# SAME DC/Northern VA Posts Small Business Conference
# Feb 22, 2017

## Cybersecuring DoD Control Systems

Chinook

Secure · Compliant · Efficient

# Overview

## History and Evolution

- Situation Awareness; Reality Check
- DoD’s Policy Progress
- Leadership / Management Considerations

## Cyber Workforce

- Framework
- Skills and Credentials

## Cyber Lifecycle

- Protecting your Business and Clients
- Supply Chain Risk Management
- RFPs and PWS
- Design and Construction

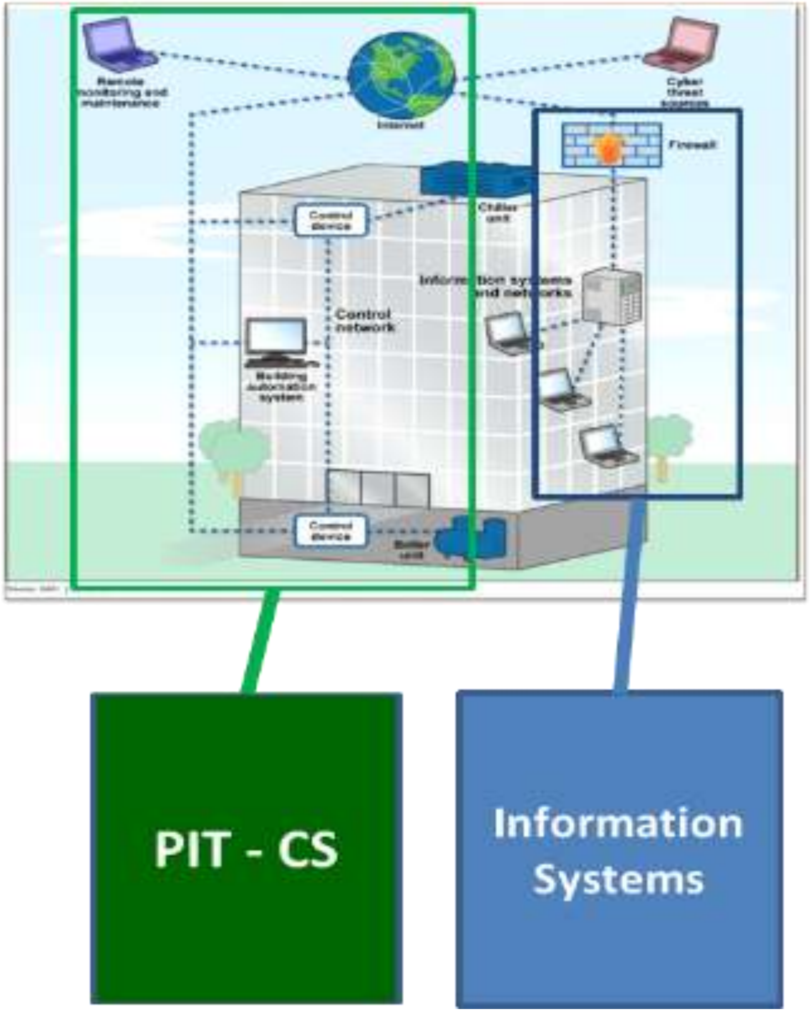
## What’s Next?

- Complete the Inventory
- People / Roles
- Governance

## Resources

# Same Meaning but Different:
# *PIT, CS, PIT-CS, ICS,OT, SCADA, CPS*

- **PIT = Platform Information Technology**
- **CS = Control Systems**
- **PIT-CS = PIT Control Systems**
- **ICS = Industrial Control Systems**
- **OT = Operational Technology**
- **SCADA = Supervisory Control And Data Acquisition**
- **CPS = Cyber Physical Systems**
- **IoT = Internet of Things**



***DoD = PIT;     DHS & NIST = ICS, SCADA, CPS;     Commercial = OT, IoT***

>500 Installations
>250K Buildings
>200K Structures

Buildings

Weapon Platforms

Operational Energy

Electrical and HVAC

Pumps and Motors

Nuclear

Vehicles / Charging Stations

Typical IP Controller; Similar Used Everywhere (10,000s of vendors)

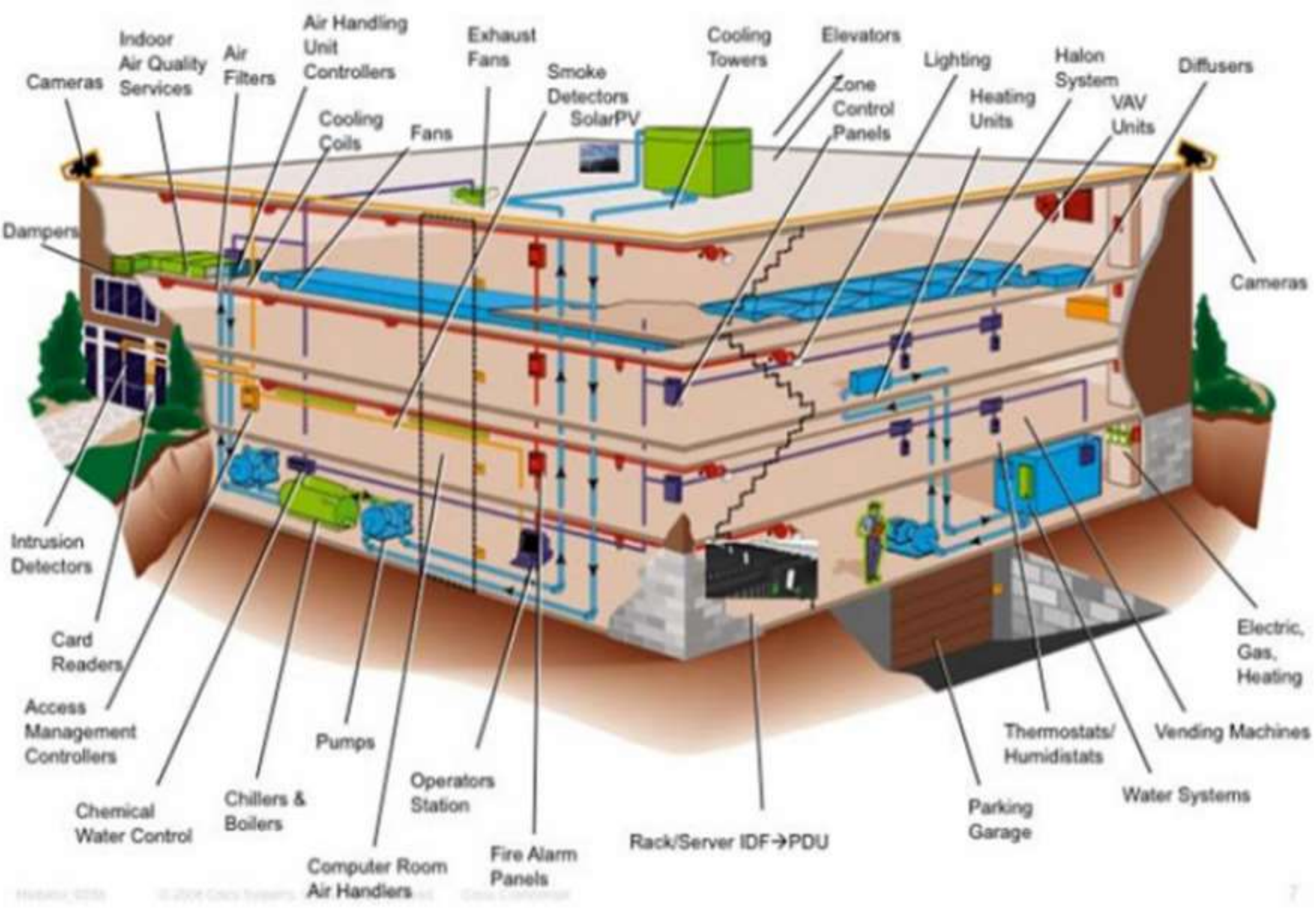
Medical

Manufacturing

***DHS: “245 = Avg # Days Undiscovered Adversary in non-IS Network”***

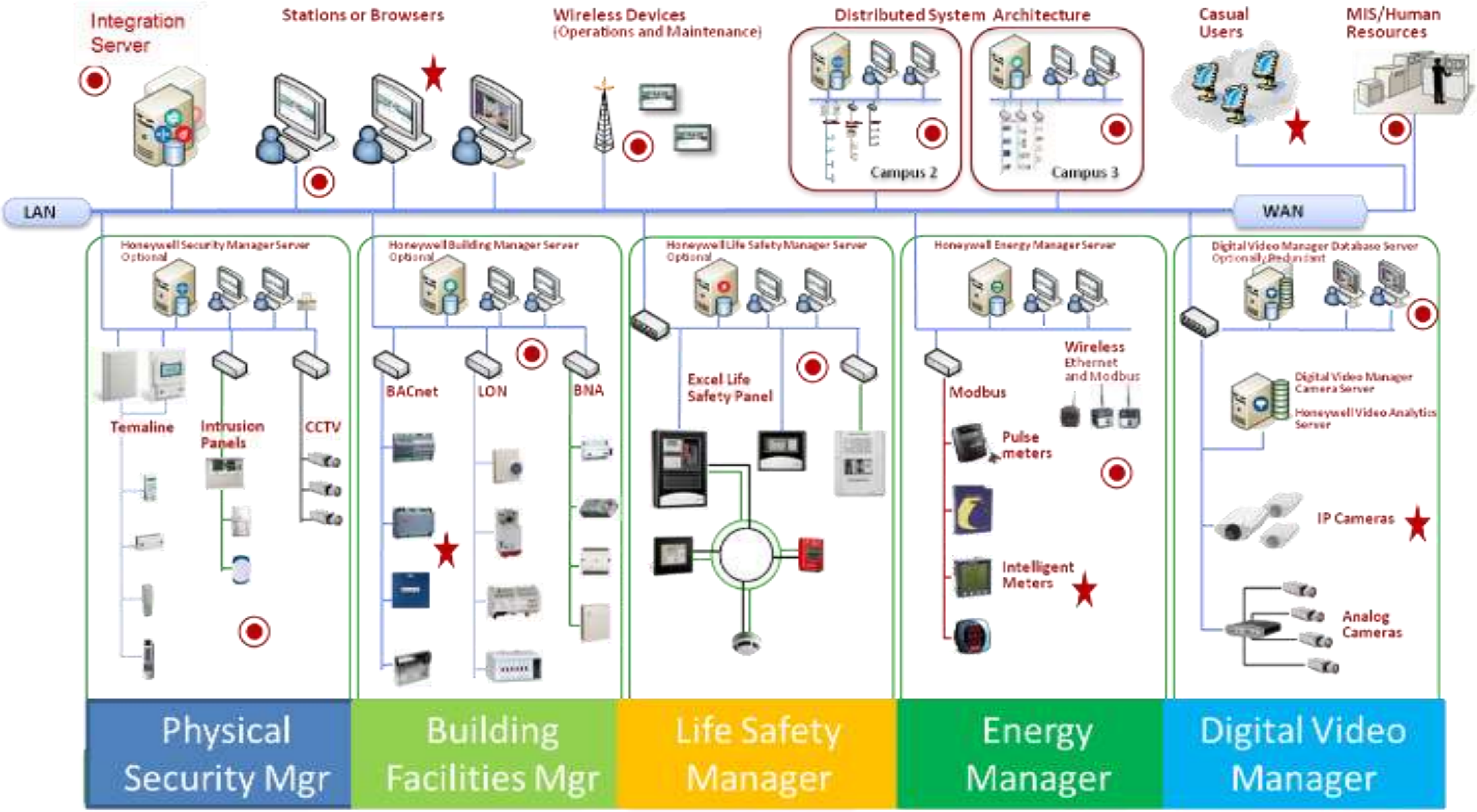
# Policy, Standards, Guidance, Procedures

