Cyber Securing Control Systems

August, 2015

Unclassified - Distribution Statement A

DoD Scope of Platform IT & Control Systems

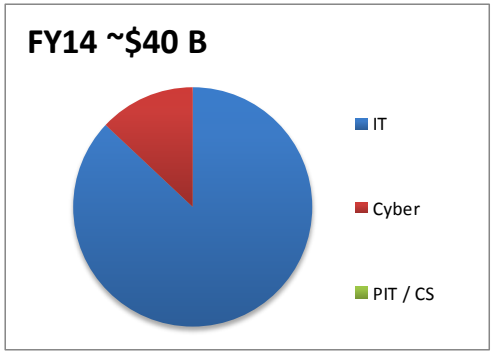
- Acquisitions / Weapon Systems
  - H,M & E (ships / subs, missiles, UVs, etc.)
  - Training Simulators, 3D printing, etc.

- EI&E
  - Buildings & linear structures
  - Airfields, piers, life-safety, AT/FP & physical security, utility/environmental monitoring and control, other infrastructure

- Medical
  - Devices & equipment, pharmacy automation
  - Imaging, CAT, MRI, etc.

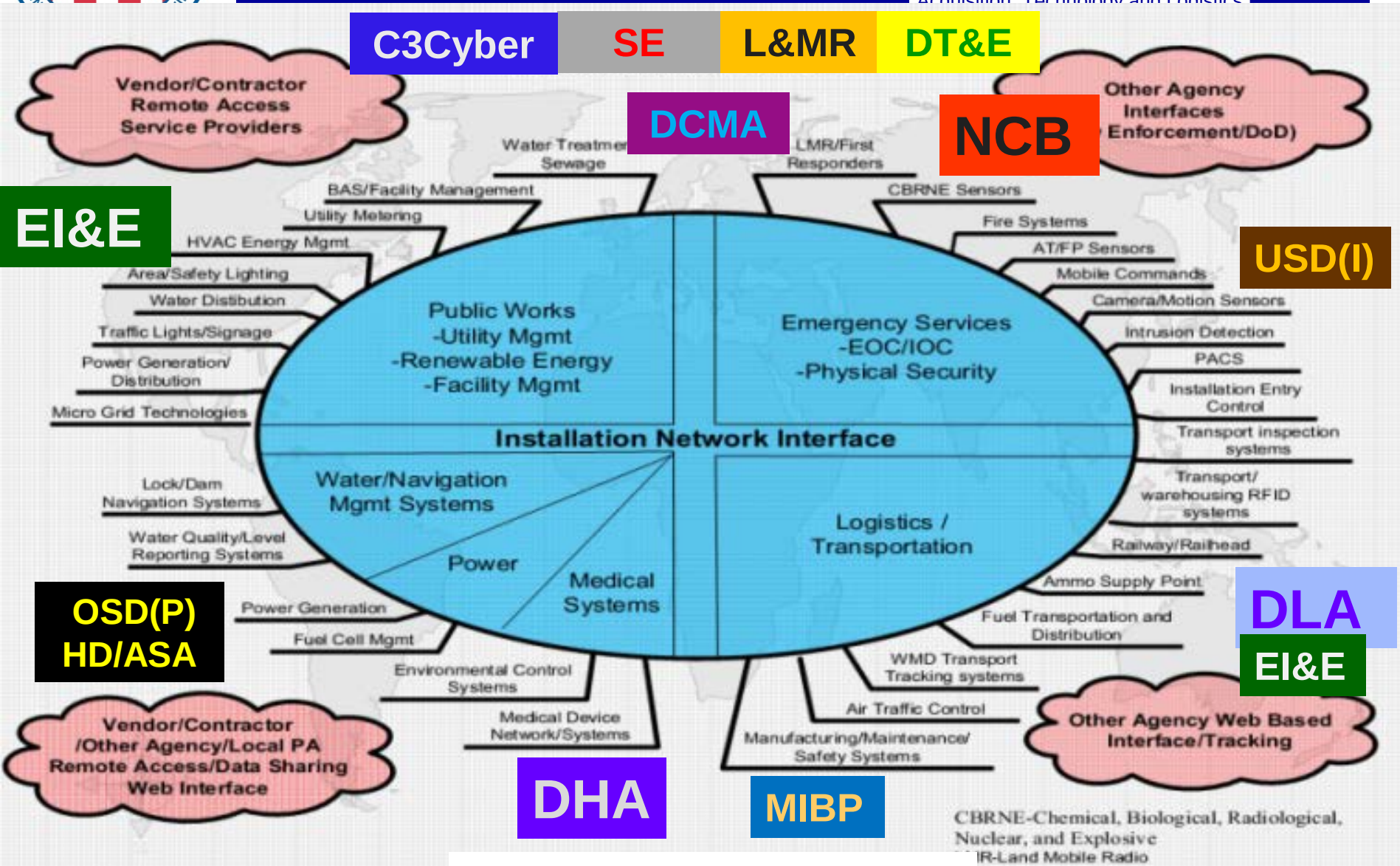
- Logistics
  - POLs, tank farms, pipelines, etc.
  - Warehousing, materials handling
  - Depots, refurbishment, plant mgmt.

- Defense Industrial Base (DIB)



DoD IT & Cyber Strategies and Investments Progressing to Incorporate PIT / CS

Installation Example: CS Stakeholder Complexity



Tactical Power – Networked?

Reduce Fuel Consumption
Increase Portability
Increase Sustainability
Integrate Power w/ Platform
Relevant Renewables
Improve Soldier Power

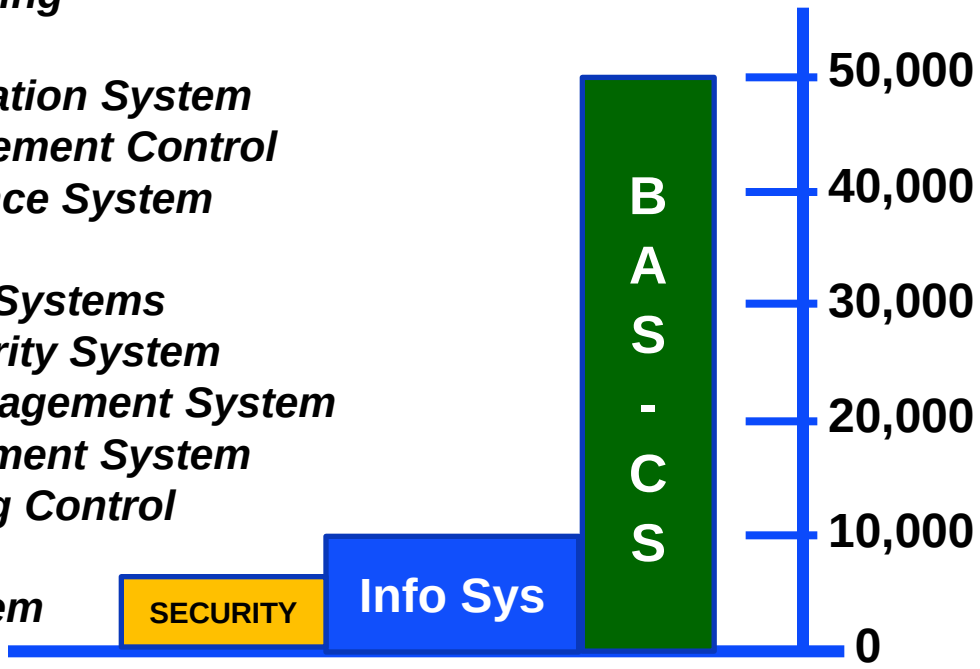
Energy Efficiency Benefit AND or VS. Cybersecurity?

What's in Your Building?

- *"Smart" / High Performance Green Buildings*
  - Since 2005 ~7,000+
  - Example: 5,000 desks, 15 floors, ~2M sqft
    - In-service / occupancy in 2011

- ***Fire Sprinkler System***
- ***Interior Lighting Control***
- ***Intrusion Detection***
- ***Land Mobile Radios***
- ***Renewable Energy Photo Voltaic Systems***
- ***Shade Control System***
- ***Smoke and Purge***
- ***Physical Access Control***
- ***Vertical Transport System (Elevators and Escalators)***

- ***Advanced Metering Infrastructure***
- ***Building Automation System***
- ***Building Management Control***
- ***CCTV Surveillance System***
- ***CO2 Monitoring***
- ***Digital Signage Systems***
- ***Electronic Security System***
- ***Emergency Management System***
- ***Energy Management System***
- ***Exterior Lighting Control Systems***
- ***Fire Alarm System***



3 Networks Independently Managed

Existing Integration Systems

Acuity Brands Roam Advantage Controls ALC Alerton AIE Alerton BACtalk Alerton BCM-WEB American Auto-Matrix Auto Pilot American Auto-Matrix Andover Controls Continuum Asi controls Auto Matrix Sage Automated Logic WebCTRL Automated Logic Barber Coleman Network 8000 Bristol Babcock CAPRON Carrier Carrier Comfort Network Carrier Com-Trol Control Microsystems SCADAPack Cylon Unitron UC32 Daikin Data Aire Dell Vostro Delta Controls ORCA Distech Echelon i.Lon Emerson-Liebert EXHAUSTO Flygt ITT Industries APP 700 General Electric WESDAC General Electric Honeywell Excel 5000 Honeywell WEBs-AX HSQ Technology Invensys I/A Series Invensys Micronet Invensys Network 8000 Johnson Controls Facility Explorer Johnson Controls Metasys Johnson Controls M-Series KMC LANDIS Landis & Staefa Integral MS2000 Landis & Staefa Liebert SiteGate LOYTEC Electronics L-VIS Lynxspring JENEsys Merlin Gerin PowerLogic Microwave Data Systems Mitsubishi Motorola SCADA Systems Odessa Engineering OmniaPRO Orion Controls Paragon EC7000 Series Raco Reliable Controls MACH-ProWebSys Richards-Zeta Robert Shaw DMS RUGID Schneider Electric I/A Series Schneider Electric PowerLogic Siebe Network 8000 Siemens ACCESS Siemens Apogee Siemens Desigo PX Siemens Synco 700 Staefa Staefa/Siemens STULZ Air Technologies TAC I/A Series TAC Network 8000 TAC Xenta TAC Vista Telvent Smart Grid Solution Trane Tracer Trane Tracer Summit Trane Varitrac TREND Trend Control Systems IQ2 Tridium Vykon

