on SNMPv3. The work also included various feature enhancements. The summary of changes is as follows:

- Migrated the 1202 MIB structure to SNMPv3
- Replaced requirements for the NTCIP 1201 and NTCIP 1103 global object standards with requirements for the new ISO 26048-1 standard
- Support for longer phase times and timing pattern cycles
- Support for changing parameters for phases, overlaps, vehicle detectors, and pedestrian detectors on a schedule (parameter sets)
- Support for activating more special functions on a schedule
- Support for longer detector no activity times before faults are reported
- Support for receiving external local control application data
- Support for receiving calls from roadside units
- Enhanced design for specifying the cycle zero point
- Support for reading signal monitoring unit diagnostics
- Support for activating backup mode manually
- Support for resetting detector diagnostics
- Support for different coordination force off modes for each phase
- Enhanced status monitoring

The proposed Recommended Standard (pRS) NTCIP 1202 v04 was presented to the NTCIP Joint Committee at the meeting in Salt Lake City. It was accepted as Recommended Standard (RS) NTCIP 1202 v04 by the NTICP Joint Committee and forwarded to AASHTO, ITE, and NEMA for approval.

Task Force Goals and Objectives

The purpose of the Task Force white paper is to address implementation concerns regarding the NTCIP 1202 v04 RS and provide recommendations for changes to the NTCIP Joint Committee.

The objectives of the white paper are:

- To define an alternative implementation of 1202 v04 using SNMPv3
- Maintain interoperability goals of the NTCIP organization
- Retain more of the 1202 v03, 1201, and 1103 data-structure
- To achieve consensus in converging to one cybersecurity technology
- To investigate the effects of ISO harmonization in the RS
- To address how this specific NTCIP problem is common to 1200 series devices
- Submitting the Task Force's findings and recommendations to the NTCIP Joint Committee.

The Task Force Charter is included as Appendix A for reference.

Problem Statement

Based on the conversation of the *NTCIP Task Force on Interoperability and Security*, the question in front of the Task Force is summarized as:

How can Infrastructure Owner-Operators *(IOOs) and manufacturers rapidly secure their existing NTCIP/SNMPv1 implementations, while also maintaining sufficient backward compatibility to ensure smooth integration between non-secure and secure environments?*

The challenge is to introduce security features in a way that minimizes disruption, preserves interoperability across diverse vendor platforms, and provides a clear migration path for systems that will operate in mixed environments of newer and older devices & software during transition periods.

Alternatives Evaluation

The Task Force discussed multiple alternative solutions to the 1202 v04 recommended standard including the current state of practice, providing security through improved network management, and non SNMP-based protocols. A brief overview of each alternative discussed is listed below.

Initial Alternatives:

- **SNMPV1 (Status Quo)** – While the current use of SNMPv1 does not meet the primary cyber-security objectives, the "what-if we do nothing?" scenario was discussed. The discussion further solidified that:
    1. The Task Force recognizes the absolute need to secure Center to Field communications in the shortest time possible, and
    2. The recommended solution must still, when enabled, provide support for legacy deployments using SNMPv1 due to the extended time necessary to upgrade infrastructure.

- **SNMPv1 with added network security** – Maintains the use of the existing 1202, SNMPv1-based standard while implementing a secure transport and networking layer such as TLS, IPSec, or VPNs. The Task Force acknowledged that this alternative can be applied to temporarily secure legacy deployments. However, its lack of authenticating individual messages makes devices vulnerable to malware or other malicious activity from within the network. Therefore, merely applying network security layers would not meet the primary objectives. This alternative would have no impact on existing system and device software code bases.

- **SNMPv3 Simplified** – Migrates the existing 1202 MIB structure to SNMPv3 and addresses specific issues in 1202 without deprecating the 1201 MIB and restructuring the 1202 MIBS. This could be done starting from the 1202 v03a, 1202 v03b, or 1202 v04 MIB. Under the alternative, 1103 Dynamic Object configuration would be retained. This alternative would have the least impact on software functionality. Manufacturers participating in the Task Force agreed this would be the fastest path to securing existing transport protocols at a device message level. Using the same MIB structure, backwards compatibility for legacy devices could be maintained without the need to support two completely separate MIB structures.

