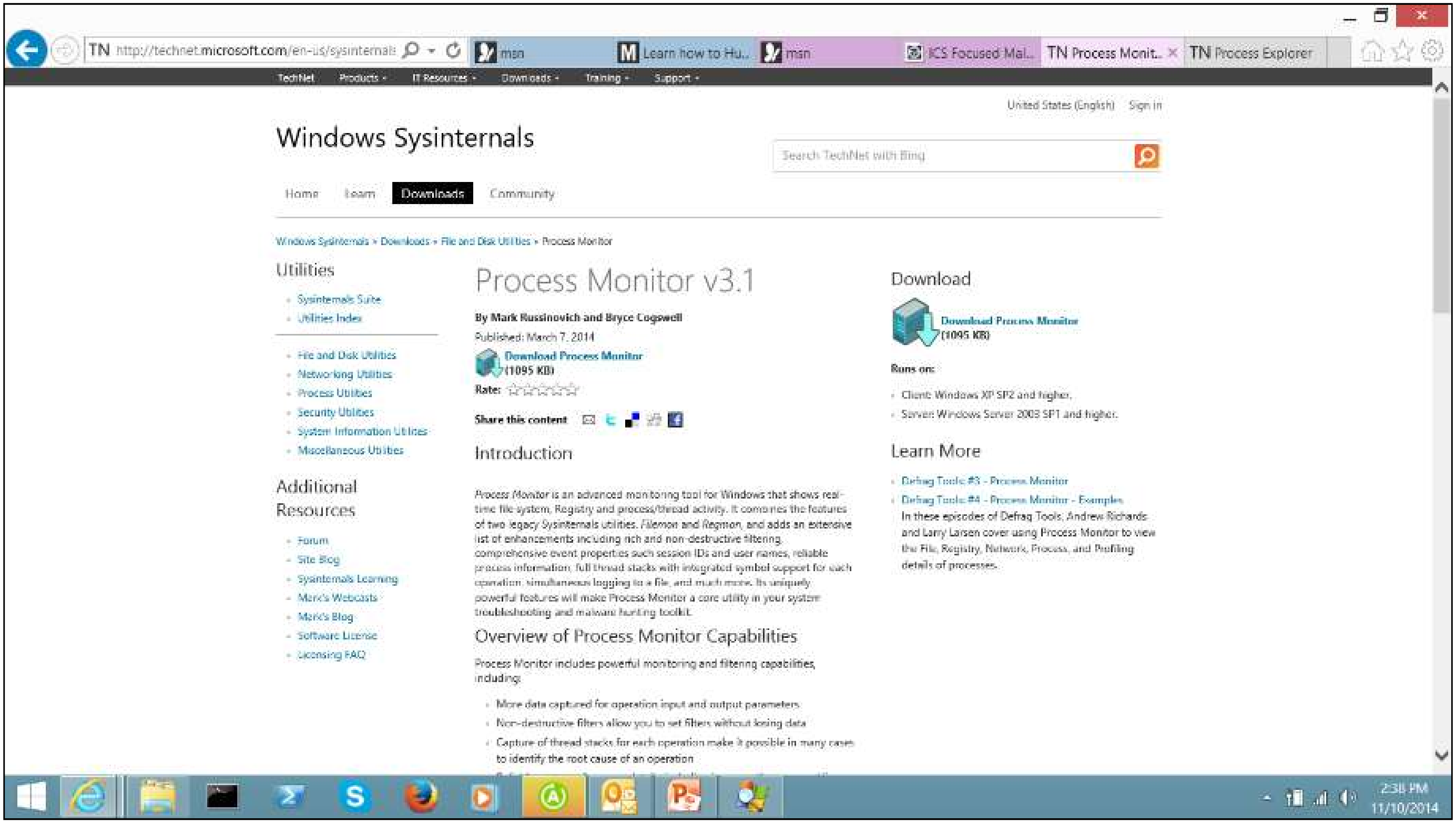
Sysinternals – Process Monitor



Windows Sysinternals

Windows Sysinternals > Downloads > File and Disk Utilities > Process Monitor

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Blog
- Software License
- Licensing FAQ

Process Monitor v3.1

By Mark Russinovich and Bryce Cogswell

Published: March 7, 2014

Download Process Monitor
(1095 KB)

Rate: ☆☆☆☆☆

Share this content

Introduction

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Overview of Process Monitor Capabilities

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation

Download

Download Process Monitor
(1095 KB)

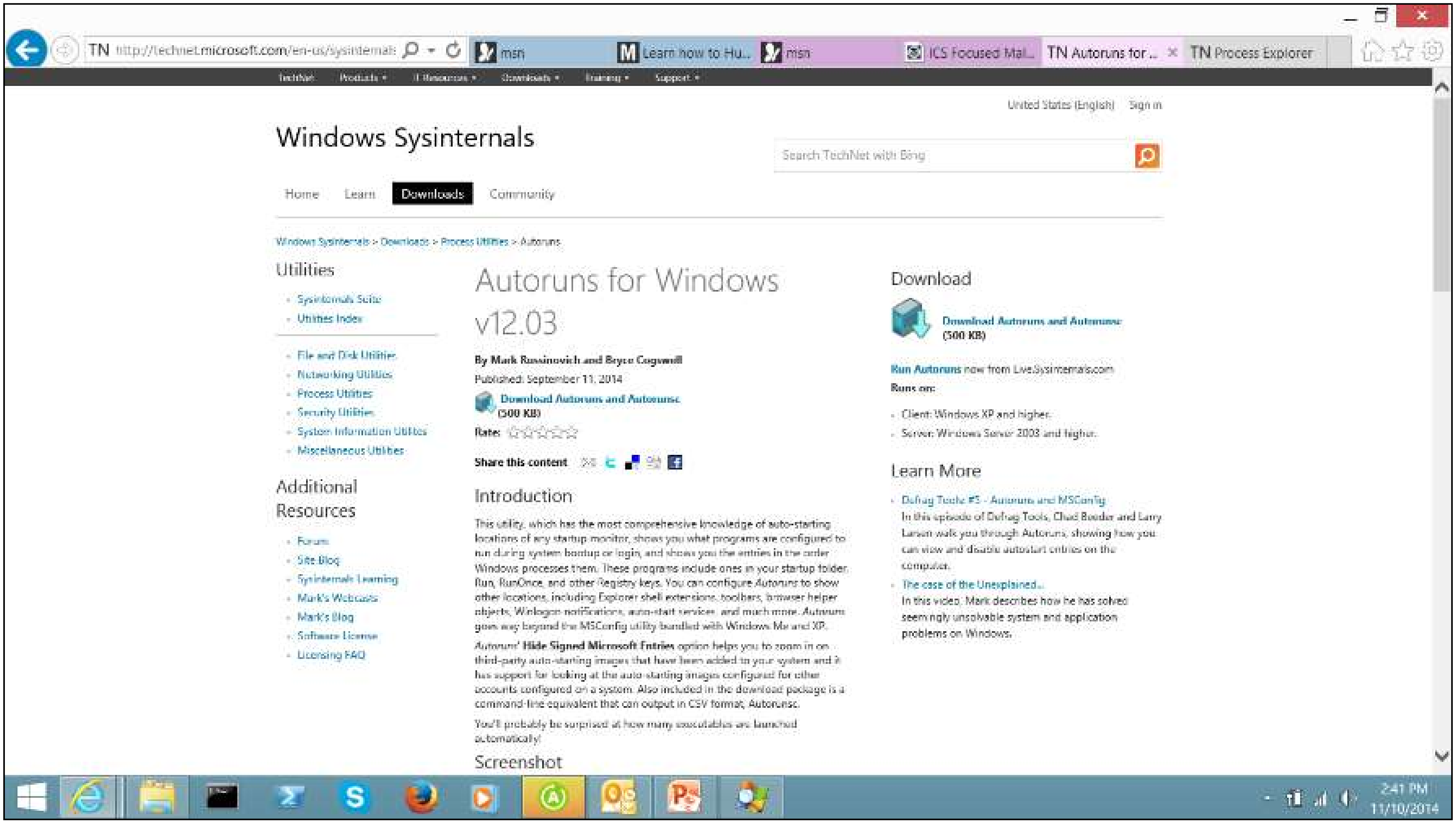
Runs on:

- Client: Windows XP SP2 and higher.
- Server: Windows Server 2003 SP1 and higher.

Learn More

- Defrag Tools: #3 - Process Monitor
- Defrag Tools: #4 - Process Monitor - Examples
  In these episodes of Defrag Tools, Andrew Richards and Larry Larsen cover using Process Monitor to view the File, Registry, Network, Process, and Profiling details of processes.

Sysinternals - Autoruns



Windows Sysinternals

Autoruns for Windows v12.03

By Mark Russinovich and Bryce Cogswell

Published: September 11, 2014

Download Autoruns and Autorunsc
(500 KB)

Introduction

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and shows you the entries in the order Windows processes them. These programs include ones in your startup folder, Run, RunOnce, and other Registry keys. You can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. Autoruns goes way beyond the MSConfig utility bundled with Windows Me and XP.

Autoruns' **Hide Signed Microsoft Entries** option helps you to zoom in on third-party auto-starting images that have been added to your system and it has support for looking at the auto-starting images configured for other accounts configured on a system. Also included in the download package is a command-line equivalent that can output in CSV format, Autorunsc.

You'll probably be surprised at how many executables are launched automatically!

Screenshot

Download

Download Autoruns and Autorunsc
(500 KB)

Run Autoruns now from Live.Sysinternals.com

Runs on:

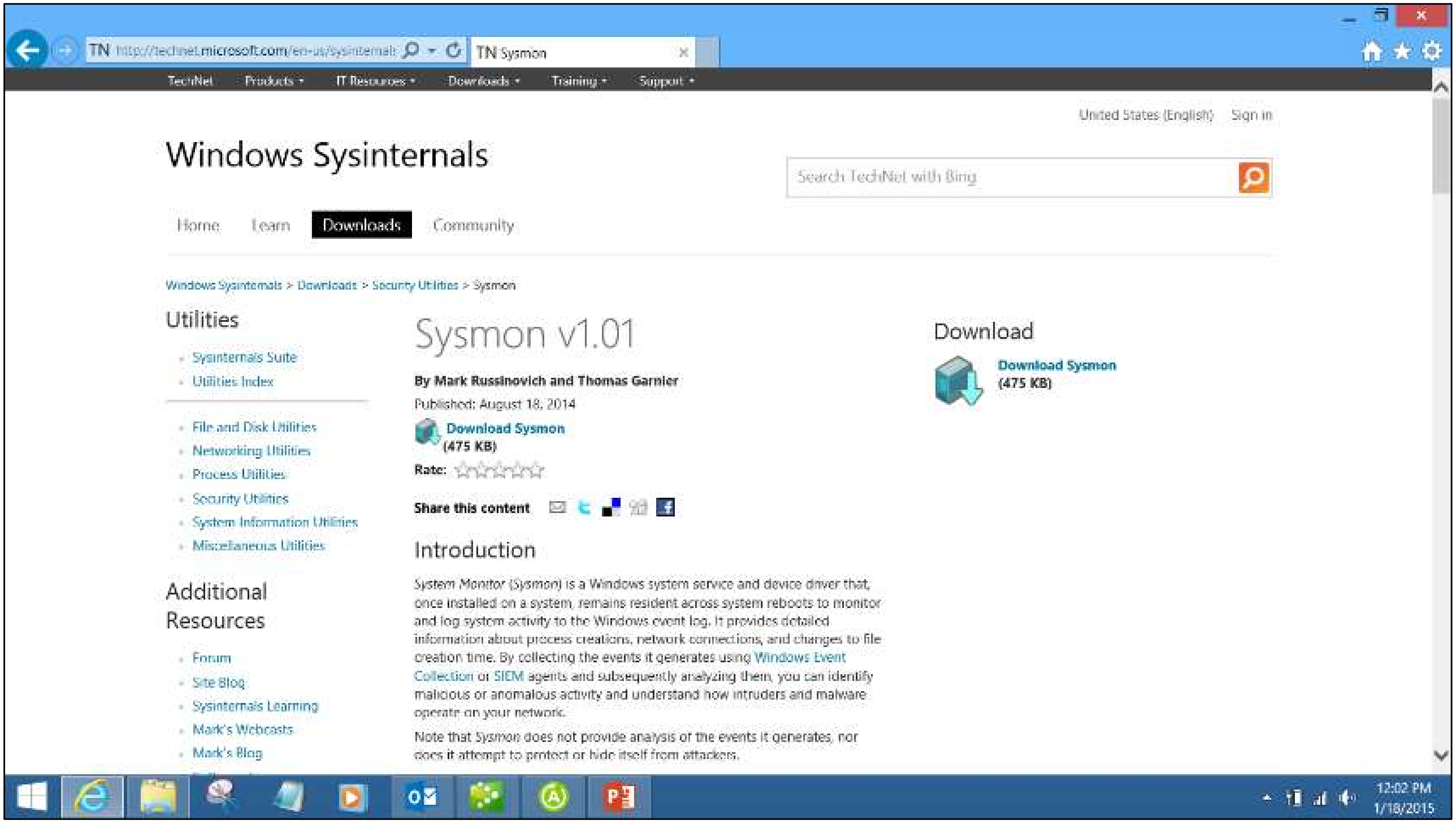
- Client: Windows XP and higher.
- Server: Windows Server 2003 and higher.

Learn More

- Defrag Tools: #5 - Autoruns and MSConfig
  In this episode of Defrag Tools, Chad Beeder and Larry Larsen walk you through Autoruns, showing how you can view and disable autostart entries on the computer.
- The case of the Unexplained...
  In this video, Mark describes how he has solved seemingly unsolvable system and application problems on Windows.

http://technet.microsoft.com/en-us/sysinternals/bb963902

Sysinternals – Sysmon v1.0



Windows Sysinternals

Windows Sysinternals > Downloads > Security Utilities > Sysmon

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Blog

Sysmon v1.01

By Mark Russinovich and Thomas Garnier

Published: August 18, 2014

Download Sysmon
(475 KB)

Rate: ☆☆☆☆☆

Share this content

Introduction

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

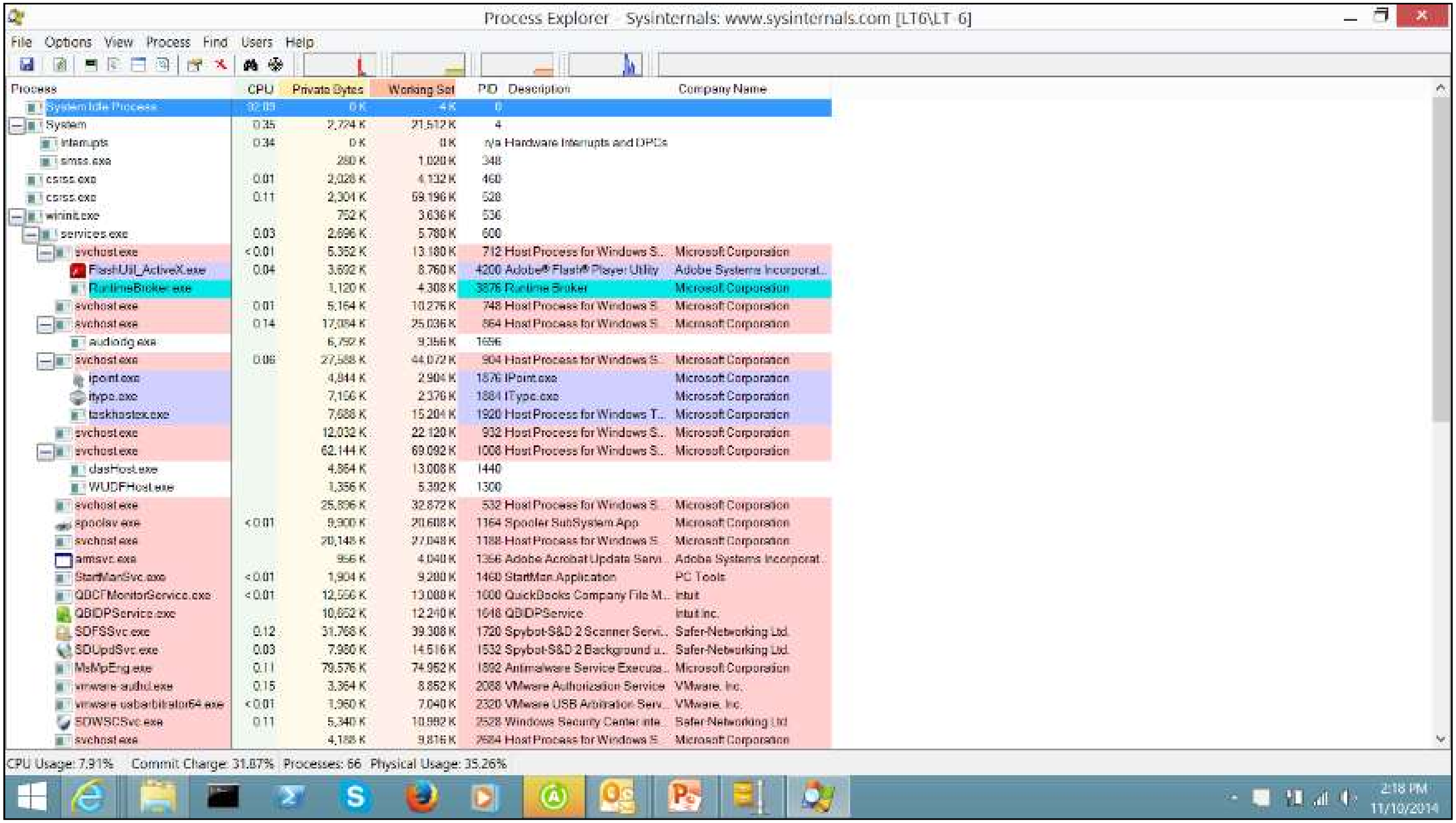
Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Download

Download Sysmon
(475 KB)

http://technet.microsoft.com/en-us/sysinternals/dn798348

Sysinternals Process Explorer

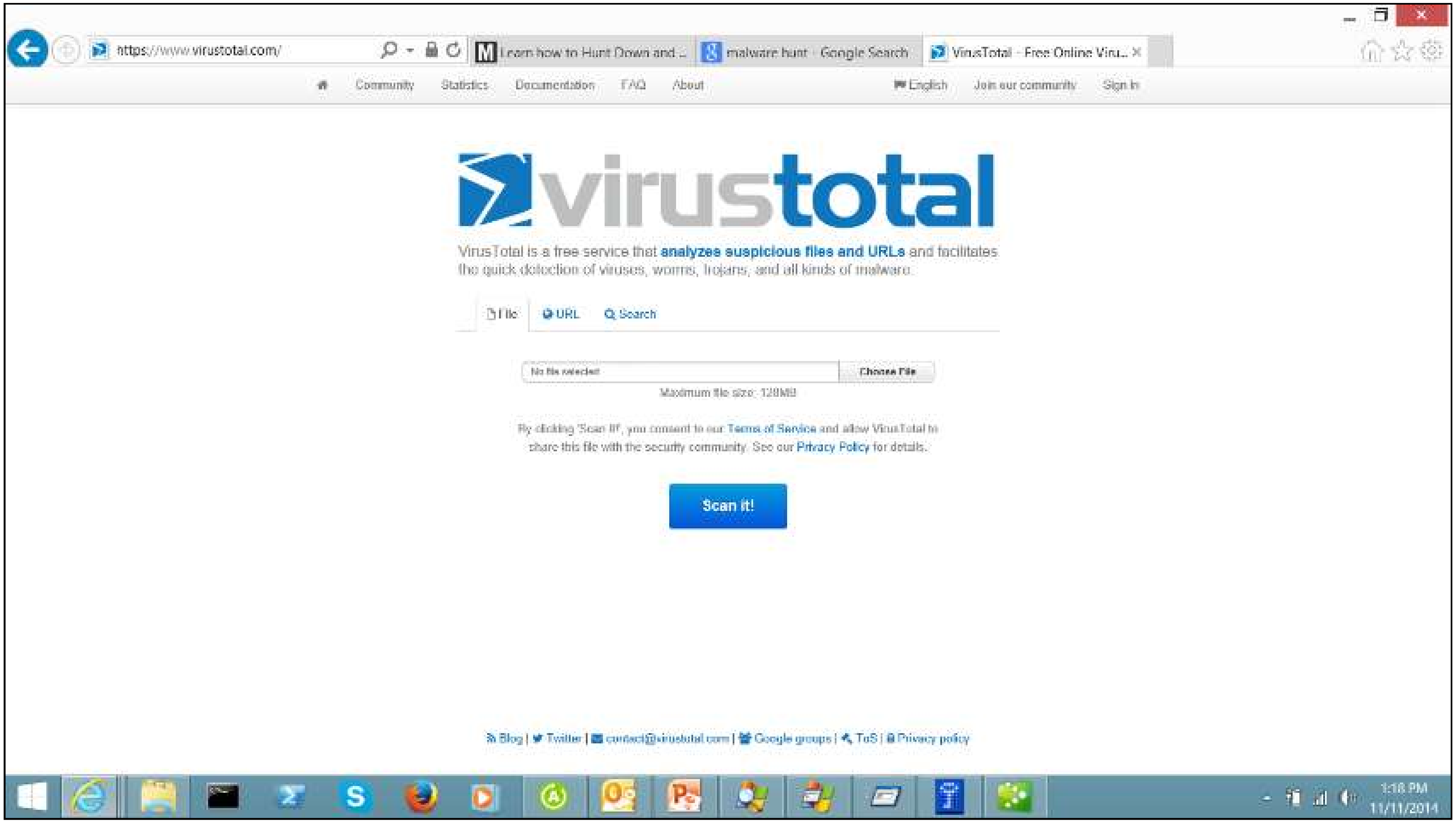

Process Explorer - Sysinternals: www.sysinternals.com [LT6\LT-6]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	92.09	0 K	4 K	0		
System	0.35	2,724 K	21,512 K	4		
Interrupts	0.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		280 K	1,020 K	348		
csrss.exe	0.01	2,028 K	4,132 K	460		
csrss.exe	0.11	2,304 K	59,196 K	528		
wininit.exe		752 K	3,636 K	536		
services.exe	0.03	2,696 K	5,780 K	600		
svchost.exe	< 0.01	5,352 K	13,180 K	712	Host Process for Windows S...	Microsoft Corporation
FlashUtil_ActiveX.exe	0.04	3,692 K	8,760 K	4200	Adobe® Flash® Player Utility	Adobe Systems Incorporat...
RuntimeBroker.exe		1,120 K	4,308 K	3876	Runtime Broker	Microsoft Corporation
svchost.exe	0.01	5,164 K	10,276 K	748	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.14	17,084 K	25,036 K	864	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		6,792 K	9,356 K	1696		
svchost.exe	0.06	27,588 K	44,072 K	904	Host Process for Windows S...	Microsoft Corporation
ipoint.exe		4,844 K	2,904 K	1876	IPoint.exe	Microsoft Corporation
itype.exe		7,156 K	2,376 K	1884	IType.exe	Microsoft Corporation
taskhostex.exe		7,688 K	15,204 K	1920	Host Process for Windows T...	Microsoft Corporation
svchost.exe		12,032 K	22,120 K	932	Host Process for Windows S...	Microsoft Corporation
svchost.exe		62,144 K	69,092 K	1008	Host Process for Windows S...	Microsoft Corporation
dasHost.exe		4,864 K	13,008 K	1440		
WUDFHost.exe		1,356 K	5,392 K	1300		
svchost.exe		25,896 K	32,872 K	532	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	< 0.01	9,900 K	20,608 K	1164	Spooler SubSystem App	Microsoft Corporation
svchost.exe		20,148 K	27,048 K	1188	Host Process for Windows S...	Microsoft Corporation
armsvc.exe		956 K	4,040 K	1356	Adobe Acrobat Update Servi...	Adobe Systems Incorporat...
StartManSvc.exe	< 0.01	1,904 K	9,280 K	1460	StartMan Application	PC Tools
QBCFMonitorService.exe	< 0.01	12,556 K	13,088 K	1600	QuickBooks Company File M...	Intuit
QBIDPService.exe		10,652 K	12,240 K	1648	QBIDPService	Intuit Inc.
SDFSSvc.exe	0.12	31,768 K	39,308 K	1720	Spybot-S&D 2 Scanner Servi...	Safer-Networking Ltd.
SDUpdSvc.exe	0.03	7,980 K	14,516 K	1532	Spybot-S&D 2 Background u...	Safer-Networking Ltd.
MsMpEng.exe	0.11	79,576 K	74,952 K	1892	Antimalware Service Executa...	Microsoft Corporation
vmware-authd.exe	0.15	3,364 K	8,852 K	2088	VMware Authorization Service	VMware, Inc.
vmware-usbarbitrator64.exe	< 0.01	1,960 K	7,040 K	2320	VMware USB Arbitration Serv...	VMware, Inc.
SDWSCSvc.exe	0.11	5,340 K	10,992 K	2528	Windows Security Center inte...	Safer-Networking Ltd.
svchost.exe		4,188 K	9,816 K	2684	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 7.91% Commit Charge: 31.87% Processes: 66 Physical Usage: 35.26%

http://technet.microsoft.com/en-us/sysinternals/bb896653

Virustotal


https://www.virustotal.com/
Learn how to Hunt Down and ...
malware hunt - Google Search
VirusTotal - Free Online Viru...
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign In
virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File
URL
Search
No file selected
Choose File

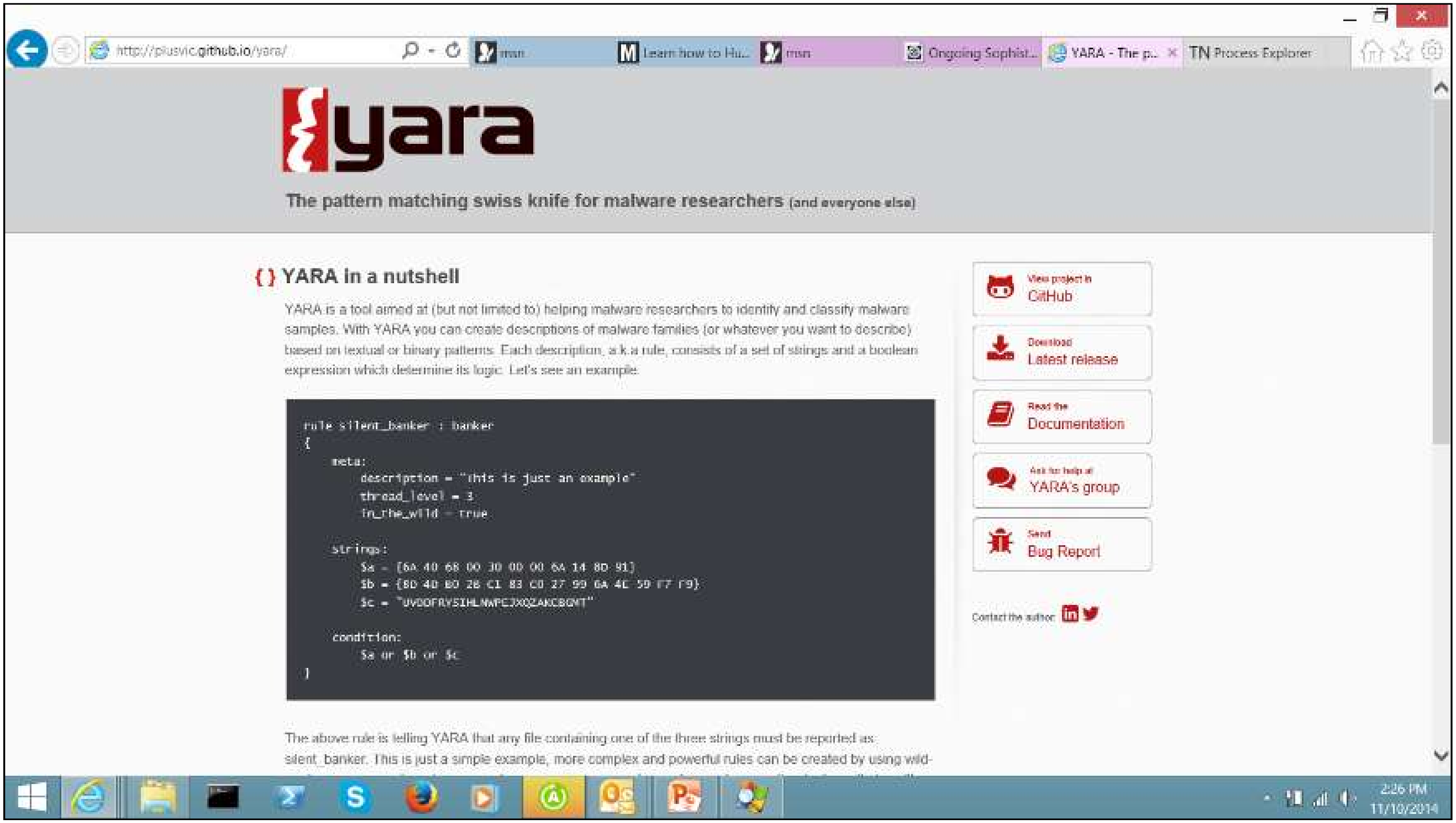
Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Scan it!
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy
1:18 PM
11/11/2014

https://www.virustotal.com/

Yara



The pattern matching swiss knife for malware researchers (and everyone else)

{ } YARA in a nutshell

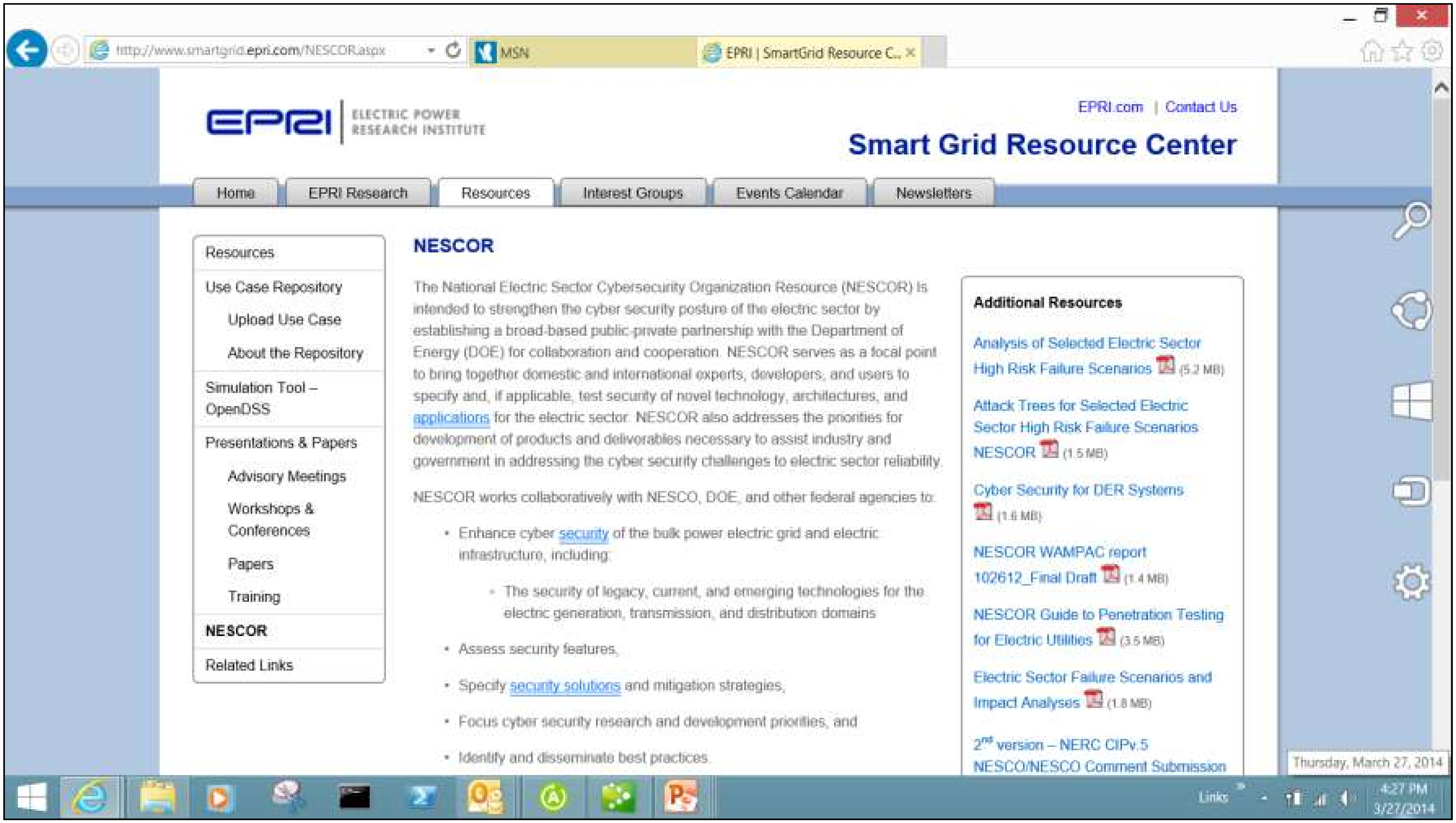
YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

The above rule is telling YARA that any file containing one of the three strings must be reported as silent_banker. This is just a simple example, more complex and powerful rules can be created by using wild-

http://plusvic.github.io/yara/

EPRI NESCOR Smart Grid Resource Center



Smart Grid Resource Center

NESCOR

The National Electric Sector Cybersecurity Organization Resource (NESCOR) is intended to strengthen the cyber security posture of the electric sector by establishing a broad-based public-private partnership with the Department of Energy (DOE) for collaboration and cooperation. NESCOR serves as a focal point to bring together domestic and international experts, developers, and users to specify and, if applicable, test security of novel technology, architectures, and applications for the electric sector. NESCOR also addresses the priorities for development of products and deliverables necessary to assist industry and government in addressing the cyber security challenges to electric sector reliability.

NESCOR works collaboratively with NESCO, DOE, and other federal agencies to:

- Enhance cyber security of the bulk power electric grid and electric infrastructure, including:
  - The security of legacy, current, and emerging technologies for the electric generation, transmission, and distribution domains
- Assess security features,
- Specify security solutions and mitigation strategies,
- Focus cyber security research and development priorities, and
- Identify and disseminate best practices.

Additional Resources

Analysis of Selected Electric Sector High Risk Failure Scenarios (5.2 MB)

Attack Trees for Selected Electric Sector High Risk Failure Scenarios NESCOR (1.5 MB)

Cyber Security for DER Systems (1.6 MB)

NESCOR WAMPAC report 102612_Final Draft (1.4 MB)

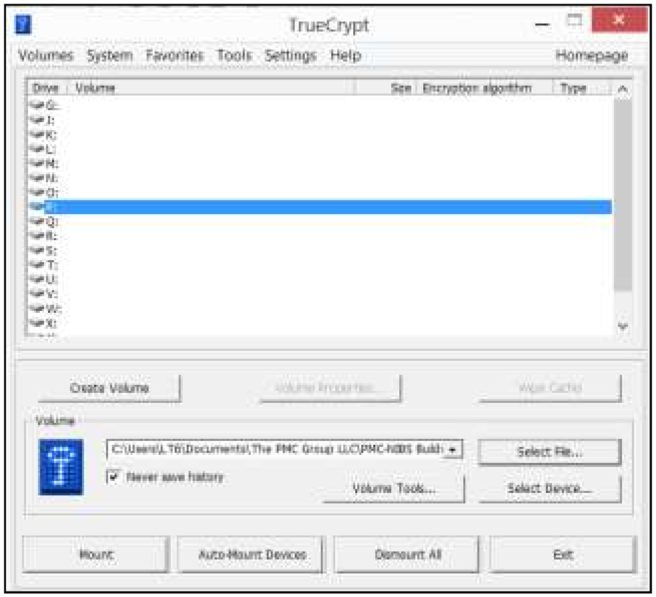
NESCOR Guide to Penetration Testing for Electric Utilities (3.5 MB)

Electric Sector Failure Scenarios and Impact Analyses (1.8 MB)

2nd version – NERC CIPv.5 NESCO/NESCO Comment Submission

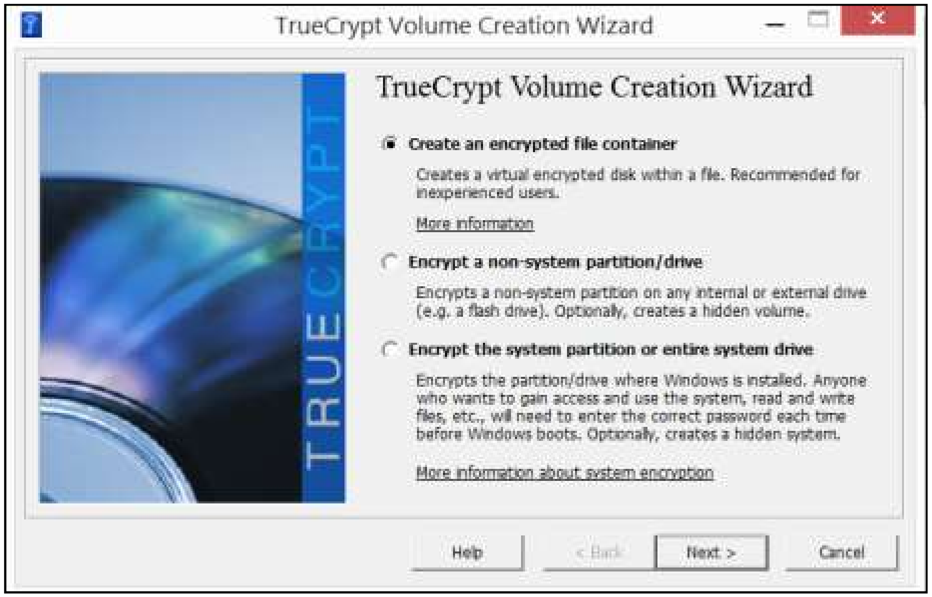
http://www.smartgrid.epri.com/NESCOR.aspx

True Crypt / Vera Crypt



C:\Users\LT6\Documents\The PMC Group LLC\PMC-NBS Buildi

☑ Never save history



TrueCrypt Volume Creation Wizard

● **Create an encrypted file container**

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

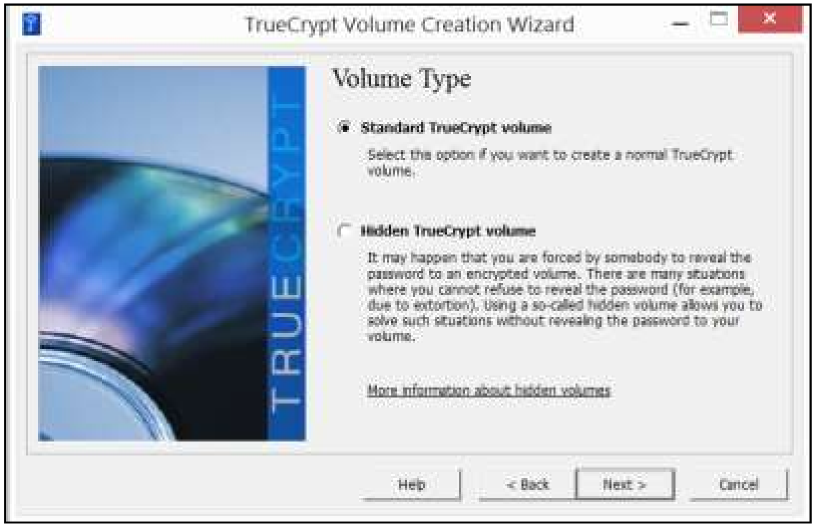
○ **Encrypt a non-system partition/drive**

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **Encrypt the system partition or entire system drive**

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption



Volume Type

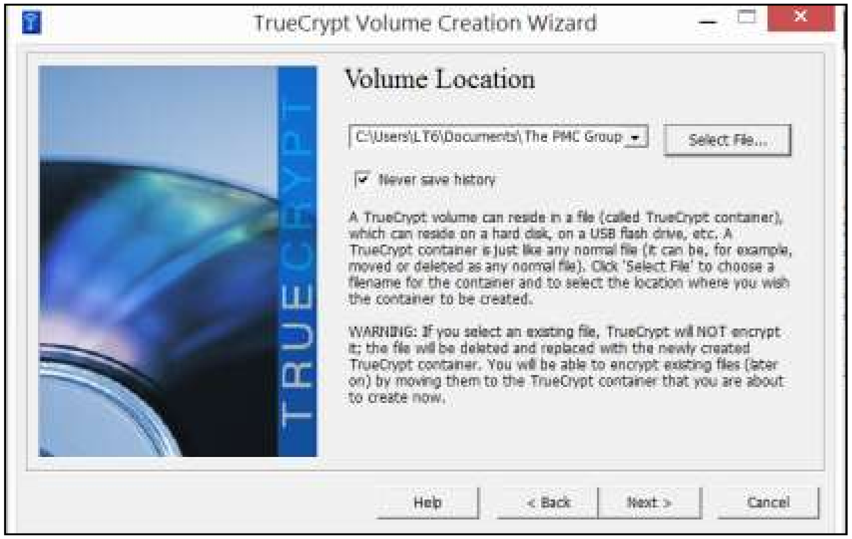
● **Standard TrueCrypt volume**

Select this option if you want to create a normal TrueCrypt volume.

○ **Hidden TrueCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes



Volume Location

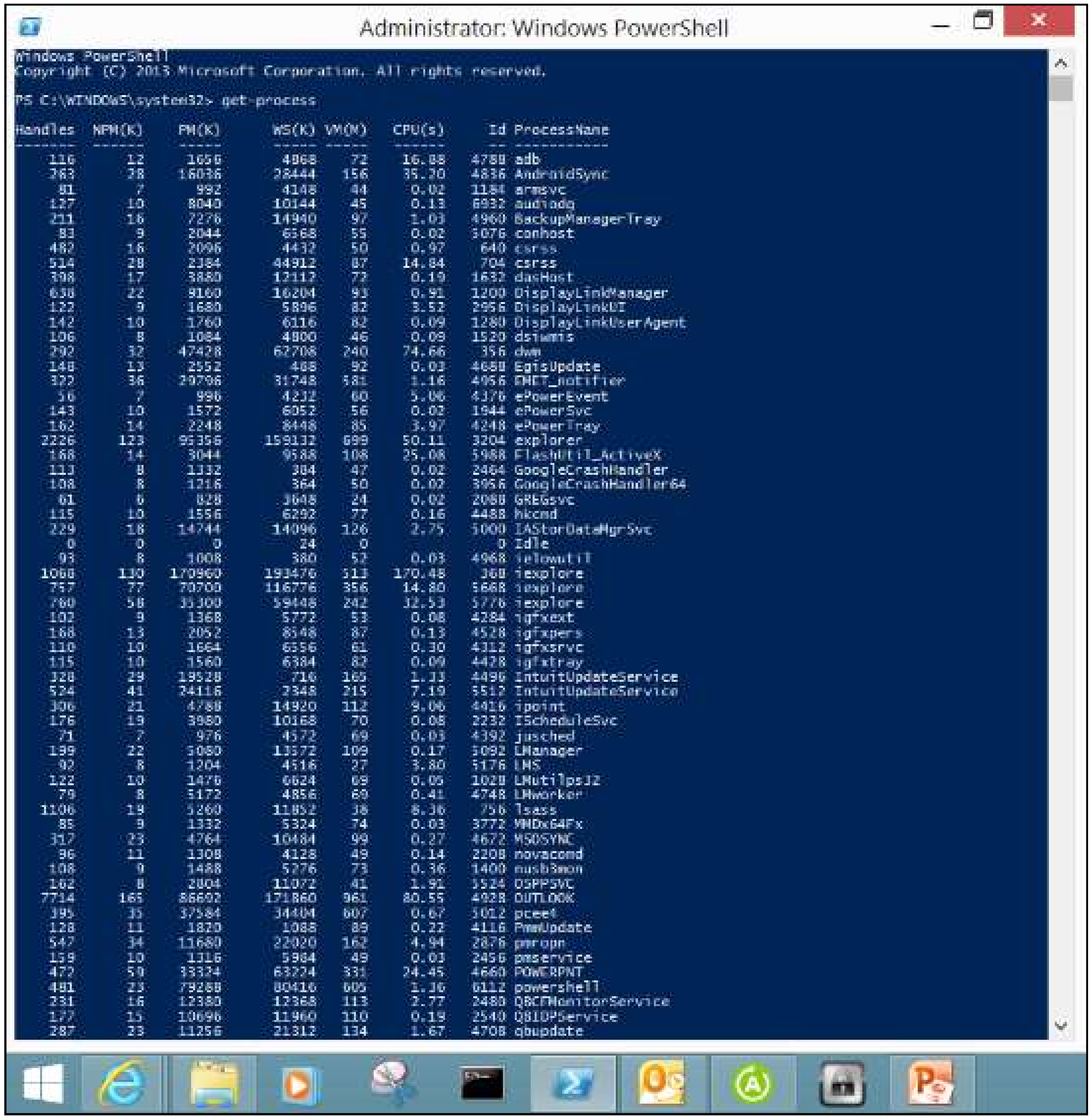
C:\Users\LT6\Documents\The PMC Group

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Windows PowerShell



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> get-process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
    116      12     1656       4868    72    16.88   4788 adb
    263      28    16036      28444   156    35.20   4836 AndroidSync
     81       7      992       4148    44     0.02   1184 armsvc
    127      10     8040      10144    45     0.13   6932 audiodg
    211      16     7276      14940    97     1.03   4960 BackupManagerTray
     83       9     2044       6568    55     0.02   3076 conhost
    482      16     2096       4432    50     0.97    640 csrss
    514      28     2384      44912    87    14.84    704 csrss
    398      17     3880      12112    72     0.19   1632 dasHost
    638      22     9160      16204    93     0.91   1200 DisplayLinkManager
    122       9     1680       5896    82     3.52   2956 DisplayLinkUI
    142      10     1760       6116    82     0.09   1280 DisplayLinkUserAgent
    106       8     1084       4800    46     0.09   1520 dsiwmis
    292      32    47428      62708   240    74.66    356 dwm
    148      13     2552        488    92     0.03   4688 EgisUpdate
    322      36    29796      31748   581     1.16   4956 EMET_notifier
     56       7      996       4232    60     5.06   4376 ePowerEvent
    143      10     1572       6052    56     0.02   1944 ePowerSvc
    162      14     2248       8448    85     3.97   4248 ePowerTray
   2226     123    95356     159132   699    50.11   3204 explorer
    168      14     3044       9588   108    25.08   5988 FlashUtil_ActiveX
    113       8     1332        304    47     0.02   2464 GoogleCrashHandler
    108       8     1216        364    50     0.02   3956 GoogleCrashHandler64
     61       6      828       3648    24     0.02   2088 GREGsvc
    115      10     1556       6292    77     0.16   4488 hkcmd
    229      18    14744      14096   126     2.75   5000 IAStorDataMgrSvc
      0       0        0         24     0               0 Idle
     93       8     1008        380    52     0.03   4968 ielowutil
   1068     130   170960     193476   513   170.48    368 iexplore
    757      77    70700     116776   356    14.80   5668 iexplore
    760      58    35300      59448   242    32.53   5776 iexplore
    102       9     1368       5772    53     0.08   4284 igfxext
    168      13     2052       8548    87     0.13   4528 igfxpers
    110      10     1664       6556    61     0.30   4312 igfxsrvc
    115      10     1560       6384    82     0.09   4428 igfxtray
    328      29    19528        716   165     1.33   4496 IntuitUpdateService
    524      41    24116       2348   215     7.19   5512 IntuitUpdateService
    306      21     4788      14920   112     9.06   4416 ipoint
    176      19     3980      10168    70     0.08   2232 IScheduleSvc
     71       7      976       4572    69     0.03   4392 jusched
    199      22     5080      13572   109     0.17   5092 LManager
     92       8     1204       4516    27     3.80   5176 LMS
    122      10     1476       6624    69     0.05   1028 LMutilps32
     79       8     5172       4856    69     0.41   4748 LMworker
   1106      19     5260      11852    38     8.36    756 lsass
     85       9     1332       5324    74     0.03   3772 MMDx64Fx
    317      23     4764      10484    99     0.27   4672 MSOSYNC
     96      11     1308       4128    49     0.14   2208 novacomd
    108       9     1488       5276    73     0.36   1400 nusb3mon
    162       8     2804      11072    41     1.91   3524 OSPPSVC
   7714     165    86692     171860   961    80.55   4928 OUTLOOK
    395      35    37584      34404   607     0.67   3012 pcee4
    128      11     1820       1088    89     0.22   4116 PmmUpdate
    547      34    11680      22020   162     4.94   2876 pmropn
    159      10     1316       5984    49     0.03   2456 pmservice
    472      59    33324      63224   331    24.45   4660 POWERPNT
    481      23    79288      80416   605     1.36   6112 powershell
    231      16    12380      12368   113     2.77   2480 QBCFMonitorService
    177      15    10696      11960   110     0.19   2540 QBIDPService
    287      23    11256      21312   134     1.67   4708 qbupdate
```

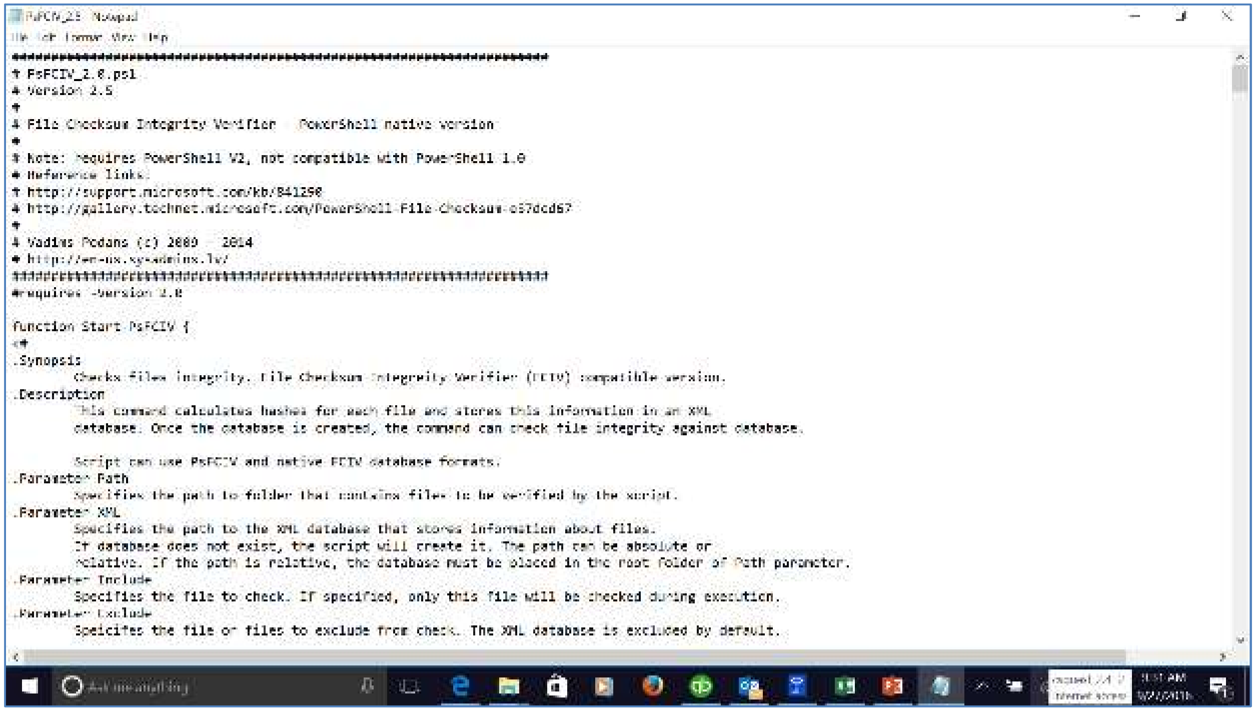
- Windows PowerShell replaces the Command Line
- Uses Cmdlets to perform common system administration tasks, such as managing the registry, services, processes, and event logs, and using Windows Management Instrumentation (WMI).

A task-based scripting language and support for existing scripts and command-line tools.

Windows PowerShell File Checksum Integrity

PowerShell File Checksum Integrity Verifier (PsFCIV)

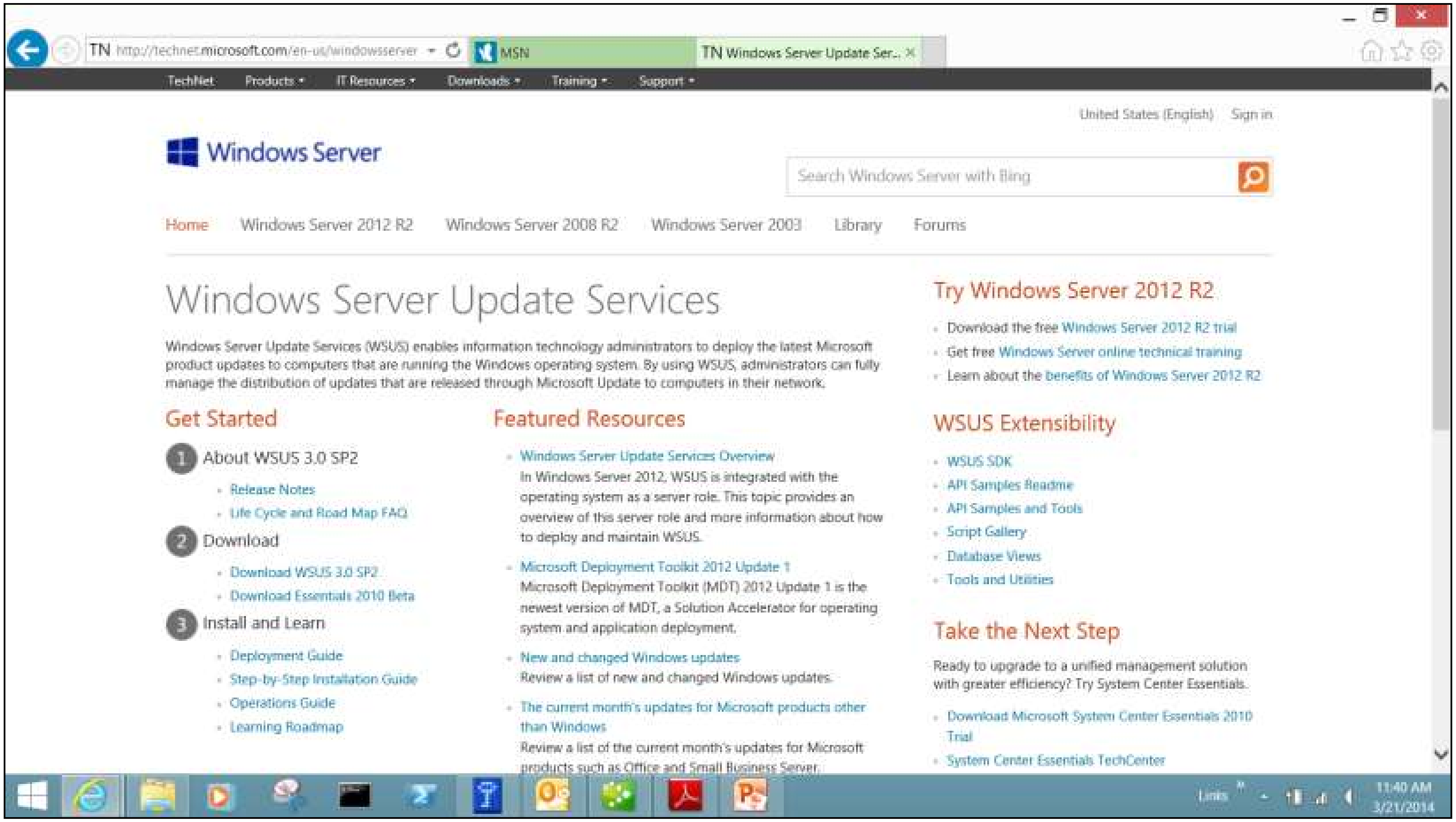
PowerShell File Checksum Integrity Verifier is a enhanced PowerShell version of legacy Microsoft FCIV.exe tool. PsFCIV is used to track your files integrity status by calculating cryptographic hashes over a file (or files) and writing them into FCIV-compatible XML database.



```
#######################################################################
# PsFCIV_2.0.ps1
# Version 2.5
#
# File Checksum Integrity Verifier - PowerShell native version
#
# Note: requires PowerShell V2, not compatible with PowerShell 1.0
# Reference links:
# http://support.microsoft.com/kb/841290
# http://gallery.technet.microsoft.com/PowerShell-File-Checksum-e57dcd67
#
# Vadims Podans (c) 2009 - 2014
# http://en-us.sysadmins.lv/
#######################################################################
#requires -Version 2.0

function Start-PsFCIV {
<#
.Synopsis
        Checks files integrity. File Checksum Integreity Verifier (FCIV) compatible version.
.Description
        This command calculates hashes for each file and stores this information in an XML
        database. Once the database is created, the command can check file integrity against database.

