Metropolitan Washington Council Of Governments June 13, 2017

Cybersecuring Control Systems

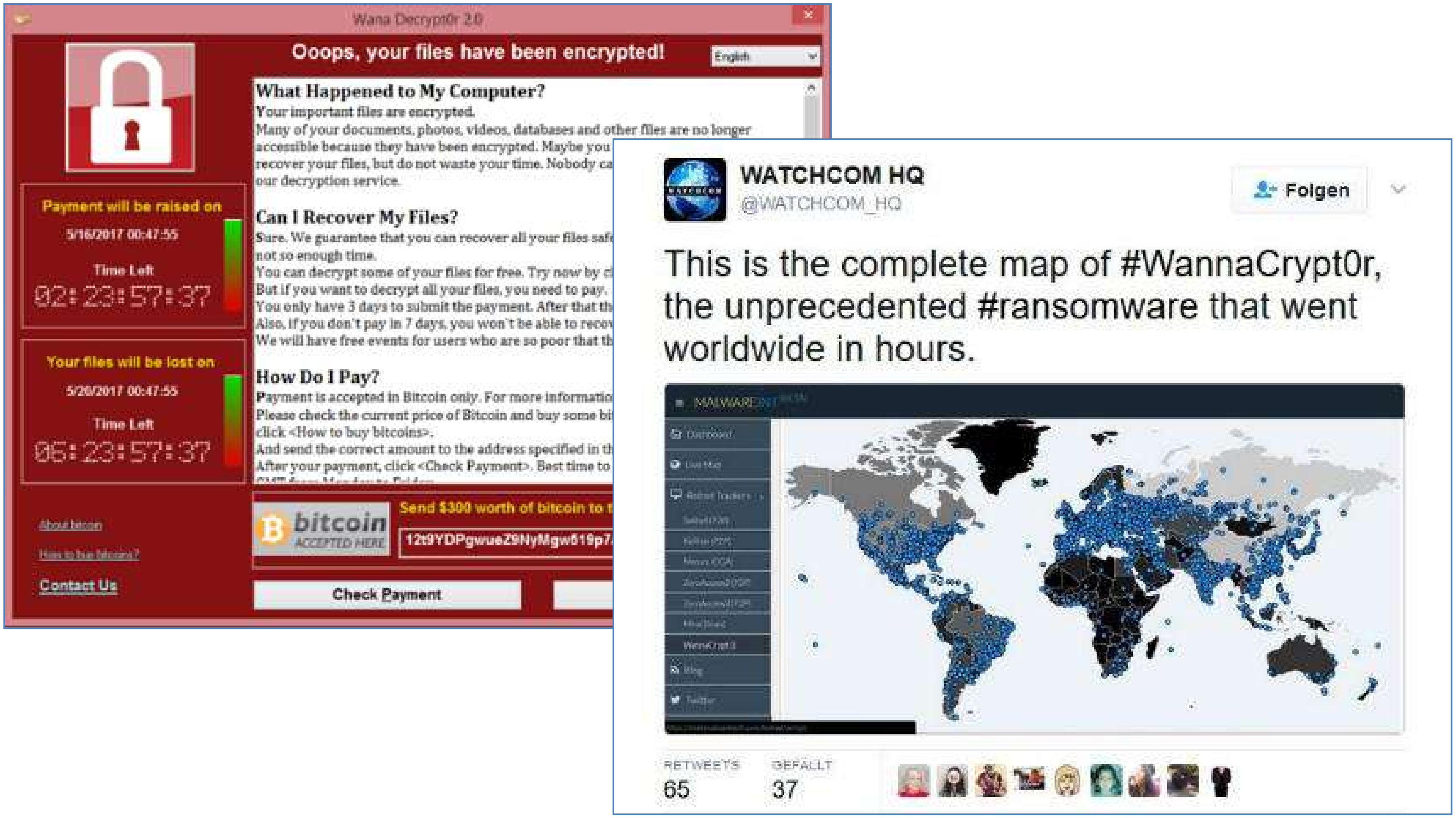
The PMC Group LLC
Engineering a better tomorrow today

Chinook
Secure · Compliant · Efficient

Overview

- Overview of Control Systems and Protocols
- Attack Sequences and Exploitation Vectors
- DHS US-CERT and ICS-CERT
- NIST SP 800-53 and SP 800-82
- UFC Cybersecuring Facility-Related Control Systems
- DoD ESTCP Cybersecurity Guidelines
- Tools – CSET, Diggity, Belarc, Kali, Samurai, GlassWire, WhiteScope
- DoD Advanced Cyber Industrial Control Systems Tactics, Techniques and Procedures
- Cybersecuring Control Systems Workshop

WannaCry(pt) Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you recover your files, but do not waste your time. Nobody ca our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files saf not so enough time.

You can decrypt some of your files for free. Try now by cl

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that th

Also, if you don't pay in 7 days, you won't be able to recov

We will have free events for users who are so poor that th

How Do I Pay?

Payment is accepted in Bitcoin only. For more informatio

Please check the current price of Bitcoin and buy some bi click <How to buy bitcoins>.

And send the correct amount to the address specified in th

After your payment, click <Check Payment>. Best time to

Send $300 worth of bitcoin to t

12t9YDPgwueZ9NyMgw519p7

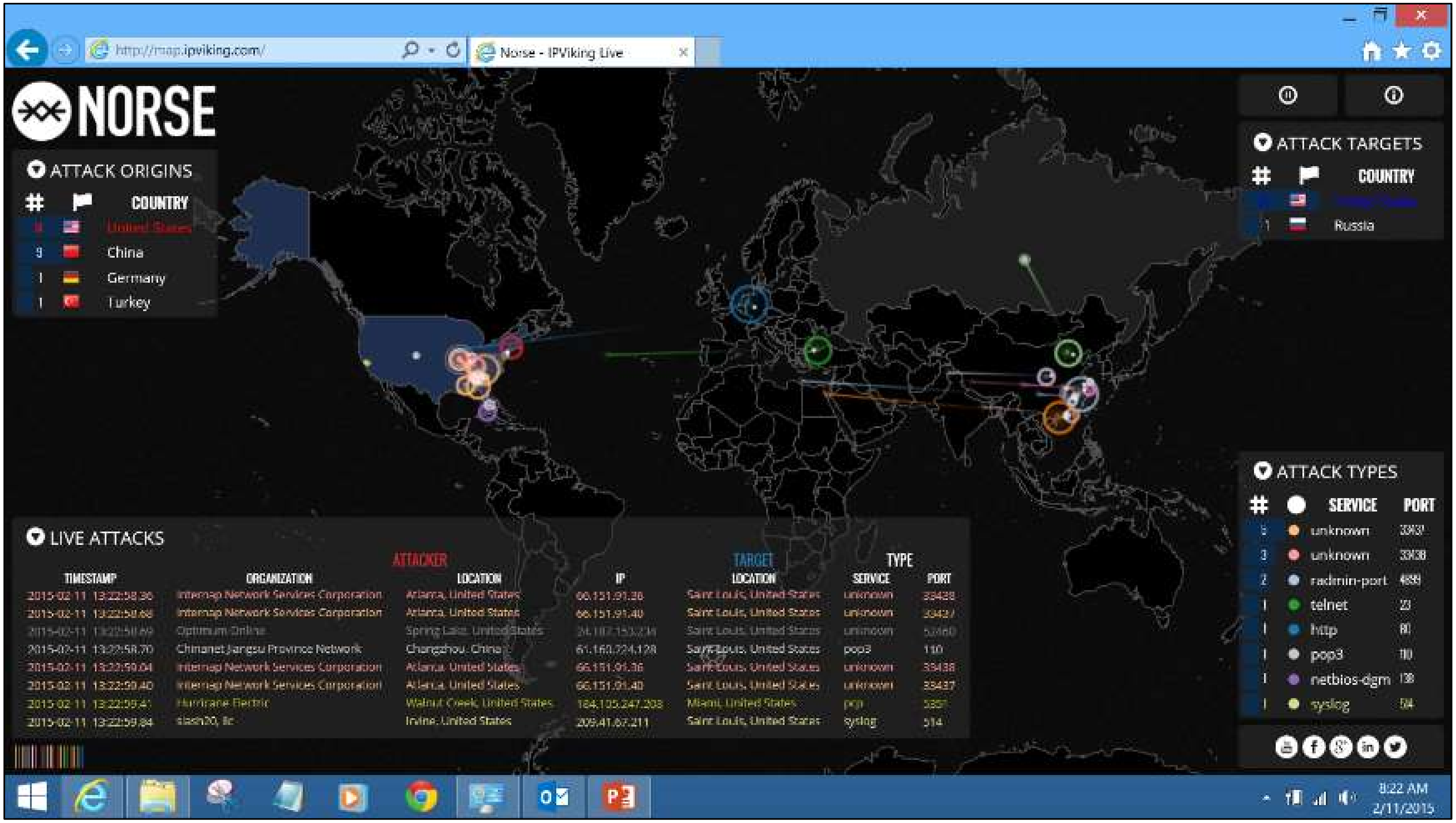
WATCHCOM HQ
@WATCHCOM_HQ

This is the complete map of #WannaCrypt0r, the unprecedented #ransomware that went worldwide in hours.

RETWEETS 65 GEFÄLLT 37

What will happen when the Control Systems are hit with malware/ransomware?