- **REST API** – Modern web-based protocol proposed to transition away from SNMP all-together. Discussions indicated that SNMP is outdated and not as well supported as it was 20 years ago. Leveraging the existing MIB structure and data schema, a REST API can provide more flexibility for dynamic objects and can be used in a pub/sub architecture to reduce device bandwidth needs on the network. It was also stated that SNMPv3 would require more resources (i.e. memory, CPU processing time, etc.) than a modern REST interface. A webserver must be running on the embedded device as a prerequisite resulting in a longer implementation for devices that do not already include a web server.

- **NETCONF/RESTCONF** – Focused on the use of NETCONF, an XML-based protocol for configuring network devices over SSH, or RESTCONF which provides a RESTful HTTP interface using JSON or XML. Discussions limited the evaluation to using a standard YANG data model that is converted from the existing SNMP MIBs. While representing a solution similar to REST API, the Task Force did not further evaluate this option.

- **MQTT** – Pub/Sub message brokering which would change NTCIP communications from the SNMP poll-based protocol to a subscribe and push protocol. MQTT can substantially reduce network bandwidth and provides a more robust alternative to connecting multiple Centers (central systems) or devices to a single field device. The Task Force discussed the substantial work required to convert SNMP-based software to MQTT. However, it was not determined how the level of effort compares to implementing the 1202v4 recommended standard.

- **gRPC AND Protobuf** - Generally meets the core requirements for security and interoperability. The protocol created by Google is flexible and would provide advantages to SNMP communications. However, the Task Force expressed concerns that the effort to migrate to gRPC is substantial compared to simplifying the updated 1202v4 MIBS.

- **gNMI** – Paired with gRPC, the gRPC Network Management Interface (gNMI) is a modern, open-source protocol developed under the OpenConfig initiative, leveraging gRPC for efficient configuration management, telemetry streaming, and operational state retrieval in network devices. Designed to address the limitations of legacy protocols like SNMP, gNMI uses YANG data models for structured data representation and Protocol Buffers (Protobuf) for serialization, making it suitable for high-performance environments.

- **Discoverable protocols** – Focused on interoperability, a discoverable protocol would define the handshake/connection from the central system to the device. The device would then provide the management system with its complete data structure. The data structure could be designed to include meta-data defining menu structure, database editor layouts, etc. In the simplest form, field devices should provide their full, manufacturer specific MIBS to a management system upon a standard request.

The technologies were narrowed down, collaboratively analyzed, and discussed by the Task Force over several meetings. After discussion of the initial alternatives, sub-groups volunteered to further refine their preferred alternatives. Each sub-group refined their alternative and presented findings to the taskforce at the August 8, 2025, meeting.

The sub-groups and refined alternatives were:

- **SNMPv3 per Recommended Standard**
  - Members: Ken Vaughn
- **Simplified SNMPv3**
  - Members: Leo Aguilar, Anthony Cox, Avery Rhodes, Mark Simpson, Wuping Xin
- **REST API with WebSockets and HTTPS**
  - Members: Doug Crawford, Pat Marnell, Whitney Nottage, Mark Knellinger, and Robert White
- **gRPC with or without gNMI**
  - Members: Wolfgang Buckel and Wuping Xin
- **Discoverable Protocol**
  - Members: Tom Stiles

On August 15, 2025, after presentation of the alternatives and subsequent discussion, the Task Force voted on which alternative was preferred for further investigation and recommendation. The “SNMPv3 per

Recommended Standard" (NTCIP 1202 v04) alternative was excluded from the voting to isolate the question of "what people would do different from the currently recommended standard."

A summary of the vote is displayed below, and the full roll call vote is documented in Appendix A.

	Recommended Alternative			
	Simplified SNMPv3	**REST w/ WebSockets & HTTPS**	**gRPC w/o gNMI**	**gRPC with gNMI**
Totals	**11**	**4**	**4**	**0**

The vote showed a mathematical majority for the "Simplified SNMPv3" approach over all API based approaches (REST, gRCP, Discoverable[1]). The Task Force therefore focused further efforts on discussing and refining the Simplified SNMPv3 approach.