        Script can use PsFCIV and native FCIV database formats.
.Parameter Path
        Specifies the path to folder that contains files to be verified by the script.
.Parameter XML
        Specifies the path to the XML database that stores information about files.
        If database does not exist, the script will create it. The path can be absolute or
        relative. If the path is relative, the database must be placed in the root folder of Path parameter.
.Parameter Include
        Specifies the file to check. If specified, only this file will be checked during execution.
.Parameter Exclude
        Speicifes the file or files to exclude from check. The XML database is excluded by default.
```

https://gallery.technet.microsoft.com/PowerShell-File-Checksum-e57dcd67

Windows Server Update Services (WSUS)



Windows Server Update Services

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

Get Started

1 About WSUS 3.0 SP2

- Release Notes
- Life Cycle and Road Map FAQ

2 Download

- Download WSUS 3.0 SP2
- Download Essentials 2010 Beta

3 Install and Learn

- Deployment Guide
- Step-by-Step Installation Guide
- Operations Guide
- Learning Roadmap

Featured Resources

- Windows Server Update Services Overview
  In Windows Server 2012, WSUS is integrated with the operating system as a server role. This topic provides an overview of this server role and more information about how to deploy and maintain WSUS.
- Microsoft Deployment Toolkit 2012 Update 1
  Microsoft Deployment Toolkit (MDT) 2012 Update 1 is the newest version of MDT, a Solution Accelerator for operating system and application deployment.
- New and changed Windows updates
  Review a list of new and changed Windows updates.
- The current month's updates for Microsoft products other than Windows
  Review a list of the current month's updates for Microsoft products such as Office and Small Business Server.

Try Windows Server 2012 R2

- Download the free Windows Server 2012 R2 trial
- Get free Windows Server online technical training
- Learn about the benefits of Windows Server 2012 R2

WSUS Extensibility

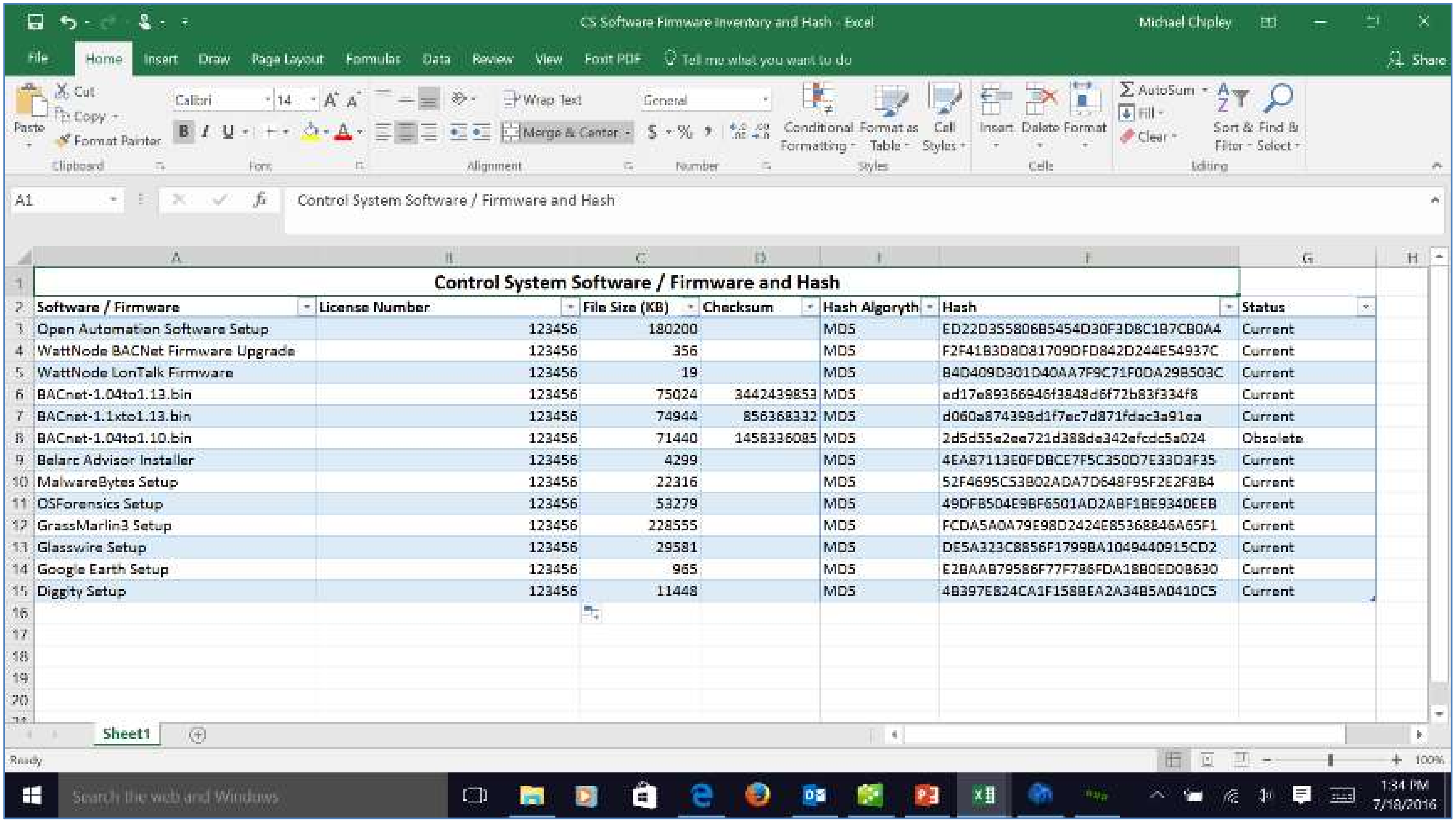
- WSUS SDK
- API Samples Readme
- API Samples and Tools
- Script Gallery
- Database Views
- Tools and Utilities

Take the Next Step

Ready to upgrade to a unified management solution with greater efficiency? Try System Center Essentials.

- Download Microsoft System Center Essentials 2010 Trial
- System Center Essentials TechCenter

Control System Software / Firmware Inventory



Control System Software / Firmware and Hash

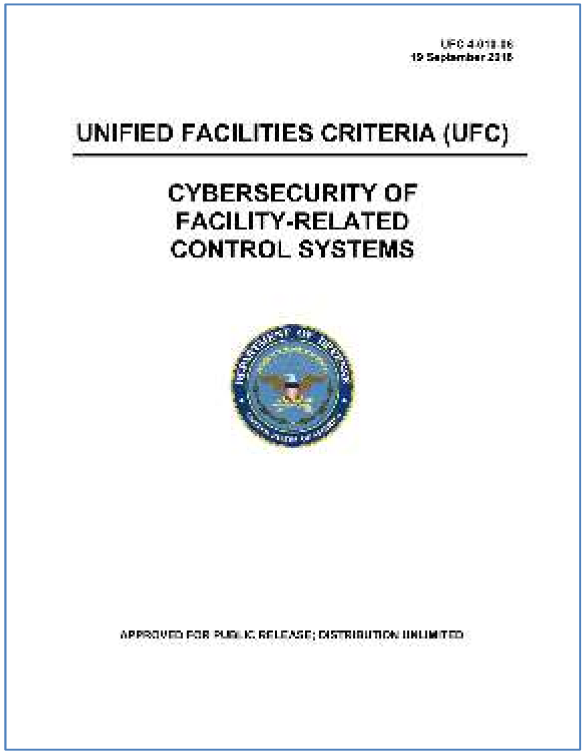
Software / Firmware	License Number	File Size (KB)	Checksum	Hash Algoryth	Hash	Status
Open Automation Software Setup	123456	180200		MD5	ED22D355806B5454D30F3D8C1B7CB0A4	Current
WattNode BACNet Firmware Upgrade	123456	356		MD5	F2F41B3D8D81709DFD842D244E54937C	Current
WattNode LonTalk Firmware	123456	19		MD5	B4D409D301D40AA7F9C71F0DA29B503C	Current
BACnet-1.04to1.13.bin	123456	75024	3442439853	MD5	ed17e89366946f3848d6f72b83f334f8	Current
BACnet-1.1xto1.13.bin	123456	74944	856368332	MD5	d060a874398d1f7ec7d871fdac3a91ea	Current
BACnet-1.04to1.10.bin	123456	71440	1458336085	MD5	2d5d55e2ee721d388de342efcdc5a024	Obsolete
Belarc Advisor Installer	123456	4299		MD5	4EA87113E0FDBCE7F5C350D7E33D3F35	Current
MalwareBytes Setup	123456	22316		MD5	52F4695C53B02ADA7D648F95F2E2F8B4	Current
OSForensics Setup	123456	53279		MD5	49DFB504E9BF6501AD2ABF1BE9340EEB	Current
GrassMarlin3 Setup	123456	228555		MD5	FCDA5A0A79E98D2424E85368846A65F1	Current
Glasswire Setup	123456	29581		MD5	DE5A323C8856F1799BA1049440915CD2	Current
Google Earth Setup	123456	965		MD5	E2BAAB79586F77F786FDA18B0ED0B630	Current
Diggity Setup	123456	11448		MD5	4B397E824CA1F158BEA2A34B5A0410C5	Current

Excel Inventory Hash: AA74ACFC4C1E1C94A3EE5C4C967B153C

Unit 4

UFC 4-010-06 Cybersecurity Of Facility-Related Control Systems, FRCS Reference Architecture, Platform Enclave, FRCS IA Contract Language for SME’s, Test and Development Environment, FAT/SAT Checklist, Penetration Testing Checklist, Design/Construction Sequence Table

DoD UFC 4-010-06 Cybersecurity



UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF
FACILITY-RELATED
CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

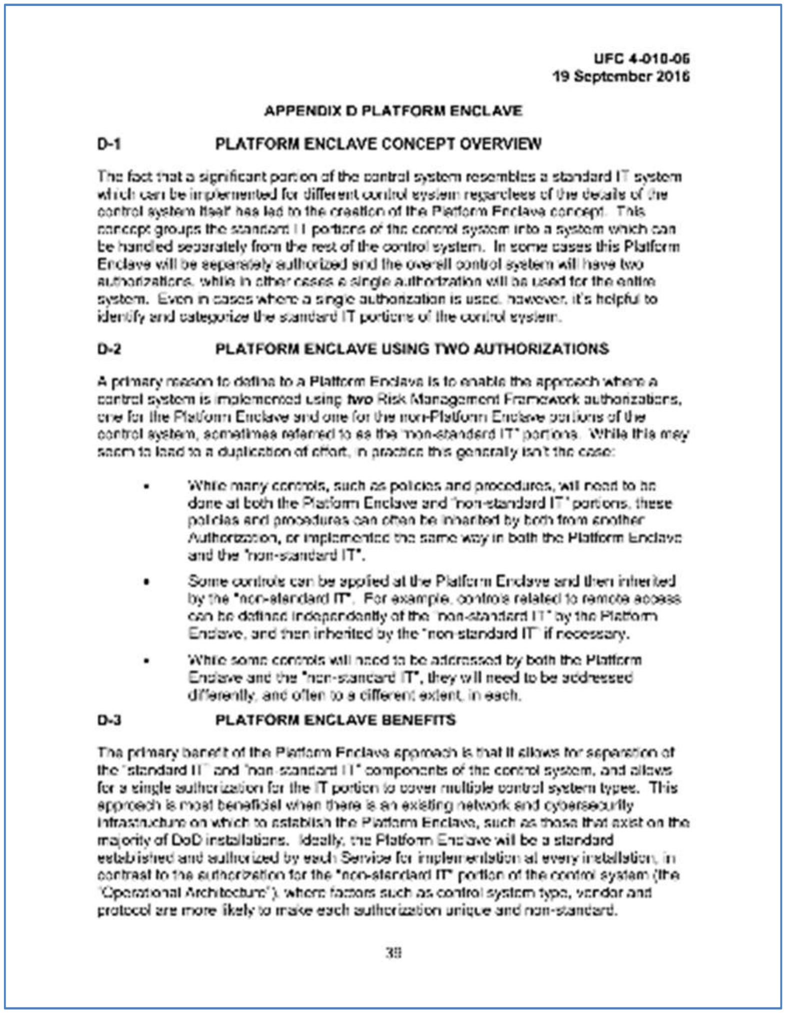
3-1.1 Five Steps for Cybersecurity Design. The five steps for cybersecurity design are:

Step 1: Based on the organizational mission and details of the control system, the System Owner (SO) and Authorizing Official (AO) determine the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) for the control system.
Step 2: Use the impact levels to select the proper list of controls from NIST SP 800-82.
Step 3: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2.
Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer’s responsibility.
Step 5: Include cybersecurity requirements in the project specifications and provide input to others as required.

DoD UFC 4-010-06 Platform Enclave

2.3 Platform Enclave. Significant portions of the control system resemble a standard IT system which can be implemented in a standard manner for different control systems, regardless of the details of the control system itself. **This has led to the creation of the Platform Enclave concept, which groups the "standard IT" portions of the control system, plus related standard policies and procedures, into an entity which can be handled separately from the rest of the control system.** In some cases this Platform Enclave will be separately authorized and the overall control system will have two authorizations, one for the Platform Enclave and one for the Operational Architecture which primarily covers the "non-standard IT" components of the system. In other cases a single authorization will be used for the entire system. Even in cases where a single authorization is used, however, it's helpful to identify and categorize the "standard IT" portions of the control system. More information on the Platform Enclave approach is in APPENDIX D

DoD UFC 4-010-06 Appendix D



UFC 4-010-06
19 September 2016

APPENDIX D PLATFORM ENCLAVE

D-1 PLATFORM ENCLAVE CONCEPT OVERVIEW

The fact that a significant portion of the control system resembles a standard IT system which can be implemented for different control system regardless of the details of the control system itself has led to the creation of the Platform Enclave concept. This concept groups the standard IT portions of the control system into a system which can be handled separately from the rest of the control system. In some cases this Platform Enclave will be separately authorized and the overall control system will have two authorizations, while in other cases a single authorization will be used for the entire system. Even in cases where a single authorization is used, however, it's helpful to identify and categorize the standard IT portions of the control system.

D-2 PLATFORM ENCLAVE USING TWO AUTHORIZATIONS

A primary reason to define to a Platform Enclave is to enable the approach where a control system is implemented using **two** Risk Management Framework authorizations, one for the Platform Enclave and one for the non-Platform Enclave portions of the control system, sometimes referred to as the "non-standard IT" portions. While this may seem to lead to a duplication of effort, in practice this generally isn't the case:

- While many controls, such as policies and procedures, will need to be done at both the Platform Enclave and "non-standard IT" portions, these policies and procedures can often be inherited by both from another Authorization, or implemented the same way in both the Platform Enclave and the "non-standard IT".
- Some controls can be applied at the Platform Enclave and then inherited by the "non-standard IT". For example, controls related to remote access can be defined independently of the "non-standard IT" by the Platform Enclave, and then inherited by the "non-standard IT" if necessary.
- While some controls will need to be addressed by both the Platform Enclave and the "non-standard IT", they will need to be addressed differently, and often to a different extent, in each.

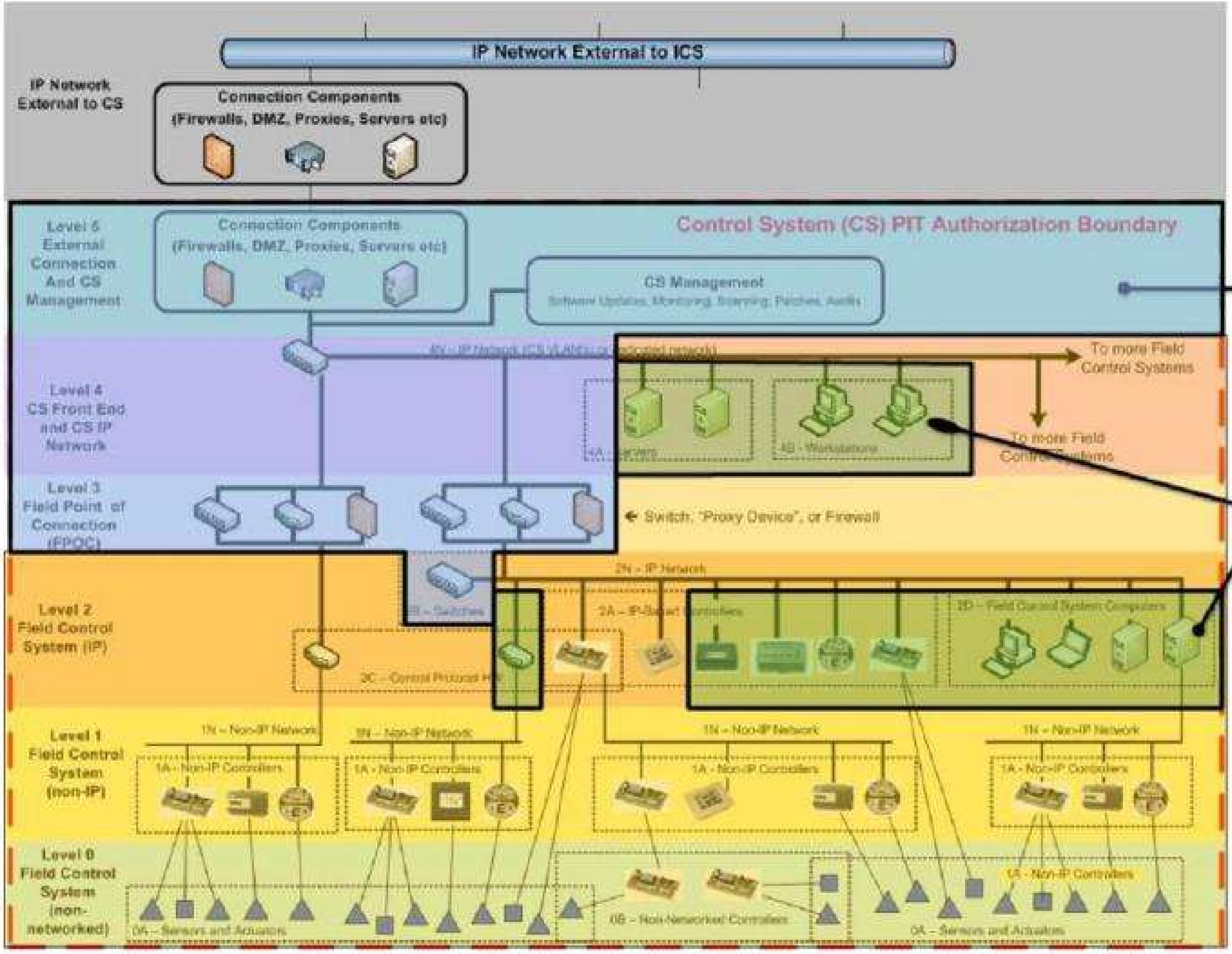
D-3 PLATFORM ENCLAVE BENEFITS

The primary benefit of the Platform Enclave approach is that it allows for separation of the "standard IT" and "non-standard IT" components of the control system, and allows for a single authorization for the IT portion to cover multiple control system types. This approach is most beneficial when there is an existing network and cybersecurity infrastructure on which to establish the Platform Enclave, such as those that exist on the majority of DoD installations. Ideally, the Platform Enclave will be a standard established and authorized by each Service for implementation at every installation, in contrast to the authorization for the "non-standard IT" portion of the control system (the "Operational Architecture"), where factors such as control system type, vendor and protocol are more likely to make each authorization unique and non-standard.

39

Platform Enclave: The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system, or is mostly implemented at the Platform Enclave but also needed within the field control system (in which case the CCI is also in the "Designer" category). For example, passwords are implemented at the Platform Enclave, but are also necessary at the control system user interface itself, local display panels and some controllers (those which support passwords). While implementation of the Platform Enclave is not the designer's responsibility (a key point of the Platform Enclave is that it is a standard approach that can be implemented across multiple control systems), it's important to document CCIs the control system expects to inherit from the Platform Enclave

DoD UFC 4-010-06 Appendix D


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

Platform Enclave (PE)

Operational Architecture (OA)

Navy Only: OA1: N-UMCS

Navy Only: OA2
All else in Levels 0-2: FCS or UMCS requiring separate accreditation prior to connecting to N-UMCS and the PE

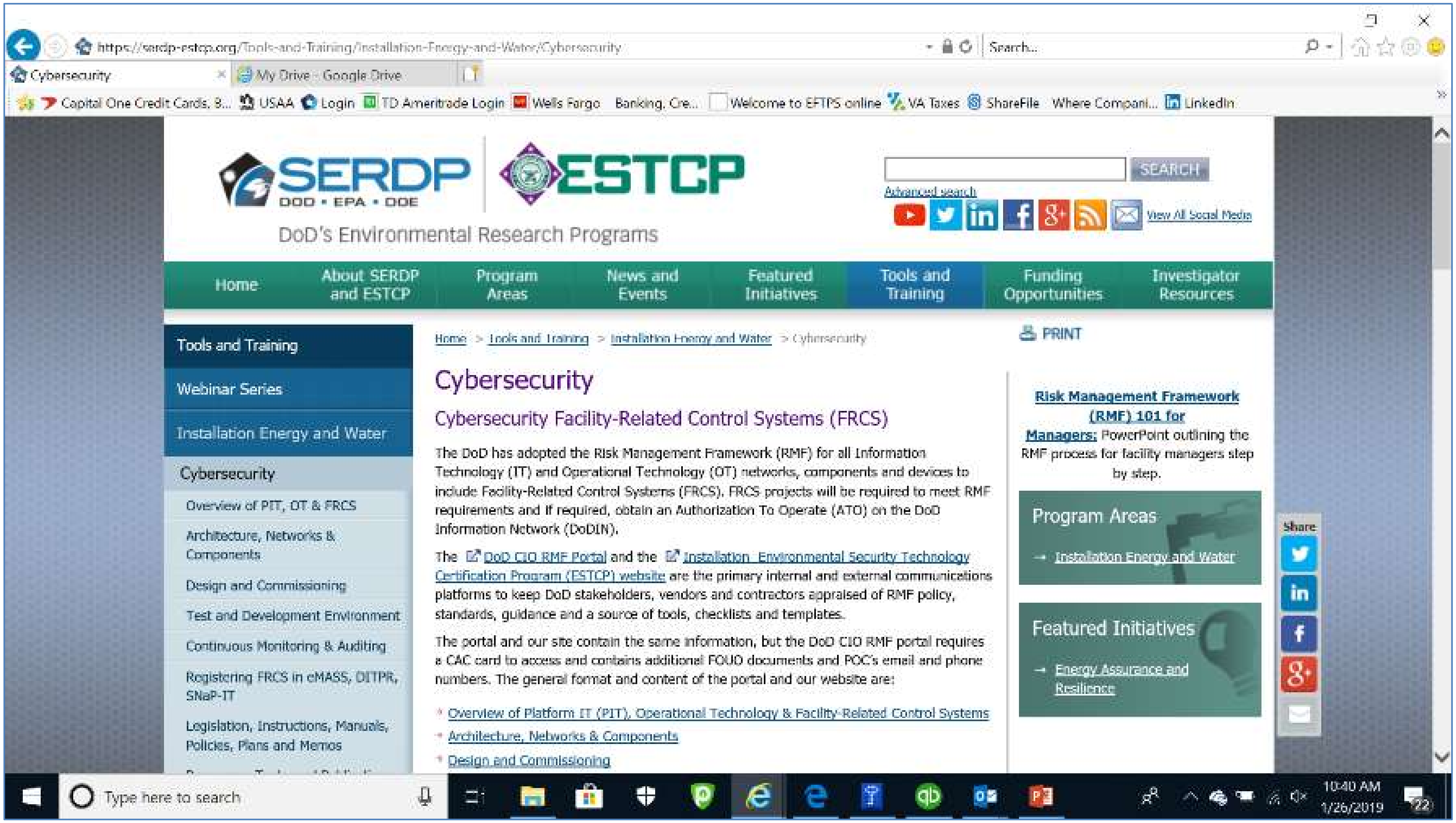
All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the FRCS-PE and NUMCS.

Enclave Summary

Create hardware and component/device inventory of all FRCS assets

1. Run SCAP - configure to STIGS
   http://iase.disa.mil/stigs/net_perimeter/enclave-dmzs/Pages/index.aspx
2. Belarc – Obtain detailed Server, Workstation, LT Level 4 inventory
3. CSET – create System Security Plan, Hardware and Component/Device inventory
4. GrassMarlin - Component/Device Hardware and Software / Firmware inventory
5. Glasswire – Network, Apps, Executables
6. Run WhiteScope and create Whitelist of BFRCS firmware
7. Hash all software and firmware
8. Hash the inventory files

ESTCP RMF FRCS Guidance and Templates


https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity
Search...
Cybersecurity
My Drive - Google Drive
Capital One Credit Cards, B...
USAA
Login
TD Ameritrade Login
Wells Fargo
Banking, Cre...
Welcome to EFTPS online
VA Taxes
ShareFile
Where Compani...
LinkedIn
SERDP
DOD • EPA • DOE
ESTCP
DoD's Environmental Research Programs
SEARCH
Advanced search
View All Social Media
Home
About SERDP and ESTCP
Program Areas
News and Events
Featured Initiatives
Tools and Training
Funding Opportunities
Investigator Resources
Tools and Training
Webinar Series
Installation Energy and Water
Cybersecurity
Overview of PIT, OT & FRCS
Architecture, Networks & Components
Design and Commissioning
Test and Development Environment
Continuous Monitoring & Auditing
Registering FRCS in eMASS, DITPR, SNaP-IT
Legislation, Instructions, Manuals, Policies, Plans and Memos
Home > Tools and Training > Installation Energy and Water > Cybersecurity
PRINT
Share
Type here to search
10:40 AM
1/26/2019
22

Cybersecurity

Cybersecurity Facility-Related Control Systems (FRCS)

The DoD has adopted the Risk Management Framework (RMF) for all Information Technology (IT) and Operational Technology (OT) networks, components and devices to include Facility-Related Control Systems (FRCS). FRCS projects will be required to meet RMF requirements and if required, obtain an Authorization To Operate (ATO) on the DoD Information Network (DoDIN).

The DoD CIO RMF Portal and the Installation Environmental Security Technology Certification Program (ESTCP) website are the primary internal and external communications platforms to keep DoD stakeholders, vendors and contractors appraised of RMF policy, standards, guidance and a source of tools, checklists and templates.

The portal and our site contain the same information, but the DoD CIO RMF portal requires a CAC card to access and contains additional FOUO documents and POC's email and phone numbers. The general format and content of the portal and our website are:

- Overview of Platform IT (PIT), Operational Technology & Facility-Related Control Systems
- Architecture, Networks & Components
- Design and Commissioning

Risk Management Framework (RMF) 101 for Managers: PowerPoint outlining the RMF process for facility managers step by step.

Program Areas

→ Installation Energy and Water

Featured Initiatives

→ Energy Assurance and Resilience

https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity

Cybersecurity Guidelines

The Cybersecurity website has several key sections that establish new RMF contractual and deliverable requirements:

Overview of Platform IT (PIT), Operational Technology & Facility-Related Control Systems
Architecture, Networks & Components
Design and Commissioning
Test and Development Environment (TDE)
Continuous Monitoring (CM) Strategy and Auditing
Registering FRCS In eMASS, DITPR and SNaP-IT
Legislation Instructions, Manuals, Policies, Plans and Memo's
Resources And Tools, and Publications
Templates and Checklists
Software
Protecting DoD Controlled Unclassified Information (CUI)
Medical Facilities-Related Control Systems, Medical Devices and Equipment
Energy Projects, Third-party Financing and Cybersecurity

Any organization can use for their FRCS

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

Cybersecurity Guideline SME's

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 (FRCSI) for the products they are integrating and/or be Control System Integrators Association (CISA) Certified.

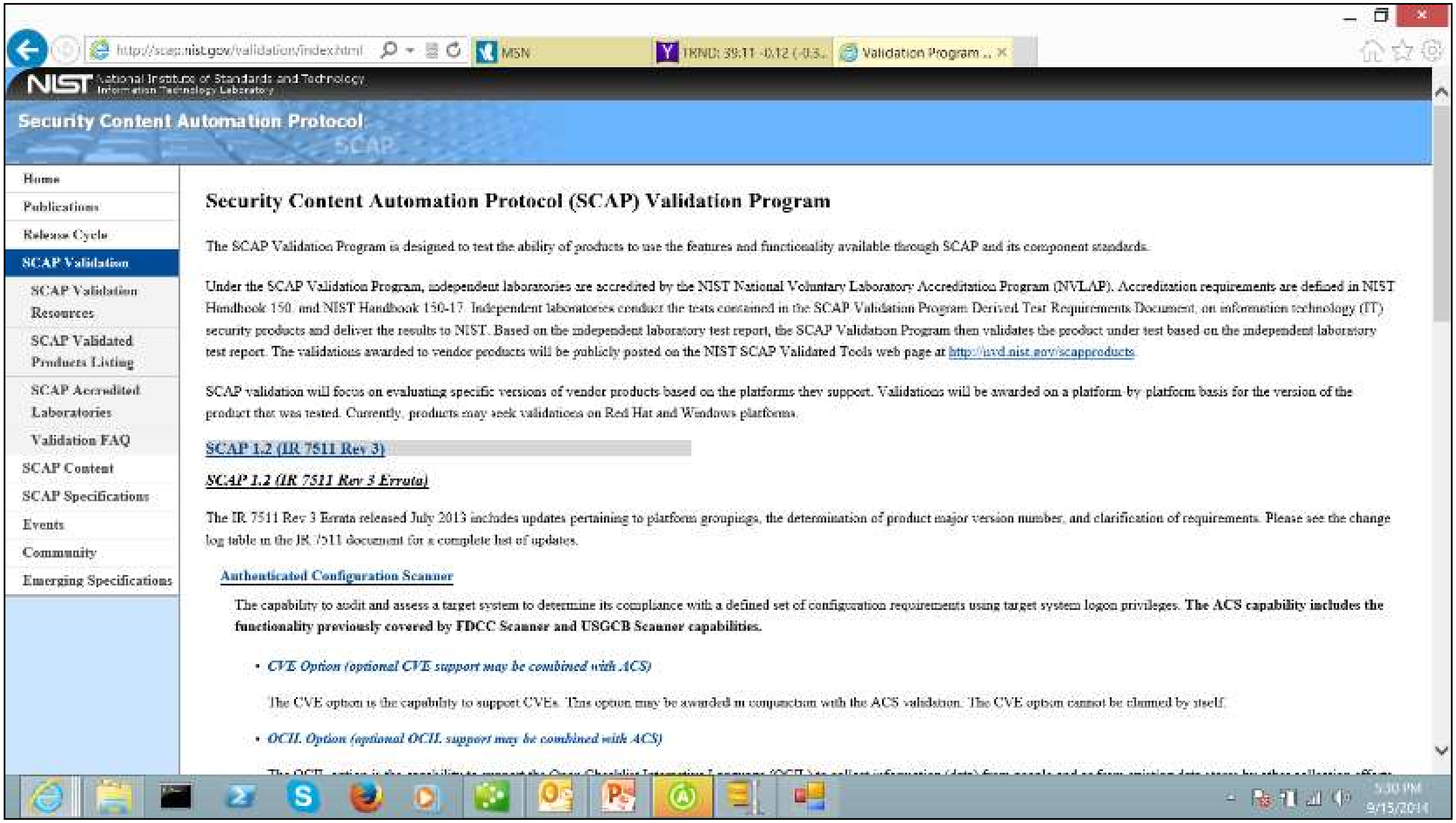
Cybersecurity Guideline TDE

1.10 TEST AND DEVELOPMENT ENVIRONMENT For new or major modernization projects, the Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators. At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and FRCS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete FRCS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).

The ESTCP Project Team/System Integrator will transfer the TDE to the ESTCP PM for inclusion into the Platform Enclave Operations Center.

NIST SCAP


http://scap.nist.gov/validation/index.html
MSN
TRND: 39.11 -0.12 (-0.3...
Validation Program ...
NIST National Institute of Standards and Technology
Information Technology Laboratory
Security Content Automation Protocol
SCAP
Home
Publications
Release Cycle
SCAP Validation
SCAP Validation Resources
SCAP Validated Products Listing
SCAP Accredited Laboratories
Validation FAQ
SCAP Content
SCAP Specifications
Events
Community
Emerging Specifications
5:30 PM
9/15/2014

Security Content Automation Protocol (SCAP) Validation Program

The SCAP Validation Program is designed to test the ability of products to use the features and functionality available through SCAP and its component standards.

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). Accreditation requirements are defined in NIST Handbook 150, and NIST Handbook 150-17. Independent laboratories conduct the tests contained in the SCAP Validation Program Derived Test Requirements Document, on information technology (IT) security products and deliver the results to NIST. Based on the independent laboratory test report, the SCAP Validation Program then validates the product under test based on the independent laboratory test report. The validations awarded to vendor products will be publicly posted on the NIST SCAP Validated Tools web page at http://nvd.nist.gov/scapproducts.

SCAP validation will focus on evaluating specific versions of vendor products based on the platforms they support. Validations will be awarded on a platform-by-platform basis for the version of the product that was tested. Currently, products may seek validations on Red Hat and Windows platforms.

SCAP 1.2 (IR 7511 Rev 3)

SCAP 1.2 (IR 7511 Rev 3 Errata)

The IR 7511 Rev 3 Errata released July 2013 includes updates pertaining to platform groupings, the determination of product major version number, and clarification of requirements. Please see the change log table in the IR 7511 document for a complete list of updates.

Authenticated Configuration Scanner

The capability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges. **The ACS capability includes the functionality previously covered by FDCC Scanner and USGCB Scanner capabilities.**

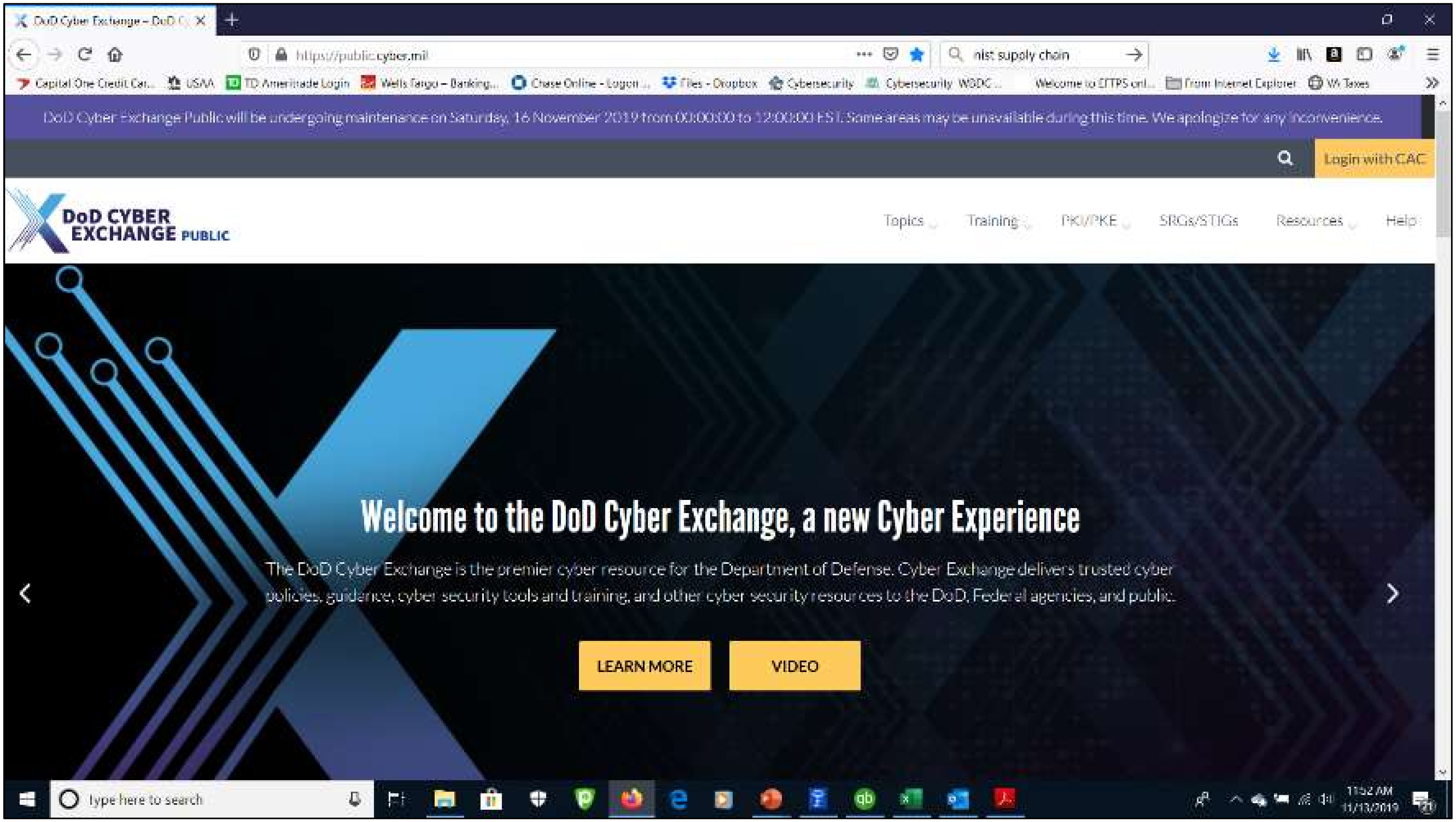
- *CVE Option (optional CVE support may be combined with ACS)*

  The CVE option is the capability to support CVEs. This option may be awarded in conjunction with the ACS validation. The CVE option cannot be claimed by itself.

- *OCIL Option (optional OCIL support may be combined with ACS)*

http://scap.nist.gov/validation/index.html

DISA STIGs



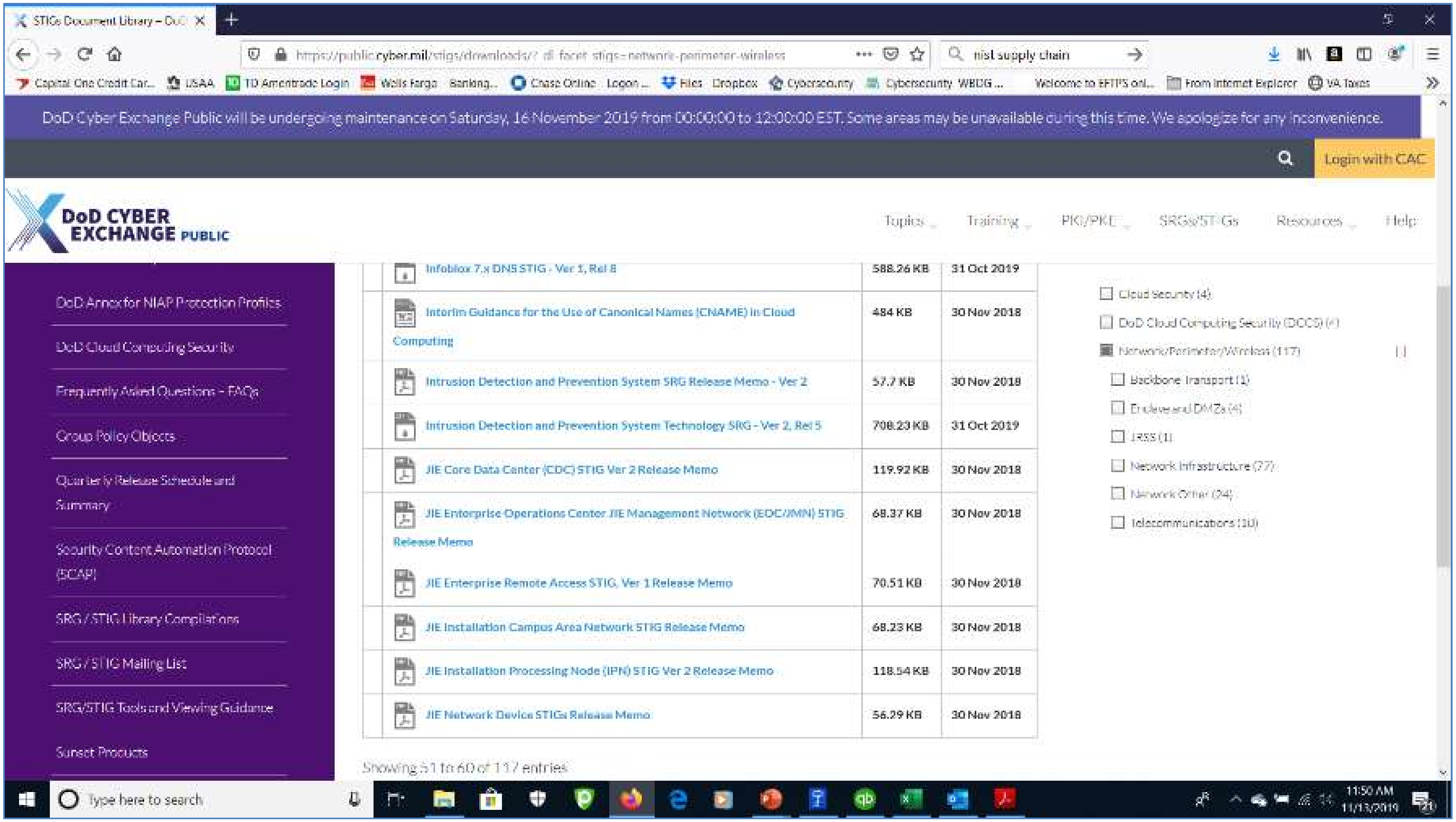
DoD Cyber Exchange Public will be undergoing maintenance on Saturday, 16 November 2019 from 00:00:00 to 12:00:00 EST. Some areas may be unavailable during this time. We apologize for any inconvenience.

Welcome to the DoD Cyber Exchange, a new Cyber Experience

The DoD Cyber Exchange is the premier cyber resource for the Department of Defense. Cyber Exchange delivers trusted cyber policies, guidance, cyber security tools and training, and other cyber security resources to the DoD, Federal agencies, and public.

https://public.cyber.mil/

JIE STIGS



DoD Cyber Exchange Public will be undergoing maintenance on Saturday, 16 November 2019 from 00:00:00 to 12:00:00 EST. Some areas may be unavailable during this time. We apologize for any inconvenience.

- DoD Annex for NIAP Protection Profiles
- DoD Cloud Computing Security
- Frequently Asked Questions - FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- Security Content Automation Protocol (SCAP)
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance
- Sunset Products

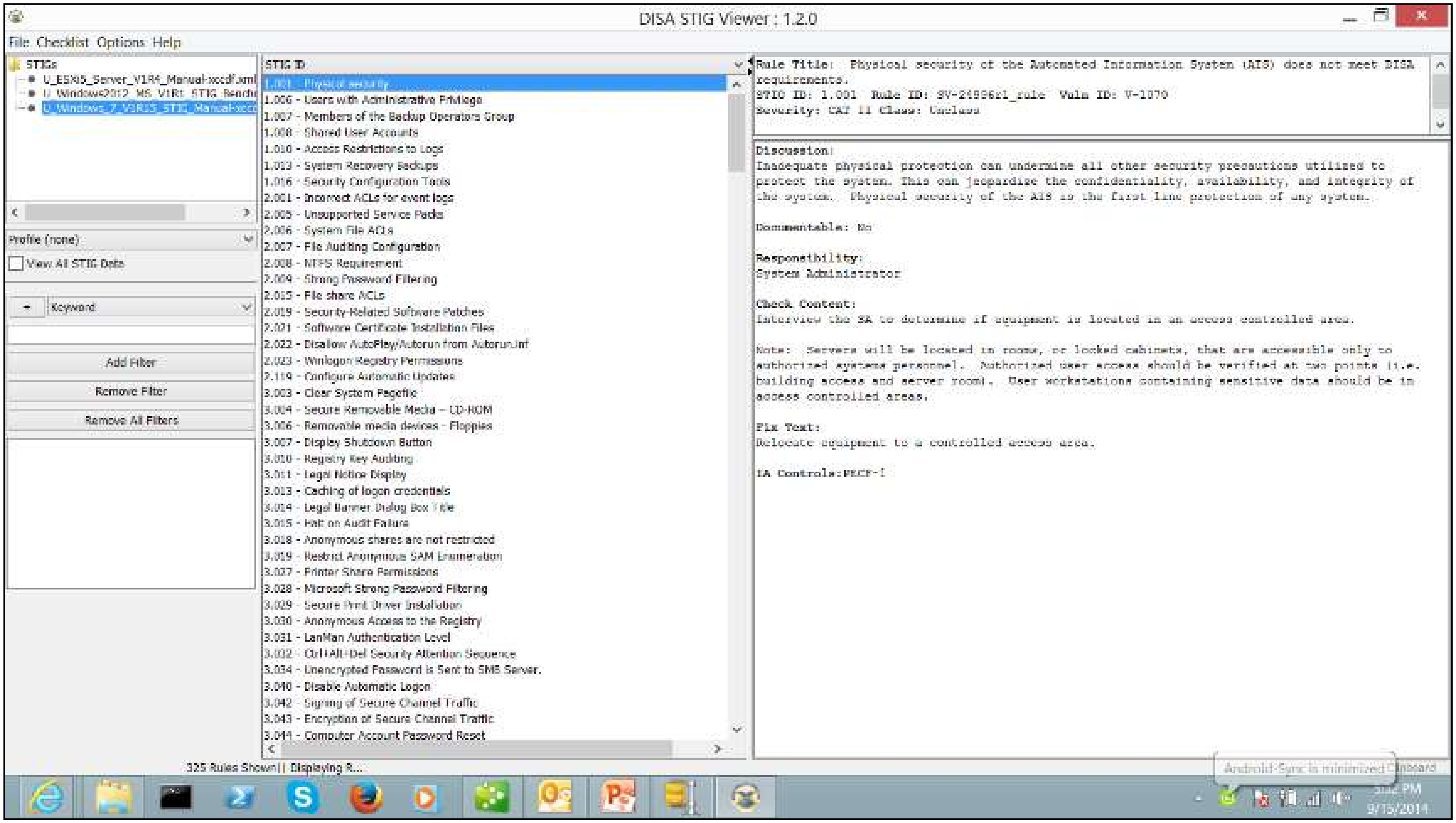
Infoblox 7.x DNS STIG - Ver 1, Rel 8	588.26 KB	31 Oct 2019
Interim Guidance for the Use of Canonical Names (CNAME) in Cloud Computing	484 KB	30 Nov 2018
Intrusion Detection and Prevention System SRG Release Memo - Ver 2	57.7 KB	30 Nov 2018
Intrusion Detection and Prevention System Technology SRG - Ver 2, Rel 5	708.23 KB	31 Oct 2019
JIE Core Data Center (CDC) STIG Ver 2 Release Memo	119.92 KB	30 Nov 2018
JIE Enterprise Operations Center JIE Management Network (EOC/JMN) STIG Release Memo	68.37 KB	30 Nov 2018
JIE Enterprise Remote Access STIG, Ver 1 Release Memo	70.51 KB	30 Nov 2018
JIE Installation Campus Area Network STIG Release Memo	68.23 KB	30 Nov 2018
JIE Installation Processing Node (IPN) STIG Ver 2 Release Memo	118.54 KB	30 Nov 2018
JIE Network Device STIGs Release Memo	56.29 KB	30 Nov 2018

Showing 51 to 60 of 117 entries

- □ Cloud Security (4)
- □ DoD Cloud Computing Security (DCCS) (4)
- ■ Network/Perimeter/Wireless (117)
  - □ Backbone Transport (1)
  - □ Enclave and DMZs (4)
  - □ JRSS (1)
  - □ Network Infrastructure (77)
  - □ Network Other (24)
  - □ Telecommunications (10)

https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=network-perimeter-wireless

DISA STIG Viewer


DISA STIG Viewer : 1.2.0
File Checklist Options Help
STIGs
U_ESXi5_Server_V1R4_Manual-xccdf.xml
U_Windows2012_MS_V1R1_STIG_Bench
U_Windows_7_V1R15_STIG_Manual-xccd
Profile (none)
View All STIG Data
Keyword
Add Filter
Remove Filter
Remove All Filters
STIG ID
Android-Sync is minimized
3:32 PM
9/15/2014

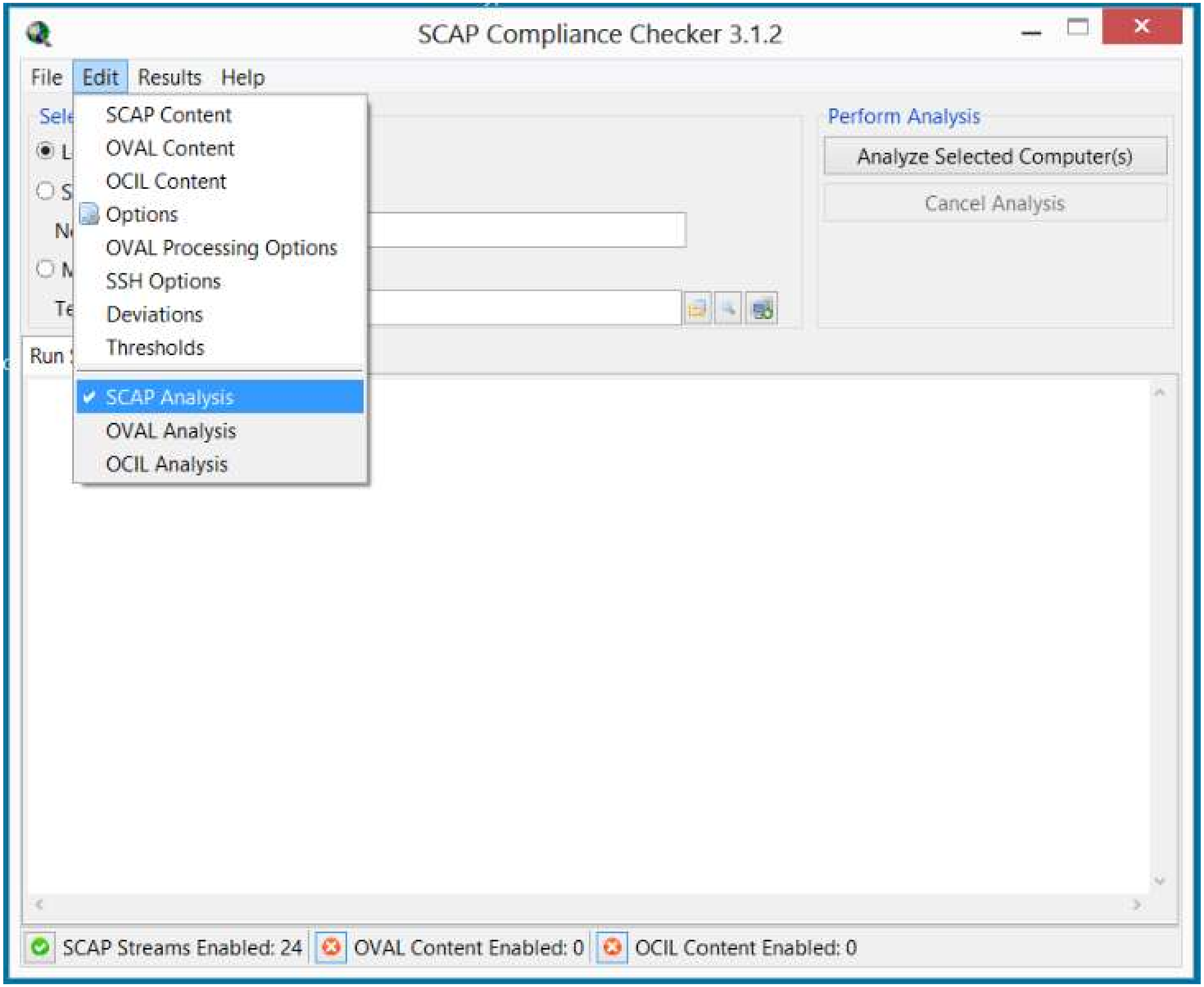
1.001 - Physical security
1.006 - Users with Administrative Privilege
1.007 - Members of the Backup Operators Group
1.008 - Shared User Accounts
1.010 - Access Restrictions to Logs
1.013 - System Recovery Backups
1.016 - Security Configuration Tools
2.001 - Incorrect ACLs for event logs
2.005 - Unsupported Service Packs
2.006 - System File ACLs
2.007 - File Auditing Configuration
2.008 - NTFS Requirement
2.009 - Strong Password Filtering
2.015 - File share ACLs
2.019 - Security-Related Software Patches
2.021 - Software Certificate Installation Files
2.022 - Disallow AutoPlay/Autorun from Autorun.inf
2.023 - Winlogon Registry Permissions
2.119 - Configure Automatic Updates
3.003 - Clear System Pagefile
3.004 - Secure Removable Media – CD-ROM
3.006 - Removable media devices - Floppies
3.007 - Display Shutdown Button
3.010 - Registry Key Auditing
3.011 - Legal Notice Display
3.013 - Caching of logon credentials
3.014 - Legal Banner Dialog Box Title
3.015 - Halt on Audit Failure
3.018 - Anonymous shares are not restricted
3.019 - Restrict Anonymous SAM Enumeration
3.027 - Printer Share Permissions
3.028 - Microsoft Strong Password Filtering
3.029 - Secure Print Driver Installation
3.030 - Anonymous Access to the Registry
3.031 - LanMan Authentication Level
3.032 - Ctrl+Alt+Del Security Attention Sequence
3.034 - Unencrypted Password is Sent to SMB Server.
3.040 - Disable Automatic Logon
3.042 - Signing of Secure Channel Traffic
3.043 - Encryption of Secure Channel Traffic
3.044 - Computer Account Password Reset

325 Rules Shown| | Displaying R...

```
Rule Title:  Physical security of the Automated Information System (AIS) does not meet DISA
requirements.
STIG ID: 1.001  Rule ID: SV-25996r1_rule  Vuln ID: V-1070
Severity: CAT II Class: Unclass
```

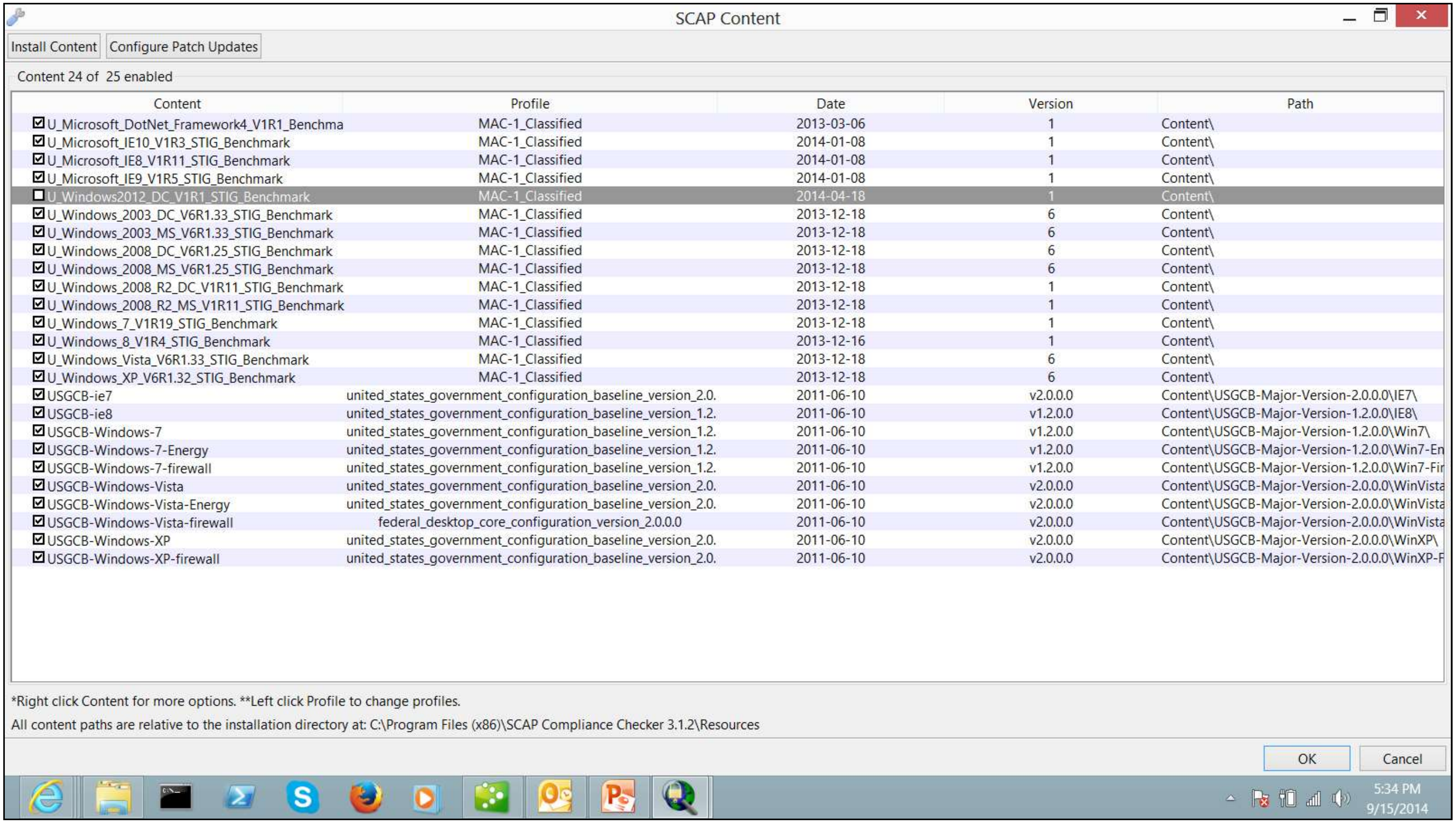
```
Discussion:
Inadequate physical protection can undermine all other security precautions utilized to
protect the system. This can jeopardize the confidentiality, availability, and integrity of
the system.  Physical security of the AIS is the first line protection of any system.

Documentable: No

Responsibility:
System Administrator

Check Content:
Interview the SA to determine if equipment is located in an access controlled area.

Note:  Servers will be located in rooms, or locked cabinets, that are accessible only to
authorized systems personnel.  Authorized user access should be verified at two points (i.e.
building access and server room).  User workstations containing sensitive data should be in
access controlled areas.

Fix Text:
Relocate equipment to a controlled access area.