Existing ICS Operating Software

Acquisition, Technology and Logistics

Desigo Insight KNX STANDARD ABB Symphony Plus OptimaxRev 4 ABB Symphony Plus 800xA SV 5.1 ABB Symphony Plus Composer 6.0 ABB Symphony Plus S+ Operations 1.1 Alerton BACTalk Envision 2.0 Alerton BACTalk Envision 2.6 Alerton VisualLogic Allen-Bradley RSLogix 500 Allen-Bradley RSLogix 500, RSView32 Automated Logic ExecB 6.0 Automated Logic SuperVision WebCTRL 5.5 Automated Logic WebCTRL WebCTRL 3 Automated Logic WebCTRL WebCTRL 3.0 Automated Logic WebCTRL WebCTRL 5 Automated Logic WebCTRL WebCTRL 5.2 Automated Logic WebCTRL WebCTRL 4.1 SP1 Automated Logic WebCTRL WebCTRL Automated Logic ExecB 4.1 SP1 Automated Logic ExecB drv_lge_4-02-175 Automated Logic ExecB drv_melgr_vanilla_4-02-175 Automated Logic ExecB Automated Logic Supervision 2.6b Automated Logic WebCTRL 4 SP1B Automated Logic WebCTRL 4.1 SP1 Automated Logic WebCTRL 4.1 SP1b Automated Logic WebCTRL SVR 5.5 Calsense Command Center 4.15.11.20 Carrier Comfort Network Comfort Network 3.0 Control Microsystems ClearSCADA 2009 Ed. R2.2 Data flow Systems HyperTAC 2 Data flow Systems HyperTAC HT3 Delta Controls ORCA ORCAview 3.30 Delta Controls ORCA ORCAview 3.40 Delta Controls Orcaview 3.22 Delta Controls Orcaview 3.30 Delta Controls OrcaView 3.3 Delta Controls Orcaview 3.33 Delta Controls Orcaview Delta Controls, TAC ORCA, I/NET ORCAview, Seven Rel 2.15 EFACAC Prism ERI Siemens Insight 3.6 GE, Intellution Proficy, iFIX, FIX Desktop _, _,4.0, _ General Electric Cimplicity Plant Edition 6.1 General Electric Multilin Config Pro 5.03 General Electric Proficy Cimplicity 7.0 General Electric Proficy iFIX 4.0 Honeywell Symmetre Station 3.5 Symmetre 3.5 Honeywell Webstation-AX Niagara Niagara 3.5.40.1 HSQ Miser 6.06 HSQ Miser HSQ, Sun Microsystems Miser, Xview 6.06 Iconics Genesis32 Genesis32 8.3 Iconics Genesis32 Genesis32 9.13 Iconics HMI SCADA Solutions Genesis 32 3.12.005 InduSoft Web Studio Intellution 7 Intellution FIX32 3.5 Intellution FIX32 Intellution iFIX 3.5 Intellution IFIX Intellution iFIX Reporter ITT Flygt AquaView AquaView 1.50 Johnson Controls Metasys 6.0.0.9000 Johnson Controls Metasys GX9100 7.05A Johnson Controls Metasys Metasys 5 Johnson Controls Metasys Metasys 5.1 Johnson Controls Metasys Project Builder 5:1 Johnson Controls Metasys Project Builder 3 Johnson Controls Metasys 5 Johnson Controls Metasys 12.04 Johnson Controls Metasys 2.0.0.70.0 Johnson Controls Metasys 5.2.0.5400 Johnson Controls Metasys Johnson Controls M-Graphics 5.3 Microsoft Explorer N/A N/A N/A N/A Pneu-Logic Pneu-Logic RACO RACO 3.14 Rainbird MAXICOM2 Central Control 4.3 ReLab Software ClearView-SCADA 7.2.8 Reliable Controls MACH ProWebSys RC-Studio 2.0 Robert Shaw Digital Management System Operator Interface 11.0 Rockwell FactoryTalk Service Platform 2.30 Rockwell FactoryTalk View, Rsview Site Editiion, Supervisory 6.0, 6.0 Rockwell Factory Talk 6.0 Rockwell Automation FactoryTalk View Machine Edition 5.1 Rockwell Automation FactoryTalk View Site Edition 4.0 Rockwell Automation FactoryTalk View Site Edition 5.1 Rockwell Automation FactoryTalk View Site Edition Rockwell Automation RSView Supervisory Edition 4.0 Rockwell Automation RSView Supervisory Edition Rockwell Automation RSView32 7.600.00 ScadaTEC SCADASIS 5.8.14.213 Schneider Electric PowerLogic ION Enterprise 5.6 Schneider Electric PowerLogic ION Enterprise Siebe Network 8000 Signal 4.4.1 Siemens S7 300 STEP 7 Siemens Apogee Insight Siemens Desigo Insight Siemens Insight Desigo Insight 2.31 Siemens Insight Desigo Insight 2.35.021 Siemens WinPM.Net 3.2 SP3 SUBNET Solutions SubSTATION Explorer 1.3.0 SUBNET Solutions SubSTATION Explorer 1.5.7 Sun Microsystems Xview 3.2 Symantec Backup Exec 2011? TAC 1/A Series WorkPlace Tech 5.7 TAC I/A Series Workbench TAC I/A Series WorkPlace Tech 5.7.2 TAC 4.1 TAC Signal, XPSI & ZPSIPC Teletrol eBuilding Telvent OaSys DNA 7.4.* Trane Tracer SC Tracer 3.5 Trane Tracer Summit Tracer 11 Trane Tracer Summit Tracer 16 Trane Tracer Summit Tracer 17 Trane Tracer Summit V14 Tracer 14 Trane Tracer Summit V16 Tracer 16 Trane Tracer Summit V17 Tracer 17 Tridium Vykon Niagara 2.301.428 Tridium Vykon Niagara 2.301.430.v1 Tridium Vykon Niagara 2.301.431.v1 Tridium Vykon Niagara 2.301.514 Tridium Vykon Niagara 2.301.514.v1 Tridium Vykon Niagara 2.301.522 Tridium Vykon Niagara 2.301.522.v1 Tridium Vykon Niagara 2.301.522.v2 Tridium Vykon Niagara 2.301.522V1 Tridium Vykon Niagara 2.301.527.v1 Tridium Vykon Niagara 2.301.529 Tridium Vykon Niagara 2.301.532 Tridium Vykon Niagara 2.301.532.v1 Tridium Vykon Niagara 3.3.31 Tridium Vykon Niagara 3.5.34 Tridium Vykon Niagara Workbench 3.6.31 Tridium Vykon Niagara Tridium Vykon Niagara AX 3.3.22.0 Tridium Vykon Niagara AX 3.5.25.0 "Tridium Vykon Niagara AX 3.5.25.0 3.3.22.0" "Tridium Vykon Niagara AX 3.5.25.0 3.4.51.0" Tridium Vykon Niagara AX 3.5.25.1 Tridium Vykon Niagara AX 3.5.34.0 Tridium Vykon Niagara AX 3.5.34.2 Tridium Vykon Niagara AX 3.5.39.0 Tridium Vykon Niagara AX 3.5.40.7 Tridium Vykon Niagara AX 3.5.7.0 Tridium Vykon Niagara AX 3.6.31.0 Tridium Vykon Niagara AX 3.6.31.4 Tridium Vykon Niagara AX 3.6.47 Tridium Vykon Niagara AX 3.6.47.0 Tridium Vykon Niagara AX Tridium Vykon Niagara R2 2.301.522 Tridium Vykon Niagara R2 2.301.522.v1 Tridium Vykon Niagara R2 2.301.529.v1 Tridium Vykon Niagara R2 2.301.532.v1 Tridium Vykon Niagara R2 R2.301.529 Tridium Vykon Niagara R2 Tridium Vykon Niagra 3.5.34.7 Tridium Vykon Workplace Pro 2.301.428 Tridium Vykon Workplace Pro 2.301.514 Tridium Vykon WorkPlace Pro 2.301.522 v2 Tridium Vykon Workplace Pro 2.301.532 Wonderware Intouch WindowViewer 10.1.200 Yokogawa Exaquantum EXAOPC R3.21 Yokogawa Exaquantum Exaquantum Server R2.60 Yokogawa DAQOPC for DARWIN R3.01 2 6.0 ACS Alerton 3.5.34 Alerton Apogee 2.8 BACnet CSIView 11.5.0 build 121 DAQ Works V1.03 Delta-V 7.4 Delta-V DOS 6.2 ERI Excel add -in I/Net 1.02 I/Net 5.1.3-57 I/Net 5.1.4-59 I/Net INET 2000 1.11 build 170 Insight Metasys Power Xpert Software PR970 Prism Protech Siemens 11 SteamEye Symmetre Station 3.5 Tracer Summit 15.0 Versaterm, Crystal Reports VMware WEStation WIN UPM2 Workbench 2.301.522 Workbench 2.310.514