The Simplified SNMPv3 approach was discussed in detail over the subsequent meetings. Based on those discussions, a framework for the Simplified SNMPv3 approach was documented in the following motion[2] at the September 12, 2025, Task Force meeting as:

> *"In light of the conversations over the past months, I move this taskforce to recommend a rapid pivot towards a "simplified SNMPv3" approach to the 1202 standard. This "simplified SNMPv3" approach represents an efficient & effective way to provide cybersecurity and interoperability for the traffic signal industry.*
>
> *This committee should now move towards refinement and documentation of the "simplified SNMPv3" approach which includes:*
>
> - *Maintaining the recommended 1202v4 MIB (removing references to ISO-26048 objects)*
> - *Using the Linted MIB produced by SWARCO and shared in the Task Force Teams channel (ITE Teams)*
> - *Not implementing NTCIP 1103 (except for Dynamic objects STMP replacement)*
> - *Maintaining the existing 1201 MIBS*
> - *Not undertaking further ISO harmonization efforts at this time.*
>
> *For clarity, the taskforce recommends that the "simplified SNMPv3" approach is not an intermediate step to a future full implementation of the NTCIP 1202 v04 Recommended Standard but would be a permanent amendment or alternative to the NTCIP 1202 v04 RS*

[1] Per recommendation by the Discoverable Protocol sub-group, this option was removed from consideration before voting.
[2] Motion by Patrick Marnell. Verbally seconded by Mark Simpson. Seconded in meeting chat by Ray Deer.

The motion was unopposed. A summary of the vote is displayed below, and the full roll call vote is documented in Appendix B.

Vote Totals	
Yes	13
No	0
Abstain	6
Not Present	4

The following section further defines the “Simplified SMNPv3” approach developed by the Task Force.

“Simplified SMNPv3” Approach Recommendation

The recommended approach is to implement a streamlined version of SNMPv3 that secures today’s SNMPv1 deployments in a short timeframe, estimated from 6-12 months instead of 24-36 months for other approaches, while maintaining interoperability, preserving data model backward compatibility, and minimizing disruption to existing device functionality and development plans. This path emphasizes targeted updates to existing MIBs rather than broad data model rewrites. Specifically, the proposal maintains the 1202 v04 MIB while removing references to ISO-26048 objects and leverages the linted 1103-STMP, 1201, and 1202 MIBs produced by the task force which were shared during the meetings on Teams and will be shared afterward on Github. The linted MIBS were also analyzed and validated by multiple parties including Econolite, Q-Free, SWARCO McCain, and Yunex.

NTCIP 1103 will not be re-implemented except for retaining dynamic objects, where the insecure STMP frame has been replaced with an OER-encoded octet string in the existing configuration tables. The established 1201 MIBs are preserved, and no further ISO harmonization efforts are undertaken currently.

For history and event logs, the Task Force recommends adopting the High-Resolution Log method developed by Indiana and Purdue and later expanded through the USDOT Pooled Fund Program TPF-5(377) sponsored by the states of California, Connecticut, Georgia, Indiana, Minnesota, North Carolina, Ohio, Pennsylvania, Texas, Utah, Wisconsin, the Federal Highway Administration, and the City of College Station. This method is currently required in a majority of agency traffic signal controller and central management system specifications and procurement documents. The method is considered the current industry best practice for logging and storing controller history and events. It is currently supported by all traffic signal controller software and central system vendors. To allow for extended logging beyond the current enumerations, it is recommended that manufacturers are required to openly share proprietary event log enumerations and documentation regarding method of retrieval. Details regarding governance and validation should be considered in the next revision of applicable NTCIP standards.

For secure transport and access control, either USM (User-based Security Model) or TSM (Transport Security Model) are recommended, allowing agencies and vendors to select the best fit for their environments. Overall, this “simplified” strategy provides a faster path to market, builds on existing deployments, and maintains interoperability while enabling supplemental APIs such as REST and/or gRPC.

Technical Steps

- **MIB Baseline:**
  - Maintain the NTCIP 1202 v04 MIB as the baseline.

    - Amend the NTCIP 1202 v04 standard to remove ISO 26048-1 references and un-deprecate the 1201 and 1103-STMP MIBs.
- **Linted MIBs:**
    - Use the linted 1103-STMP, 1201v0307, 1202v033b, and 1202v0411b MIBs (validated at level 6), available under the `SmiV2Mibs` folder under the "Protocol Task Force" ITE TEAMs channel. (Link: SmiV2Mibs).
    - Original MIBs are provided alongside linted versions for comparison.
- **Implementation Principle:**
    - Functional changes are intentionally minimal to reduce vendor implementation effort and focus on security and interoperability.
    - Updated MIBs can be implemented within existing SNMPv1 stacks, extending the data model to ensure greater consistency between v1 and v3 during system upgrades.