IA Controls:PECF-1
```

DISA SCAP



✓ SCAP Streams Enabled: 24 | ☒ OVAL Content Enabled: 0 | ☒ OCIL Content Enabled: 0

DISA SCAP Contents



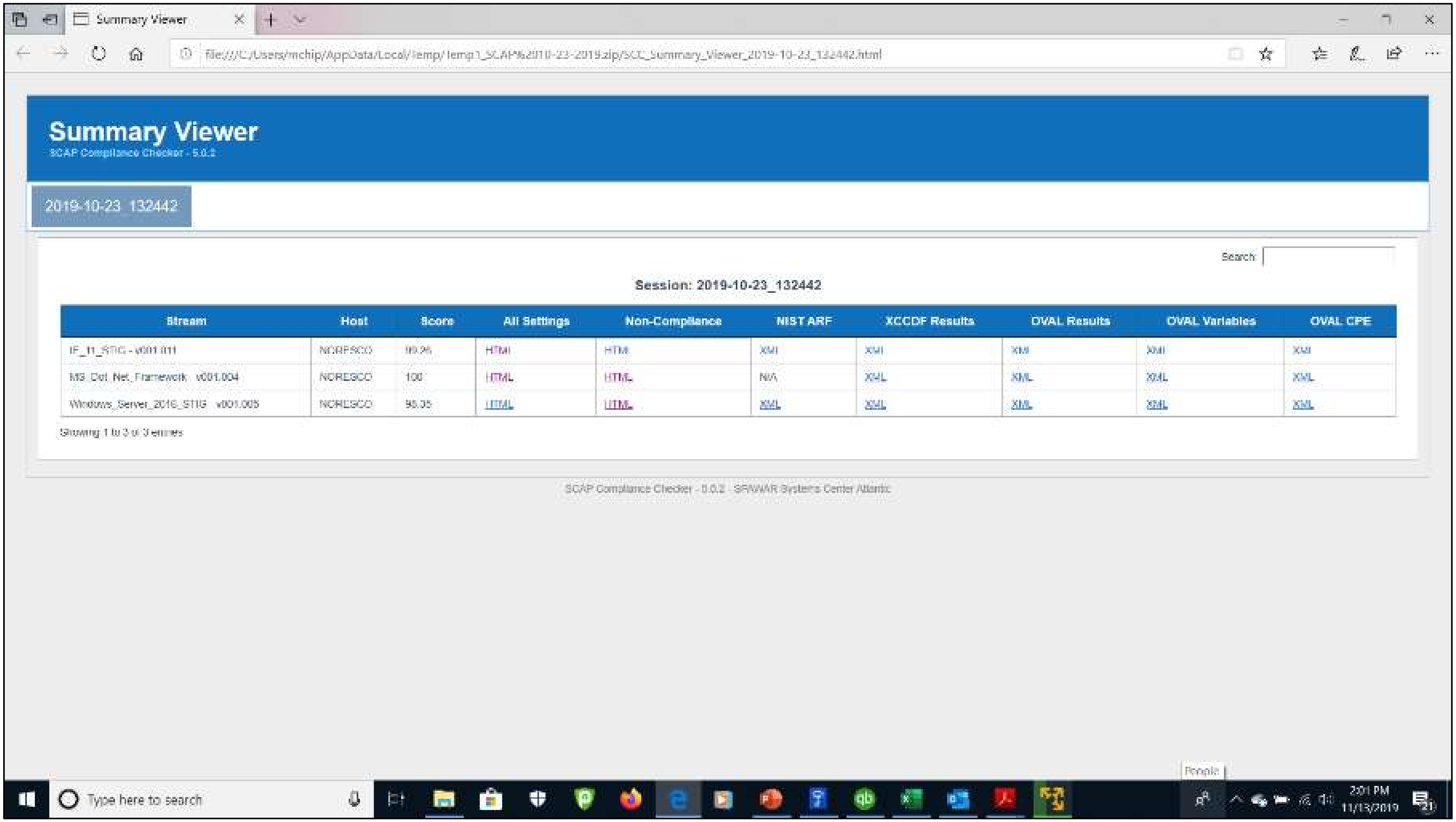
Content 24 of 25 enabled

Content	Profile	Date	Version	Path
☑ U_Microsoft_DotNet_Framework4_V1R1_Benchma	MAC-1_Classified	2013-03-06	1	Content\
☑ U_Microsoft_IE10_V1R3_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
☑ U_Microsoft_IE8_V1R11_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
☑ U_Microsoft_IE9_V1R5_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
☐ U_Windows2012_DC_V1R1_STIG_Benchmark	MAC-1_Classified	2014-04-18	1	Content\
☑ U_Windows_2003_DC_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ U_Windows_2003_MS_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ U_Windows_2008_DC_V6R1.25_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ U_Windows_2008_MS_V6R1.25_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ U_Windows_2008_R2_DC_V1R11_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
☑ U_Windows_2008_R2_MS_V1R11_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
☑ U_Windows_7_V1R19_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
☑ U_Windows_8_V1R4_STIG_Benchmark	MAC-1_Classified	2013-12-16	1	Content\
☑ U_Windows_Vista_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ U_Windows_XP_V6R1.32_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
☑ USGCB-ie7	united_states_government_configuration_baseline_version_2.0.	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\IE7\
☑ USGCB-ie8	united_states_government_configuration_baseline_version_1.2.	2011-06-10	v1.2.0.0	Content\USGCB-Major-Version-1.2.0.0\IE8\
☑ USGCB-Windows-7	united_states_government_configuration_baseline_version_1.2.	2011-06-10	v1.2.0.0	Content\USGCB-Major-Version-1.2.0.0\Win7\
☑ USGCB-Windows-7-Energy	united_states_government_configuration_baseline_version_1.2.	2011-06-10	v1.2.0.0	Content\USGCB-Major-Version-1.2.0.0\Win7-En
☑ USGCB-Windows-7-firewall	united_states_government_configuration_baseline_version_1.2.	2011-06-10	v1.2.0.0	Content\USGCB-Major-Version-1.2.0.0\Win7-Fir
☑ USGCB-Windows-Vista	united_states_government_configuration_baseline_version_2.0.	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\WinVista
☑ USGCB-Windows-Vista-Energy	united_states_government_configuration_baseline_version_2.0.	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\WinVista
☑ USGCB-Windows-Vista-firewall	federal_desktop_core_configuration_version_2.0.0.0	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\WinVista
☑ USGCB-Windows-XP	united_states_government_configuration_baseline_version_2.0.	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\WinXP\
☑ USGCB-Windows-XP-firewall	united_states_government_configuration_baseline_version_2.0.	2011-06-10	v2.0.0.0	Content\USGCB-Major-Version-2.0.0.0\WinXP-F

*Right click Content for more options. **Left click Profile to change profiles.

All content paths are relative to the installation directory at: C:\Program Files (x86)\SCAP Compliance Checker 3.1.2\Resources

DISA SCAP Results



Summary Viewer
file:///C:/Users/mchip/AppData/Local/Temp/Temp1_SCAP%2010-23-2019.zip/SCC_Summary_Viewer_2019-10-23_132442.html

Summary Viewer

SCAP Compliance Checker - 5.0.2

2019-10-23_132442

Search:

Session: 2019-10-23_132442

Stream	Host	Score	All Settings	Non-Compliance	NIST ARF	XCCDF Results	OVAL Results	OVAL Variables	OVAL CPE
IE_11_STIG - v001.011	NORESCO	99.26	HTML	HTML	XML	XML	XML	XML	XML
MS_Dot_Net_Framework - v001.004	NORESCO	100	HTML	HTML	N/A	XML	XML	XML	XML
Windows_Server_2016_STIG - v001.005	NORESCO	98.35	HTML	HTML	XML	XML	XML	XML	XML

Showing 1 to 3 of 3 entries

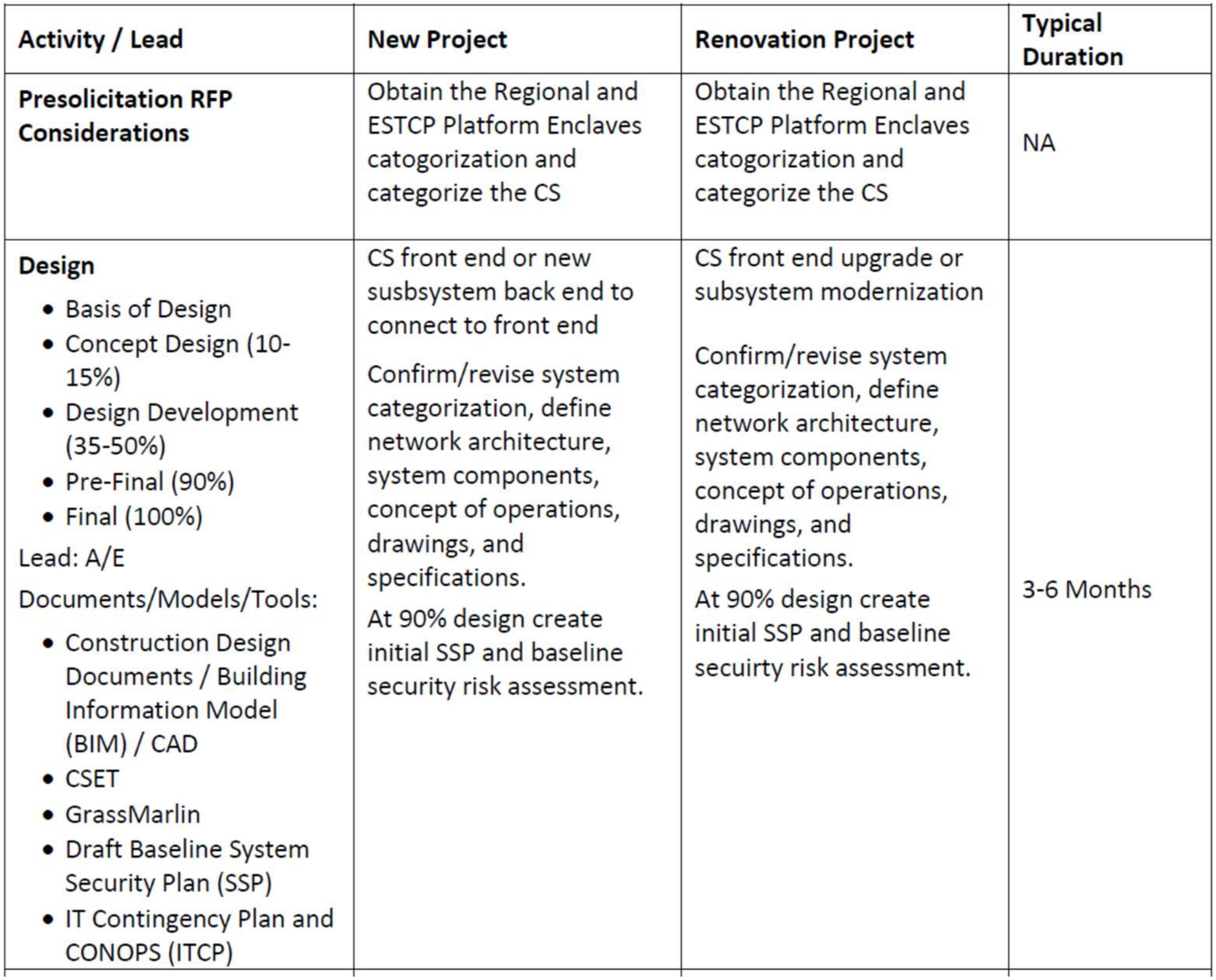
SCAP Compliance Checker - 5.0.2 - SPAWAR Systems Center Atlantic

Assemble the Stakeholders

The FRCS owner should assemble representatives from the following communities to participate in development of the FRCS PE authorization boundary and network architecture:

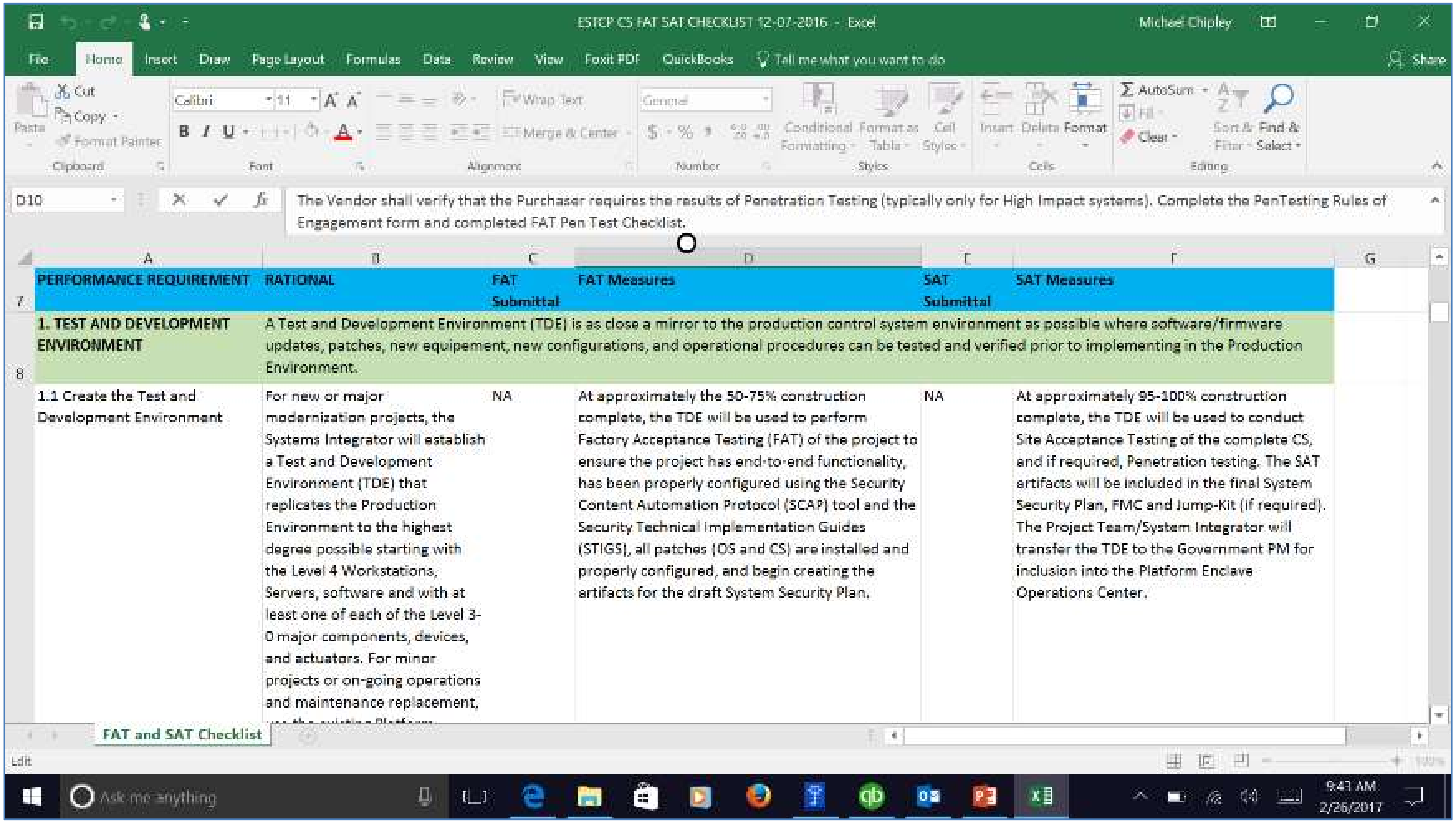
- Facility Engineer/Manager
- Facility Operations & Maintenance/Technician
- Physical Security Specialist
- Emergency Manager
- IT Network/Communications Specialist
- Information Assurance Specialist
- Tenants (Defense Health Agency, Defense Logistics Agency, etc)
- Operations and Maintenance Contractors
- Control System Vendor/Integrators
- Information Assurance IA/RMF Contractor

Cybersecurity Guideline Sequence



Activity / Lead	New Project	Renovation Project	Typical Duration
Presolicitation RFP Considerations	Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the CS	Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the CS	NA
Design • Basis of Design • Concept Design (10-15%) • Design Development (35-50%) • Pre-Final (90%) • Final (100%) Lead: A/E Documents/Models/Tools: • Construction Design Documents / Building Information Model (BIM) / CAD • CSET • GrassMarlin • Draft Baseline System Security Plan (SSP) • IT Contingency Plan and CONOPS (ITCP)	CS front end or new susbsystem back end to connect to front end Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline security risk assessment.	CS front end upgrade or subsystem modernization Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline secuirty risk assessment.	3-6 Months

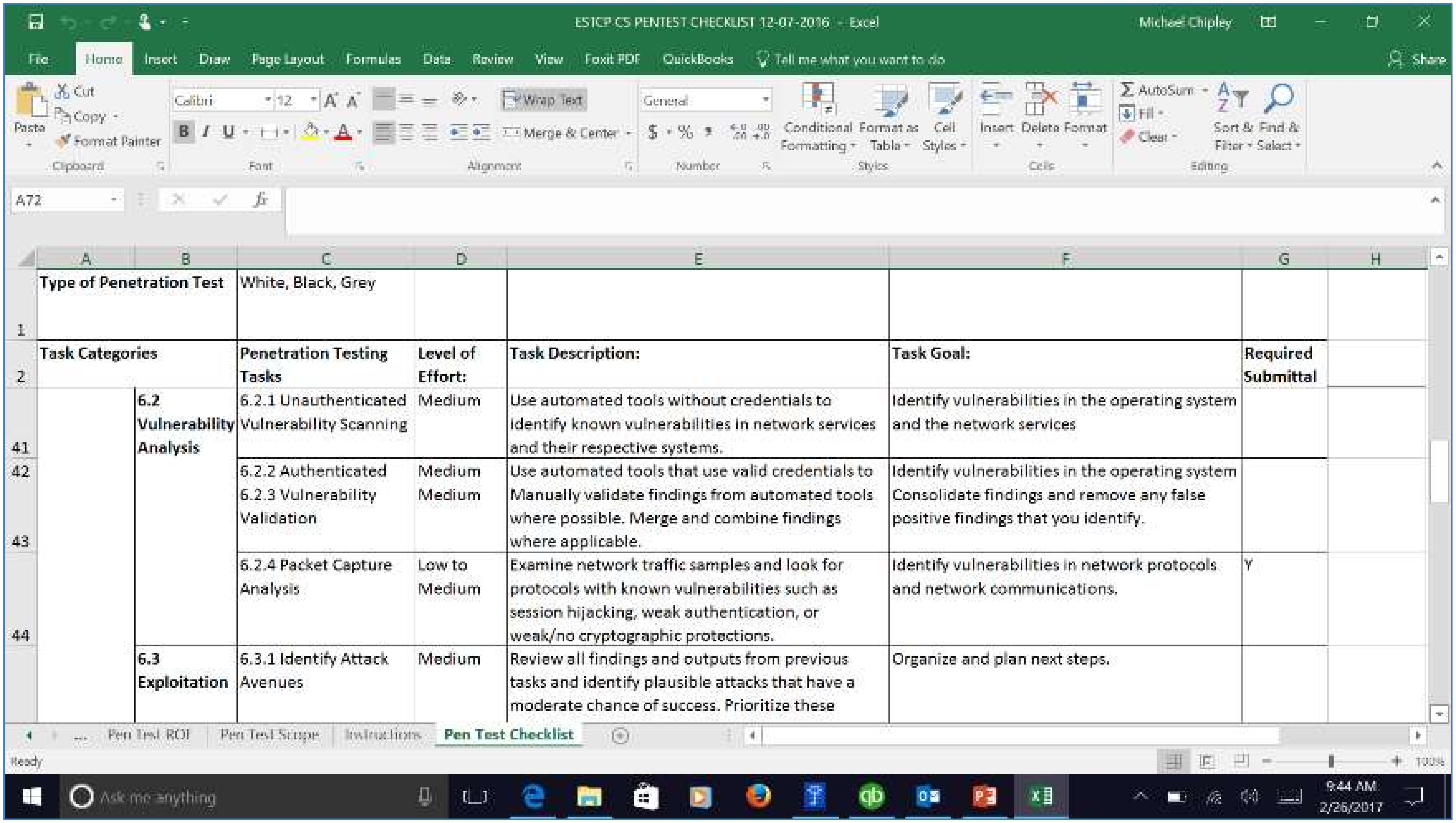
Cybersecurity Guideline FAT/SAT



The Vendor shall verify that the Purchaser requires the results of Penetration Testing (typically only for High Impact systems). Complete the PenTesting Rules of Engagement form and completed FAT Pen Test Checklist.

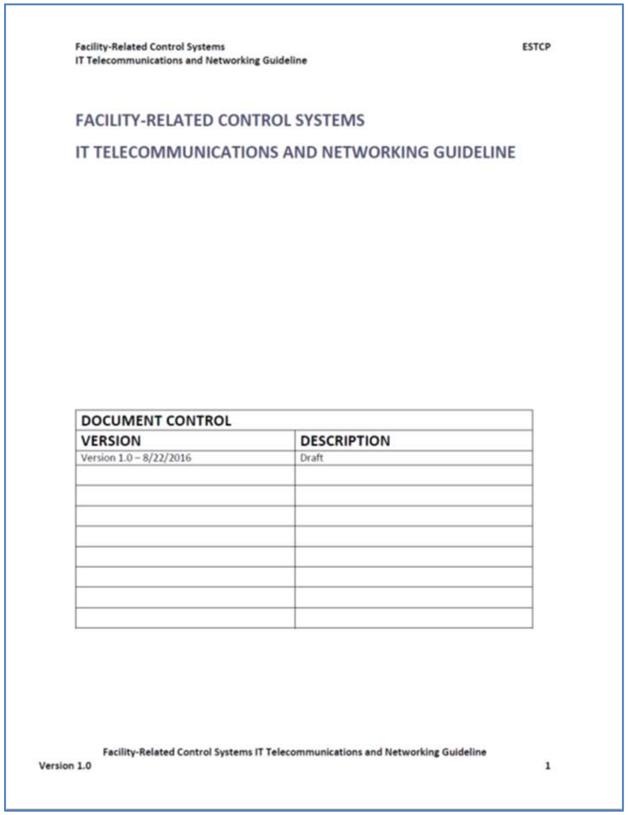
	A	B	C	D	E	F
7	**PERFORMANCE REQUIREMENT**	**RATIONAL**	**FAT Submittal**	**FAT Measures**	**SAT Submittal**	**SAT Measures**
8	**1. TEST AND DEVELOPMENT ENVIRONMENT**	A Test and Development Environment (TDE) is as close a mirror to the production control system environment as possible where software/firmware updates, patches, new equipement, new configurations, and operational procedures can be tested and verified prior to implementing in the Production Environment.				
	1.1 Create the Test and Development Environment	For new or major modernization projects, the Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators. For minor projects or on-going operations and maintenance replacement,	NA	At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and CS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.	NA	At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required). The Project Team/System Integrator will transfer the TDE to the Government PM for inclusion into the Platform Enclave Operations Center.

Cybersecurity Guideline Pen Test



	A	B	C	D	E	F	G	H
1	Type of Penetration Test		White, Black, Grey					
2	Task Categories		Penetration Testing Tasks	Level of Effort:	Task Description:	Task Goal:	Required Submittal	
41		6.2 Vulnerability Analysis	6.2.1 Unauthenticated Vulnerability Scanning	Medium	Use automated tools without credentials to identify known vulnerabilities in network services and their respective systems.	Identify vulnerabilities in the operating system and the network services		
42			6.2.2 Authenticated	Medium	Use automated tools that use valid credentials to	Identify vulnerabilities in the operating system		
43			6.2.3 Vulnerability Validation	Medium	Manually validate findings from automated tools where possible. Merge and combine findings where applicable.	Consolidate findings and remove any false positive findings that you identify.		
44			6.2.4 Packet Capture Analysis	Low to Medium	Examine network traffic samples and look for protocols with known vulnerabilities such as session hijacking, weak authentication, or weak/no cryptographic protections.	Identify vulnerabilities in network protocols and network communications.	Y	
		6.3 Exploitation	6.3.1 Identify Attack Avenues	Medium	Review all findings and outputs from previous tasks and identify plausible attacks that have a moderate chance of success. Prioritize these	Organize and plan next steps.		

Telecommunications and Network Guideline



Facility-Related Control Systems
IT Telecommunications and Networking Guideline

ESTCP

FACILITY-RELATED CONTROL SYSTEMS

IT TELECOMMUNICATIONS AND NETWORKING GUIDELINE

DOCUMENT CONTROL	
VERSION	**DESCRIPTION**
Version 1.0 – 8/22/2016	Draft

Facility-Related Control Systems IT Telecommunications and Networking Guideline

Version 1.0

1

1.1 PURPOSE AND SCOPE This document defines the IT Telecommunications and Network Standards for ESTCP Facility-Related Control System (FRCS) projects. The intention of this document is to provide a general outline and guide to ensure the IT Telecommunications and Network Transport Backbone, cabling, wireless, firewalls, routers, switches and end-point devices are properly installed, configured and tested to meet DoD CIO, DISA and service/agency connectivity requirements.

Telecommunications and Network Guideline

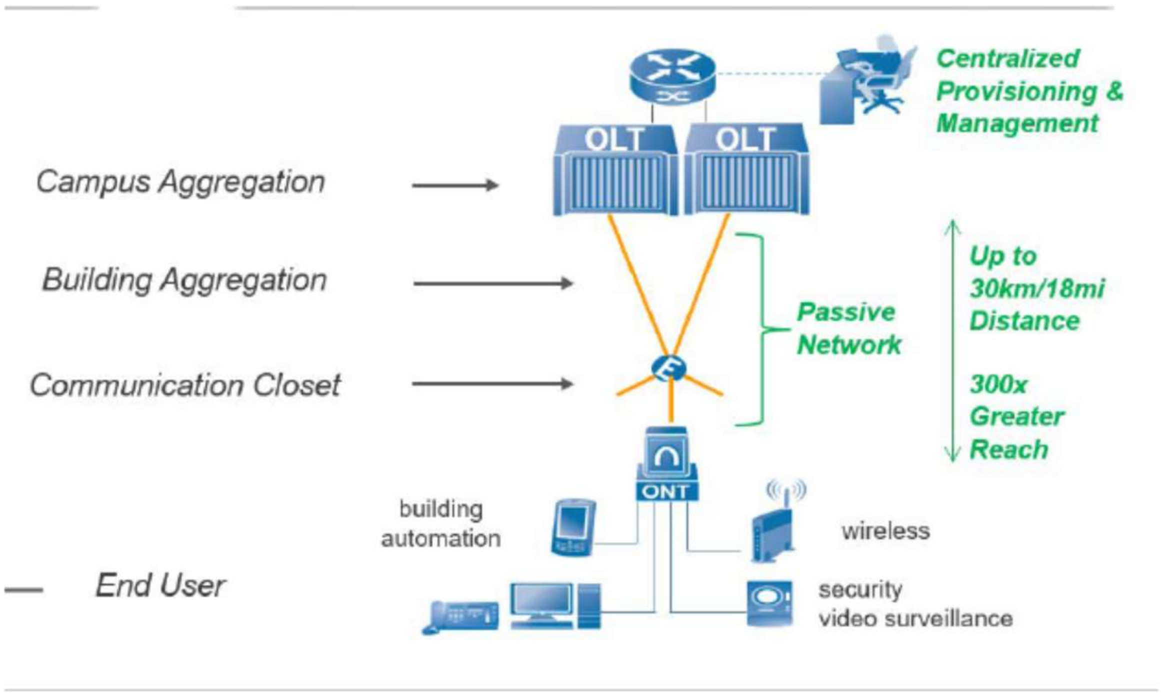
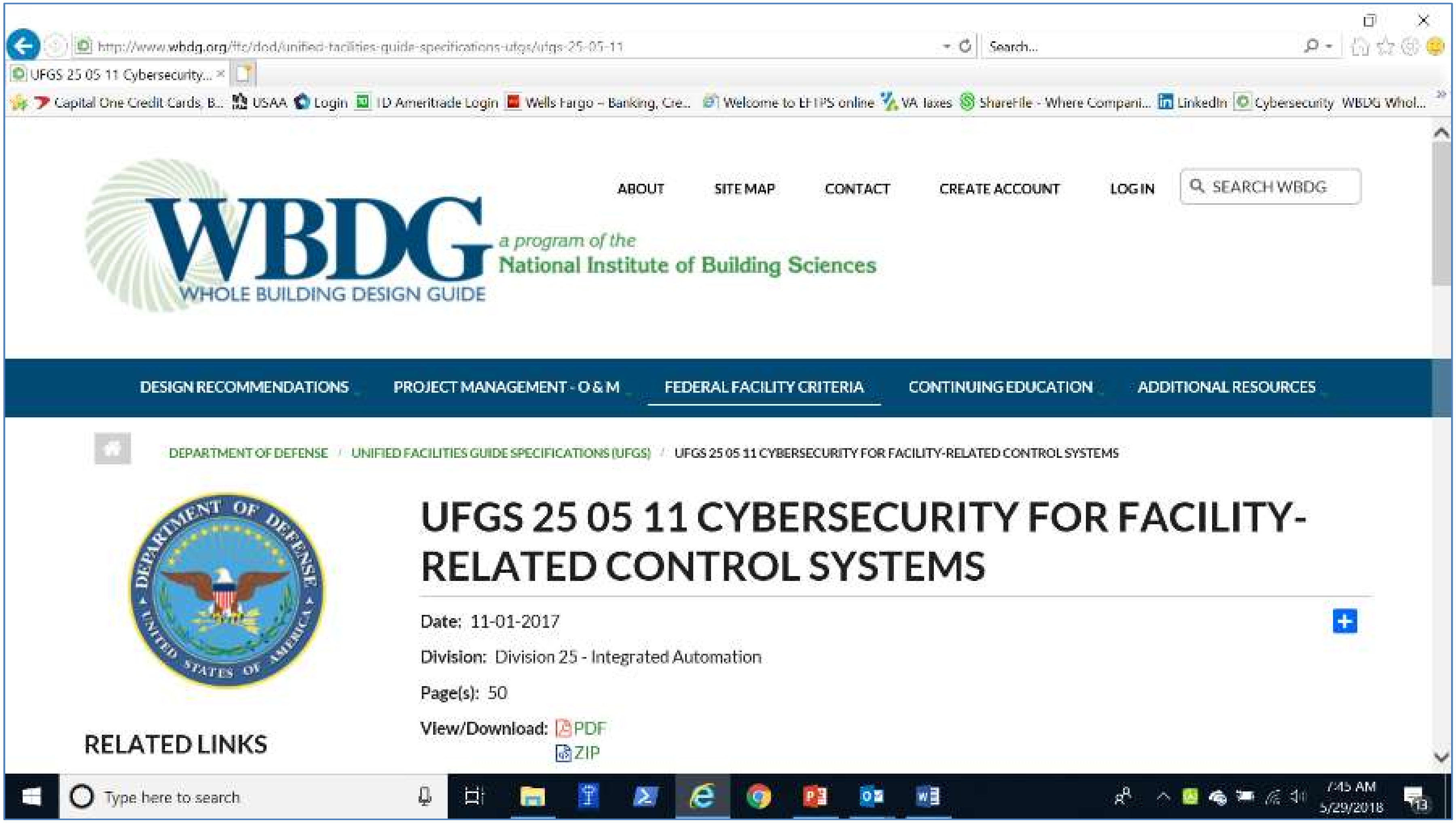


Figure 5.3 – End to End PON Schema

A passive optical network (PON) is a point-to-multipoint network architecture in which unpowered optical splitters are used to enable a single optical fiber strand to serve multiple end-points. Passive optical LANs are an implementation of PON technology for the enterprise LAN (e.g., large Layer 2 Ethernet networks). The solution reduces physical cabling infrastructure, minimizes the telecommunications space requirements through the use of passive optical splitters, and reduces the typical energy requirements to support traditional Ethernet deployments.

UFGS 25 05 11 Cybersecurity For FRCS


http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11
Search...
UFGS 25 05 11 Cybersecurity...
Capital One Credit Cards, B...
USAA
Login
TD Ameritrade Login
Wells Fargo – Banking, Cre...
Welcome to EFTPS online
VA Taxes
ShareFile - Where Compani...
LinkedIn
Cybersecurity WBDG Whol...
WBDG
WHOLE BUILDING DESIGN GUIDE
a program of the
National Institute of Building Sciences
ABOUT
SITE MAP
CONTACT
CREATE ACCOUNT
LOG IN
SEARCH WBDG
DESIGN RECOMMENDATIONS
PROJECT MANAGEMENT - O & M
FEDERAL FACILITY CRITERIA
CONTINUING EDUCATION
ADDITIONAL RESOURCES
Type here to search
7:45 AM
5/29/2018

DEPARTMENT OF DEFENSE / UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS) / UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

Date: 11-01-2017

Division: Division 25 - Integrated Automation

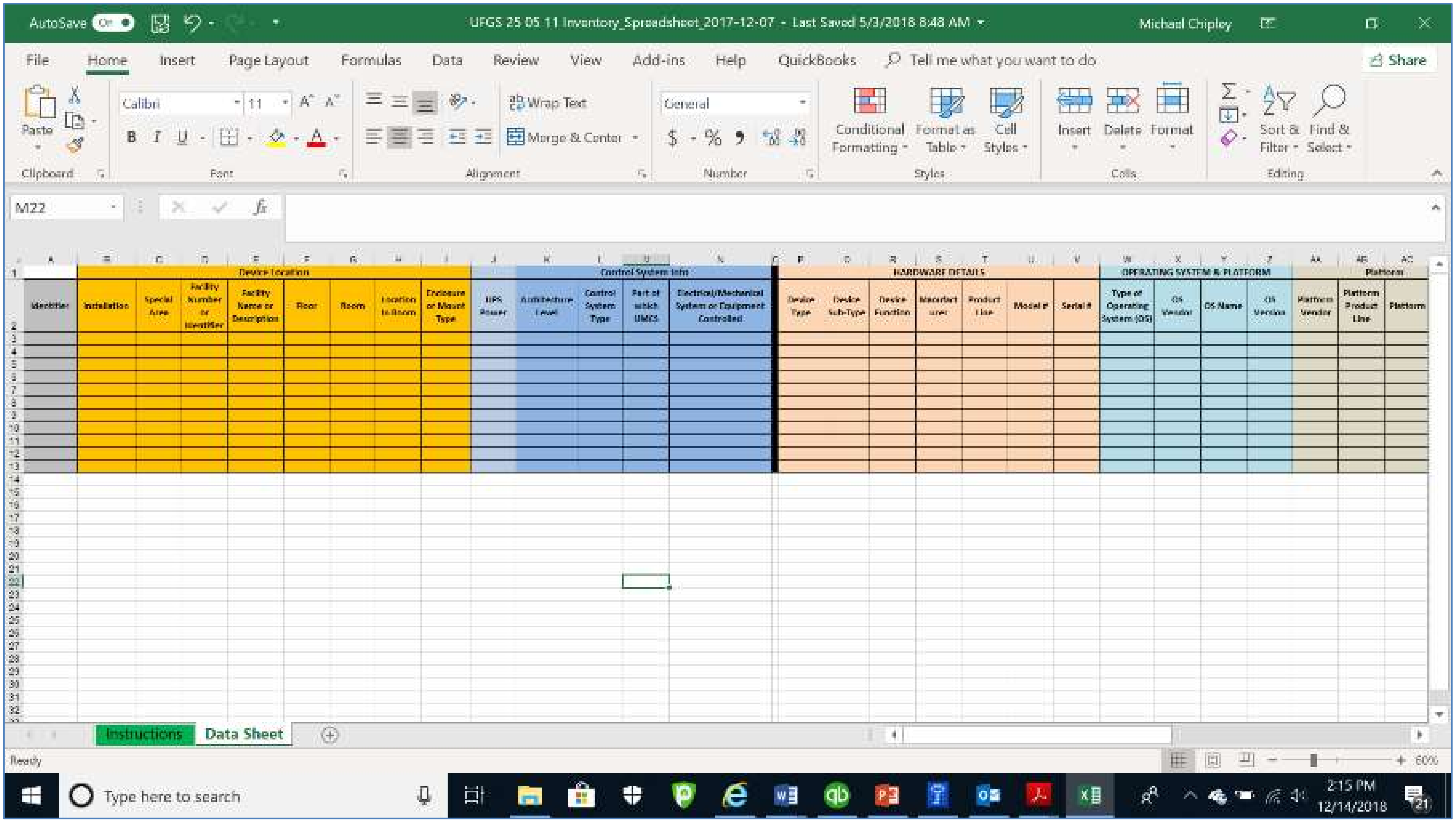
Page(s): 50

View/Download: PDF
ZIP

RELATED LINKS

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

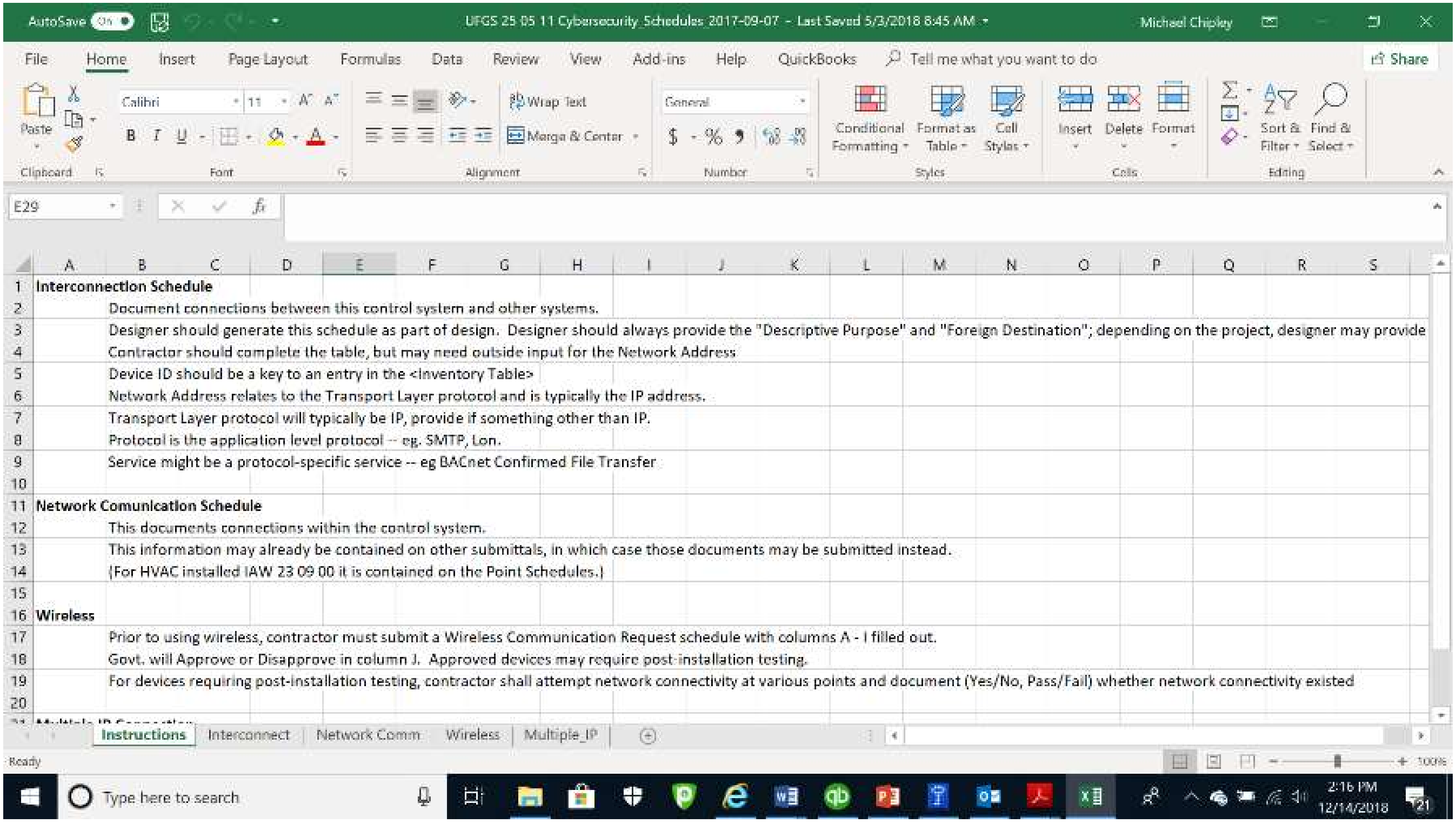
UFGS 25 05 11 Inventory



	Device Location								Control System Info					HARDWARE DETAILS							OPERATING SYSTEM & PLATFORM				Platform		
Identifier	Installation	Special Area	Facility Number or Identifier	Facility Name or Description	Floor	Room	Location in Room	Enclosure or Mount Type	UPS Power	Architecture Level	Control System Type	Part of which UMCS	Electrical/Mechanical System or Equipment Controlled	Device Type	Device Sub-Type	Device Function	Manufact urer	Product Line	Model #	Serial #	Type of Operating System (OS)	OS Vendor	OS Name	OS Version	Platform Vendor	Platform Product Line	Platform

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

UFGS 25 05 11 Schedules



Interconnection Schedule

Document connections between this control system and other systems.

Designer should generate this schedule as part of design. Designer should always provide the "Descriptive Purpose" and "Foreign Destination"; depending on the project, designer may provide

Contractor should complete the table, but may need outside input for the Network Address

Device ID should be a key to an entry in the <Inventory Table>

Network Address relates to the Transport Layer protocol and is typically the IP address.

Transport Layer protocol will typically be IP, provide if something other than IP.

Protocol is the application level protocol -- eg. SMTP, Lon.

Service might be a protocol-specific service -- eg BACnet Confirmed File Transfer

Network Comunication Schedule

This documents connections within the control system.

This information may already be contained on other submittals, in which case those documents may be submitted instead.

(For HVAC installed IAW 23 09 00 it is contained on the Point Schedules.)

Wireless

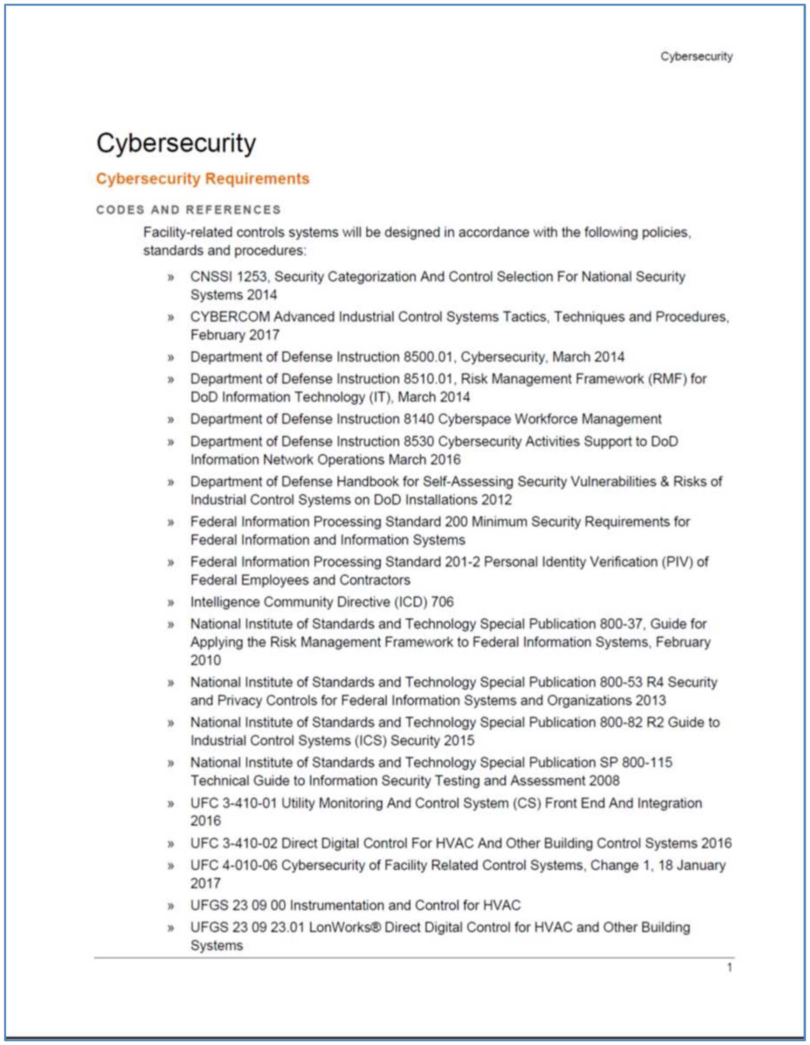
Prior to using wireless, contractor must submit a Wireless Communication Request schedule with columns A - I filled out.

Govt. will Approve or Disapprove in column J. Approved devices may require post-installation testing.

For devices requiring post-installation testing, contractor shall attempt network connectivity at various points and document (Yes/No, Pass/Fail) whether network connectivity existed

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

Create the Cyber Narrative



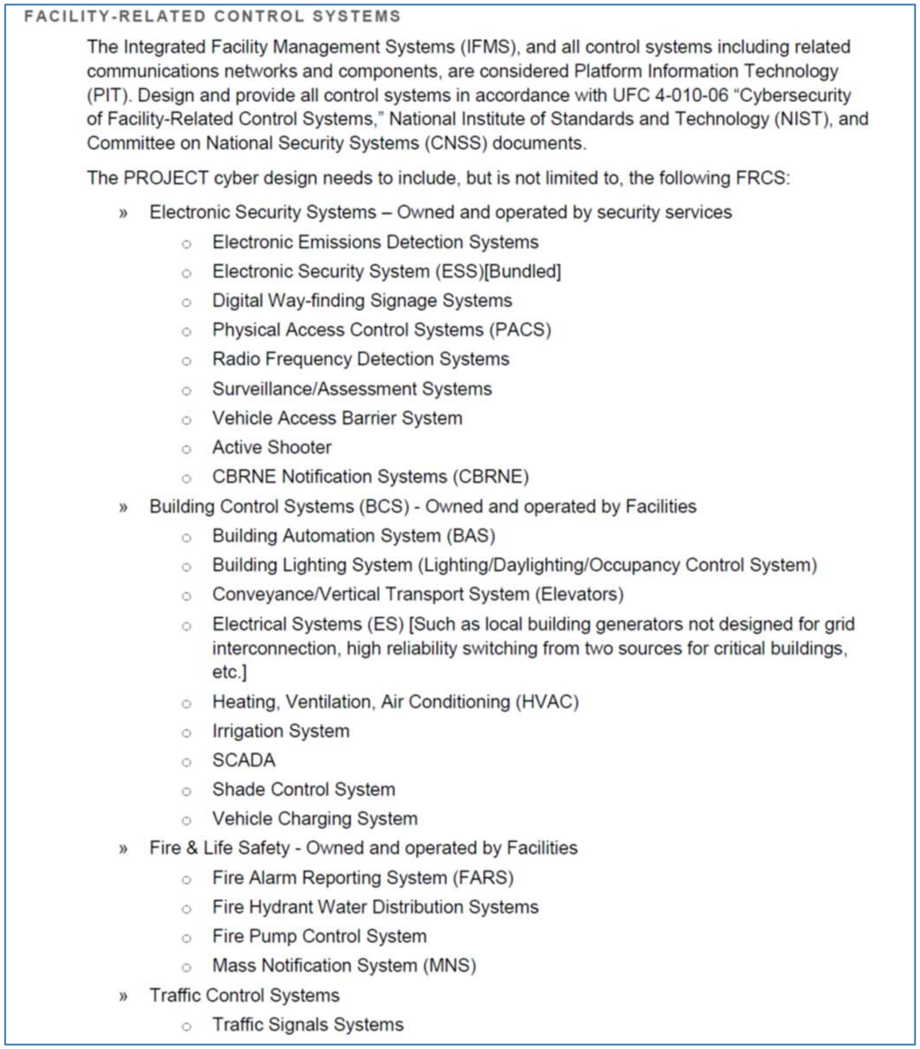
Cybersecurity

Cybersecurity Requirements

CODES AND REFERENCES

Facility-related controls systems will be designed in accordance with the following policies, standards and procedures:

- CNSSI 1253, Security Categorization And Control Selection For National Security Systems 2014
- CYBERCOM Advanced Industrial Control Systems Tactics, Techniques and Procedures, February 2017
- Department of Defense Instruction 8500.01, Cybersecurity, March 2014
- Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014
- Department of Defense Instruction 8140 Cyberspace Workforce Management
- Department of Defense Instruction 8530 Cybersecurity Activities Support to DoD Information Network Operations March 2016
- Department of Defense Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations 2012
- Federal Information Processing Standard 200 Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- Intelligence Community Directive (ICD) 706
- National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- National Institute of Standards and Technology Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations 2013
- National Institute of Standards and Technology Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015
- National Institute of Standards and Technology Special Publication SP 800-115 Technical Guide to Information Security Testing and Assessment 2008
- UFC 3-410-01 Utility Monitoring And Control System (CS) Front End And Integration 2016
- UFC 3-410-02 Direct Digital Control For HVAC And Other Building Control Systems 2016
- UFC 4-010-06 Cybersecurity of Facility Related Control Systems, Change 1, 18 January 2017
- UFGS 23 09 00 Instrumentation and Control for HVAC
- UFGS 23 09 23.01 LonWorks® Direct Digital Control for HVAC and Other Building Systems



FACILITY-RELATED CONTROL SYSTEMS

The Integrated Facility Management Systems (IFMS), and all control systems including related communications networks and components, are considered Platform Information Technology (PIT). Design and provide all control systems in accordance with UFC 4-010-06 "Cybersecurity of Facility-Related Control Systems," National Institute of Standards and Technology (NIST), and Committee on National Security Systems (CNSS) documents.

The PROJECT cyber design needs to include, but is not limited to, the following FRCS:

- Electronic Security Systems – Owned and operated by security services
  - Electronic Emissions Detection Systems
  - Electronic Security System (ESS)[Bundled]
  - Digital Way-finding Signage Systems
  - Physical Access Control Systems (PACS)
  - Radio Frequency Detection Systems
  - Surveillance/Assessment Systems
  - Vehicle Access Barrier System
  - Active Shooter
  - CBRNE Notification Systems (CBRNE)
- Building Control Systems (BCS) - Owned and operated by Facilities
  - Building Automation System (BAS)
  - Building Lighting System (Lighting/Daylighting/Occupancy Control System)
  - Conveyance/Vertical Transport System (Elevators)
  - Electrical Systems (ES) [Such as local building generators not designed for grid interconnection, high reliability switching from two sources for critical buildings, etc.]
  - Heating, Ventilation, Air Conditioning (HVAC)
  - Irrigation System
  - SCADA
  - Shade Control System
  - Vehicle Charging System
- Fire & Life Safety - Owned and operated by Facilities
  - Fire Alarm Reporting System (FARS)
  - Fire Hydrant Water Distribution Systems
  - Fire Pump Control System
  - Mass Notification System (MNS)
- Traffic Control Systems
  - Traffic Signals Systems

Assign Cyber Team

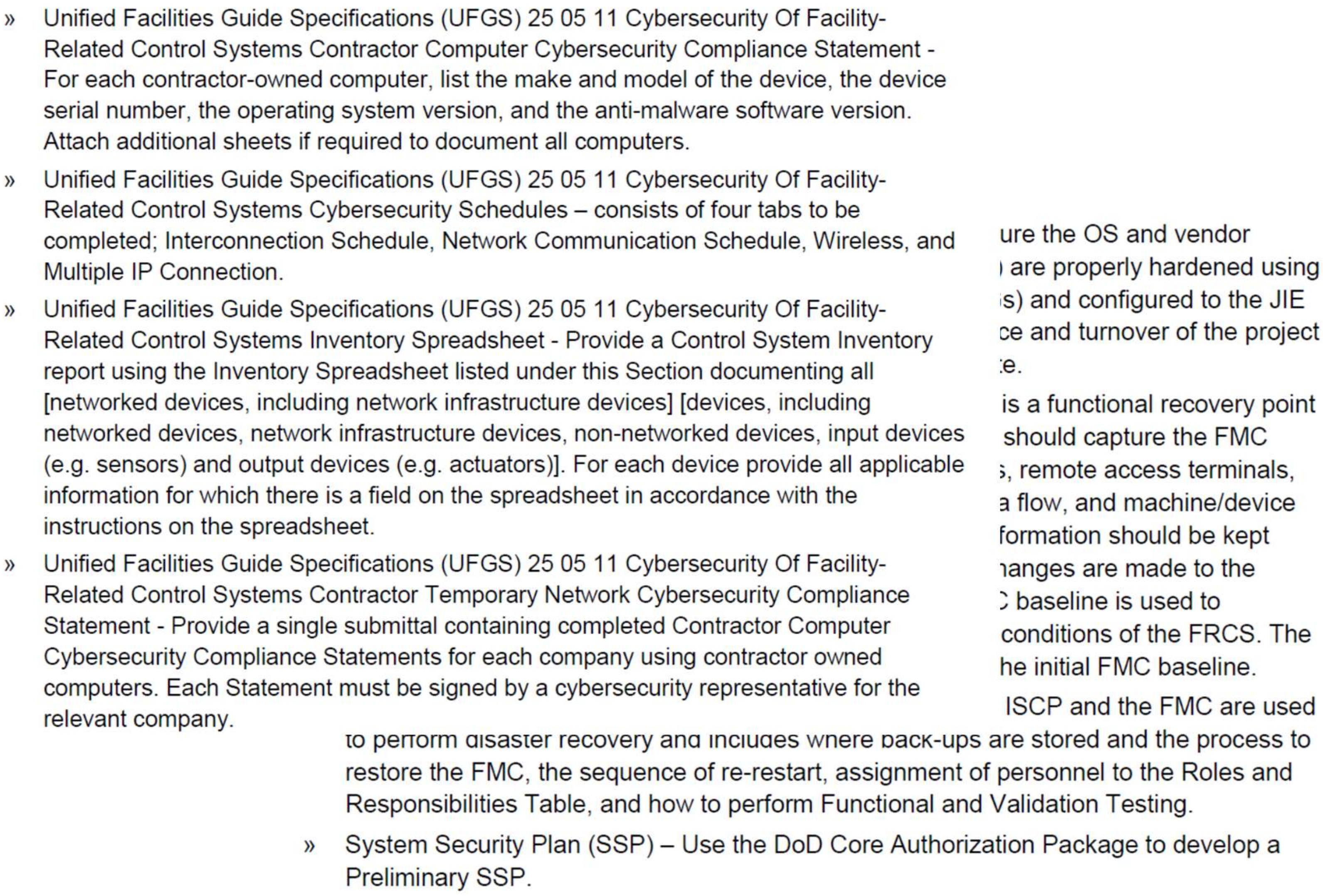
CYBERSECURITY TEAM PERSONNEL

The PROJECT Cybersecurity Team is comprised of highly skilled and certified IT and OT cybersecurity subject matter experts with extensive experience with the NIST Risk Management Framework and the DoD implementation of the RMF:

Cyber Team Lead: GICSP or CISSP
Cyber System Administrator: MCSE, Security +
Cyber Commissioning: CEM, CISSP, CEH, CxA, DGCP
Cyber Auditing: CDFM, CFE, CISA, CPA

The Cyber Team will be responsible for the project cyber lifecycle and will begin at project award with a Cyber Workshop Charette to baseline the PROJECT Team and **initiate the development of the RMF package documents, begin the auditing of the PROJECT Team's project NIST 800-171 Cyber Risk Management Plans (CRMP), create the Test and Development Environment (TDE), perform system hardening (SCAP/STIGS) of the equipment and components, create and manage the Fully-Mission Capable Baseline (FMC), perform sysadmin duties on the TDE and Production OT systems, audit the FRCS, and perform cyber commissioning of the facility.**

Cyber Commissioning



- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Contractor Computer Cybersecurity Compliance Statement - For each contractor-owned computer, list the make and model of the device, the device serial number, the operating system version, and the anti-malware software version. Attach additional sheets if required to document all computers.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Cybersecurity Schedules – consists of four tabs to be completed; Interconnection Schedule, Network Communication Schedule, Wireless, and Multiple IP Connection.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Inventory Spreadsheet - Provide a Control System Inventory report using the Inventory Spreadsheet listed under this Section documenting all [networked devices, including network infrastructure devices] [devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators)]. For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Contractor Temporary Network Cybersecurity Compliance Statement - Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Each Statement must be signed by a cybersecurity representative for the relevant company.

ure the OS and vendor
are properly hardened using
s) and configured to the JIE
ce and turnover of the project
e.

is a functional recovery point
should capture the FMC
, remote access terminals,
a flow, and machine/device
formation should be kept
nanges are made to the
baseline is used to
conditions of the FRCS. The
he initial FMC baseline.

ISCP and the FMC are used
to perform disaster recovery and includes where back-ups are stored and the process to restore the FMC, the sequence of re-restart, assignment of personnel to the Roles and Responsibilities Table, and how to perform Functional and Validation Testing.

- System Security Plan (SSP) – Use the DoD Core Authorization Package to develop a Preliminary SSP.

Unit 5

Using CSET: SAL, Network Arch Diagram, Inventory, Templates, Security Controls Evaluation, Reports, Data Aggregation & Trending, System Security Plan

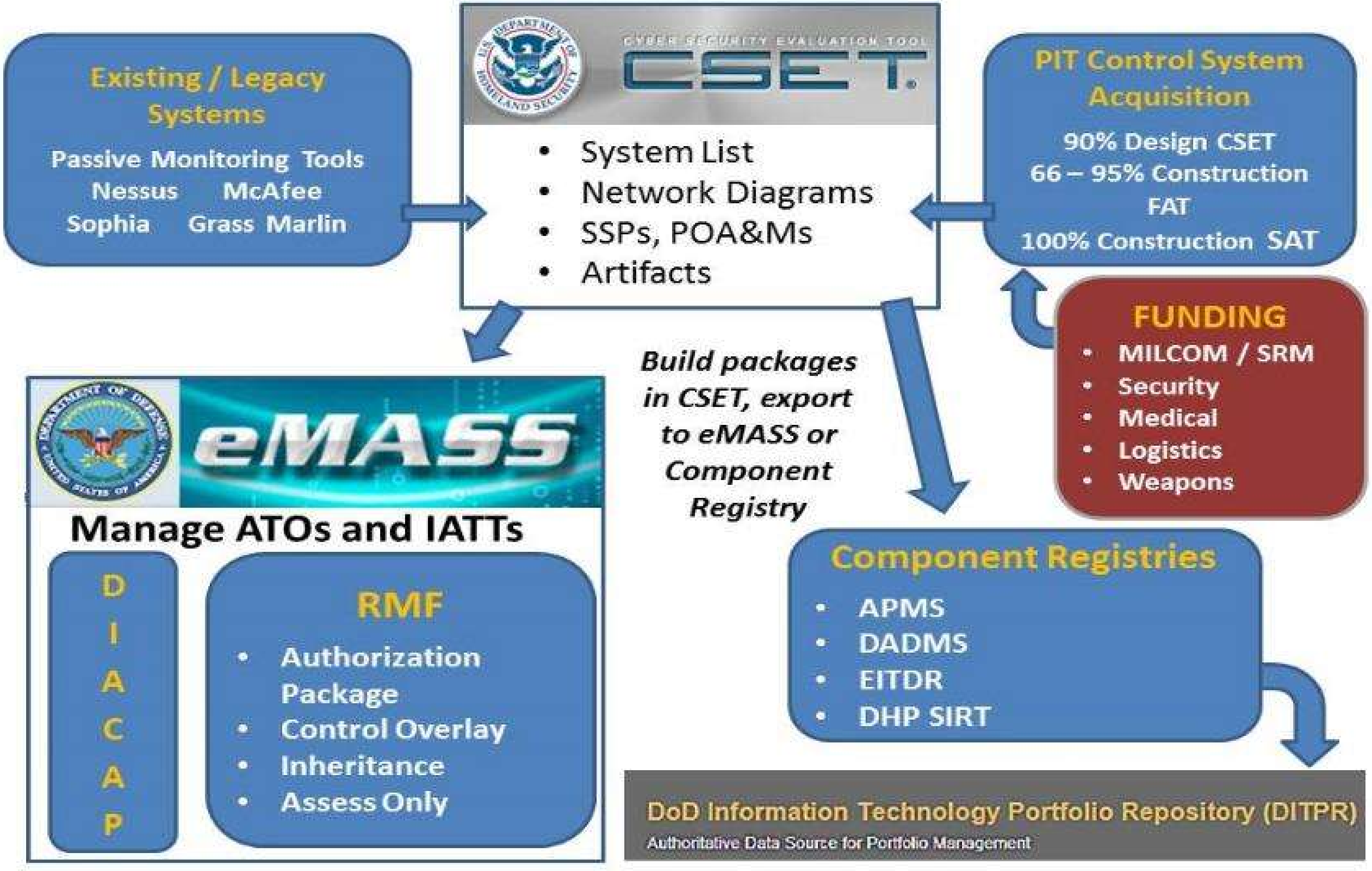
DHS CSET

- Stand-alone Software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

www.ics-cert.us-cert.gov/Downloading-and-Installing-CSET

CSET and eMASS Relationship



CYBER SECURITY EVALUATION TOOL CSET

- System List
- Network Diagrams
- SSPs, POA&Ms
- Artifacts

Existing / Legacy Systems

Passive Monitoring Tools
Nessus McAfee
Sophia Grass Marlin

PIT Control System Acquisition

90% Design CSET
66 – 95% Construction
FAT
100% Construction SAT

FUNDING

- MILCOM / SRM
- Security
- Medical
- Logistics
- Weapons

Build packages in CSET, export to eMASS or Component Registry

eMASS

Manage ATOs and IATTs

D I A C A P

RMF

- Authorization Package
- Control Overlay
- Inheritance
- Assess Only

Component Registries

- APMS
- DADMS
- EITDR
- DHP SIRT

DoD Information Technology Portfolio Repository (DITPR)
Authoritative Data Source for Portfolio Management

Vendors/Contractor can use CSET to build eMASS packages!!

CSET Process

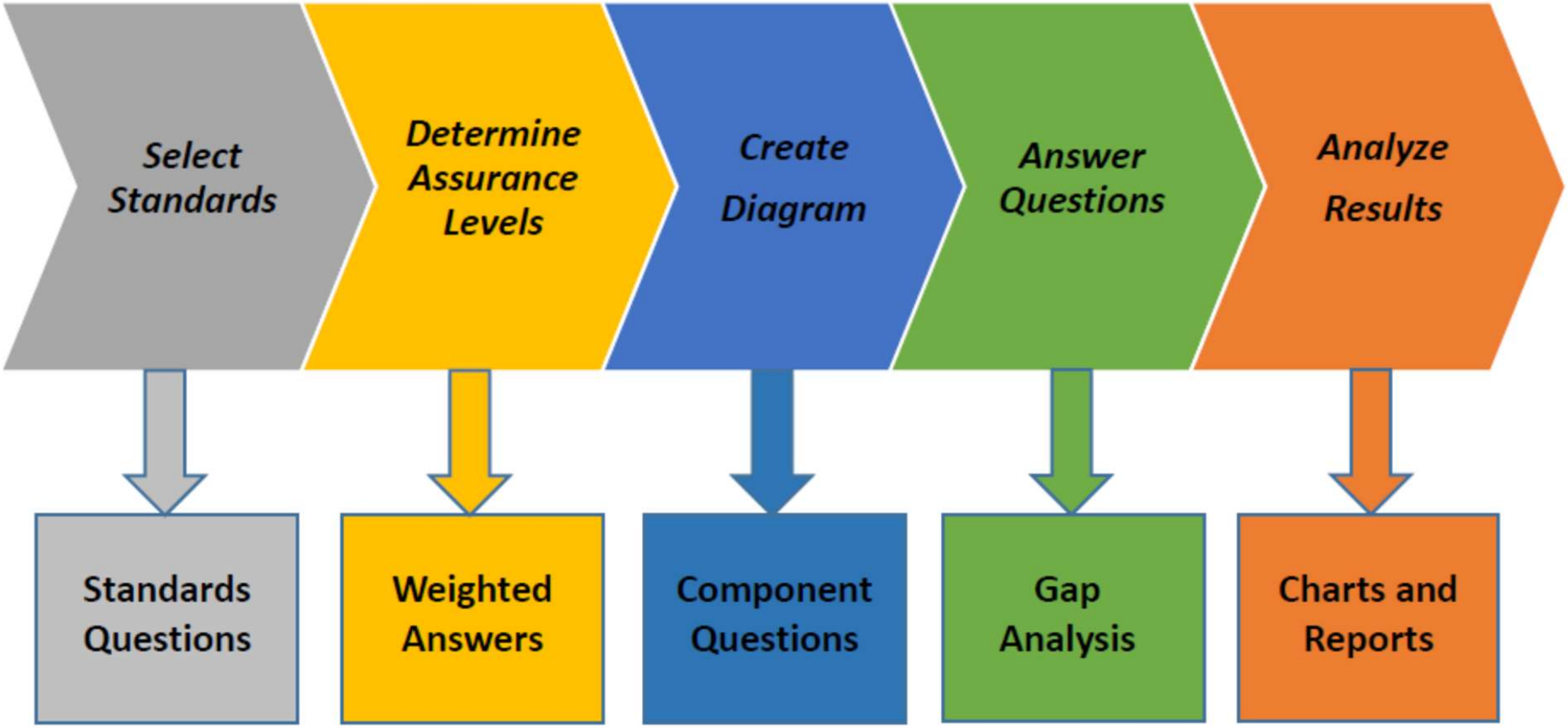
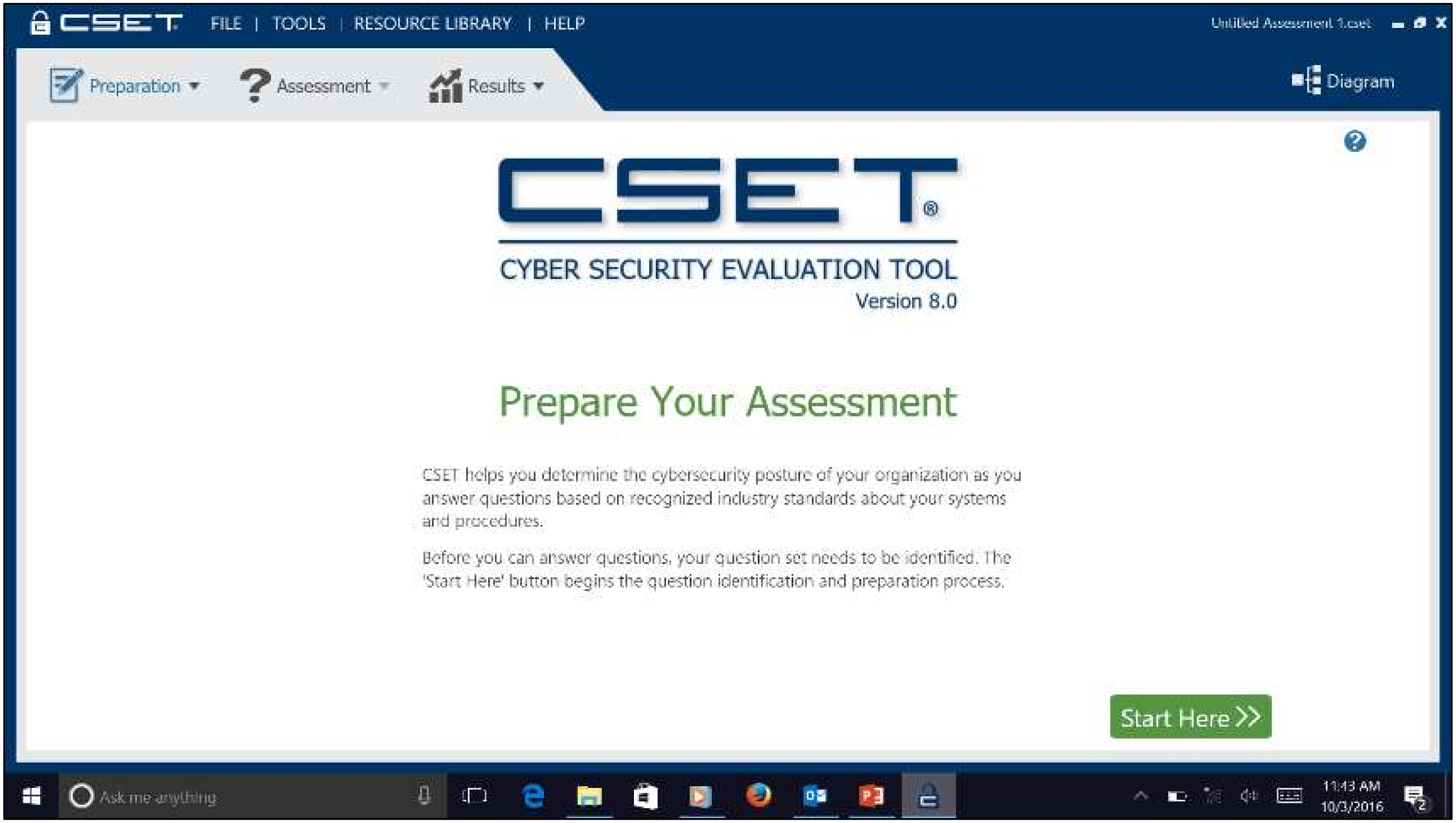


Figure 3-1. CSET process.

CSET Start

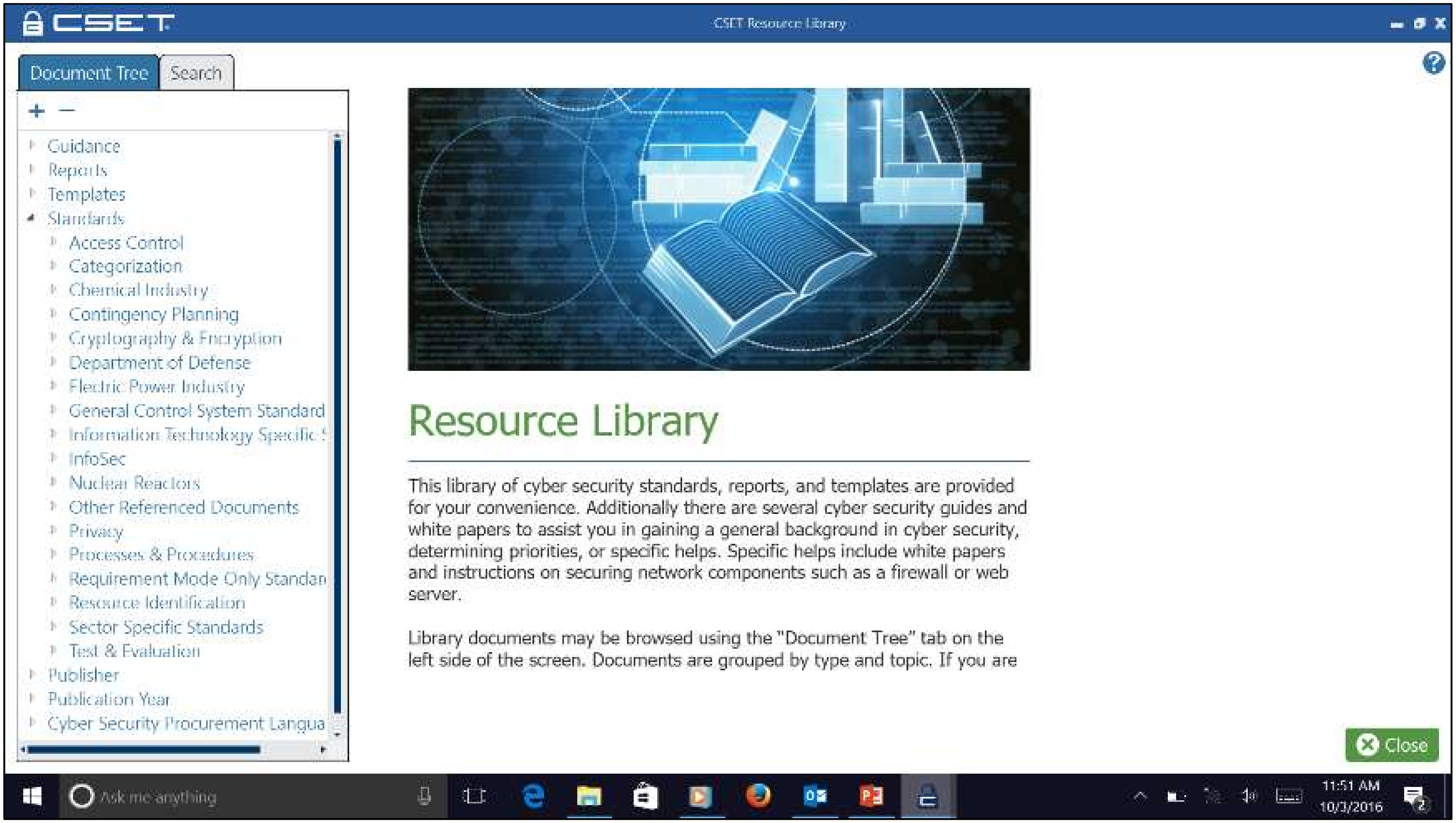

FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset
Preparation
Assessment
Results
Diagram
CSET®
CYBER SECURITY EVALUATION TOOL
Version 8.0

Prepare Your Assessment

CSET helps you determine the cybersecurity posture of your organization as you answer questions based on recognized industry standards about your systems and procedures.

Before you can answer questions, your question set needs to be identified. The 'Start Here' button begins the question identification and preparation process.

Resource Library

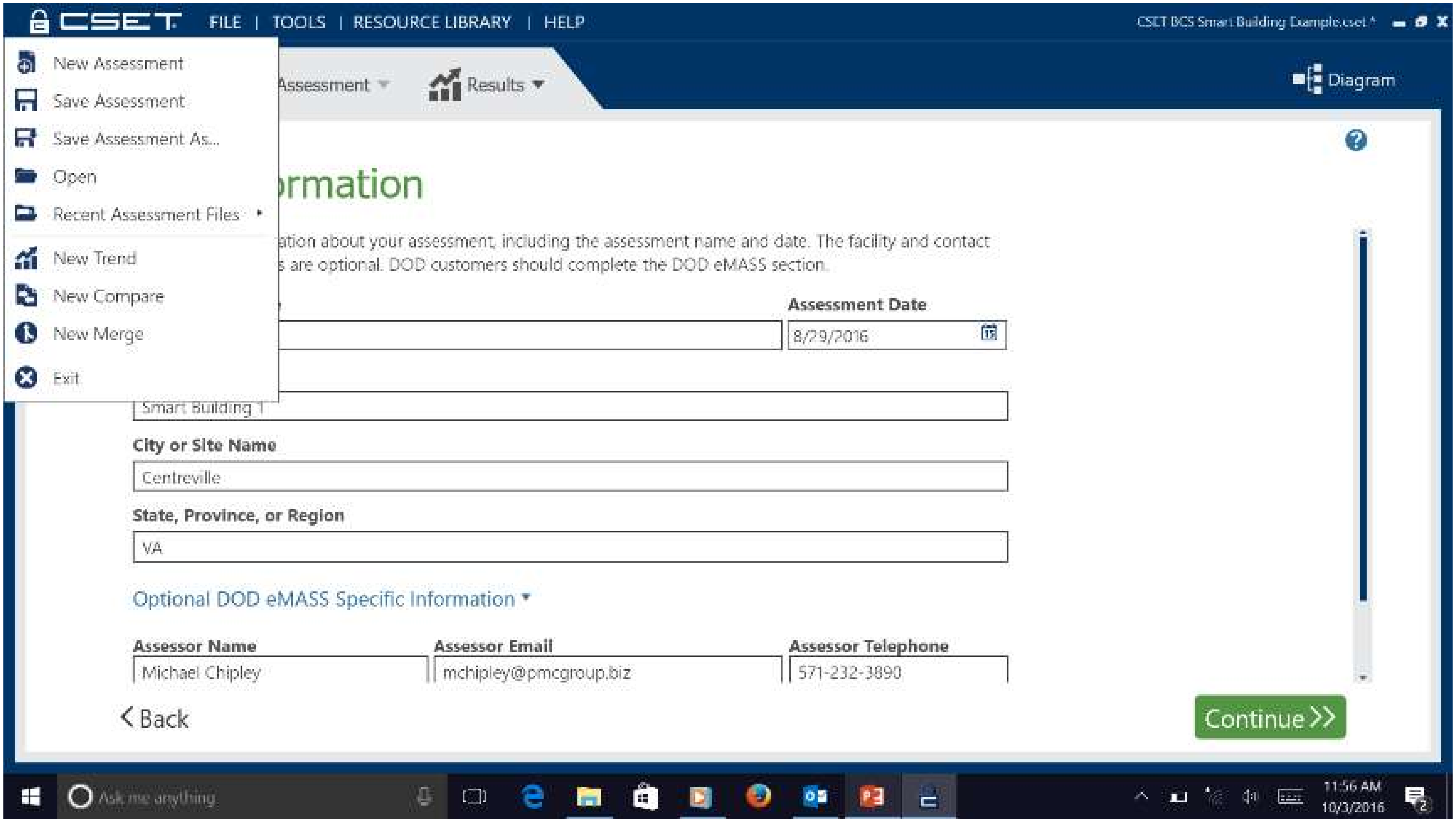


Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific helps. Specific helps include white papers and instructions on securing network components such as a firewall or web server.

Library documents may be browsed using the "Document Tree" tab on the left side of the screen. Documents are grouped by type and topic. If you are

Home and Site Information



rmation

ation about your assessment, including the assessment name and date. The facility and contact s are optional. DOD customers should complete the DOD eMASS section.

Assessment Date: 8/29/2016

Smart Building 1

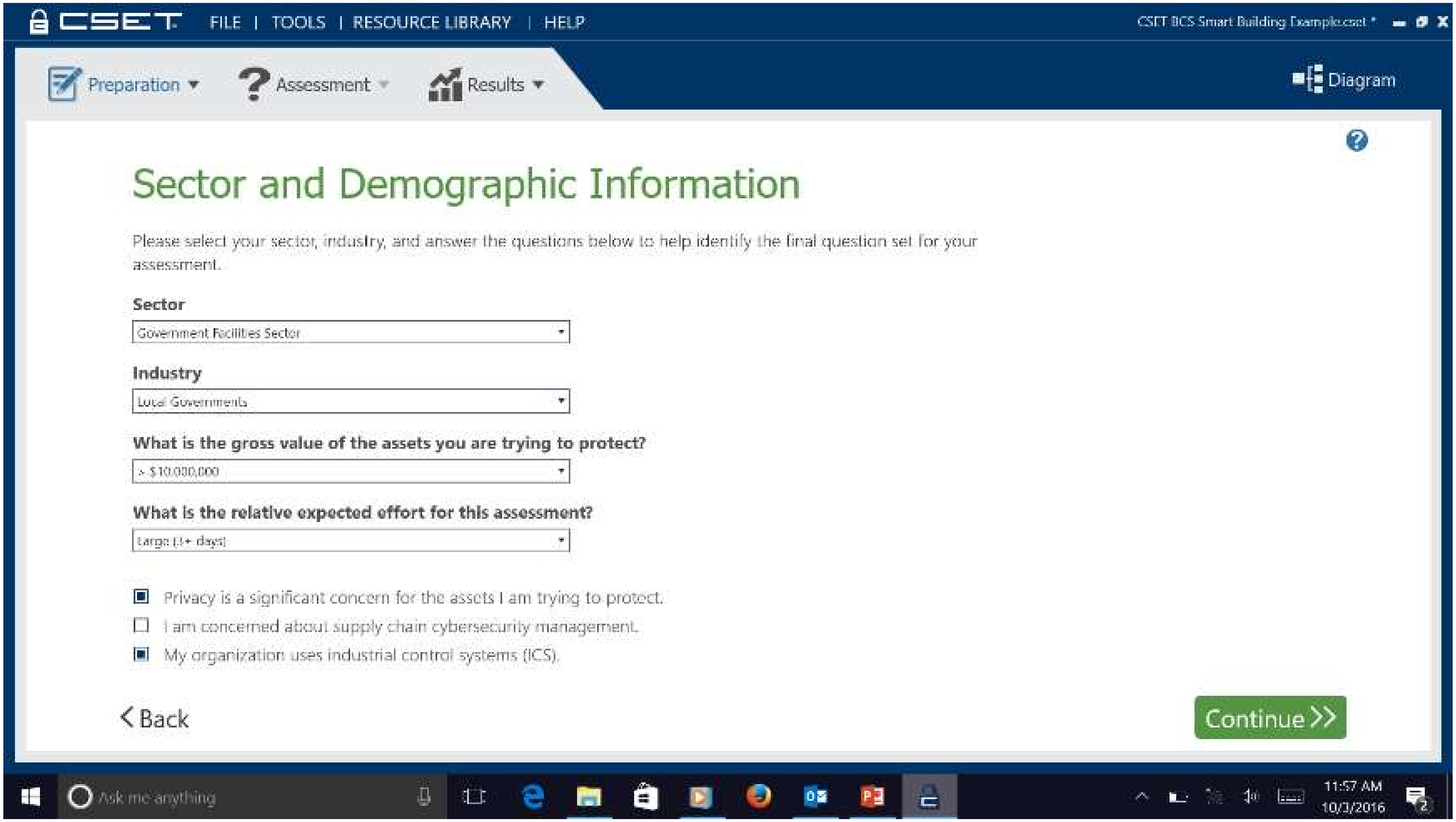
City or Site Name: Centreville

State, Province, or Region: VA

Optional DOD eMASS Specific Information

Assessor Name	Assessor Email	Assessor Telephone
Michael Chipley	mchipley@pmcgroup.biz	571-232-3890

Sector and Demographic Information



CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
CSET BCS Smart Building Example.cset *
Preparation
Assessment
Results
Diagram

Sector and Demographic Information

Please select your sector, industry, and answer the questions below to help identify the final question set for your assessment.

Sector

Government Facilities Sector

Industry

Local Governments

What is the gross value of the assets you are trying to protect?

> $10,000,000

What is the relative expected effort for this assessment?

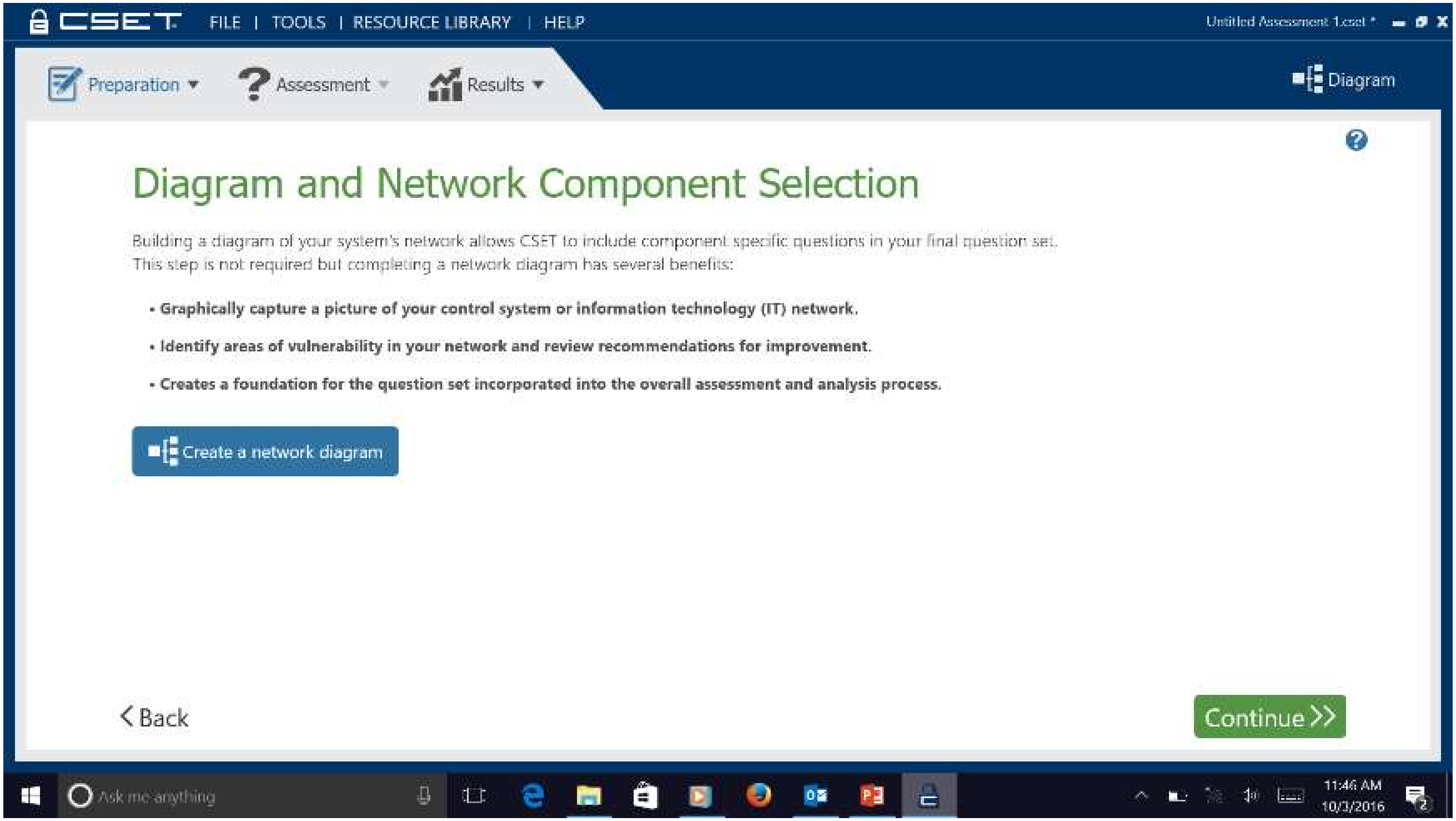
Large (3+ days)

☒ Privacy is a significant concern for the assets I am trying to protect.

☐ I am concerned about supply chain cybersecurity management.

☒ My organization uses industrial control systems (ICS).

Design and Network Component Selection



CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset *
Preparation
Assessment
Results
Diagram

Diagram and Network Component Selection

Building a diagram of your system's network allows CSET to include component specific questions in your final question set. This step is not required but completing a network diagram has several benefits:

- Graphically capture a picture of your control system or information technology (IT) network.
- Identify areas of vulnerability in your network and review recommendations for improvement.
- Creates a foundation for the question set incorporated into the overall assessment and analysis process.

Network Diagrams

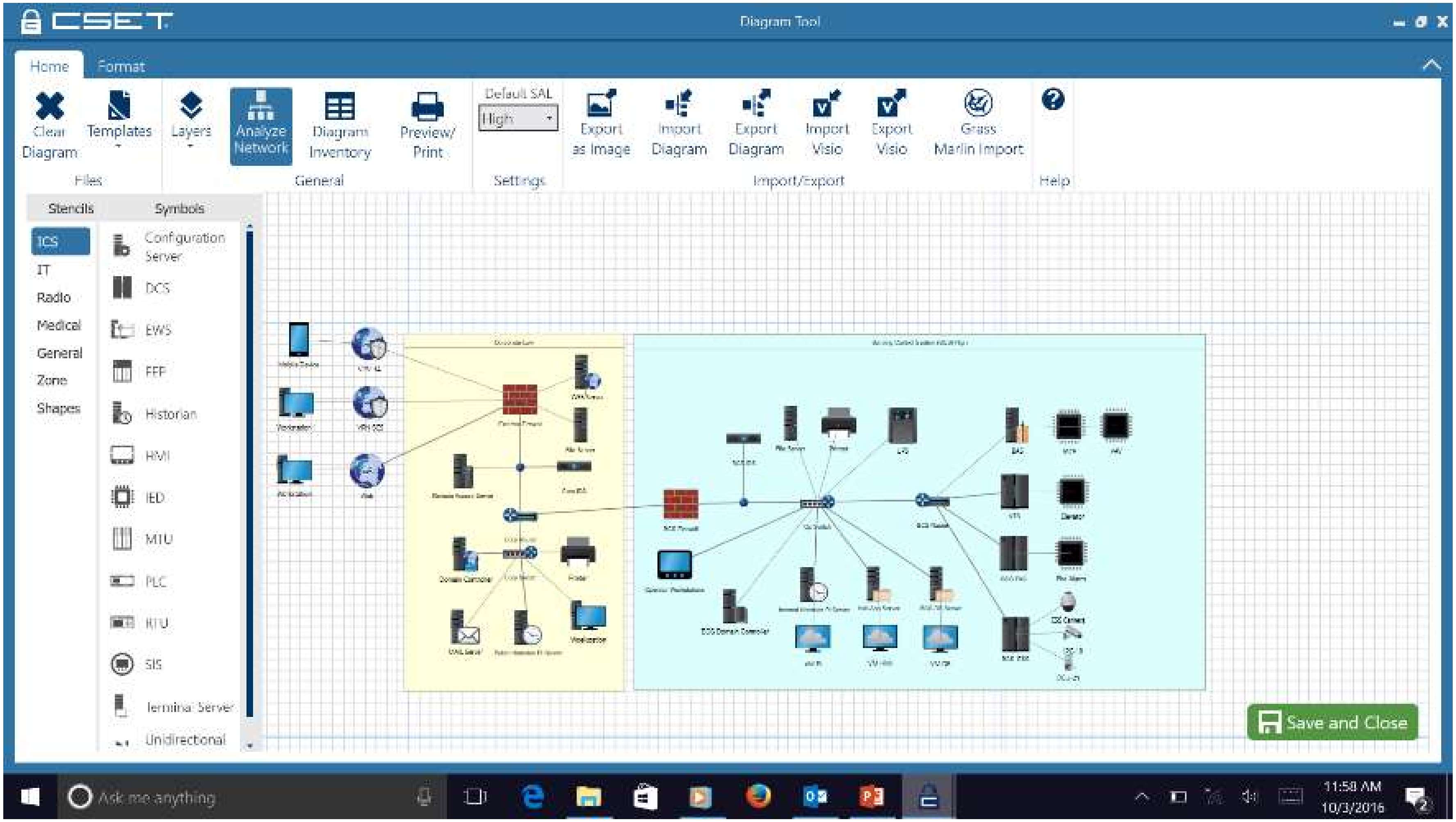


Diagram – Tools, Templates, Inventory

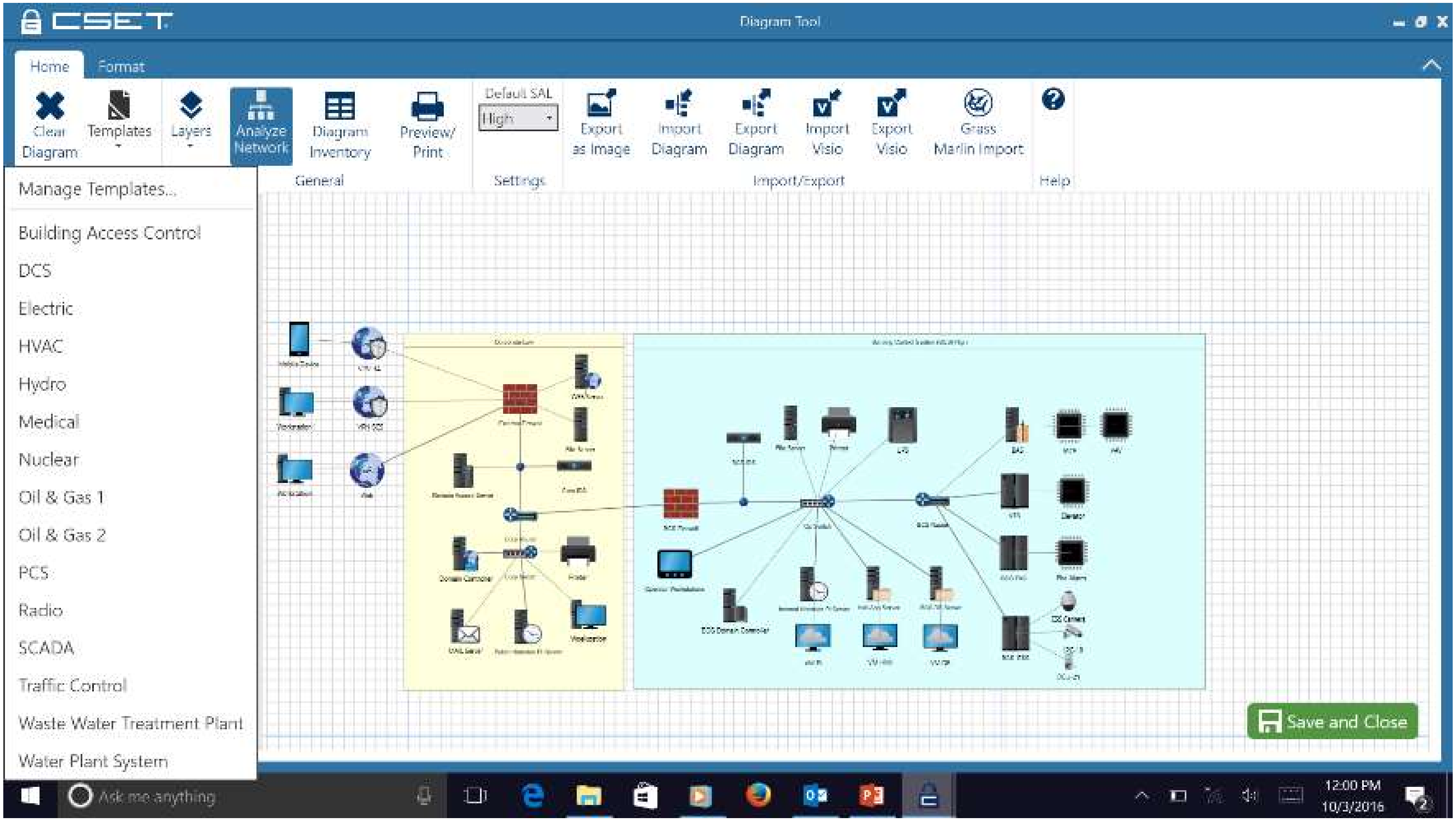


Diagram – Zones, Layers

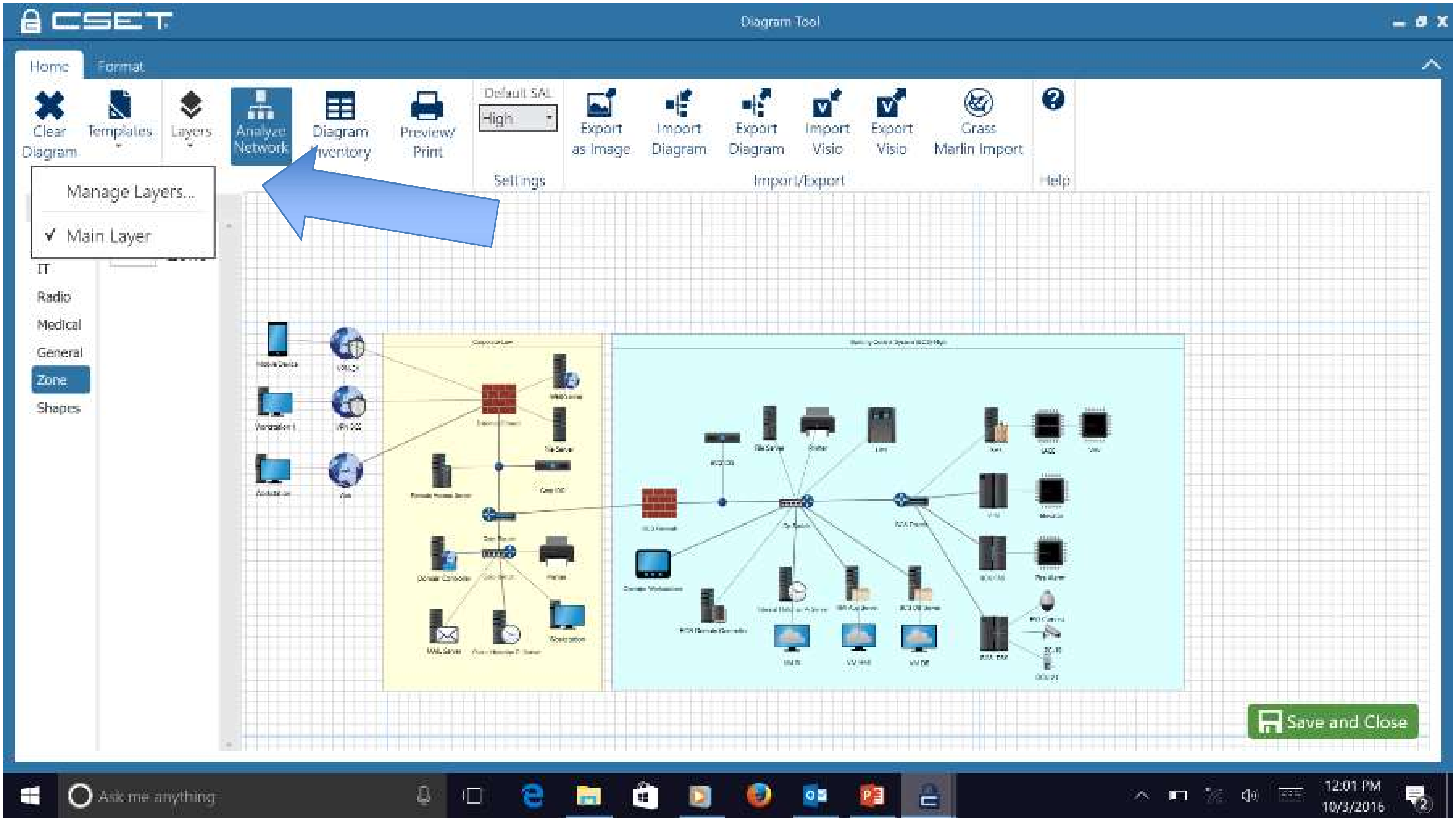
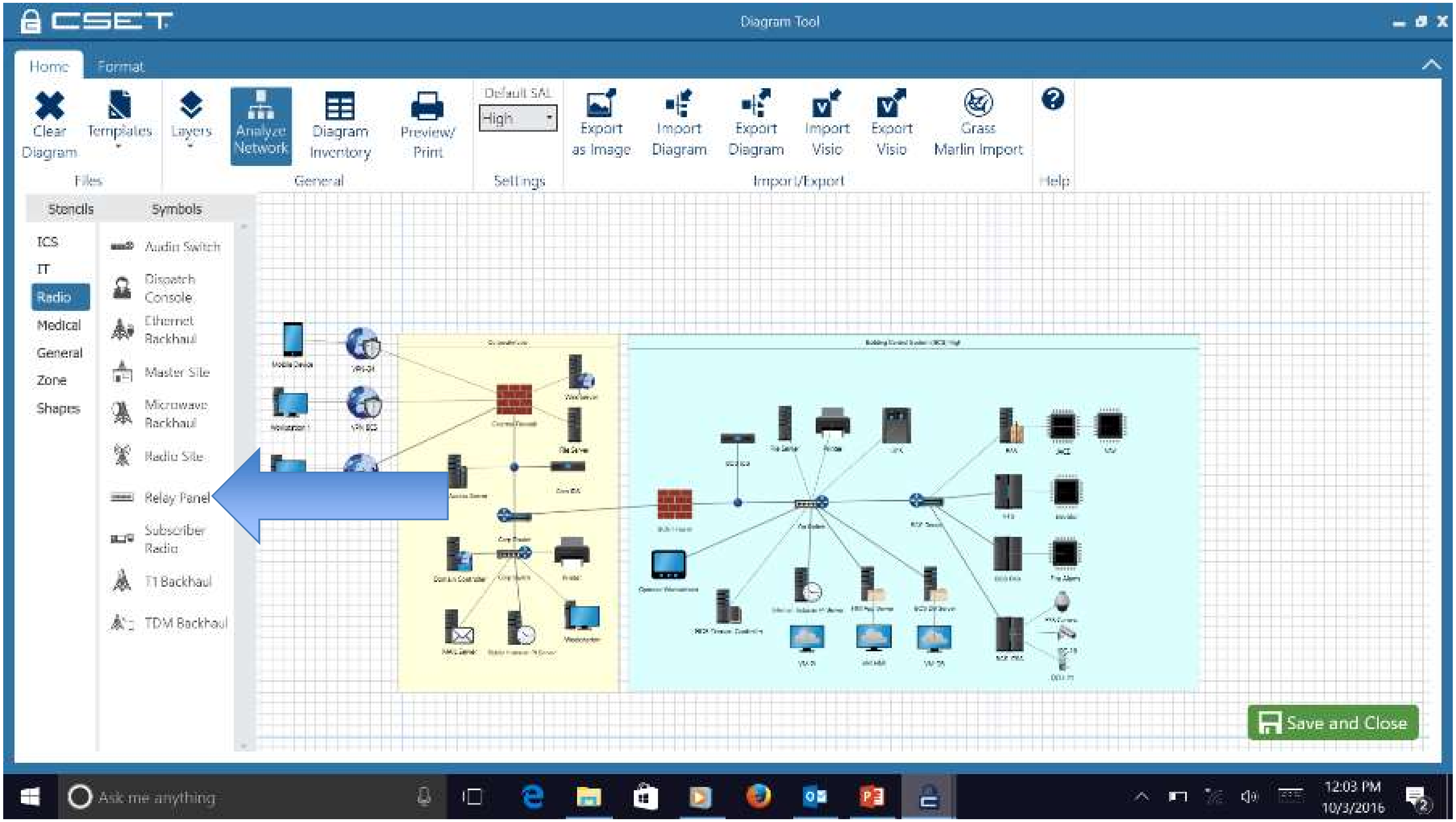
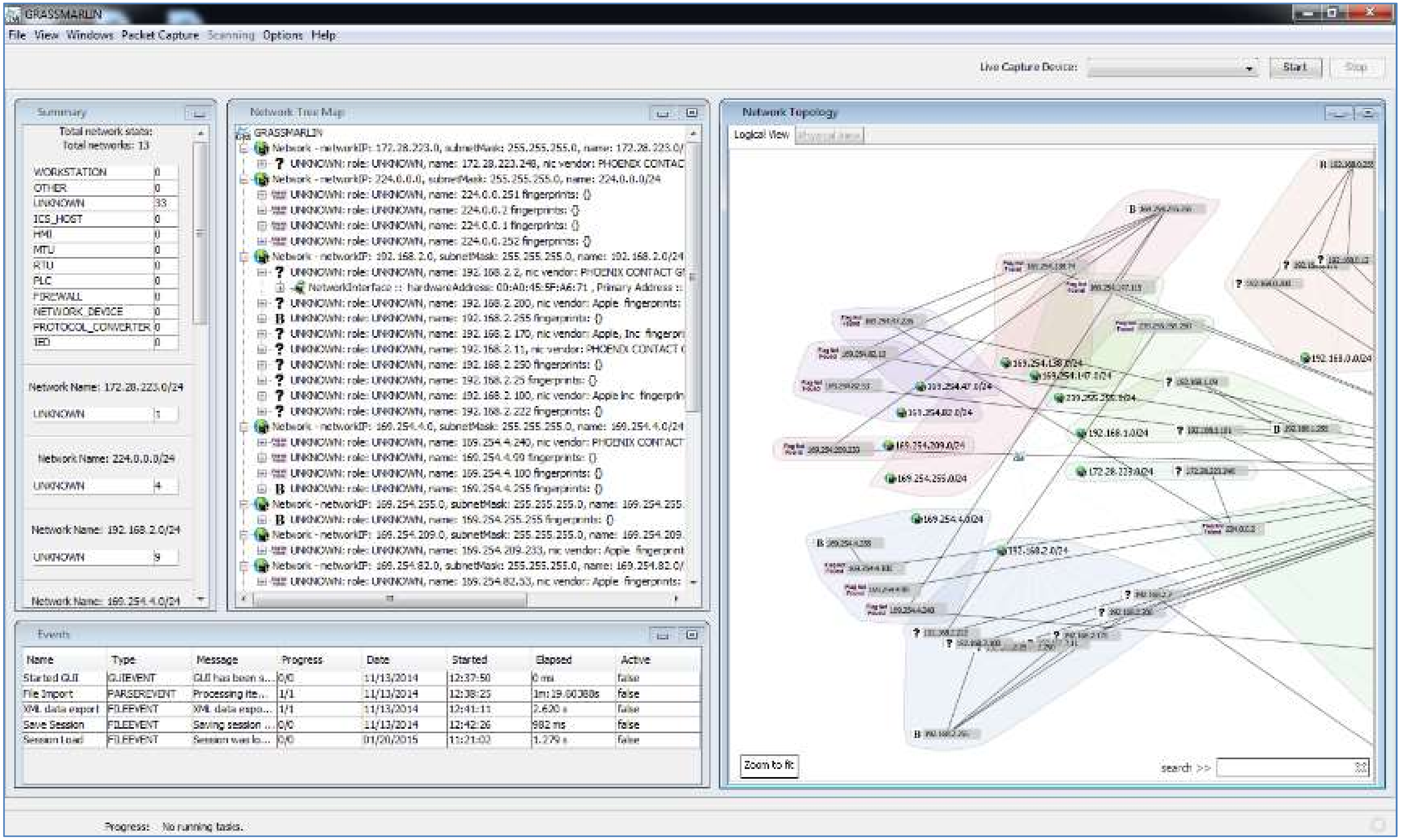


Diagram – Components



GrassMarlin Plug-In



Total network stats:
Total networks: 13

WORKSTATION	0
OTHER	0
UNKNOWN	33
ICS_HOST	0
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	0

Network Name: 172.28.223.0/24

UNKNOWN	1

Network Name: 224.0.0.0/24

UNKNOWN	4

Network Name: 192.168.2.0/24

UNKNOWN	9

Network Name: 169.254.4.0/24

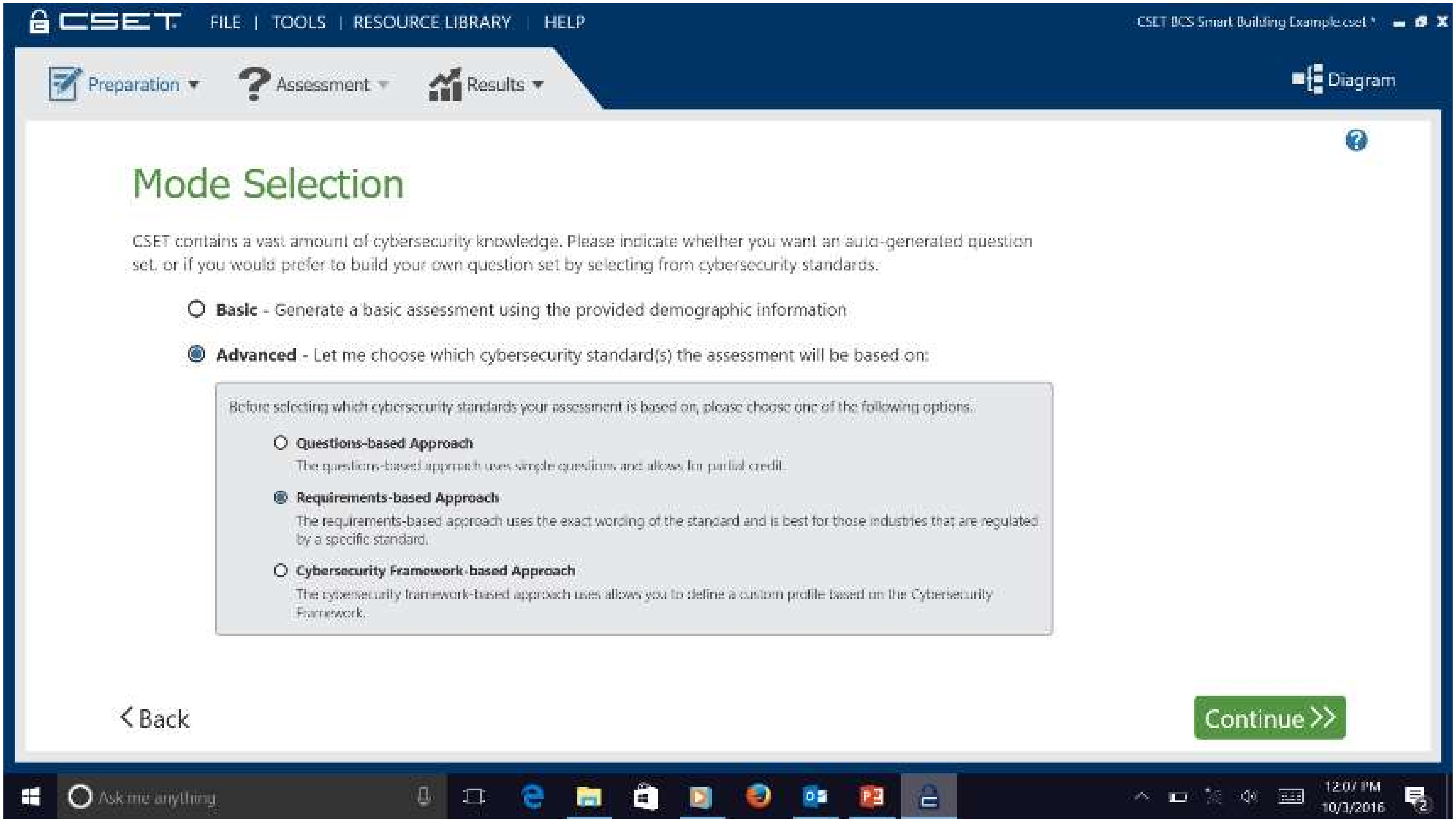
```
GRASSMARLIN
  Network - networkIP: 172.28.223.0, subnetMask: 255.255.255.0, name: 172.28.223.0/
    ? UNKNOWN: role: UNKNOWN, name: 172.28.223.248, nic vendor: PHOENIX CONTAC
  Network - networkIP: 224.0.0.0, subnetMask: 255.255.255.0, name: 224.0.0.0/24
    UNKNOWN: role: UNKNOWN, name: 224.0.0.251 fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 224.0.0.2 fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 224.0.0.1 fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 224.0.0.252 fingerprints: {}
  Network - networkIP: 192.168.2.0, subnetMask: 255.255.255.0, name: 192.168.2.0/24
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.2, nic vendor: PHOENIX CONTACT GI
        NetworkInterface :: hardwareAddress: 00:A0:45:5F:A6:71 , Primary Address ::
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.200, nic vendor: Apple fingerprints:
    B UNKNOWN: role: UNKNOWN, name: 192.168.2.255 fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.170, nic vendor: Apple, Inc fingerpri
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.11, nic vendor: PHOENIX CONTACT (
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.250 fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.25 fingerprints: {}
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.100, nic vendor: Apple Inc fingerprin
    ? UNKNOWN: role: UNKNOWN, name: 192.168.2.222 fingerprints: {}
  Network - networkIP: 169.254.4.0, subnetMask: 255.255.255.0, name: 169.254.4.0/24
    UNKNOWN: role: UNKNOWN, name: 169.254.4.240, nic vendor: PHOENIX CONTACT
    UNKNOWN: role: UNKNOWN, name: 169.254.4.99 fingerprints: {}
    UNKNOWN: role: UNKNOWN, name: 169.254.4.100 fingerprints: {}
    B UNKNOWN: role: UNKNOWN, name: 169.254.4.255 fingerprints: {}
  Network - networkIP: 169.254.255.0, subnetMask: 255.255.255.0, name: 169.254.255.
    B UNKNOWN: role: UNKNOWN, name: 169.254.255.255 fingerprints: {}
  Network - networkIP: 169.254.209.0, subnetMask: 255.255.255.0, name: 169.254.209.
    UNKNOWN: role: UNKNOWN, name: 169.254.209.233, nic vendor: Apple fingerprint
  Network - networkIP: 169.254.82.0, subnetMask: 255.255.255.0, name: 169.254.82.0/
    UNKNOWN: role: UNKNOWN, name: 169.254.82.53, nic vendor: Apple fingerprints:
```

Name	Type	Message	Progress	Date	Started	Elapsed	Active
Started GUI	GUIEVENT	GUI has been s...	0/0	11/13/2014	12:37:50	0 ms	false
File Import	PARSEREVENT	Processing ite...	1/1	11/13/2014	12:38:25	1m: 19.60388s	false
XML data export	FILEEVENT	XML data expo...	1/1	11/13/2014	12:41:11	2.620 s	false
Save Session	FILEEVENT	Saving session ...	0/0	11/13/2014	12:42:26	982 ms	false
Session Load	FILEEVENT	Session was lo...	0/0	01/20/2015	11:21:02	1.279 s	false

Progress: No running tasks.

Working with other products to get Visio import templates

Mode Selection


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
CSET BCS Smart Building Example.cset *
Preparation
Assessment
Results
Diagram
Ask me anything
12:07 PM
10/3/2016

Mode Selection

CSET contains a vast amount of cybersecurity knowledge. Please indicate whether you want an auto-generated question set, or if you would prefer to build your own question set by selecting from cybersecurity standards.

○ **Basic** - Generate a basic assessment using the provided demographic information

● **Advanced** - Let me choose which cybersecurity standard(s) the assessment will be based on:

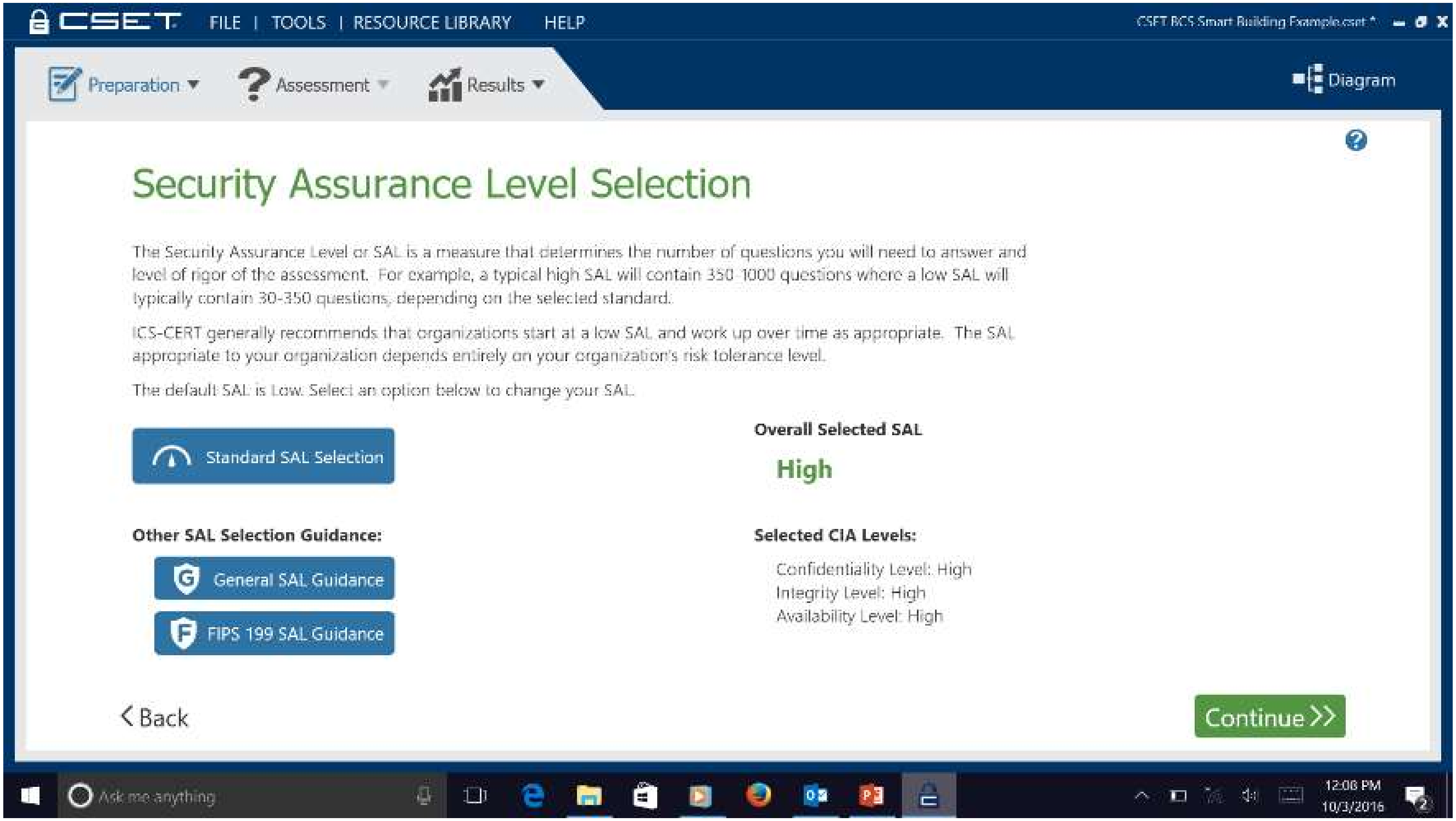
Before selecting which cybersecurity standards your assessment is based on, please choose one of the following options.

○ **Questions-based Approach**
The questions-based approach uses simple questions and allows for partial credit.

● **Requirements-based Approach**
The requirements-based approach uses the exact wording of the standard and is best for those industries that are regulated by a specific standard.

○ **Cybersecurity Framework-based Approach**
The cybersecurity framework-based approach uses allows you to define a custom profile based on the Cybersecurity Framework.

Security Assurance Level Selection


CSET
FILE | TOOLS | RESOURCE LIBRARY HELP
CSET BCS Smart Building Example.cset *
Preparation
Assessment
Results
Diagram
Ask me anything
12:08 PM
10/3/2016

Security Assurance Level Selection

The Security Assurance Level or SAL is a measure that determines the number of questions you will need to answer and level of rigor of the assessment. For example, a typical high SAL will contain 350-1000 questions where a low SAL will typically contain 30-350 questions, depending on the selected standard.

ICS-CERT generally recommends that organizations start at a low SAL and work up over time as appropriate. The SAL appropriate to your organization depends entirely on your organization's risk tolerance level.

The default SAL is Low. Select an option below to change your SAL.

Overall Selected SAL

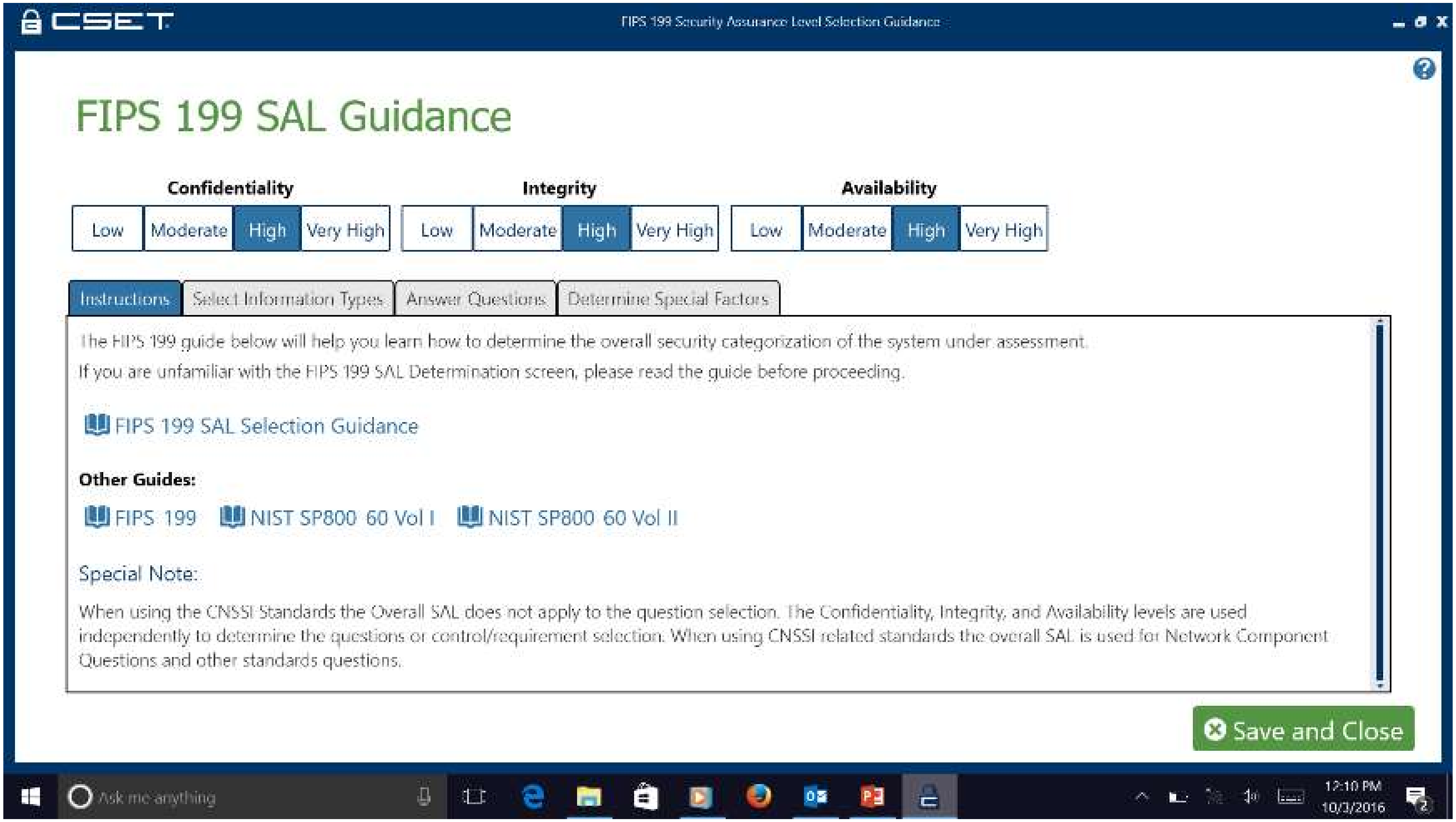
High

Other SAL Selection Guidance:

Selected CIA Levels:

Confidentiality Level: High
Integrity Level: High
Availability Level: High

FIPS 199 SAL Guidance



FIPS 199 SAL Guidance

Confidentiality	Integrity	Availability
Low ○ Moderate ○ [✓ High] ○ Very High	Low ○ Moderate ○ [✓ High] ○ Very High	Low ○ Moderate ○ [✓ High] ○ Very High

The FIPS 199 guide below will help you learn how to determine the overall security categorization of the system under assessment.

If you are unfamiliar with the FIPS 199 SAL Determination screen, please read the guide before proceeding.

FIPS 199 SAL Selection Guidance

Other Guides:

FIPS 199 NIST SP800 60 Vol I NIST SP800 60 Vol II

Special Note:

When using the CNSSI Standards the Overall SAL does not apply to the question selection. The Confidentiality, Integrity, and Availability levels are used independently to determine the questions or control/requirement selection. When using CNSSI related standards the overall SAL is used for Network Component Questions and other standards questions.

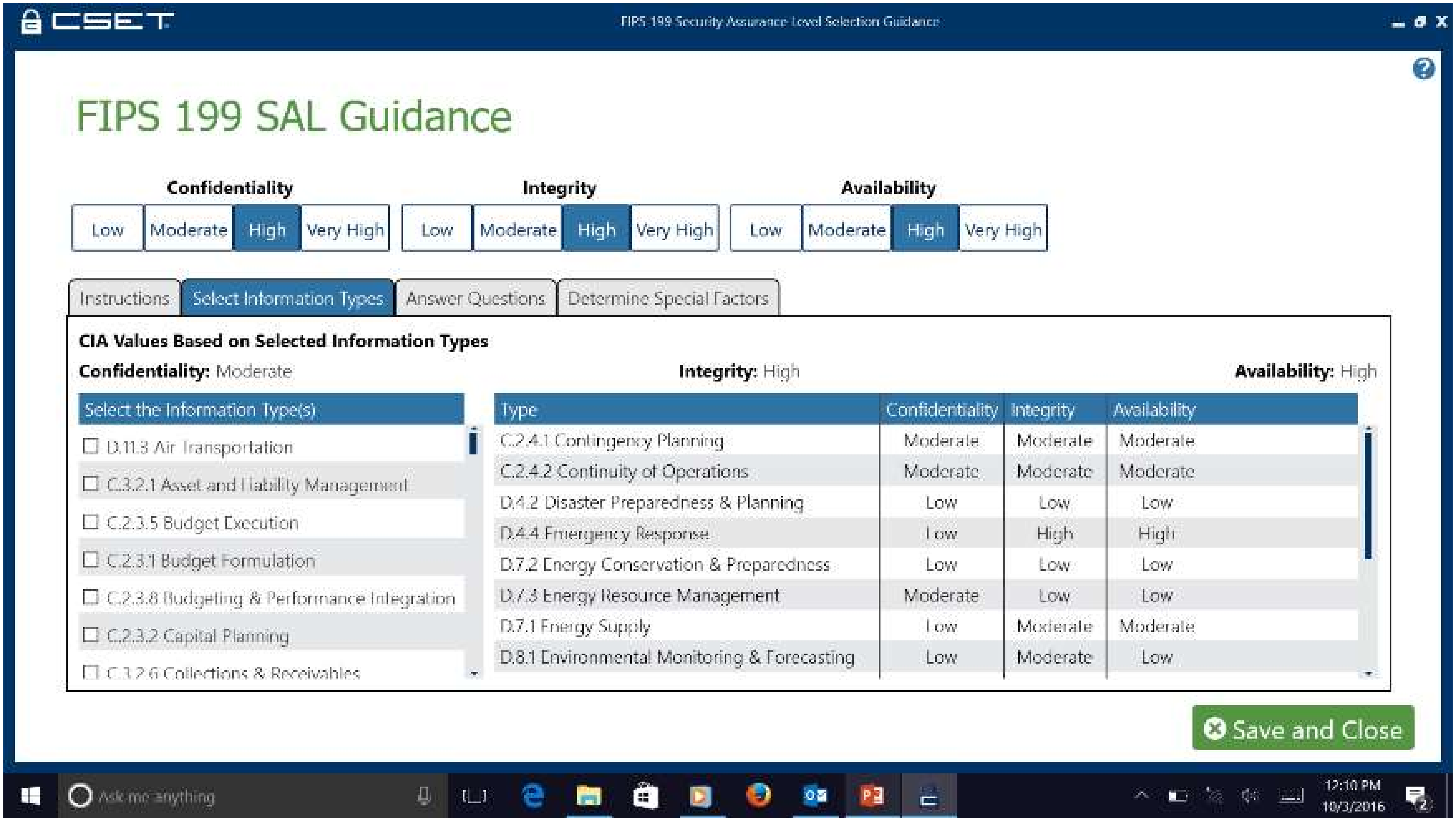
FIPS 199 SAL Impact Levels

The *potential impact* is **LOW** if—
− The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—
− The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The *potential impact* is **HIGH** if—
− The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

FIPS SAL Information Types



CSET
FIPS 199 Security Assurance Level Selection Guidance

FIPS 199 SAL Guidance

Confidentiality				Integrity				Availability			
Low	Moderate	[✓ High]	Very High	Low	Moderate	[✓ High]	Very High	Low	Moderate	[✓ High]	Very High

Instructions
Select Information Types
Answer Questions
Determine Special Factors

CIA Values Based on Selected Information Types

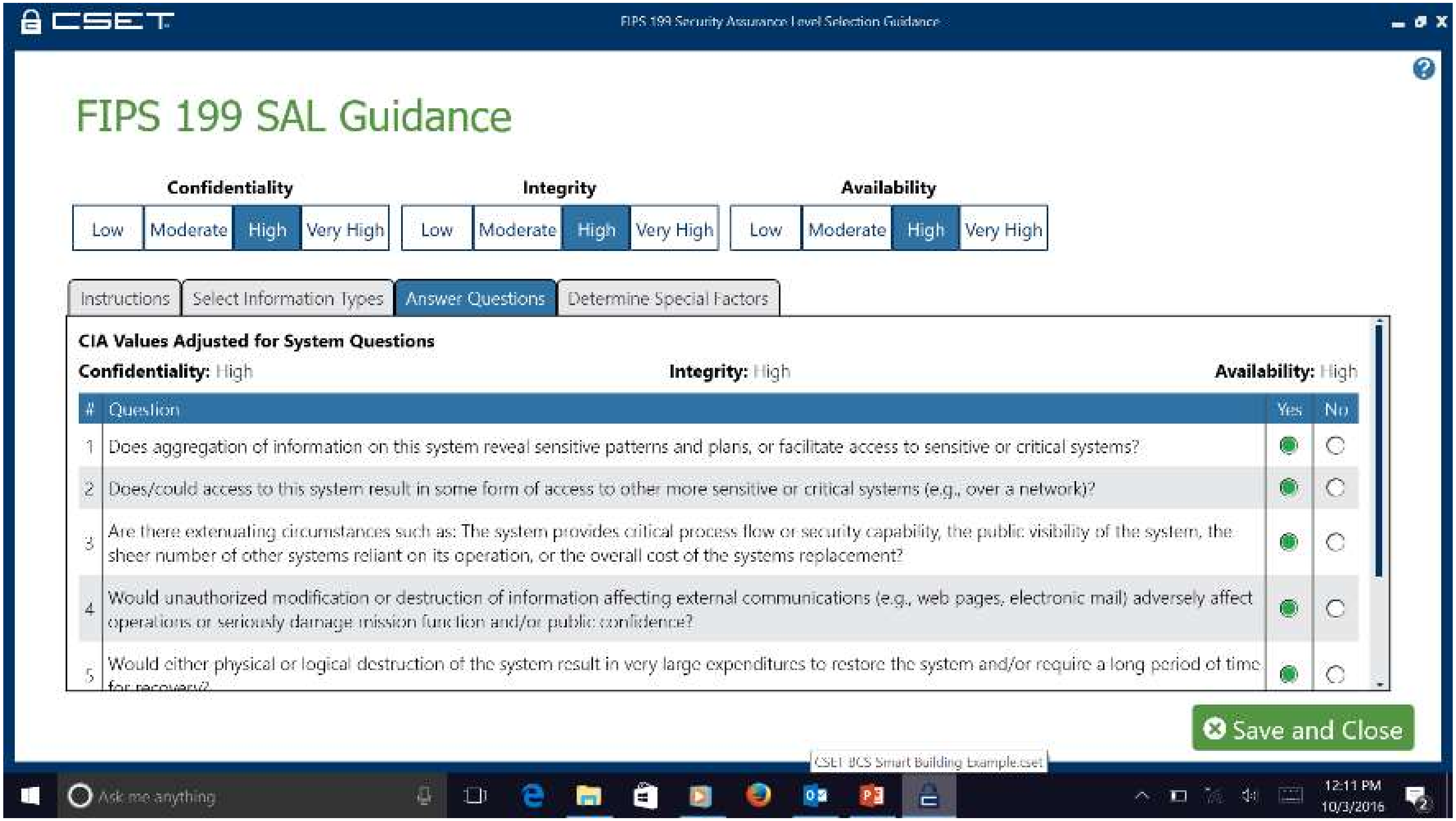
Confidentiality: Moderate **Integrity:** High **Availability:** High

Select the Information Type(s)

- ☐ D.11.3 Air Transportation
- ☐ C.3.2.1 Asset and Liability Management
- ☐ C.2.3.5 Budget Execution
- ☐ C.2.3.1 Budget Formulation
- ☐ C.2.3.8 Budgeting & Performance Integration
- ☐ C.2.3.2 Capital Planning
- ☐ C.3.2.6 Collections & Receivables

Type	Confidentiality	Integrity	Availability
C.2.4.1 Contingency Planning	Moderate	Moderate	Moderate
C.2.4.2 Continuity of Operations	Moderate	Moderate	Moderate
D.4.2 Disaster Preparedness & Planning	Low	Low	Low
D.4.4 Emergency Response	Low	High	High
D.7.2 Energy Conservation & Preparedness	Low	Low	Low
D.7.3 Energy Resource Management	Moderate	Low	Low
D.7.1 Energy Supply	Low	Moderate	Moderate
D.8.1 Environmental Monitoring & Forecasting	Low	Moderate	Low

FIPS 199 SAL Answer Questions


CSET
FIPS 199 Security Assurance Level Selection Guidance
Save and Close
CSET BCS Smart Building Example.cset
Ask me anything
12:11 PM
10/3/2016

FIPS 199 SAL Guidance

Confidentiality: Low | Moderate | [✓ High] | Very High

Integrity: Low | Moderate | [✓ High] | Very High

Availability: Low | Moderate | [✓ High] | Very High

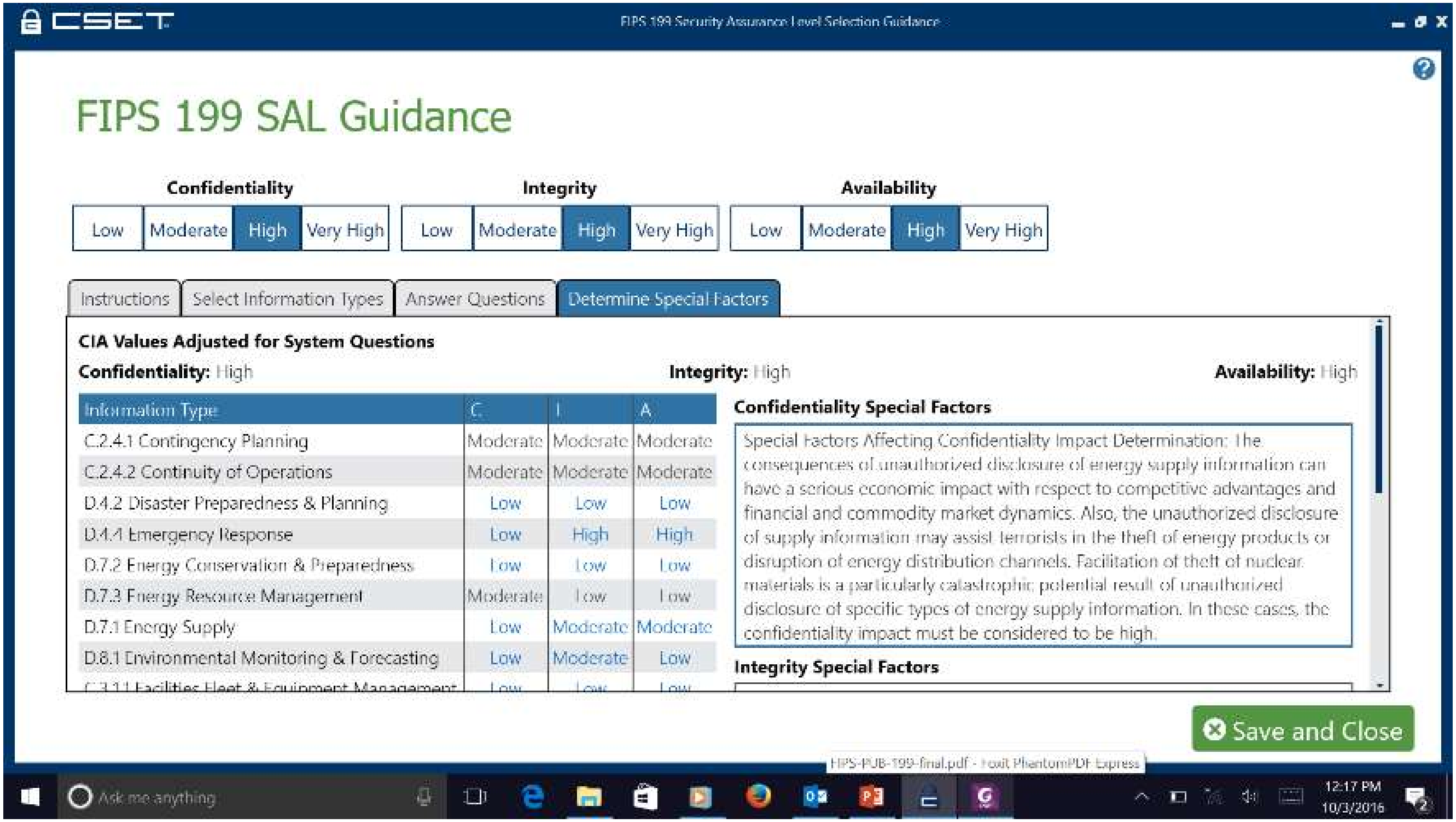
Instructions | Select Information Types | [✓ Answer Questions] | Determine Special Factors

CIA Values Adjusted for System Questions

Confidentiality: High **Integrity:** High **Availability:** High

#	Question	Yes	No
1	Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?	●	○
2	Does/could access to this system result in some form of access to other more sensitive or critical systems (e.g., over a network)?	●	○
3	Are there extenuating circumstances such as: The system provides critical process flow or security capability, the public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of the systems replacement?	●	○
4	Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?	●	○
5	Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?	●	○

FIPS 199 SAL Special Factors



FIPS 199 SAL Guidance

CIA Values Adjusted for System Questions

Confidentiality: High **Integrity:** High **Availability:** High

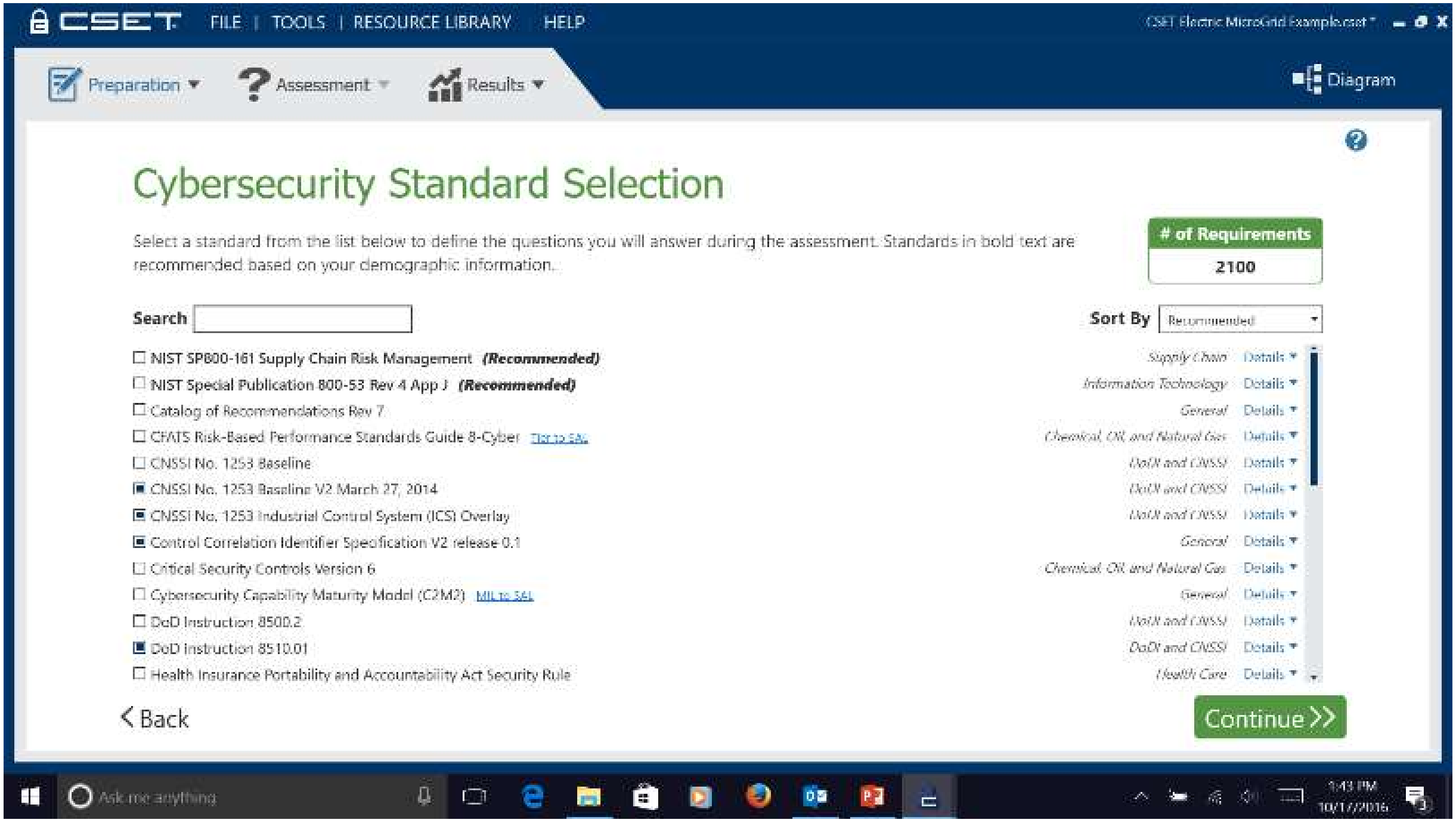
Information Type	C	I	A
C.2.4.1 Contingency Planning	Moderate	Moderate	Moderate
C.2.4.2 Continuity of Operations	Moderate	Moderate	Moderate
D.4.2 Disaster Preparedness & Planning	Low	Low	Low
D.4.4 Emergency Response	Low	High	High
D.7.2 Energy Conservation & Preparedness	Low	Low	Low
D.7.3 Energy Resource Management	Moderate	Low	Low
D.7.1 Energy Supply	Low	Moderate	Moderate
D.8.1 Environmental Monitoring & Forecasting	Low	Moderate	Low
C.3.1.1 Facilities Fleet & Equipment Management	Low	Low	Low

Confidentiality Special Factors

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of energy supply information can have a serious economic impact with respect to competitive advantages and financial and commodity market dynamics. Also, the unauthorized disclosure of supply information may assist terrorists in the theft of energy products or disruption of energy distribution channels. Facilitation of theft of nuclear materials is a particularly catastrophic potential result of unauthorized disclosure of specific types of energy supply information. In these cases, the confidentiality impact must be considered to be high.

Integrity Special Factors

Cybersecurity Standard Selection



Cybersecurity Standard Selection

Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

# of Requirements

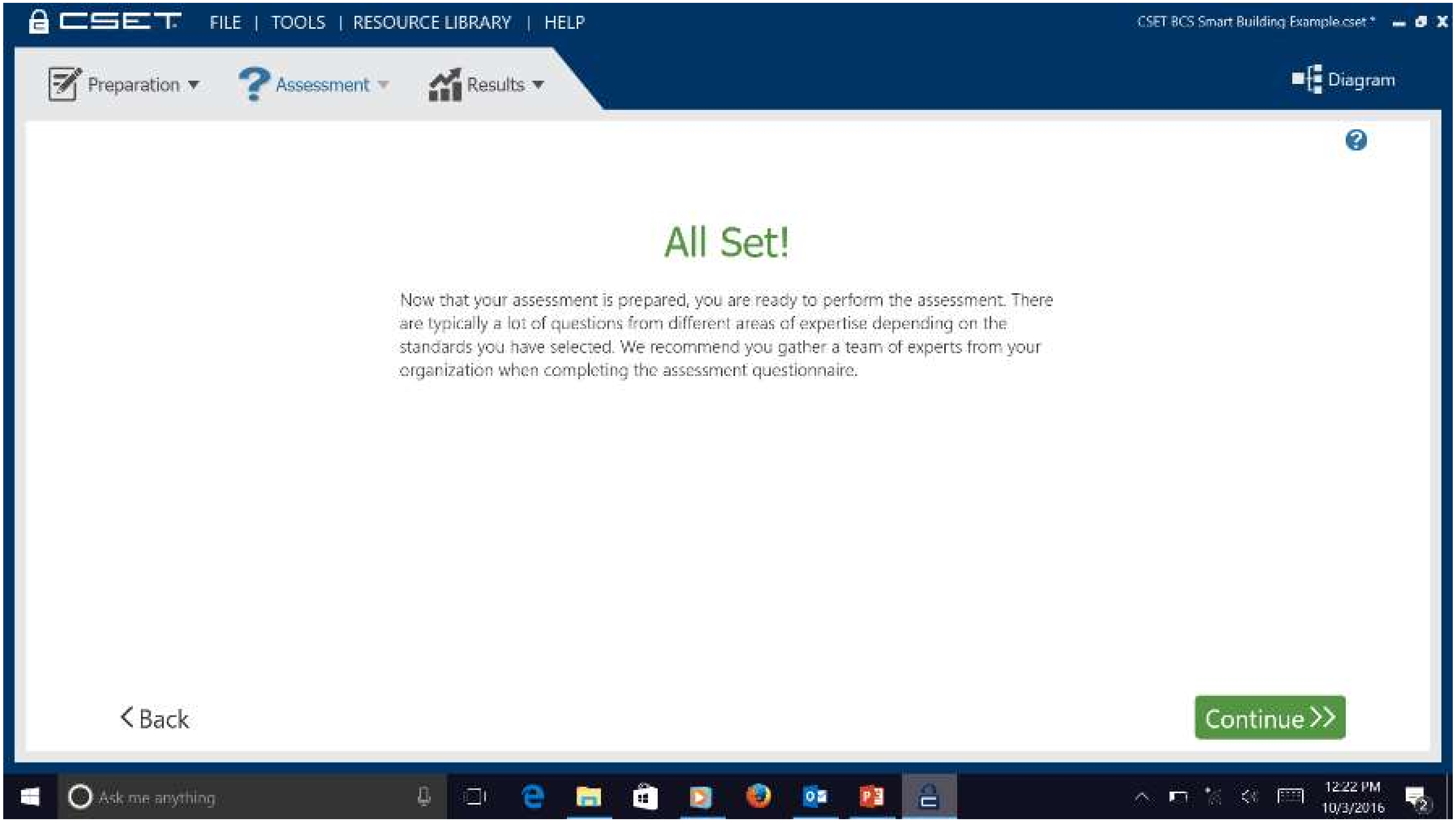
2100

Search

Sort By Recommended

☐ **NIST SP800-161 Supply Chain Risk Management** ***(Recommended)***	*Supply Chain*	Details ▾
☐ **NIST Special Publication 800-53 Rev 4 App J** ***(Recommended)***	*Information Technology*	Details ▾
☐ Catalog of Recommendations Rev 7	*General*	Details ▾
☐ CFATS Risk-Based Performance Standards Guide 8-Cyber Tier to SAL	*Chemical, Oil, and Natural Gas*	Details ▾
☐ CNSSI No. 1253 Baseline	*DoD and CNSSI*	Details ▾
■ CNSSI No. 1253 Baseline V2 March 27, 2014	*DoD and CNSSI*	Details ▾
■ CNSSI No. 1253 Industrial Control System (ICS) Overlay	*DoD and CNSSI*	Details ▾
■ Control Correlation Identifier Specification V2 release 0.1	*General*	Details ▾
☐ Critical Security Controls Version 6	*Chemical, Oil, and Natural Gas*	Details ▾
☐ Cybersecurity Capability Maturity Model (C2M2) MIL to SAL	*General*	Details ▾
☐ DoD Instruction 8500.2	*DoD and CNSSI*	Details ▾
■ DoD Instruction 8510.01	*DoD and CNSSI*	Details ▾
☐ Health Insurance Portability and Accountability Act Security Rule	*Health Care*	Details ▾

All Set!

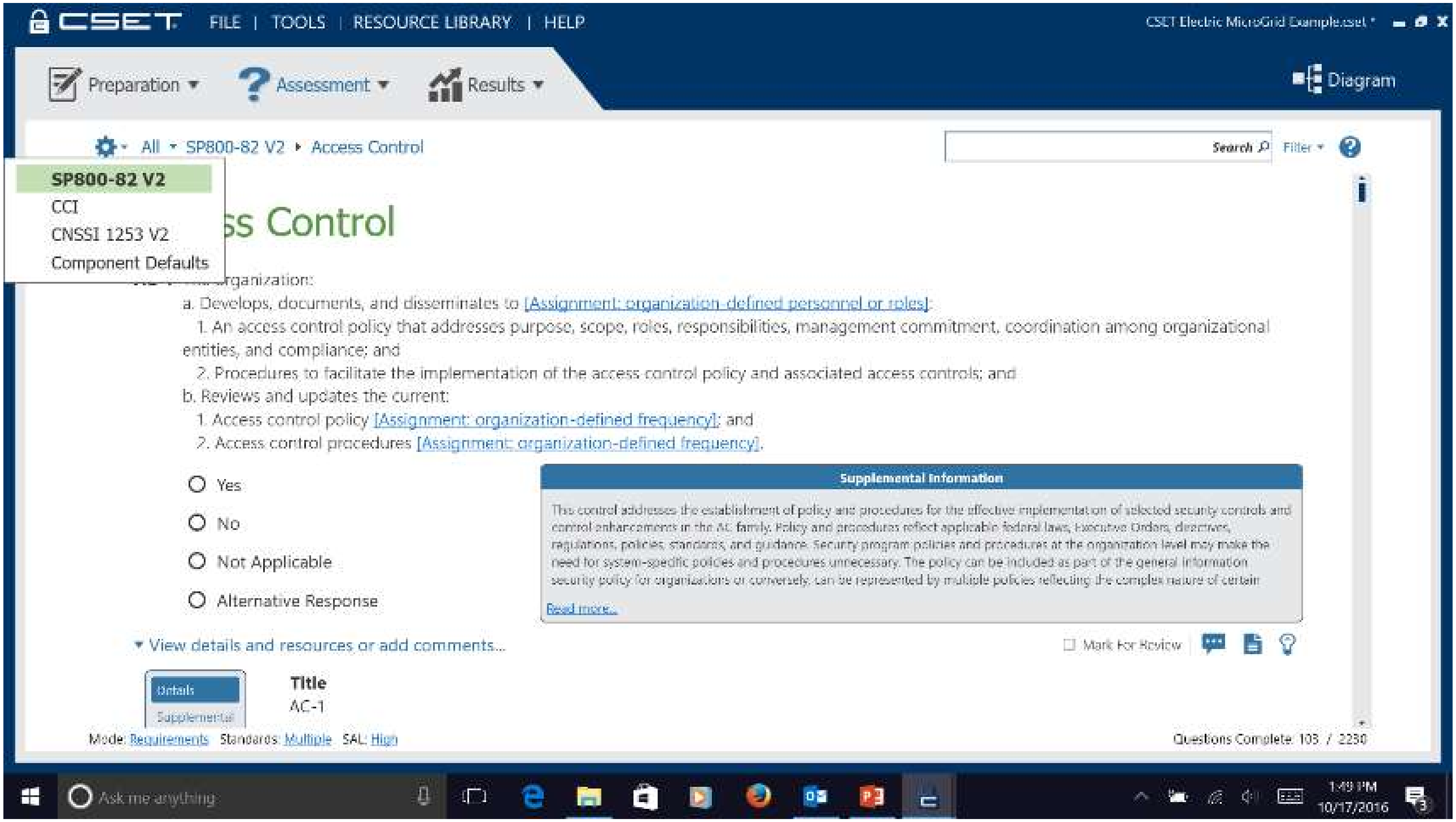