***Leadership / Management Roles: Provide Clear Direction…***



# *Who's Cyber Securing These?*

# Controls System Owners



★ Possible entry point of attack ◉ Potential compromise

# Control Systems Companies

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

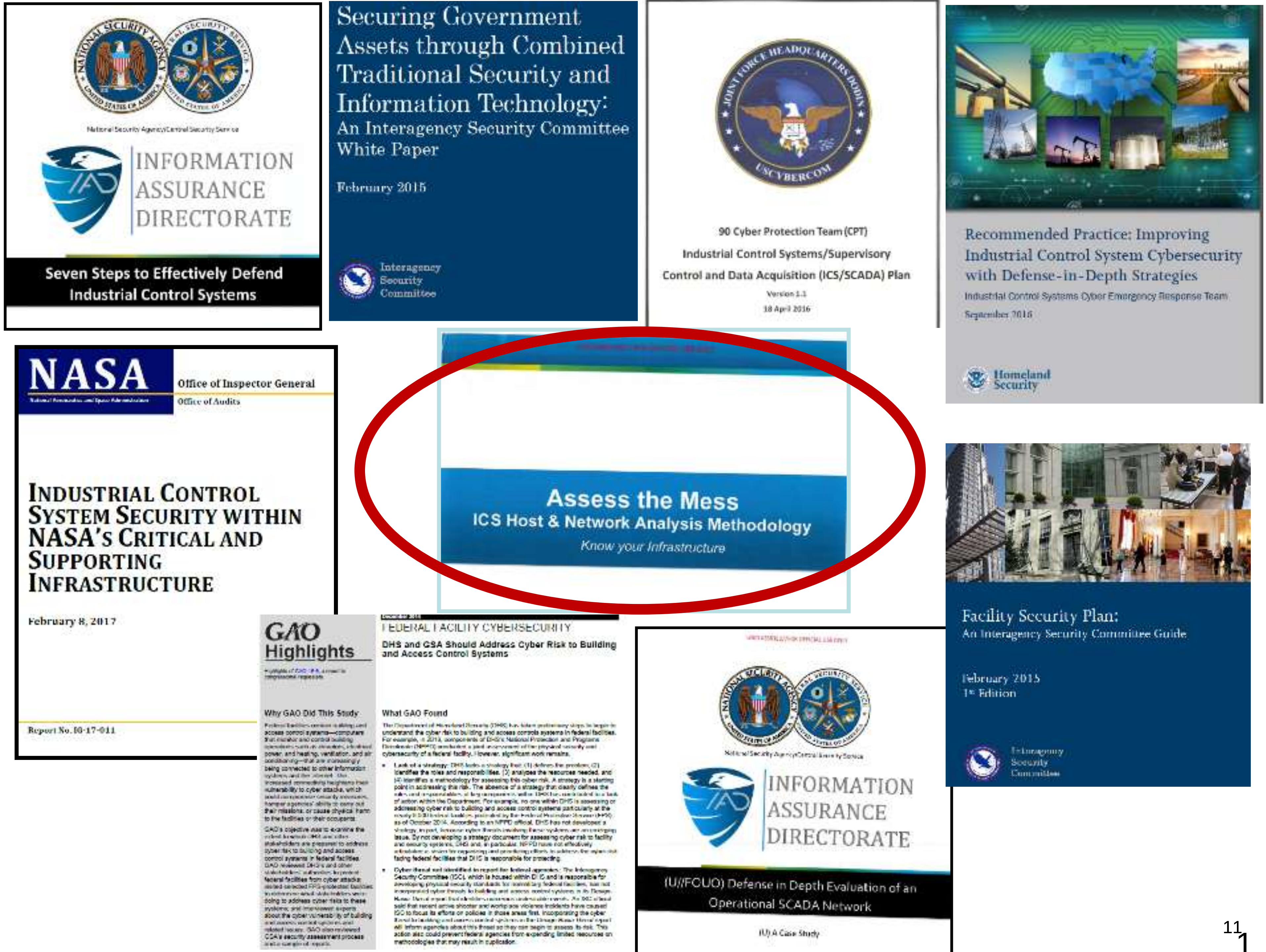
# Operating Software

Axon    CAT SARL    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

# Device Level Controllers

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 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!***



National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Seven Steps to Effectively Defend Industrial Control Systems

Securing Government Assets through Combined Traditional Security and Information Technology: An Interagency Security Committee White Paper

February 2015

Interagency Security Committee

90 Cyber Protection Team (CPT)

Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) Plan

Version 1.1

18 April 2016

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team

September 2016

Homeland Security

NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

INDUSTRIAL CONTROL SYSTEM SECURITY WITHIN NASA'S CRITICAL AND SUPPORTING INFRASTRUCTURE

February 8, 2017

Report No. IG-17-011

[illegible]

Assess the Mess

ICS Host & Network Analysis Methodology

*Know your Infrastructure*

GAO Highlights

Highlights of GAO-15-6, a report to congressional requesters

December 2014

FEDERAL FACILITY CYBERSECURITY

DHS and GSA Should Address Cyber Risk to Building and Access Control Systems

Why GAO Did This Study

Federal facilities contain building and access control systems—computers that monitor and control building operations such as elevators, electrical power, and heating, ventilation, and air conditioning—that are increasingly being connected to other information systems and the Internet. The increased connectivity heightens their vulnerability to cyber attacks, which could compromise security measures, hamper agencies' ability to carry out their missions, or cause physical harm to the facilities or their occupants.

GAO's objective was to examine the extent to which DHS and other stakeholders are prepared to address cyber risk to building and access control systems in federal facilities. GAO reviewed DHS's and other stakeholders' [illegible] to protect federal facilities from cyber attacks, visited selected FPS-protected facilities to determine what stakeholders were doing to address cyber risks to these systems, and interviewed experts about the cyber vulnerability of building and access control systems and related issues. GAO also reviewed GSA's security assessment process and a sample of reports.

What GAO Found

The Department of Homeland Security (DHS) has taken preliminary steps to begin to understand the cyber risk to building and access controls systems in federal facilities. For example, in 2013, components of DHS's National Protection and Programs Directorate (NPPD) conducted a pilot assessment of the physical security and cybersecurity of a federal facility. However, significant work remains.

- Lack of a strategy: DHS lacks a strategy that: (1) defines the problem, (2) identifies the roles and responsibilities, (3) analyzes the resources needed, and (4) identifies a methodology for assessing this cyber risk. A strategy is a starting point in addressing this risk. The absence of a strategy that clearly defines the roles and responsibilities of key components within DHS has contributed to a lack of action within the Department. For example, no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by the Federal Protective Service (FPS) as of October 2014. According to an NPPD official, DHS has not developed a strategy, in part, because cyber threats involving these systems are an emerging issue. By not developing a strategy document for assessing cyber risk to facility and security systems, DHS and, in particular, NPPD have not effectively articulated a vision for organizing and prioritizing efforts to address the cyber risk facing federal facilities that DHS is responsible for protecting.
- Cyber threat not identified in report for federal agencies: The Interagency Security Committee (ISC), which is housed within DHS and is responsible for developing physical security standards for nonmilitary federal facilities, has not incorporated cyber threats to building and access control systems in its Design-Basis Threat report that identifies numerous undesirable events. An ISC official said that recent active shooter and workplace violence incidents have caused ISC to focus its efforts on policies in those areas first. Incorporating the cyber threat to building and access control systems in the Design-Basis Threat report will inform agencies about this threat so they can begin to assess its risk. This action also could prevent federal agencies from expending limited resources on methodologies that may result in duplication.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

(U//FOUO) Defense in Depth Evaluation of an Operational SCADA Network

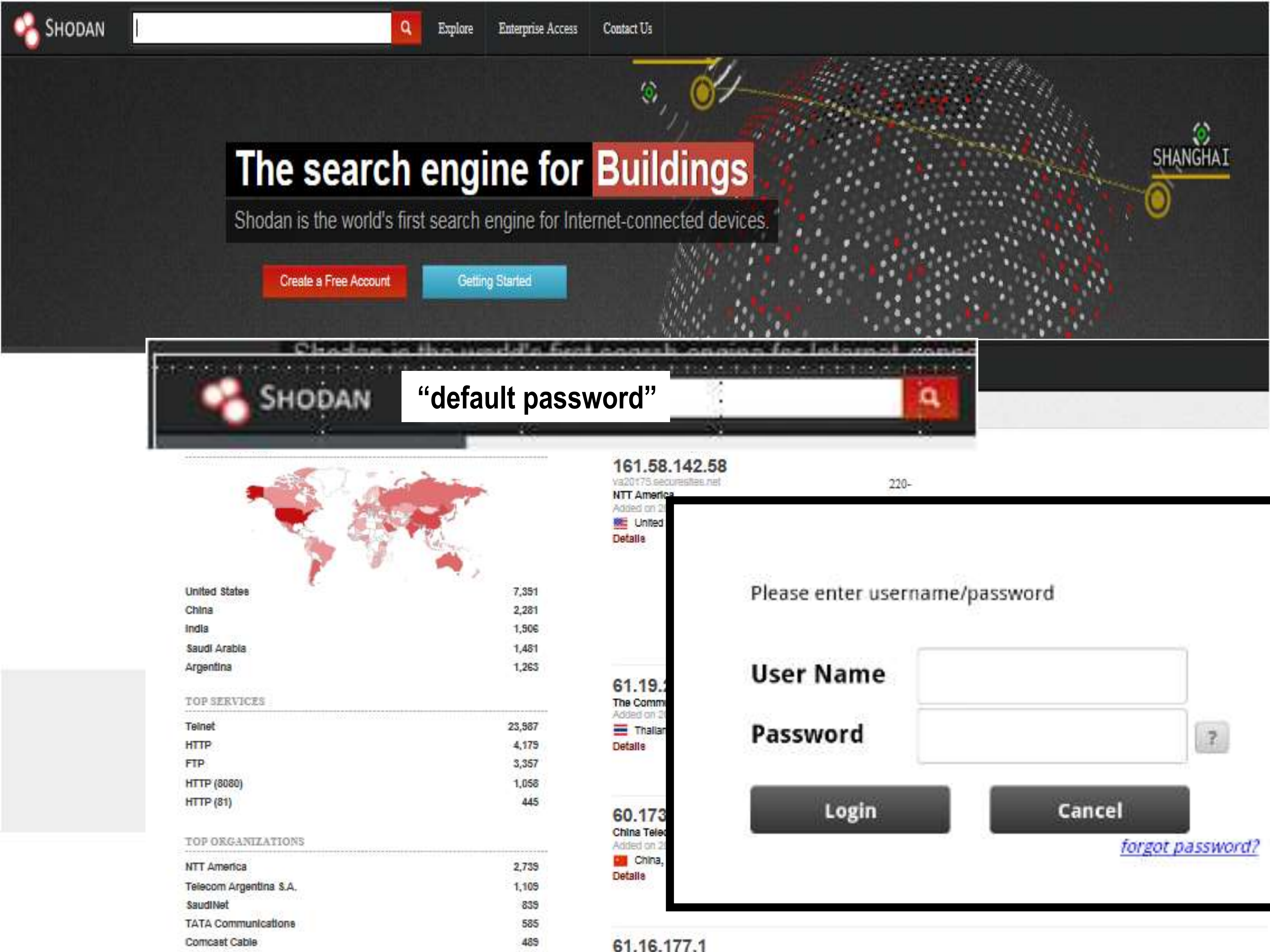
(U) A Case Study

Facility Security Plan: An Interagency Security Committee Guide

February 2015

1st Edition

Interagency Security Committee



The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

"default password"

| | |
|---|---|
| United States | 7,351 |
| China | 2,281 |
| India | 1,906 |
| Saudi Arabia | 1,481 |
| Argentina | 1,263 |

TOP SERVICES

| | |
|---|---|
| Telnet | 23,587 |
| HTTP | 4,179 |
| FTP | 3,357 |
| HTTP (8080) | 1,058 |
| HTTP (81) | 445 |

TOP ORGANIZATIONS

| | |
|---|---|
| NTT America | 2,739 |
| Telecom Argentina S.A. | 1,109 |
| SaudiNet | 839 |
| TATA Communications | 585 |
| Comcast Cable | 489 |

161.58.142.58
va20175.securesites.net
NTT America
Added on 2
United
Details

220-

61.19.
The Comm
Added on 2
Thailar
Details

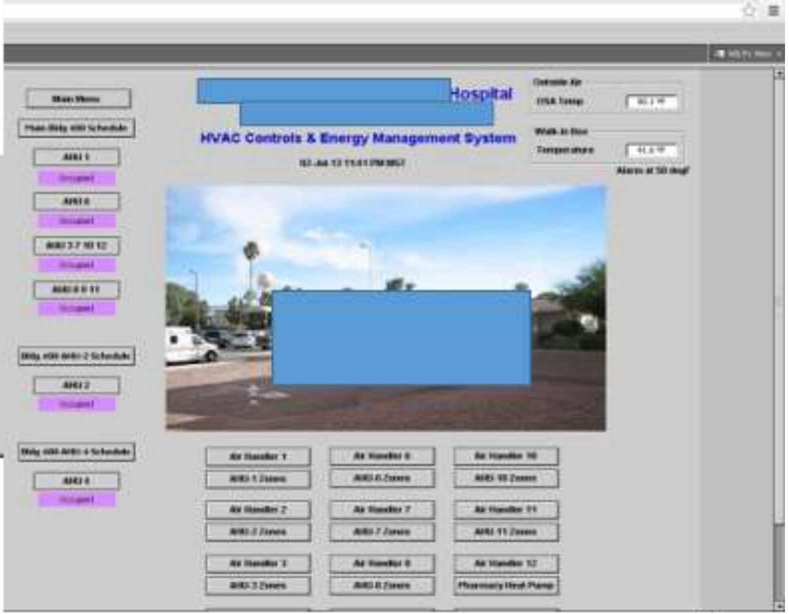
60.173
China Tele
Added on 2
China,
Details