MIB Updates

- **NTCIP 1103 (Dynamic Objects):**
    - The STMP protocol payload data is now carried inside an OER-encoded octet string for `get/set` operations. This is the only minor functional change. All other changes are syntactic.

```
-- A.3.4.3 Dynamic Object Variable Data for get and set operations
dynObjVariableData  OBJECT-TYPE
   SYNTAX  OCTET STRING
   MAX-ACCESS  read-write
   STATUS  current
   DESCRIPTION
      "<Definition> This is the OER binary encoded dynamic object data.
      It can be used to get or set the data associated with the dynamic
object.
      This payload may not exceed the maximum packet size of the
communications network.
       <Object Definition> 1.3.6.1.4.1.1206.4.1.3.3.1.3
       "
::= { dynObjConfigEntry 3 }
```

- **1201 MIB:**
    - Obsoleted (`globalTime, timeBaseScheduleDate, dstBeginSecondsToTransition, dstEndSecondsToTransition)` and added `(globalTimeV2, timeBaseScheduleDateV2, dstBeginSecondsToTransitionV2, dstEndSecondsToTransitionV2)` updated to use `Unsigned32`, should not functionally change anything.
- **1202 MIBs (v0333b and v0411b):**
    - Numerous syntactic changes, no functional changes.
    - `commPortProtocolsSupported` signed range adjusted, with reserved bits updated was (6–31) now (6-30) for v033b. This object was deprecated in v0411b.

History/Event Log Changes

- **History/Event Log Data Structure -** Adopt High Resolution Event Enumerations specified in USDOT Pooled Fund Program TPF-5(377)
- **Event Log Retrieval (SNMP does not support file transfer natively) -** Standardize method of retrieval to continue use of SCP, VSFTP, and HTTPS

- **Event Enumeration Sharing -** Manufacturers must share or provide upon request all proprietary enumerations and documentation for method of retrieval

Security Implications

Given that the USA has hundreds of thousands of ASCs deployed in daily use across the country, it is not practical to imagine a mass update of this equipment to add SNMPv3 capabilities. Intelligent Transportation System (ITS) network IOOs are expected to apply appropriate cybersecurity controls to keep their ITS networks safe from disruptive activities of malicious threat actors. The implementation of appropriate cyber protections and controls is normally directed holistically at the network as a whole and compensating controls will typically be implemented to protect aspects of the network that lack robust cybersecurity protections.

It is expected that ITS network IOOs are already applying cybersecurity compensating controls when deploying ASCs that use the insecure SNMPv1 protocol. The cybersecurity rationale for putting forward the streamlined version of SNMPv3 deployment model is that it speeds delivery of ASCs with SNMPv3 implemented while maintaining a greater consistency with the current SNMPv1 data model. Thus, new cybersecurity capabilities are delivered in a package that IOOs can choose to deploy as other elements in their ITS networks add SNMPv3 management capabilities as well.

Conclusion

In conclusion, this Task Force recommends adopting the **Simplified SNMPv3 Approach** as the most practical and effective path forward. By leveraging the supplied linted MIBs and upgrading existing SNMPv1 stacks to SNMPv3, agencies and vendors can secure their systems with SNMPv3 with minimal disruption by maintaining a greater consistency with the current SNMPv1 data model. This approach balances speed, interoperability, and security, ensuring that the infrastructure can be protected without unnecessary delays or reinvention.

Although the white paper specifically addresses the 1202 standard and its objects, the Task Force recognizes that these recommendations also affect other 1200 series standards. The Task Force encourages the NTCIP JC and 1200 series Working Groups to consider this approach and other alternative approaches.

From the beginning of the Task Force formation, members acknowledged that three primary objectives of any Task Force recommendation were to:

- Maintain, or improve on the current state of Interoperability provided by the NTCIP 1202 series standard.
- Provide a secure protocol for the exchange of information between traffic management and field devices.
- Make efforts to maintain backward compatibility for existing 1202 deployments

In addition to the recommended “Simplified SNMPv3” method defined above, the task force recommends improving interoperability by adopting the following requirement: Define a standard location on each device where MIBS can be retrieved, like the high-resolution log. This enables third-party integrators to reliably support device-specific data sets. Management stations can then use SCP and/or VSFTP to securely retrieve MIBS from that location. From a market perspective, this recommendation resolves the long-standing limitations to providing true interoperability where manufacturers could choose when, and to whom they provide manufacturer specific MIB objects.