Existing Device Level Controllers

Acquisition, Technology and Logistics

AAEON Electronics AAON SS1016 ABB ACH550-UH-045A-4 ABB ACH550-UH-04A1-4 ABB ACH550-UH-246A-4 Acuity Brands Roam Gateway ADDER ADDERLink INFINITY ALIF 1000R-US ADDER ADDERLink INFINITY ALIF 1000T-US Advantech Touch Panel Computer TCP-1770H-C2BE Advantech Touch Panel Computer TPC-1780H Advantech Touch Panel Computer TPC-650H AEG BLR-CX 04R AEG Schneider Automation Modicon Micro 612 Alerton VLC-1188 Alerton VLC-444 Alerton VLC-550 Alerton VLC-853 Alerton BACtalk BCM-PWS Alerton BACtalk VAV-SD Alerton BACtalk VLC-1180 Alerton BACtalk VLC-1188 Alerton BACtalk VLC-444 Alerton BACtalk VLC-550 Alerton BACtalk VLC-651R Alerton BACtalk VLC-660R Alerton BACtalk VLC-853 Allen-Bradley Allen-Bradley CompactLogix L23E Allen-Bradley CompactLogix L32E Allen-Bradley ControlLogix 1756-A10 Allen-Bradley ControlLogix 1756-L61 Allen-Bradley ControlLogix OEM Allen-Bradley FlexLogix 1794-L34 Allen-Bradley FlexLogix 5433 Allen-Bradley FlexLogix FLEX I/O Allen-Bradley Integrated Display Computers 6181P Allen-Bradley MicroLogix 1000 1761 Allen-Bradley MicroLogix 1000 1761-L16BWB Allen-Bradley MicroLogix 1100 1763 Allen-Bradley MicroLogix 1100 1763-L16AWA Allen-Bradley MicroLogix 1100 1763-L16BWA Allen-Bradley MicroLogix 1400 Allen-Bradley Micrologix 1400 1766-L32AWAA 8/10.00 Allen-Bradley MicroLogix 1500 1764-24AWA Allen-Bradley MicroLogix 1761-NET-ENI Allen-Bradley PanelView Plus 1000 Allen-Bradley PanelView Plus 2711P-KM420D Allen-Bradley PanelView Plus 600 Allen-Bradley PanelView Plus 700 Allen-Bradley PowerMonitor 3000 Allen-Bradley PowerMonitor 3000 1404-DM A Allen-Bradley PowerMonitor 3000 1404-M405A-ENT B Allen-Bradley SLC 500 DH-485 Allen-Bradley SLC 500 SLC 5/00 Allen-Bradley SLC 500 SLC 5/02 Allen-Bradley SLC 500 SLC 5/03 Allen-Bradley SLC 500 SLC 5/04 Allen-Bradley SLC 500 SLC 5/05 Allen-Bradley VersaView 1500P Andover Controls Continuum Infinet II i2810 Andover Controls Infinity SCX 920 APC AP7960 APC PNET 1 APC Back-UPS BE350R APC Back-UPS BE750G APC Back-UPS BX900R APC Back-UPS ES550 APC Back-UPS Pro 1000 APC Back-UPS RS800 APC Back-UPS XS1500 APC Smart-UPS 1000XL APC Smart-UPS 2200 APC Smart-UPS 2200XL APC Smart-UPS 750 APC Smart-UPS AP5719 APC Smart-UPS SMT3000RM2U APC Smart-UPS SU2200NET APC Smart-UPS SU220RMXL APC Smart-UPS SU3000RMXL APC Smart-UPS SU3000XLM APC Smart-UPS SUA1000RM1U APC Smart-UPS SUA1500 APC Symettra APC Symmetra AP9617 / Symmetra 40K Arena EX III Arista ARP-2217AP Armstrong SteamEye Gateway 3000M Autoflame DTI MK6DTI Automated Logic LGR1000 Automated Logic LGR25 Automated Logic M line M0100 Automated Logic M line M220nx Automated Logic M line M4106 Automated Logic M line M8102 Automated Logic M line M8102nx Automated Logic M line Mcpu Automated Logic ME812u line ME812u Automated Logic S line S6104 Automated Logic U line UNI/32 AutomationDirect DL06 AutomationDirect DL205 AutomationDirect EA7-T10C AutomationDirect EA-T10C AutomationDirect C-More EA7-T6CL AVG EZ-T10C-F AVG EZ-T15C-FSU Axiomtek DIN-rail Embedded System rBOX201-4COM-FL Axis 214 PTZ Axis 2400PTZ Axis 241Q Axis P5512 B&B Electronics MES1B Badger Meter Disc Series 120 Badger Meter Disc Series 170 Badger Meter Disc Series 35 Badger Meter Disc Series 70 Badger Meter M Series 4000 Badger Meter Turbo Series 2000 Badger Meter Turbo Series 450 Barber Coleman Network 8000 MZ2A Basler Electric BE1-25 Basler Electric BE1-700V Basler Electric BE1-CDS220 Basler Electric BE1-GPS100 E3N2R0U Bay Controls BayNet Belkin F6C1100-AVR Belkin F6C750-AVR Bitronics PowerPlex MTWIN3 Black Box ME838A-R2 Black Box ME838A-R3 BOCA Bristol Babcock DPC 3335 Brother HL-2270DW Brother HL-4040CDN Brother HLYOC Buffalo TS-H0.0TGL\RG Buffalo TeraStation Pro TS-H03TGL-R5 CalAmp VIPER SC Campbell Scientific CR1000 Carel pCO3 Carrier 30RRB06052_00__3 Carrier 30XAB50062-03X93 Carrier Comfort Network Comfort Controller 6400 Cohen OEM Computrol 32X Control Microsystems 5000 Series 5302 Control Microsystems SCADAPack 100 Control Microsystems SCADAPack 334 Cooper Power Systems CL-6A Cooper Power Systems CL-6A WA366B67G6AR Cooper Power Systems CL-6A WE383F44K6XR CyberPower 1500ADR CyberPower CPS1500AVR Cylon Unitron UC32 Daikin McQuay MicroTech II WMC Danfoss OEM Danfoss BACLink VLT DEC LA400-A2 Dell 3000CN Dell 71PXP Dell UPS1000W Dell Color Laser Printer 1320C Dell Laser Printer 1110 Dell Laser Printer 2330dn Dell Laser Printer 3100CN Dell PowerValut MD3000i Dell PowerValut TL2000 Delta Controls ORCA DSC-1212E Delta Controls ORCA DSC-1616E Delta Controls ORCA DSC-633E Deltak OEM Digi AccelePort C/X (1P) 50000598-01 Digital Loggers Web Power Switch III Dolch ORCA-19 Dolch ORCA-19PM DROBO 902-00001-001 Eason Technology 950 Eaton RO LIC-100 HMI Eaton Power Xpert PX4000 Eaton Powerware 3105 Eaton Powerware 5125 Eaton Powerware 9125 Eaton Powerware FE2.1KVA Eaton Powerware PW9130L1500T-XL Electro Industries Nexus 1262 Electro Industries Nexus 1270-S-SWB2-20-60-4IPO-SE Electro Industries Nexus 1272 Electro Industries Shark 100S elo Touch Solutions Touch systems Elo Touch Solutions Touchmonitor ET1739L Elo TouchSystems Elster American Meter 3.5M Elster American Meter AL-425 Elster American Meter AL-800 Elster American Meter GT-3 Elster American Meter RPM Series 1.5M Elster American Meter RPM Series 2M Elster American Meter RPM Series 3.5M EMC CLARiiON CX4-120 Emerson M-Series MD Plus Encorp KWS GDU Encorp KWS2222501 Encorp UPC GDU Endress+Hausser Promass 80 Endress+Hausser Prowirl 72W EPSON FX 2190 Fireye Nexus NX6100 Flygt ITT Industries APP 700 APP700F Fuji HDC 500 Fuji Micrex-F F120S F120S Fuji Micrex-SX SPH3000MM Gamewell 1033502501VD General Electric 16SB1BB339SSS2V General Electric 16SB1CB201SDM2Y General Electric 510-0183-01A General Electric 526-2006 General Electric IC695ETM001 General Electric Fanuc 90-30 IC693CPU311 General Electric Fanuc 90-30 IC693CPU311-AD General Electric Fanuc 90-30 IC693CPU311-AE General Electric Fanuc 90-30 IC693CPU311-BE General Electric Fanuc 90-30 IC693CPU311N General Electric Fanuc 90-30 IC693CPU311T General Electric Fanuc 90-30 IC693CPU311W General Electric Fanuc 90-30 IC693CPU311-XX General Electric Fanuc 90-30 IC693CPU311Y General Electric Fanuc 90-30 IC693CPU350 General Electric Fanuc 90-30 IC693CPU352 General Electric Fanuc 90-30 IC693CPU360 General Electric Fanuc 90-30 IC693CPU363 General Electric Multilin 469 General Electric Multilin 750P5G5S5HIA20R General Electric Multilin SR489-P5-HI-A20 General Electric Multilin SR74555HI485 General Electric PACSystems RX3i General Electric PQMII PQMII General Electric RRTD RRTD General Electric Rx3i PacSystem IC694MDL240 General Electric Rx3i PacSystem IC694MDL940 General Electric Rx3i PacSystem IC695ALG112 General Electric Smart Meter kV2c General Electric SR 745 General Electric SR 750 General Electric Versamax IC200CPUE05 Genicom 3850 Hach SC100 Hadax Series 6000 Heliodyne Delta-T Pro Honeywell HC900 Honeywell XL50-MMI Honeywell Excel 5000 Q7055A BNA- Honeywell Excel 5000 Q7750A-2003 Honeywell Excel 5000 XC5010 Honeywell Excel 5000 XCL5010 Honeywell Excel 5000 XL100 Honeywell Excel 5000 XL100C Honeywell Excel 5000 XL20 Honeywell Excel 5000 XL50 Honeywell Excel 5000 XL5010 Honeywell Excel 5000 XL5010C Honeywell Excel 5000 XL50-MMI Honeywell Excel 5000 XL80 Honeywell Excel 5000 XLC50 Honeywell Excel 5000 XLC5010 Honeywell Excel 5000 XLC50-MMI Honeywell Excel 5000 XLC8010 Honeywell Excel 5000 XLC8010A HP 700/43 HP 8100 