IP Viking



ATTACK ORIGINS

#	🏳	COUNTRY
[illegible]	🇺🇸	United States
9	🇨🇳	China
1	🇩🇪	Germany
1	🇹🇷	Turkey

ATTACK TARGETS

#	🏳	COUNTRY
[illegible]	🇺🇸	[illegible]
1	🇷🇺	Russia

ATTACK TYPES

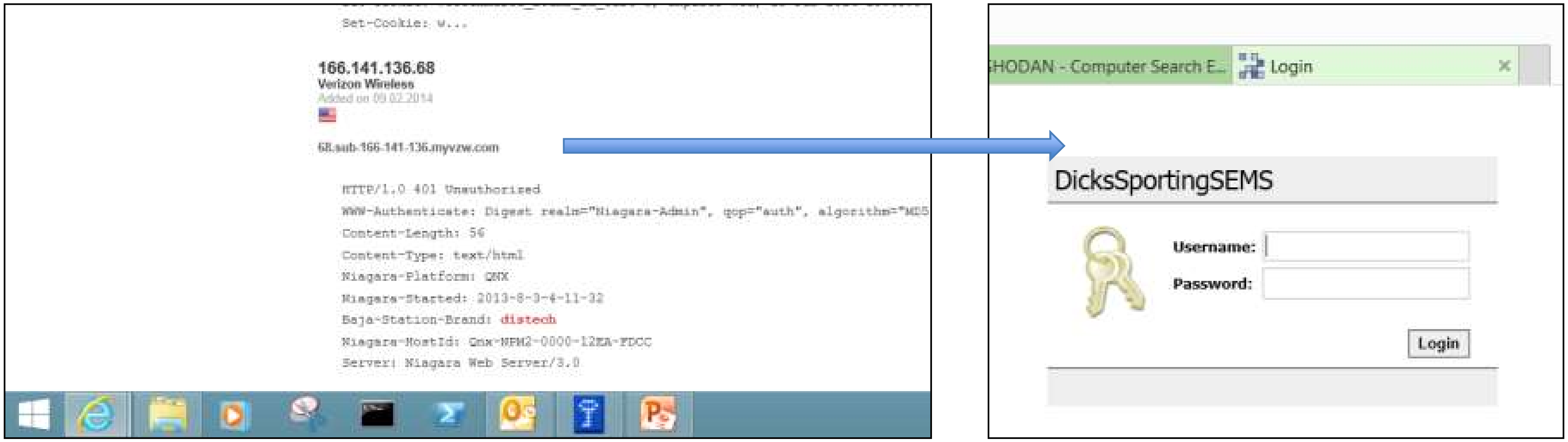
#	●	SERVICE	PORT
5	●	unknown	33437
3	●	unknown	33438
2	●	radmin-port	4899
1	●	telnet	23
1	●	http	80
1	●	pop3	110
1	●	netbios-dgm	138
1	●	syslog	514

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-02-11 13:22:58.36	Internap Network Services Corporation	Atlanta, United States	66.151.91.36	Saint Louis, United States	unknown	33438
2015-02-11 13:22:58.68	Internap Network Services Corporation	Atlanta, United States	66.151.91.40	Saint Louis, United States	unknown	33427
2015-02-11 13:22:58.69	Optimum Online	Spring Lake, United States	24.187.153.234	Saint Louis, United States	unknown	52460
2015-02-11 13:22:58.70	Chinanet Jiangsu Province Network	Changzhou, China	61.160.224.128	Saint Louis, United States	pop3	110
2015-02-11 13:22:59.04	Internap Network Services Corporation	Atlanta, United States	66.151.91.36	Saint Louis, United States	unknown	33438
2015-02-11 13:22:59.40	Internap Network Services Corporation	Atlanta, United States	66.151.91.40	Saint Louis, United States	unknown	33437
2015-02-11 13:22:59.41	Hurricane Electric	Walnut Creek, United States	184.105.247.203	Miami, United States	pop	5357
2015-02-11 13:22:59.84	slash20, llc	Irvine, United States	209.41.67.211	Saint Louis, United States	syslog	514

http://map.ipviking.com/

Shodan – Distech Search

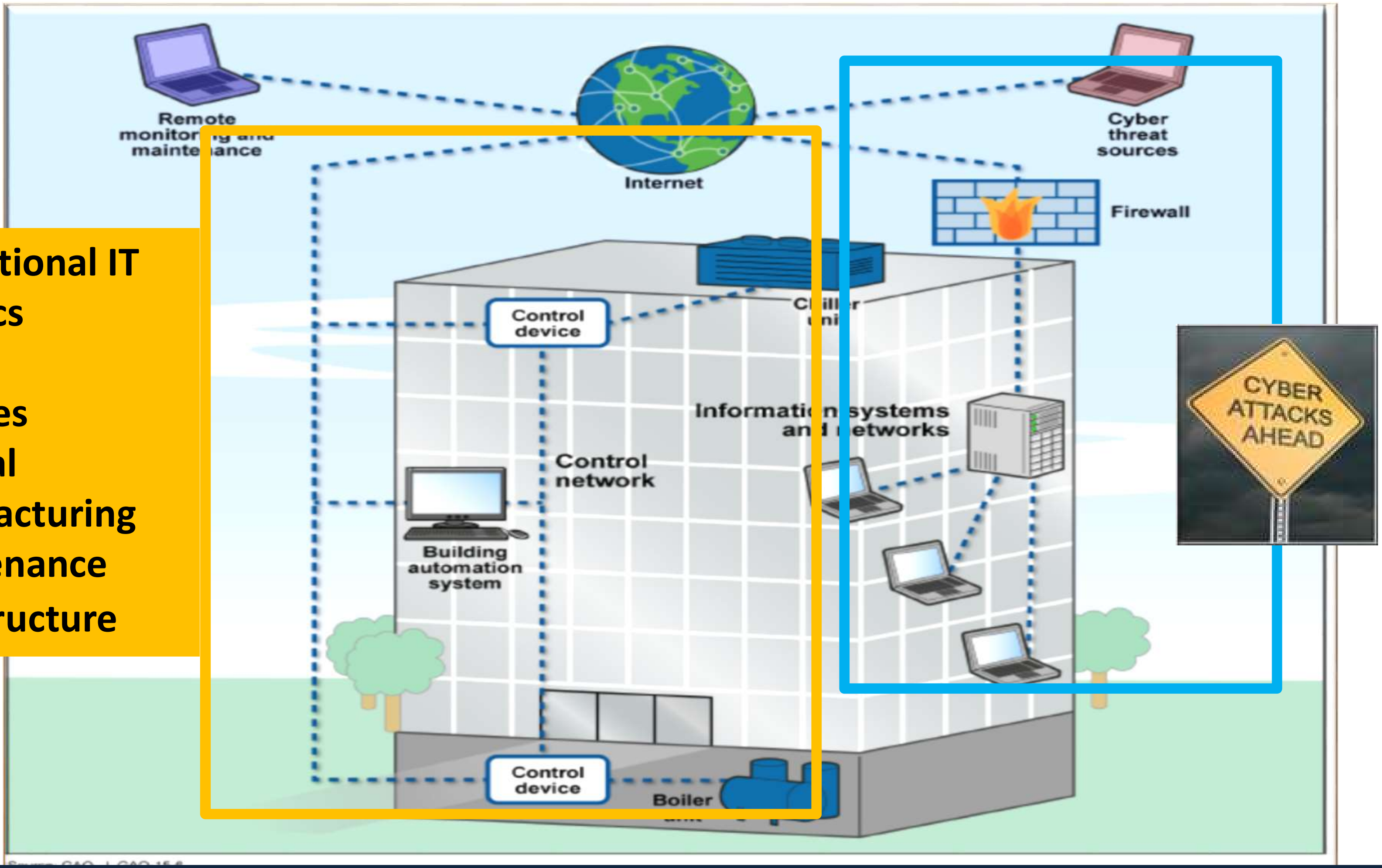


```
Set-Cookie: w...

166.141.136.68
Verizon Wireless
Added on 09.02.2014

68.sub-166-141-136.myvzw.com

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32
Baja-Station-Brand: distech
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC
Server: Niagara Web Server/3.0
```

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="**Niagara-Admin**", qop="auth", algorithm="**MD5**", nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32
Baja-Station-Brand: **distech**
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC
Server: **Niagara Web Server/3.0**

Non-Traditional IT

- Logistics
- Fuel
- Facilities
- Medical
- Manufacturing
- Maintenance
- Infrastructure