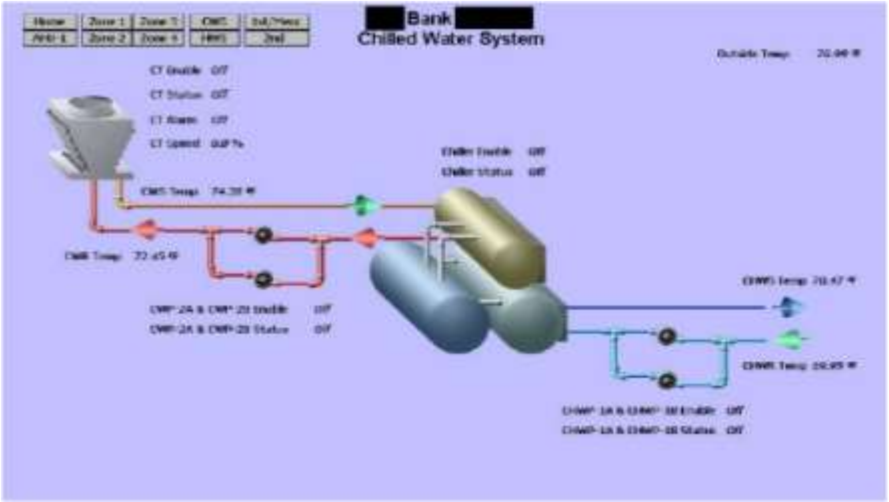
61.16.177.1

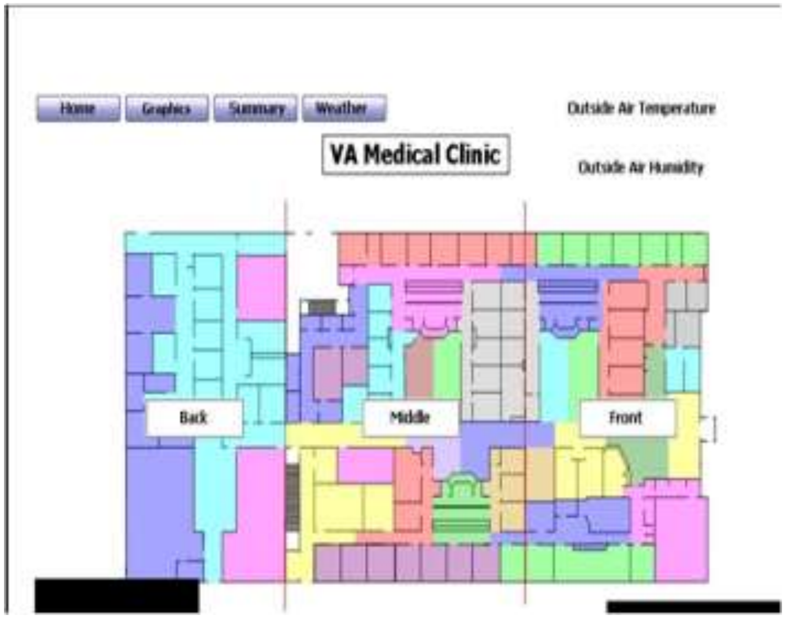
Please enter username/password

User Name

Password



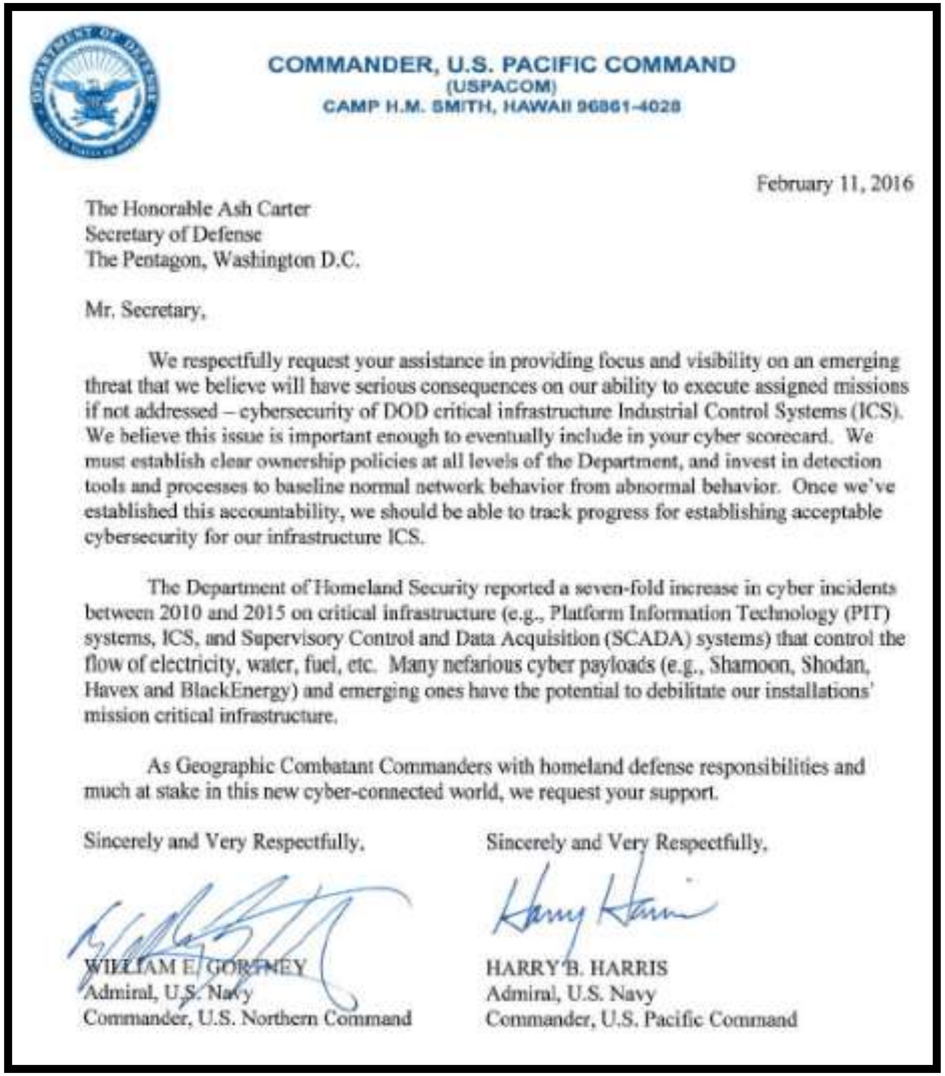




**Never Attribute Evil When Stupid is Still Available**

# "8 Star Memo"

## Cybersecurity of DoD Critical Infrastructure ICS



COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we've established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitate our installations' mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

Sincerely and Very Respectfully,

Harry Harris

HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

- Establish Clear Ownership
- Include in Scorecard
- Invest in Detection Tools
- 7x cyber incidents

LIVE
THE SKY IS FALLING!
CNN
CHICKEN LITTLE REVEALS SHOCKING NEWS TO THE WORLD
GRAVITY 4.25
NEIGHBOURS REPORT THAT LITTLE WAS A "QUIET KID, KEPT TO HIM

# Assistant Secretary of Defense EI&E Memo 31 Mar’16

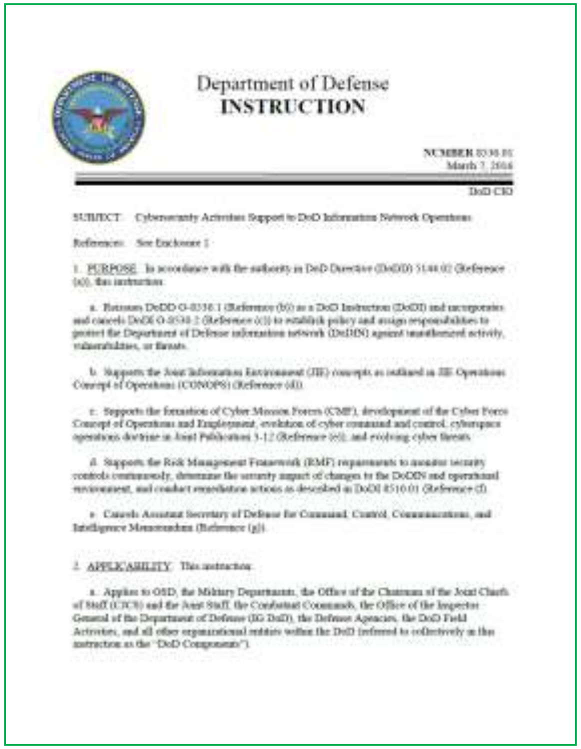
THE DOD CYBER STRATEGY

- Affirms "**the system owners/operators are accountable for the system’s operational resilience and defense posture, to include cybersecurity and are responsible for securing their IT networks, systems and devices**"

- Directs “staffs develop plans identifying **the goals, milestones and resources needed to identify, register, and implement cyber security controls** on DoD facility-related Control Systems under your cognizance”

Plans due 31Dec’16; implement cybersecurity controls on most critical facility-related control systems by end FY19

# DoDI 8530 – Cybersecurity Activities Support to DoD Info Network Operations



Department of Defense
**INSTRUCTION**

**NUMBER** 8530.01
March 7, 2016

DoD CIO

SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), this instruction:

a. Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2 (Reference (c)) to establish policy and assign responsibilities to protect the Department of Defense information network (DoDIN) against unauthorized activity, vulnerabilities, or threats.

b. Supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).

c. Supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats.

d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DoDIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f)).

e. Cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum (Reference (g)).

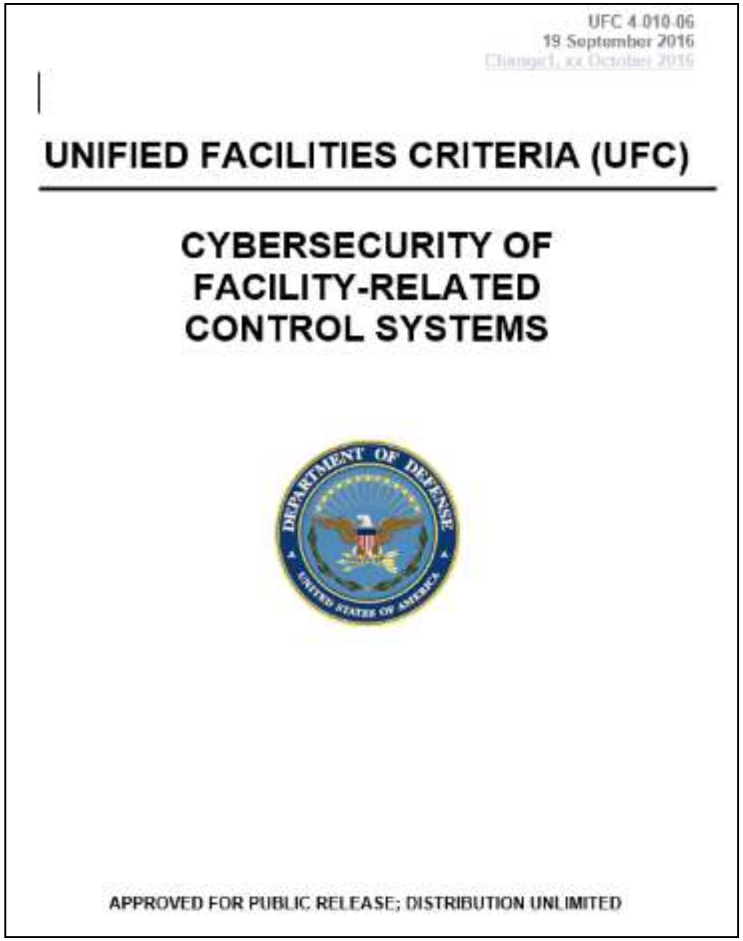
2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

2. APPLICABILITY. This instruction:

b. Applies to the DoDIN. The DoDIN includes DoD information technology (IT) (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 (Reference (h)) **and control systems and industrial control systems (ICS)** as defined in National Institute (NIST) Special Publication (SP) 800-82 (Reference (i)) that are **owned or operated by or on behalf of DoD Components**.

# Cybersecurity Controls Apply to New Construction



UFC 4-010-06
19 September 2016
Change1, xx October 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

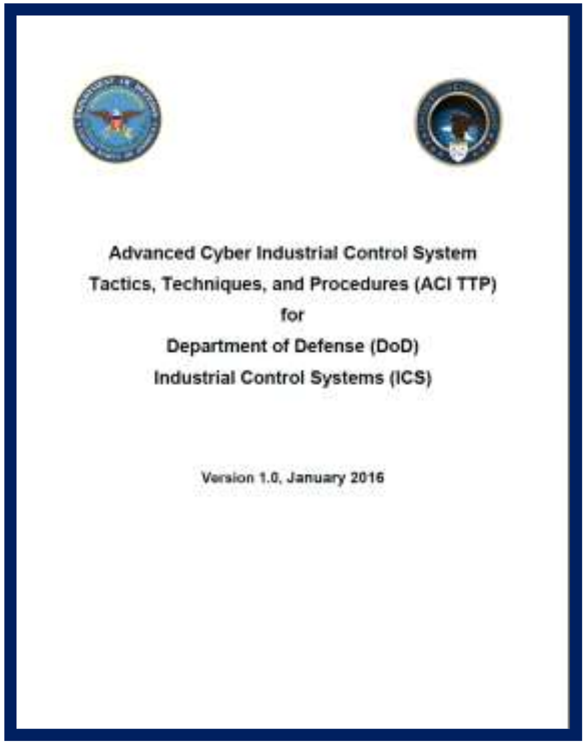
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

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)

***UFC 4-010-06  Published 19 Sept '16***

# DoD Advanced Cyber ICS (ACI) TTP

**Designed to enable managers of ICS networks to Detect, Mitigate, and Recover from nation-state-level cyber attacks (strategic, deliberate, well-trained, and funded attacks to support greater strategic objectives).**



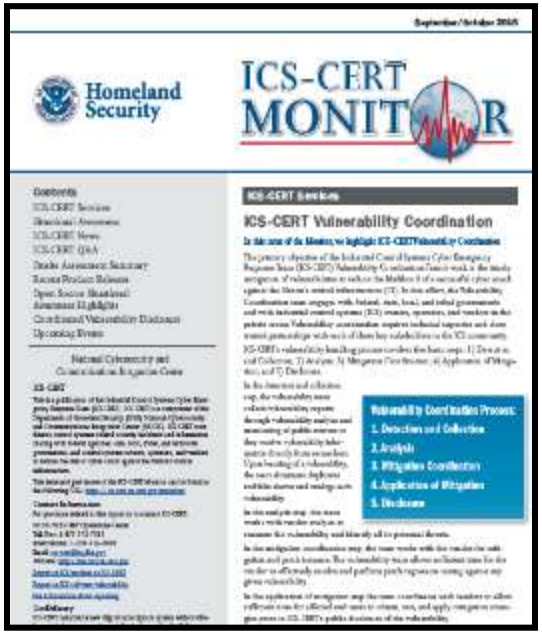
Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Version 1.0, January 2016

Divided into four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures** (**Detection, Mitigation, Recovery**) (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