ELITE HP Color LaserJet 4500 HP Color LaserJet CP2025 HP Deskjet 6122 HP InkJet BC354A HP Jetdirect 170x J3258B HP LaserJet HP LaserJet 02461A HP LaserJet 4 HP LaserJet 4600n HP LaserJet 4MV HP LaserJet 5 C3916A HP LaserJet 5200tn HP LaserJet C3980A HP LaserJet CB94A HP LaserJet CP2025 HP LaserJet CP2025DN HP LaserJet CP5225DN HP LaserJet P1102W HP LaserJet P2015 HP LaserJet P4014dn HP OfficeJet 7000 E809a HP Officejet CM755A/8500A HP StorageWorks Tape Array 5300 HSQ Technology HSQ Technology 22501 HSQ Technology 86004862 HSQ Technology 8600-4862 HSQ Technology 8600-6135L HSQ Technology 8602 HSQ Technology 8602-080 HSQ Technology 8602-080A Rev E HSQ Technology 8602-RTU-080-A Rev E HSQ Technology HSQ9588T HSQ Technology V86VR-R030 iEi Technology AFOLUX LX AFL-12A Infinias Intelli-M eIDC Invensys Invensys I/A Series FCM 10E Invensys I/A Series UNC-520-2 ITRON IX100X Johnson Controls Johnson Controls Facility Explorer FX-PCG2611 Johnson Controls M Series MS-N30 Supervisory Controller Kiltech Embedded Field Controllers SX-CPU/RS-485 190715 Koyo DL205 Koyo DL206 Koyo DL207 Koyo DL250 CPU Landis & Staefa Integral MS2000 NRK16-NICO Landis & Staefa Integral RSA NRK16/A Lantronix Lantronix Universal Device Server UDS100 Lexmark Optra E312L LG V-NET PQNFB17B0 Liebert StieLink 12 Liebert StieLink 4 LOYTEC Electronics LINX LINX-101 LOYTEC Electronics L-VIS LVIS-3E100 LOYTEC Electronics L-VIS ME215 Maple Systems OIT3175 Maple Systems OIT3250-B00 Maple Systems PC217B Mcquay H62PY McQuay Maverick I OM 1077 MCS MCS-R010 MechoShade Systems SunDialer I-Con Meidensha ADC5000 Meidensha T01E-E01A Meidensha T01E-E01A-A Meidensha Uniseque RC500 MGE UPS SYS UPS 1500 MGE UPS SYS UPS 800 Mitsubishi Mitsubishi AG-150A Mitsubishi MP-22-AF Mitsubishi MP-22-AR Mitsubishi MP-22-CB Mitsubishi CITY MULTI BAC-HD150 Mitsubishi CITY MULTI GB-50ADA Mitsubishi MELSEC Q63P Mitsubishi Q Series FX2N Modicon Micro Modicon Momentum 170ADM39030 Modicon Quantum Automation Series 140CPU113 MODICON TSX Quantum Modicon TSX Series TSX3705028 Modicon TSX TSX3705028 Motion Control Engineering Motion Control Engineering 24-10-0012 Motorola MOSCAD-L Motorola SCADA Systems ACE3600 Moxa MGate IMC-101-M-SC Nalco Switch 2226 3D Trasar NETGEAR ReadyNAS 3200 NETGEAR ReadyNAS Pro NOVAR NL INC B541200039 NovaTech Orion5r Obvius Holdings AcquiSuite A8812 Odessa Engineering DiaLog Plug Okidata MicroLine 321 Turbo Okidata MICROLINE ML420 OMNTEC OEL8000II OEL8000IIP Opto 22 Opto Brian Panasonic BB-HCM531 Panasonic GN 15 Panasonic i-Pro WV-NP244 Panasonic i-Pro WV-NS202A Panasonic i-Pro WV-NW964 Patton Copper Link 2156 Perle IOLAN SCS PML ION7350 PML PowerLogic ION7300 PML PowerLogic ION7330 PML PowerLogic ION7350 PML PowerLogic ION7500 PML PowerLogic ION7550 PML PowerLogic ION7600 PML PowerLogic ION7650 PML PowerLogic ION7700 PML PowerLogic ION8600 Pneu-Logic 10A22646 Pneu-Logic PL4000 DCM Powerlynx OEM Preferred Instruments PCC-III Preferred Instruments PCC-III-0000 Preferred Instruments PCC-III-F000 Preferred Instruments PCC-III-FZ00 Pro-Face GP577R-TC11-OY ProSoft MVI46-MNET Qualitrol ITM 509 ITM RACO VERBATIM DFP RACO VERBATIM SFP Raritan CompuSwitch CS4R Raritan Dominion KX II 216 Raritan Dominion KX II DKX2-216 Raritan Dominion KX II DKX2-432 Red Lion G308 Red Lion G310C Ricoh Aficio MP C2050 RUGID RUG6D RUGID RUG7D RUGID RUG9 RUGID RUG9B RUGID RUG9D Sanyo Denki SANUPS A11H Schneider Electric 170INT11000 Schneider Electric 171CCS76000 Schneider Electric HMIPSCIDE03 Schneider Electric Modicon M340 Schneider Electric I/A Series MNB-1000 Schneider Electric Magelis XBT GT 2330 Schneider Electric Momentum Processor 171CCC96020 Schneider Electric Momentum Processor 171CCS78000 Schneider Electric Powerlogic CM2000 Schneider Electric Powerlogic CM3000 Schneider Electric Powerlogic CM4000 Schneider Electric Powerlogic ECC Schneider Electric Powerlogic EGX 100 Schneider Electric Powerlogic EGX 200 Schneider Electric Powerlogic EGX 400 Schneider Electric Powerlogic enercept Meter Schneider Electric Powerlogic Energy Meter Schneider Electric PowerLogic ION7330 Schneider Electric PowerLogic ION7350 Schneider Electric PowerLogic ION7500 Schneider Electric PowerLogic ION7600 Schneider Electric PowerLogic ION7650 Schneider Electric PowerLogic ION8300 Schneider Electric PowerLogic PM710 Schneider Electric PowerLogic PM850 Schneider Electric Powerlogic Power Meter Schneider Electric TSX Momentum Schneider Electric TSX Momentum 171CCC9803 Schneider Electric TSX Quantum 170-ENT-110-00 Schneider Electric Xenta 280 282 Schneider Electric Xenta 300 301 Schweitzer Engineering Laboratories SEL-2020 Schweitzer Engineering Laboratories SEL-2032 Schweitzer Engineering Laboratories SEL-2407 Schweitzer Engineering Laboratories SEL-2411 Schweitzer Engineering Laboratories SEL-2440 Schweitzer Engineering Laboratories SEL-3332 Schweitzer Engineering Laboratories SEL-351S-7 Schweitzer Engineering Laboratories SEL-3530 Schweitzer Engineering Laboratories SEL-451 Schweitzer Engineering Laboratories SEL-487E Schweitzer Engineering Laboratories SEL-587Z Schweitzer Engineering Laboratories SEL-700G Schweitzer Engineering Laboratories SEL-751A Schweitzer Engineering Laboratories smart-UPS SEL-3332 Seiko TS-2540 Siebe Siebe CP-8161-333-3 Siebe DMS-3501 Siebe MSC-P1502 Siebe MSC-P1504-D Siemens MP277 10 TOUCH Siemens PXC36 Siemens ACCESS 9510 Siemens Apogee Series 200 MEC Siemens Apogee 545-793 Siemens Apogee AEM200 Siemens Apogee Power MEC Siemens Apogee Power MEC 1200 Siemens Apogee Power MEC 1210 Siemens Apogee Power Mec 1210E Siemens Apogee Power MEC 40 Siemens Apogee Power MEC 40 System 600 Siemens Apogee Power Mec Series 200 Siemens Apogee Power Mec System 600 Siemens Apogee PXC100 Siemens Apogee PXC24 Siemens Desigo PX PXC36 Siemens Desigo PX PXC52 Siemens Desigo RCX PXR11 Siemens Desigo RCX PXR12 Siemens HydroRanger 200 7ML50342AA01 Siemens SIMATIC S7-1200 Silex SX-3000GB Solar OEM STULZ Air Technologies Fieldserver DCC828 Symmetricom bc635PCI Symmetricom TrueTime 820-202 Symmetricom TrueTime XL-DC TAC Xenta 302/N/P Teletrol eBuilding Concentrator Telvent Smart Grid Solution SAGE 2300 Telvent Smart Grid Solution SAGE 2400 Terminator T1H-EBC100 Terminator T1H-EBC101 Toshiba OIS-DS52 Total Control Products QuickPanel Trane EMTF000AAC02100 Trane OEM Trane TNS1 Trane UC800 Trane Tracer CH530 Trane Tracer EX2 Trane Tracer MP503 Trane Tracer MP580/581 Trane Tracer MP581 Trane Tracer SC Trane Tracer Summit BCU Transformative Wave Technologies eIQ nSITE 600 Trend Control Systems IQ250 Trend Control Systems NXNI Trend Control Systems XCITE Trend Control Systems IQ2 IQ204 Trend Control Systems IQ21x IQ210 Trend Control Systems IQ21x IQ233 Trend Control Systems IQ21x IQL-SDK Trend Control Systems IQ22x IQ220 Trend Control Systems IQ24X IQ241 Trend Control Systems IQ25X IQ250 Trend Control Systems IQ25X IQ251 Trend Control Systems IQ3s EINC Tridium JACE-403 Trijay Triplite AVR900U USRobotics Uticor 100G-PL08S2R0 Viconics VT7600 WAGO 750-841 Walchem WMT8130-2LNNN Westinghouse WEStation Woodward 505 9907-163 Woodward LinkNet 9905-966 Woodward LinkNet 9905-970 Woodward LinkNet 9905-971 Yokogawa AIP578 Yokogawa AIP578 Style S1 Yokogawa CP40110-S Yokogawa CP703 Yokogawa DA100-11-1M Yokogawa DA100-22-1M Yokogawa DC100-21-11-1M Yokogawa DC100-21-21-1M Yokogawa DC100-21-31-1M Yokogawa DS400-00-1M Yokogawa DS600-00-1M Yokogawa FA-M3 Yokogawa PFCD-H2612 Yokogawa PFCS Yokogawa TOP77RT Yokogawa STARDOM NFJT100