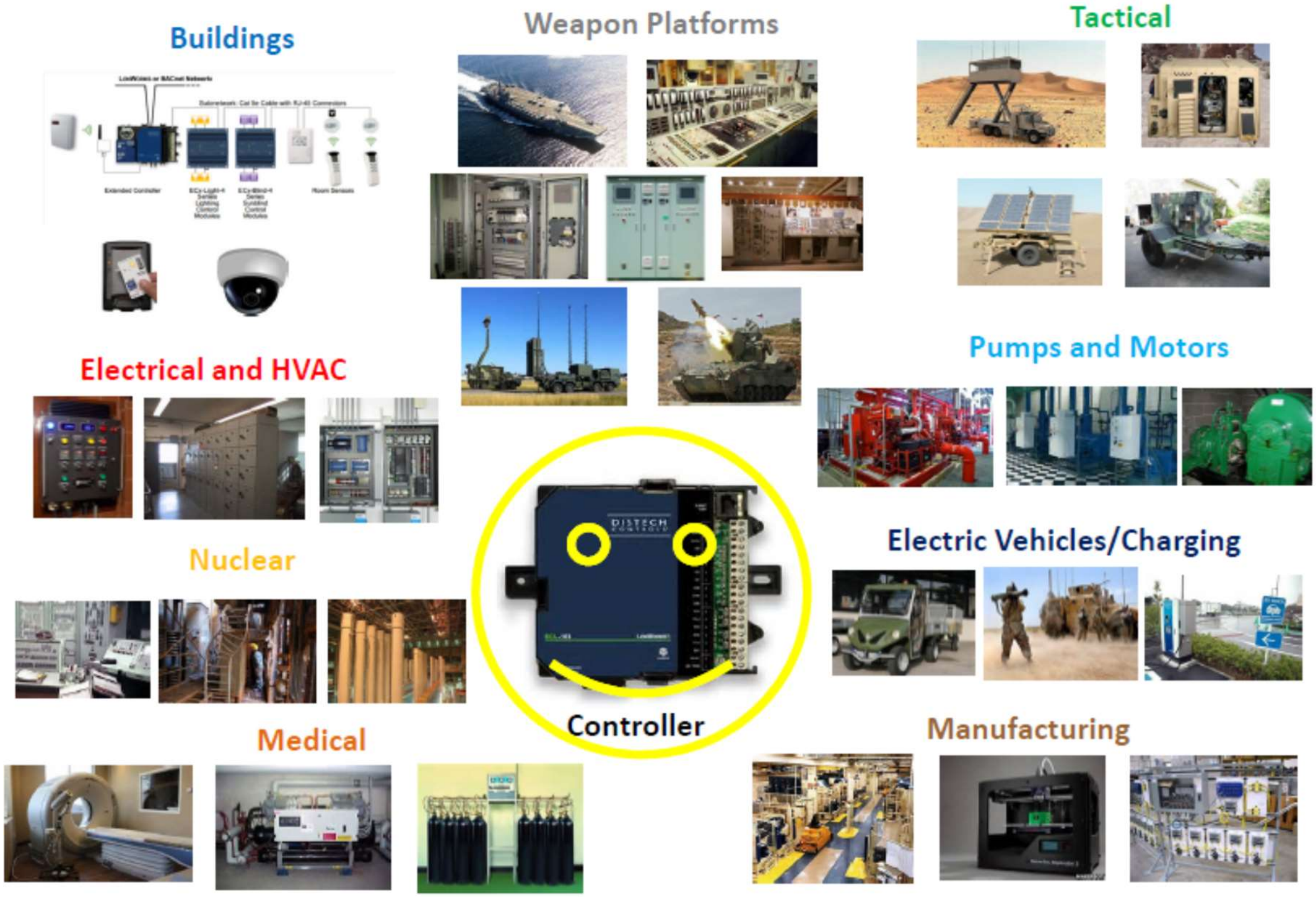


245 = Avg # Days Undiscovered Adversary

DHS ICS CERT

OT IP Based Controllers Are in Everything

UNCLASSIFIED



Weapon Platforms

Buildings

Tactical

Electrical and HVAC

Pumps and Motors

Nuclear

Controller

Electric Vehicles/Charging

Medical

Manufacturing

LonWorks or BACnet Network
Subnetwork: Cat 5e Cable with RJ-45 Connectors
Extended Controller
ECy-Light-4 Series Lighting Control Modules
ECy-Blind-4 Series Sunblind Control Modules
Room Sensors
DISTECH CONTROLS

Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

ASD EI&E Memo 31 Mar’16

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

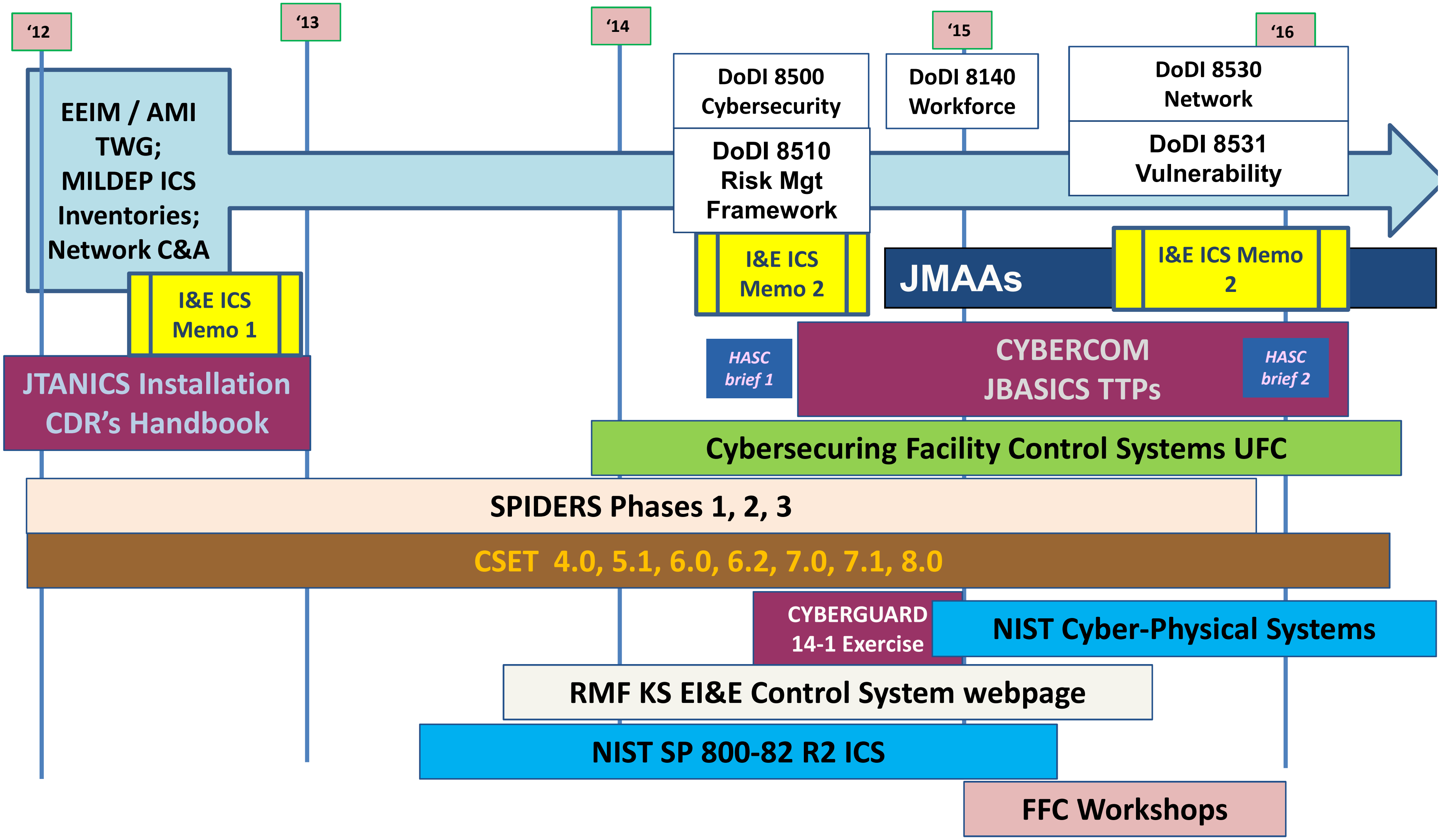
Plans received Feb’17

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

- Prioritize implementing cybersecurity controls on most critical facility-related control systems by end FY19

ONLY Applies to Facility-Related Control Systems

Broader DoD Control System Efforts



'12

'13

'14

'15

'16

EEIM / AMI TWG; MILDEP ICS Inventories; Network C&A

I&E ICS Memo 1

JTANICS Installation CDR's Handbook

DoDI 8500 Cybersecurity

DoDI 8510 Risk Mgt Framework

I&E ICS Memo 2

DoDI 8140 Workforce

DoDI 8530 Network

DoDI 8531 Vulnerability

JMAAs

I&E ICS Memo 2

HASC brief 1

CYBERCOM JBASICS TTPs

HASC brief 2

Cybersecuring Facility Control Systems UFC

SPIDERS Phases 1, 2, 3

CSET 4.0, 5.1, 6.0, 6.2, 7.0, 7.1, 8.0

CYBERGUARD 14-1 Exercise

NIST Cyber-Physical Systems

RMF KS EI&E Control System webpage

NIST SP 800-82 R2 ICS

FFC Workshops

Congressional Focus on Control Systems (1)

NDAA 17 SEC. 1650. Evaluation of Cyber Vulnerabilities of DoD Critical Infrastructure

NLT June 30 ’17 SECDEF, via a covered research laboratory, shall initiate a pilot program to shall assess **feasibility and advisability of applying new, innovative methodologies or engineering** approaches at 2+ installations supporting critical mission-essential functions:

(A) improve the **defense of control systems** against cyber attacks;

(B) increase the **resilience of military installations against cybersecurity threats;**

(C) **prevent or mitigate** the potential for high-consequence cyber attacks; and

(D) **inform future requirements** for the development of such control systems.

NDAA 17 SEC. 1644. (c) Joint Standard for Protection of Control Systems

NLT June 30 ‘17, SECDEF shall issue a **joint training and certification standard for the protection of control systems for use by all cyber operations forces** within DoD.

(1) provide for applied training and exercise capabilities; and

(2) use expertise & capabilities from other departments and agencies of the FedGovt

Congressional Focus on Control Systems (2)

NDAA 17 Report 114-255 TITLE XXVIII—Military Construction General Provisions

DoD transitioning to smart buildings, higher connectivity enables increased vulnerabilities, provide report NLT 30 June '17 that:

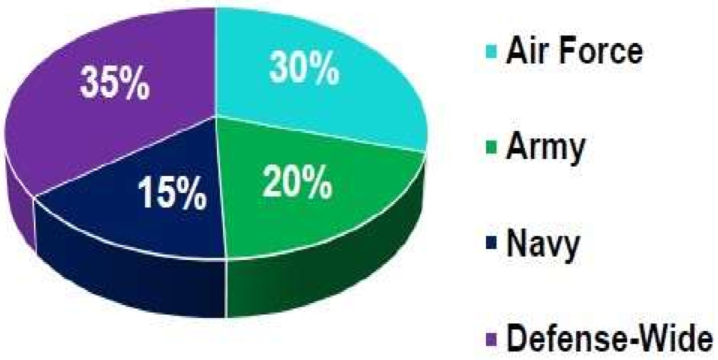
1) Delineates **risks inherent in control systems and networks,** and the potential consequences associated with a system compromise through a cyber event;
2) Assesses current **vulnerabilities to cyber attack** initiated through Industrial Control Systems (ICS) at DoD installations worldwide, for the purpose of **determining risk mitigation actions for current and future implementation;**
3) Proposes a **common, Dept wide implementation plan** to upgrade and improve the security of control systems and networks to mitigate identified risks;
4) Assesses DoD military **construction directives, regulations, and instructions require the consideration of cybersecurity vulnerabilities** and cyber risk in preconstruction design processes and requirements development processes for military construction projects;
5) Capabilities of USACE, NAVFAC, AFCEC, and others to **identify and mitigate full-spectrum cyber-enabled risk to new facilities and major renovations.**