# DHS ICS-CERT / CSET 8.0



September/October 2015

Homeland Security

ICS-CERT MONITOR

Contents

ICS-CERT Services

Situational Awareness

ICS-CERT News

ICS-CERT Q&A

Onsite Assessment Summary

Recent Product Releases

Open Source Situational Awareness Highlights

Coordinated Vulnerability Disclosure

Upcoming Events

National Cybersecurity and Communications Integration Center

ICS-CERT

ICS-CERT Services

ICS-CERT Vulnerability Coordination

In this issue of the Monitor, we highlight ICS-CERT Vulnerability Coordination

[illegible]

Vulnerability Coordination Process:

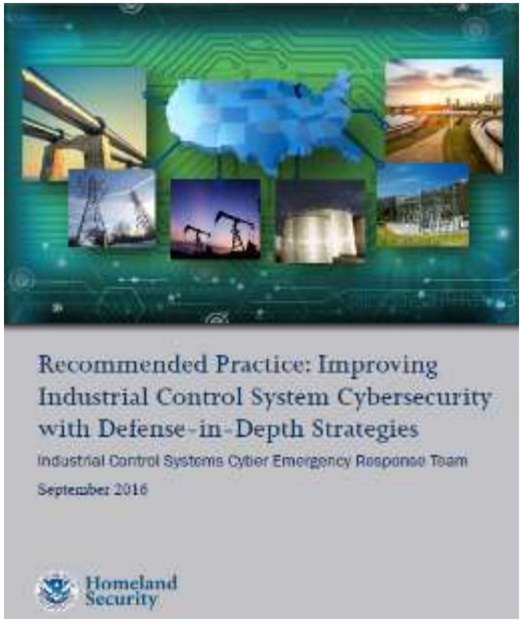
1. Detection and Collection

2. Analysis

3. Mitigation Coordination

4. Application of Mitigation

5. Disclosure

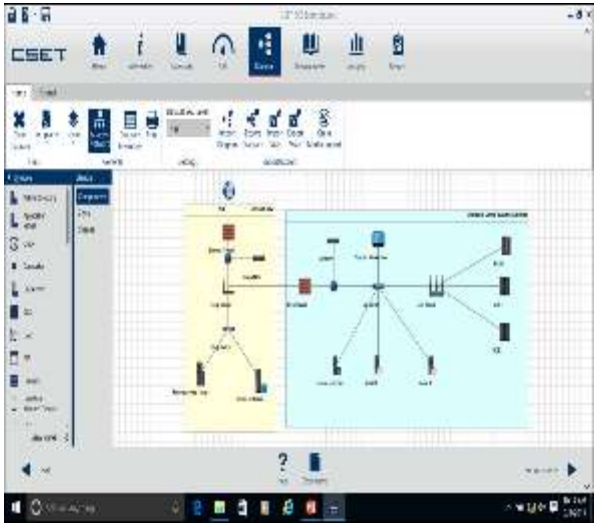


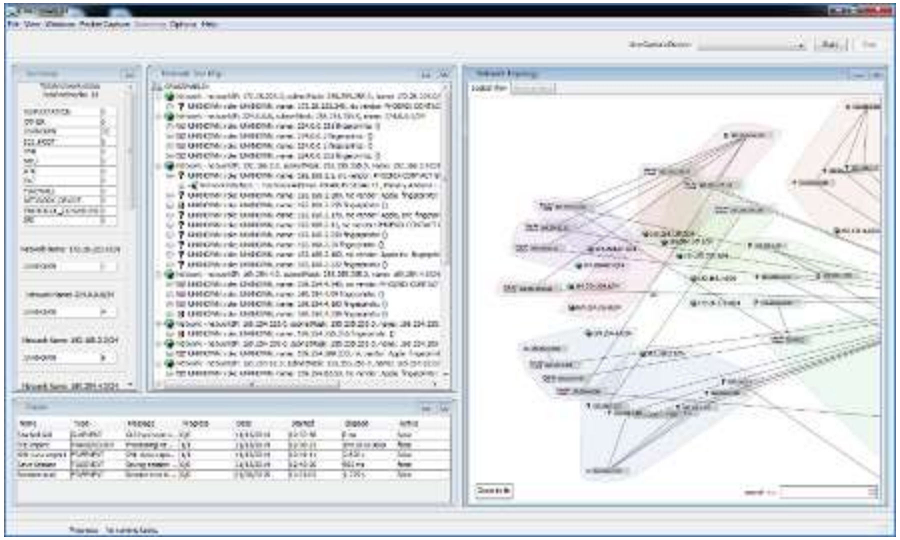
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

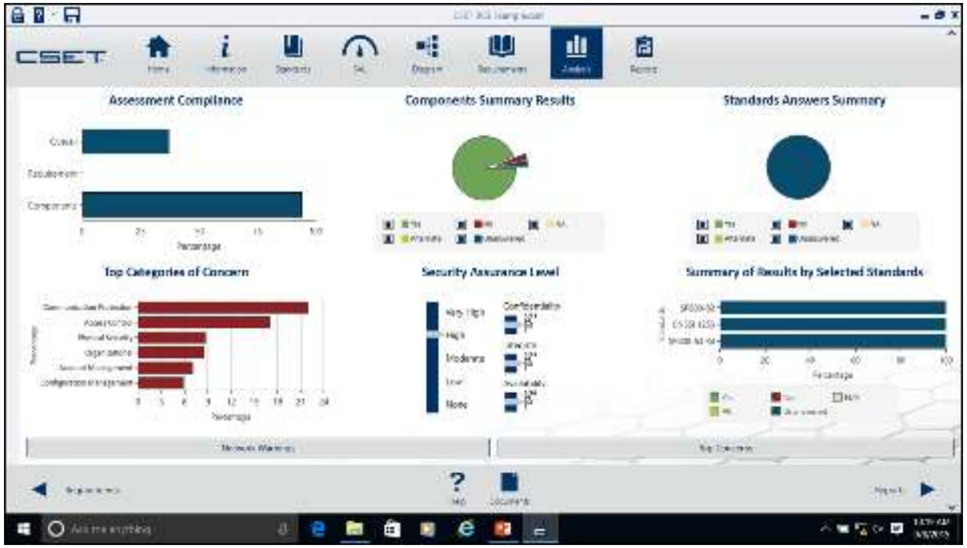
Industrial Control Systems Cyber Emergency Response Team

September 2016

Homeland Security

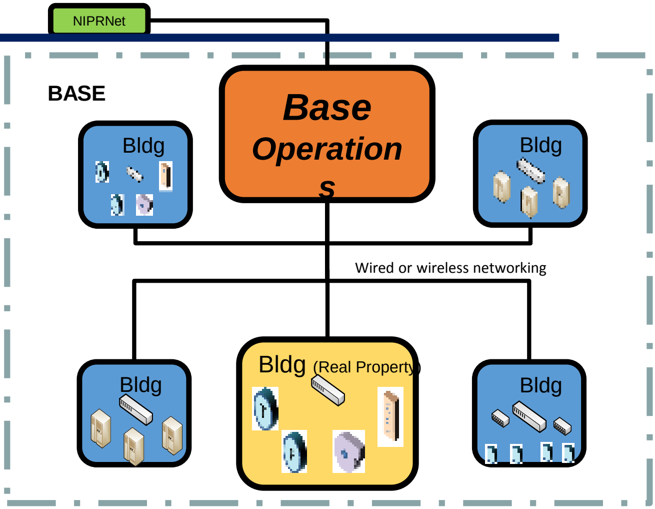


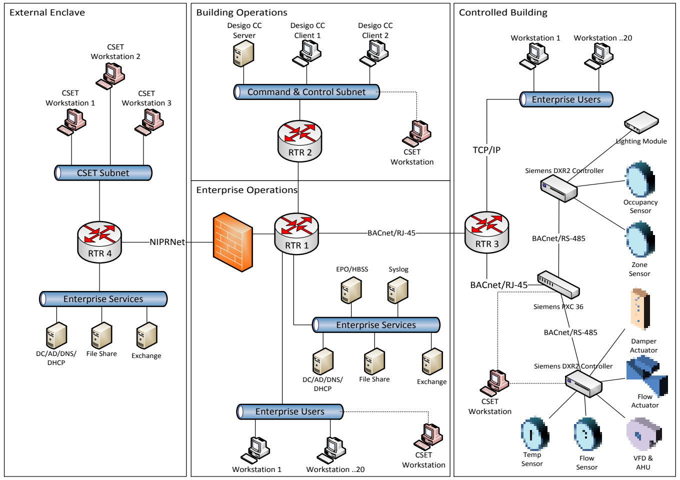




# Control Systems Cyber Security (CS2) Challenge

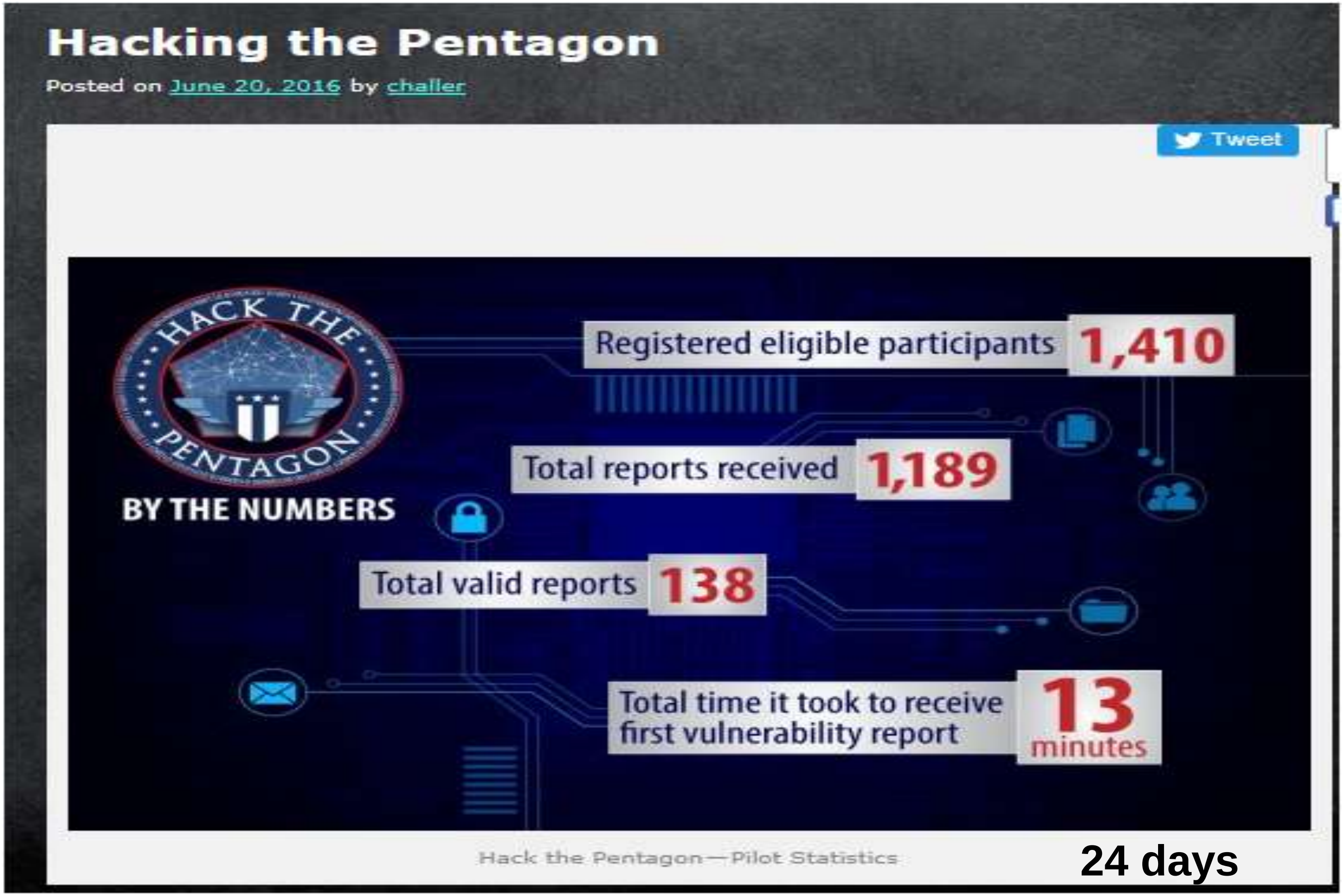
- Goal
  - Evaluate DoD industrial and building control system ability to detect, monitor, recover capabilities use cutting-edge commercial and government tools and techniques
- Relevance
  - Historically, facility developers and managers have not integrated Cybersecurity testing as part of their facility design, build-out, AO or sustainment O&M processes.
  - CS systems are connected and exploitable; DOD remotely monitors & control physical process via DoD networks or Internet
  - CS protection systems and services enter marketplace but without vetting in real-world complex environments
- Next Steps
  - Collaborative effort with OSD ASD for Energy, Installations, and Environment OASD (EI&E)
  - Build out complex/to-scale representation of a Real Property Management system to demonstrate new CS monitoring technology using crawl, walk run methodology
  - ***Crawl*** – Build CS Environment and demonstrate function!