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
CSET BCS Smart Building Example.cset *
Preparation
Assessment
Results
Diagram
Ask me anything
12:22 PM
10/3/2016

All Set!

Now that your assessment is prepared, you are ready to perform the assessment. There are typically a lot of questions from different areas of expertise depending on the standards you have selected. We recommend you gather a team of experts from your organization when completing the assessment questionnaire.

Questions – Family, Detail, Info


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
CSET Electric MicroGrid Example.cset *
Preparation ▾
Assessment ▾
Results ▾
Diagram
All ▾ SP800-82 V2 ▸ Access Control
Search
Filter ▾
SP800-82 V2
CCI
CNSSI 1253 V2
Component Defaults

ss Control

rganization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [Assignment: organization-defined frequency]; and
2. Access control procedures [Assignment: organization-defined frequency].

○ Yes

○ No

○ Not Applicable

○ Alternative Response

Supplemental Information

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain

Read more...

▾ View details and resources or add comments...

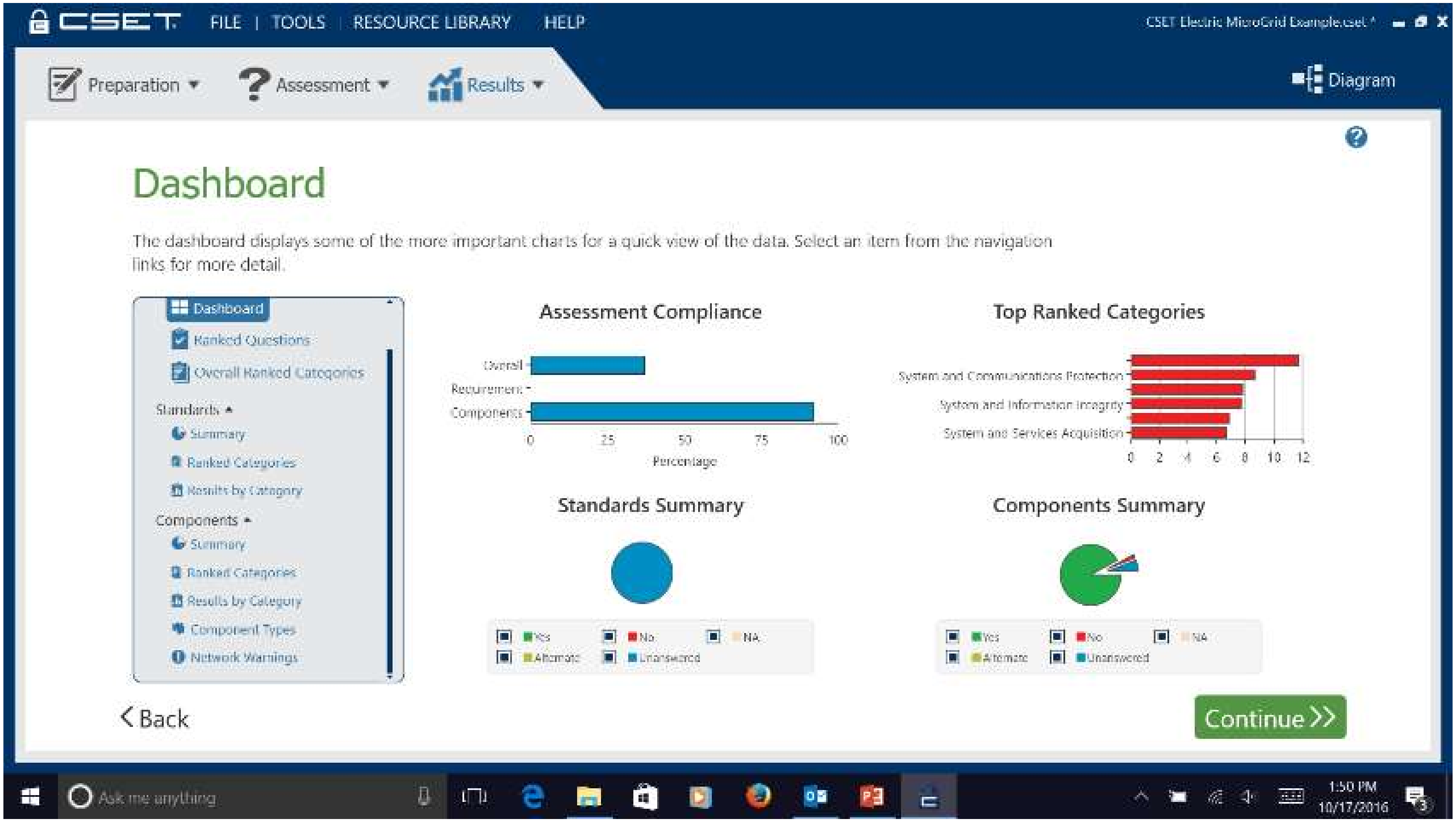
☐ Mark For Review

Title
AC-1

Mode: Requirements Standards: Multiple SAL: High

Questions Complete: 103 / 2230

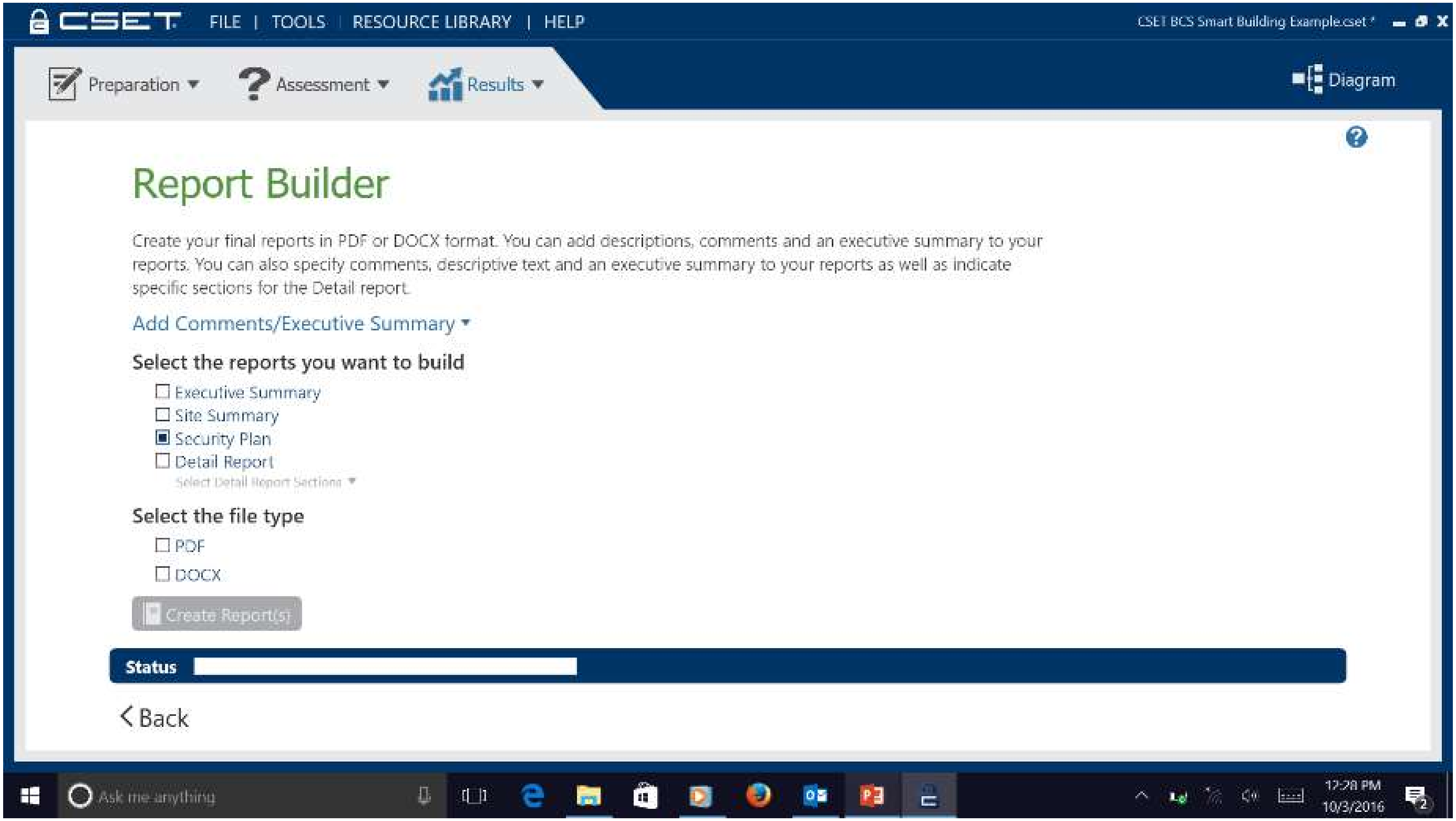
Analysis - Dashboard



Dashboard

The dashboard displays some of the more important charts for a quick view of the data. Select an item from the navigation links for more detail.

Report Builder


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
CSET BCS Smart Building Example.cset *
Preparation ▾
Assessment ▾
Results ▾
Diagram

Report Builder

Create your final reports in PDF or DOCX format. You can add descriptions, comments and an executive summary to your reports. You can also specify comments, descriptive text and an executive summary to your reports as well as indicate specific sections for the Detail report.

Add Comments/Executive Summary ▾

Select the reports you want to build

- ☐ Executive Summary
- ☐ Site Summary
- ☒ Security Plan
- ☐ Detail Report

Select Detail Report Sections ▾

Select the file type

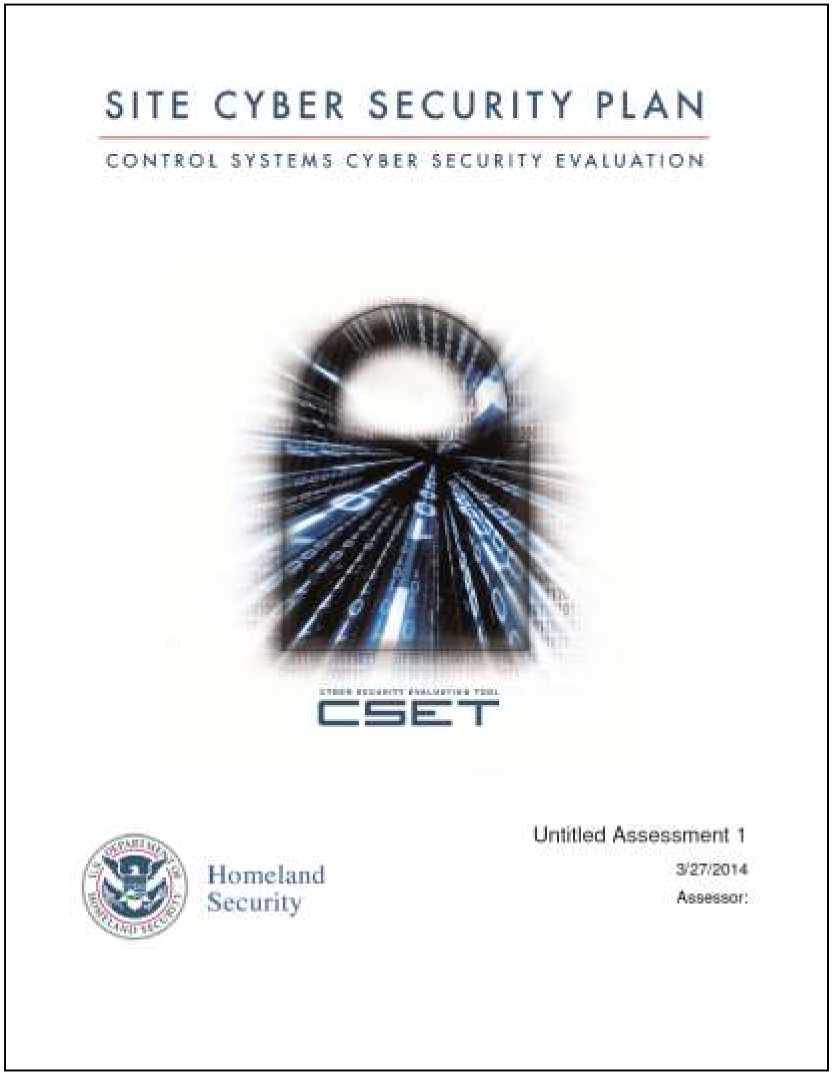
- ☐ PDF
- ☐ DOCX

Create Report(s)

Status

< Back

System Security Plan



SITE CYBER SECURITY PLAN

CONTROL SYSTEMS CYBER SECURITY EVALUATION

CYBER SECURITY EVALUATION TOOL

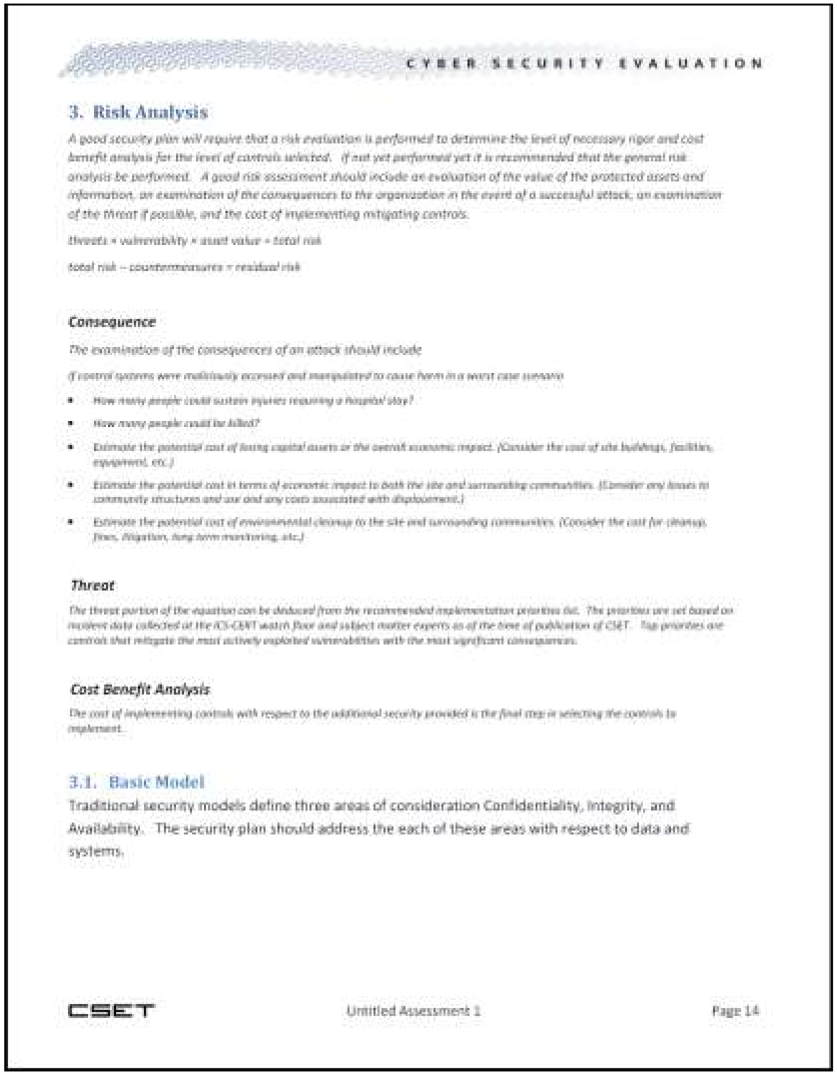
CSET

Homeland Security

Untitled Assessment 1

3/27/2014

Assessor:



CYBER SECURITY EVALUATION

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. If not yet performed yet it is recommended that the general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

threats × vulnerability × asset value = total risk

total risk – countermeasures = residual risk

Consequence

The examination of the consequences of an attack should include

If control systems were maliciously accessed and manipulated to cause harm in a worst case scenario

- *How many people could sustain injuries requiring a hospital stay?*
- *How many people could be killed?*
- *Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)*
- *Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and use and any costs associated with displacement.)*
- *Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, litigation, long term monitoring, etc.)*

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are set based on incident data collected at the ICS-CERT watch floor and subject matter experts as of the time of publication of CSET. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

Cost Benefit Analysis

The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

3.1. Basic Model

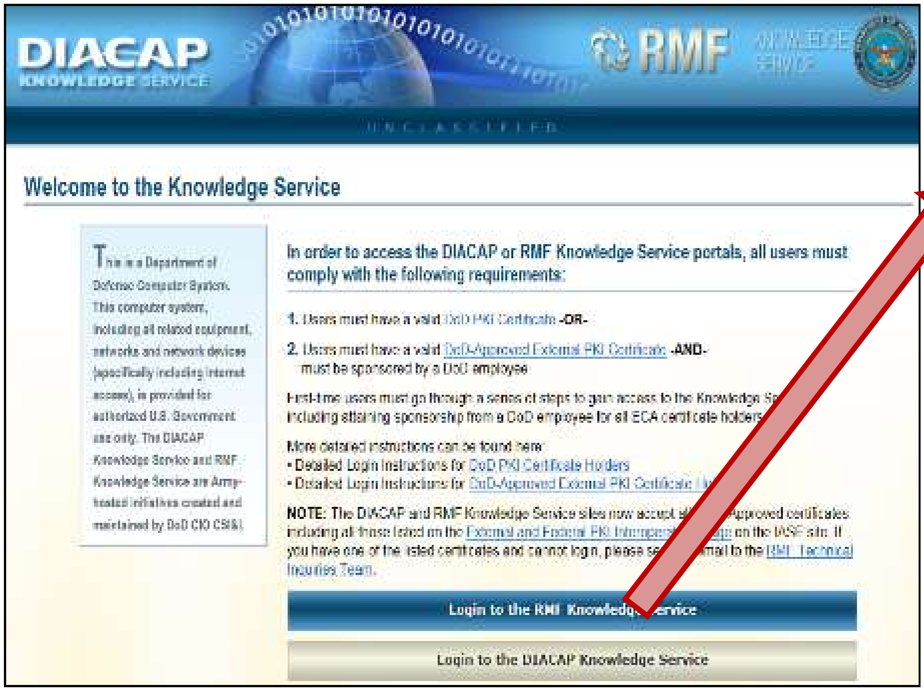
Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address the each of these areas with respect to data and systems.

CSET Untitled Assessment 1 Page 14

Unit 6

RMF KS Control Systems Webpage and eMASS demonstration, FRCS Master List and C-I-A, Using the Interim Excel files for uploading into eMASS; FRCS IA Contract Language for SME's, Test and Development Environment, FAT/SAT Checklist, Penetration Testing Checklist, Design/Construction Sequence Table

RMF KS FRCS PIT Webpage



Welcome to the Knowledge Service

This is a Department of Defense Computer System. This computer system, including all related equipment, networks and network devices (specifically including Internet access), is provided for authorized U.S. Government use only. The DIACAP Knowledge Service and RMF Knowledge Service are Army-hosted initiatives created and maintained by DoD CIO CS&I.

In order to access the DIACAP or RMF Knowledge Service portals, all users must comply with the following requirements:

1. Users must have a valid DoD PKI Certificate -OR-
2. Users must have a valid DoD-Approved External PKI Certificate -AND- must be sponsored by a DoD employee

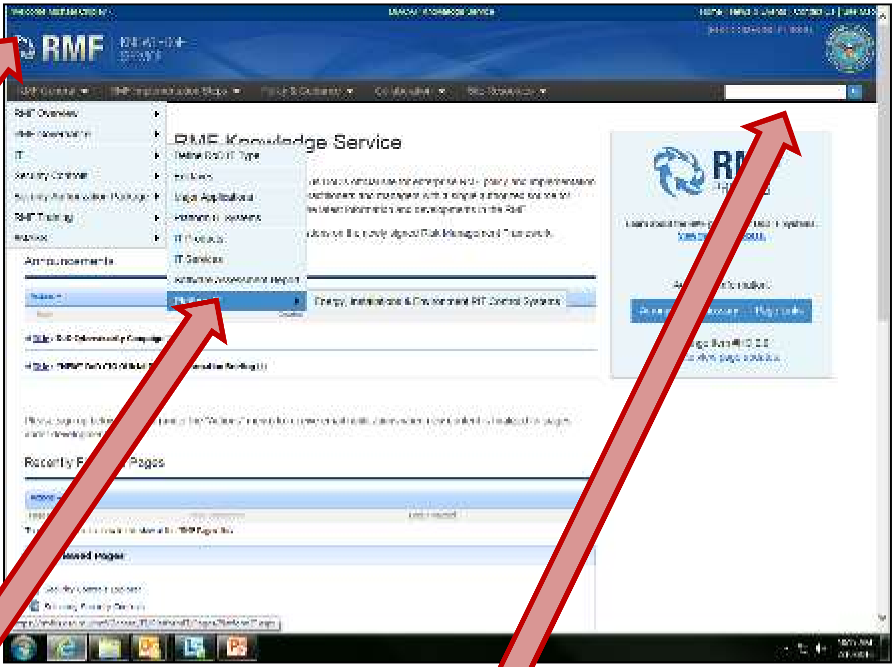
First-time users must go through a series of steps to gain access to the Knowledge Se[illegible] including attaining sponsorship from a DoD employee for all ECA certificate holders.

More detailed instructions can be found here:
- Detailed Login Instructions for DoD PKI Certificate Holders
- Detailed Login Instructions for DoD-Approved External PKI Certificate H[illegible]

NOTE: The DIACAP and RMF Knowledge Service sites now accept al[illegible] Approved certificates including all those listed on the External and Federal PKI Interopera[illegible] on the IASE site. If you have one of the listed certificates and cannot login, please se[illegible] mail to the RMF Technical Inquiries Team.

Login to the RMF Knowledge Service

Login to the DIACAP Knowledge Service



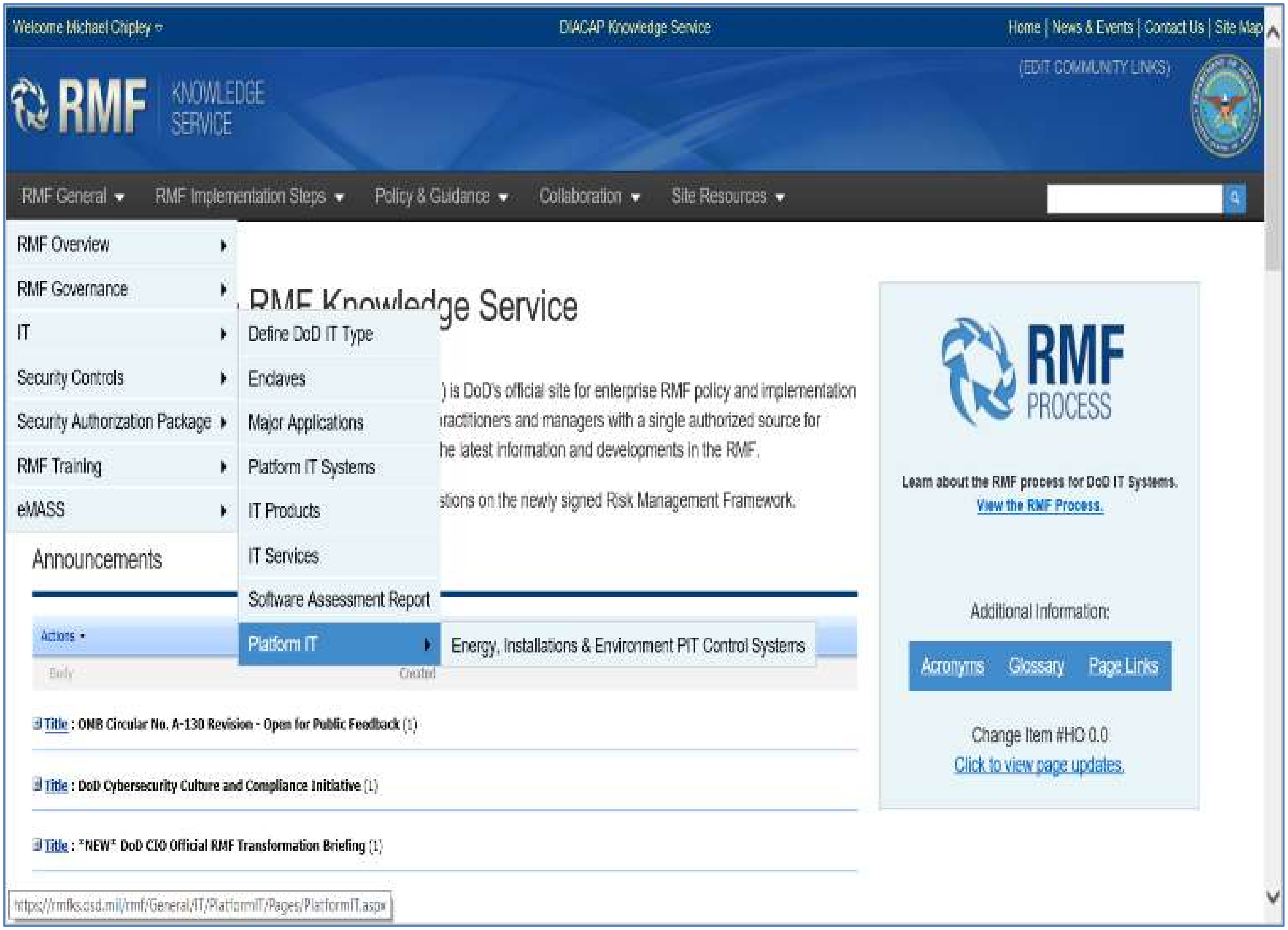
1. Navigate to DoD CIO Knowledge Service (requires CAC) https://rmfks.osd.mil/login.htm

2. Select RMF KS login bar

3. Mouse over RMF General, IT, Platform IT = EI&E PIT Control Systems

Or type in Search box “Control Systems”

RMF KS PIT Home Webpage



RMF Knowledge Service

) is DoD's official site for enterprise RMF policy and implementation
ractitioners and managers with a single authorized source for
he latest information and developments in the RMF.

stions on the newly signed Risk Management Framework.

Announcements

Title : OMB Circular No. A-130 Revision - Open for Public Feedback (1)

Title : DoD Cybersecurity Culture and Compliance Initiative (1)

Title : *NEW* DoD CIO Official RMF Transformation Briefing (1)

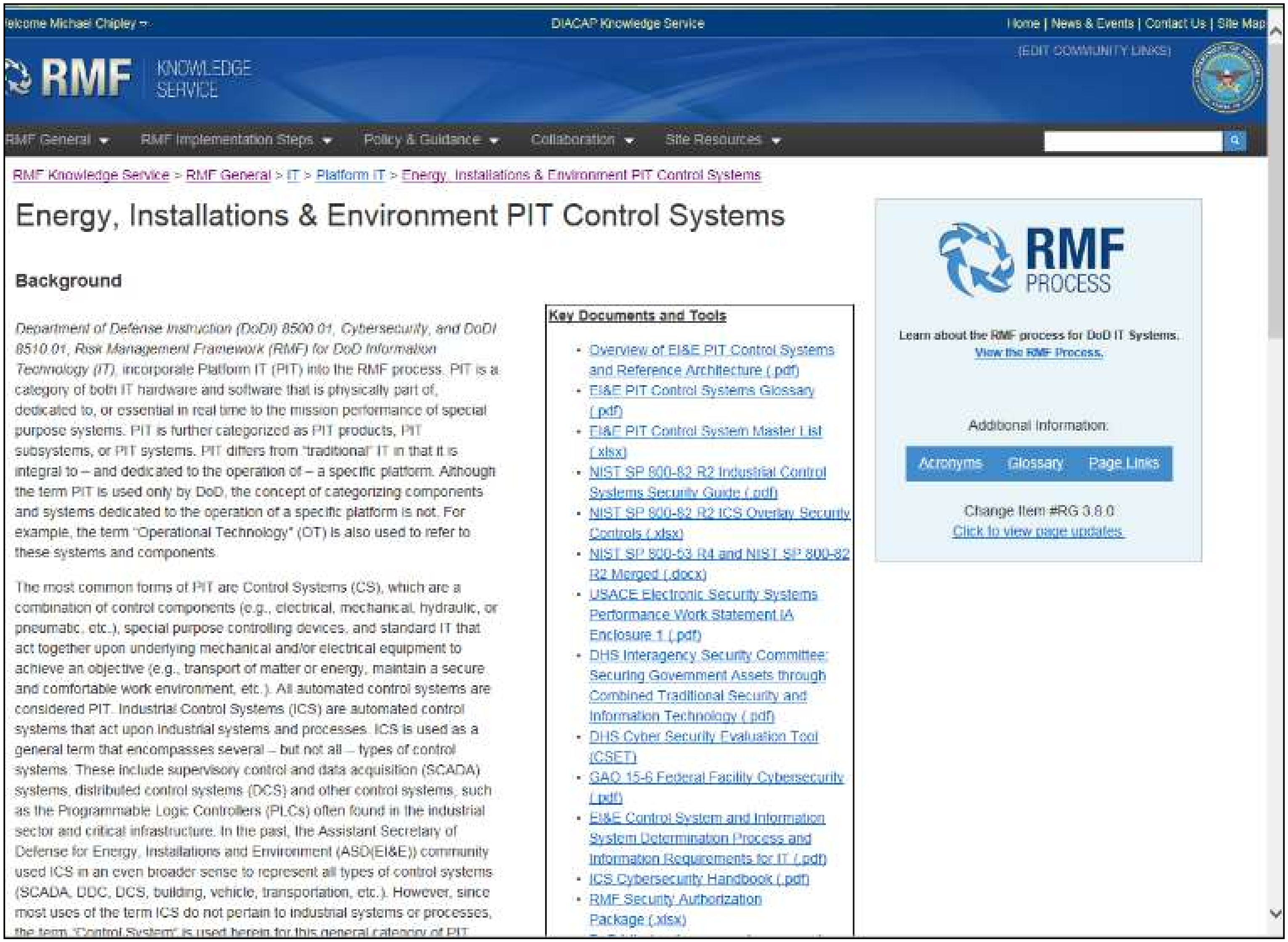
Learn about the RMF process for DoD IT Systems.
View the RMF Process.

Additional Information:

Change Item #HO 0.0
Click to view page updates.

https://rmfks.osd.mil/rmf/General/IT/PlatformIT/Pages/PlatformIT.aspx

RMF KS EI&E FRCS PIT Home Webpage



RMF Knowledge Service > RMF General > IT > Platform IT > Energy, Installations & Environment PIT Control Systems

Energy, Installations & Environment 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 uses of the term ICS do not pertain to industrial systems or processes, the term "Control System" is used herein for this general category of PIT

Key Documents and Tools

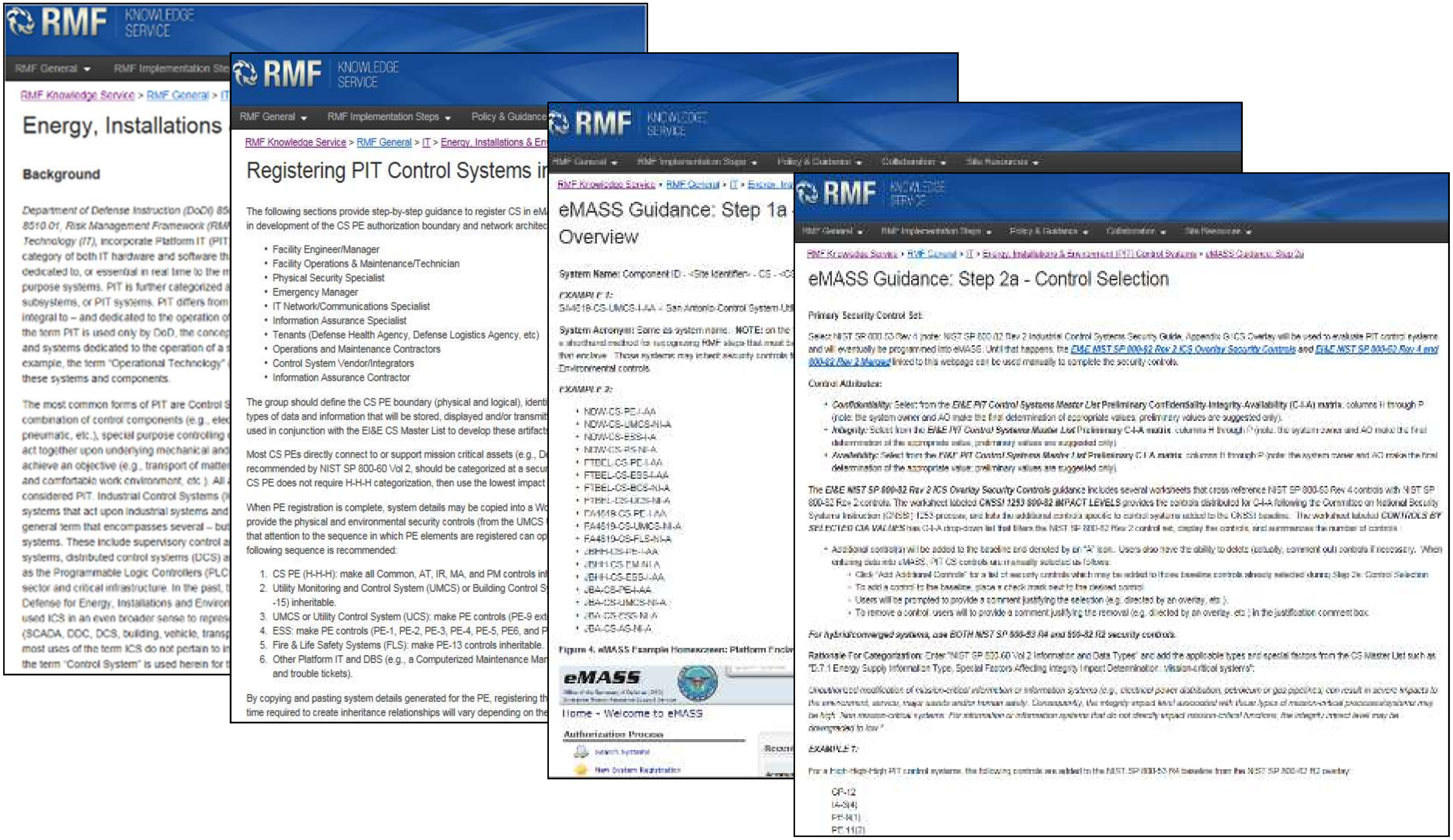
- Overview of EI&E PIT Control Systems and Reference Architecture (.pdf)
- EI&E PIT Control Systems Glossary (.pdf)
- EI&E PIT Control System Master List (.xlsx)
- NIST SP 800-82 R2 Industrial Control Systems Security Guide (.pdf)
- NIST SP 800-82 R2 ICS Overlay Security Controls (.xlsx)
- NIST SP 800-53 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)
- ICS Cybersecurity Handbook (.pdf)
- RMF Security Authorization Package (.xlsx)

Learn about the RMF process for DoD IT Systems.
View the RMF Process.

Additional Information:

Change Item #RG 3.8.0
Click to view page updates.

RMF KS EI&E FRCS PIT Webpages



RMF Knowledge Service > RMF General > IT

Energy, Installations

Background

Department of Defense Instruction (DoDI) 85
8510.01, Risk Management Framework (RMF
Technology (IT), incorporate Platform IT (PIT
category of both IT hardware and software th
dedicated to, or essential in real time to the m
purpose systems. PIT is further categorized a
subsystems, or PIT systems. PIT differs from
integral to – and dedicated to the operation of
the term PIT is used only by DoD, the concep
and systems dedicated to the operation of a s
example, the term "Operational Technology" (
these systems and components.

The most common forms of PIT are Control S
combination of control components (e.g., elec
pneumatic, etc.), special purpose controlling
act together upon underlying mechanical and
achieve an objective (e.g., transport of matter
and comfortable work environment, etc.). All a
considered PIT. Industrial Control Systems (I
systems that act upon industrial systems and
general term that encompasses several – but
systems. These include supervisory control a
systems, distributed control systems (DCS) a
as the Programmable Logic Controllers (PLC
sector and critical infrastructure. In the past, t
Defense for Energy, Installations and Environ
used ICS in an even broader sense to repres
(SCADA, DDC, DCS, building, vehicle, transp
most uses of the term ICS do not pertain to in
the term "Control System" is used herein for t

RMF Knowledge Service > RMF General > IT > Energy, Installations & En

Registering PIT Control Systems ir

The following sections provide step-by-step guidance to register CS in eM
in development of the CS PE authorization boundary and network architec

- Facility Engineer/Manager
- Facility Operations & Maintenance/Technician
- Physical Security Specialist
- Emergency Manager
- IT Network/Communications Specialist
- Information Assurance Specialist
- Tenants (Defense Health Agency, Defense Logistics Agency, etc)
- Operations and Maintenance Contractors
- Control System Vendor/Integrators
- Information Assurance Contractor

The group should define the CS PE boundary (physical and logical), identi
types of data and information that will be stored, displayed and/or transmit
used in conjunction with the EI&E CS Master List to develop these artifacts

Most CS PEs directly connect to or support mission critical assets (e.g., De
recommended by NIST SP 800-60 Vol 2, should be categorized at a secur
CS PE does not require H-H-H categorization, then use the lowest impact

When PE registration is complete, system details may be copied into a Wo
provide the physical and environmental security controls (from the UMCS
that attention to the sequence in which PE elements are registered can op
following sequence is recommended:

1. CS PE (H-H-H): make all Common, AT, IR, MA, and PM controls inh
2. Utility Monitoring and Control System (UMCS) or Building Control Sy
   -15) inheritable.
3. UMCS or Utility Control System (UCS): make PE controls (PE-9 ext
4. ESS: make PE controls (PE-1, PE-2, PE-3, PE-4, PE-5, PE6, and P
5. Fire & Life Safety Systems (FLS): make PE-13 controls inheritable.
6. Other Platform IT and DBS (e.g., a Computerized Maintenance Man
   and trouble tickets).

By copying and pasting system details generated for the PE, registering th
time required to create inheritance relationships will vary depending on the

RMF Knowledge Service › RMF General › IT › Energy, Ins

eMASS Guidance: Step 1a - Overview

System Name: Component ID - <Site Identifier> - CS - <C

EXAMPLE 1:
SA4619-CS-UMCS-I-AA - San Antonio-Control System-Uti

System Acronym: Same as system name. **NOTE:** on the
a shorthand method for recognizing RMF steps that must b
that enclave. Those systems may inherit security controls f
Environmental controls.

EXAMPLE 2:

- NDW-CS-PE-I-AA
- NDW-CS-UMCS-NI-A
- NDW-CS-ESS-I-A
- NDW-CS-PS-NI-A
- FTBEL-CS-PE-I-AA
- FTBEL-CS-ESS-I-AA
- FTBEL-CS-BCS-NI-A
- FTBEL-CS-UCS-NI-A
- FA4619-CS-PE-I-AA
- FA4619-CS-UMCS-NI-A
- FA4619-CS-FLS-NI-A
- JBHH-CS-PE-I-AA
- JBHH-CS-EM-NI-A
- JBHH-CS-ESS-I-AA
- JBA-CS-PE-I-AA
- JBA-CS-UMCS-NI-A
- JBA-CS-ESS-NI-A
- JBA-CS-AS-NI-A

Figure 4. eMASS Example Homescreen: Platform Enclo

RMF Knowledge Service › RMF General › IT › Energy, Installations & Environment (EI&E) Control Systems › eMASS Guidance: Step 2a

eMASS Guidance: Step 2a - Control Selection

Primary Security Control Set:

Select NIST SP 800-53 Rev 4 (note: NIST SP 800-82 Rev 2 Industrial Control Systems Security Guide, Appendix G ICS Overlay will be used to evaluate PIT control systems and will eventually be programmed into eMASS. Until that happens, the *EI&E NIST SP 800-82 Rev 2 ICS Overlay Security Controls* and *EI&E NIST SP 800-53 Rev 4 and 800-82 Rev 2 Merged* linked to this webpage can be used manually to complete the security controls.

Control Attributes:

- ***Confidentiality:*** Select from the ***EI&E PIT Control Systems Master List*** **Preliminary Confidentiality-Integrity-Availability (C-I-A) matrix**, columns H through P (note: the system owner and AO make the final determination of appropriate values; preliminary values are suggested only).
- ***Integrity:*** Select from the ***EI&E PIT Control Systems Master List*** Preliminary **C-I-A matrix**, columns H through P (note: the system owner and AO make the final determination of the appropriate value; preliminary values are suggested only).
- ***Availability:*** Select from the ***EI&E PIT Control Systems Master List*** **Preliminary C-I-A matrix**, columns H through P (note: the system owner and AO make the final determination of the appropriate value; preliminary values are suggested only).

The ***EI&E NIST SP 800-82 Rev 2 ICS Overlay Security Controls*** guidance includes several worksheets that cross-reference NIST SP 800-53 Rev 4 controls with NIST SP 800-82 Rev 2 controls. The worksheet labeled ***CNSSI 1253 800-82 IMPACT LEVELS*** provides the controls distributed for C-I-A following the Committee on National Security Systems Instruction (CNSSI) 1253 process, and lists the additional controls specific to control systems added to the CNSSI baseline. The worksheet labeled ***CONTROLS BY SELECTED CIA VALUES*** has C-I-A drop-down list that filters the NIST SP 800-82 Rev 2 control set, display the controls, and summarizes the number of controls.

- Additional control(s) will be added to the baseline and denoted by an "A" icon. Users also have the ability to delete (actually, comment out) controls if necessary. When entering data into eMASS, PIT CS controls are manually selected as follows:
  - Click "Add Additional Controls" for a list of security controls which may be added to those baseline controls already selected during Step 2a: Control Selection
  - To add a control to the baseline, place a check mark next to the desired control
  - Users will be prompted to provide a comment justifying the selection (e.g. directed by an overlay, etc.).
  - To remove a control, users will to provide a comment justifying the removal (e.g. directed by an overlay, etc.) in the justification comment box.

For hybrid/converged systems, use BOTH NIST SP 800-53 R4 and 800-82 R2 security controls.

Rationale For Categorization: Enter "NIST SP 800-60 Vol 2 Information and Data Types" and add the applicable types and special factors from the CS Master List such as "D.7.1 Energy Supply Information Type, Special Factors Affecting Integrity Impact Determination: Mission-critical systems":

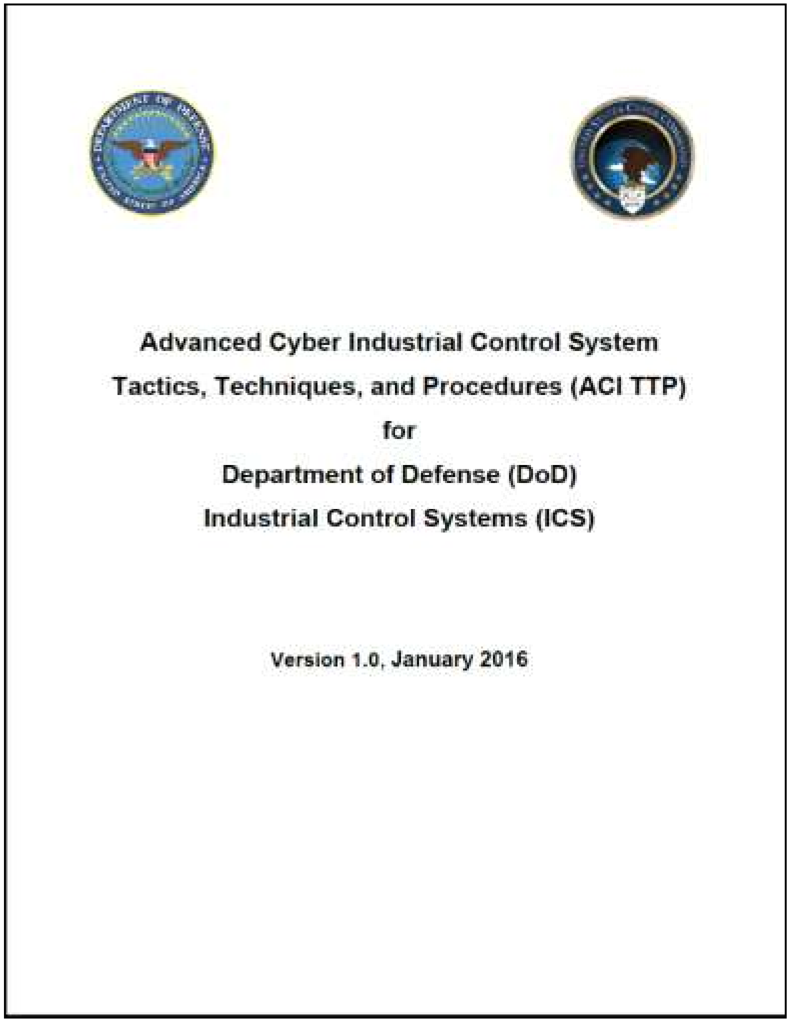
Unauthorized modification of mission-critical information or information systems (e.g., electrical power distribution, petroleum or gas pipelines) can result in severe impacts to the environment, service, major assets and/or human safety. Consequently, the integrity impact level associated with these types of mission-critical processes/systems may be high. Non mission-critical systems: For information or information systems that do not directly impact mission-critical functions, the integrity impact level may be downgraded to low."

EXAMPLE 7:

For a High-High-High PIT control systems, the following controls are added to the NIST SP 800-53 R4 baseline from the NIST SP 800-82 R2 overlay:

CP-12
IA-3(4)
PE-9(1)
PE-11(1)

RMF KS ICS PIT Webpage Key Docs



Advanced Cyber Industrial Control System

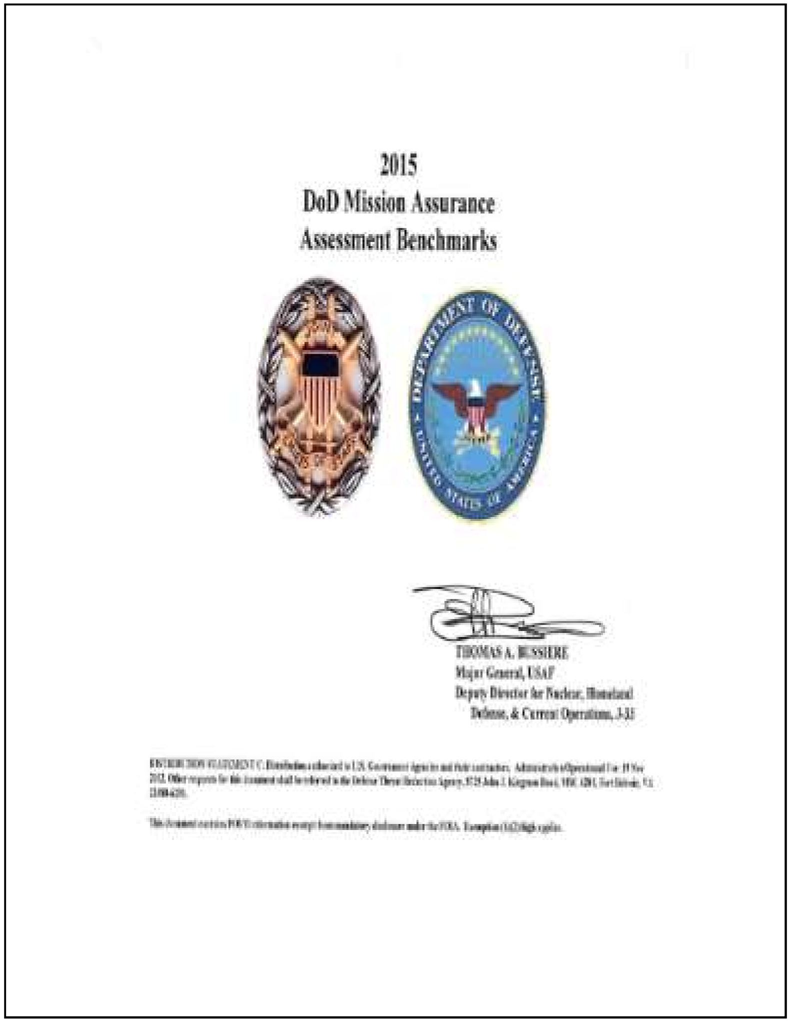
Tactics, Techniques, and Procedures (ACI TTP)

for

Department of Defense (DoD)

Industrial Control Systems (ICS)

Version 1.0, January 2016



2015
DoD Mission Assurance
Assessment Benchmarks

THOMAS A. BUSSIERE
Major General, USAF
Deputy Director for Nuclear, Homeland
Defense, & Current Operations, J-33

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors. Administrative/Operational Use: 19 Nov 2012. Other requests for this document shall be referred to the Defense Threat Reduction Agency, 8725 John J. Kingman Road, MSC 6201, Fort Belvoir, VA 22060-6201.

This document contains FOUO information exempt from mandatory disclosure under the FOIA. Exemption (b)(2)high applies.

DoD Mission Areas and Leads

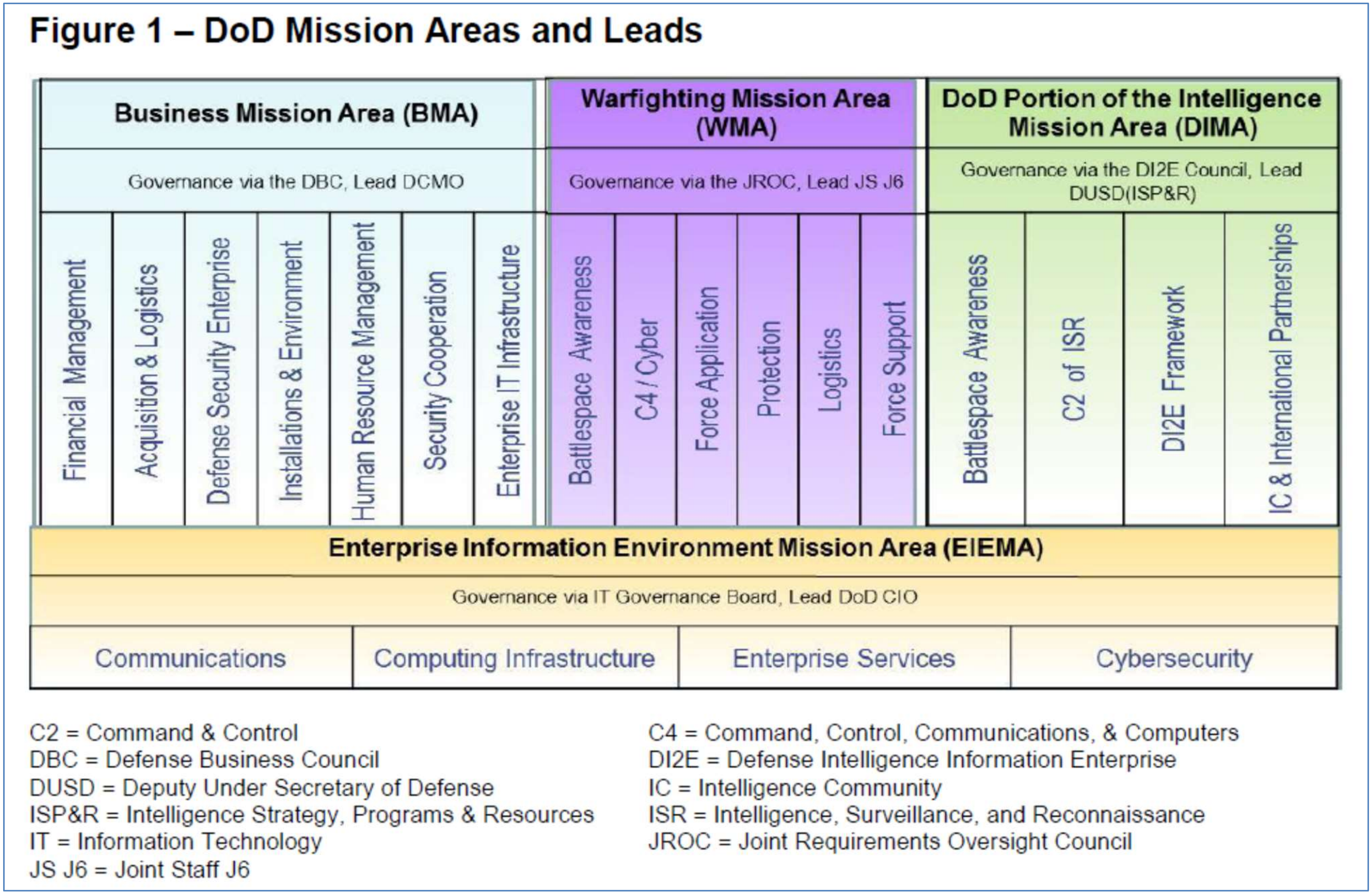


Figure 1 – DoD Mission Areas and Leads

Business Mission Area (BMA)

Governance via the DBC, Lead DCMO

- Financial Management
- Acquisition & Logistics
- Defense Security Enterprise
- Installations & Environment
- Human Resource Management
- Security Cooperation
- Enterprise IT Infrastructure

Warfighting Mission Area (WMA)

Governance via the JROC, Lead JS J6

- Battlespace Awareness
- C4 / Cyber
- Force Application
- Protection
- Logistics
- Force Support

DoD Portion of the Intelligence Mission Area (DIMA)

Governance via the DI2E Council, Lead DUSD(ISP&R)

- Battlespace Awareness
- C2 of ISR
- DI2E Framework
- IC & International Partnerships

Enterprise Information Environment Mission Area (EIEMA)

Governance via IT Governance Board, Lead DoD CIO

- Communications
- Computing Infrastructure
- Enterprise Services
- Cybersecurity

C2 = Command & Control
DBC = Defense Business Council
DUSD = Deputy Under Secretary of Defense
ISP&R = Intelligence Strategy, Programs & Resources
IT = Information Technology
JS J6 = Joint Staff J6

C4 = Command, Control, Communications, & Computers
DI2E = Defense Intelligence Information Enterprise
IC = Intelligence Community
ISR = Intelligence, Surveillance, and Reconnaissance
JROC = Joint Requirements Oversight Council

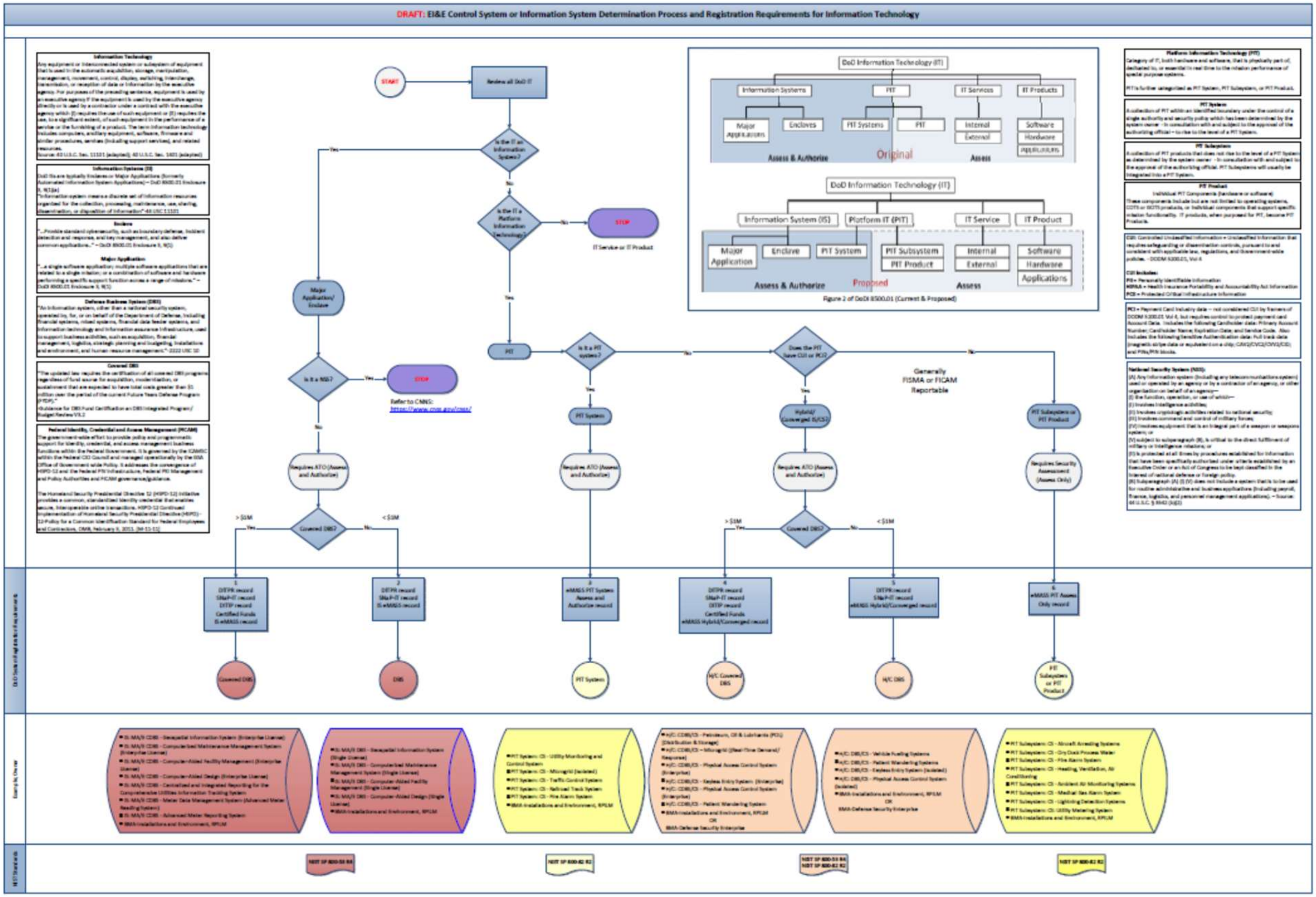
FMR 2016 Section J – SNaP-IT

The CIO SNaP-IT office issued DoD Financial Management Regulation (FMR) Volume 2B, Chapter 18 in June, 2015. This revised chapter applies to the FY 2017 budget and addresses PIT/FRCS in Section J:

> “J. Industrial Control Systems (ICS)/ Platform Information Technology (PIT)/ Supervisory Control and Data Acquisition (SCADA)
>
> “As stated in NIST Special Publication 800-82, "ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems." These systems, while not generally considered a typical Information System, are just as vulnerable to interception, modification, interruption and fabrication that threaten typical Information Technology Systems. Likewise, the defensive measures taken to protect ICS/PIT/SCADA systems are similar to the cybersecurity measures currently taken to protect IT systems: Firewalls, Intrusion Detection Systems, strong passwords, and encryption to name a few. Therefore, the documented planning, programming and budgeting of the costs of researching, procuring, operating and maintaining these defensive mechanisms used to protect ICS/PIT/SCADA from these vulnerability exploitations should begin in the FY17 President's Budget using SNaP-IT. PIT ICS purchased as part of a weapons systems or some other turn-key non-IT solution (i.e., as part of an HVAC system) would not be reported in the IT/Cyber Budget. In summary, if the turn-key solution is IT then the ICS/PIT/SCADA systems would be reported within the turn-key investments IT/Cyber budget. If the PIT FRCS is being purchased on its own or upgraded to address cyber security shortfalls, it would be reported in the IT/cyber budget. Lastly there is no need register PIT FRCS as a separate IT investment -- it can be a part of a larger investment.”

IMPORTANT: As DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations,* the Joint Information Environment (JIE), and the new Chapter 18 FMR Volume 2B are implemented, many of the IS and FRCS perimeter and boundary edge protection devices as well as continuous monitoring will be part of the IT/Cyber budget. Expenditures for new PIT products needed for cybersecurity of existing IT will be reported as part of the IT/Cyber budget. Software, services, or major applications – which are not part of the Host Based Security System/Assured Compliance Assessment Solution that are acquired to provide continuous monitoring of PIT – will also be part of the IT/Cyber budget.

RMF KS IT-PIT Decision Tree



DRAFT: EI&E Control System or Information System Determination Process and Registration Requirements for Information Technology

Information Technology
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Source: 40 U.S.C. Sec. 11101 (adapted); 40 U.S.C. Sec. 1401 (adapted)

Information Systems (IS)
DoD ISs are typically Enclaves or Major Applications (formerly Automated Information System Applications) – DoD 8500.01 Enclosure 3, 9(1)(a)
"Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" 44 USC 11101

Enclave
"...Provide standard cybersecurity, such as boundary defense, incident detection and response, and key management, and also deliver common applications..." – DoDI 8500.01 Enclosure 3, 9(1)

Major Application
"...a single software application; multiple software applications that are related to a single mission; or a combination of software and hardware performing a specific support function across a range of missions." – DoDI 8500.01 Enclosure 3, 9(1)

Defense Business System (DBS)
"An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management." -2222 USC 10

Covered DBS
"The updated law requires the certification of all covered DBS programs regardless of fund source for acquisition, modernization, or sustainment that are expected to have total costs greater than $1 million over the period of the current Future Years Defense Program (FYDP)."
-Guidance for DBS Fund Certification an DBS Integrated Program/Budget Review V3.2

Federal Identity, Credential and Access Management (FICAM)
The government-wide effort to provide policy and programmatic support for identity, credential, and access management business functions within the Federal Government. It is governed by the ICAMSC within the Federal CIO Council and managed operationally by the GSA Office of Government-wide Policy. It addresses the convergence of HSPD-12 and the Federal PIV Infrastructure, Federal PKI Management and Policy Authorities and FICAM governance/guidance.

The Homeland Security Presidential Directive 12 (HSPD-12) initiative provides a common, standardized identity credential that enables secure, interoperable online transactions. HSPD-12 Continued Implementation of Homeland Security Presidential Directive (HSPD)-12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

START
Review all DoD IT
Is the IT an Information System?
Yes
No
Is the IT a Platform Information Technology?
No
STOP
IT Service or IT Product
Yes
Major Application/ Enclave
Is it a NSS?
Yes
STOP
No
Requires ATO (Assess and Authorize)
Covered DBS?
> $1M
Yes
< $1M
No
PIT
Is it a PIT system?
Yes
PIT System
Requires ATO (Assess and Authorize)
No
Does the PIT have CUI or PCI?
Yes
Hybrid/ Converged IS/CS?
Requires ATO (Assess and Authorize)
Covered DBS?
> $1M
Yes
< $1M
No
No
Generally FISMA or FICAM Reportable
PIT Subsystem or PIT Product
Requires Security Assessment (Assess Only)

Refer to CNNS:
https://www.cnss.gov/cnss/

Figure 2 of DoDI 8500.01 (Current & Proposed)

Platform Information Technology (PIT)
Category of IT, both 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 System, PIT Subsystem, or PIT Product.

PIT System
A collection of PIT within an identified boundary under the control of a single authority and security policy which has been determined by the system owner – in consultation with and subject to the approval of the authorizing official – to rise to the level of a PIT System.

PIT Subsystem
A collection of PIT products that does not rise to the level of a PIT System as determined by the system owner – in consultation with and subject to the approval of the authorizing official. PIT Subsystems will usually be integrated into a PIT System.

PIT Product
Individual PIT Components (hardware or software)
These components include but are not limited to operating systems, COTS or GOTS products, or individual components that support specific mission functionality. IT products, when purposed for PIT, become PIT Products.

CUI: Controlled Unclassified Information = Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. - DODM 5200.01, Vol 4

CUI includes:
PII = Personally Identifiable Information
HIPAA = Health Insurance Portability and Accountability Act Information
PCII = Protected Critical Infrastructure Information

PCI = Payment Card Industry data – not considered CUI by framers of DODM 5200.01 Vol 4, but requires control to protect payment card Account Data. Includes the following Cardholder data: Primary Account Number; Cardholder Name; Expiration Date; and Service Code. Also includes the following Sensitive Authentication data: Full track data (magnetic stripe data or equivalent on a chip; CAV2/CVC2/CVV2/CID; and PINs/PIN blocks.

National Security System (NSS):
(A) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
(i) the function, operation, or use of which—
(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). – Source: 44 U.S.C. § 3542 (b)(2)

- IS: MA/IS CDBS – Geospatial Information System (Enterprise License)
- IS: MA/IS CDBS – Computerized Maintenance Management System (Enterprise License)
- IS: MA/IS CDBS – Computer-Aided Facility Management (Enterprise License)
- IS: MA/IS CDBS – Computer-Aided Design (Enterprise License)
- IS: MA/IS CDBS – Centralized and Integrated Reporting for the Comprehensive Utilities Information Tracking System
- IS: MA/IS CDBS – Meter Data Management System (Advanced Meter Reading System)
- IS: MA/IS CDBS – Advanced Meter Reporting System
- BMA-Installations and Environment, RPILM

- IS: MA/IS DBS – Geospatial Information System (Single License)
- IS: MA/IS DBS – Computerized Maintenance Management System (Single License)
- IS: MA/IS DBS – Computer-Aided Facility Management (Single License)
- IS: MA/IS DBS – Computer-Aided Design (Single License)
- BMA-Installations and Environment, RPILM

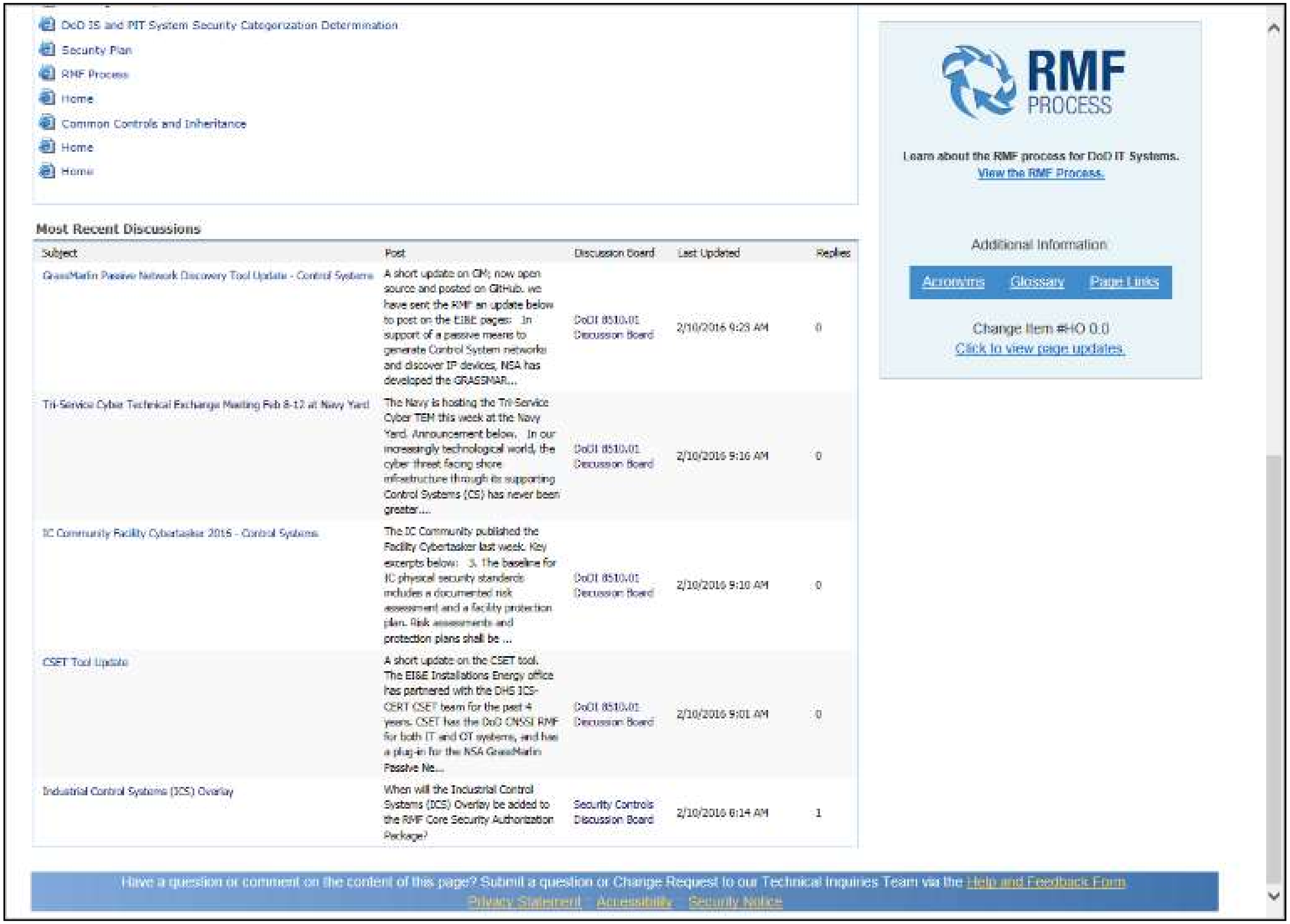
- PIT System: CS – Utility Monitoring and Control System
- PIT System: CS – Microgrid (Isolated)
- PIT System: CS – Traffic Control System
- PIT System: CS – Railroad Track System
- PIT System: CS – Fire Alarm System
- BMA-Installations and Environment, RPILM

- H/C: CDBS/CS – Petroleum, Oil & Lubricants (POL) (Distribution & Storage)
- H/C: CDBS/CS – Microgrid (Real-Time Demand/Response)
- H/C: CDBS/CS – Physical Access Control System (Enterprise)
- H/C: CDBS/CS – Keyless Entry System (Enterprise)
- H/C: CDBS/CS – Physical Access Control System (Enterprise)
- H/C: CDBS/CS – Patient Wandering System
- BMA-Installations and Environment, RPILM
OR
BMA-Defense Security Enterprise

- H/C: DBS/CS – Vehicle Fueling Systems
- H/C: DBS/CS – Patient Wandering Systems
- H/C: DBS/CS – Keyless Entry System (Isolated)
- H/C: DBS/CS – Physical Access Control System (Isolated)
- BMA-Installations and Environment, RPILM
OR
BMA-Defense Security Enterprise

- PIT Subsystem: CS – Aircraft Arresting Systems
- PIT Subsystem: CS – Dry Dock Process Water
- PIT Subsystem: CS – Fire Alarm System
- PIT Subsystem: CS – Heating, Ventilation, Air Conditioning
- PIT Subsystem: CS – Ambient Air Monitoring Systems
- PIT Subsystem: CS – Medical Gas Alarm System
- PIT Subsystem: CS – Lightning Detection Systems
- PIT Subsystem: CS – Utility Metering System
- BMA-Installations and Environment, RPILM

RMF KS FRCS PIT Webpage Discussions



- DoD IS and PIT System Security Categorization Determination
- Security Plan
- RMF Process
- Home
- Common Controls and Inheritance
- Home
- Home

Most Recent Discussions

Subject	Post	Discussion Board	Last Updated	Replies
GrassMarlin Passive Network Discovery Tool Update - Control Systems	A short update on GM; now open source and posted on GitHub. we have sent the RMF an update below to post on the EI&E pages: In support of a passive means to generate Control System networks and discover IP devices, NSA has developed the GRASSMAR...	DoDI 8510.01 Discussion Board	2/10/2016 9:23 AM	0
Tri-Service Cyber Technical Exchange Meeting Feb 8-12 at Navy Yard	The Navy is hosting the Tri-Service Cyber TEM this week at the Navy Yard. Announcement below. In our increasingly technological world, the cyber threat facing shore infrastructure through its supporting Control Systems (CS) has never been greater....	DoDI 8510.01 Discussion Board	2/10/2016 9:16 AM	0
IC Community Facility Cybertasker 2016 - Control Systems	The IC Community published the Facility Cybertasker last week. Key excerpts below: 3. The baseline for IC physical security standards includes a documented risk assessment and a facility protection plan. Risk assessments and protection plans shall be ...	DoDI 8510.01 Discussion Board	2/10/2016 9:10 AM	0
CSET Tool Update	A short update on the CSET tool. The EI&E Installations Energy office has partnered with the DHS ICS-CERT CSET team for the past 4 years. CSET has the DoD CNSSI RMF for both IT and OT systems, and has a plug-in for the NSA GrassMarlin Passive Ne...	DoDI 8510.01 Discussion Board	2/10/2016 9:01 AM	0
Industrial Control Systems (ICS) Overlay	When will the Industrial Control Systems (ICS) Overlay be added to the RMF Core Security Authorization Package?	Security Controls Discussion Board	2/10/2016 8:14 AM	1

RMF PROCESS

Learn about the RMF process for DoD IT Systems.
View the RMF Process.

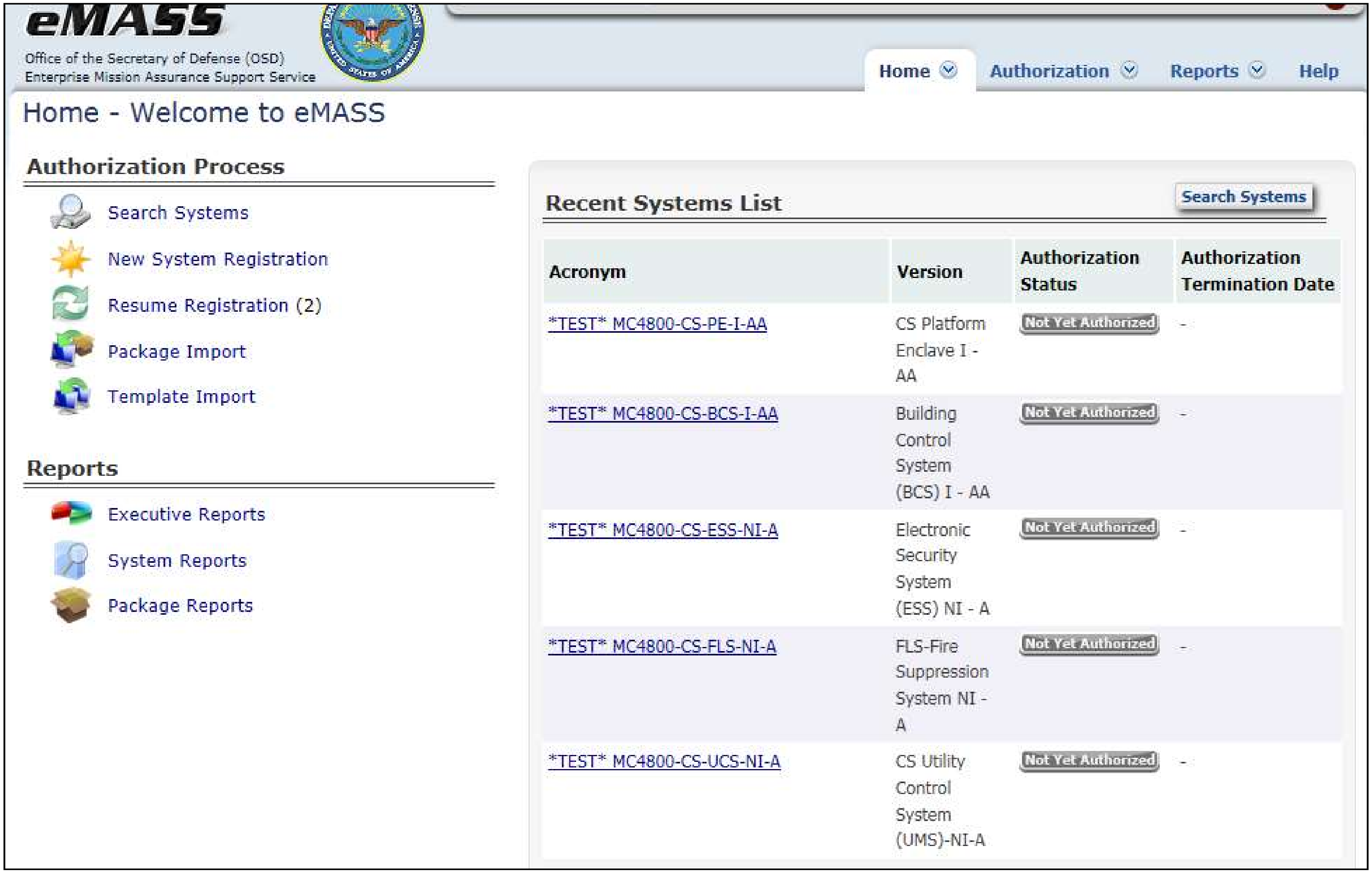
Additional Information

Acronyms Glossary Page Links

Change Item #HO 0.0
Click to view page updates

Have a question or comment on the content of this page? Submit a question or Change Request to our Technical Inquiries Team via the Help and Feedback Form
Privacy Statement Accessibility Security Notice

eMASS Home



Home - Welcome to eMASS

Authorization Process

- Search Systems
- New System Registration
- Resume Registration (2)
- Package Import
- Template Import

Reports

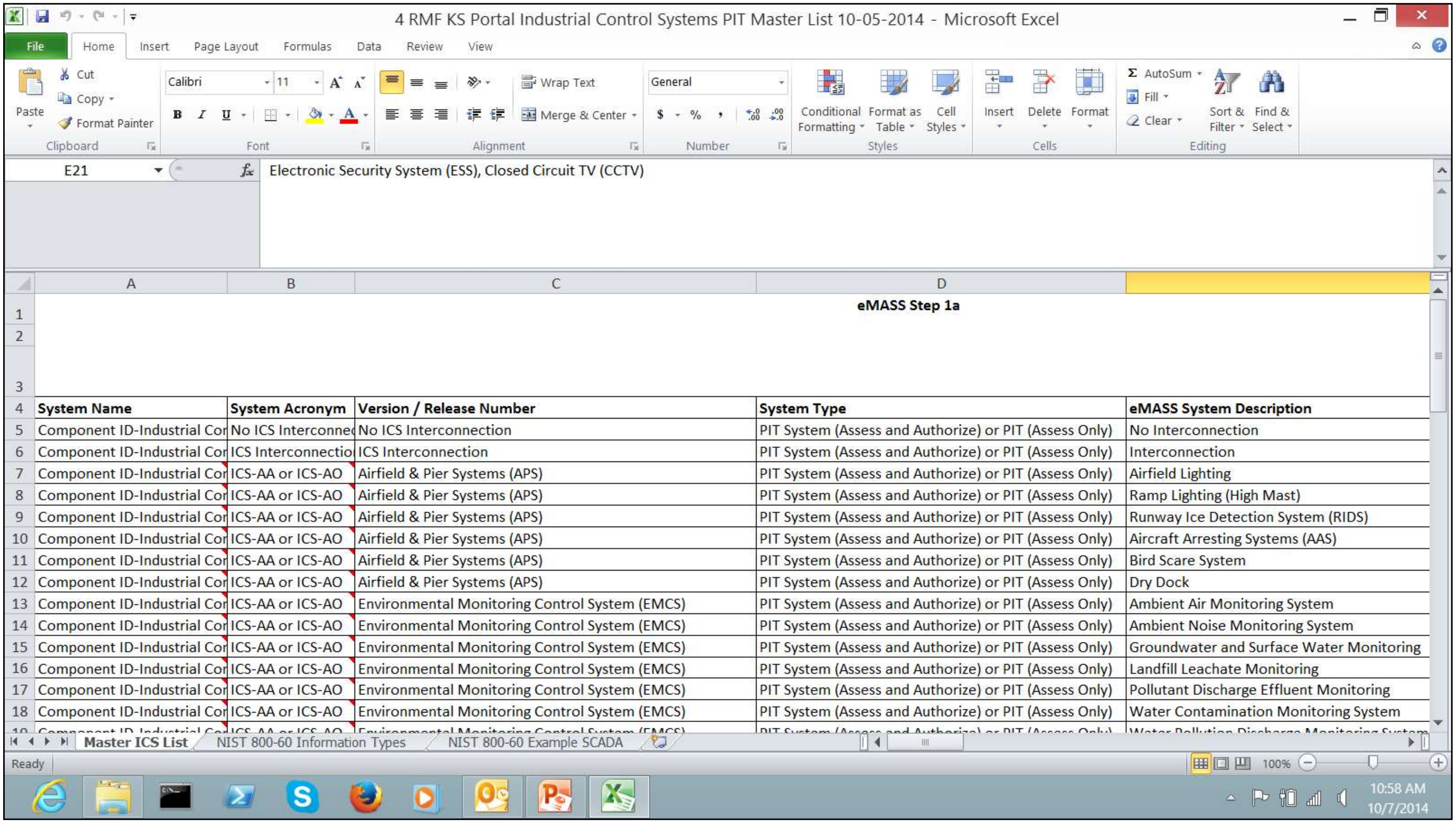
- Executive Reports
- System Reports
- Package Reports

Recent Systems List

Acronym	Version	Authorization Status	Authorization Termination Date
TEST MC4800-CS-PE-I-AA	CS Platform Enclave I - AA	Not Yet Authorized	-
TEST MC4800-CS-BCS-I-AA	Building Control System (BCS) I - AA	Not Yet Authorized	-
TEST MC4800-CS-ESS-NI-A	Electronic Security System (ESS) NI - A	Not Yet Authorized	-
TEST MC4800-CS-FLS-NI-A	FLS-Fire Suppression System NI - A	Not Yet Authorized	-
TEST MC4800-CS-UCS-NI-A	CS Utility Control System (UMS)-NI-A	Not Yet Authorized	-

Manually input FRCS information

eMASS Step 1a



4 RMF KS Portal Industrial Control Systems PIT Master List 10-05-2014 - Microsoft Excel

E21 Electronic Security System (ESS), Closed Circuit TV (CCTV)

eMASS Step 1a

	System Name	System Acronym	Version / Release Number	System Type	eMASS System Description
5	Component ID-Industrial Co	No ICS Interconne	No ICS Interconnection	PIT System (Assess and Authorize) or PIT (Assess Only)	No Interconnection
6	Component ID-Industrial Co	ICS Interconnectio	ICS Interconnection	PIT System (Assess and Authorize) or PIT (Assess Only)	Interconnection
7	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Airfield Lighting
8	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Ramp Lighting (High Mast)
9	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Runway Ice Detection System (RIDS)
10	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Aircraft Arresting Systems (AAS)
11	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Bird Scare System
12	Component ID-Industrial Co	ICS-AA or ICS-AO	Airfield & Pier Systems (APS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Dry Dock
13	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Ambient Air Monitoring System
14	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Ambient Noise Monitoring System
15	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Groundwater and Surface Water Monitoring
16	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Landfill Leachate Monitoring
17	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Pollutant Discharge Effluent Monitoring
18	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Water Contamination Monitoring System
19	Component ID-Industrial Co	ICS-AA or ICS-AO	Environmental Monitoring Control System (EMCS)	PIT System (Assess and Authorize) or PIT (Assess Only)	Water Pollution Discharge Monitoring System

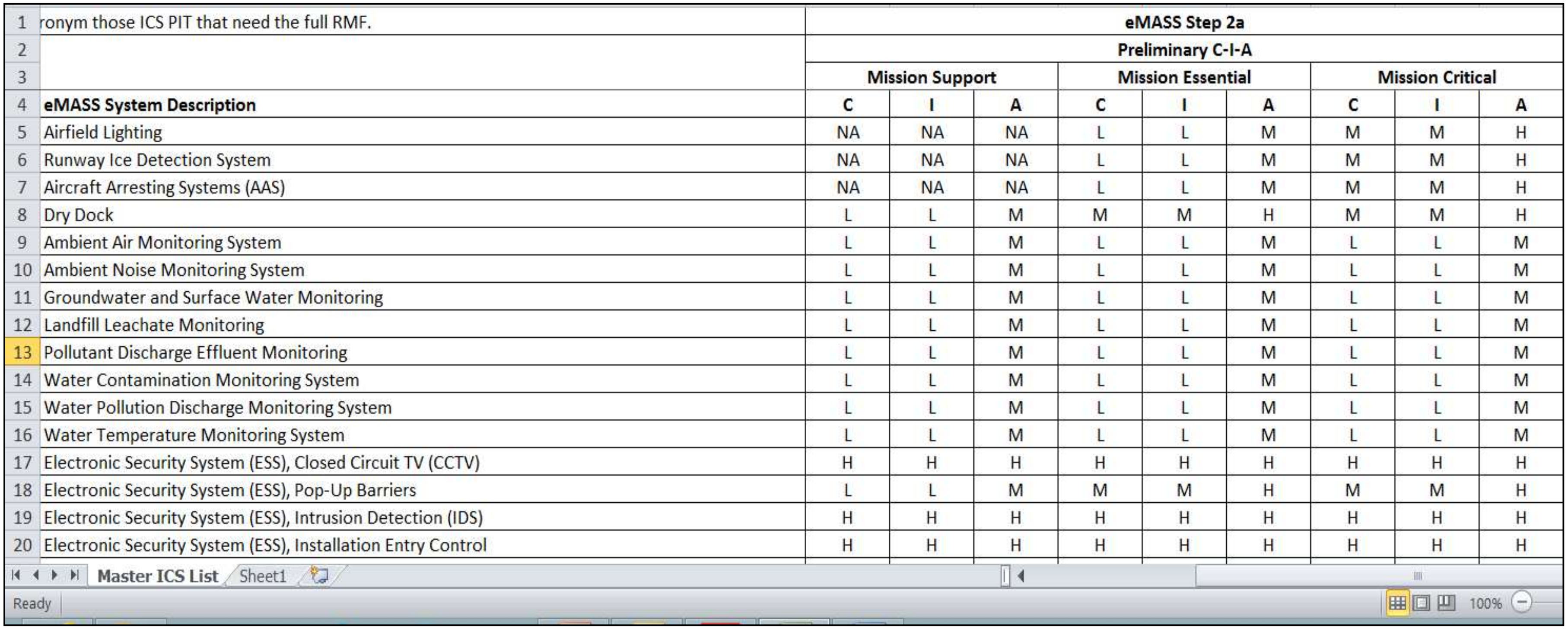
Manually input ICS information

eMASS Step 2a

DoD has been an active contributor to the **NIST SP 800-82 Industrial Control Systems Security Guide**. Appendix G is the ICS Overlay and provides the tailoring and supplemental guidance to cyber secure ICS. The incorporation of NIST SP 800-82 into eMASS is in progress but not expected to be available until spring 2015. In the interim, the excel file **NIST SP 800-82 R2 Controls** can be used to manually enter data into eMASS for an ICS PIT.

Although NIST SP 800-82 R 2 defines ICS as Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DFRCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), **the security controls can be used by an organization to address other control systems that are not typically thought of as “Industrial”. For example, there are many building, transportation, medical, security and logistics systems that although similar in many respects to traditional ICS, use different protocols, ports and services and are configured and operate in different modes than SCADA or DFRCS systems.**

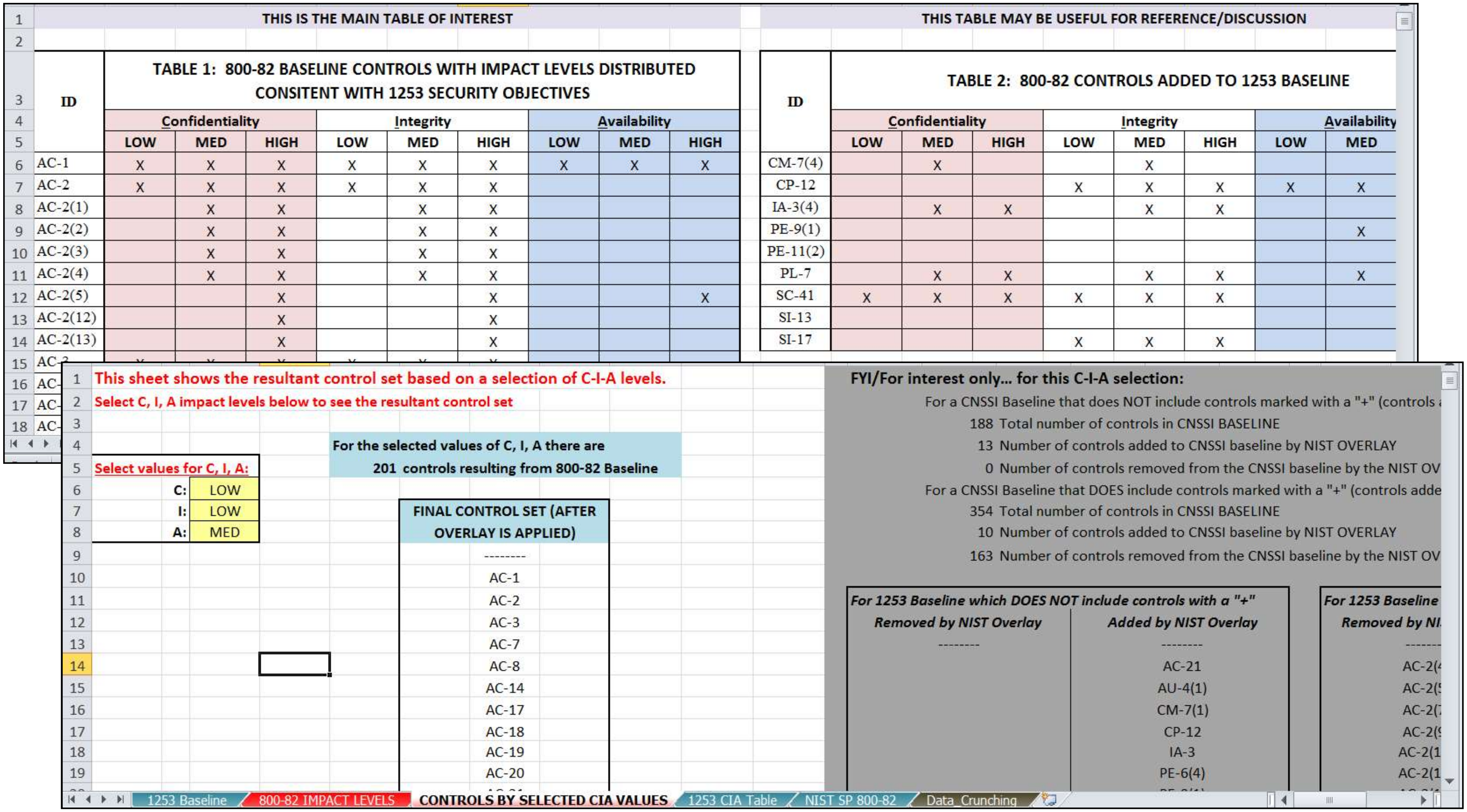
eMASS Step 2a C-I-A



1	ronym those ICS PIT that need the full RMF.	eMASS Step 2a								
2		Preliminary C-I-A								
3		Mission Support			Mission Essential			Mission Critical		
4	**eMASS System Description**	**C**	**I**	**A**	**C**	**I**	**A**	**C**	**I**	**A**
5	Airfield Lighting	NA	NA	NA	L	L	M	M	M	H
6	Runway Ice Detection System	NA	NA	NA	L	L	M	M	M	H
7	Aircraft Arresting Systems (AAS)	NA	NA	NA	L	L	M	M	M	H
8	Dry Dock	L	L	M	M	M	H	M	M	H
9	Ambient Air Monitoring System	L	L	M	L	L	M	L	L	M
10	Ambient Noise Monitoring System	L	L	M	L	L	M	L	L	M
11	Groundwater and Surface Water Monitoring	L	L	M	L	L	M	L	L	M
12	Landfill Leachate Monitoring	L	L	M	L	L	M	L	L	M
13	Pollutant Discharge Effluent Monitoring	L	L	M	L	L	M	L	L	M
14	Water Contamination Monitoring System	L	L	M	L	L	M	L	L	M
15	Water Pollution Discharge Monitoring System	L	L	M	L	L	M	L	L	M
16	Water Temperature Monitoring System	L	L	M	L	L	M	L	L	M
17	Electronic Security System (ESS), Closed Circuit TV (CCTV)	H	H	H	H	H	H	H	H	H
18	Electronic Security System (ESS), Pop-Up Barriers	L	L	M	M	M	H	M	M	H
19	Electronic Security System (ESS), Intrusion Detection (IDS)	H	H	H	H	H	H	H	H	H
20	Electronic Security System (ESS), Installation Entry Control	H	H	H	H	H	H	H	H	H

Manually input FRCS information

eMASS NIST SP 800-82 Controls



THIS IS THE MAIN TABLE OF INTEREST

ID	TABLE 1: 800-82 BASELINE CONTROLS WITH IMPACT LEVELS DISTRIBUTED CONSITENT WITH 1253 SECURITY OBJECTIVES								
	Confidentiality			Integrity			Availability		
	LOW	MED	HIGH	LOW	MED	HIGH	LOW	MED	HIGH
AC-1	X	X	X	X	X	X	X	X	X
AC-2	X	X	X	X	X	X			