DoD FY17 PB Request for Cybersecurity Overall

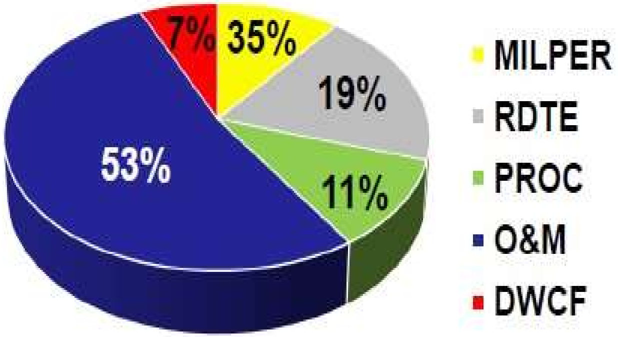
($M)	FY16En	FY17	
Air Force	1,545.6	1,990.5	+28%
Army	945.1	1,329.6	+41%
Navy	950.2	1,038.2	+9%
Defense-Wide	2,300.8	2,375.4	+3%
Total	5,741.7	6,733.7	+17%

($M)	FY16 En	FY17	
MILPER	637.3	713.3	+12%
RDTE	1,062.9	1,299.1	+22%
PROC	587.7	725.2	+23%
O&M	2,992.0	3,545.1	+18%
DWCF	462.2	451.0	-2%

FY17



FY17



CYBERSECURITY BUDGET INCREASES AS THE PRIORITY INCREASES

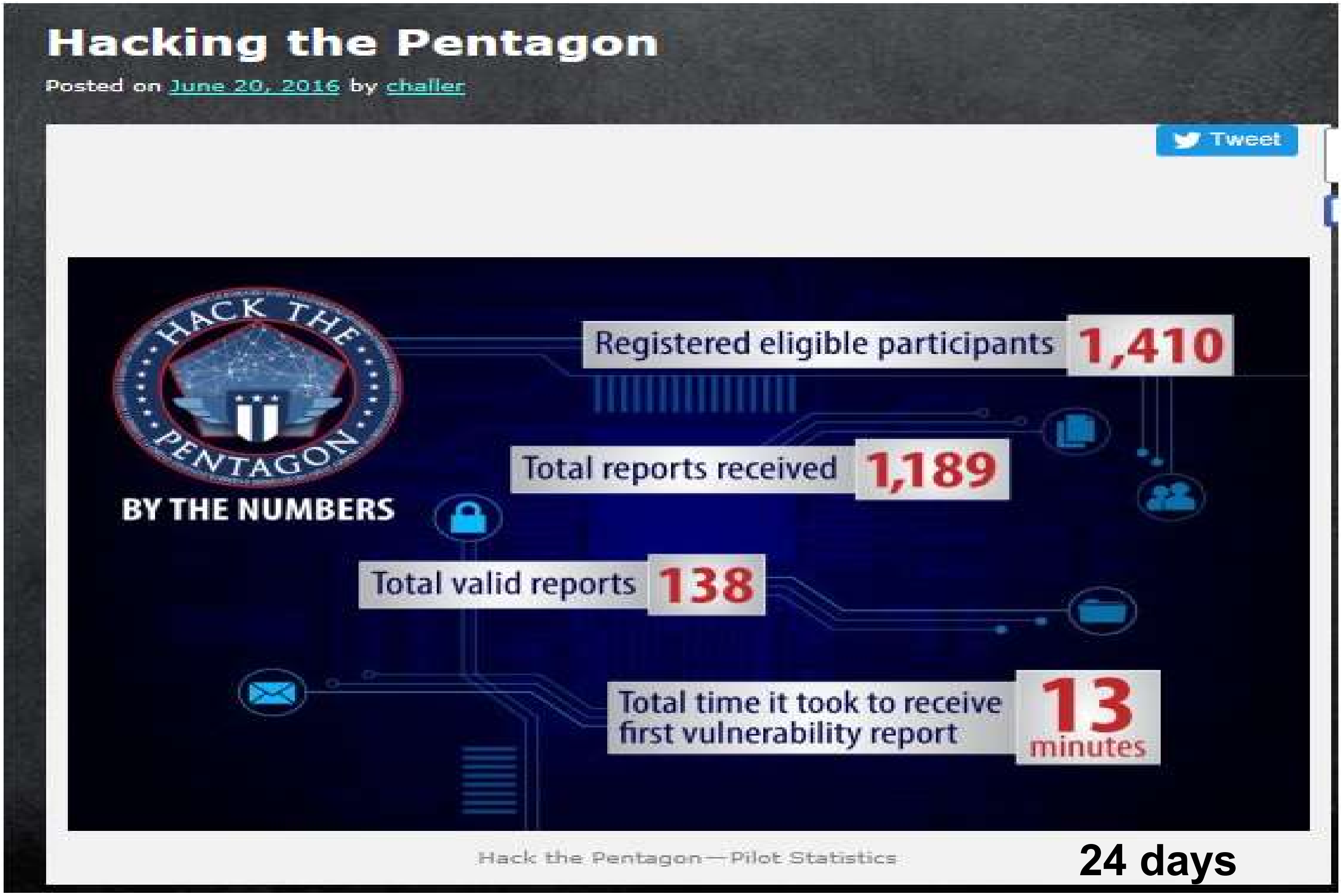
2017

$2B

requested for cybersecurity procurement and RDT&E

MILPER:	Military Personnel
RDTE:	Research, Development, Test and Evaluation
PROC:	Procurement
O&M:	Operations and Maintenance
DWCF:	Defense Working Capital Fund

Embracing Silicon Valley Crowdsourcing:
“Bug Bountys” *Will Control Systems ICS be Next*?



Hacking the Pentagon

Posted on June 20, 2016 by challer

HACK THE PENTAGON

BY THE NUMBERS

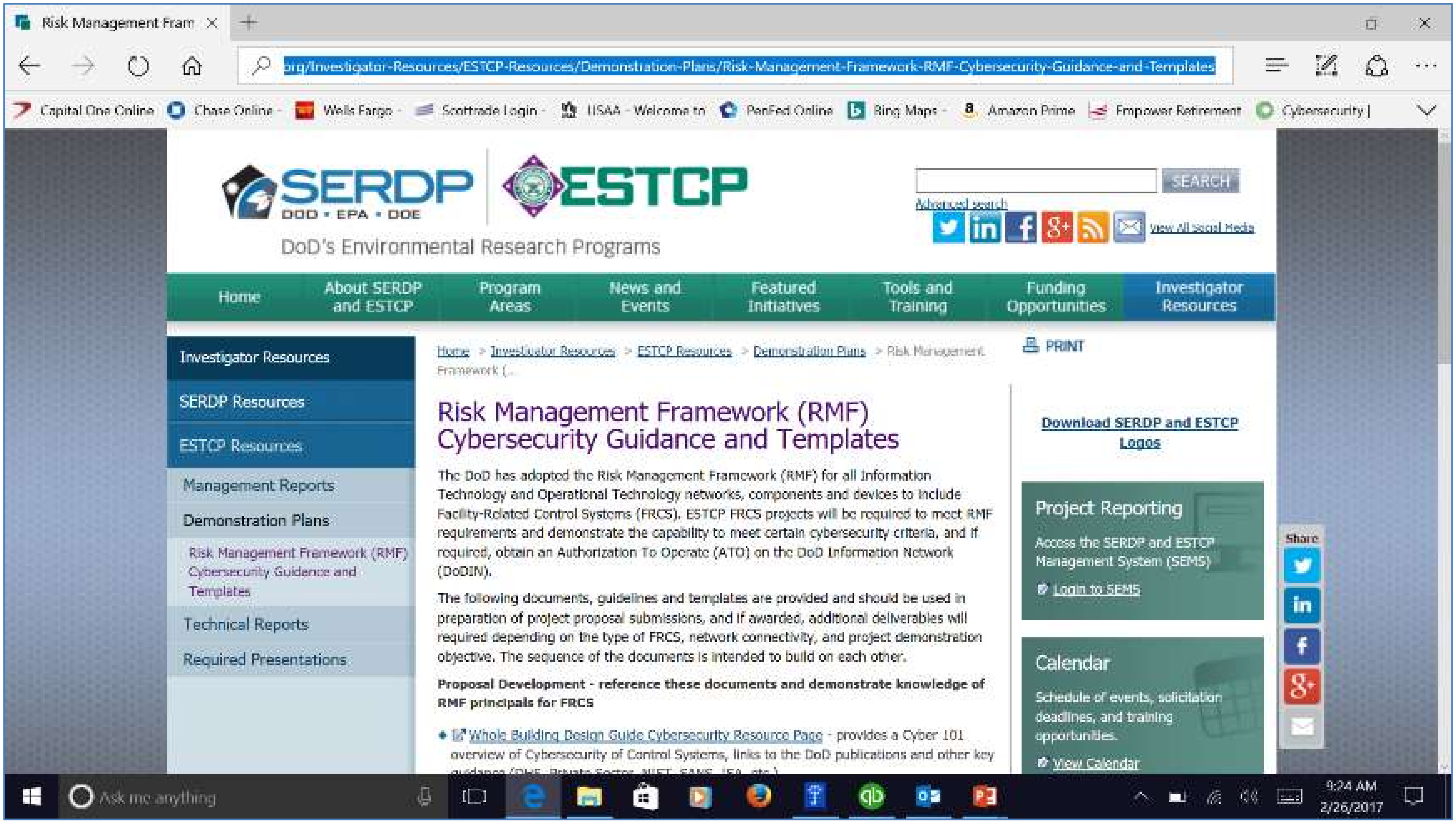
Registered eligible participants	1,410
Total reports received	1,189
Total valid reports	138
Total time it took to receive first vulnerability report	13 minutes

