IFMAP for ICS environment – TNC Standard Comments;

GENERAL QUESTIONS

- How does the standard address Industrial Control Networks where a single VLAN spans across multiple sites/locations due to legacy reasons where the BHI is not traversed?
- BHI to BHI encryption is through the use of encrypted link – is this SSL?
- How does BHI to BHI communication between different entities (organization) through MAP be federated – example O&G organization having business partnership with a 3rd party organization?
- How does HIP based traffic be processed through traditional stateful-firewalls that may already exist within IVS environments?
- How can legacy ICS devices support to public IFMAP metadata when these are legacy devices?
- How does the provisioning client know about ICS device identities?
- IF5 or Overlay Communication (say between HMI and PLC) across different sites using backhaul – how this differs from having security gateway with VPN and enforcement through Source IP/Destination IP security policies across the firewalls.

STANDARD SPECIFIC QUESTIONS;

Page 15 BHI functionality embedded in a security gateway device between the backhaul network and the ICS devices on the overlay network. In this situation, the gateway device is often called an "Endbox".

[SS and AI] – Security Gateway will act as an IFMAP client publishing IFMAP metadata to the MAP server. How is the security gateway aware of ICS devices residing behind the gateway?

Page 16 – IF3 Multiple layer-2 (e.g., 802.3) interfaces for control systems data links

[SS and AI] – What defines the IF3 communications and how is this translated into device identifiers…

Page 20 - Self-Provisioning Backhaul Interfaces

[SS and AI] – Currently no commercial IFMAP server exist that can perform previsioning of IFMAP client – how is BHI expected to perform this when MAP server does not have this functionality within the TNC specifications.

Page 23 - The validity of the FCert SHOULD be at least two years from the date of manufacturer.

[SS and AI] – 2 years would seem to be too short

4.1.6 Publishing Discovered ICS Devices

[SS and AI] – The BHI should also send device-identifier or serial number similar to metadata identity (username) to the MAP server – IP addresses can change and are not true reflectors of identifiers.

5.3.3 Securing Backhaul Network

[SS and AI] Why not leverage Group Based VPN (L2 VPLS or L3 MPLS) ?