AC-2(1)		X	X		X	X			
AC-2(2)		X	X		X	X			
AC-2(3)		X	X		X	X			
AC-2(4)		X	X		X	X			
AC-2(5)			X			X			X
AC-2(12)			X			X			
AC-2(13)			X			X			
AC-3	X	X	X	X	X	X			
AC-									
AC-									
AC-									

THIS TABLE MAY BE USEFUL FOR REFERENCE/DISCUSSION

ID	TABLE 2: 800-82 CONTROLS ADDED TO 1253 BASELINE							
	Confidentiality			Integrity			Availability	
	LOW	MED	HIGH	LOW	MED	HIGH	LOW	MED
CM-7(4)		X			X			
CP-12				X	X	X	X	X
IA-3(4)		X	X		X	X		
PE-9(1)								X
PE-11(2)								
PL-7		X	X		X	X		X
SC-41	X	X	X	X	X	X		
SI-13								
SI-17				X	X	X		

This sheet shows the resultant control set based on a selection of C-I-A levels.

Select C, I, A impact levels below to see the resultant control set

For the selected values of C, I, A there are
201 controls resulting from 800-82 Baseline

Select values for C, I, A:	
C:	LOW
I:	LOW
A:	MED

FINAL CONTROL SET (AFTER OVERLAY IS APPLIED)

AC-1
AC-2
AC-3
AC-7
AC-8
AC-14
AC-17
AC-18
AC-19
AC-20

FYI/For interest only... for this C-I-A selection:

For a CNSSI Baseline that does NOT include controls marked with a "+" (controls

188 Total number of controls in CNSSI BASELINE

13 Number of controls added to CNSSI baseline by NIST OVERLAY

0 Number of controls removed from the CNSSI baseline by the NIST OV

For a CNSSI Baseline that DOES include controls marked with a "+" (controls adde

354 Total number of controls in CNSSI BASELINE

10 Number of controls added to CNSSI baseline by NIST OVERLAY

163 Number of controls removed from the CNSSI baseline by the NIST OV

For 1253 Baseline which DOES NOT include controls with a "+"	
Removed by NIST Overlay	***Added by NIST Overlay***
--------	--------
	AC-21
	AU-4(1)
	CM-7(1)
	CP-12
	IA-3
	PE-6(4)

For 1253 Baseline
Removed by NI

AC-2(
AC-2(
AC-2(
AC-2(
AC-2(1
AC-2(1

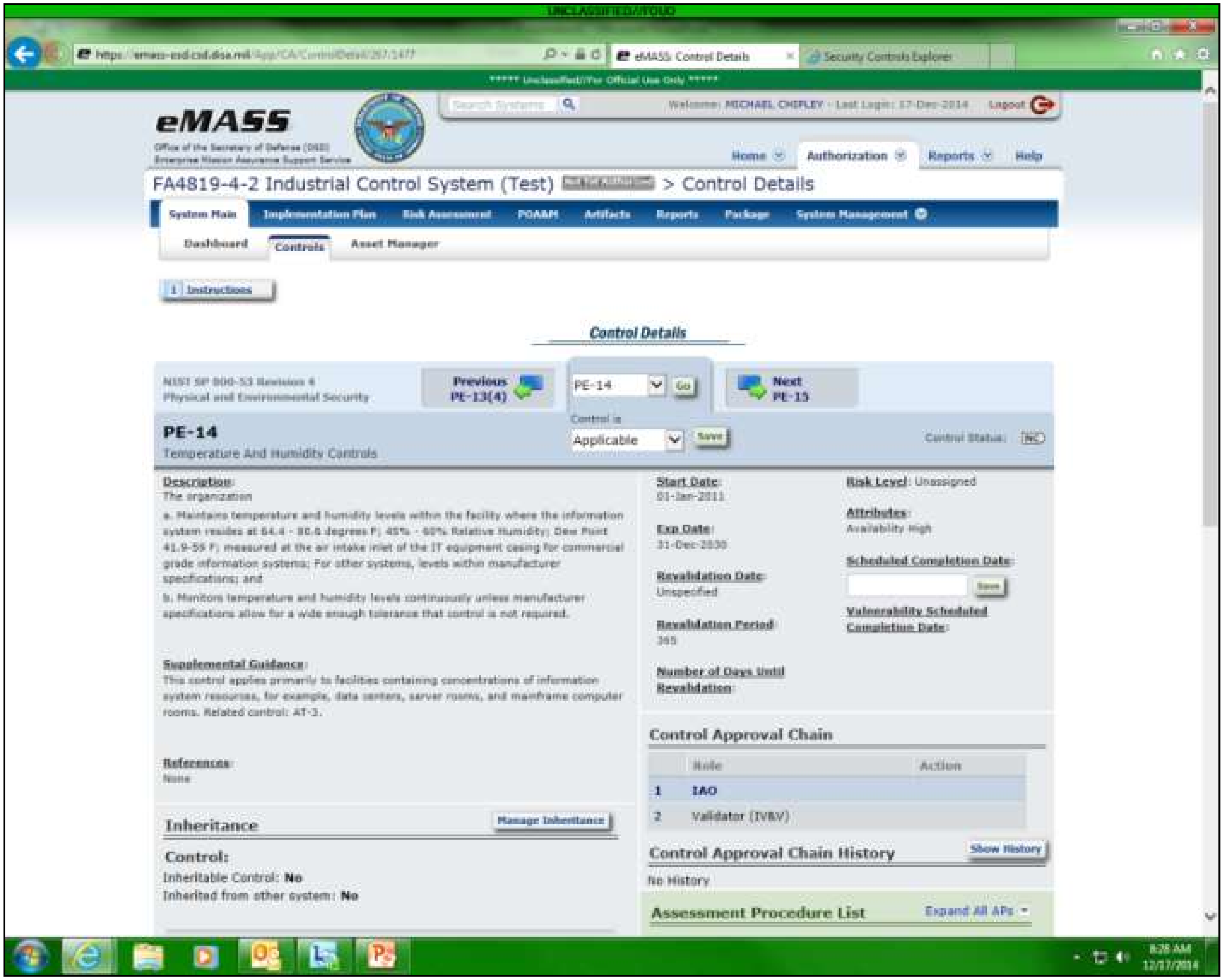
FRCS Overlay adds and deletes to the CNSSI 1253 Baseline

Add/Comment Out Baseline Controls

The remainder of eMASS is completed in a similar manner as IT systems. The **NIST SP 800-82 R2 Controls** has several worksheets that cross-walk the NIST SP 800-53 R4 controls with the NIST SP 800-53 R2 controls. The Worksheet labeled 800-82 IMPACT LEVELS provides the controls distributed for C-I-A following the CNSSI 1253 process and lists the additional controls added to the CNSSI Baseline specific to ICS. The Worksheet labeled CONTROLS SELECTED BY CIA VALUES has CIA Drop Down data lists that filters the 800-82 control set and displays the controls and a summary of the number of controls.

Manually input FRCS information

eMASS Controls Information



FA4819-4-2 Industrial Control System (Test) > Control Details

Control Details

NIST SP 800-53 Revision 4
Physical and Environmental Security

PE-14

Control is: Applicable

PE-14
Temperature And Humidity Controls

Control Status: NC

Description:
The organization

a. Maintains temperature and humidity levels within the facility where the information system resides at 64.4 - 80.6 degrees F; 45% - 60% Relative Humidity; Dew Point 41.9-59 F; measured at the air intake inlet of the IT equipment casing for commercial grade information systems; For other systems, levels within manufacturer specifications; and

b. Monitors temperature and humidity levels continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.

Supplemental Guidance:
This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.

References:
None

Start Date:
01-Jan-2011

Exp Date:
31-Dec-2030

Revalidation Date:
Unspecified

Revalidation Period:
365

Number of Days Until Revalidation:

Risk Level: Unassigned

Attributes:
Availability High

Scheduled Completion Date:

Vulnerability Scheduled Completion Date:

Inheritance

Control:
Inheritable Control: **No**
Inherited from other system: **No**

Control Approval Chain

	Role	Action
1	IAO	
2	Validator (IV&V)	

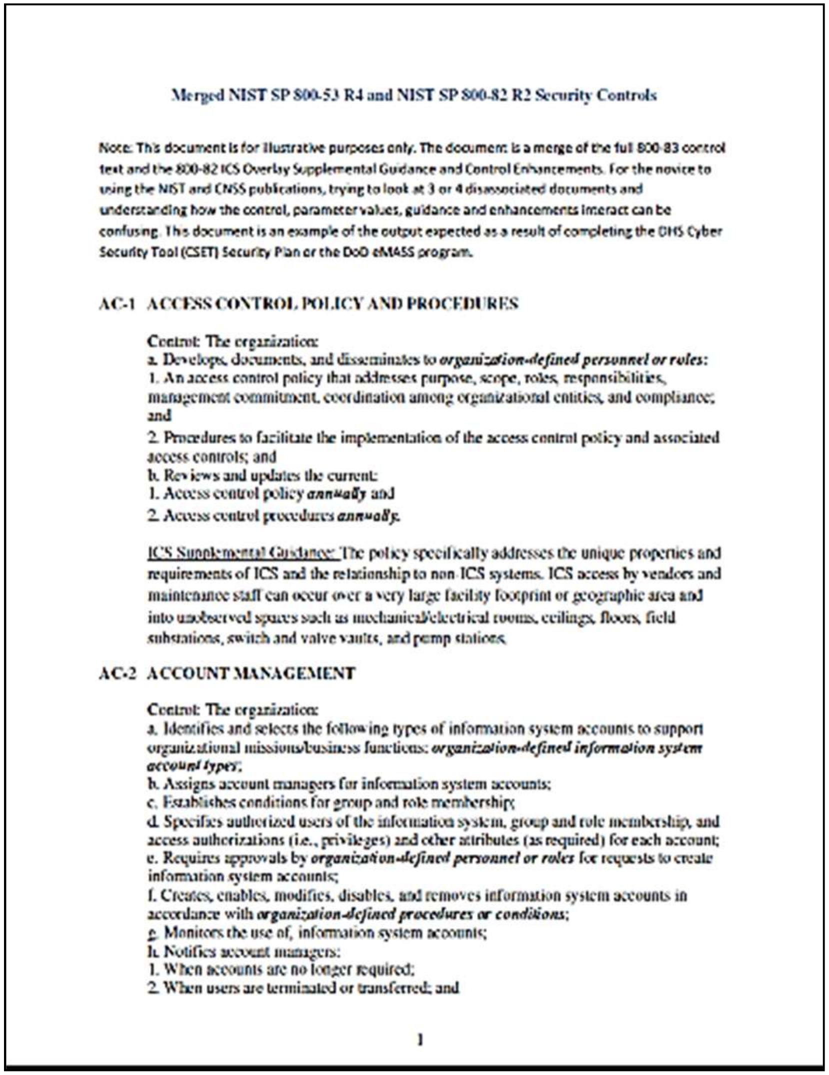
Control Approval Chain History

No History

Assessment Procedure List

8:28 AM
12/17/2014

Example of Merged Controls



Merged NIST SP 800-53 R4 and NIST SP 800-82 R2 Security Controls

Note: This document is for illustrative purposes only. The document is a merge of the full 800-83 control text and the 800-82 ICS Overlay Supplemental Guidance and Control Enhancements. For the novice to using the NIST and CNSS publications, trying to look at 3 or 4 disassociated documents and understanding how the control, parameter values, guidance and enhancements interact can be confusing. This document is an example of the output expected as a result of completing the DHS Cyber Security Tool (CSET) Security Plan or the DoD eMASS program.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles:***
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
1. Access control policy ***annually*** and
2. Access control procedures ***annually.***

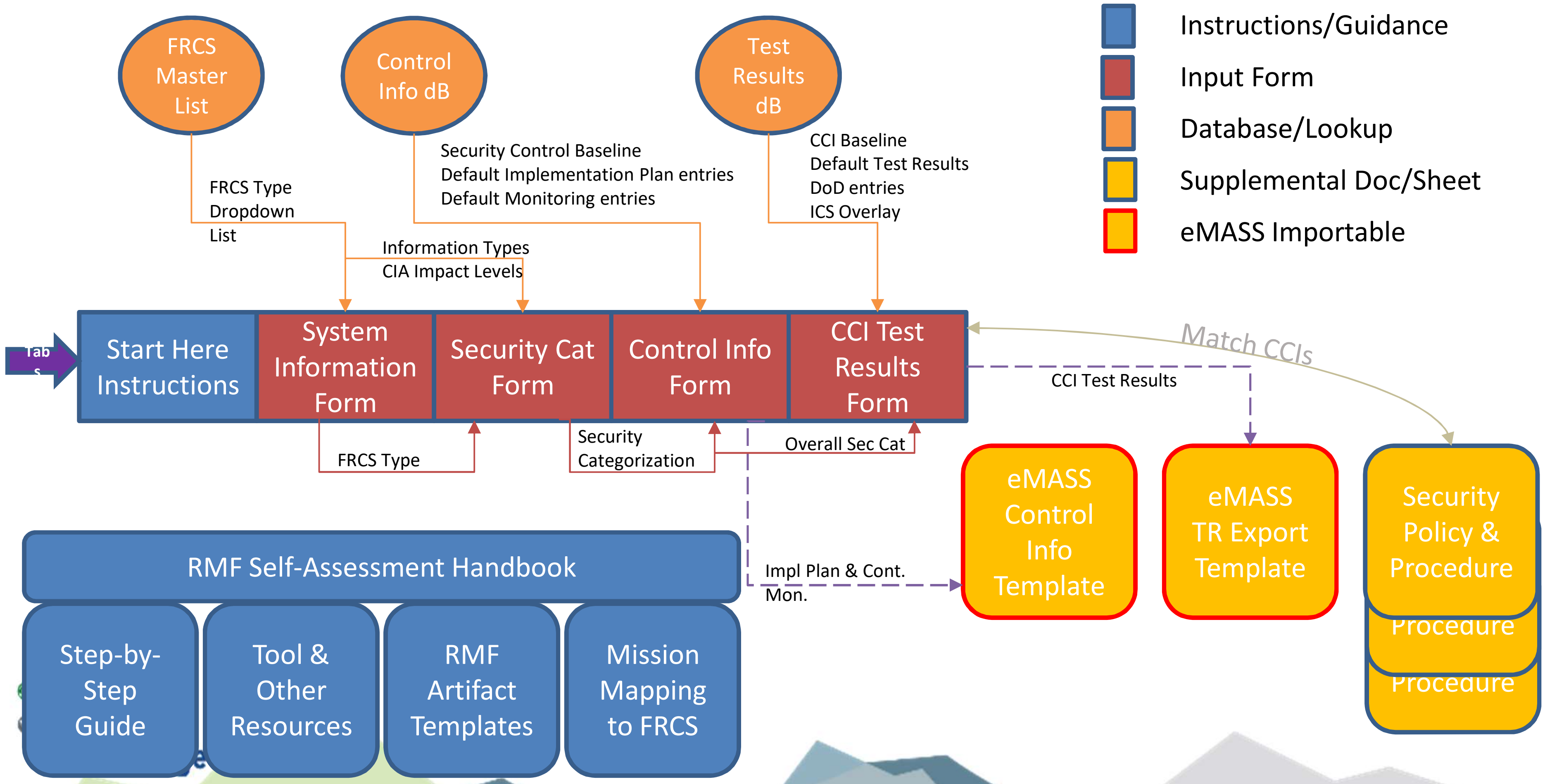
ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems. ICS access by vendors and maintenance staff can occur over a very large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: ***organization-defined information system account types;***
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by ***organization-defined personnel or roles*** for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with ***organization-defined procedures or conditions***;
g. Monitors the use of, information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and

At the completion of the eMASS security controls, the Security Plan can be generated. An example of a Security Plan with the **NIST SP 800-53 R4 and NIST SP 800-82 R2 Merged** security control set and ICS Overlay shows how the security control, parameter value, Supplemental Guidance and Control Enhancements are combined into a full narrative text.

ESCTP FRCS RMF Tool – Coming Soon!



- 🟦 Instructions/Guidance
- 🟥 Input Form
- 🟧 Database/Lookup
- 🟨 Supplemental Doc/Sheet
- 🟨 eMASS Importable

FRCS Master List

Control Info dB

Test Results dB

FRCS Type Dropdown List

Security Control Baseline
Default Implementation Plan entries
Default Monitoring entries

CCI Baseline
Default Test Results
DoD entries
ICS Overlay

Information Types
CIA Impact Levels

Tab s

Start Here Instructions

System Information Form

Security Cat Form

Control Info Form

CCI Test Results Form

Match CCIs

CCI Test Results

FRCS Type

Security Categorization

Overall Sec Cat

Impl Plan & Cont. Mon.

eMASS Control Info Template

eMASS TR Export Template

Security Policy & Procedure

Procedure

Procedure

RMF Self-Assessment Handbook

Step-by-Step Guide

Tool & Other Resources

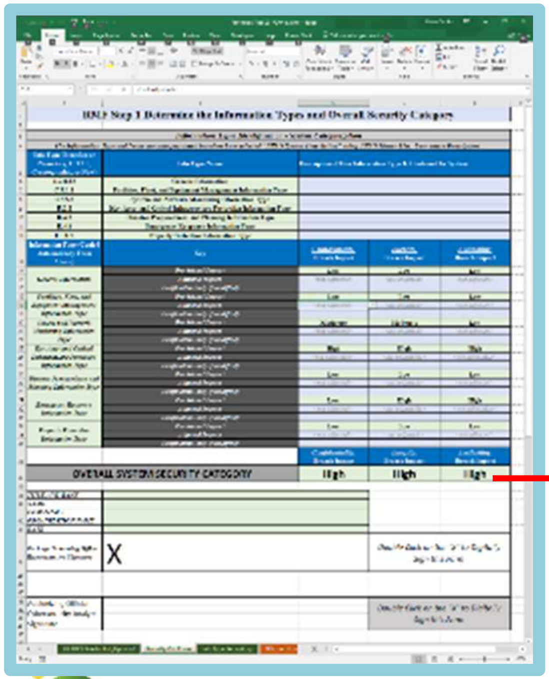
RMF Artifact Templates

Mission Mapping to FRCS

ESCTP FRCS RMF Tool

Step 3
Implement Controls

CCI Test Results Form



RMF Step 1 Determine the Information Types and Overall Security Category

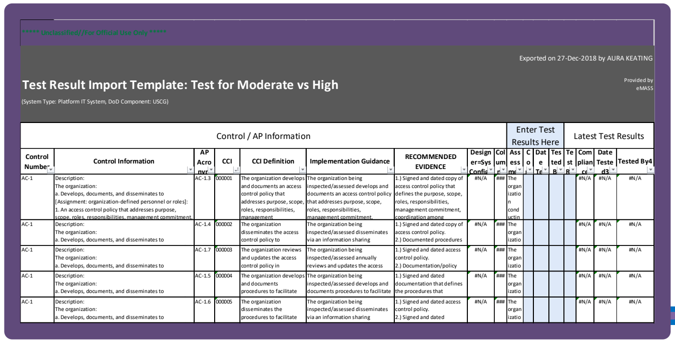
OVERALL SYSTEM SECURITY CATEGORY		High	High	High
	X			

Security Categorization Form

NIST 800-82
800-82 ICS
Overlay

DoD-level
Policies

UFC
4-010-06



***** Unclassified//For Official Use Only *****

Exported on 27-Dec-2018 by AURA KEATING

Provided by eMASS

Test Result Import Template: Test for Moderate vs High

(System Type: Platform IT System, DoD Component: USCG)

Control / AP Information										Enter Test Results Here				Latest Test Results		
Control Numbe	Control Information	AP Acro nyr	CCI	CCI Definition	Implementation Guidance	RECOMMENDED EVIDENCE	Design er=Sys Config	Col um n	Ass ess me	C o	Dat e Te	Tes ted B	Te st R	Com plian ce	Date Teste d3	Tested By4
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment,	AC-1.3	000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment,	1.) Signed and dated copy of access control policy that defines the purpose, scope, roles, responsibilities, management commitment, coordination among	#N/A	###	The organ izatio n cond uctin					#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.4	000002	The organization disseminates the access control policy to	The organization being inspected/assessed disseminates via an information sharing	1.) Signed and dated copy of access control policy. 2.) Documented procedures	#N/A	###	The organ izatio					#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.7	000003	The organization reviews and updates the access control policy in	The organization being inspected/assessed annually reviews and updates the access	1.) Signed and dated access control policy. 2.) Documentation/policy	#N/A	###	The organ izatio					#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.5	000004	The organization develops and documents procedures to facilitate	The organization being inspected/assessed develops and documents procedures to facilitate	1.) Signed and dated documentation that defines the procedures that	#N/A	###	The organ izatio					#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.6	000005	The organization disseminates the procedures to facilitate	The organization being inspected/assessed disseminates via an information sharing	1.) Signed and dated access control policy. 2.) Signed and dated	#N/A	###	The organ izatio					#N/A	#N/A	#N/A

eMASS Import of Test Results

Test Result Export Form

- eMASS format
- Autofill of CCI Test Results to apply ICS Overlay
- Autofill of CCI Test Results for DoD-level policies
- Autofill of CCI Test Results with UFC 4-010-06 supplemental controls to ICS Overlay
- Auto-color to identify remaining User input fields
- Excel formula provided to pull tool data into eMASS template for import

Unit 7

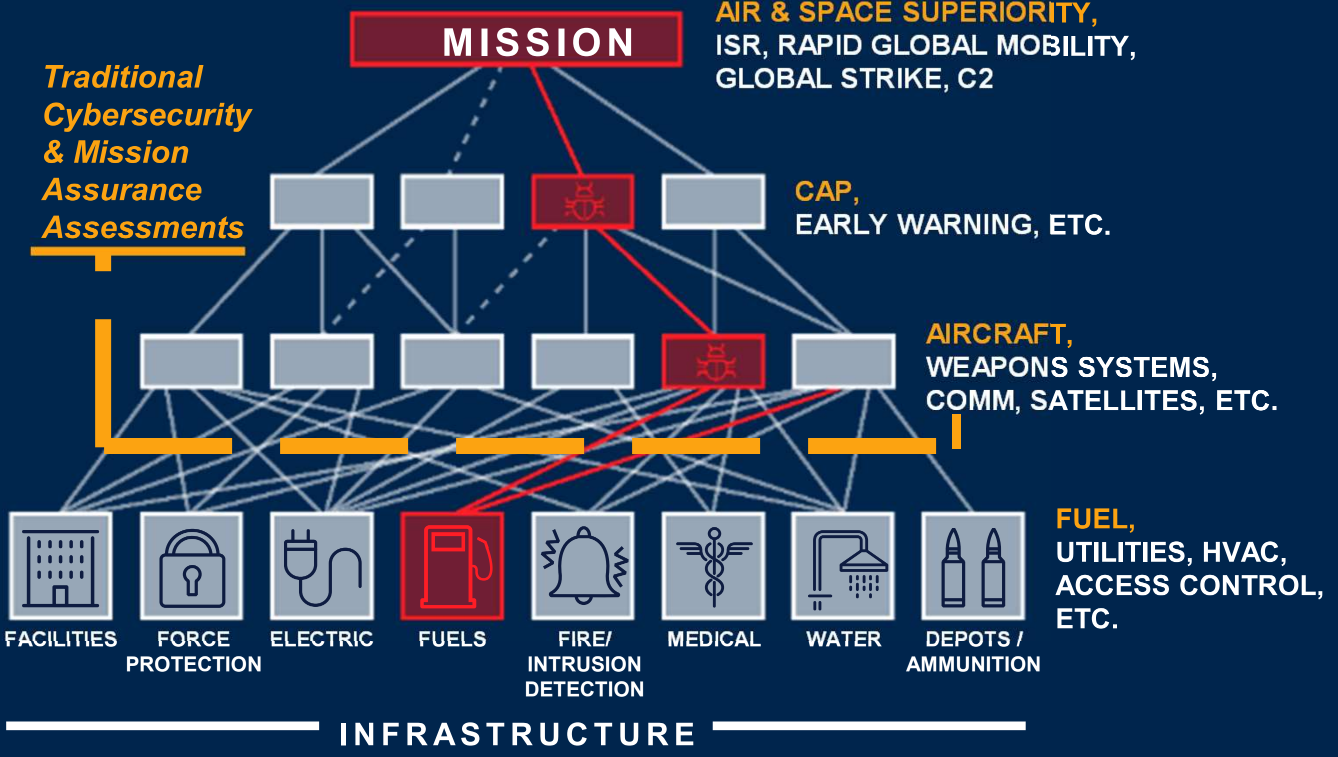
Joint Mission Assurance Vulnerability Benchmarks; Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures; Incident Reporting; Wrap Up Q&A

Infrastructure Vulnerabilities Disrupt Missions

INFRASTRUCTURE VULNERABILITIES DISRUPT MISSIONS

NOTIONAL MISSION THREAD CRITICAL PATH

An adversary could disrupt, degrade, or deny a mission by targeting the foundational assets that underpin the system of systems



Traditional Cybersecurity & Mission Assurance Assessments

AIR & SPACE SUPERIORITY, ISR, RAPID GLOBAL MOBILITY, GLOBAL STRIKE, C2

CAP, EARLY WARNING, ETC.

AIRCRAFT, WEAPONS SYSTEMS, COMM, SATELLITES, ETC.

FUEL, UTILITIES, HVAC, ACCESS CONTROL, ETC.

Who to Best Defend Control Systems: IT or OT SMEs?

DoD Mission Assurance Assessment Benchmarks

2015
DoD Mission Assurance
Assessment Benchmarks

THOMAS A. BUSSIERE
Major General, USAF
Deputy Director for Nuclear, Homeland
Defense, & Current Operations, J-33

DISTRIBUTION STATEMENT D: Distribution authorized to U.S. Government Agencies and their contractors. Administrative/Operational Use 19 Nov 2015. Other requests for this document shall be referred to the Defense Threat Reduction Agency, 8725 John J. Kingman Road, MSC 6201, Fort Belvoir, VA 22060-6201.

This document contains FOUO information exempt from mandatory disclosure under the FOIA. Exemption (b)(2) high applies.

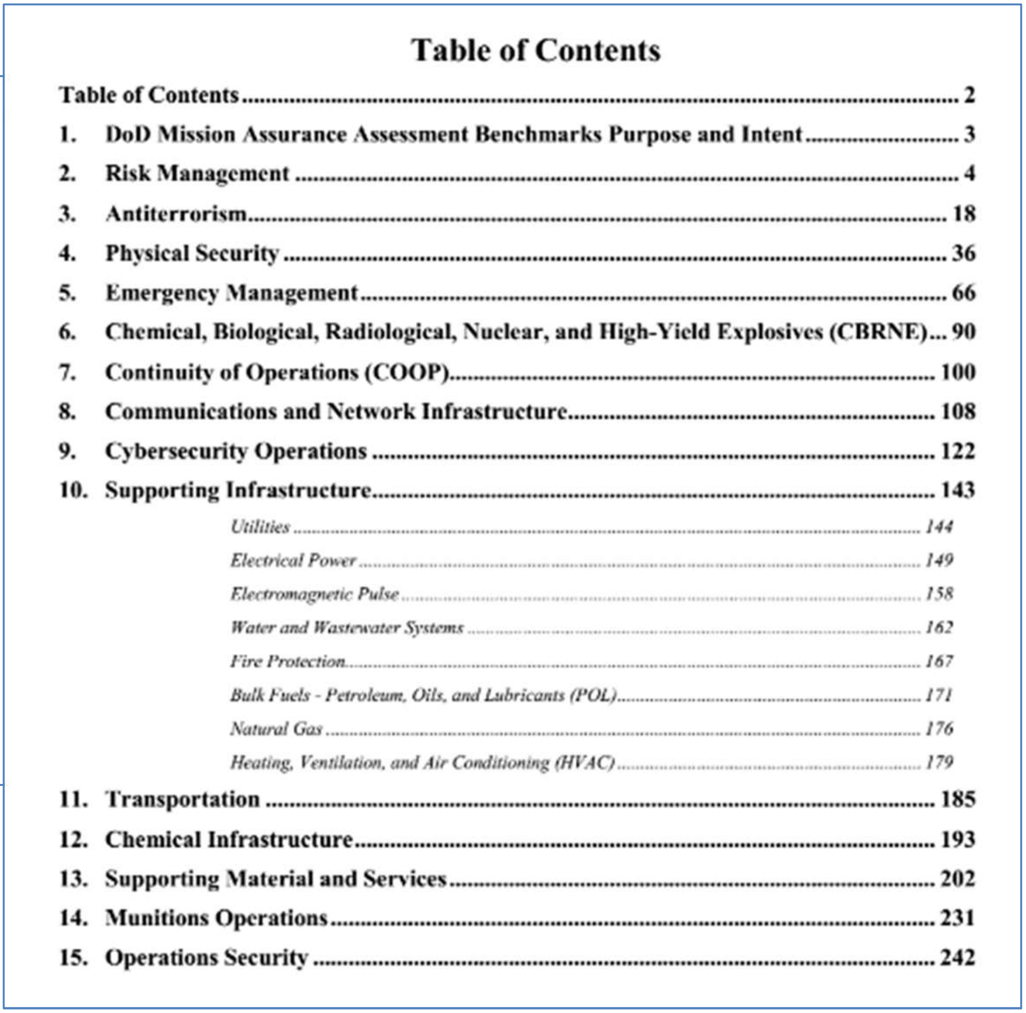
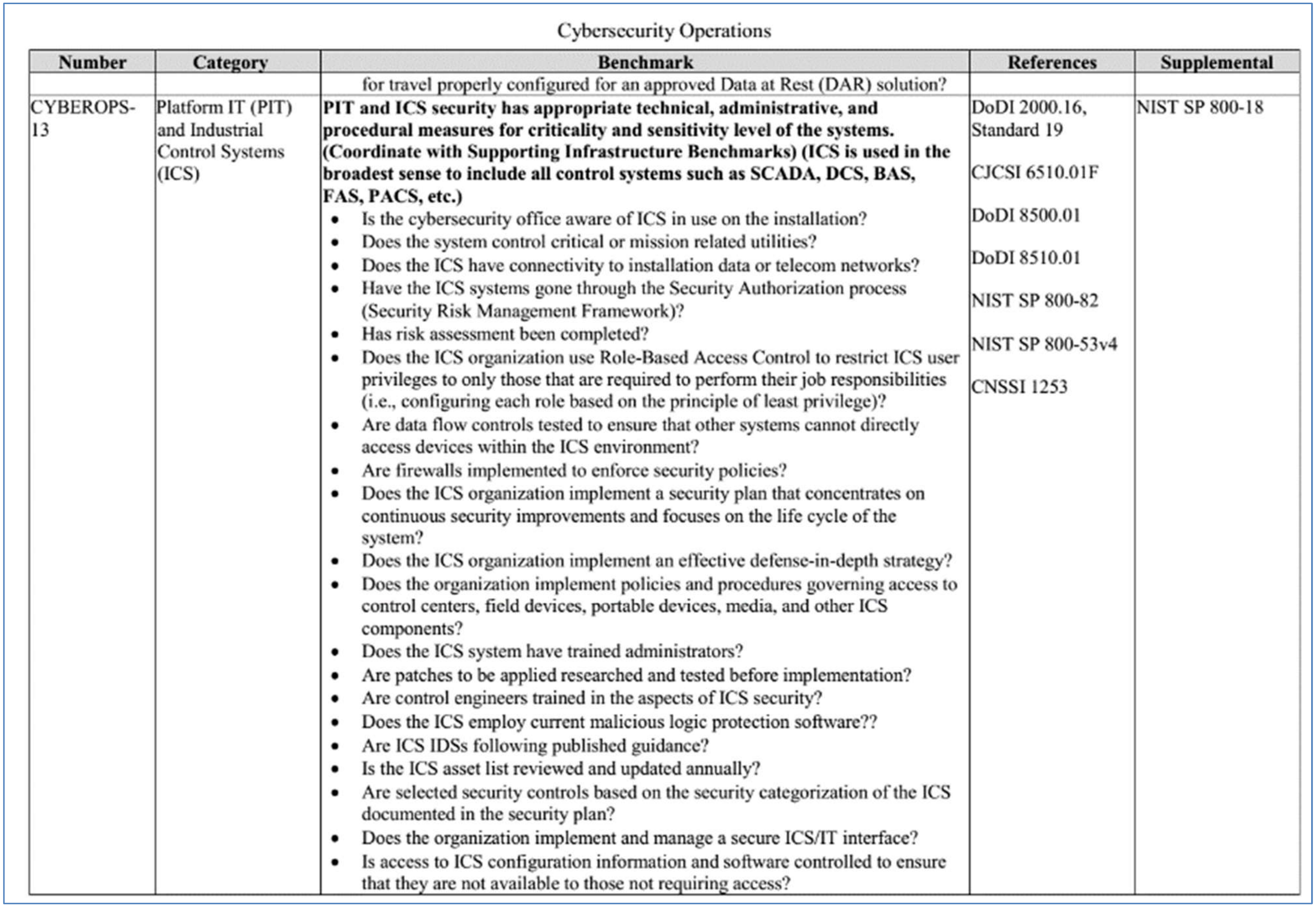


Table of Contents

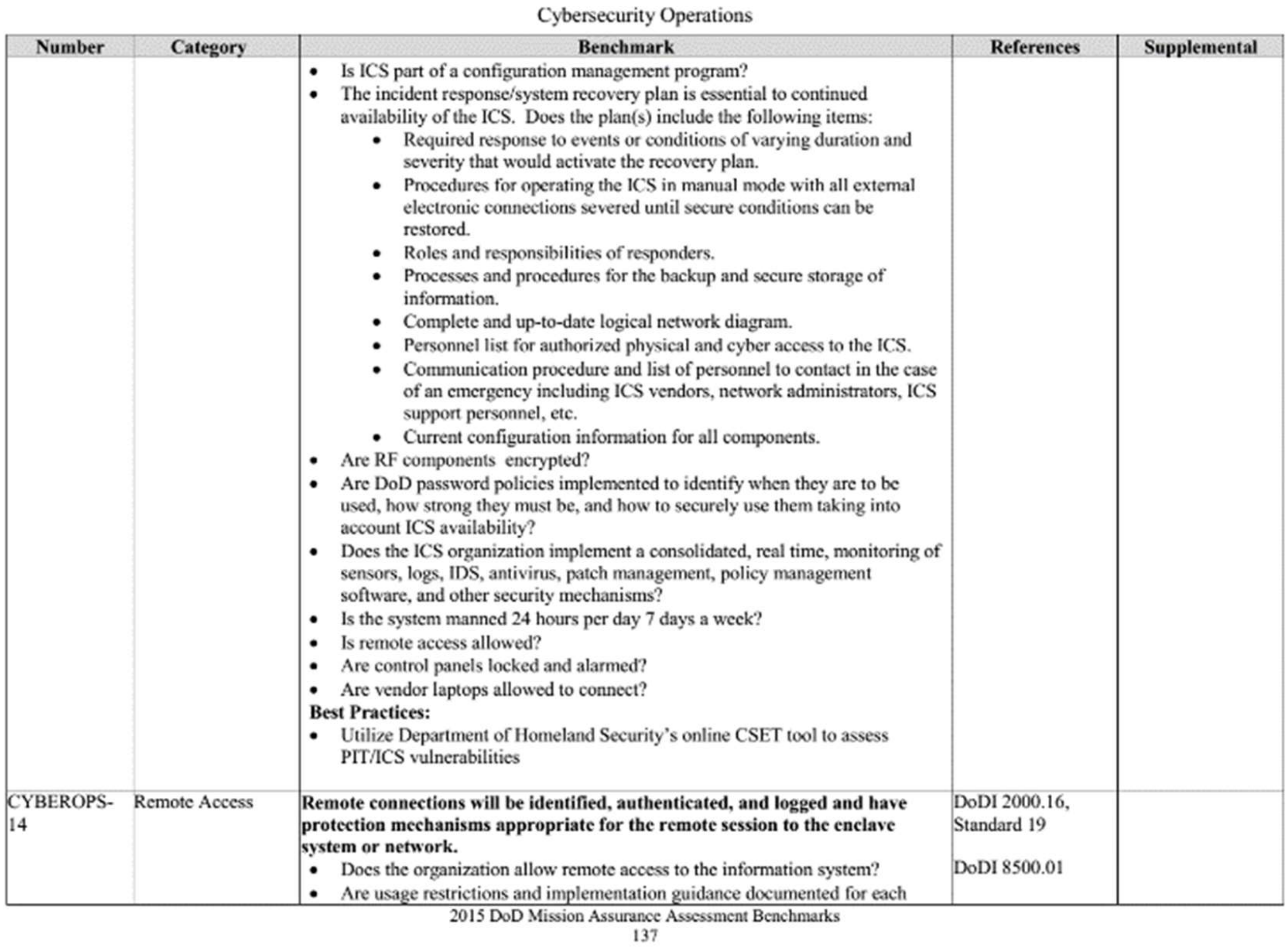
DoD Mission Assurance Assessment Benchmarks



Cybersecurity Operations

Number	Category	Benchmark	References	Supplemental
		for travel properly configured for an approved Data at Rest (DAR) solution?		
CYBEROPS-13	Platform IT (PIT) and Industrial Control Systems (ICS)	**PIT and ICS security has appropriate technical, administrative, and procedural measures for criticality and sensitivity level of the systems. (Coordinate with Supporting Infrastructure Benchmarks) (ICS is used in the broadest sense to include all control systems such as SCADA, DCS, BAS, FAS, PACS, etc.)** • Is the cybersecurity office aware of ICS in use on the installation? • Does the system control critical or mission related utilities? • Does the ICS have connectivity to installation data or telecom networks? • Have the ICS systems gone through the Security Authorization process (Security Risk Management Framework)? • Has risk assessment been completed? • Does the ICS organization use Role-Based Access Control to restrict ICS user privileges to only those that are required to perform their job responsibilities (i.e., configuring each role based on the principle of least privilege)? • Are data flow controls tested to ensure that other systems cannot directly access devices within the ICS environment? • Are firewalls implemented to enforce security policies? • Does the ICS organization implement a security plan that concentrates on continuous security improvements and focuses on the life cycle of the system? • Does the ICS organization implement an effective defense-in-depth strategy? • Does the organization implement policies and procedures governing access to control centers, field devices, portable devices, media, and other ICS components? • Does the ICS system have trained administrators? • Are patches to be applied researched and tested before implementation? • Are control engineers trained in the aspects of ICS security? • Does the ICS employ current malicious logic protection software?? • Are ICS IDSs following published guidance? • Is the ICS asset list reviewed and updated annually? • Are selected security controls based on the security categorization of the ICS documented in the security plan? • Does the organization implement and manage a secure ICS/IT interface? • Is access to ICS configuration information and software controlled to ensure that they are not available to those not requiring access?	DoDI 2000.16, Standard 19 CJCSI 6510.01F DoDI 8500.01 DoDI 8510.01 NIST SP 800-82 NIST SP 800-53v4 CNSSI 1253	NIST SP 800-18

DoD Mission Assurance Assessment Benchmarks

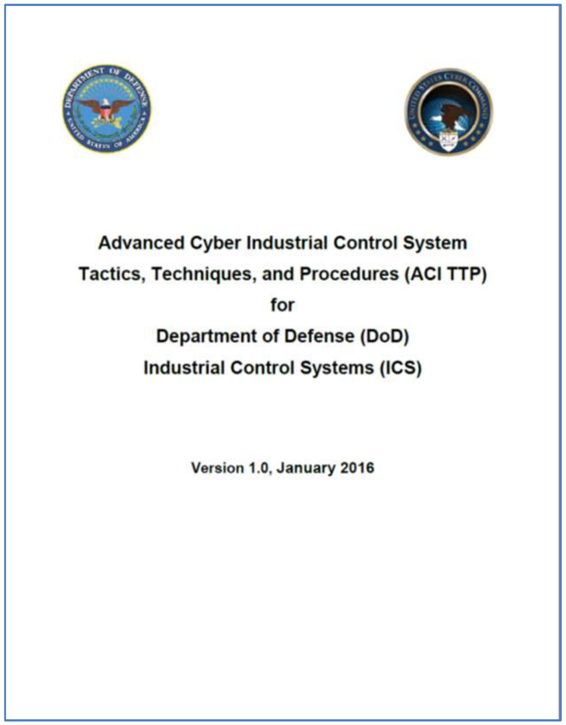


Cybersecurity Operations

Number	Category	Benchmark	References	Supplemental
		• Is ICS part of a configuration management program? • The incident response/system recovery plan is essential to continued availability of the ICS. Does the plan(s) include the following items: • Required response to events or conditions of varying duration and severity that would activate the recovery plan. • Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored. • Roles and responsibilities of responders. • Processes and procedures for the backup and secure storage of information. • Complete and up-to-date logical network diagram. • Personnel list for authorized physical and cyber access to the ICS. • Communication procedure and list of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc. • Current configuration information for all components. • Are RF components encrypted? • Are DoD password policies implemented to identify when they are to be used, how strong they must be, and how to securely use them taking into account ICS availability? • Does the ICS organization implement a consolidated, real time, monitoring of sensors, logs, IDS, antivirus, patch management, policy management software, and other security mechanisms? • Is the system manned 24 hours per day 7 days a week? • Is remote access allowed? • Are control panels locked and alarmed? • Are vendor laptops allowed to connect? **Best Practices:** • Utilize Department of Homeland Security's online CSET tool to assess PIT/ICS vulnerabilities		
CYBEROPS-14	Remote Access	**Remote connections will be identified, authenticated, and logged and have protection mechanisms appropriate for the remote session to the enclave system or network.** • Does the organization allow remote access to the information system? • Are usage restrictions and implementation guidance documented for each	DoDI 2000.16, Standard 19 DoDI 8500.01	

ACT TTP for DoD ICS

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include **supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS),** and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. **ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation.**



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

3. How to Use These TTP

This ACI TTP is divided into essentially 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)

TTP ‘s Apply to IT and OT

The Tactics, Techniques and Procedures can be used by any organization and apply to:

Information Technology (IT) Systems – Business and Home
Operational Technologies (OT) Systems – Any Kind (Utility, Building, Environmental, Medical, Logistics, Transportation, Weapons, etc.)

The tools that will be used are almost all open source and free to use (premium or business versions are modestly priced)

At the conclusion of the workshop, you will appreciate your IT and OT networks in a new way and have situational awareness of normal versus abnormal behavior, know what actions to take, what contract language to add to SOW’s, and how to protect sensitive information as the Internet of Things and the convergence of IT and OT continues to evolve.

For the foreseeable future, the trend to co-mingle IT and OT data on non-segmented networks is likely to be the norm; DON’T BE A TREND FOLLOWER, DON’T DO IT!

- ***Segment and VLAN IT and OT networks; DMZ’s with gateways and/or firewalls***
- ***Separate the OS and OT data (C: OS and D: OT data), enable BitLocker on OT drive***

ACT TTP Concepts

ACI TTP Concepts. The concepts provide background information to assist in explaining the scope, prerequisites, applicability, and limitations of the components of this TTP. The concept chapters should be read prior to responding to indication of malicious cyber activity.

In the 1990s, in order to leverage newly identified efficiencies in ICS, formerly physically isolated ICS networks were adapted to interface with the Internet. In the early 2000s, active cyber threats were still in their infancy. However, today the cyber threat to ICS has grown from an obscure annoyance to one of the most significant threats to national security (Rogers, 2015).

The threat, coupled with the inherent lack of cyber security and a long-life span for ICS equipment, has created ideal conditions for a cyber attack causing physical and tangible repercussions. This has led to a need for tactics, techniques, and procedures (TTP) relative to the operations of traditional ICS equipment as well as information technology (IT) components.

Threat-Response Procedures

b. Threat-Response Procedures (Detection, Mitigation, and Recovery).

Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general each section is designed for execution by the individuals responsible for the operations of the equipment, regardless of formal designations. **Successful Detection of cyber anomalies is best achieved when IT and ICS managers remain in close coordination.** The *Integrity Checks Table* (enclosure A, section A.3, table A.3.1) lists the procedures to use when identifying malicious cyber activity.

Baselining and Routine Monitoring

Baselining and Routine Monitoring of the Network.

Before the ACI TTP are adopted, ICS and IT managers should establish what a FMC network is as it pertains to their specific installations and missions. The ACI TTP defines FMC as a functional recovery point for both the ICS and the SCADA. Once this is defined, ICS and IT managers should capture the FMC condition of their network entry points (e.g., firewalls, routers, remote access terminals, wireless access points, etc.), network topology, network data flow, and machine/device configurations, then store these in a secure location**. This information should be kept under configuration management and updated every time changes are made to the network.** This information forms the FMC baseline**. The FMC baseline is used to determine normal operational conditions versus anomalous conditions of the ICS.**

Reference Materials

Reference Materials.

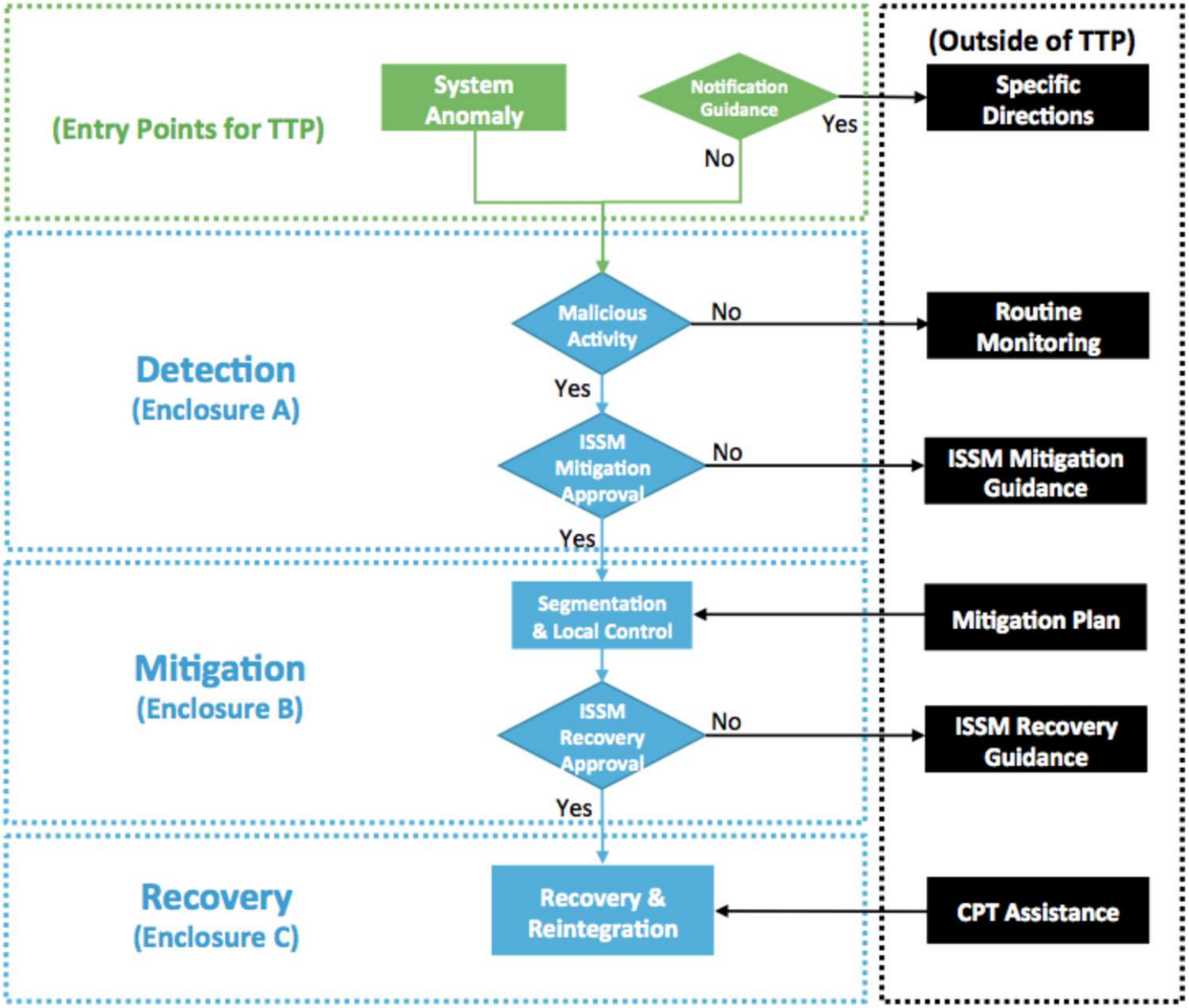
To further enhance the ACI TTP as a tool**, operators are encouraged to refer to additional resources provided by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Computer Security series** (see Appendix D: References).

Detection, Mitigation, Recovery Overview

Navigating Detection, Mitigation, and Recovery Procedures

Detection, Mitigation, and Recovery Procedures are contained within enclosures A through C. **While Detection Procedures lead to Mitigation Procedures, and Mitigation Procedures lead to Recovery Procedures, each enclosure can also be executed as a stand-alone resource as well as be incorporated into local procedures.** The following is an overview for navigating the Detection, Mitigation, and Recovery portions of the TTP.

Detection, Mitigation, Recovery Overview



E.2. FMC Baseline Overview

E.2. FMC Baseline Overview

a. Before the ACI TTP can be executed, operators should have several system characteristics documented. This documentation forms the system's current FMC baseline. Documenting the FMC baseline does not imply the system may not already have an adversary present. In fact, many systems might have an adversary present. If an adversary is present, and that adversary is lying in wait, if the adversary moves laterally or attempts to communicate or otherwise initiate an exploit (and eventually the adversary will), the ACI TTP is designed to Detect that type of movement by comparing system characteristics to its baseline.

b. This section provides specific details for developing the FMC baseline of an ICS. **The FMC Baseline establishes normal ICS behavior.** During Routine Monitoring and the Detection Phase of the ACI TTP, normal behaviors are compared to observed behaviors. If observed behaviors deviate from normal behaviors, these are either by design (approved and intentional) or anomalous (unapproved, unintentional, not communicated, or nefarious).

E.3. FMC Baseline Procedures

E.3. FMC Baseline Procedures

The procedures for establishing an FMC Baseline involve the following:

(1) Produce ICS Topology Diagram

(2) Document network traffic entering and exiting the ICS in *Enclave Entry Point Char*t on page E-4

(3) Document server/workstation user accounts; normal tasks and processes; connecting devices with ports, protocols, and services

(4) Document normal network traffic

Tools: Belarc, Glasswire, GrassMarlin, CSET

E.4. FMC Baseline Instructions

E.4. FMC Baseline Instructions

The ICS Topology Diagram describes which devices are located at which locations and how they connect. Generating an ICS Topology Diagram is accomplished using automated tools specifically designed for ICS in conjunction with manual “walk through” or simply using a manual “walk through” and inventory information or schematics if automated tools are not available.

a. Capture Assets

If you are using a network scanner, such as NMap (using SCADA script) or Nessus (with SCADA Plugin) or another tool that can provide an enumeration of live hosts on SCADA, scan your network to identify live assets.

(1) Most scanning tools do not capture the location of devices that are not active. These devices are located when validating the active device list.

(2) If a scanning tool is not available, use existing ICS documentation (inventory lists and schematics) to capture a list of assets deployed in the ICS.

E.4. FMC Baseline Instructions (cont)

b. Validate Active Hosts

(1) Validate active hosts and locate inactive assets by walking through the ICS installation, documenting the assets located and how they are connected.

a. Create an ICS Topology Diagram, which includes the assets you located, the connections, IP addresses, and location of the asset using the tools made available by your command. Figure E-1 shows an example of an ICS Topology Diagram.

b. Store the ICS Topology Diagram in the binder entitled FMC Baseline Documents.

c. **NOTE:** For your site, ensure your diagram includes IP addresses, make and model of device, and operating system

E.5. FMC Baseline Creation: Enclave

E.5. FMC Baseline Creation: ICS Enclave Entry Points

What you will need:

1. ICS Topology.
2. *FMC Baseline Documents* binder
3. Vendor documentation or Help web pages for devices being listed in the table.

a. From the next page, extract Table E-1: ICS Enclave Entry Points (make as many copies as needed). Insert this table (and copies) into FMC Baseline Documents binder.

b. Use the ICS topology to identify all devices that provide entry to the ICS enclave from external networks. This can be a router or firewall connecting the command's enterprise, virtual private network (VPN) connections (possibly connecting to an engineering workstation), wireless connections, and any asset vendors use to connect from corporate locations to the ICS.

Almost every FRCS has vendor support and the SLA requires the vendor to have access to the FRCS, vast majority use http

- **Allow remote access only during specified maintenance windows; RDP, VPN or https**

F.1. Jump-Kit Introduction

F.1. Jump-Kit Introduction

a. Description. A Recovery Jump-Kit contains the tools the ICS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery. Knowing what the Recovery point should be is the key to ensuring all known remnants of an attack have been removed from all components of the ICS. This means all hardware and software are configured in accordance with operational requirements, and checksums and hashes are in conformance with vendor specifications.

b. Key Components

(1) Routine Monitoring
(2) Inspection
(3) Identification of adversarial presence
(4) Documentation
(5) Notifications

c. Prerequisites. FMC baseline

F.2. Jump-Kit Contents

F.2. Jump-Kit Contents

a. Overview

(1) The Jump-Kit is a critical tool for the Recovery phase. In addition to **containing the operating software for all devices, it also contains the software hashes of the devices on the network and the firmware and software updates for all system devices.**

(2) During Recovery, **the Jump-Kit will be utilized to reimage the firmware/software operating on the affected device.** Care shall be used when the Jump-Kit machine is used for the reinstallation/reimaging potentially infected devices. The malware residing on the device, which is being reimaged, could manifest itself onto the Jump-Kit machine, which could then re-infect other system devices when reconnected.

F.2. Jump-Kit Contents

(3) Due to this potential back door access for malware, **ensure that the Jump-Kit machine is connected only to network devices that are completely isolated from the network.** Additionally, the Jump-Kit should be write-protected and/or operating in a virtual environment. Virus scans are performed after connection to each device.

(4) **The ICS Jump-Kit and the IT Jump-Kit can be combined or be separate** depending on the environment and system architecture. In general, a Recovery Jump-Kit should include the following:

Jump-Kit Contents: Documentation

- Incident Notifications List: document contact information for command's Information Assurance Manager
- Document stakeholders who could be affected by a Cyber attack on ICS
- Establish notification procedures with chain of command

F.2. Jump-Kit Contents: Tools

Jump-Kit Contents: Tools

- Universal serial bus (USB) drives, bootable USB (or LiveCD) with up-to-date antimalware, and other software tools that can read and/or write to file system (Example: Bart’s PE disk)

- Laptop with anti-malware utilities and Internet access (for downloads)

- Computer and network tool kit to add/remove components, hard drives, connectors, wire cables, etc.

- Hard disk duplicators with write-block capabilities to capture hard drive images

F.2. Jump-Kit Contents: Config Files

Jump-Kit Contents: Configuration Files

- Firewall access control lists
- Firewall hard disk image
- IDS rules
- IDS image
    - Back up of firewall, router, and switch IOS
- Backup of PLC configurations and firmware
- Backup RTU software, database, and configurations
- Back up of all other computer assets to include HMI, Historian, and Database
- Network map of all expected connections to the ICS

F.3. Jump-Kit Maintenance F.4. Rescue CD

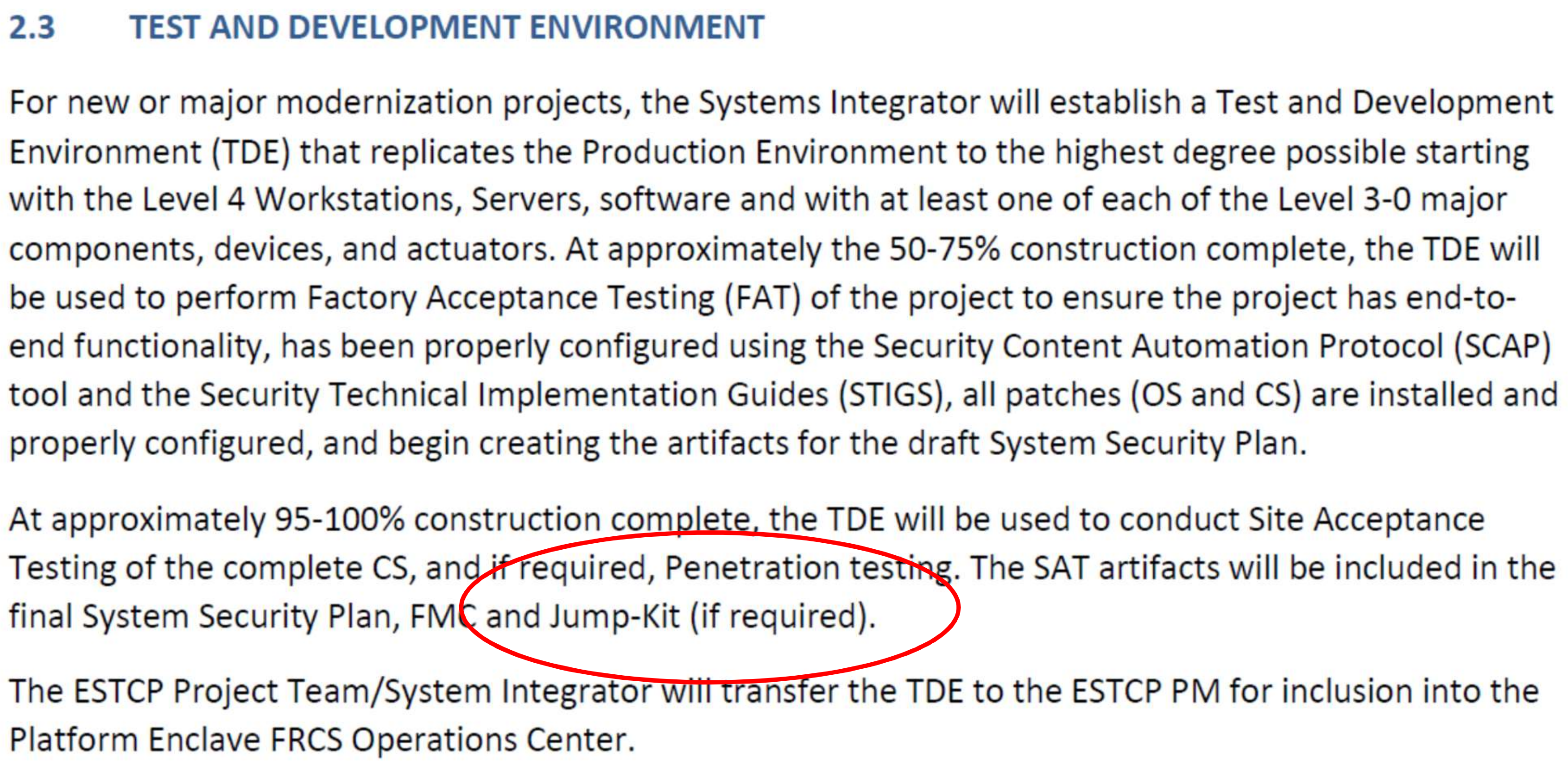
F.3. Jump-Kit Maintenance

The Jump-Kits must be maintained and be a part of configuration management. **When configuration files or new versions of operating systems or applications are updated, the Jump-Kits need to be updated as well.**

F.4. Jump-Kit Rescue CD

The Rescue CD is a bootable CD with tools, rootkit detection, master boot record check, and other capabilities

ESTCP Cybersecurity Guidance with the TTP’s



2.3 TEST AND DEVELOPMENT ENVIRONMENT

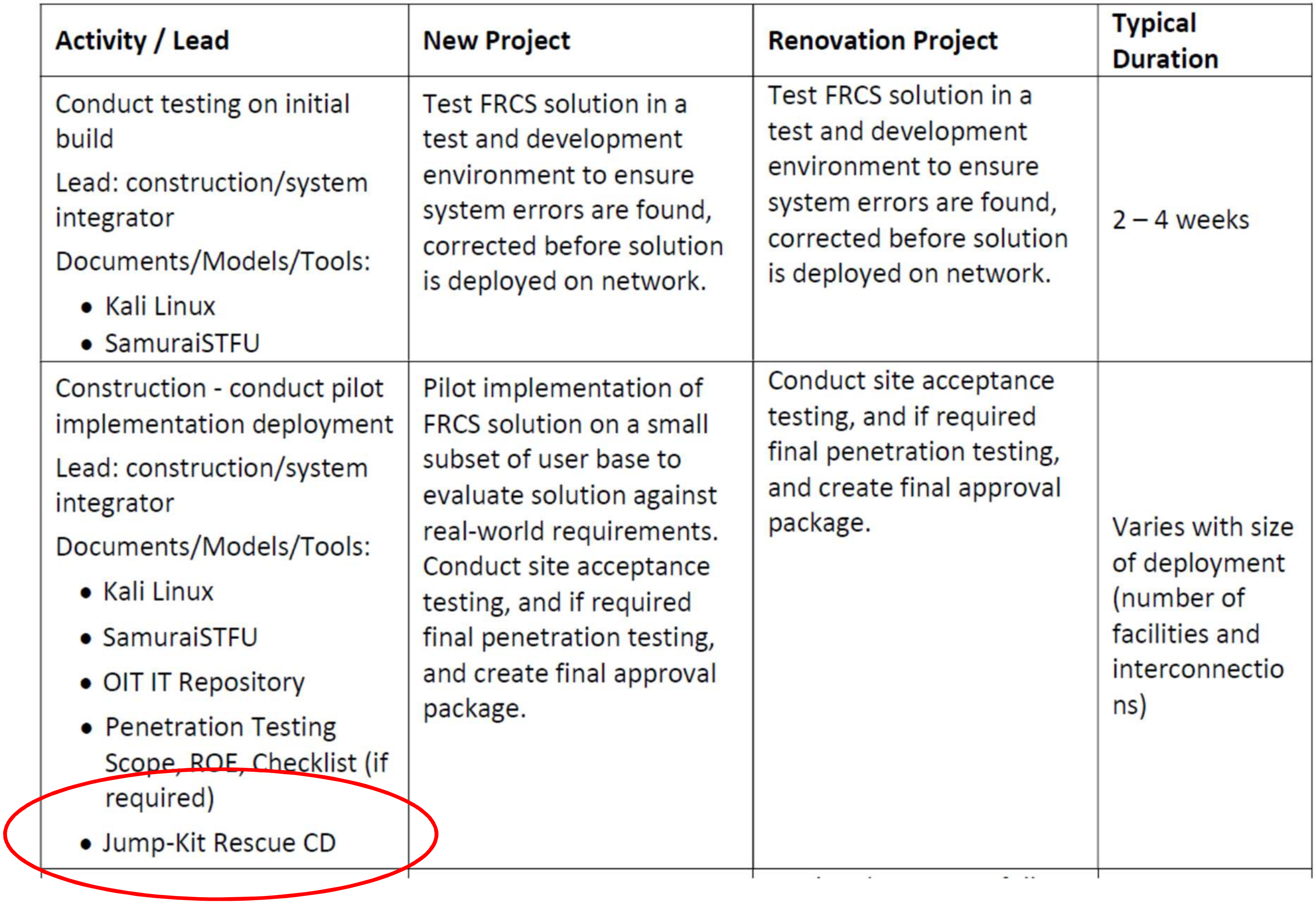
For new or major modernization projects, the Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators. At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and CS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).

The ESTCP Project Team/System Integrator will transfer the TDE to the ESTCP PM for inclusion into the Platform Enclave FRCS Operations Center.

TTP Jump-Kit Rescue CD

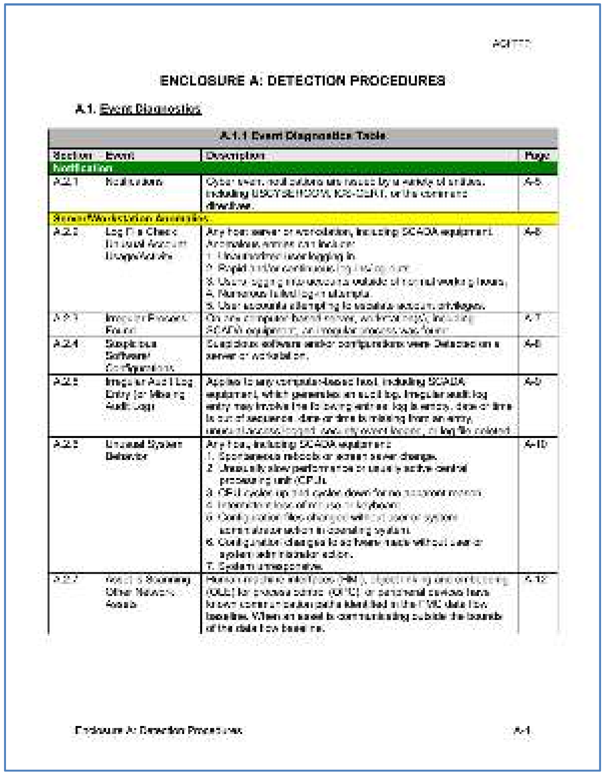
ESTCP Cybersecurity Guidance with the TTP’s



Activity / Lead	New Project	Renovation Project	Typical Duration
Conduct testing on initial build Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	2 – 4 weeks
Construction - conduct pilot implementation deployment Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU • OIT IT Repository • Penetration Testing Scope, ROE, Checklist (if required) • Jump-Kit Rescue CD	Pilot implementation of FRCS solution on a small subset of user base to evaluate solution against real-world requirements. Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Varies with size of deployment (number of facilities and interconnectio ns)

Design and Construction Sequence TTP Jump-Kit Rescue CD

ENCLOSURE A: DETECTION PROCEDURES



ACI TTP

ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostics Table

Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log [illegible] 3. Users logging into accounts outside of normal working hours. 4. Numerous failed login attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation, including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver changes. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset Is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

Enclosure A: Detection Procedures A-4

Notification

A.2.1 Notifications

Server/Workstation Anomalies

A.2. Event Diagnostic Procedures

A.2.2 Server/Workstation: Log File Check: Unusual Account Usage/Activity

A.2.3 Server/Workstation: Irregular Process Found

A.2.4 Server/Workstation: Suspicious Software/Configurations

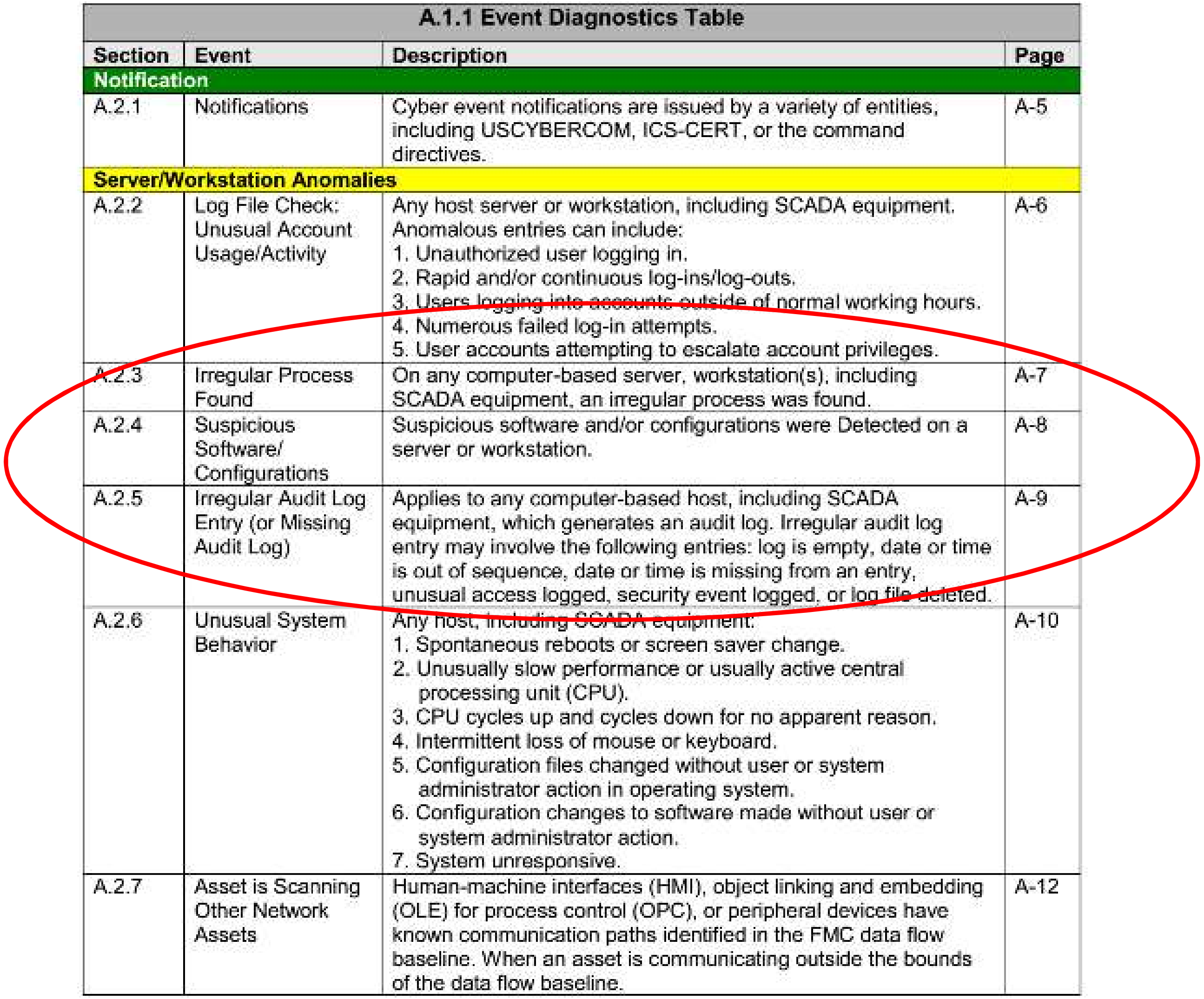
A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)

A.2.6 Server/Workstation: Unusual System Behavior

A.2.7 Server/Workstation: Asset Is Scanning Other Network Assets

A.2.8 Server/Workstation: Unexpected Behavior: HMI, OPC, and Control Server

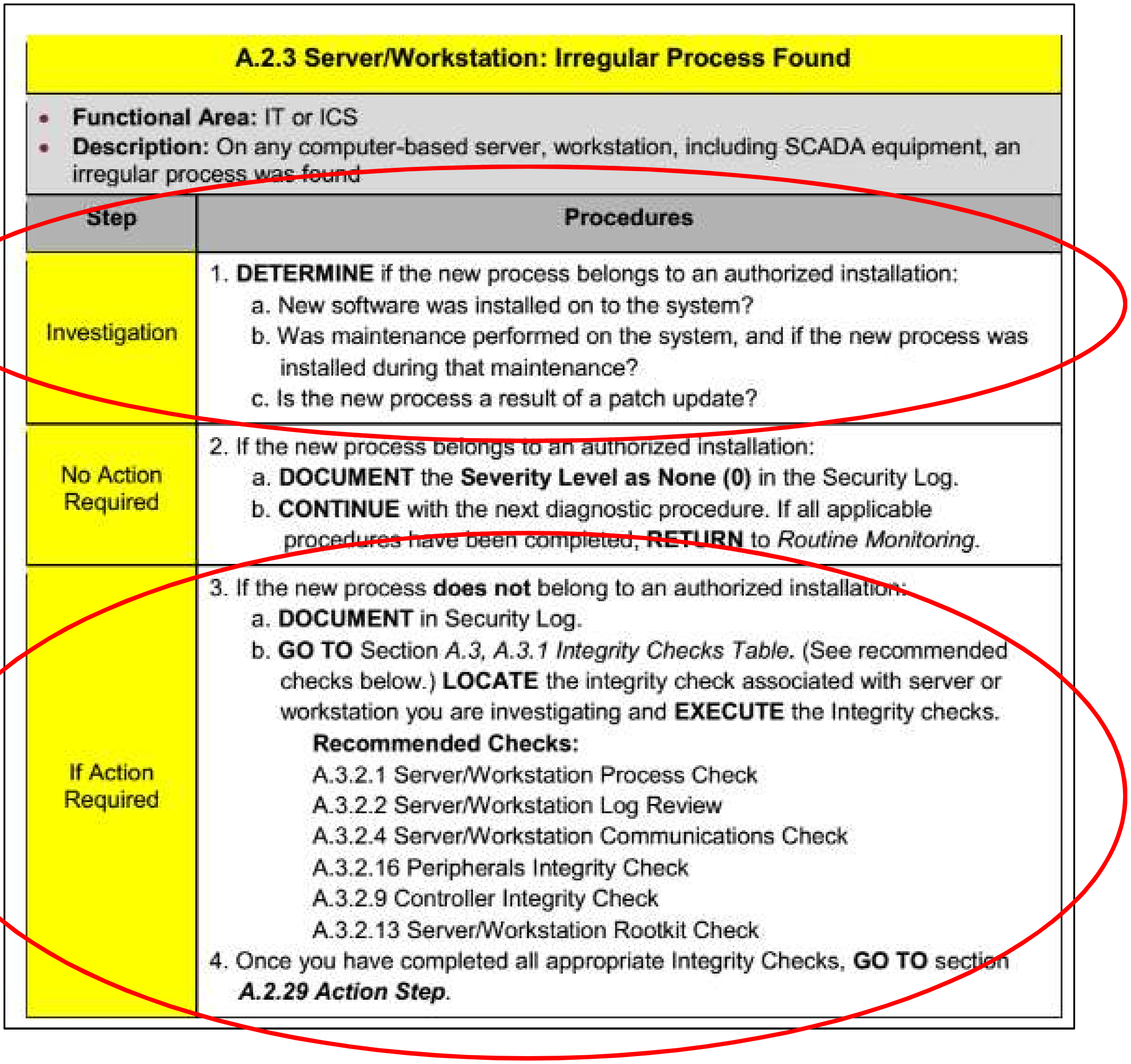
DETECTION PROCEDURES SERVER EXAMPLE 1



A.1.1 Event Diagnostics Table

Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log-ins/log-outs. 3. Users logging into accounts outside of normal working hours. 4. Numerous failed log-in attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver change. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

DETECTION PROCEDURES SERVER EXAMPLE 1

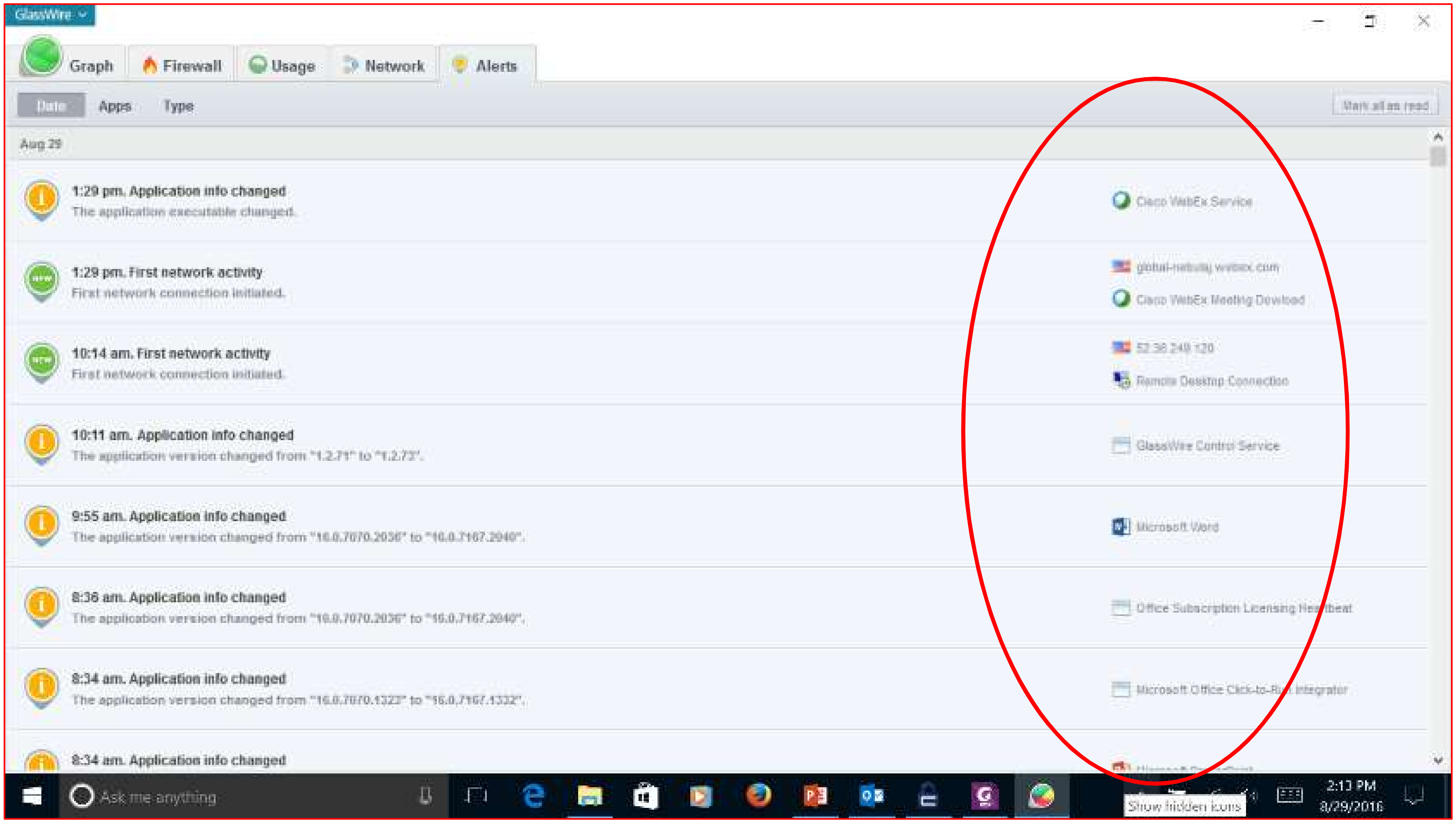


A.2.3 Server/Workstation: Irregular Process Found

- **Functional Area:** IT or ICS
- **Description:** On any computer-based server, workstation, including SCADA equipment, an irregular process was found

Step	Procedures
Investigation	1. **DETERMINE** if the new process belongs to an authorized installation: a. New software was installed on to the system? b. Was maintenance performed on the system, and if the new process was installed during that maintenance? c. Is the new process a result of a patch update?
No Action Required	2. If the new process belongs to an authorized installation: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the new process **does not** belong to an authorized installation: a. **DOCUMENT** in Security Log. b. **GO TO** Section *A.3, A.3.1 Integrity Checks Table*. (See recommended checks below.) **LOCATE** the integrity check associated with server or workstation you are investigating and **EXECUTE** the Integrity checks. **Recommended Checks:** A.3.2.1 Server/Workstation Process Check A.3.2.2 Server/Workstation Log Review A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

DETECTION PROCEDURES SERVER EXAMPLE 1



Aug 29

1:29 pm. Application info changed
The application executable changed.
Cisco WebEx Service

1:29 pm. First network activity
First network connection initiated.
global-nebulaj.webex.com
Cisco WebEx Meeting Dowload

10:14 am. First network activity
First network connection initiated.
52.36.249.120
Remote Desktop Connection

10:11 am. Application info changed
The application version changed from "1.2.71" to "1.2.73".
GlassWire Control Service

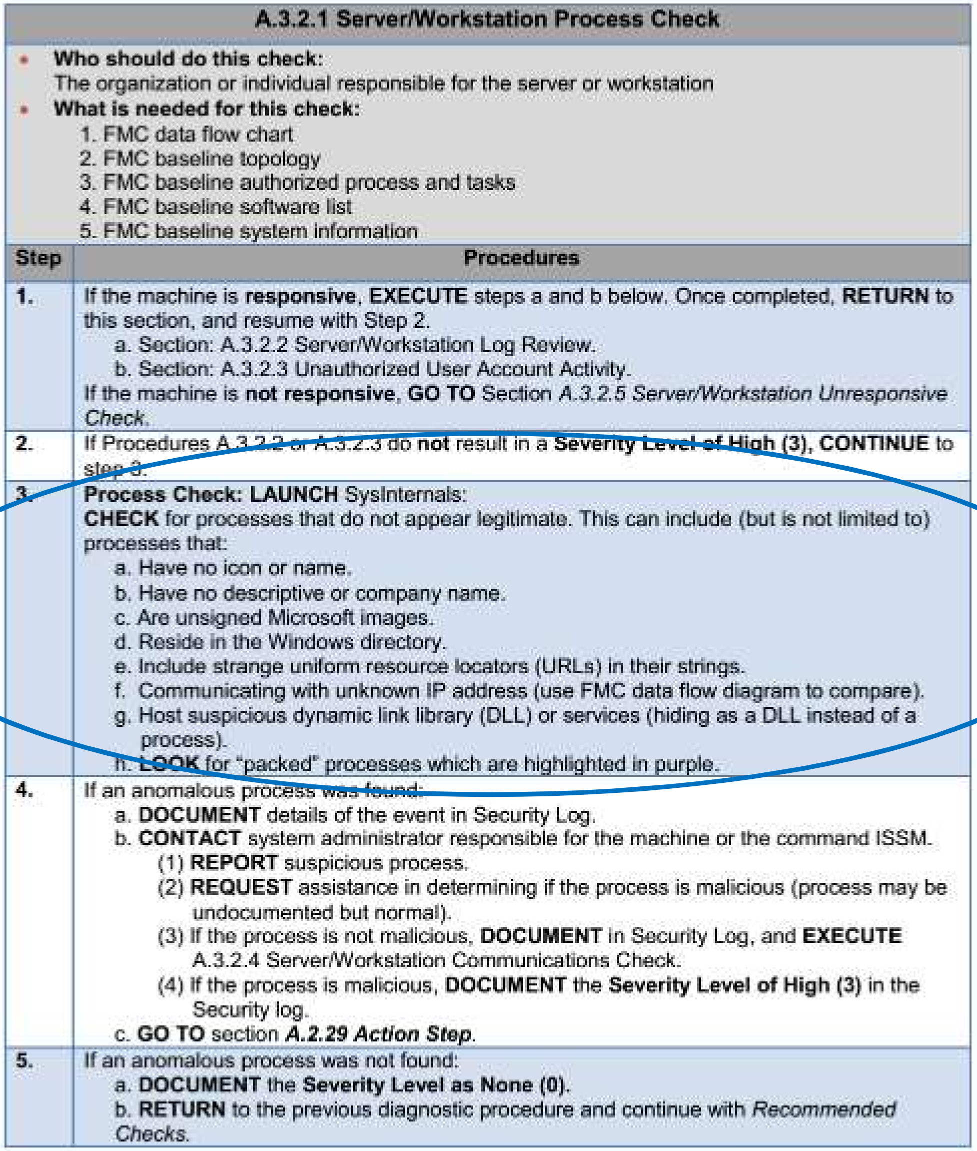
9:55 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Microsoft Word

8:36 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Office Subscription Licensing Heartbeat

8:34 am. Application info changed
The application version changed from "16.0.7070.1323" to "16.0.7167.1332".
Microsoft Office Click-to-Run Integrator

8:34 am. Application info changed

DETECTION PROCEDURES SERVER EXAMPLE 1

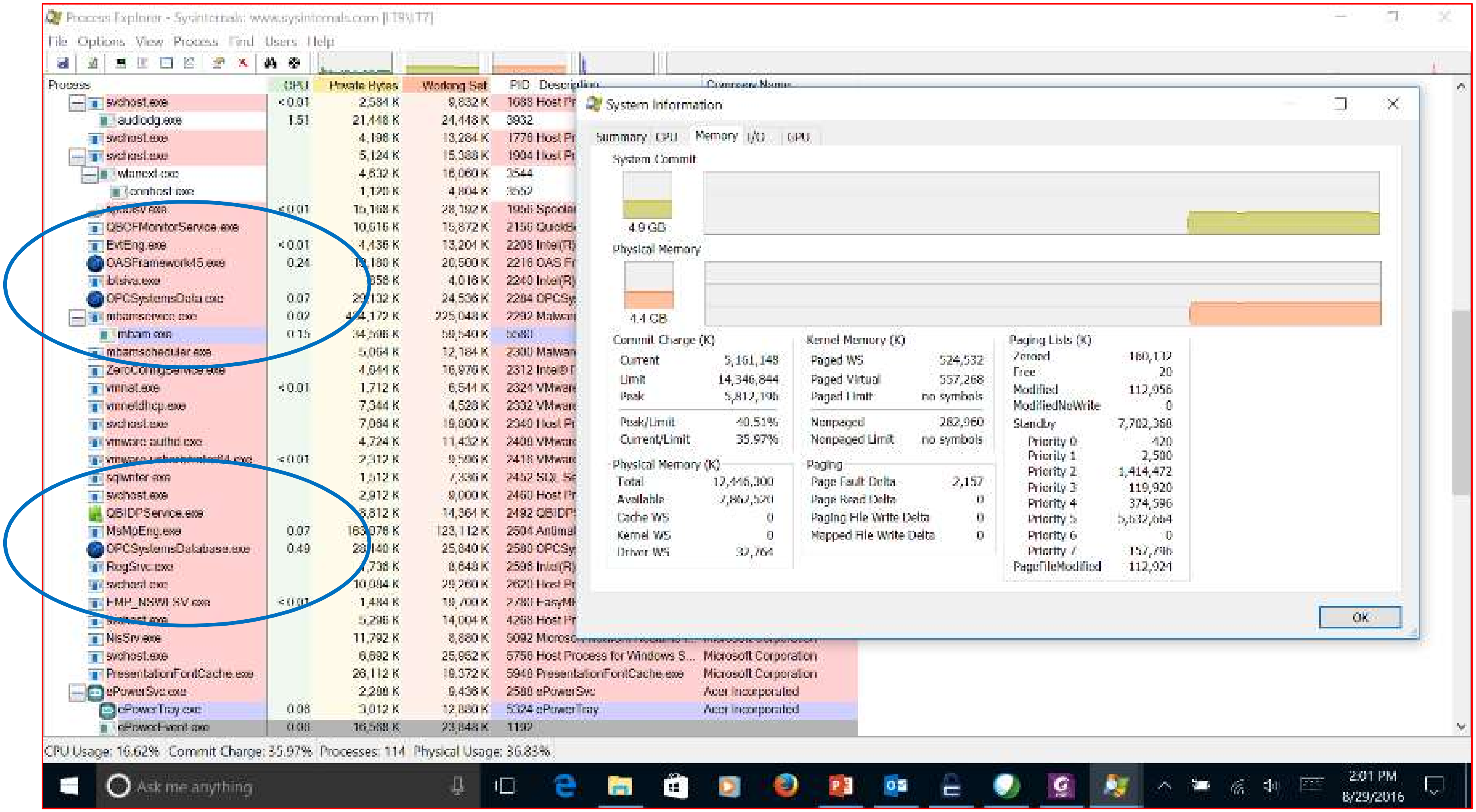


A.3.2.1 Server/Workstation Process Check

- **Who should do this check:**
  The organization or individual responsible for the server or workstation
- **What is needed for this check:**
  1. FMC data flow chart
  2. FMC baseline topology
  3. FMC baseline authorized process and tasks
  4. FMC baseline software list
  5. FMC baseline system information

Step	Procedures
1.	If the machine is **responsive**, **EXECUTE** steps a and b below. Once completed, **RETURN** to this section, and resume with Step 2. a. Section: A.3.2.2 Server/Workstation Log Review. b. Section: A.3.2.3 Unauthorized User Account Activity. If the machine is **not responsive**, **GO TO** Section *A.3.2.5 Server/Workstation Unresponsive Check*.
2.	If Procedures A.3.2.2 or A.3.2.3 do **not** result in a **Severity Level of High (3), CONTINUE** to step 3.
3.	**Process Check: LAUNCH** SysInternals: **CHECK** for processes that do not appear legitimate. This can include (but is not limited to) processes that: a. Have no icon or name. b. Have no descriptive or company name. c. Are unsigned Microsoft images. d. Reside in the Windows directory. e. Include strange uniform resource locators (URLs) in their strings. f. Communicating with unknown IP address (use FMC data flow diagram to compare). g. Host suspicious dynamic link library (DLL) or services (hiding as a DLL instead of a process). h. **LOOK** for "packed" processes which are highlighted in purple.
4.	If an anomalous process was found: a. **DOCUMENT** details of the event in Security Log. b. **CONTACT** system administrator responsible for the machine or the command ISSM. (1) **REPORT** suspicious process. (2) **REQUEST** assistance in determining if the process is malicious (process may be undocumented but normal). (3) If the process is not malicious, **DOCUMENT** in Security Log, and **EXECUTE** A.3.2.4 Server/Workstation Communications Check. (4) If the process is malicious, **DOCUMENT** the **Severity Level of High (3)** in the Security log. c. **GO TO** section ***A.2.29 Action Step***.
5.	If an anomalous process was not found: a. **DOCUMENT** the **Severity Level as None (0)**. b. **RETURN** to the previous diagnostic procedure and continue with *Recommended Checks*.

DETECTION PROCEDURES SERVER EXAMPLE 1

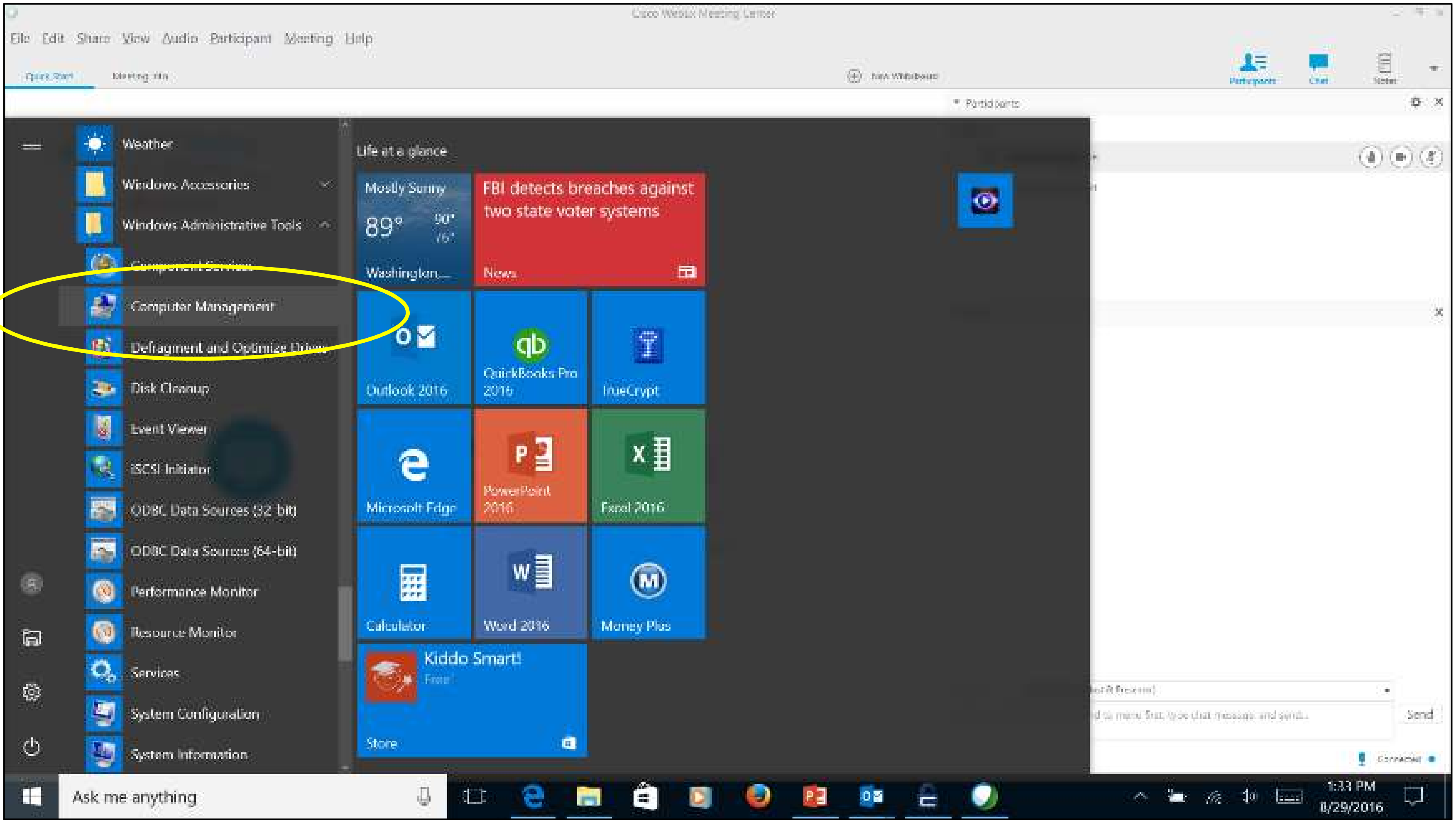