Hack the Pentagon — Pilot Statistics

24 days

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

ESTCP RMF FRCS Guidance and Templates



Risk Management Framework (RMF) Cybersecurity Guidance and Templates

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

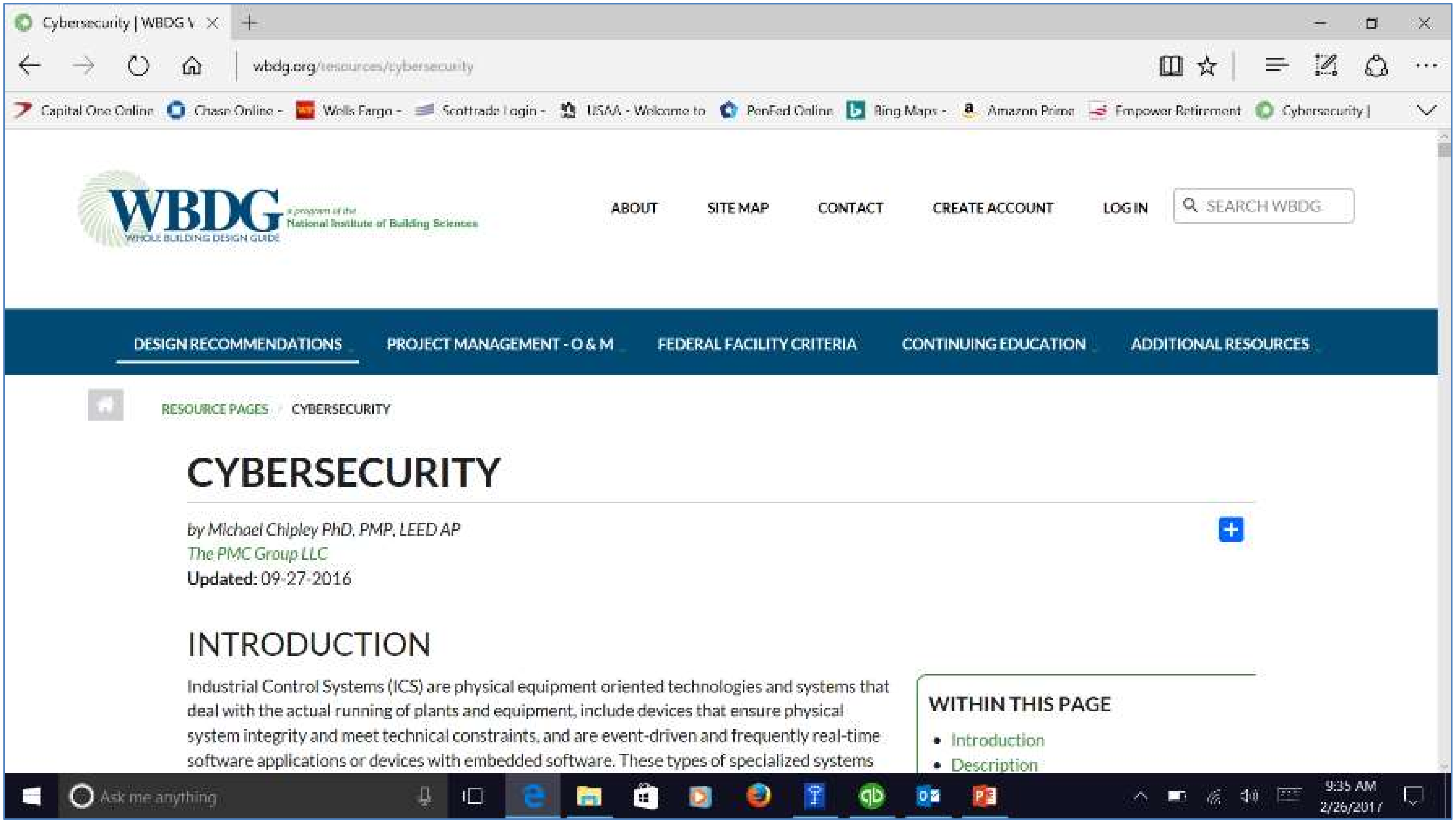
The following documents, guidelines and templates are provided and should be used in preparation of project proposal submissions, and if awarded, additional deliverables will required depending on the type of FRCS, network connectivity, and project demonstration objective. The sequence of the documents is intended to build on each other.

Proposal Development - reference these documents and demonstrate knowledge of RMF principals for FRCS

- Whole Building Design Guide Cybersecurity Resource Page - provides a Cyber 101 overview of Cybersecurity of Control Systems, links to the DoD publications and other key guidance (DHS, Private Sector, NIST, SANS, ISA, etc.)

https://www.serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Risk-Management-Framework-RMF-Cybersecurity-Guidance-and-Templates

WBDG Cybersecurity Resource Page



CYBERSECURITY

by Michael Chipley PhD, PMP, LEED AP
The PMC Group LLC
Updated: 09-27-2016

INTRODUCTION

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems

WITHIN THIS PAGE

- Introduction
- Description

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

Client-Server and Cloud Architectures

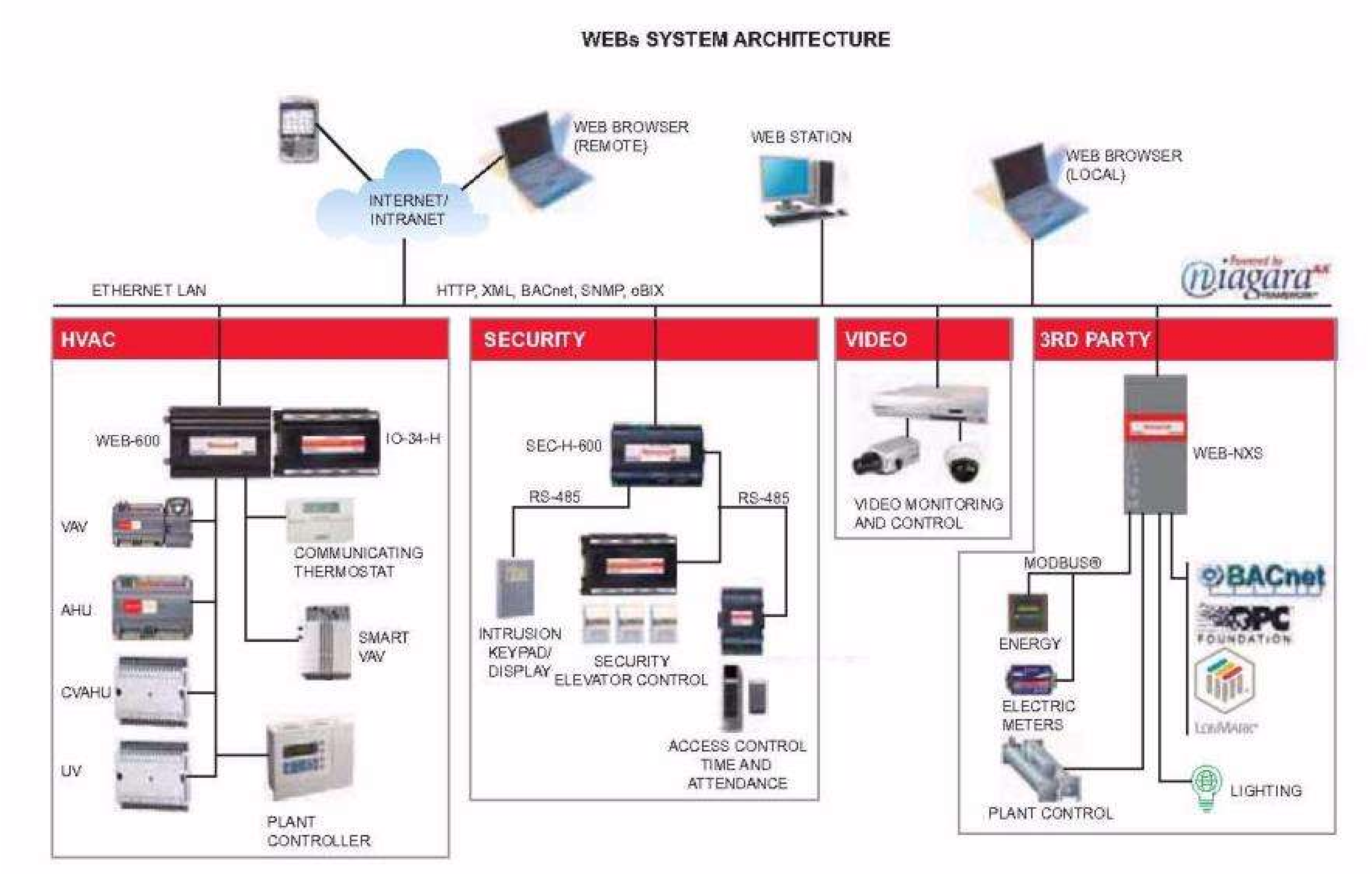
Traditional FRCS Client-Server Architecture

- Vast majority of FRCS are organization owned client-server architecture
- Systems can last 15-20 years
- Probably 80% or more of the legacy systems are running Windows 95, XP, CE
- Many have hardcoded passwords or no passwords at device level
- Level 4 servers and workstations can be virtualized, and some Level 3 FPOC's controllers can support some logging