Difference Between DoD & Commercial Products = None!

US Chamber of Commerce – Dec 2011

CIO / IA Techs

- **Not mine**
- **Not funded**
- **Not trained**

Facility Mgr / Eng

- **Not Mine**
- **Not funded**
- **Not trained**

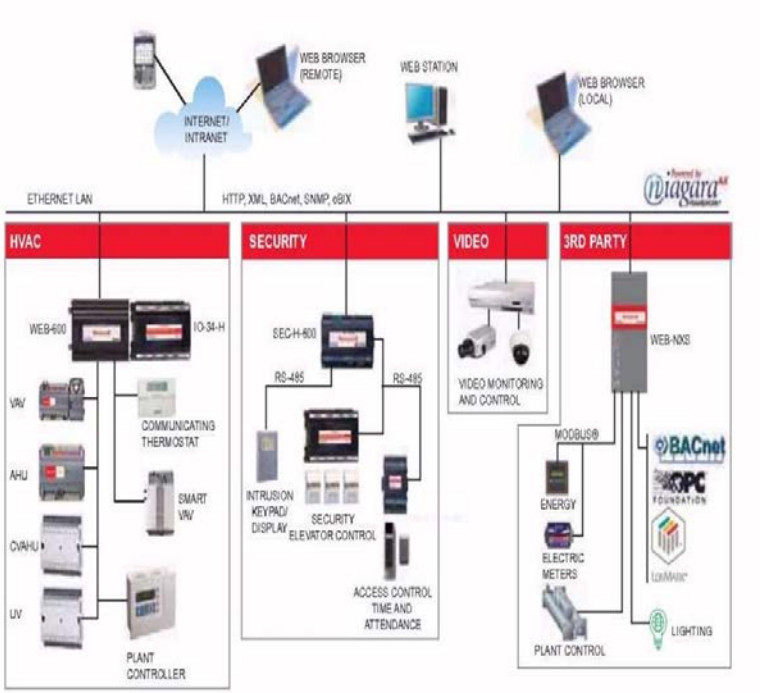
Which Group Best to Cyber Protect Control Systems?

Shodan Internet Connection Exploit

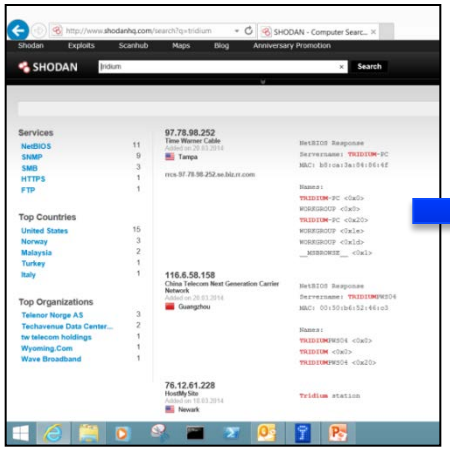
Acquisition, Technology and Logistics

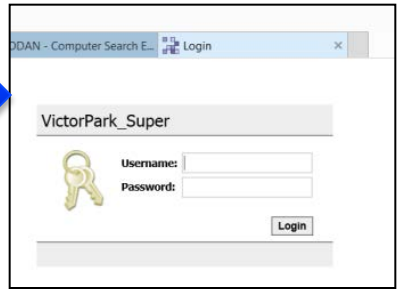
ICSA-12-228-01A: Tridium Niagara Vulnerabilities (Updat
ICSA-15-029-01 : Honeywell HART DTM Vulnerability
ICSA-15-076-02 : Honeywell XL Web Controller Directory Traversal Vulnerability
ICSA-13-189-01 : QNX Multiple Vulnerabilities

Direct Internet connected HMI http, not https



Shodan – Tridium Search





HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5", nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32 Baja-Station-Brand: distech
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC

Never Attribute Evil When Stupid is Still Available

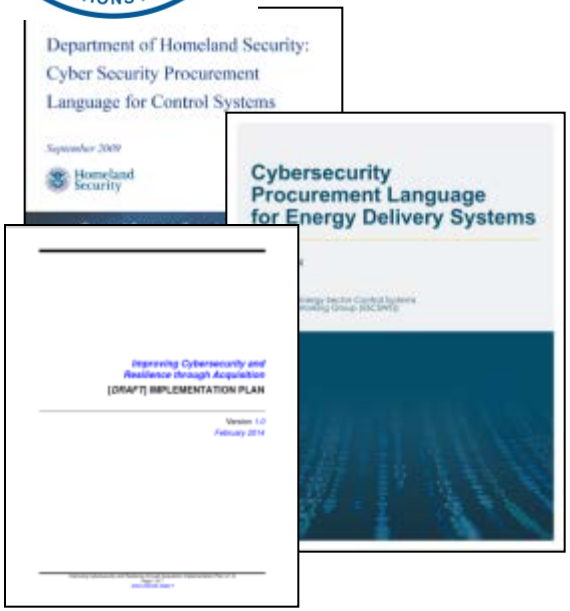
PIT / CS in DoD Policy & NIST Guide

- DoDI 8500.01 ***Cybersecurity*** ***(14Mar14)***
  - **Defines Platform Information Technology (PIT) [ICS]**
  - **Directs identify and centrally register at Component level**
  - **Directs use of NIST standards**

- DoDI 8510.01 ***Risk Management Framework (RMF)*** for DoD Information Technology ***(12Mar14)***
  - **DIACAP replaced by RMF *[goal: reduce C&A time 50%]***
  - **Manages life-cycle cybersecurity risk; promotes reciprocity**
- Under SECDEF for Installations & Environment (OUSD(I&E) memo ***Real Property-related ICS Cybersecurity*** ***(19Mar14)***
- NIST SP 800-82 r2 ***Guide to Industrial Control Systems (ICS) Security*** ***(May15)***
- DoDI 8530.01 ***Cybersecurity Activities Support to DoD Network Operations*** ***(FINAL DRAFT)***
  - **DoD IN include systems operated by contractor, research centers, labs, agencies, non-DoD orgs**

Cybersecurity Rules Apply to CS & Info Systems

Draft DoD Acquisition Language



Based on DHS procurement document, DoD RMF, and GSA-DOD acquisition reform publications

Planning and Design

- Apply hardening criteria (e.g. DoD STIGS)
- Penetration Testing (artifacts)
- Complete initial CSET evaluation at 90% design, initial system security plan/ baseline risk assessment
- Conform with relevant **UFC** and UFGS

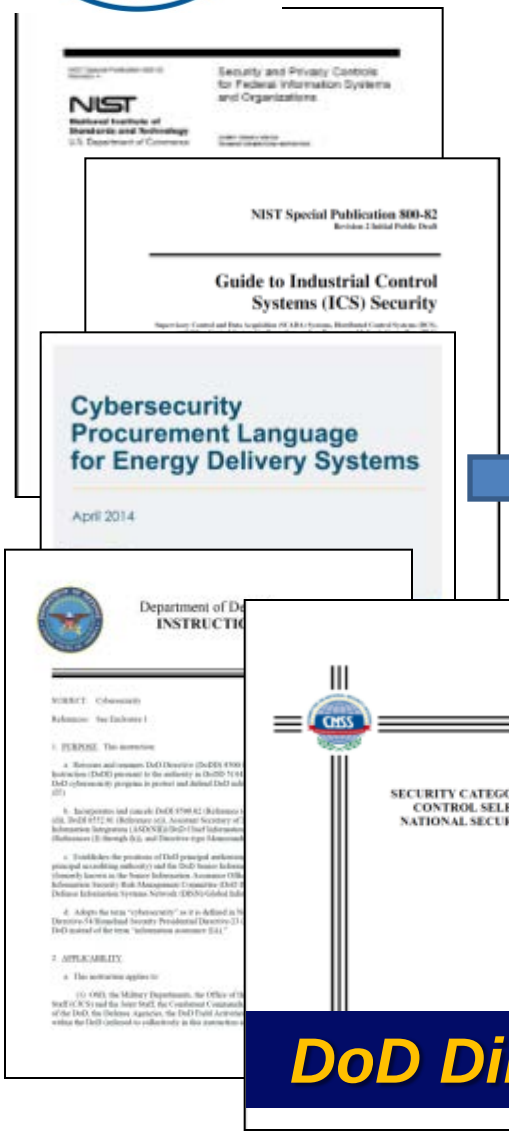
Construction

- 50-75% construction complete: conduct Factory Acceptance Testing (FAT) of major components
- 100% construction complete: conduct Site Acceptance Testing (SAT)
- Conduct Penetration Testing(e.g. SamuraiSTFU, special tool for ICS)
- Create System Security Plan (SSP)
- Create System Assessment Plan (SAP)
- Create CONOPS
- Create Plan of Action and Milestones (POAM)
- Create Incident Response Plan (IRP)