APPENDIX A

Task Force Charter

TASK FORCE GOALS

- Resolve a limited work scope to address a specific NTCIP problem common to 1200 series devices within a short timeframe (3 months)
- Submit TF findings and recommendations paper to NTCIP JC approval

TASK FORCE BASIC RULES

- Roberts Rules
- Respectful behavior required (check your company hats and egos at the door)
- Participation is voluntary basis
- Decisions based on consensus (majority of TF members)
- No rehashing of past votes and decisions (in general)
- Problems raised without a proposed solution will be shelved or ignored
- Have fun (we insist) while getting things done

DISCUSSION ITEMS

- Goals of NTCIP standards
    - INTEROPERABILITY (since 1990s),
    - INTEROPERABILITY + SECURITY (recently)
    - Proprietary and non-interoperable solutions will not be considered by Task Force
- SNMP v1 (White paper)
    - Background and context
    - Strengths, weaknesses, opportunities and threats (SWOT)
- Identify Needs and Requirements (White paper)
    - **TF covers only 1202 standard**
    - Support for legacy devices
        - Define **minimal** requirements for support of legacy devices
        - For how long do we keep this up?
        - Should we cut the umbilical cord? If yes, time horizon?
    - Data dictionary merits
    - Short-term and long-term objectives
        - What are we trying to achieve in the short term?
            - Quick turnaround to achieve 80-90% security updates
            - Turnaround time ~ 6 to 12 months for implementation
            - What can we achieve in that timeframe? Quick and dirty and effective interim solution(s), must not require new hardware to deploy, COTS
            - What can we do here that is **reusable** in the longer-term solution?
            - What is the transition strategy when the long-term solution is available?

        - What are we trying to achieve ultimately (long term)?
            - What can we achieve if we had 2-3 years to implement? Look at technology SWOTs, how does this affect existing hardware AND software
            - ISO vs. US compatibility concerns (global objects, etc.)
    - Review of best practices and literature (White paper)Ken Vaughn to share his work on SWOTs of SNMP v3
        - Short term or long term? Provide justifications for either case.
        - Can work invested in v3 be reusable?
    - Mass DOT talked about RFCs 6353 and 9147
    - Vendors to propose other solutions for consideration beside v3
        - Short term
        - Long term
- Could we come up with a solution for 1202 that is uniform (applicable) across different vendors' platforms to facilitate security, transport and handshaking?
    - If we could pool our resources into solving this problem:
        - Puts burden of development on ONE consultant/vendor instead of X vendors (work for hire, no IP)
        - Frees vendors to work on their products
        - Model after the "NTCIP JC" structure – consultant to work under the guidance of the "JC" consisting of pooled resources
        - Open-source solution, no IP
        - Consistent, predictable outcome

LIFE OF THE TF

Approximately 2-3 months from start to finish, with biweekly meetings (ending 7/30/25)

- 1 meeting for problem statement, goals and objectives, background, context, etc.
- 4-5 meetings for problem resolution
- 1 meeting for wrap-up

TF MEMBERSHIP

Open to all to attend and comment.

- 1 public agency and 1 private company as co-chairs of the TF reporting to the JC
- 1 vote per organization/agency
- Vote and polling are by consensus; unanimity is not required to move forward with problem resolution