***National Cyber Range – Kickoff Feb; First Run Apr***

# Embracing Silicon Valley Crowdsourcing: "Bug Bounty" Efforts



## Hacking the Pentagon

Posted on June 20, 2016 by challer

BY THE NUMBERS

Registered eligible participants 1,410

Total reports received 1,189

Total valid reports 138

Total time it took to receive first vulnerability report 13 minutes

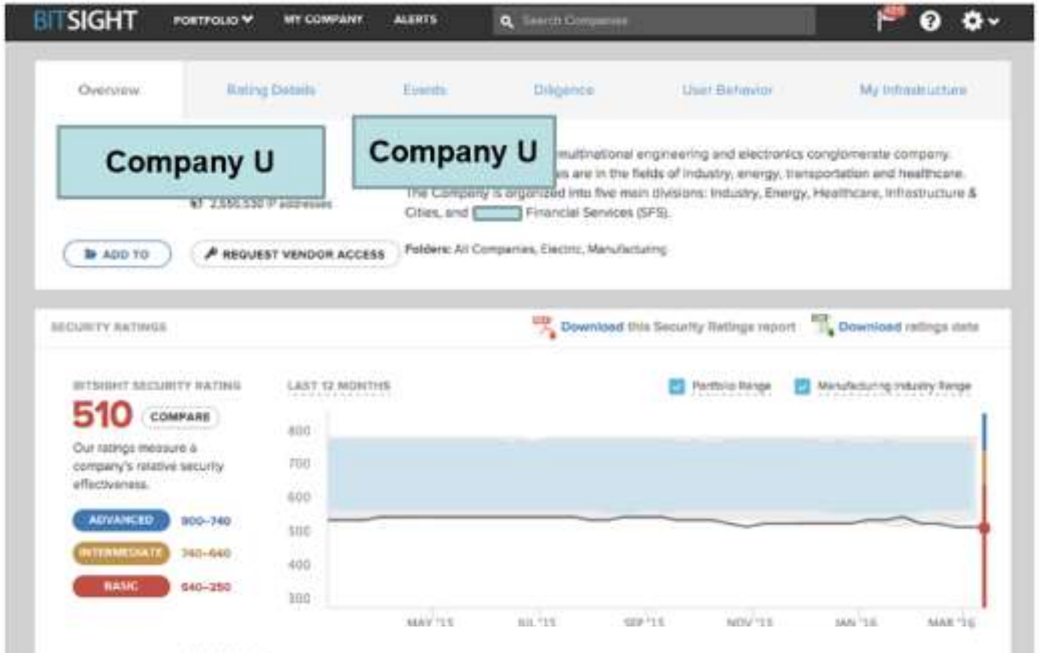
Hack the Pentagon—Pilot Statistics

24 days

***Cost: $175K vs. Typical Contractor $1M***

# "Cyber Trust" Rating…What's Yours?

- Rating # Correlates to Breach Potential
- Detailed Event and Configuration Information via External Parties



Company U

2,330,530 IP addresses

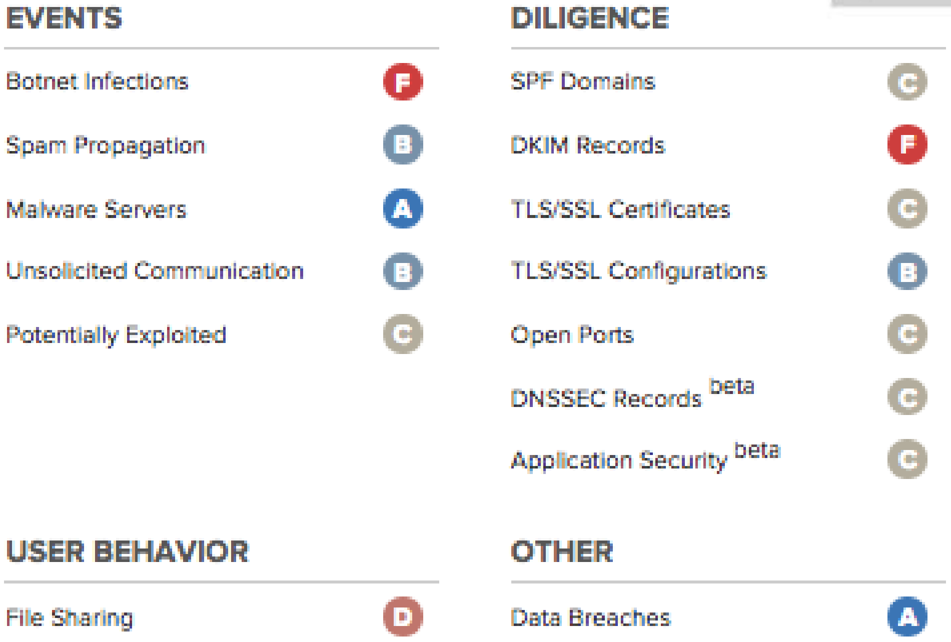
Company U multinational engineering and electronics conglomerate company. …s are in the fields of industry, energy, transportation and healthcare. The Company is organized into five main divisions: Industry, Energy, Healthcare, Infrastructure & Cities, and [redacted] Financial Services (SFS).

Folders: All Companies, Electric, Manufacturing

510

Our ratings measure a company's relative security effectiveness.

| | |
|---|---|
| ADVANCED | 900–740 |
| INTERMEDIATE | 740–640 |
| BASIC | 640–250 |

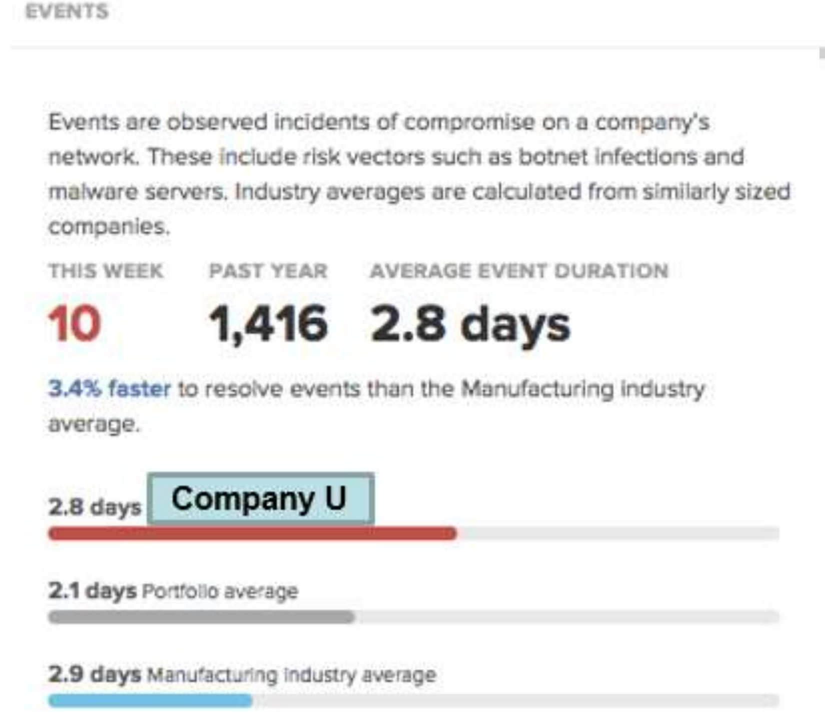


| EVENTS | |
|---|---|
| Botnet Infections | F |
| Spam Propagation | B |
| Malware Servers | A |
| Unsolicited Communication | B |
| Potentially Exploited | C |

| DILIGENCE | |
|---|---|
| SPF Domains | C |
| DKIM Records | F |
| TLS/SSL Certificates | C |
| TLS/SSL Configurations | B |
| Open Ports | C |
| DNSSEC Records beta | C |
| Application Security beta | C |

| USER BEHAVIOR | |
|---|---|
| File Sharing | D |

| OTHER | |
|---|---|
| Data Breaches | A |



EVENTS

Events are observed incidents of compromise on a company's network. These include risk vectors such as botnet infections and malware servers. Industry averages are calculated from similarly sized companies.

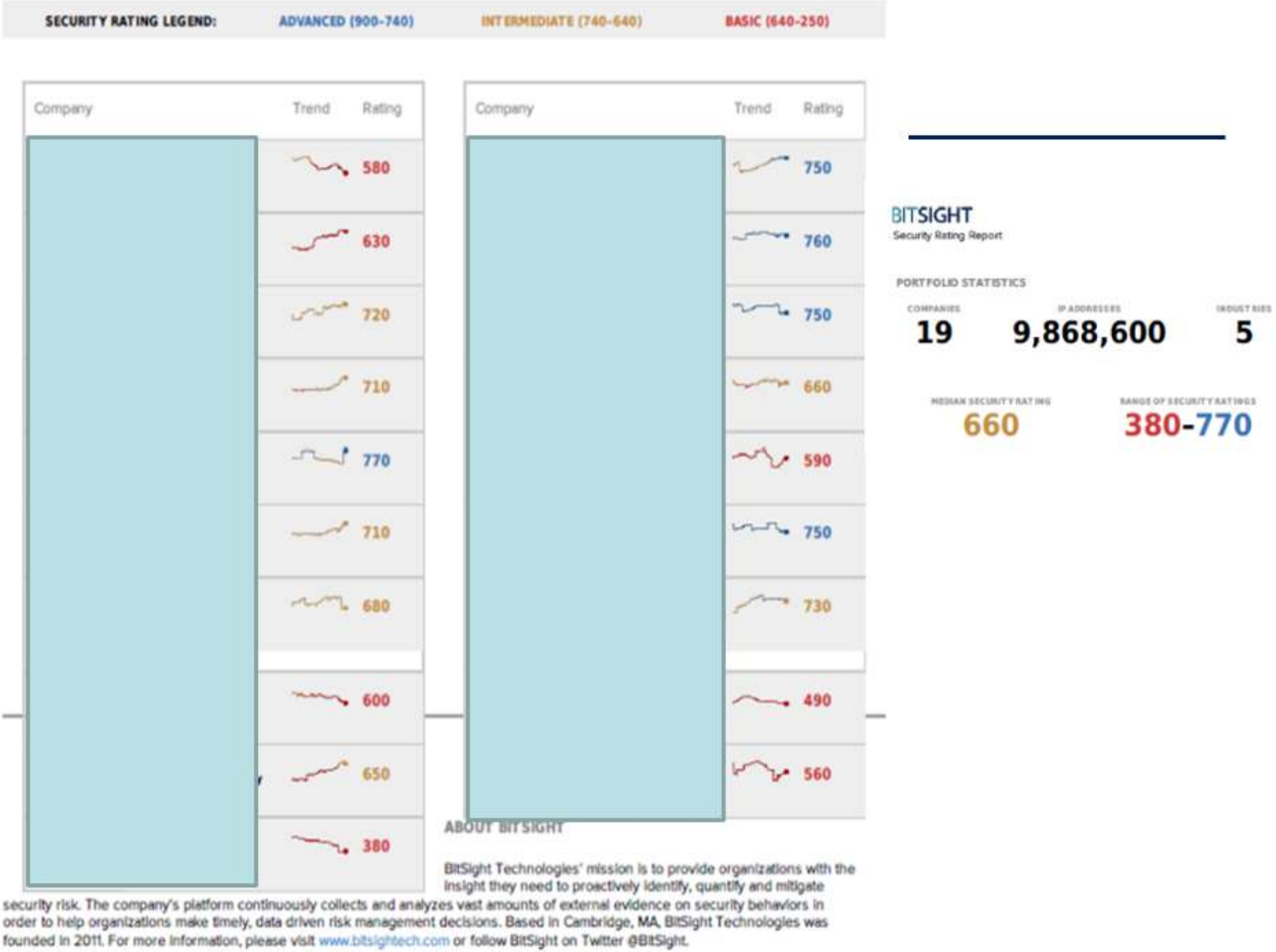
| THIS WEEK | PAST YEAR | AVERAGE EVENT DURATION |
|---|---|---|
| 10 | 1,416 | 2.8 days |

3.4% faster to resolve events than the Manufacturing industry average.

2.8 days Company U

2.1 days Portfolio average

2.9 days Manufacturing industry average



**SECURITY RATING LEGEND:** ADVANCED (900-740) INTERMEDIATE (740-640) BASIC (640-250)

| Company | Trend | Rating |
|---|---|---|
| [redacted] | | 580 |
| [redacted] | | 630 |
| [redacted] | | 720 |
| [redacted] | | 710 |
| [redacted] | | 770 |
| [redacted] | | 710 |
| [redacted] | | 680 |
| [redacted] | | 600 |
| [redacted] | | 650 |
| [redacted] | | 380 |

| Company | Trend | Rating |
|---|---|---|
| [redacted] | | 750 |
| [redacted] | | 760 |
| [redacted] | | 750 |
| [redacted] | | 660 |
| [redacted] | | 590 |
| [redacted] | | 750 |
| [redacted] | | 730 |
| [redacted] | | 490 |
| [redacted] | | 560 |