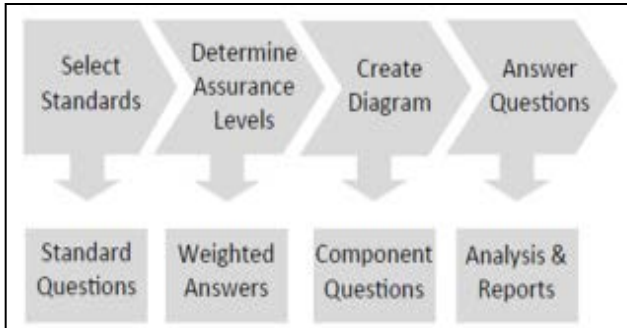
Testing Use Cases: SPIDERS, Fort Belvoir Microgrid

DHS Cyber Security Evaluation Tool (CSET)

Acquisition, Technology and Logistics



CSET 6.2 has new DoD, CNSS, NIST and DHS references & GM plugin



Standards/Question Sets in CSET	Short Name
NIST Special Publication 800-53 Rev 3	800-53 R3
NIST Special Publication 800-53 Rev 3 App I	800-53 R3 App I
NIST Special Publication 800-53 Rev 4	800-53 R4
NIST Special Publication 800-53 Rev 4 App J	800-53 R4 App J
NIST Special Publication 800-82	SP800-82
NIST Special Publication 800-82 Rev 1	SP800-82 V1
NIST Special Publication 800-82 Rev 2 (Draft)	SP800-82 V2
Consensus Audit Guidelines (CAG)	CAG
Components Questions Set	Components
CFATS Risk-Based Performance Standards Guide 8-Cyber	CFATS
CNSSI No. 1253 Baseline	CNSSI 1253
CNSSI No. 1253 Industrial Control System (ICS) Overlay V1	CNSSI ICS
Catalog of Recommendations Rev 7	COR 7
DOD Instruction 8500.2	DOD 8500.2
INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	INGAA
Key Questions Set	Key
NIST Framework for Improving Critical Infrastructure Cybersecurity V1	NCSF V1
NEI 0809 Cyber Security Plan for Nuclear Power Reactors	NEI 0809
NERC CIP-002 through CIP-009 Rev 3	NERC Rev 3
NERC CIP-002 through CIP-009 Rev 4	NERC Rev 4
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	NISTIR 7628
NRC Regulatory Guide 5.71	NRC 5.71
TSA Pipeline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

DoD Directed Standardized Assessments via CSET

DoD CIO RMF KS Portal – PIT/CS

Acquisition, Technology and Logistics

EI&E Platform IT (PIT) Control Systems

Background

Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*, and DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, incorporate Platform IT (PIT) into the RMF process. PIT is a category of both IT hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subsystems, or PIT systems. PIT differs from "traditional" IT in that it is integral to – and dedicated to the operation of – a specific platform. Although the term PIT is used only by DoD, the concept of categorizing components and systems dedicated to the operation of a specific platform is not. For example, the term "Operational Technology" (OT) is also used to refer to these systems and components.

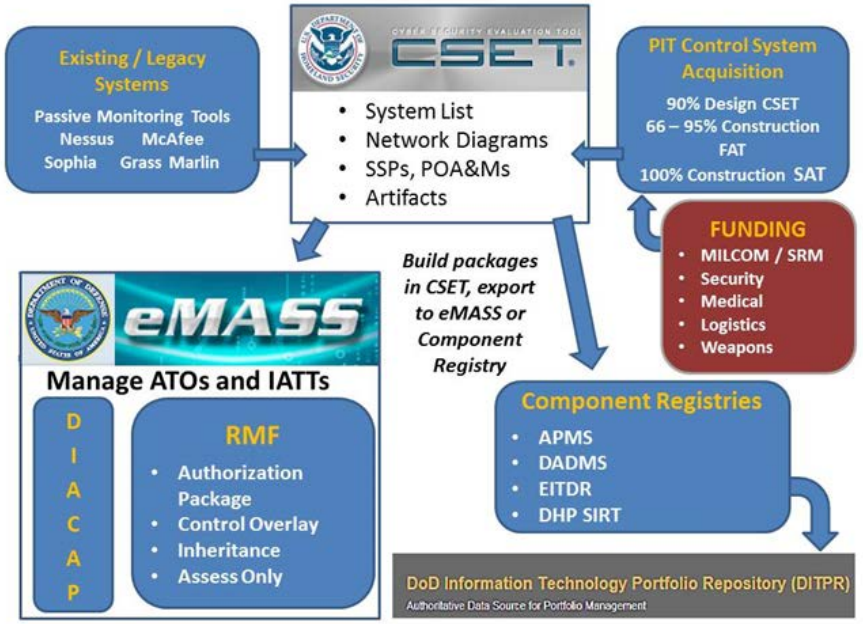
The most common forms of PIT are Control Systems (CS), which are a combination of control components (e.g., electrical, mechanical, hydraulic, or pneumatic, etc.), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (e.g., transport of matter or energy, maintain a secure and comfortable work environment, etc.). All automated control systems are considered PIT. Industrial Control Systems (ICS) are automated control systems that act upon industrial systems and processes. ICS is used as a general term that encompasses several – but not all -- types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems, such as the Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructure. In the past, the Assistant Secretary of Defense for Energy, Installations and Environment (ASD(EI&E)) community used ICS in an even broader sense to represent all types of control systems (SCADA, DDC, DCS, building, vehicle, transportation, etc.). However, since most

1

Key Documents and Tools

- Overview of EI&E PIT Control Systems and Reference Architecture (.pdf)
- EI&E PIT Control Systems Glossary (.pdf)
- EI&E PIT Control System Master List (.xlsx)
- NIST SP 800-82 R2 Industrial Control Systems Security Guide (.pdf)
- NIST SP 800-82 R2 ICS Overlay Security Controls (.xlsx)
- NIST SP 800-53 R4 and NIST SP 800-82 R2 Merged (.docx)
- USACE Electronic Security Systems Performance Work Statement IA Enclosure 1 (.pdf)
- DHS Interagency Security Committee: Securing Government Assets through Combined Traditional Security and Information Technology (.pdf)
- DHS Cyber Security Evaluation Tool (CSET)
- GAO 15-6 Federal Facility Cybersecurity (.pdf)
- EI&E Control System and Information System Determination Process and Information Requirements for IT (.pdf)

Figure 8 – Relationship of CSET, Component Registry, eMASS, and DITPR



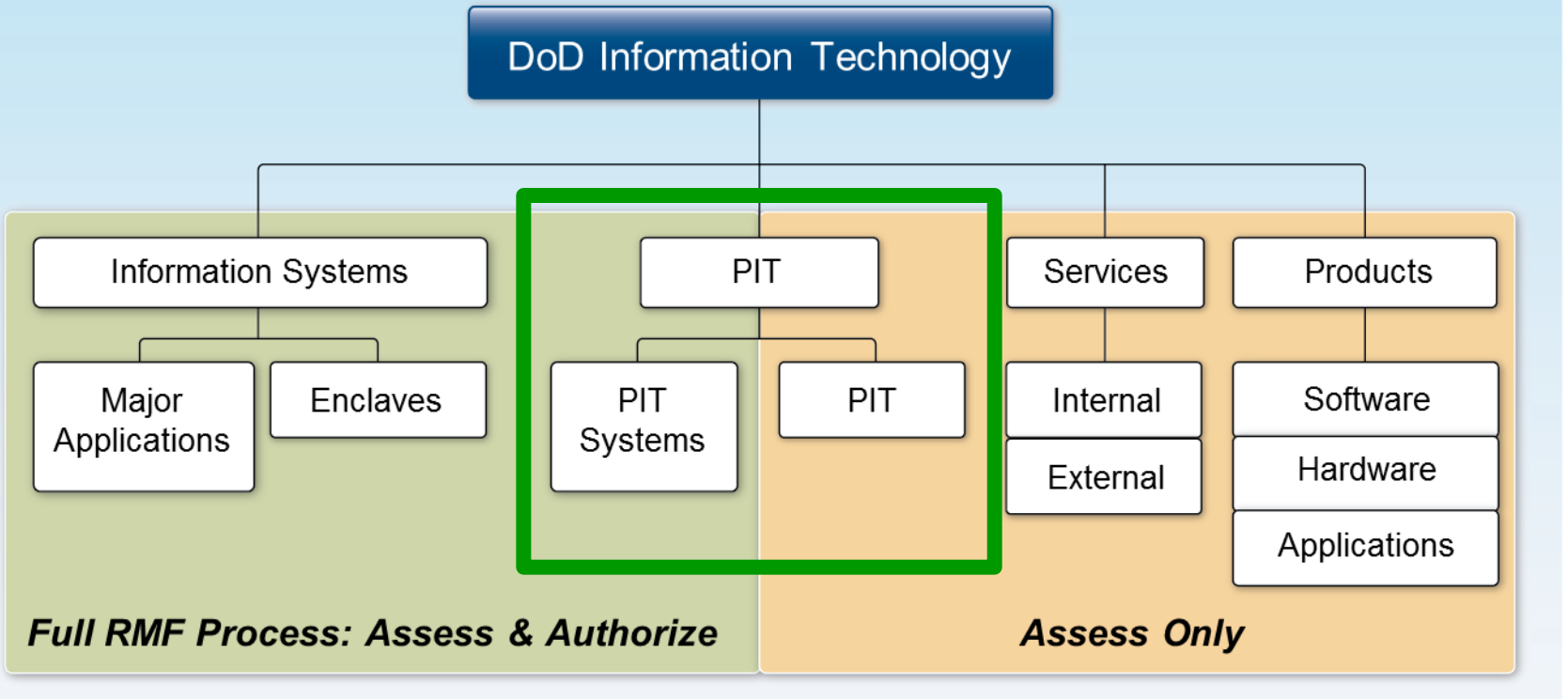
RMF KS PIT CS Website Released DoD-wide Aug'15

