Applied Systems Engineering, Inc.
a kalkitech company

1671 Dell Ave, STE 200
Campbell, CA , 95008
Tel: 408-364-0500
Fax: 408-364-0500
www.ase-systems.com

December 8, 2016

CIP-010 R4 Requirements ASE2000 Transient Cyber Asset

What is the Transient Cyber Asset

CIP-010 R4 standards effective in 2017 require protection against *Software Vulnerability Migration* and *Malicious Code Migration* for Transient Cyber Assets. The ASE2000 being used for diagnostic tests is considered a Transient Cyber Asset and ASE has been requested to address the CIP concerns.

The ASE2000 is a software application that runs on a computer in a Windows environment. The ASE2000 cannot be used itself without the computer and Windows. That is, the Transient Cyber Asset is the combined computer with Windows and the ASE2000, not the ASE2000 itself. ASE supplies the ASE2000 software. ASE does not supply the computer or operating system. Those items are provided by ASE's customer and CIP concerns for those components of the integrated diagnostic test equipment cannot be addressed by ASE. ASE can address concerns regarding the ASE2000 application.

Software Vulnerability Mitigation, Section 1.3

The CIP *Software Vulnerability Mitigation* requirement addresses concerns regarding software patches. There are two types of software patches: those to the Windows operating system and those to the ASE2000. Windows is not supplied by ASE. Patches cannot therefore be controlled by ASE. The concern in this area can only be addressed by policies of each organization's IT department. Please note that the ASE2000 is designed to work on the Windows release current as of the time the ASE2000 software is shipped.

Regarding the AE2000, ASE never provides patches to the ASE2000 product. Fully-contained new releases can be downloaded from the ASE web site at the discretion of each customer, as long as the customer's support license is valid. Software downloads do not need to be made directly to the Transient Cyber Asset. They can be downloaded to a separate computer where they may be scanned for virus or other malicious software before being moved to, and installed on, the Transient Cyber Asset.

Introduction of Malicious Code Mitigation, Section 1.4

The CIP *Introduction of Malicious Code Mitigation* requirement can be addressed by application of protective items such as Antivirus software. Antivirus software is a product produced by others that can be installed and operate under Windows on the integrated Transient Cyber Asset that includes the ASE2000. It is not a component of the ASE2000 package supplied by ASE, but rather of the environment that the customer has acquired on which to operate the ASE2000. As such, this protection can be applied to the Transient Cyber Asset by acquisition of commercially available software not part of the ASE offering.