BITSIGHT
Security Rating Report

PORTFOLIO STATISTICS

| COMPANIES | IP ADDRESSES | INDUSTRIES |
|---|---|---|
| 19 | 9,868,600 | 5 |

| MEDIAN SECURITY RATING | RANGE OF SECURITY RATINGS |
|---|---|
| 660 | 380-770 |

ABOUT BITSIGHT

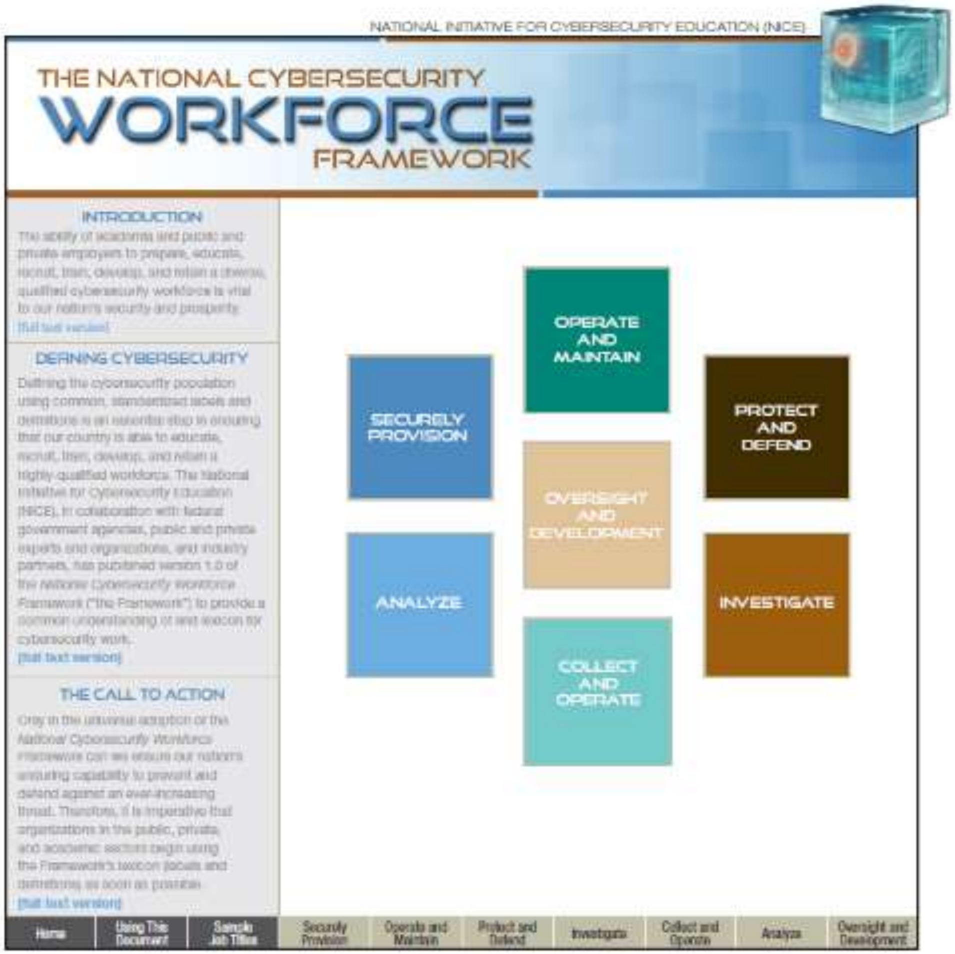
BitSight Technologies' mission is to provide organizations with the insight they need to proactively identify, quantify and mitigate security risk. The company's platform continuously collects and analyzes vast amounts of external evidence on security behaviors in order to help organizations make timely, data driven risk management decisions. Based in Cambridge, MA, BitSight Technologies was founded in 2011. For more information, please visit www.bitsightech.com or follow BitSight on Twitter @BitSight.

# DoD 8140 – Cyberspace Workforce Mgt

“Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements.”

***DoDM 8570 changed to DoDD 8140 Cyberspace Workforce Management – Authorizing Officials (AO) will need “Specialized Skills and Knowledge”***

# Workforce Cyber Skills –
# NIST National Initiative for Cybersecurity Education



NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a diverse, qualified cybersecurity workforce is vital to our nation's security and prosperity.
[full text version]

DEFINING CYBERSECURITY

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the National Cybersecurity Workforce Framework ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.
[full text version]

THE CALL TO ACTION

Only by the universal adoption of the National Cybersecurity Workforce Framework can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.
[full text version]

**Collect and Analyze Data** Capture cybersecurity workforce and training data to understand capabilities and needs.

**Recruit and Retain** Incentivize the hiring and retention of highly skilled and adaptive professionals needed for a secure digital nation.

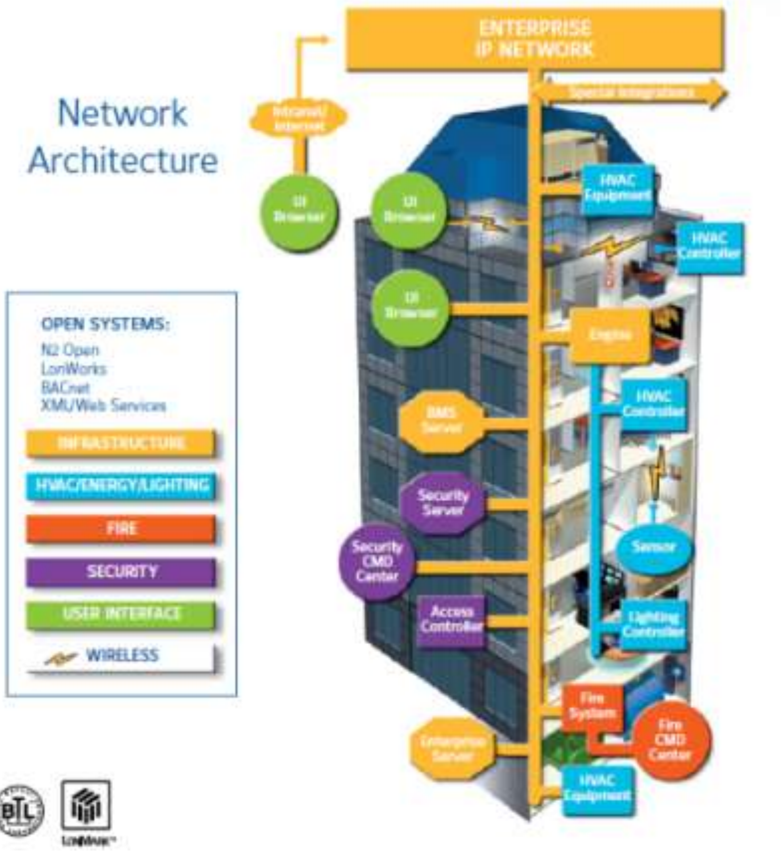
**Educate, Train, and Develop** Expand the pipeline for and deliberately develop an unrivaled cybersecurity workforce.

**Engage Educate and Energize** all cybersecurity workforces and the American public to strengthen the nation's front lines of cybersecurity.

# Workforce Cyber Skills – Controls Systems, PIT, OT

## Securely Provision

- Information Assurance (IA) Compliance
- Software Assurance and Security Engineering
- Systems Security Architecture
- Technology Research and Development
- Systems Requirements Planning
- Test and Evaluation
- Systems Development



## Operate and Maintain

- Data Administration
- Knowledge Management
- Customer Service and Technical Support
- Network Services
- System Administration
- Systems Security Analysis

## Protect and Defend

- Computer Network Defense (CND) Analysis
- Incident Response
- Computer Network Defense (CND) Infrastructure Support
- Vulnerability Assessment and Management

# You think you are doing fine?

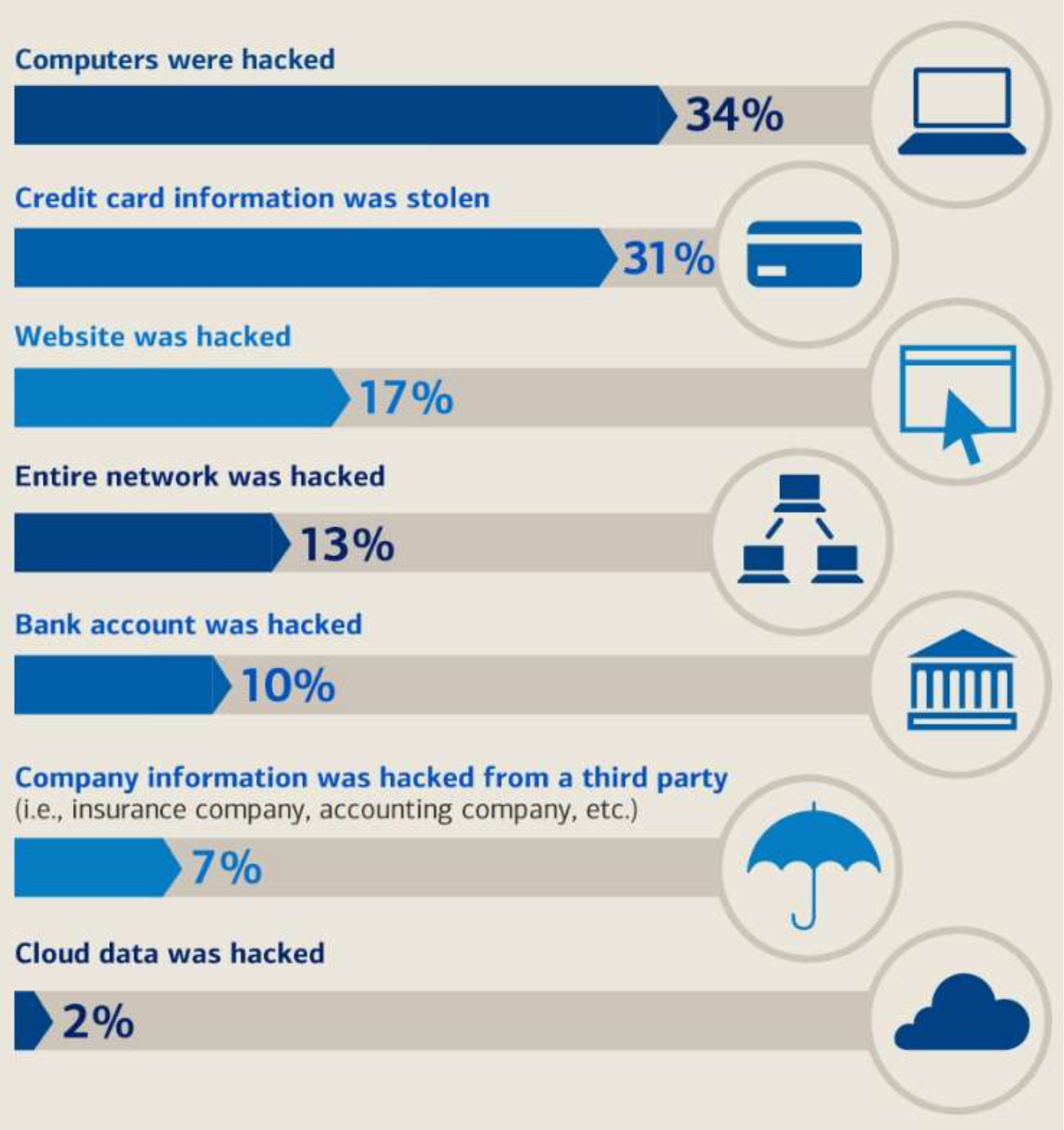
Nothing could be further than the truth

Often, small and midsize businesses don't have the resources to invest in robust security measures, making them attractive targets to cybercriminals and leading to devastating results.

A 2015 survey by Bank of America found that 12% of small business owners were victims of cyberbreaches, while another report estimated that 60% of small businesses close within six months of a cyberattack.

# Cyberattack Weak Spots

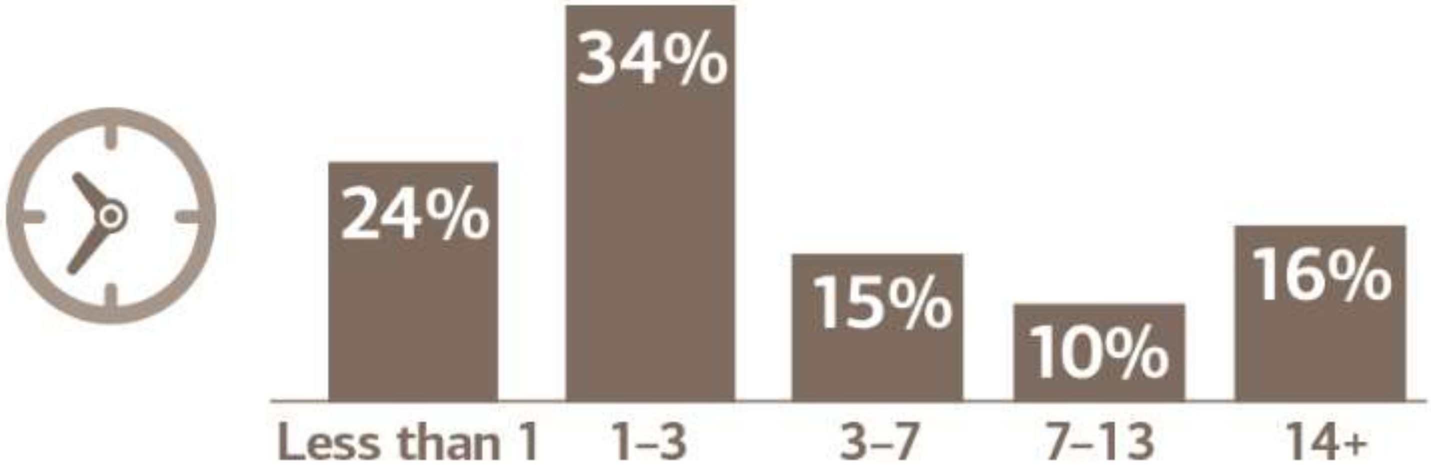
**Keep in mind**
A 2014 report by Verizon found that 11% of attacks from inside a business took over a month to be detected.



# The Impact

## Time spent on cyberattacks (in days)[3]

Resolving cyberattacks took small business owners on average:



?

Average cost to a small or midsize business to recover from a secruity breach?

$38,000

# Contract Cybersecurity Risk Management Plan

The ultimate objective of an organization-wide risk management program is to enable the organization to conduct it’s day-to-day operations and accomplish its missions within a secure environment commensurate with risk.

Why is security risk management important? Attacks on information systems today are often well-organized, disciplined, aggressive, well-funded, and extremely sophisticated. Successful attacks on public and private sector information systems can result in harm to U.S. National and economic security interests.

Given the significant danger of these attacks, all individuals within the organization must understand their responsibilities in managing the risk from operating information systems that support the mission / business functions of the organizations, and take responsibility for risk consequences and mitigation.