Cloud Architectures

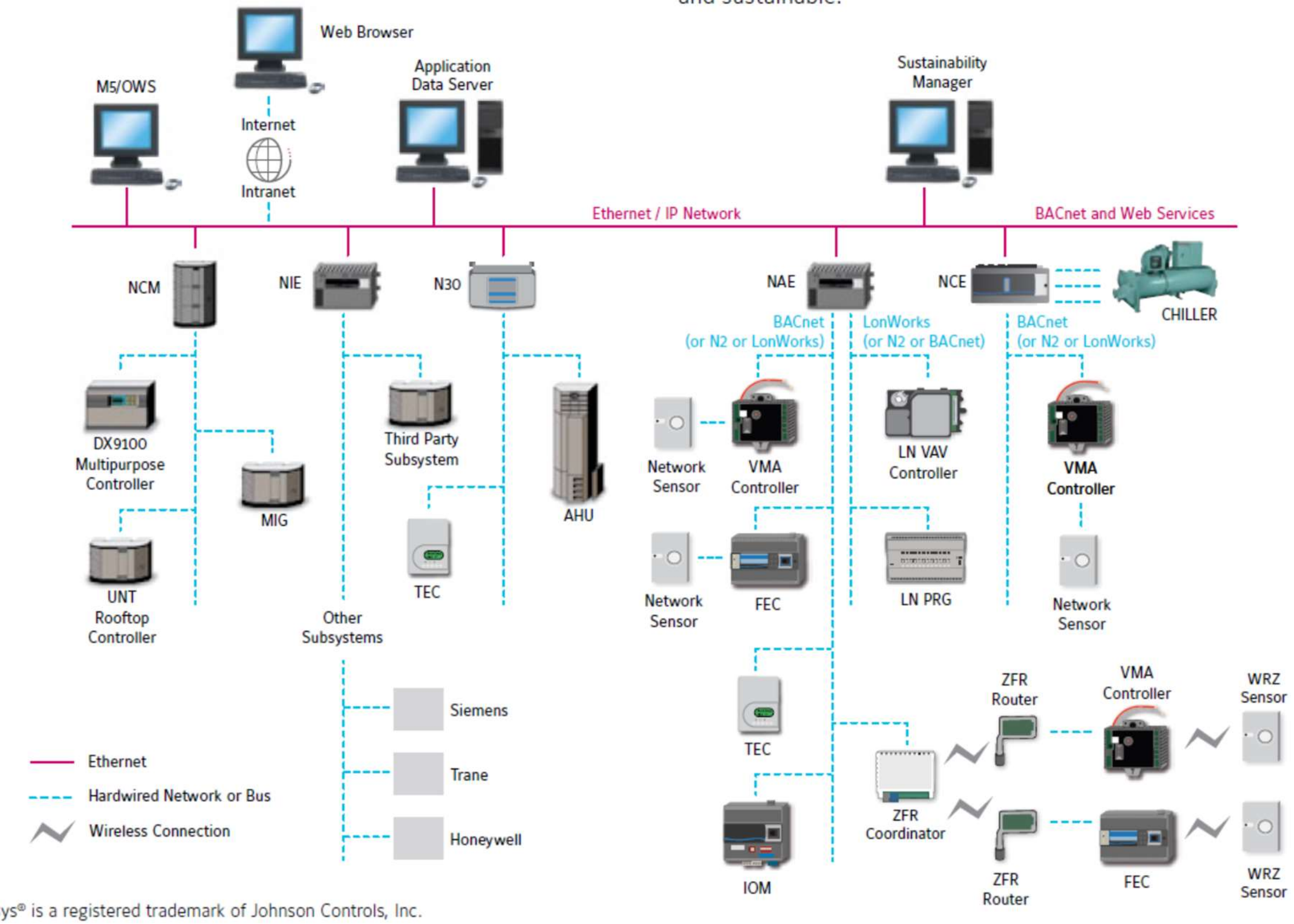
- Smart buildings/cities are moving to cloud architectures at a rapid pace
- Manages the building functions, energy, tenant data very efficiently
- Controllers still need to be in the Levels 3-0 physical space; Level 4 can be in cloud space
- Cloud security is typically much better than organization owned client-server architecture; they follow NIST RMF, conduct continuous monitoring, multi-factor authentication can be enabled
- If network connectivity is lost, controllers default to safe mode

Tridium Architecture



Johnson Controls Architecture

and sustainable.



Metasys® is a registered trademark of Johnson Controls, Inc.

System & Terminal Unit Controllers, Actuators

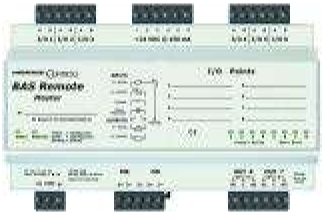
JACE

Field Server

iLon Smart Server

VAV

L-switch



BAS Remote Server

Valve Actuator

Valve Actuator

Pressure Sensor

Temperature Sensor

Analog voltage, resistance, current signal is converted to digital and then IP

Control System Protocols (1)

Internet Protocols

- IPv4 and IPv6
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP) - Port 80
- Hypertext Transfer Protocol Secure (HTTPS) - Port 443
- Simple Mail Transfer Protocol – Port 587

Open Control Systems Protocols

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1628/29
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- ZigBee - Peer to Peer
- Bluetooth – Master/Slave
- HART: Peer to Peer – Port 5094

Proprietary Control Systems Protocols

- Tridium NiagraAX/Fox
- Johnson Metasys N2
- OSISoft Pi System
- Many others…

Control System Protocols (2)

Control systems are fundamentally different than IT

- Can be based on Master and Slaves or Peer to Peer
- Slaves have Registers and Coils
- Devices use several different programming languages to perform operations
- Not originally designed for security or encryption

Master = Client : sends requests for values in the address
Slave = Server : replies with data
Registers and Coils = memory locations

Typical file extensions:
*.ACD
*.CXP
*.ESD
*.ESX
*.LDA
*.LCD
*.LDO
*.LCX
*.plcproject
*.PRJ
*.PRT
*.RSP
*.QXD
*.SCD

Attack Processes

SANS Process

- Reconnaissance
- Scanning
- Intrusion Detection System (IDS) evasion
- Network-Level attacks
- Gathering and parsing packets
- Operating System and application-level attacks
- Netcat: The attacker's best friend
- Password cracking
- Web application attacks
- Denial of service attacks
- Maintaining access
- Covering the tracks

http://www.sans.org/course/hacker-techniques-exploits-incident-handling

Root9b Process (Advanced Workshop)

- Footprinting
- Scanning
- Enumeration
- Network Mapping
- Gaining Access
- Privilege Escalation
- Post Exploitation
- Target Survey & Remote Forensics Analysis
- Cover Tracks (cleanup)
- Data Collection
- Rootkit (aka Backdoor, aka Implant, aka Persistence)
- Computer Network Attack

Attack Sequence (1)

Footprinting: This is the process of ***conducting target analysis, identification, and discovery***; typically through the use of open source tools. This includes dumpster diving, social engineering and the use of utilities such as web-search hacking, traceroutes, pings, network lookups, etc.

Scanning: This step will take the findings from footprinting and begin to drill-down a bit further. In a traditional sense, this step includes ***port scanning, OS identification, and determining whether or not a machine is accessible***.

Enumeration: This is the phase where you further interrogate specific services to determine exact operating systems, software, etc. Normal enumeration techniques include searching for ***network share information, specific version of applications running, user accounts, SNMP traffic***, etc.

Network Mapping: This step is exactly as the name implies, laying out an illustration of the targeted network. This includes taking all available resources (logs, target surveys, etc) to ***create a visualization of the target environment***. This often looks different from the exploiters perspective then from the Admin's perspective. Depending on the scope of activities being conducted this step may or may not be necessary.

Attack Sequence (2)

Gaining Access: This step is the exploitation process. Basically, this is gaining ***access to the machine or the network by a client-side exploit, insider threat, supply interdiction attack, or remote exploitation opportunity***. This could be conducted via spear-fishing attacks, buffer overflows, embedded device exploitation, credential masquerade attacks, etc.

Privilege Escalation: Depending on the exploitation opportunity which was used the attacker may need to elevate privileges to a different user. There are various different scenarios in which the attacker will need to use this procedure. Typically, this is conducted through the use of a ***local exploit opportunity in order to gain root or system-level privileges – the highest possible user***.

Attack Sequence (3)

Post Exploitation: This step is really a compilation of many steps and is dependent upon the objective of the mission. This step could include any combination or all of the following examples;

- ✓ Target Survey & Remote Forensics Analysis
- ✓ Cover Tracks (cleanup)
- ✓ Data Collection
- ✓ Rootkit (aka Backdoor, Implant, Persistence)
- ✓ Computer Network Attack (the 6 D’s)
  - ✓ Disrupt
  - ✓ Deny
  - ✓ Degrade
  - ✓ Deceive
  - ✓ Destroy
  - ✓ Delay

Attack Sequence (4)

Target Survey & Remote Forensics Analysis: This step is to conduct analysis on the target machine for potential security mechanisms, files, or users which could either assist in obtaining the objective or harm the assessment. This is the ***process of analysing the targets operating environment***.

Cover Tracks (cleanup): This step is the process ***of removing any forensically relevant residue that was left behind as the result of exploitation or presence***. This is one of the most important steps that a ***hacker can perform to maintain stealth***. This is often one of the most important opportunities for ***defenders to profile an attacker***.

Data Collection: The attacker is in the network to perform some activity. Usually, this is not to show Cyber prowess, but instead to ***extract as much data as possible***. ***Network traffic analysis is key*** during this phase.