Public agency with IT experience participation desired

INTEREST LIST

JOHN THAI (City of Anaheim) jthai@anaheim.net (CO-CHAIR)
TOM STILES (McCain SWARCO) tom.stiles@swarco.com (CO-CHAIR)
James Barnhart (Skyline) JamesBarnhart@SkylineProducts.com
Luke Aldrich (Skyline) LukasAldrich@skylineproducts.com
Michael Mullen (Caltrans) michael.mullen@dot.ca.gov
Michael Robinson (Caltrans) Michael.robinson@dot.ca.gov
Paul Tykodi (Massachusetts DOT) paul.tykodi@dot.state.ma.us
Donald Wang (Western Systems) dwang@westernsystems-inc.com
Craig Hinners (NoTraffic) craig@notraffic.tech
Meadow Cho meadow.cho@saesol.tech
Woody Kim woody.kim@saesol.tech
Mark Simpson (McCain SWARCO) mark.simpson@swarco.com
Marisa Migliore (FHWA) marisa.migliore@dot.gov
Doug Tarico (Econolite) dtarico@econolite.com
Shea Tomsin (Econolite) stomsin@econolite.com
Jeff Fort (Econolite) jfort@econolite.com
Whitney Nottage (QFREE) whitney.nottage@q-free.com
Doug Crawford (QFREE) doug.crawford@q-free.com
Patrick Marnell, (QFREE) patrick.marnell@q-free.com
Matt Luker (UDOT) mluker@utah.gov
Jonathan Grant (Yunex) jonathan.grant@yunextraffic.com
Wolfgang Buckel (Yunex) wolfgang.buckel@yunextraffic.com
Tony Pallissery (Yunex) tony.pallissery@yunextraffic.com
Avery Rhodes - avery@advtraffic.com
Shain Jacob (NETSDOT) Shain.jacob@dot.ny.gov
Matt Barron (Cubic) matt.barron@cubic.com
Shaun Allford (Cubic) shaun.allford@cubic.com
AJ Lahiri (Consystec)
Patrick Chan (Consystec)
Ken Vaughn (Trevilon)
Frank Provenzano - frankprov7@gmail.com
Bob Rausch (Transcore) Robert.rausch@transcore.com
Ralph Boaz (Pillar Consulting)
Ray Deer (Oriux)
Robert White (Nashville DOT)
Wuping Xin

PROPOSED TASK FORCE DELIVERABLES

1. Vision, goals, objectives, statement of the problem and needs

2. SNMP v1 SWOT

3. Needs and requirements of the industry

4. Best practices and literature

5. Findings and recommendations

APPENDIX B

Task Force Votes

First Vote - August 15, 2025

On August 15, after presentation of the alternatives and subsequent discussion, the Task Force voted on which alternative was preferred for further investigation and recommendation. The “SNMPv3 per Recommended Standard” (NTCIP 1202v4) alternative was excluded from the voting to isolate the question of “what people would do different from the currently recommended standard.”

Company	Recommended Alternative			
	SNMPv3 Simple	REST	gRPC w/o gNMI	gRPC with gNMI
ATS	1			
Caltrans	1			
Cisco		1		
Cubic	1			
Econolite	1			
FHWA				
Frank P			1	
John Thai	1			
MnDOT		1		
Nashville DOT		1		
Oriux	1			
Pillar	1			
Q-Free		1		
Skyline Products	1			
SWARCO	1			
Transcore			1	
Trevilon			1	
Western Systems	1			
Yunex	1			
JMC			1	
Totals	**11**	**4**	**4**	**0**

Second Vote - September 12, 2025

The Simplified SNMPv3 approach was discussed in detail over several meetings. The following motion was voted on at the September 12, 2025, Task Force meeting.

In light of the conversations over the past months, I move this taskforce to recommend a rapid pivot towards a "simplified SNMPv3" approach to the 1202 standard. This "simplified SNMPv3" approach represents an efficient & effective way to provide cybersecurity and interoperability for the traffic signal industry.

This committee should now move towards refinement and documentation of the "simplified SNMPv3" approach which includes:

- *Maintaining the recommended 1202v4 MIB (removing references to ISO-26048 objects)*
- *Using the Linted MIB produced by SWARCO and shared in the Task Force Teams channel (ITE Teams)*
- *Not implementing NTCIP 1103 (except for Dynamic objects STMP replacement)*
- *Maintaining the existing 1201 MIBS*
- *Not undertaking further ISO harmonization efforts at this time.*

Added during discussion: For clarity, the taskforce recommends that the "simplified SNMPv3" approach is not an intermediate step to a future full implementation of the NTCIP 1202v4 Recommended Standard but would be a permanent amendment or alternative to the NTCIP 1202v4 RC.

The vote on the above motion was unopposed, and the results of the vote are displayed below.

	Vote Tallys (Yes/No/Abstain)
ATS	Yes
Caltrans	Not present
Cisco	Not present
Cubic	Not present
Econolite	Yes
Frank P	Yes
John Thai	Abstain
MnDOT	Yes
Nashville DOT	Yes
Oriux	Yes
Pillar	Yes
Q-Free	Yes
Skyline Products	Abstain
SWARCO	Yes
Transcore	Yes
Trevilon	Abstain
Western Systems	Yes
Yunex	Yes
JMC	Not present
Utah DOT	Yes
Caliper	Abstain
Mass. DOT	Abstain
Consystec	Abstain