# Contract Cybersecurity Risk Management Plan

The contractor shall provide a Contract Cybersecurity Risk Management Plan (CCRMP) containing documentation sufficient to demonstrate its systematic and organizational ability to provide solutions that include appropriate security controls for any task within the scope of the contract. The CCRMP shall also describe how these are related to the organization's enterprise approach to risk management, and how its approach to cybersecurity risk management provides appropriate assurance for the types of deliverables it intends to provide under the contract.

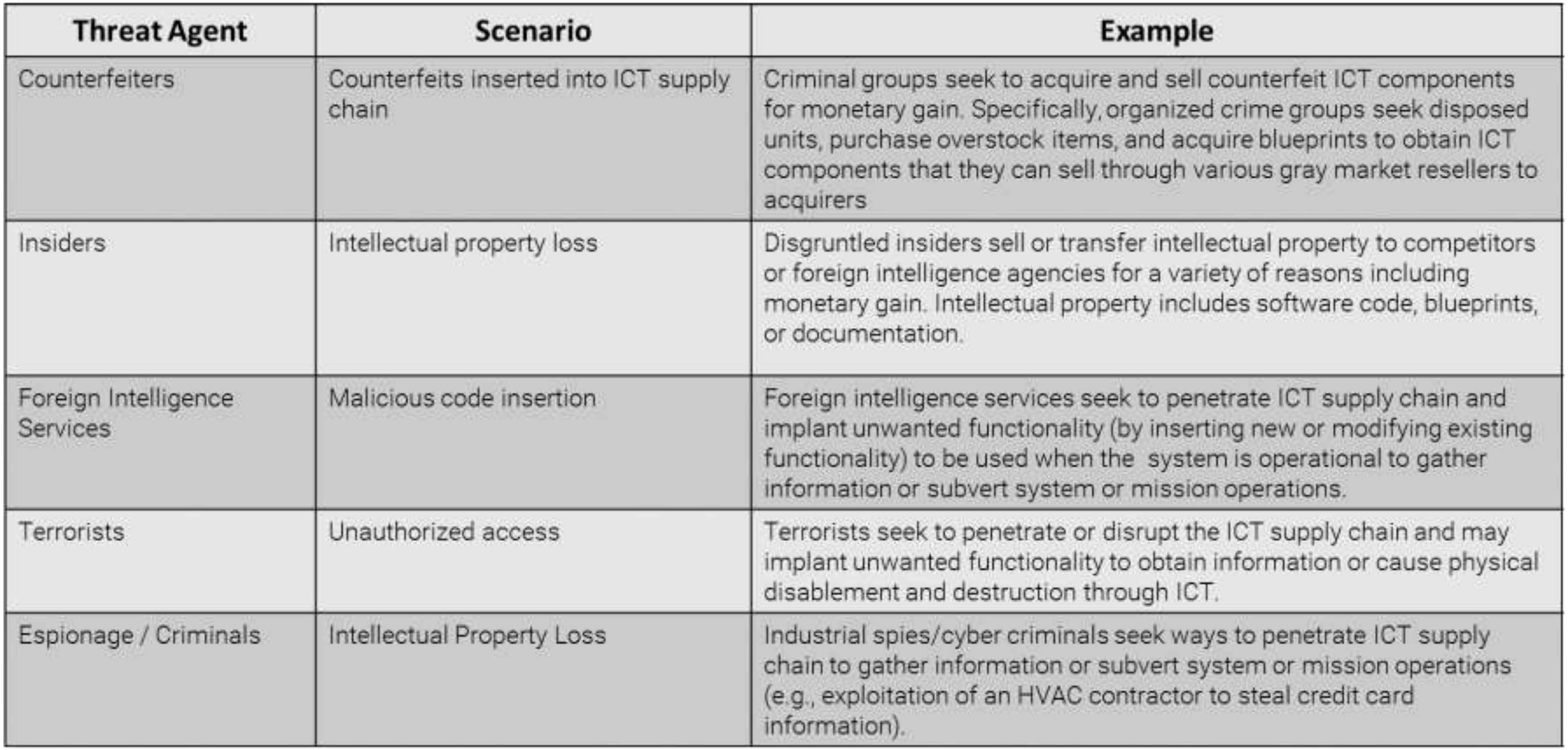
All Contract Cybersecurity Risk Management Plans shall be submitted with the proposal.

# Supply Chain Risk Management

The New Insider Threat?  Is not a person, it's information and communications technology (ICT).

The complexities, including lack of visibility and traceability of the global supply chain, creates security challenges that dramatically increase vulnerabilities adversaries seek to exploit for purposes of sabotage and espionage.

# Threat Landscape



| Threat Agent | Scenario | Example |
|---|---|---|
| Counterfeiters | Counterfeits inserted into ICT supply chain | Criminal groups seek to acquire and sell counterfeit ICT components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain ICT components that they can sell through various gray market resellers to acquirers |
| Insiders | Intellectual property loss | Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation. |
| Foreign Intelligence Services | Malicious code insertion | Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be used when the system is operational to gather information or subvert system or mission operations. |
| Terrorists | Unauthorized access | Terrorists seek to penetrate or disrupt the ICT supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction through ICT. |
| Espionage / Criminals | Intellectual Property Loss | Industrial spies/cyber criminals seek ways to penetrate ICT supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information). |

# Controls System Reference Architecture

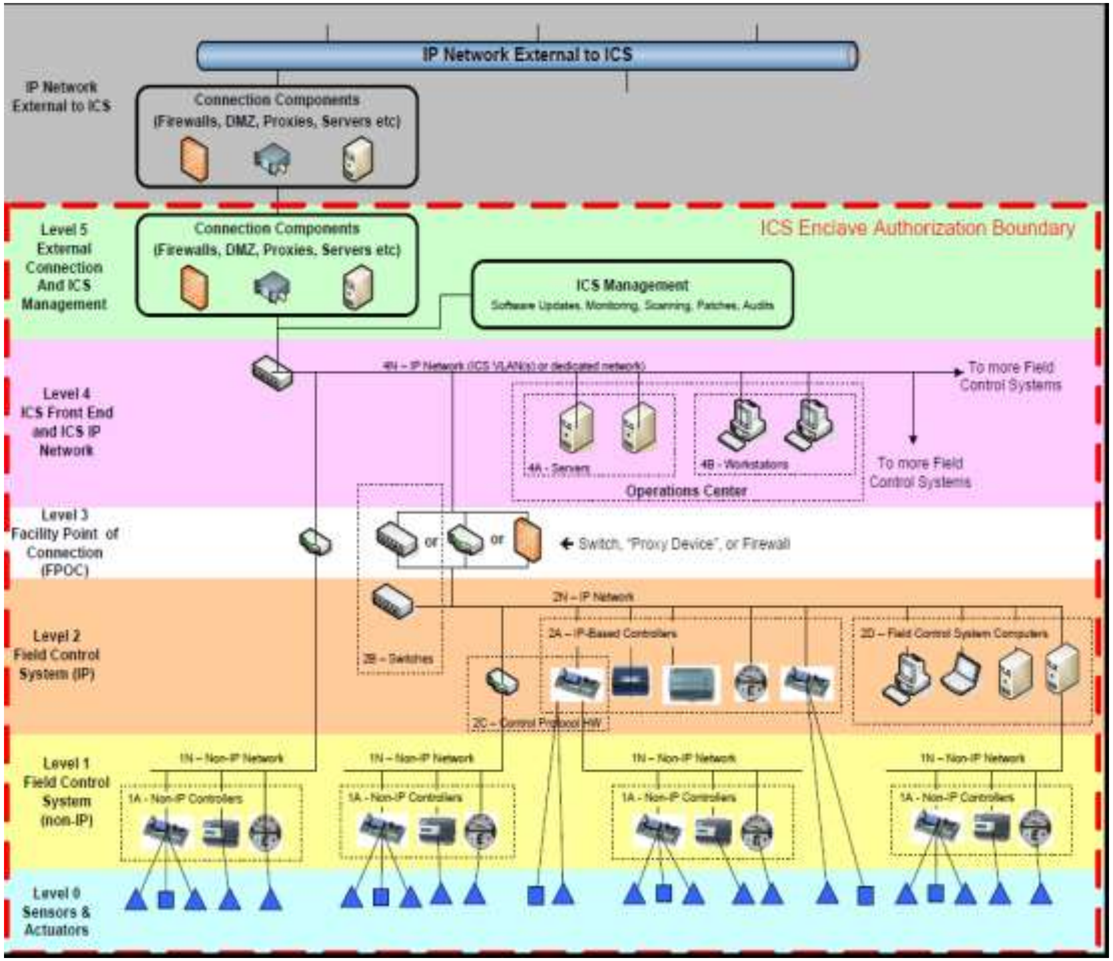
Each individual component or piece of hardware or software contributes to the overall mission and thus is a potential vulnerability.

Client Side Attacks

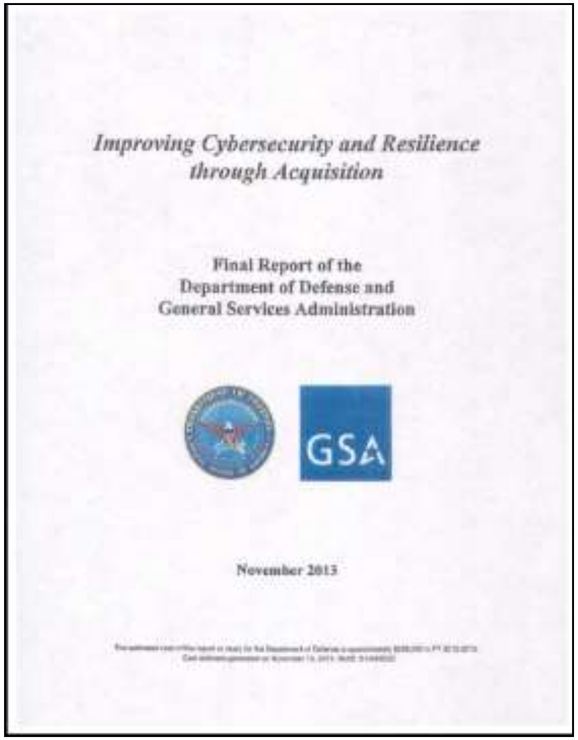
Server Side Attacks

Network Attacks

Hardware Attacks


IP Network External to ICS
IP Network External to ICS
Connection Components
(Firewalls, DMZ, Proxies, Servers etc)
ICS Enclave Authorization Boundary
Level 5 External Connection And ICS Management
Connection Components
(Firewalls, DMZ, Proxies, Servers etc)
ICS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 ICS Front End and ICS IP Network
4N – IP Network (ICS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
To more Field Control Systems
Operations Center
Level 3 Facility Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
Level 0 Sensors & Actuators

# Acquisition Reform



*Improving Cybersecurity and Resilience through Acquisition*

Final Report of the
Department of Defense and
General Services Administration

November 2013

[illegible]
[illegible]

## Six reform recommendations:

1. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions

2. Include cybersecurity in acquisition training

3. Develop common cybersecurity definitions for federal acquisitions

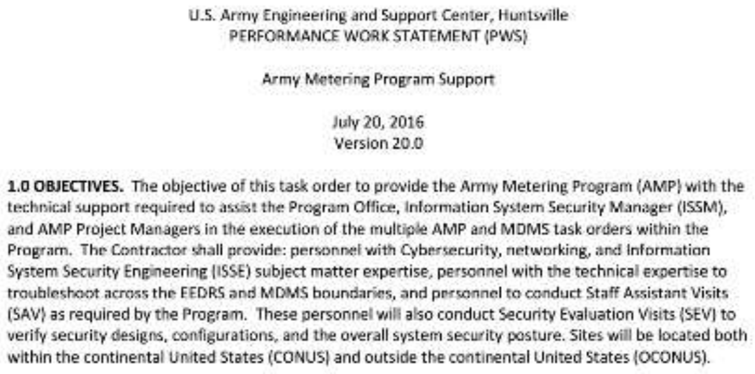
4. Institute a federal acquisition cyber risk management strategy

5. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources

6. Increase government accountability for cyber risk management

***http://www.gsa.gov/portal/content/176547***

# RMF RFP’s and PWS

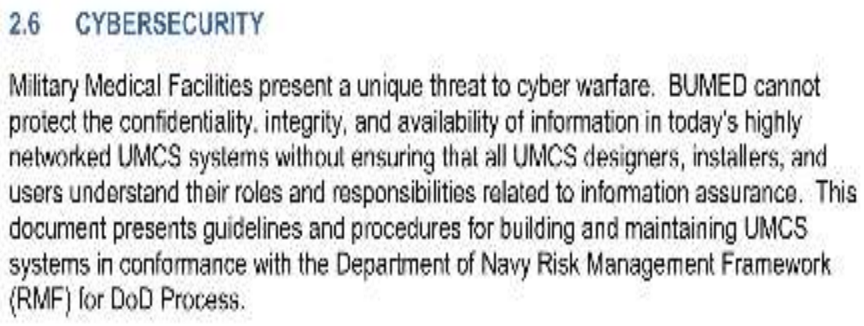


U.S. Army Engineering and Support Center, Huntsville
PERFORMANCE WORK STATEMENT (PWS)

Army Metering Program Support

July 20, 2016
Version 20.0

**1.0 OBJECTIVES.** The objective of this task order to provide the Army Metering Program (AMP) with the technical support required to assist the Program Office, Information System Security Manager (ISSM), and AMP Project Managers in the execution of the multiple AMP and MDMS task orders within the Program. The Contractor shall provide: personnel with Cybersecurity, networking, and Information System Security Engineering (ISSE) subject matter expertise, personnel with the technical expertise to troubleshoot across the EEDRS and MDMS boundaries, and personnel to conduct Staff Assistant Visits (SAV) as required by the Program. These personnel will also conduct Security Evaluation Visits (SEV) to verify security designs, configurations, and the overall system security posture. Sites will be located both within the continental United States (CONUS) and outside the continental United States (OCONUS).



