

Pennsylvania
Department of Transportation

On Board Diagnostics Test Procedure

**OBD II Equipment Specification
Requirements Addendum
Equipment and Software**

Version 1.0

July 19, 2018

Revision History

Revision	Date	Description
1.0	07-19-2018	Initial version and release of OBD II Equipment Addendum.

Table of Contents

1.0	Section One – Terms and General Specifications	4
1.1	Acronyms	4
1.2	General Specifications.....	4
1.3	Software Versioning.....	4
2.0	Secure Wireless Network Connection on PAS Unit	5
2.1	Supplied Wireless Routers	5
2.2	Wireless Network Security.....	5
3.0	OBDII Diagnostic Package	6

1.0 Section One – Terms and General Specifications

1.1 Acronyms

Acronym	Definition
OBD	On Board Diagnostics
SSID	Service Set Identifier
WPA2	Wi-Fi Protected Access II

1.2 General Specifications

This addendum to the OBDII Equipment Specification Requirement outlines two optional additions to the stand alone OBD inspection equipment. Participating Equipment Manufacturers may choose to submit one, both, or neither of the additions detailed. The two optional additions are provisions for Equipment Manufacturers to add the capability for a secure wireless network connection on the PAS unit and for the addition of an OBD Diagnostics Package to the PAS unit software. If either or both solutions are offered, the associated PAS units must meet the applicable requirements outlined below and pass Acceptance Testing as determined by PennDOT prior to certification and field release.

The requirements in this addendum do not supersede the requirements in the primary equipment specification document, **Pennsylvania Department of Transportation On Board Diagnostics Test Procedure, Stand Alone Equipment and Software Specifications, Version 3.2, October 13, 2016**, or any subsequent revisions. In the event there is a contradiction between the actual specifications provided by PennDOT and the requirements described in this document, the published specifications shall be considered correct and the addendum in error. If there are requirements in the primary specification that are not specifically covered in this document, the equipment is still expected to meet all requirements in the primary specification.

1.3 Software Versioning

Any changes to an existing approved OBD analyzer hardware/software configuration for either optional addition shall result in a new software version for all active OBD equipment in the Pennsylvania I/M program for the applicable Equipment Manufacturer. The software may include logical switches to control the availability of either or both of the optional additions.

2.0 Secure Wireless Network Connection on PAS Unit

- A. Participating Equipment Manufacturers must provide and properly configure the analyzer and wireless router as a complete package to offer wireless network connection capability.
- B. The PAS units must meet the network and internet connections requirements in the Pennsylvania Department of Transportation On Board Diagnostics Test Procedure Stand Alone Equipment and Software Specifications.

2.1 Supplied Wireless Routers

- A. The supplied routers must have a unique Service Set Identifier (SSID) name. Router SSID cannot remain in the default configuration. The SSID must be hidden and not broadcast.
- B. The supplied routers must have a unique administrator password. Router administrator password cannot remain in the default configuration. The minimum requirements for the WPA2 password are:
 - 1. Minimum length of twelve (12) characters; and
 - 2. Includes three of the following four character sets: lower case letters, upper case letters, numbers, and special characters.
- C. Factory reset must be disabled in the device configuration and by physically blocking access to the switch.
- D. Bridge mode must be disabled in the device configuration and by physically blocking access to the switch.
- E. The supplied routers cannot act as an access point (ad hoc mode).

2.2 Wireless Network Security

- A. Wireless devices must use one of the current Wi-Fi technology standards (802.11g, 802.11i, 802.11n, or 802.11ac).
- B. The wireless equipment must be Wi-Fi Alliance certified.
 - 1. Wireless LAN Technology - ITP-NET001 states: "Equipment is to meet Wi-Fi Alliance certification standards and comply with FCC regulations."
- C. The wireless equipment must use Wi-Fi Protected Access II (WPA2). The minimum requirements for the WPA2 password are:
 - 1. Minimum length of twelve (12) characters; and
 - 2. Includes three of the following four character sets: lower case letters, upper case letters, numbers, and special characters.
- D. All wireless access to the router configuration page must be blocked.
- E. Only an encrypted wired connection can access the router configuration page.
- F. Internet-based access to the router configuration page must be blocked.
- G. Only encrypted access can make changes to the router configuration page (HTTPS).
- H. Unencrypted protocol (HTTP) must be disabled.
- I. Unnecessary services (telnet, SSH, FTP, etc.) must be disabled.
- J. The wireless network security must block all external access to the local network using the built-in firewall.

3.0 OBDII Diagnostic Package

- A. The OBDII Diagnostics option must be offered as part of the PAS Inspection Software. The OBDII Diagnostics cannot be a standalone application.
- B. The PAS software must not call another application or executable to access the OBDII Diagnostics screen(s).
- C. The OBDII Diagnostics software must not access the internet, including Websites or Web Services, at any time.
- D. The OBDII Diagnostics option must only be accessed through the Technician Menu in the PAS software. Technicians cannot access the feature through any other means.
- E. The OBDII Diagnostics option must not include any capabilities or functions that facilitate enabling a vehicle to improperly bypass or circumvent any portion of the emissions inspection process.