DoD CIO Policy

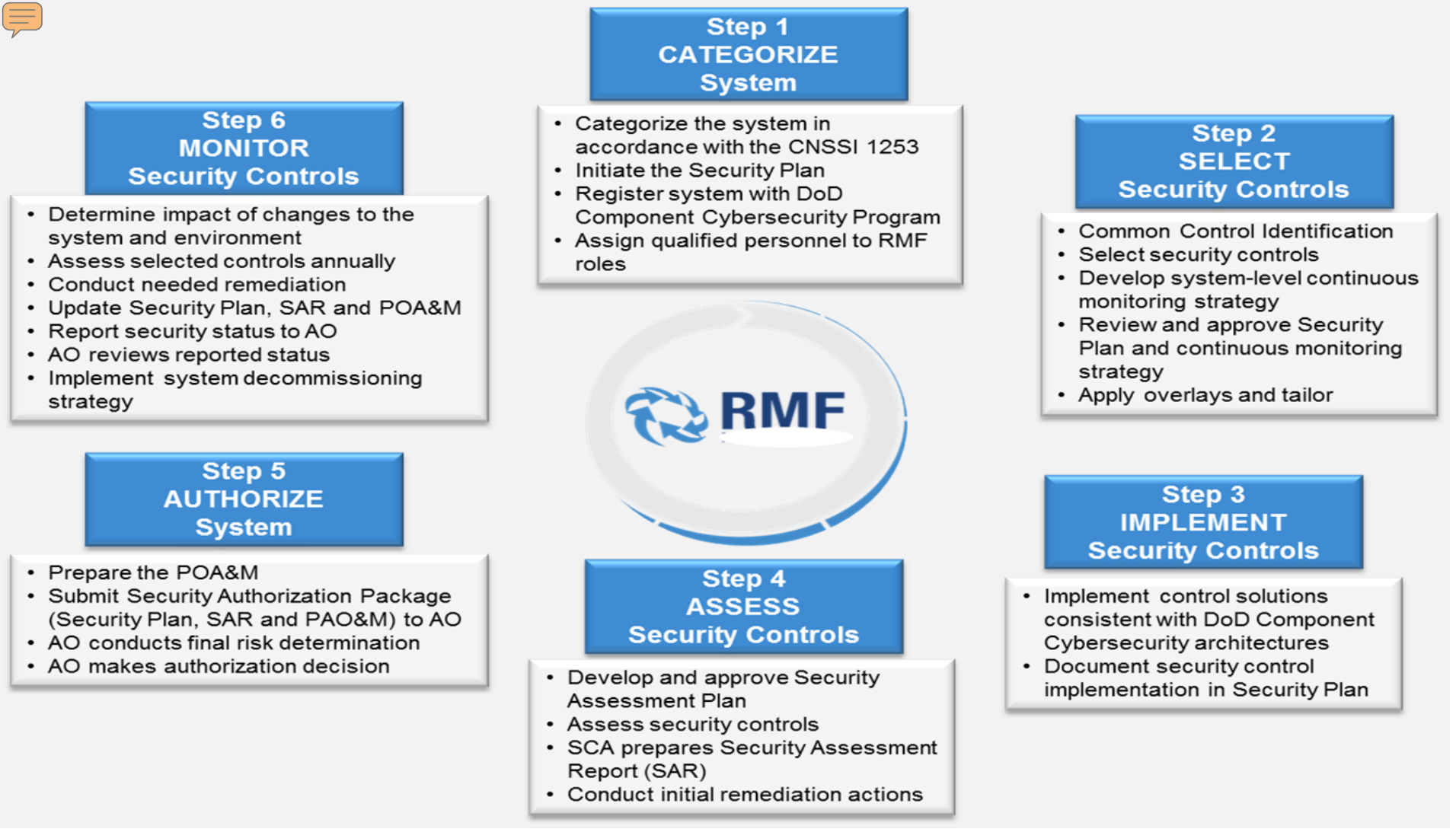
RMF applies to all Information Technology

Reduces exploitation of vulnerabilities in PIT, Services, or Products previously not secured or assessed

"All DoD-owned or DoD-controlled IT that receive, process, display or transmit DoD information"



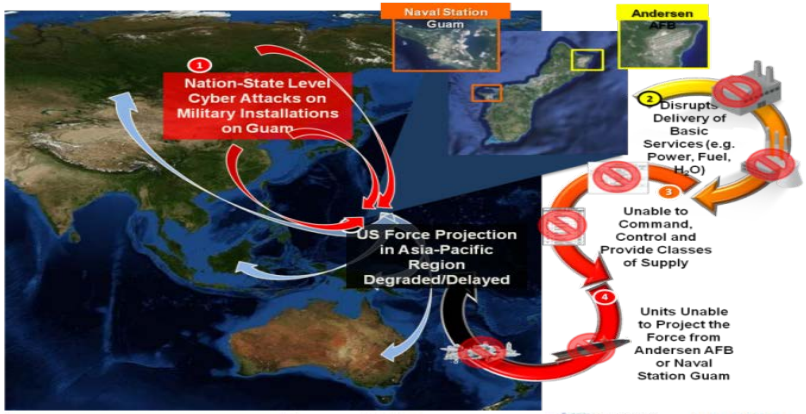
Not a One Size Fits All Approach to Securing IT

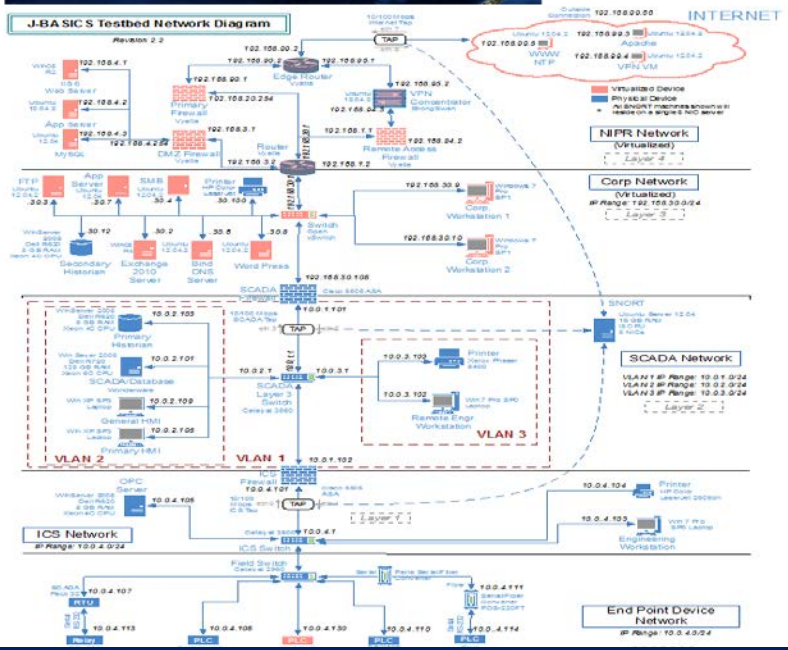


Completed DIACAP Package Submitted to AO for Signature	ATO Date	Maximum Duration of ATO under DIACAP
DoD CIO Memo Date through May 31, 2015	Determined by AO Signature Date	2.5 years from AO signature date
June 1, 2015 through February 1, 2016		2 years from AO signature date
February 2, 2016 through October 1, 2016		1.5 years from AO signature date