```
Process Explorer - Sysinternals: www.sysinternals.com [LTRV\T7]
File  Options  View  Process  Find  Users  Help

Process                       CPU    Private Bytes  Working Set  PID  Description
svchost.exe                   < 0.01     2,584 K       9,832 K   1088 Host Pr
  audiodg.exe                 1.51      21,448 K      24,448 K   3932
svchost.exe                              4,196 K      13,284 K   1776 Host Pr
svchost.exe                              5,124 K      15,388 K   1904 Host Pr
  wlanext.exe                            4,632 K      16,060 K   3544
    conhost.exe                          1,120 K       4,804 K   3552
spoolsv.exe                   < 0.01    15,168 K      28,192 K   1956 Spooler
QBCFMonitorService.exe                  10,616 K      15,872 K   2156 QuickB
EvtEng.exe                    < 0.01     4,436 K      13,204 K   2208 Intel(R)
OASFramework45.exe            0.24      19,180 K      20,500 K   2216 OAS Fr
Ibtsiva.exe                                658 K       4,016 K   2240 Intel(R)
OPCSystemsData.exe            0.07      29,132 K      24,536 K   2264 OPCSy
mbamservice.exe               0.02     424,172 K     225,048 K   2292 Malwar
  mbam.exe                    0.15      34,508 K      59,540 K   5680
mbamscheduler.exe                        5,064 K      12,184 K   2300 Malwar
ZeroConfigService.exe                    4,044 K      16,976 K   2312 Intel® P
vmnat.exe                     < 0.01     1,712 K       6,544 K   2324 VMware
vmnetdhcp.exe                            7,344 K       4,528 K   2332 VMware
svchost.exe                              7,084 K      19,800 K   2340 Host Pr
vmware-authd.exe                         4,724 K      11,432 K   2408 VMware
vmware-usbarbitrator64.exe    < 0.01     2,312 K       9,596 K   2416 VMware
sqlwriter.exe                            1,512 K       7,336 K   2452 SQL Se
svchost.exe                              2,912 K       9,000 K   2460 Host Pr
QBIDPService.exe                         8,812 K      14,364 K   2492 QBIDP
MsMpEng.exe                   0.07     163,076 K     123,112 K   2504 Antimal
OPCSystemsDatabase.exe        0.49      28,140 K      25,840 K   2580 OPCSy
RegSrvc.exe                              1,738 K       8,648 K   2598 Intel(R)
svchost.exe                             10,084 K      29,260 K   2620 Host Pr
HMP_NSWLSV.exe                < 0.01     1,484 K      19,700 K   2780 EasyMI
svchost.exe                              5,296 K      14,004 K   4268 Host Pr
NisSrv.exe                              11,792 K       8,880 K   5092 Microso...                        Microsoft Corporation
svchost.exe                              6,692 K      25,952 K   5756 Host Process for Windows S...       Microsoft Corporation
PresentationFontCache.exe               28,112 K      19,372 K   5948 PresentationFontCache.exe       Microsoft Corporation
ePowerSvc.exe                            2,288 K       9,436 K   2588 ePowerSvc                       Acer Incorporated
  ePowerTray.exe              0.08       3,012 K      12,880 K   5324 ePowerTray                      Acer Incorporated
  ePowerEvent.exe             0.08      16,588 K      23,848 K   1192