## 2.6 CYBERSECURITY

Military Medical Facilities present a unique threat to cyber warfare. BUMED cannot protect the confidentiality, integrity, and availability of information in today’s highly networked UMCS systems without ensuring that all UMCS designers, installers, and users understand their roles and responsibilities related to information assurance. This document presents guidelines and procedures for building and maintaining UMCS systems in conformance with the Department of Navy Risk Management Framework (RMF) for DoD Process.

[illegible] IN SUPPORT OF THE UTILITY MONITORING AND CONTROL SYSTEMS (UMCS) PROGRAM, THE ELECTRONIC SECURITY SYSTEMS (ESS) PROGRAM, AND THE ARMY METERING PROGRAM (AMP)

https://www.fbo.gov/index?s=opportunity&mode=form&id=f32ae504fba609e15ec84adc9c6ec812&tab=core&_cview=0

# Guidelines For Facility-Related Controls Systems – Subject Matter Experts

**Control Systems Cybersecurity Specialist:** The Control Systems Cybersecurity specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Global Industrial Cyber Security Professional (GISCP) or Certified Information Systems Security Professional (CISSP).

**Information and Communication Technology Specialist:** The Information and Communication Technology specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Registered Communications Distribution Designer (RCDD®).

**System Integration Specialist:** The System Integration specialist shall have a minimum of five years' experience in control system network and shall maintain current certification as a Certified System Integrator (CSI) for the products they are integrating and/or be Control System Integrators Association (CISA) Certified.

# Guidelines For Facility-Related Controls Systems – Subject Matter Experts

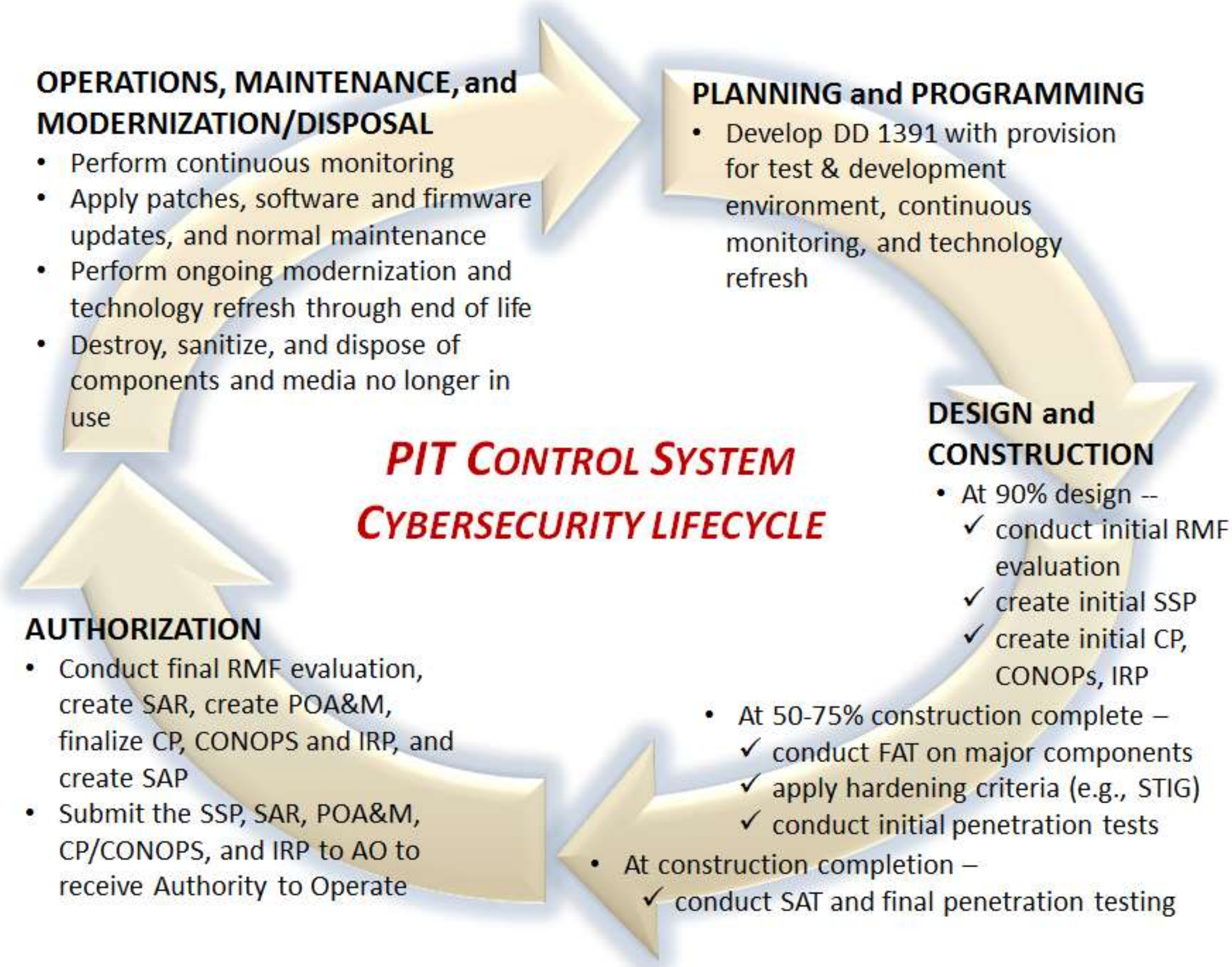
**Systems Security Engineering (SSE),** a specialty discipline within systems engineering, supports the development of programs and design-to-specifications that provide life cycle protection for critical defense resources.

The primary vehicle for integrating systems security engineering into systems engineering processes during the Acquisition life cycle is program protection planning.

Programs perform criticality analysis to identify their systems' mission-critical functions and components; assess threats, vulnerabilities, risks, and impacts; and select and apply countermeasures and mitigations.

***http://www.gsa.gov/portal/content/176547***

# Control System Cyber Lifecycle



**OPERATIONS, MAINTENANCE, and MODERNIZATION/DISPOSAL**

- Perform continuous monitoring
- Apply patches, software and firmware updates, and normal maintenance
- Perform ongoing modernization and technology refresh through end of life
- Destroy, sanitize, and dispose of components and media no longer in use

**PLANNING and PROGRAMMING**

- Develop DD 1391 with provision for test & development environment, continuous monitoring, and technology refresh

**PIT CONTROL SYSTEM CYBERSECURITY LIFECYCLE**

**DESIGN and CONSTRUCTION**

- At 90% design --
  - ✓ conduct initial RMF evaluation
  - ✓ create initial SSP
  - ✓ create initial CP, CONOPs, IRP
- At 50-75% construction complete –
  - ✓ conduct FAT on major components
  - ✓ apply hardening criteria (e.g., STIG)
  - ✓ conduct initial penetration tests
- At construction completion –
  - ✓ conduct SAT and final penetration testing

**AUTHORIZATION**

- Conduct final RMF evaluation, create SAR, create POA&M, finalize CP, CONOPS and IRP, and create SAP
- Submit the SSP, SAR, POA&M, CP/CONOPS, and IRP to AO to receive Authority to Operate

# What’s Next?

All intelligent electronic devices must be protected for the entire system lifecycle from raw goods to end user; conception to decommissioning

Agency CIOs are developing their risk mitigation plans for reducing risk in the supply chain. This includes the “people” and the “goods”

- Supply Chain Risk Management (NIST SP 800-161)
- Acquisition and contract language to require contractors and vendors IT Business Systems to meet DoD standards (NIST SP 800-171) per DFAR 2015 Compliance Date: Dec 2017

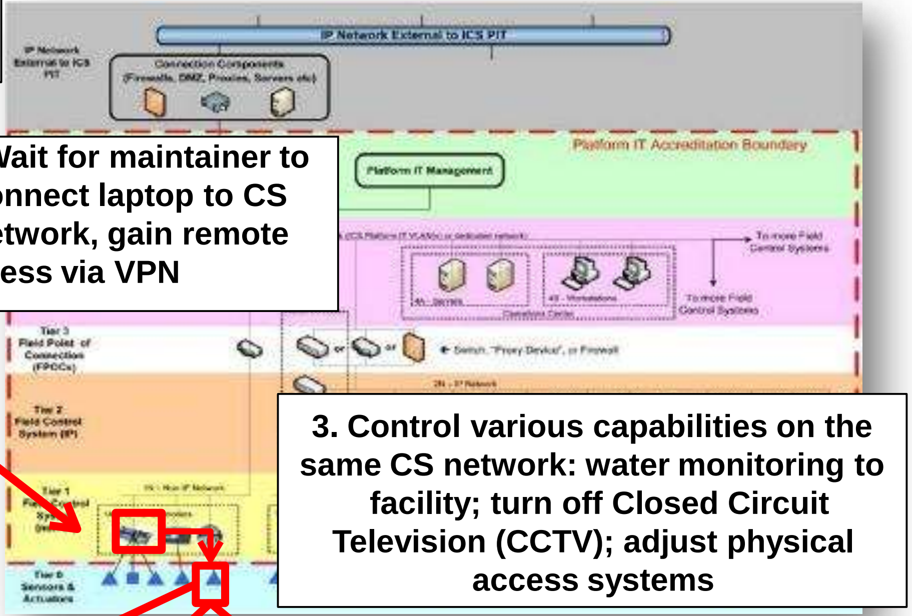
FARS will require Contract Cyber Risk Management Plans (CCRMPs) for all actors in the supply chain by Dec 2017 in order to respond to any solicitation with the Federal Government

- All agencies are in the process of training qualified staff to perform security control assessments and continuous monitoring of controls systems
- All designers and contractors must have qualified staff to design, procure, and install controls systems that will meet these cyber security requirements

# Illustrative Scenario: Remote Control of Similar Systems on Same CS Network

1. Target an internet connected maintenance laptop with malware

2. Wait for maintainer to connect laptop to CS network, gain remote access via VPN


IP Network External to ICS PIT
IP Network External to ICS PIT
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Platform IT Accreditation Boundary
Platform IT Management
ICS Platform IT VLAN(s) or dedicated network
To more Field Control Systems
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Tier 3 Field Point of Connection (FPOCs)
or
or
Switch, "Proxy Device", or Firewall
2N - IP Network
Tier 2 Field Control System (IP)
Tier 1 Field Control System
1N - Non IP Network
Tier 0 Sensors & Actuators

3. Control various capabilities on the same CS network: water monitoring to facility; turn off Closed Circuit Television (CCTV); adjust physical access systems

Results in

4. Results in preparations for unauthorized entry to enable physical theft and/or damage to facility

- Specific Attack: Exploit Windows 7 maintenance laptop for VPN access to CS networks
- Level of Effort: DSB Tier 2; novice capability to access CS network and breach the controlled facility
- Impact: Targeting a maintenance worker's system can allow internal access to facility CS

# DoD & Commercial Resources

**DoD CIO Knowledge Service (requires CAC)** **https://rmfks.osd.mil/login.htm**

**Department of Defense Advanced Control System Tactics, Techniques, and Procedures (TTPs) 2016:**

**https://www.cybercom.mil/ICSTTP/Forms/AllItems.aspx**

**UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS Sept 2016**

**https://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06**

**Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) [info & funding solicitations]**

**https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines**

**DoD OASD(EI&E) and Federal Facilities Council (FFC), under the National Research Council (NRC) sponsored a 3-day Building Control System Cyber Resilience Forum in Nov '15.**

**http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792**

**DoDI 5000.02 Cybersecurity in the Defense Acquisition System Jan 2017**

**http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf**

**Whole Building Design Guide website cyber references**

**http://www.wbdg.org/resources/cybersecurity**

**Tools**

**https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A**

**https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B**

**Workshops / Building Control Systems Cyber Security Training**

**http://hpac.com/training/workshop-what-do-when-building-control-systems-get-hacked-set**

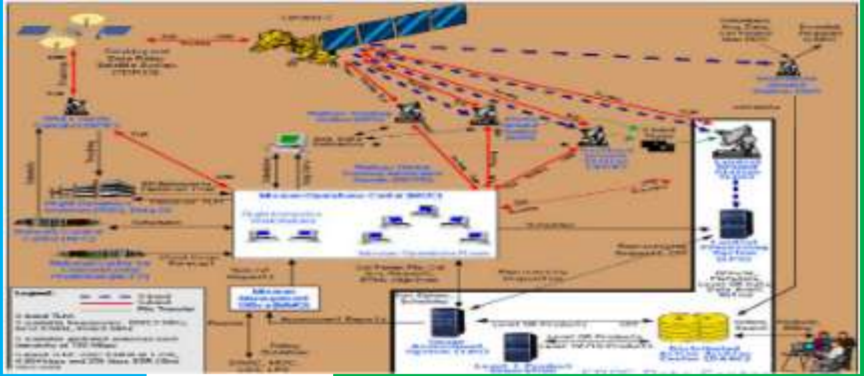
**Industrial Control Systems Joint Working Group (ICSJWG_**

**https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG**

# Discussion

## Information Systems

## Control Systems



Wanda Lenkewich
President, Chinook Systems, Inc.
703-232-6536
wlenkewich@chinooksystems.com

Michael Chipley
President, The PMC Group LLC
571-232-3890
mchipley@pmcgroup.biz

***Who's Role? Detect, Mitigate & Recover from Cyber Exploit***