Joint Base Architecture for Secure Industrial Control Systems

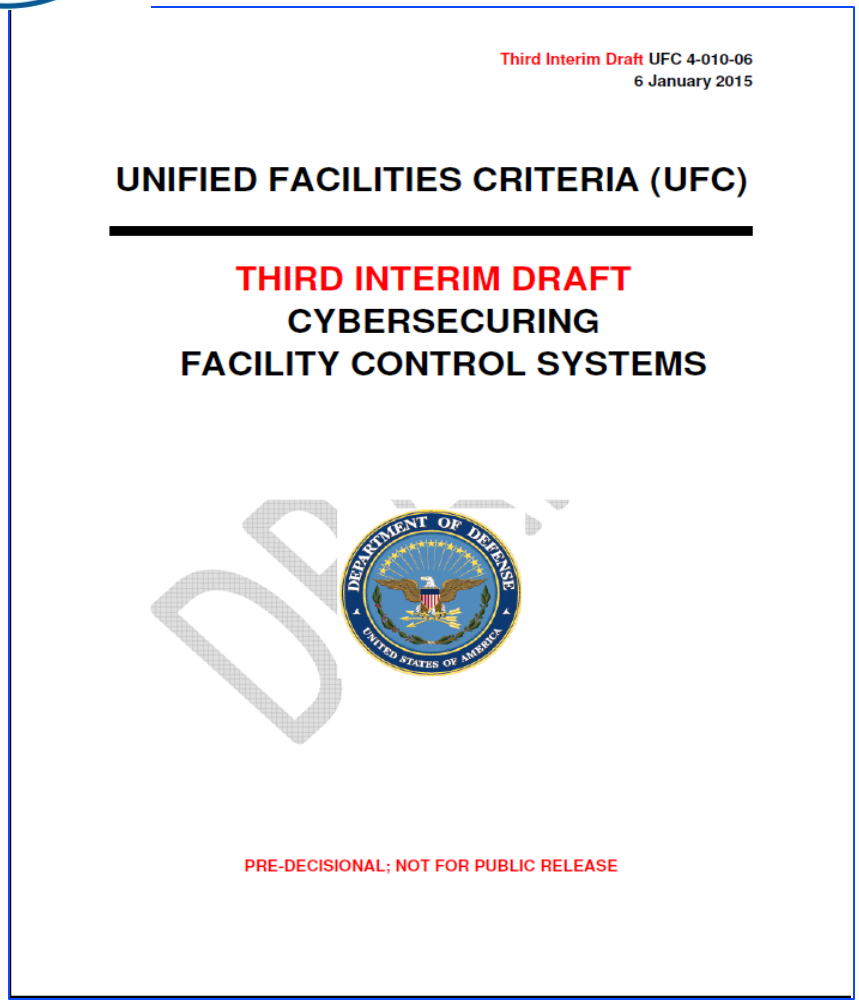
- **Detect, Mitigate, Recover**
  - **Develop TTP for defending DoD ICS / SCADA & PIT**
  - **Test topology based on networks found during surveys**
  - **Passive taps inserted for network monitoring**
  - **Test focused on SCADA network, CS network, and End Point Device network**
  - **Recognize enterprise network primarily used for attack positioning**
  - **2nd "field test" completed July '15**
  - **TTP transition Dec '15**





Monitor CS Networks For Malevolent / Unexpected Behavior

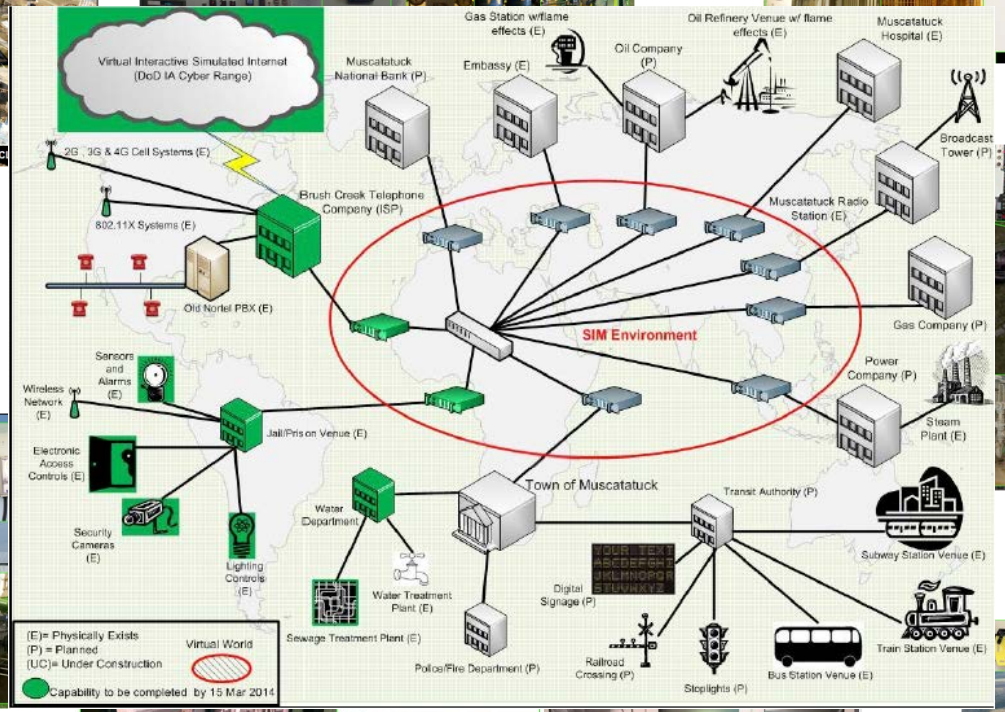
UFC Objectives

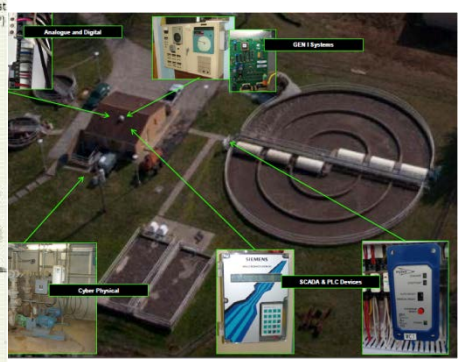


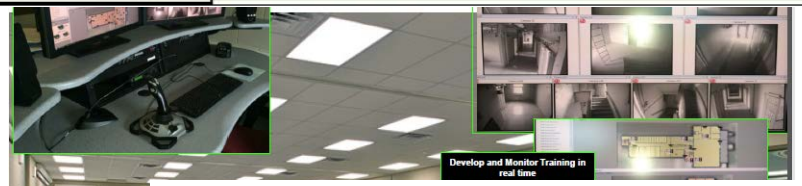
1. **Define new Design and Construction Methodology to apply RMF & NIST SP 800-82 ICS Security Guide**
2. **Define IT / CS Reference Architecture as it applies to Control Systems**
3. **Verify controls @ 50-75% construction: conduct Factory Acceptance Testing (FAT) of major components**
4. **Verify controls @ 100% construction complete: conduct Site Acceptance Testing (SAT)**

Pre-Final Version by 30 Sept '15

Cyber Range Control Systems?
An option: Camp Atterbury - Edinburgh, IN







FY15 / 16 JS Special Interest Items

- **Critical infrastructure links to Industrial Control Systems-Supervisory Control and Data Acquisition (ICS/SCADA)**
  - **a. Identify critical infrastructure dependent upon ICS/SCADA**
  - **b. Validate Info Sys architecture supporting operation of ICS/SCADA**
  - **c. Threat/Hazards identified to ICS/SCADA w/ appropriate countermeasures**
- **Have ICS / SCADA systems been identified that support infrastructure throughout the installation?**
- **Has a Risk & Threat Assessment on all ICS / SCADA systems been conducted IAW NIST SP 800-82,800-30, and DoDI 8510.01?**
- **Are all appropriate ICS / SCADA Security Control Measures implemented IAW DoDI 8510.01 and NIST SP 800-53v4? [NIST SP 800-82 r2]**

Requires CIO & Facility SME Collaboration

Brief to HASC by 1/1/16

- DoD is transitioning to **smart buildings** increasingly utilizing wireless controls for heating, ventilation and air conditioning, security systems, lighting, electrical power, fire alarms, elevators, visitor controls, cellular communications, Wi-Fi networks, and first responder communications and other systems are increasing interconnected and online.

- Higher connectivity has increased the threat and vulnerability to cyber-attacks. Government Accountability Office study (GAO–15–6) highlighted the vulnerabilities and cyber risks to building and access control systems.

- Therefore, SECDEF to brief HASC **1/1/16** on the **cyber risks to smart buildings and access control systems** from **radio frequency systems** and **wireless communications**, and identification of **available technologies and practices available** to potentially **counter and mitigate the identified security risks**."

OASD EI&E OPR, Coord w/ Components, USCC, CIO, USD(I)…

Control Systems Cyber Security Analysis

Acquisition, Technology and Logistics

Challenge: Cyber security for control systems is a formidable effort; DoD requires insight to problem scope and solutions

Focus: 10 installations directly supporting operations [IE&OE]

3 Complementary Lines of Effort – 12 months

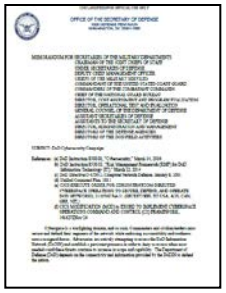
- DoD's ICS Exposure to Internet Threats
- Gap Analysis of Tech. Solutions to Monitor DoD ICS
- Workforce Training Evaluation and Development

Benefits: Advances nascent ICS efforts in Defense community

- Give execs insight to set policy, reveal relevant cyber CS threats and vulnerabilities and gap between current and desired states
- Identify appropriate EI&E cyber workforce skills and requirements

JHU-APL Will Complete Assessments & Analysis w/ Service SMEs

Consistent Weak Link = WETWARE



DoD Cybersecurity Campaign memo (USCC, AT&L, CIO)

“ Adversaries are actively attempting to access & establish a persistent presence in order to deny us access when most needed—and these threats continue to increase in scope and capability.”

“Most successful cyber attacks …have been attributed to human error, either through improperly configured technological solutions or non-compliance with existing cybersecurity policy. Inspection reports continue to reveal Department-wide, systemic shortfalls in implementing basic cybersecurity requirements found in current policy, directives, and orders.”

Take-Away's

- Include PIT/CS in 'cyber-scape' analysis
- Partner Facility Engineer & CIO SMEs
- Baseline: Establish Your PIT/CS "*Position Zero*"
  - Known inventory, topology, processes and tasks, users, data flows
- Implement routine monitoring to recognize deviations; determine legit / malicious
- Exercise methodology prior to needing it!
- Implement Alert process (register w/ DHS)

- **POC: Mr. Daryl Haegley daryl.r.haegley.civ@mail.mil**