CPU Usage: 16.62%  Commit Charge: 35.97%  Processes: 114  Physical Usage: 36.83%
```

```
System Information
Summary  CPU  Memory  I/O  GPU

System Commit
4.9 GB
Physical Memory
4.4 GB

Commit Charge (K)                 Kernel Memory (K)                   Paging Lists (K)
  Current        5,161,148          Paged WS              524,532       Zeroed            160,132
  Limit         14,346,844          Paged Virtual         557,268       Free                   20
  Peak           5,812,196          Paged Limit        no symbols       Modified          112,956
                                                                        ModifiedNoWrite         0
  Peak/Limit        40.51%          Nonpaged              282,960       Standby         7,702,368
  Current/Limit     35.97%          Nonpaged Limit     no symbols         Priority 0          420
                                                                          Priority 1        2,500
Physical Memory (K)               Paging                                  Priority 2    1,414,472
  Total         12,446,300          Page Fault Delta        2,157         Priority 3      119,920
  Available      7,867,520          Page Read Delta             0         Priority 4      374,596
  Cache WS               0          Paging File Write Delta     0         Priority 5    5,632,664
  Kernel WS              0          Mapped File Write Delta     0         Priority 6            0
  Driver WS         32,764                                                Priority 7      157,796
                                                                        PageFileModified  112,924
```

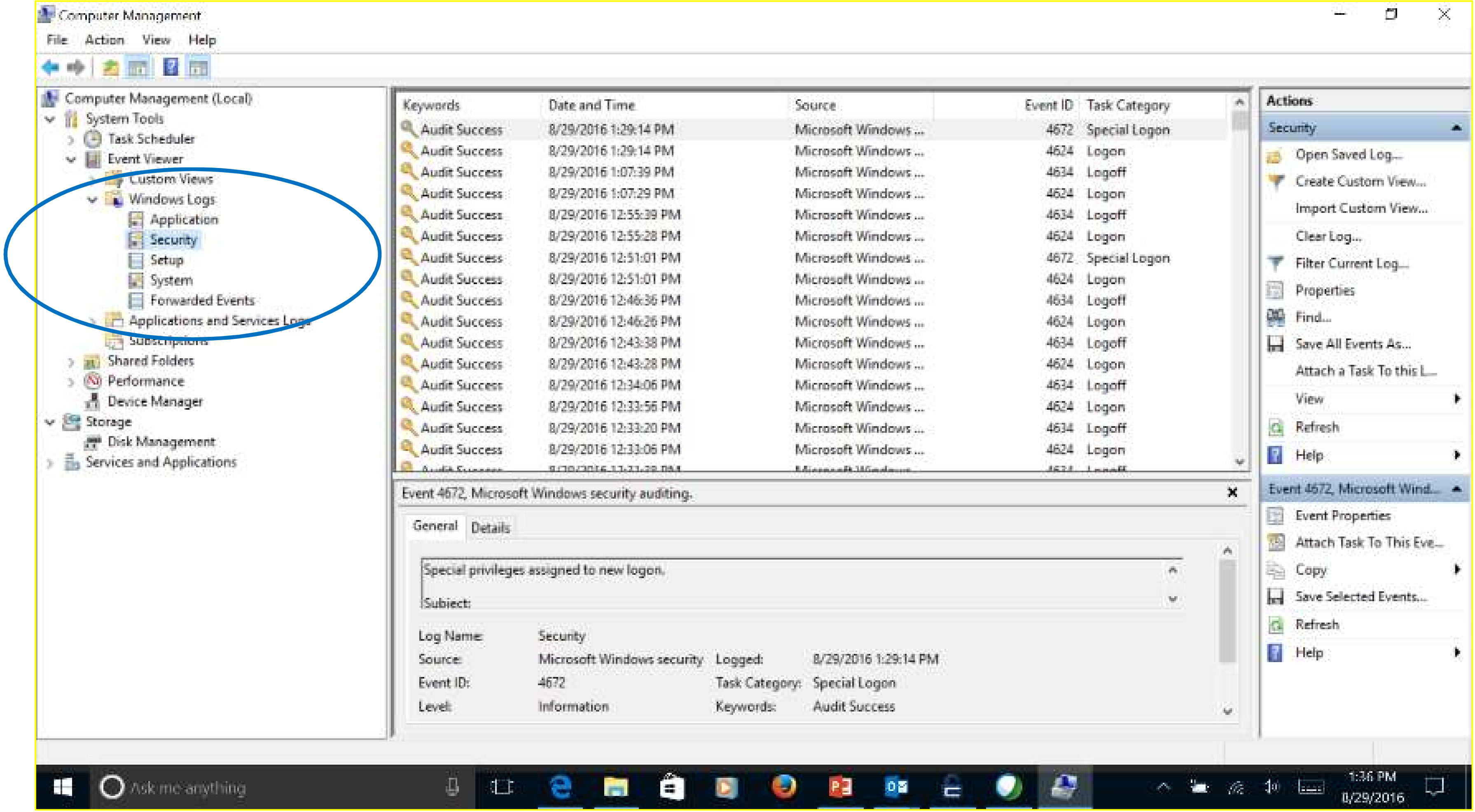
MS Process Explorer

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management

DETECTION PROCEDURES SERVER EXAMPLE 1



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 1:07:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 1:07:29 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:55:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:55:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:46:36 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:46:26 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:43:38 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:43:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:34:06 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:56 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:33:20 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:06 PM	Microsoft Windows ...	4624	Logon

Event 4672, Microsoft Windows security auditing.

General | Details

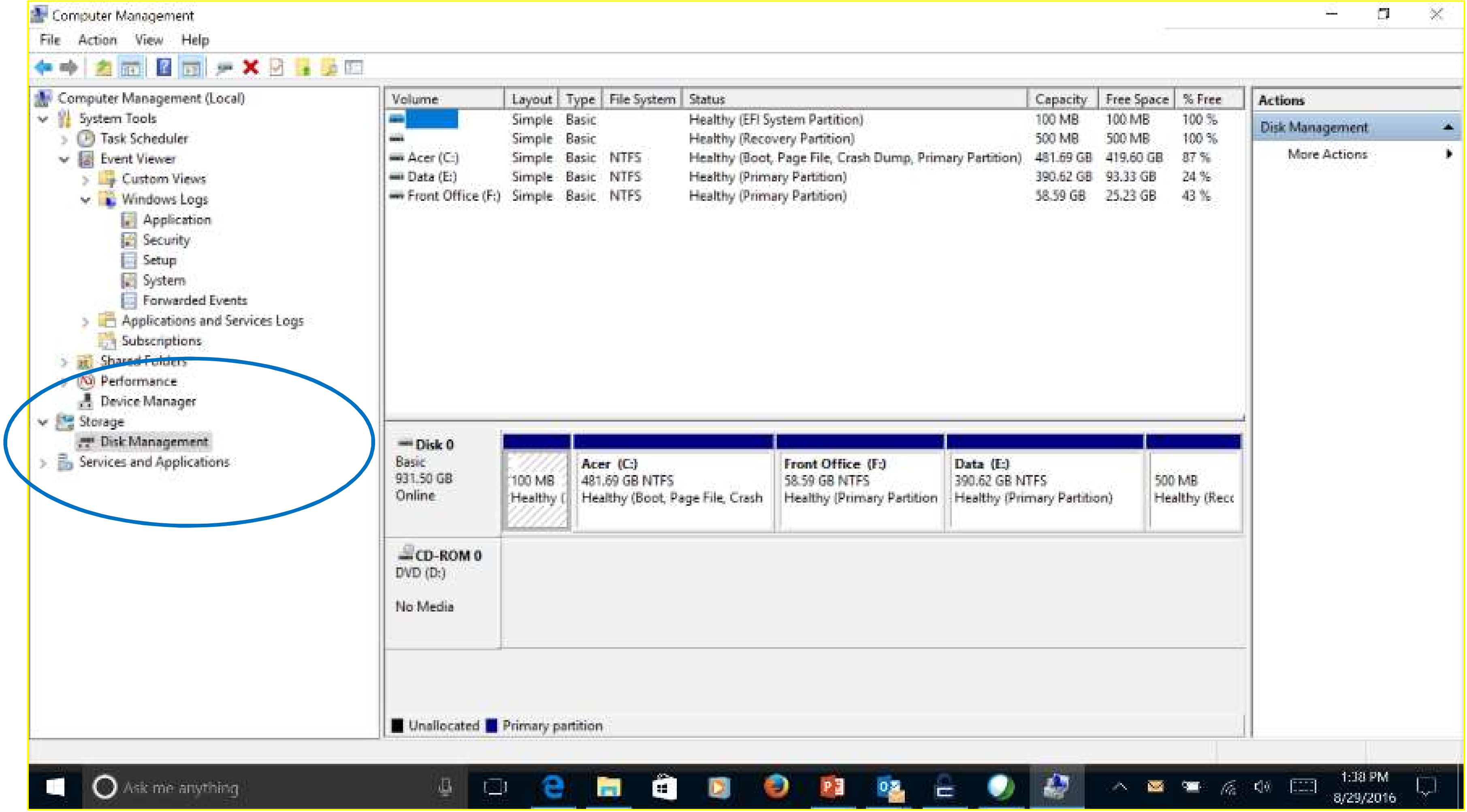
Special privileges assigned to new logon.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/29/2016 1:29:14 PM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success

Windows Administrative Tools Computer Management Windows Logs

DETECTION PROCEDURES SERVER EXAMPLE 1



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 MB	100 %
	Simple	Basic		Healthy (Recovery Partition)	500 MB	500 MB	100 %
Acer (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	481.69 GB	419.60 GB	87 %
Data (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	390.62 GB	93.33 GB	24 %
Front Office (F:)	Simple	Basic	NTFS	Healthy (Primary Partition)	58.59 GB	25.23 GB	43 %

Disk 0
Basic
931.50 GB
Online

100 MB
Healthy (

Acer (C:)
481.69 GB NTFS
Healthy (Boot, Page File, Crash

Front Office (F:)
58.59 GB NTFS
Healthy (Primary Partition

Data (E:)
390.62 GB NTFS
Healthy (Primary Partition)

500 MB
Healthy (Recc

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition

Windows Administrative Tools Computer Management Data Management

ENCLOSURE G: FORENSICS

ENCLOSURE G: DATA COLLECTION FOR FORENSICS

G.1. Data Collection for Forensics Introduction

a. Description. Data collection for forensics involves the acquisition of volatile and nonvolatile data from a host, a network device, and ICS field controllers. Memory acquisition involves copying the contents for volatile memory to transportable, non-volatile storage. Data acquisition is copying non-volatile data stored on any form of media to transportable, non-volatile storage. A digital investigator seeks to preserve the state of the digital environment in a manner that allows the investigator to reach reliable inferences through analysis. (Ligh, 2014)

b. Key Components

(1) Volatile memory
(2) Non-volatile data
(3) Collection
(4) Documentation
(5) Notifications

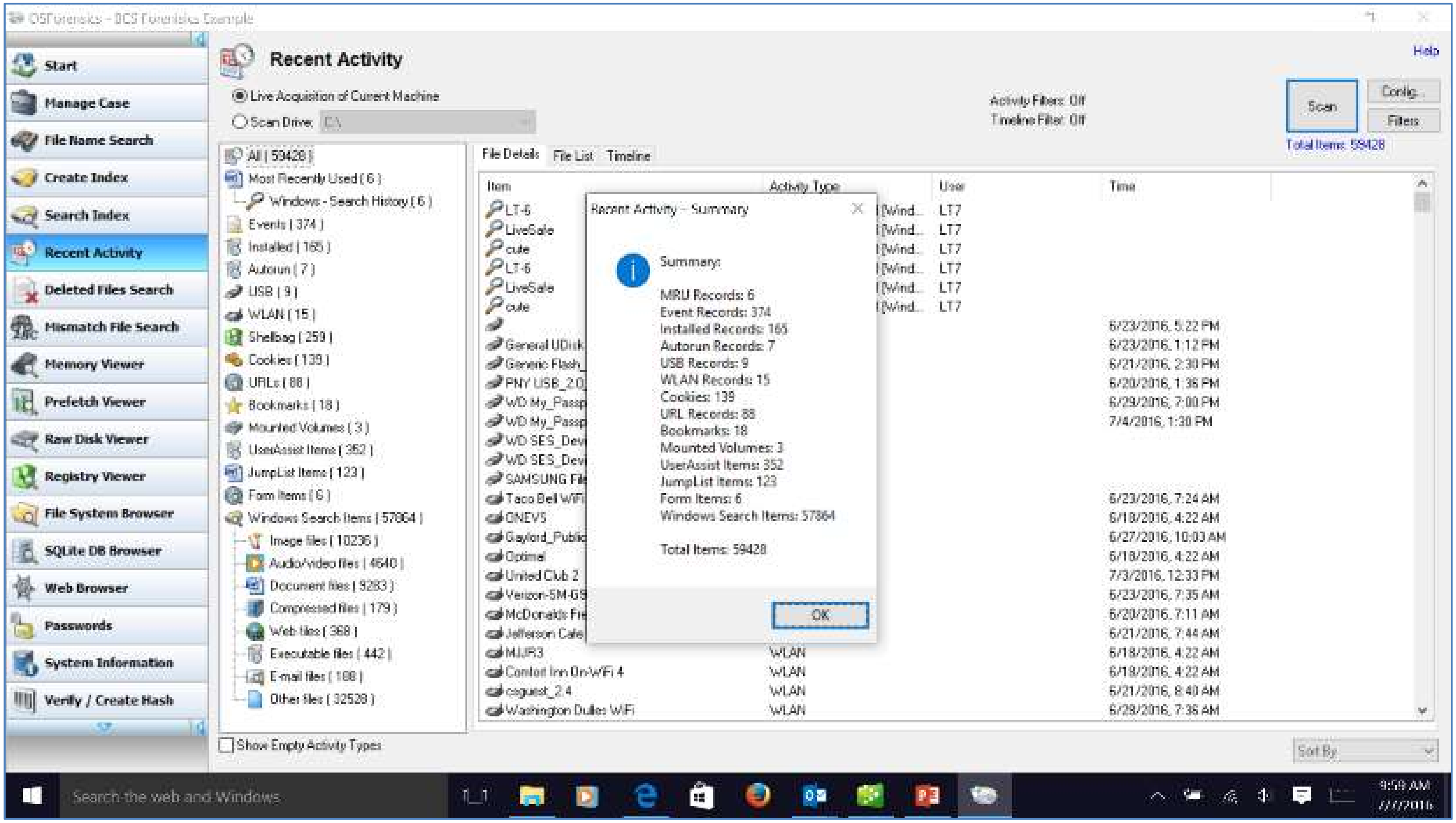
c. Prerequisites
(1) Administrative tools for acquisition
(2) Storage devices to capture and transport evidence

G.3. Data Collection Tools

G.3. Data Collection Tools

- Mandiant Redline
- Mandiant Memoryze
- Microsoft SysInternals
- Microsoft Windows system utilities
- Linux system utilities
- Glasswire
- OSForensics
- RegRipper
- Belarc

OS Forensics Recent Activity



Recent Activity

● Live Acquisition of Current Machine

○ Scan Drive: C:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 59428

- All [59428]
- Most Recently Used (6)
  - Windows - Search History (6)
- Events (374)
- Installed (165)
- Autorun (7)
- USB (9)
- WLAN (15)
- Shellbag (259)
- Cookies (139)
- URLs (88)
- Bookmarks (18)
- Mounted Volumes (3)
- UserAssist Items (352)
- JumpList Items (123)
- Form Items (6)
- Windows Search Items (57864)
  - Image files (10236)
  - Audio/video files (4640)
  - Document files (9283)
  - Compressed files (179)
  - Web files (368)
  - Executable files (442)
  - E-mail files (188)
  - Other files (32528)

□ Show Empty Activity Types

Item	Activity Type	User	Time
LT-6	[Wind...	LT7	
LiveSafe	[Wind...	LT7	
cute	[Wind...	LT7	
LT-6	[Wind...	LT7	
LiveSafe	[Wind...	LT7	
cute	[Wind...	LT7	
			6/23/2016, 5:22 PM
General UDisk			6/23/2016, 1:12 PM
Generic Flash_			6/21/2016, 2:30 PM
PNY USB_2.0			6/20/2016, 1:36 PM
WD My_Passp			6/29/2016, 7:00 PM
WD My_Passp			7/4/2016, 1:30 PM
WD SES_Dev			
WD SES_Dev			
SAMSUNG File			
Taco Bell WiFi			6/23/2016, 7:24 AM
ONEVS			6/18/2016, 4:22 AM
Gaylord_Public			6/27/2016, 10:03 AM
Optimal			6/18/2016, 4:22 AM
United Club 2			7/3/2016, 12:33 PM
Verizon-SM-GS			6/23/2016, 7:35 AM
McDonalds Fre			6/20/2016, 7:11 AM
Jefferson Cafe			6/21/2016, 7:44 AM
MJJR3	WLAN		6/18/2016, 4:22 AM
Comfort Inn On-WiFi 4	WLAN		6/18/2016, 4:22 AM
csguest_2.4	WLAN		6/21/2016, 8:40 AM
Washington Dulles WiFi	WLAN		6/28/2016, 7:36 AM

Recent Activity - Summary

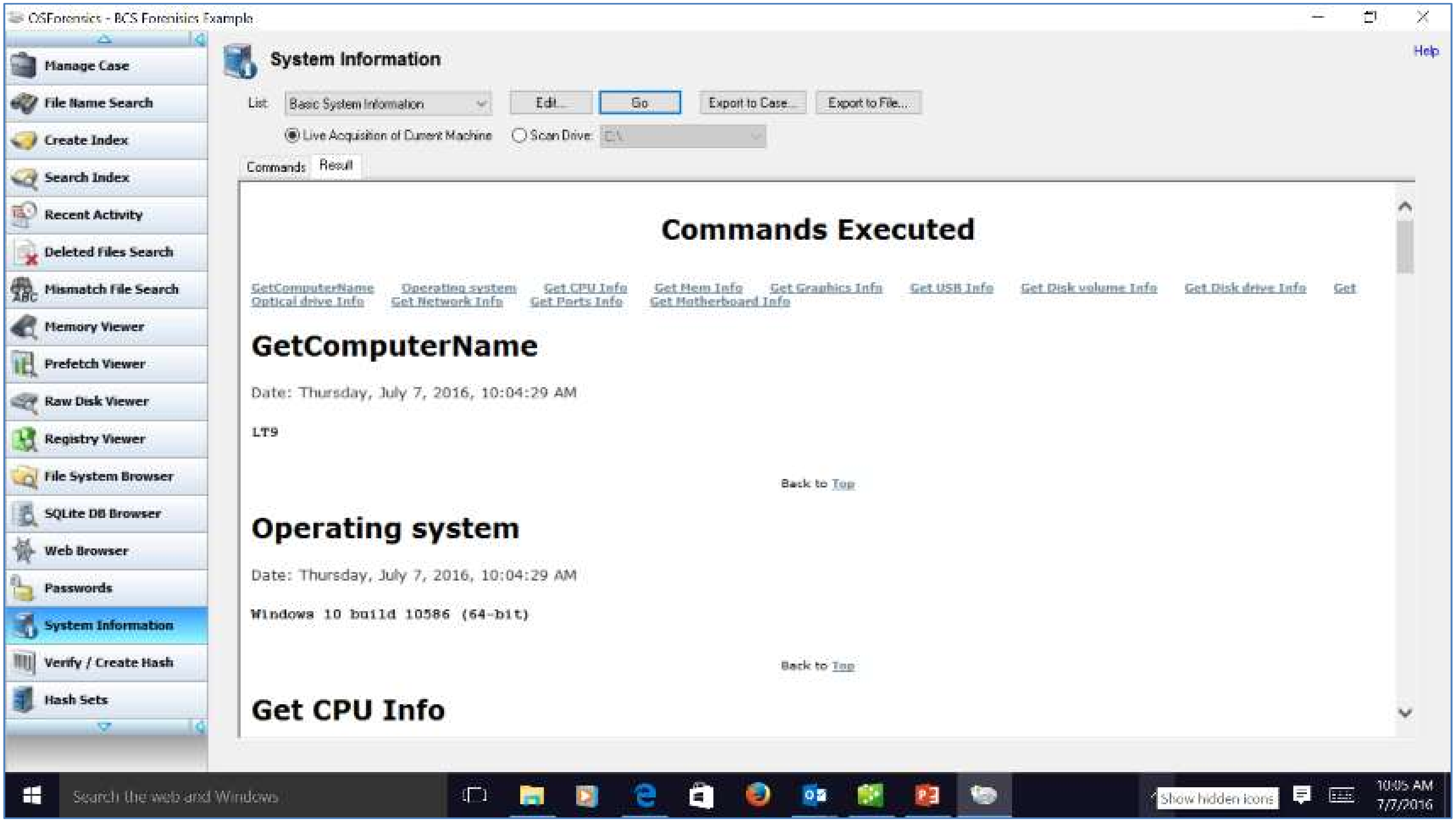
Summary:

MRU Records: 6
Event Records: 374
Installed Records: 165
Autorun Records: 7
USB Records: 9
WLAN Records: 15
Cookies: 139
URL Records: 88
Bookmarks: 18
Mounted Volumes: 3
UserAssist Items: 352
JumpList Items: 123
Form Items: 6
Windows Search Items: 57864

Total Items: 59428

OK

OS Forensics System Information



List: Basic System Information

● Live Acquisition of Current Machine ○ Scan Drive: C:\

Commands Executed

GetComputerName Operating system Get CPU Info Get Mem Info Get Graphics Info Get USB Info Get Disk volume Info Get Disk drive Info Get Optical drive Info Get Network Info Get Ports Info Get Motherboard Info

GetComputerName

Date: Thursday, July 7, 2016, 10:04:29 AM

