

# Anti Virus on Control Systems

# Purpose

- ◆ **IG formed at last years PCSF Meeting**
  - Identified list of CS specific requirements
  - Activity stalled
- ◆ **CS specific A/V may not be feasible**
  - Requirements for using IT version
- ◆ **Interactive dialog**
- ◆ **Consensus of A/V usage and deployment requirements**
  - Usage and guidelines document
  - IT Exception specification
- ◆ **Continue IG**

# Agenda

- ◆ **Role of Anti-Virus Software in IT**
- ◆ **Role of IT with Anti-Virus Software**
- ◆ **Control Systems and malware**
- ◆ **Role of Anti-Virus Software on control systems**
- ◆ **Requirements for Anti-Virus Software on Control Systems**
- ◆ **Discussion**

# Role of Anti-Virus Software in IT

## ◆ Reactive technology

- Protect system from malware injection
- Detect malware

## ◆ Why?

- User access to malware
  - Web site access
  - Email attachments

## ◆ Protect the desktops

## ◆ Server deployment sometimes different

# Role of IT with Anti-Virus Software

- ◆ **Select A/V software vendor**
- ◆ **Qualify A/V software**
- ◆ **Manage A/V software deployment**
- ◆ **Centrally managed**
- ◆ **Repository for alerts**
- ◆ **Response to alerts and outbreaks**

# Control Systems and malware

- ◆ **Now IT connected**

- Should be firewalled from corporate IT network

- ◆ **No email on control systems**

- ◆ **Should not have outside web site access**

- Only access trusted internal web sites

# Anti-Virus Software on control system

- ◆ **Can impact performance**

- Slow display callup

- ◆ **Can impact availability**

- Quarantine critical files

- ◆ **Subject to malware from**

- File copies
- sneaker-net
- Edge servers

# Anti-Virus Software Requirements for CS

- ◆ **Only Anti-Virus**
  - Other malware not needed
- ◆ **On-access scanning should exclude control system directories**
- ◆ **Disable automatic full system scans**
  - Can be done offline
- ◆ **Controlled updates**
  - Even for air-gapped systems
- ◆ **Qualified by CS vendors**
  - What about A/V software not qualified?

# Discussion

- ◆ Any further points?