```
LT9
```

Back to Top

Operating system

Date: Thursday, July 7, 2016, 10:04:29 AM

```
Windows 10 build 10586 (64-bit)
```

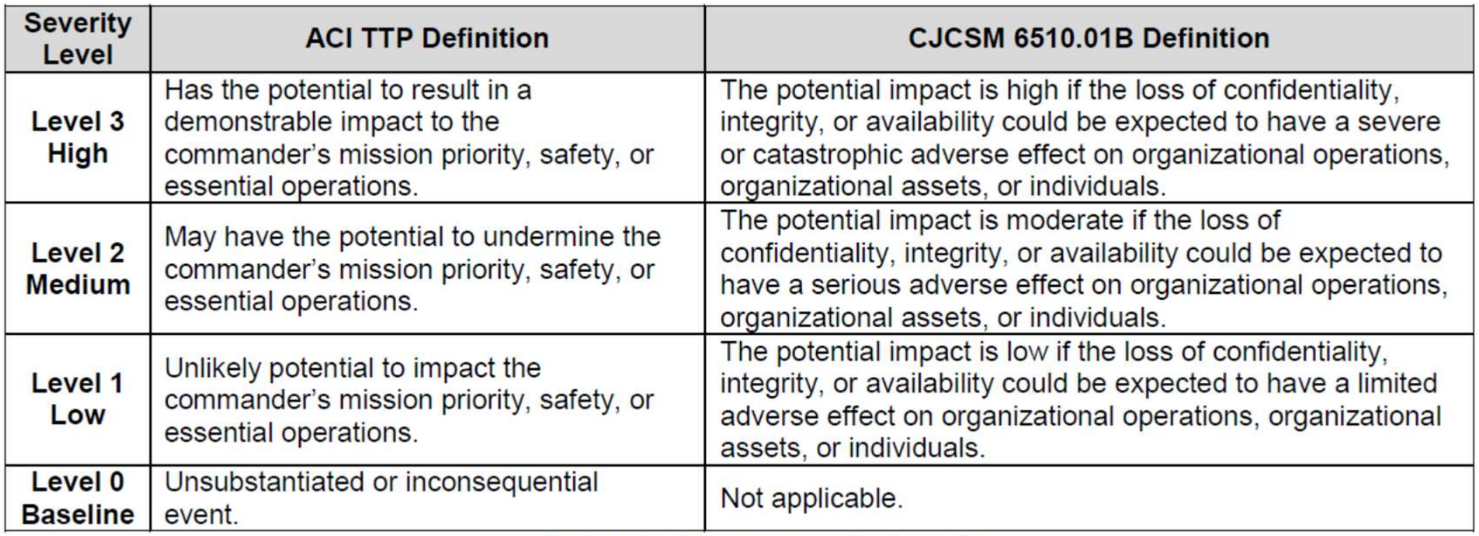
Back to Top

Get CPU Info

ENCLOSURE I: CYBER SEVERITY LEVELS

I.2. Cyber Severity Levels Overview

While ICS/SCADA can be attacked in a variety of ways, there are a number of steps that are common, or at least present in most attacks. Each of these steps could yield some behavioral change in the system that could be detected by an operator. However, not all Detections require a Mitigation action. Mitigation is a disruptive process, which could degrade the operational capabilities. Given those circumstances, a more graduated approach to Detection/Mitigation allows IT and ICS managers to take steps to assess the cyber event to determine what level of response is required and react proportionately. Table I-1 provides the incident level severity rating approach used in the ACI TTP.



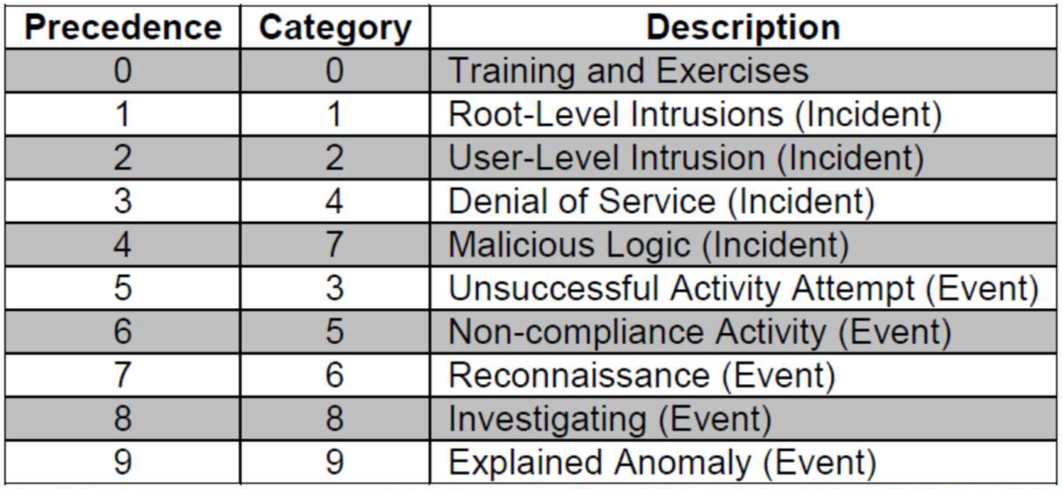
Severity Level	ACI TTP Definition	CJCSM 6510.01B Definition
Level 3 High	Has the potential to result in a demonstrable impact to the commander's mission priority, safety, or essential operations.	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Level 2 Medium	May have the potential to undermine the commander's mission priority, safety, or essential operations.	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Level 1 Low	Unlikely potential to impact the commander's mission priority, safety, or essential operations.	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Level 0 Baseline	Unsubstantiated or inconsequential event.	Not applicable.

Table I-1: Incident Severity Levels

ENCLOSURE I: CYBER SEVERITY LEVELS

I.4. Precedence and Category Levels

The ACI TTP provides that additional guidance to ICS operators for the handling of cyber events during active hostilities or emergencies. However, to ensure consistent reporting and integration with the cyber incident/event chain of command, the ACI TTP will characterize cyber incidences/events using the CJFRCSM 6510.01B Precedence and Category Levels Table (table I-2). This table represents the precedence and category levels located throughout the ACI TTP. The table is provided for informational purposes, as the ACI TTP characterizes cyber incidents and events within the reporting schemas.



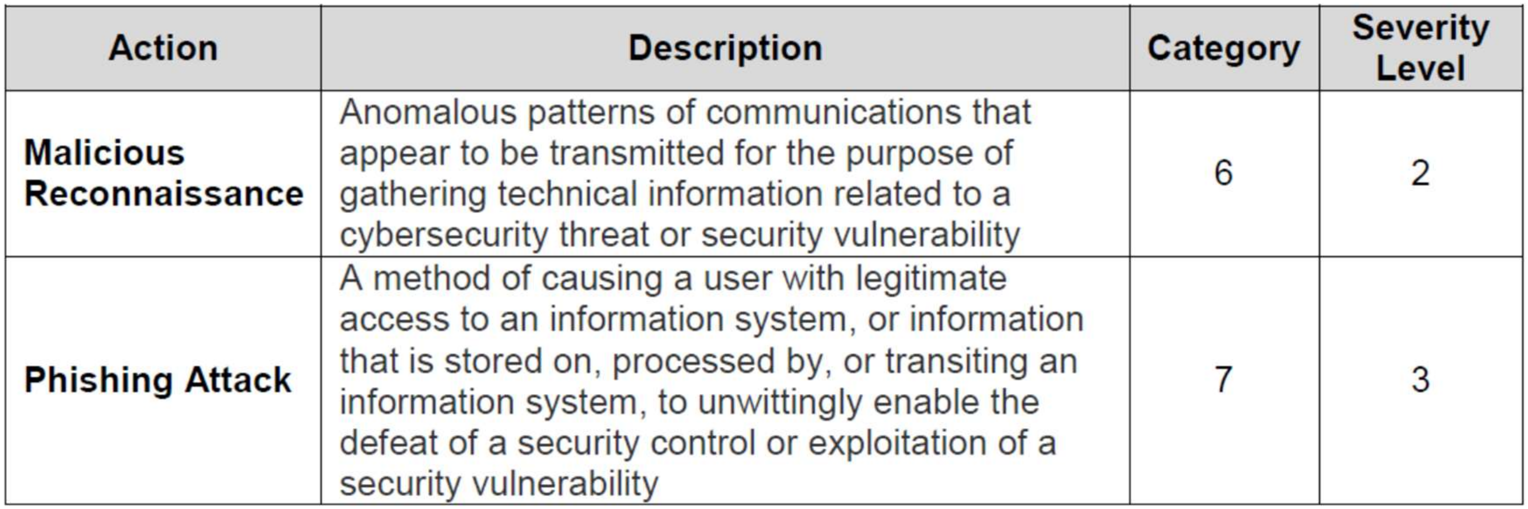
Precedence	Category	Description
0	0	Training and Exercises
1	1	Root-Level Intrusions (Incident)
2	2	User-Level Intrusion (Incident)
3	4	Denial of Service (Incident)
4	7	Malicious Logic (Incident)
5	3	Unsuccessful Activity Attempt (Event)
6	5	Non-compliance Activity (Event)
7	6	Reconnaissance (Event)
8	8	Investigating (Event)
9	9	Explained Anomaly (Event)

Table I-2: Precedence and Category Levels Table (CJCSM 6510.01B)

ENCLOSURE I: CYBER SEVERITY LEVELS

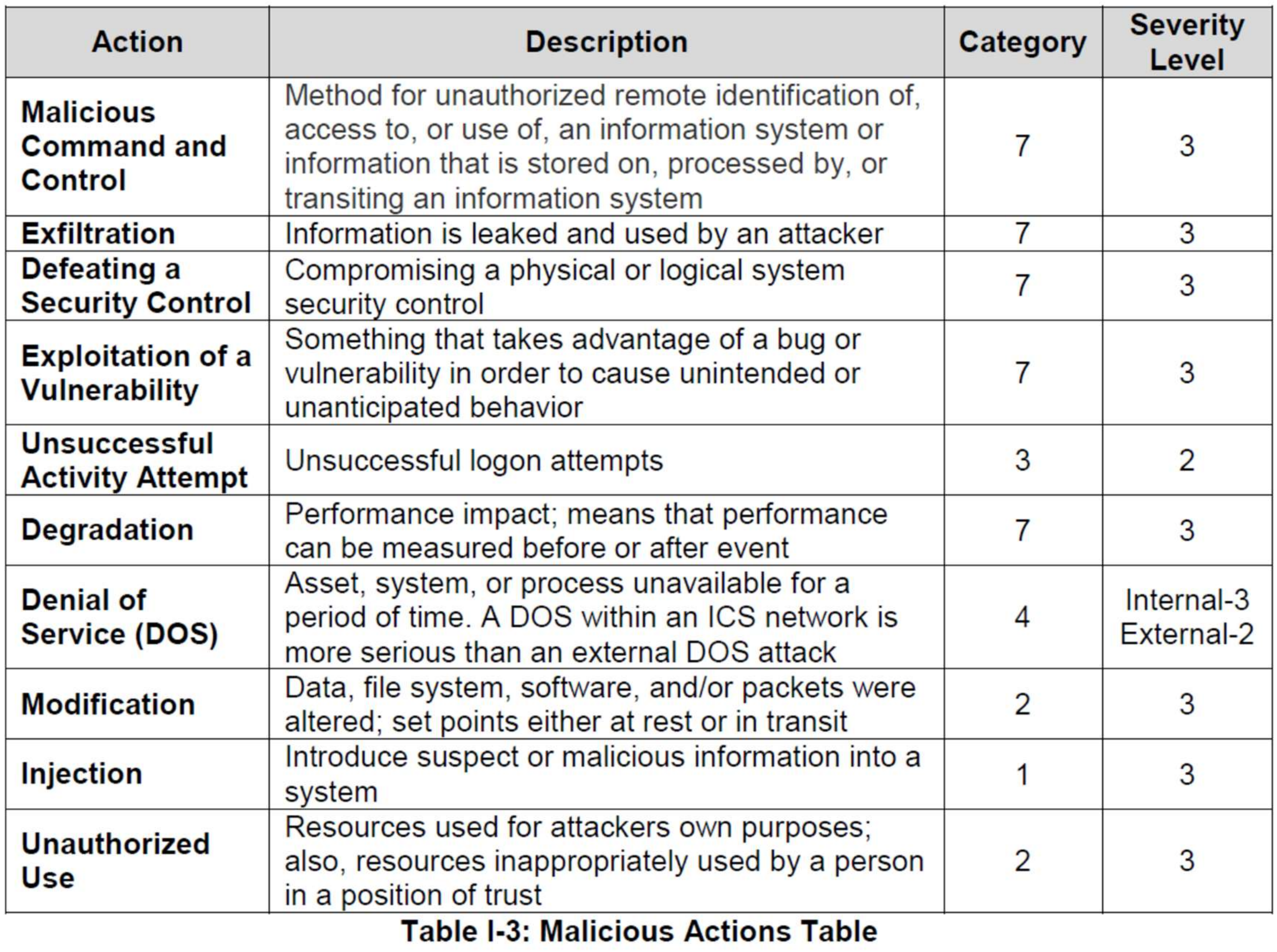
I.5. Malicious Actions Table

The Malicious Actions Table (table I-3) provides actions and the resulting Severity Level.



Action	Description	Category	Severity Level
Malicious Reconnaissance	Anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability	6	2
Phishing Attack	A method of causing a user with legitimate access to an information system, or information that is stored on, processed by, or transiting an information system, to unwittingly enable the defeat of a security control or exploitation of a security vulnerability	7	3

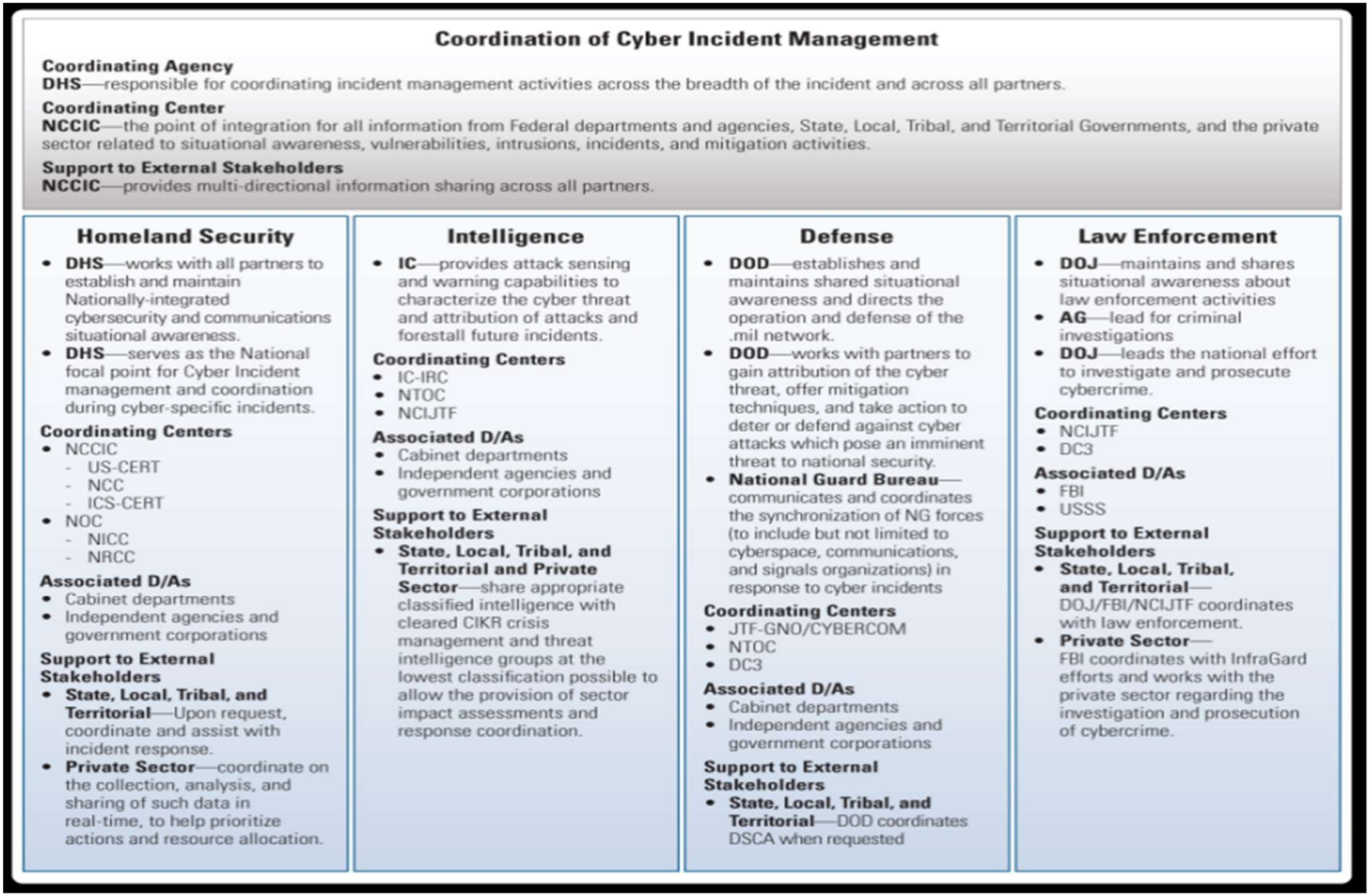
ENCLOSURE I: CYBER SEVERITY LEVELS



Action	Description	Category	Severity Level
Malicious Command and Control	Method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system	7	3
Exfiltration	Information is leaked and used by an attacker	7	3
Defeating a Security Control	Compromising a physical or logical system security control	7	3
Exploitation of a Vulnerability	Something that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior	7	3
Unsuccessful Activity Attempt	Unsuccessful logon attempts	3	2
Degradation	Performance impact; means that performance can be measured before or after event	7	3
Denial of Service (DOS)	Asset, system, or process unavailable for a period of time. A DOS within an ICS network is more serious than an external DOS attack	4	Internal-3 External-2
Modification	Data, file system, software, and/or packets were altered; set points either at rest or in transit	2	3
Injection	Introduce suspect or malicious information into a system	1	3
Unauthorized Use	Resources used for attackers own purposes; also, resources inappropriately used by a person in a position of trust	2	3

Table I-3: Malicious Actions Table

Coordination of Cyber Incident Management



Coordination of Cyber Incident Management

Coordinating Agency
DHS—responsible for coordinating incident management activities across the breadth of the incident and across all partners.

Coordinating Center
NCCIC—the point of integration for all information from Federal departments and agencies, State, Local, Tribal, and Territorial Governments, and the private sector related to situational awareness, vulnerabilities, intrusions, incidents, and mitigation activities.

Support to External Stakeholders
NCCIC—provides multi-directional information sharing across all partners.

Homeland Security

- **DHS**—works with all partners to establish and maintain Nationally-integrated cybersecurity and communications situational awareness.
- **DHS**—serves as the National focal point for Cyber Incident management and coordination during cyber-specific incidents.

Coordinating Centers

- NCCIC
  - US-CERT
  - NCC
  - ICS-CERT
- NOC
  - NICC
  - NRCC

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to External Stakeholders

- **State, Local, Tribal, and Territorial**—Upon request, coordinate and assist with incident response.
- **Private Sector**—coordinate on the collection, analysis, and sharing of such data in real-time, to help prioritize actions and resource allocation.

Intelligence

- **IC**—provides attack sensing and warning capabilities to characterize the cyber threat and attribution of attacks and forestall future incidents.

Coordinating Centers

- IC-IRC
- NTOC
- NCIJTF

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to External Stakeholders

- **State, Local, Tribal, and Territorial and Private Sector**—share appropriate classified intelligence with cleared CIKR crisis management and threat intelligence groups at the lowest classification possible to allow the provision of sector impact assessments and response coordination.

Defense

- **DOD**—establishes and maintains shared situational awareness and directs the operation and defense of the .mil network.
- **DOD**—works with partners to gain attribution of the cyber threat, offer mitigation techniques, and take action to deter or defend against cyber attacks which pose an imminent threat to national security.
- **National Guard Bureau**—communicates and coordinates the synchronization of NG forces (to include but not limited to cyberspace, communications, and signals organizations) in response to cyber incidents

Coordinating Centers

- JTF-GNO/CYBERCOM
- NTOC
- DC3

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to External Stakeholders

- **State, Local, Tribal, and Territorial**—DOD coordinates DSCA when requested

Law Enforcement

- **DOJ**—maintains and shares situational awareness about law enforcement activities
- **AG**—lead for criminal investigations
- **DOJ**—leads the national effort to investigate and prosecute cybercrime.

Coordinating Centers

- NCIJTF
- DC3

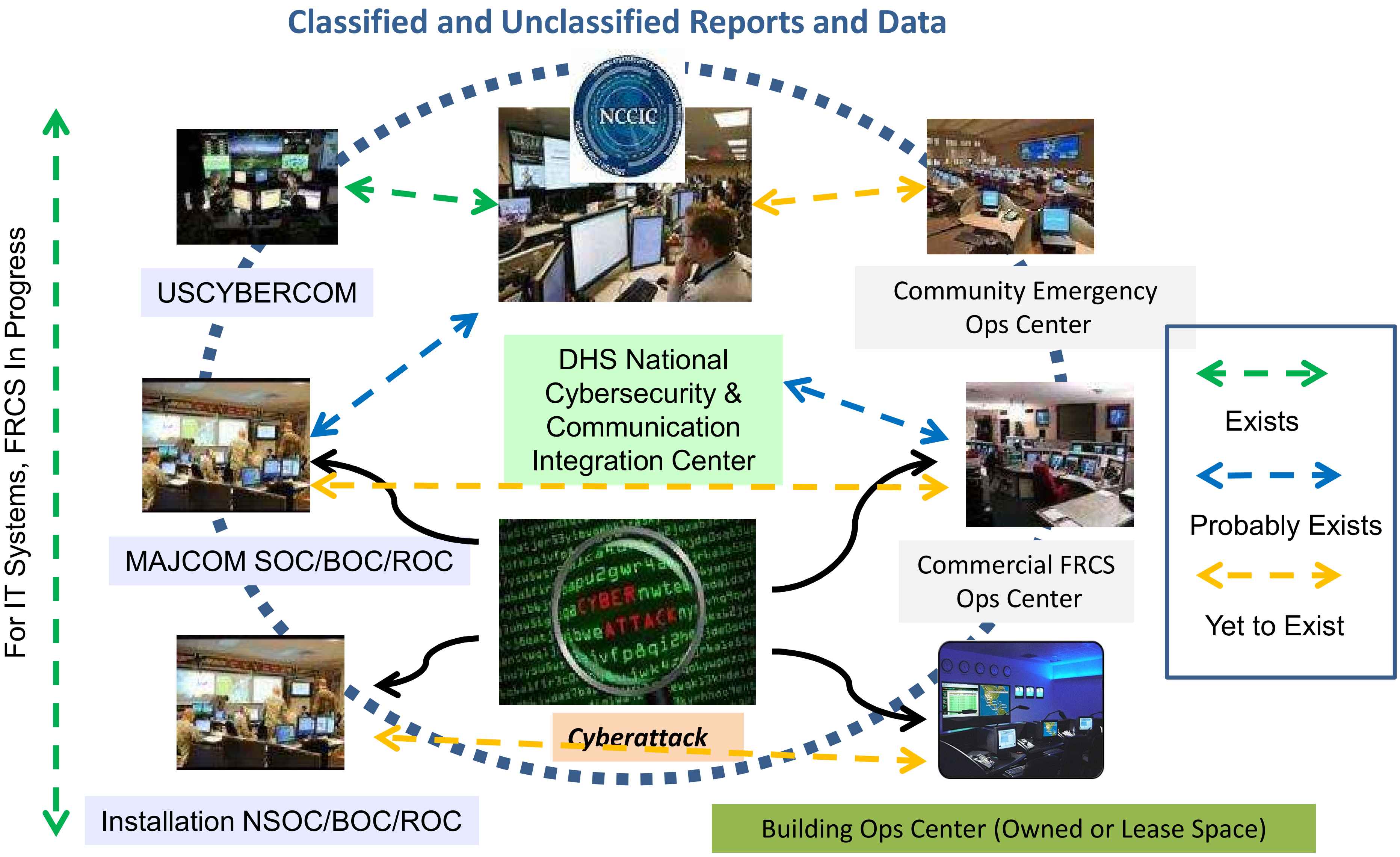
Associated D/As

- FBI
- USSS

Support to External Stakeholders

- **State, Local, Tribal, and Territorial**—DOJ/FBI/NCIJTF coordinates with law enforcement.
- **Private Sector**—FBI coordinates with InfraGard efforts and works with the private sector regarding the investigation and prosecution of cybercrime.

Conceptual Information Sharing



Classified and Unclassified Reports and Data

USCYBERCOM

NCCIC

Community Emergency Ops Center

DHS National Cybersecurity & Communication Integration Center

MAJCOM SOC/BOC/ROC

Commercial FRCS Ops Center

Cyberattack

Installation NSOC/BOC/ROC

Building Ops Center (Owned or Lease Space)

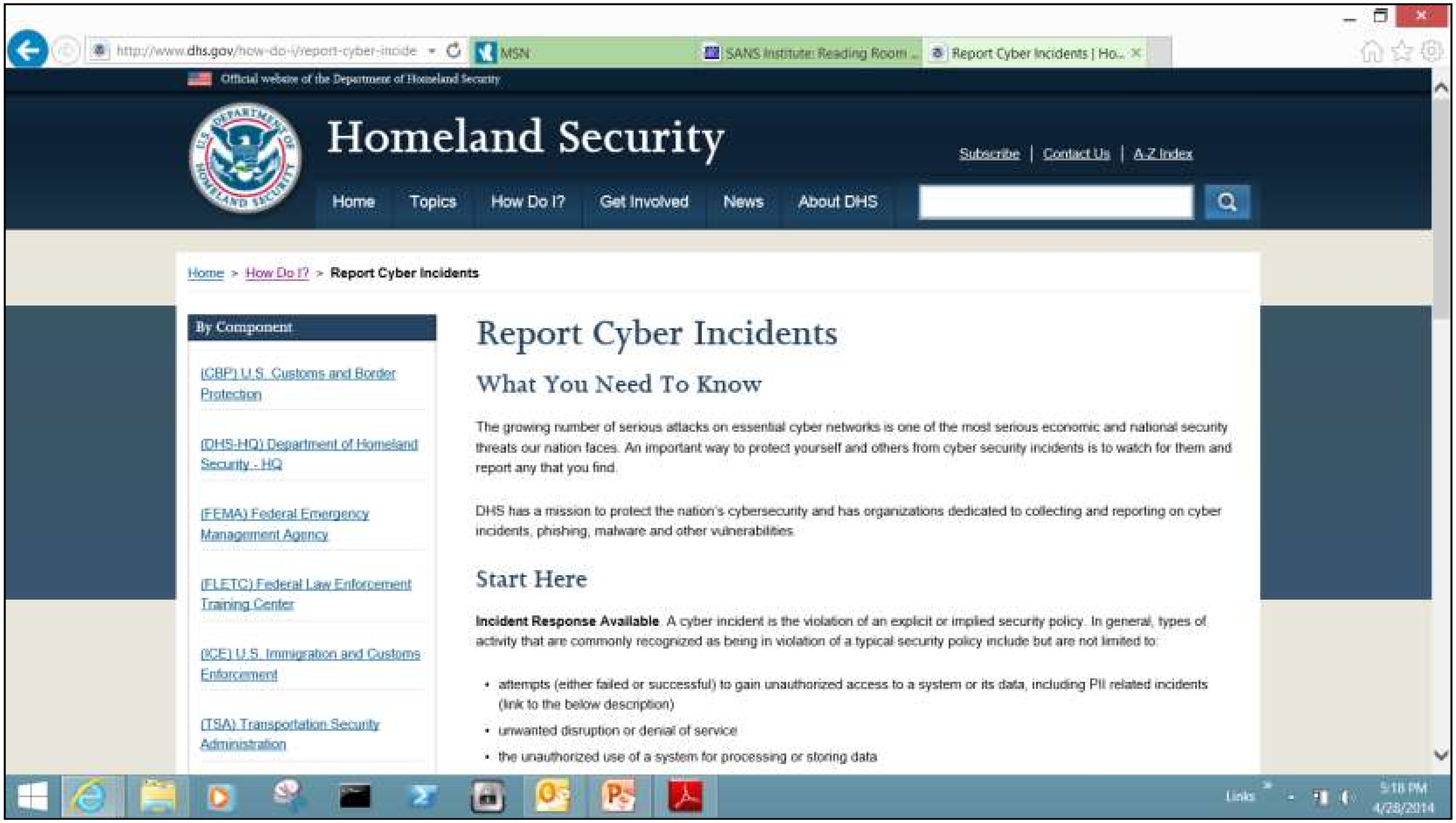
For IT Systems, FRCS In Progress

Exists

Probably Exists

Yet to Exist

US-CERT Incident Reporting System



http://www.dhs.gov/how-do-i/report-cyber-incide
MSN
SANS Institute: Reading Room ...
Report Cyber Incidents | Ho...
Official website of the Department of Homeland Security
Homeland Security
Subscribe | Contact Us | A-Z Index
Home
Topics
How Do I?
Get Involved
News
About DHS
Home > How Do I? > Report Cyber Incidents
By Component
(CBP) U.S. Customs and Border Protection
(DHS-HQ) Department of Homeland Security - HQ
(FEMA) Federal Emergency Management Agency
(FLETC) Federal Law Enforcement Training Center
(ICE) U.S. Immigration and Customs Enforcement
(TSA) Transportation Security Administration
Links
5:18 PM
4/28/2014

Report Cyber Incidents

What You Need To Know

The growing number of serious attacks on essential cyber networks is one of the most serious economic and national security threats our nation faces. An important way to protect yourself and others from cyber security incidents is to watch for them and report any that you find.

DHS has a mission to protect the nation's cybersecurity and has organizations dedicated to collecting and reporting on cyber incidents, phishing, malware and other vulnerabilities.

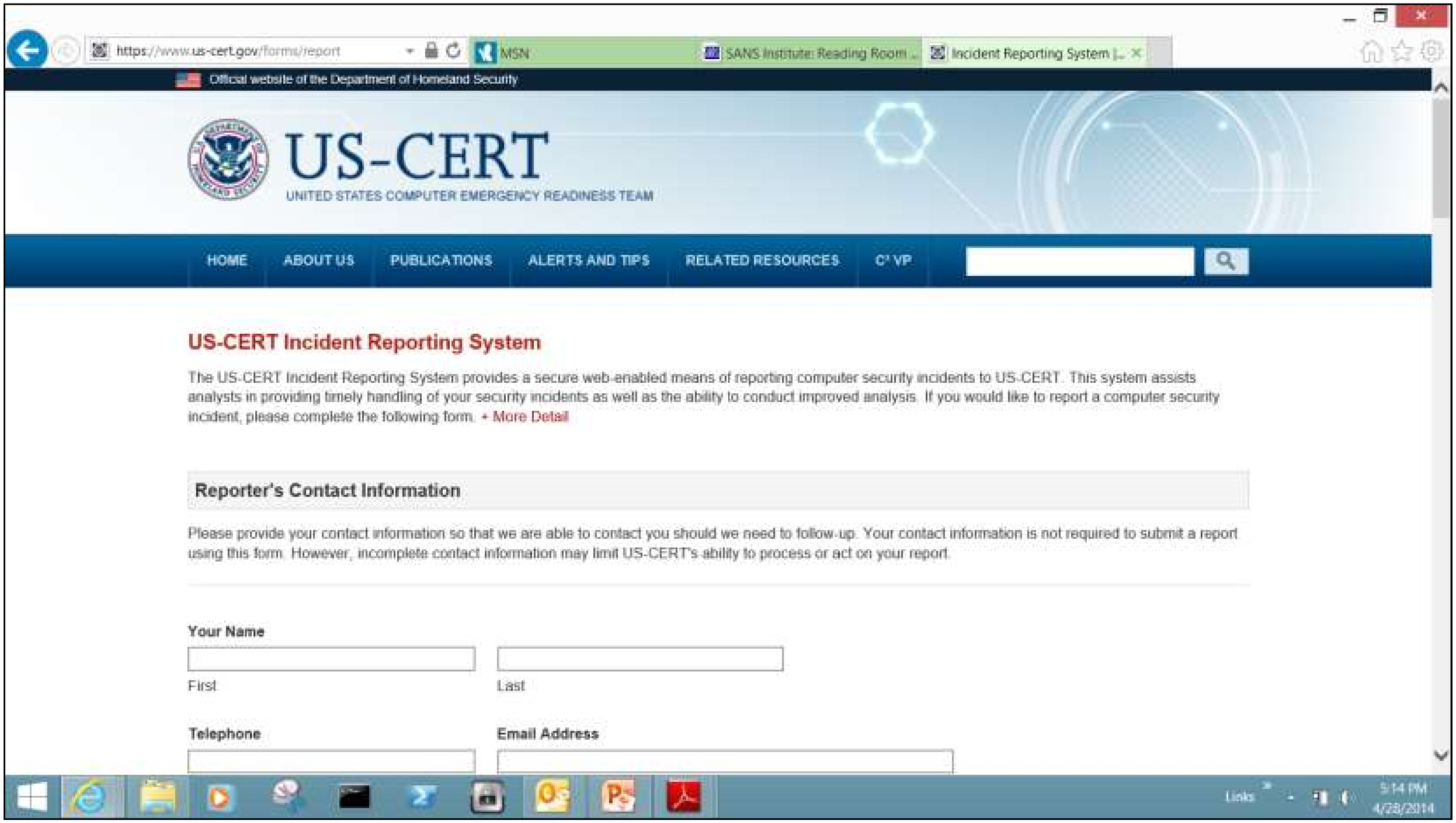
Start Here

Incident Response Available. A cyber incident is the violation of an explicit or implied security policy. In general, types of activity that are commonly recognized as being in violation of a typical security policy include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII related incidents (link to the below description)
- unwanted disruption or denial of service
- the unauthorized use of a system for processing or storing data

http://www.dhs.gov/how-do-i/report-cyber-incidents

US-CERT Incident Reporting System


https://www.us-cert.gov/forms/report
MSN
SANS Institute: Reading Room ...
Incident Reporting System |...
Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
Links
5:14 PM
4/28/2014

US-CERT Incident Reporting System

The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. + More Detail

Reporter's Contact Information

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

Your Name

First

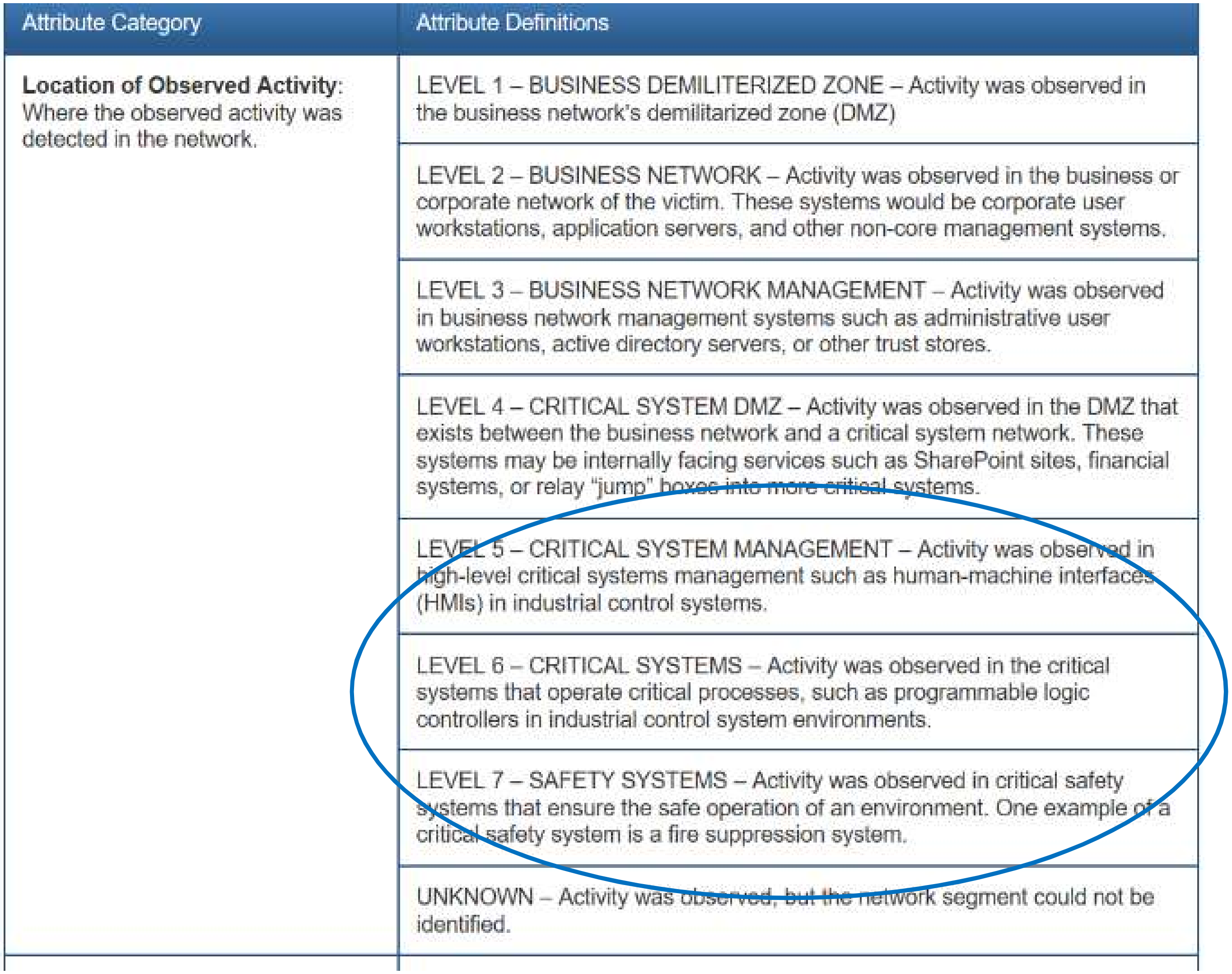
Last

Telephone

Email Address

https://www.us-cert.gov/forms/report

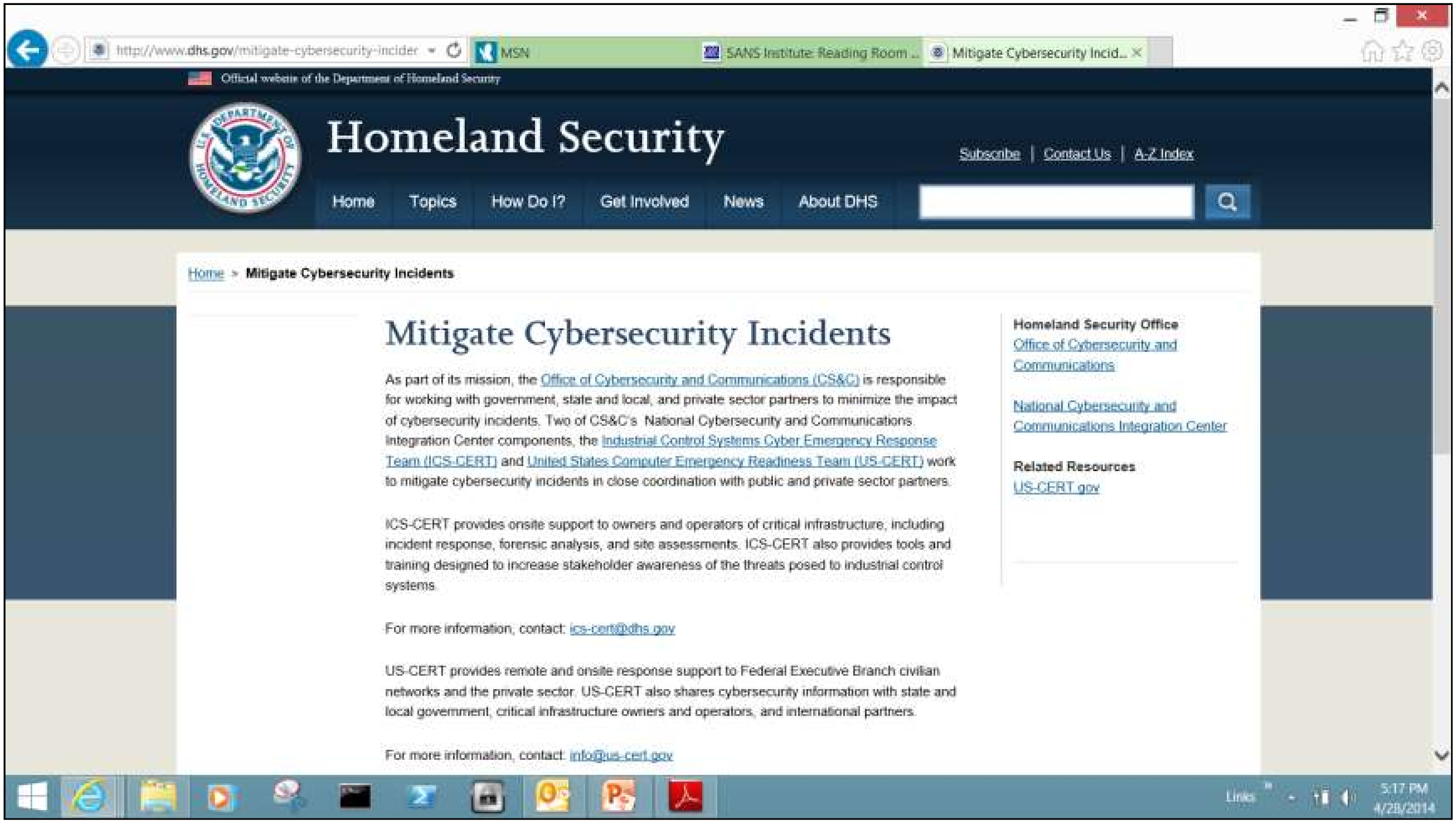
US-CERT Incident Reporting System



Attribute Category	Attribute Definitions
Location of Observed Activity: Where the observed activity was detected in the network.	LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
	LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.
	LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores.
	LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
	LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
	LEVEL 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments.
	LEVEL 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.
	UNKNOWN – Activity was observed, but the network segment could not be identified.

https://www.us-cert.gov/incident-notification-guidelines

US-CERT Incident Reporting System


http://www.dhs.gov/mitigate-cybersecurity-incider
MSN
SANS Institute: Reading Room ...
Mitigate Cybersecurity Incid...
Official website of the Department of Homeland Security
Homeland Security
Subscribe | Contact Us | A-Z Index
Home
Topics
How Do I?
Get Involved
News
About DHS
Links
5:17 PM
4/28/2014

Home > **Mitigate Cybersecurity Incidents**

Mitigate Cybersecurity Incidents

As part of its mission, the Office of Cybersecurity and Communications (CS&C) is responsible for working with government, state and local, and private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C's National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

For more information, contact: ics-cert@dhs.gov

US-CERT provides remote and onsite response support to Federal Executive Branch civilian networks and the private sector. US-CERT also shares cybersecurity information with state and local government, critical infrastructure owners and operators, and international partners.

For more information, contact: info@us-cert.gov

Homeland Security Office

Office of Cybersecurity and Communications

National Cybersecurity and Communications Integration Center

Related Resources

US-CERT.gov

http://www.dhs.gov/mitigate-cybersecurity-incidents

SANS Interfacing with Law Enforcement

Table of Contents

Should information security policies include incident-handling procedures for computer crimes?

Are computer forensic evidence handling and analysis procedures helpful to business and law enforcement?

Are there standardized guidelines or procedures for reporting an incident to law enforcement? If not, what information will I need to have ready to report?

What type of access to evidence and key personal should I expect upon the involvement of Law Enforcement?

Will law enforcement obstruct my business if I call them?

How does law enforcement deal with the investigation of an active computer intrusion on a live network?

How do I maintain the proper chain of custody of my electronic evidence?

What is admissible evidence in court?

What are the federal, state, and local law enforcement agencies that I may contact?

Should I report a computer crime to law enforcement, and if so, at what stage of an investigation?

What guidelines should be provided to employees in case they are personally contacted by law enforcement as part of an incident investigation?

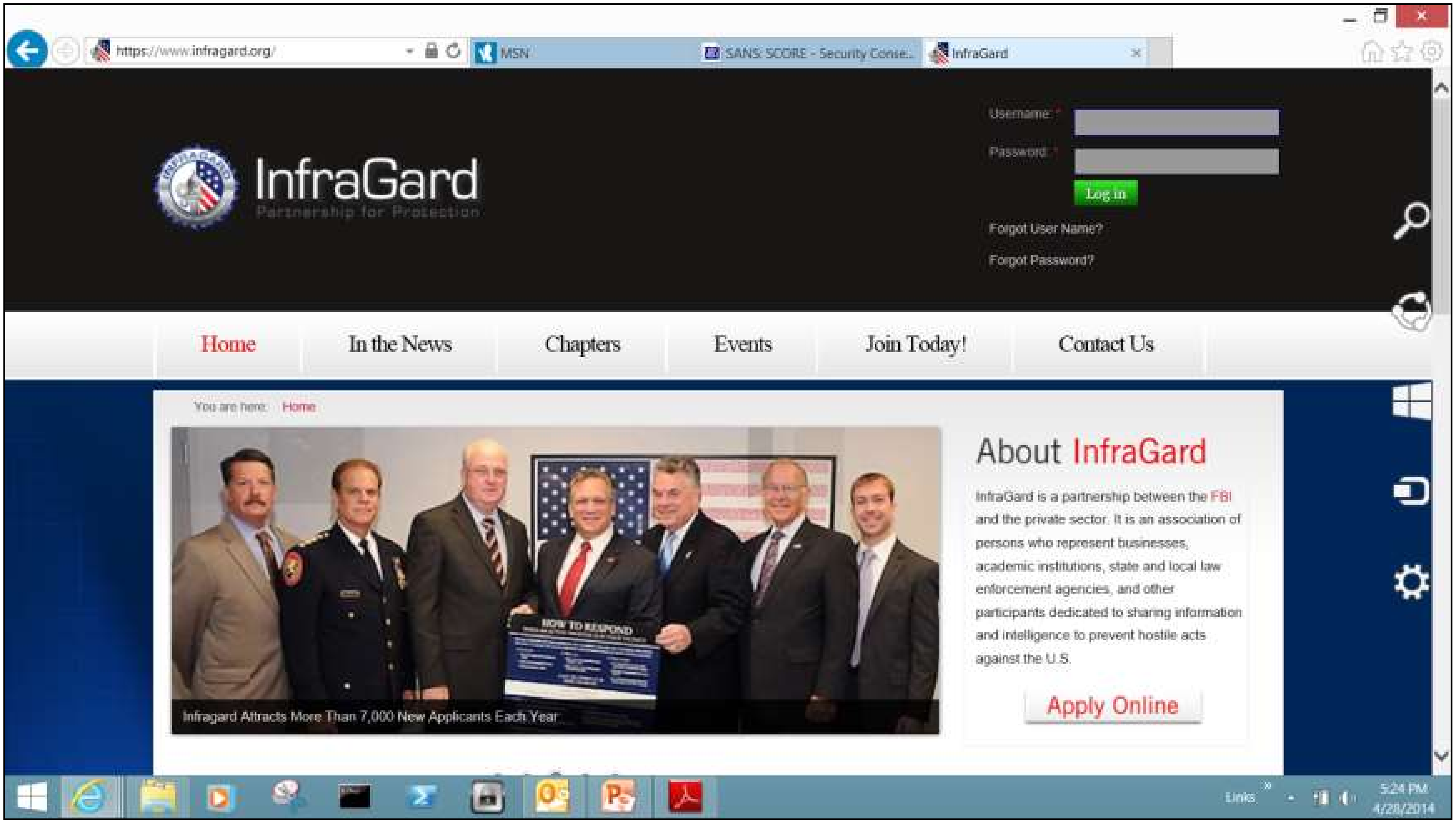
If confidential business information is involved in the incident, will law enforcement take any efforts to preserve its confidentiality during the investigation? During any subsequent prosecution?

How do I identify and preserve the crime scene or crime scenes in computer crime incidents?

How long do I need to retain evidence?

http://www.sans.org/score/faq/law_enf_faq/

InfraGard



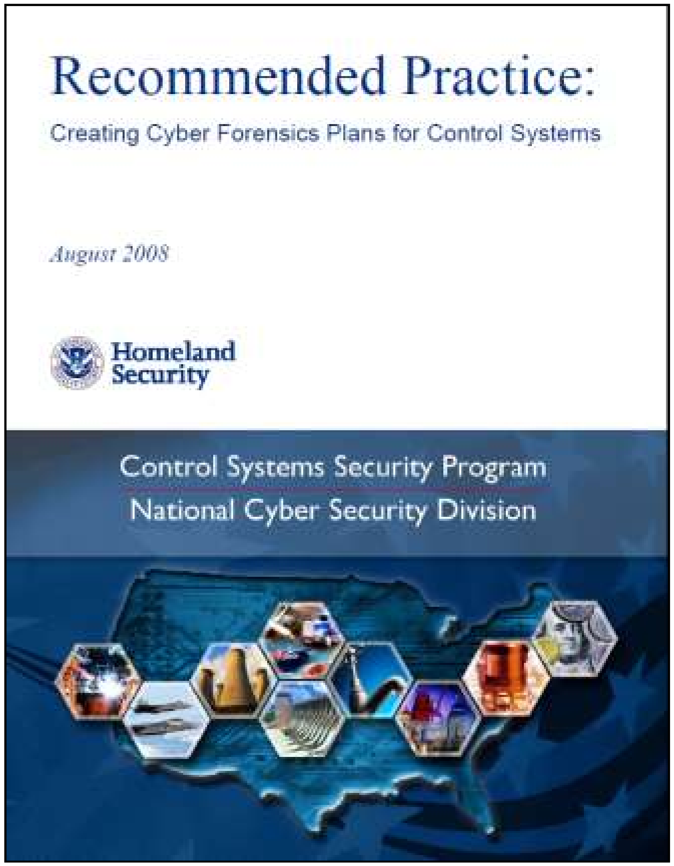
Infragard Attracts More Than 7,000 New Applicants Each Year

About InfraGard

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

https://www.infragard.org/

DHS Cyber Forensics Plans



Recommended Practice:

Creating Cyber Forensics Plans for Control Systems

August 2008

Homeland Security

Control Systems Security Program

National Cyber Security Division

The ***legacy nature and somewhat diverse or disparate component*** aspects of control systems environments can often prohibit the smooth translation of modern forensics analysis into the control systems domain. Compounded by a wide variety of proprietary technologies and protocols, as well as critical ***system technologies with no capability to store significant amounts of event information***, the task of creating a ubiquitous and unified strategy for technical ***cyber forensics on a control systems device or computing resource is far from trivial***.

DHS Control Systems Forensics

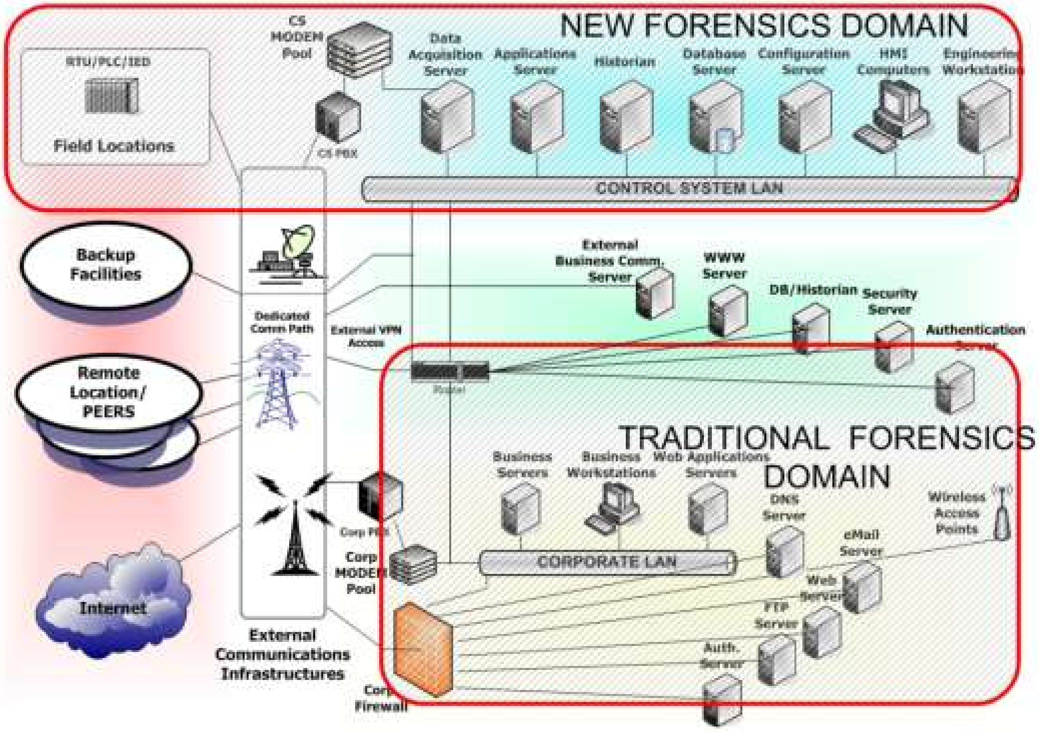
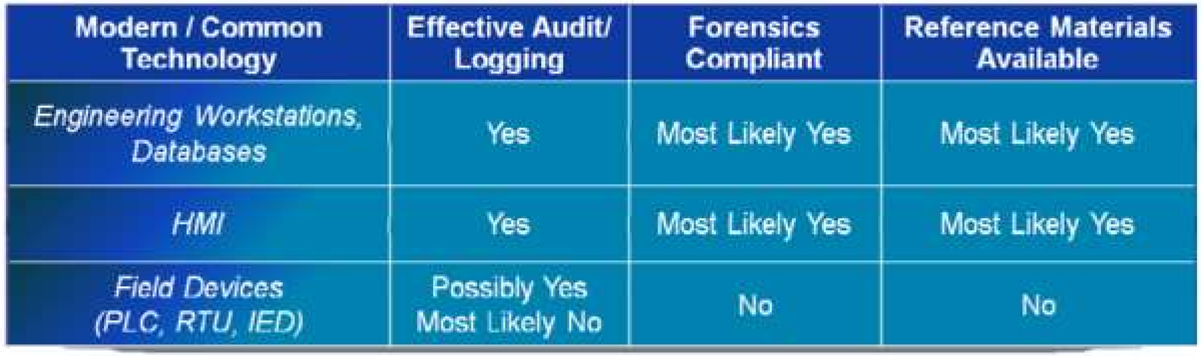


Figure 1. Control systems forensics domain and CSSP reference architecture.[6]



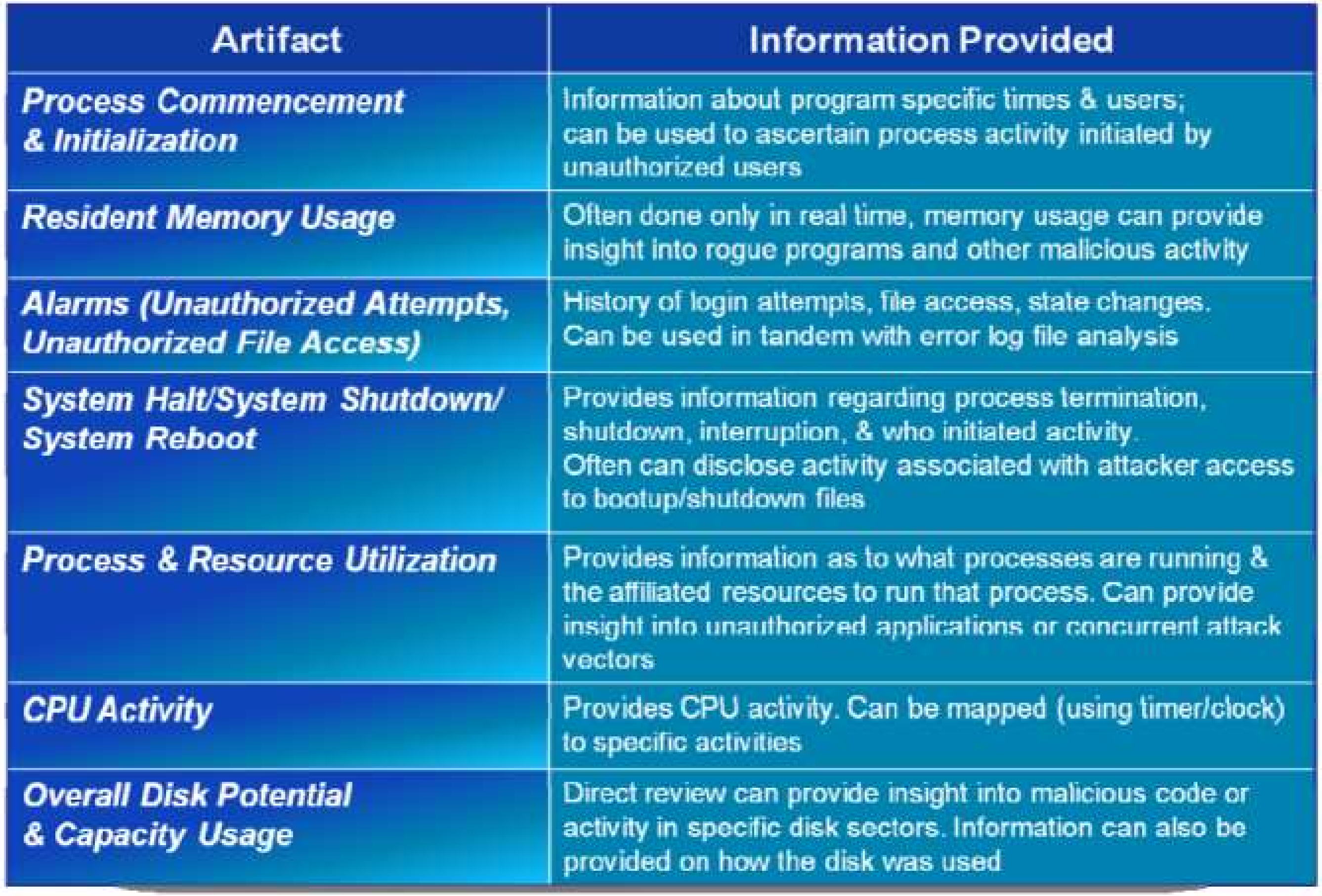
Modern / Common Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases	Yes	Most Likely Yes	Most Likely Yes
HMI	Yes	Most Likely Yes	Most Likely Yes
Field Devices (PLC, RTU, IED)	Possibly Yes Most Likely No	No	No

DHS Control Systems Forensics Framework

The basic framework for any investigation, as it pertains to ***the identification and collection of digital evidence*** (whether it is in the control systems environment or not) will have several core components or elements that must be adhered to by any investigator. To ensure the investigator has a concise and effective framework for ***executing a forensics program in a control systems environment***, the following traditional forensics elements will be examined and the uniqueness of a control systems environment and the impacts on these elements will be discussed. These elements are:

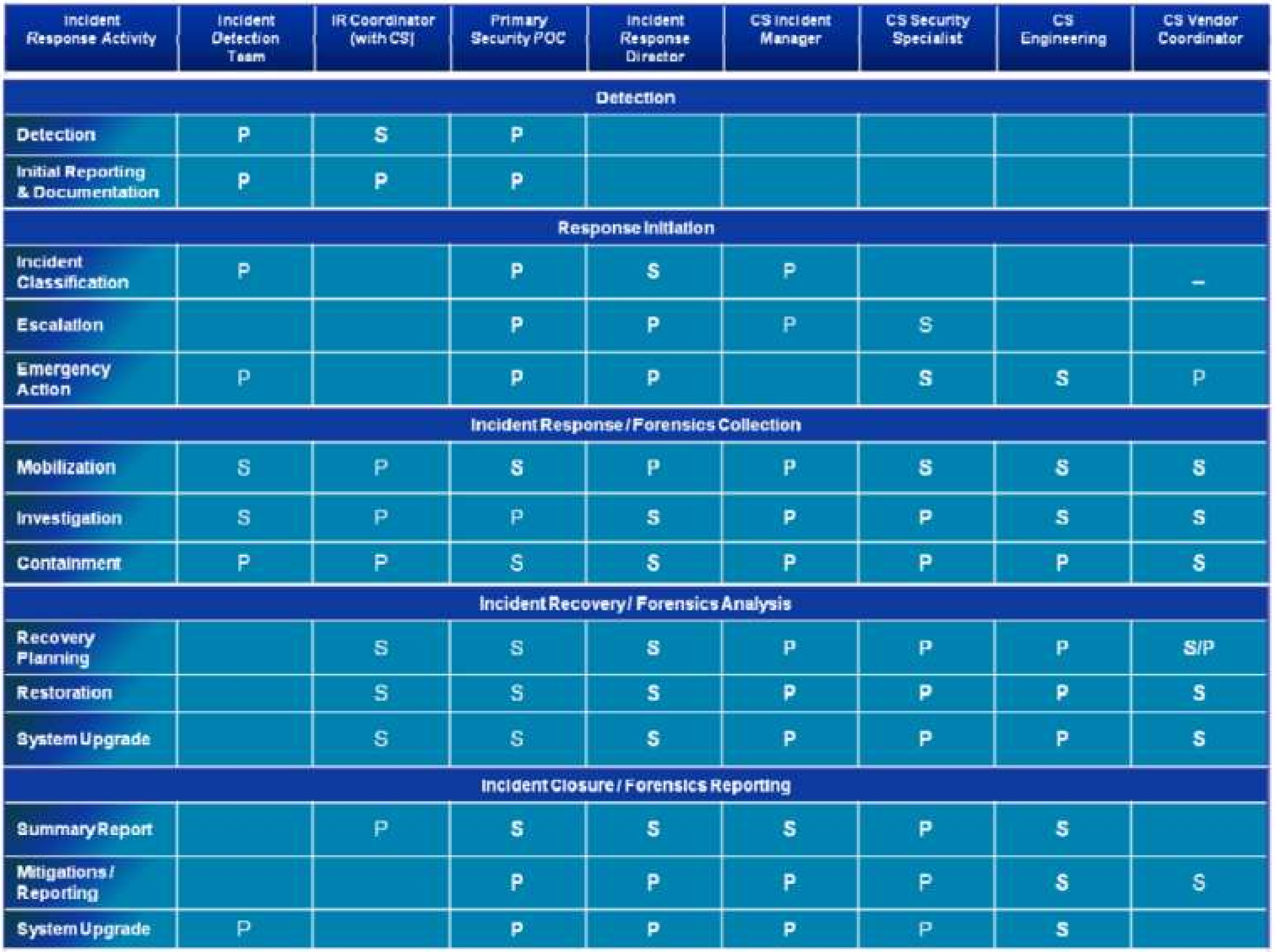
- Reference clock system
- Activity logs and transaction logs
- Other sources of data
- General system failures
- Real time forensics
- Device integrity monitoring
- Enhanced all-source logging and auditing

DHS Control Systems Forensics Artifacts



Artifact	Information Provided
Process Commencement & Initialization	Information about program specific times & users; can be used to ascertain process activity initiated by unauthorized users
Resident Memory Usage	Often done only in real time, memory usage can provide insight into rogue programs and other malicious activity
Alarms (Unauthorized Attempts, Unauthorized File Access)	History of login attempts, file access, state changes. Can be used in tandem with error log file analysis
System Halt/System Shutdown/ System Reboot	Provides information regarding process termination, shutdown, interruption, & who initiated activity. Often can disclose activity associated with attacker access to bootup/shutdown files
Process & Resource Utilization	Provides information as to what processes are running & the affiliated resources to run that process. Can provide insight into unauthorized applications or concurrent attack vectors
CPU Activity	Provides CPU activity. Can be mapped (using timer/clock) to specific activities
Overall Disk Potential & Capacity Usage	Direct review can provide insight into malicious code or activity in specific disk sectors. Information can also be provided on how the disk was used

DHS Control Systems Response Activity



Incident Response Activity	Incident Detection Team	IR Coordinator (with CS)	Primary Security POC	Incident Response Director	CS Incident Manager	CS Security Specialist	CS Engineering	CS Vendor Coordinator
Detection								
Detection	P	S	P					
Initial Reporting & Documentation	P	P	P					
Response Initiation								
Incident Classification	P		P	S	P			–
Escalation			P	P	P	S		
Emergency Action	P		P	P		S	S	P
Incident Response / Forensics Collection								
Mobilization	S	P	S	P	P	S	S	S
Investigation	S	P	P	S	P	P	S	S
Containment	P	P	S	S	P	P	P	S
Incident Recovery / Forensics Analysis								
Recovery Planning		S	S	S	P	P	P	S/P
Restoration		S	S	S	P	P	P	S
System Upgrade		S	S	S	P	P	P	S
Incident Closure / Forensics Reporting								
Summary Report		P	S	S	S	P	S	
Mitigations / Reporting			P	P	P	P	S	S
System Upgrade	P		P	P	P	P	S	

QUESTIONS

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