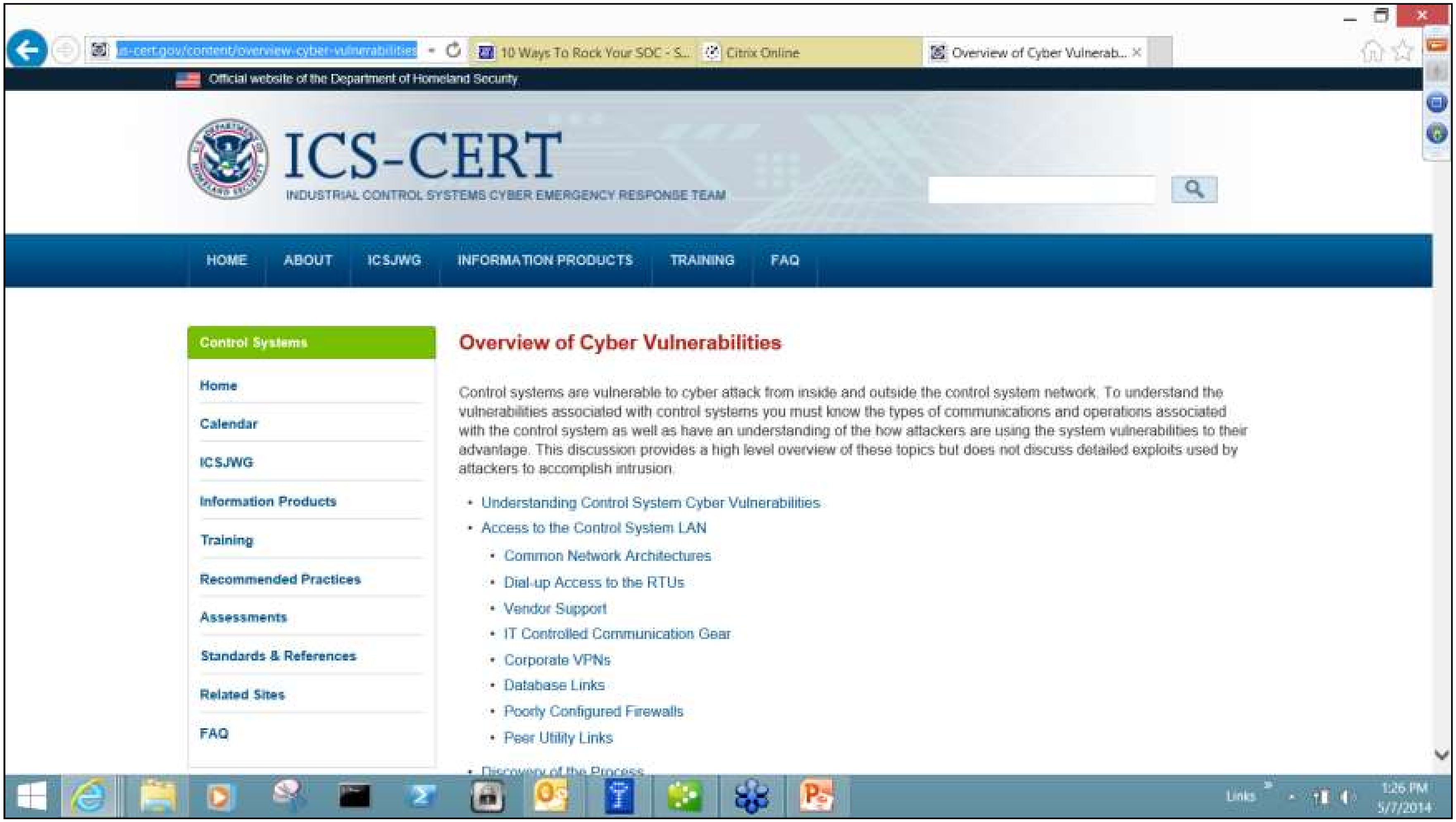
Rootkit (aka Backdoor, aka Implant, aka Persistence): This step is the process of ***installing an application, hooking the kernel, or laying down some mechanism which allows the attacker to maintain continued access*** to the host or network. If the implant is well designed, the attacker can live in your network for extended periods of time.

Attack Sequence (5)

Computer Network Attack. In this step the attacker has already identified the network as a target of opportunity and has identified plans to launch an attack. This attack could be remote or local in nature and could come from already established access or with no access to the targeted environment. The attacker will ***typically identify core and vital network processes and perform various attacks to disrupt, deny, degrade, destroy, or deceive their "adversary.***"

The most sophisticated attackers would likely obtain access to the target environment. After obtaining access to the critical infrastructure, techniques will be utilized to achieve the 6D's of Computer Network Attack.

Control System Vulnerabilities



us-cert.gov/content/overview-cyber-vulnerabilities
10 Ways To Rock Your SOC - S...
Citrix Online
Overview of Cyber Vulnerab...
Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ
Links
1:26 PM
5/7/2014

Overview of Cyber Vulnerabilities

Control systems are vulnerable to cyber attack from inside and outside the control system network. To understand the vulnerabilities associated with control systems you must know the types of communications and operations associated with the control system as well as have an understanding of the how attackers are using the system vulnerabilities to their advantage. This discussion provides a high level overview of these topics but does not discuss detailed exploits used by attackers to accomplish intrusion.

- Understanding Control System Cyber Vulnerabilities
- Access to the Control System LAN
  - Common Network Architectures
  - Dial-up Access to the RTUs
  - Vendor Support
  - IT Controlled Communication Gear
  - Corporate VPNs
  - Database Links
  - Poorly Configured Firewalls
  - Peer Utility Links
- Discovery of the Process

http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Control System Exploitation Vectors

Access to the Control System LAN

- Common Network Architectures
- Dial-up Access to the RTUs
- Vendor Support
- IT Controlled Communication Gear
- Corporate VPNs
- Database Links
- Poorly Configured Firewalls
- Peer Utility Links

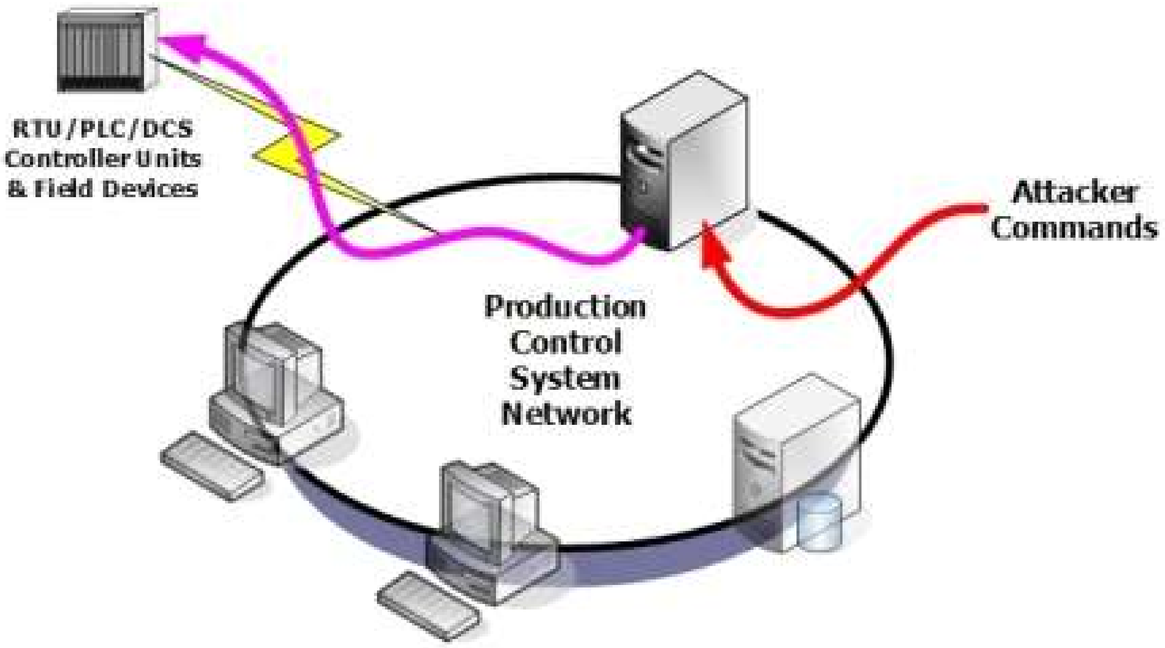
Discovery of the Process

- Details of how the process is implemented to surgically attack it
- Find the points in the data acquisition server database and the HMI display screens

Control of the Process

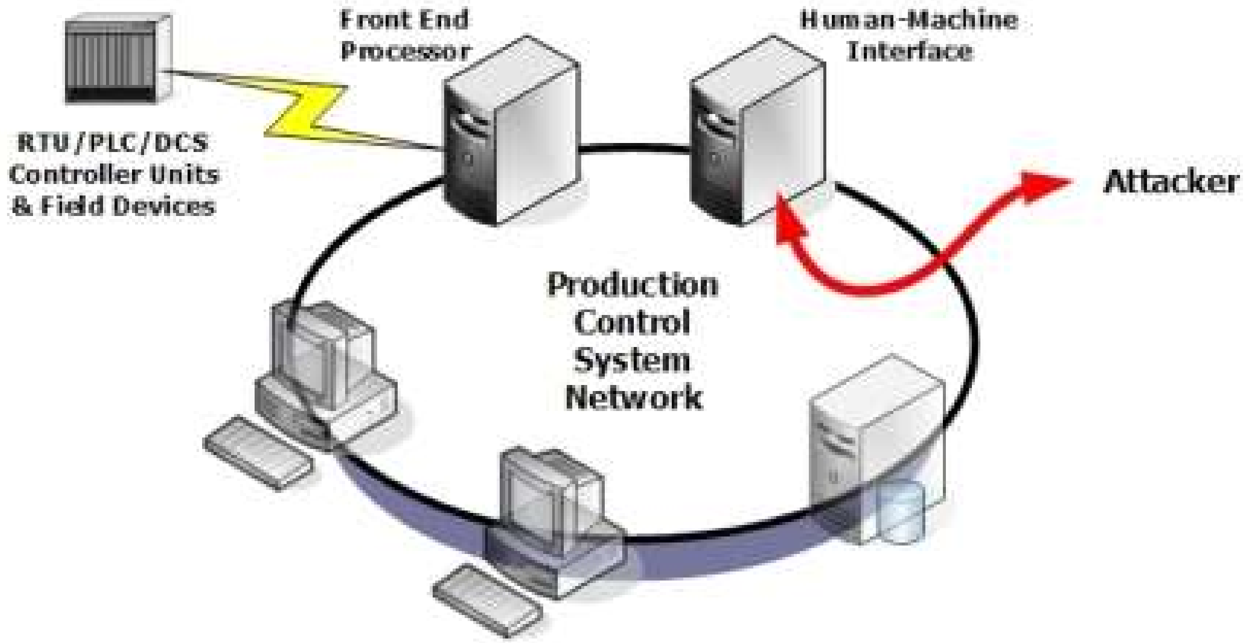
- Sending Commands Directly to the Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks

Sending Commands Directly



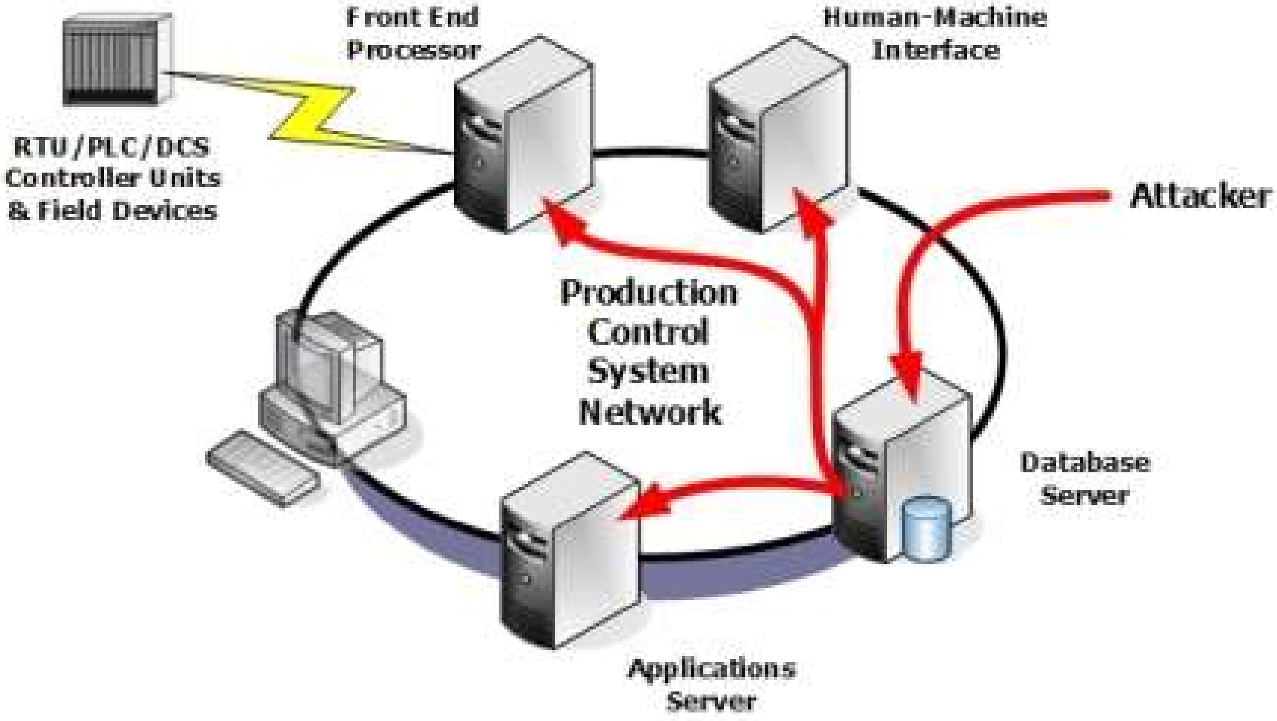
The easiest way to control the process is to send commands directly to the data acquisition equipment. **Most PLCs, protocol converters, or data acquisition servers lack even basic authentication. They generally accept any properly formatted command.** An attacker wishing control simply establishes a connection with the data acquisition equipment and issues the appropriate commands.

Exporting the HMI Screen



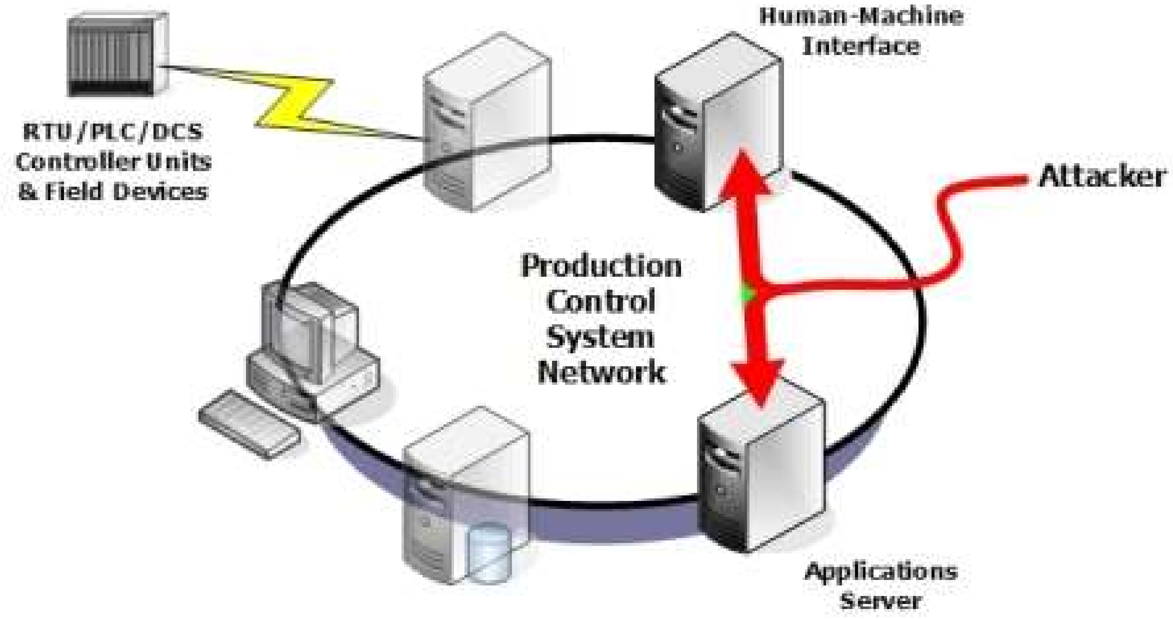
An effective attack is to export the screen of the operator's HMI console back to the attacker (see Figure 14). Off-the-shelf tools can perform this function in both Microsoft Windows and Unix environments. **The operator will see a "voodoo mouse" clicking around on the screen unless the attacker blanks the screen.** The attacker is also limited to the commands allowed for the currently logged-in operator. For instance, he probably could not change the phase tap on a transformer.

Changing the Database



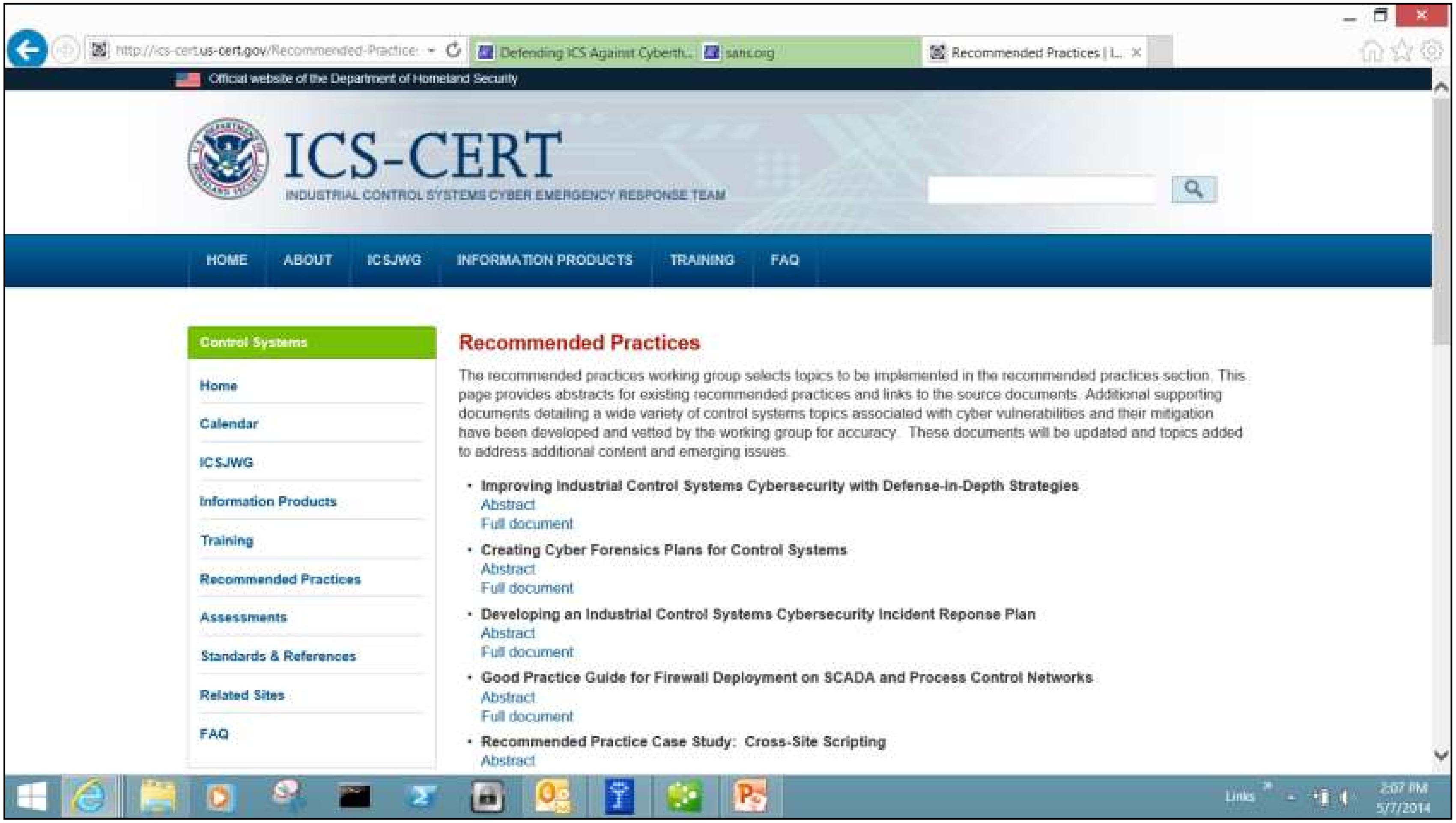
In some, but not all, vendor's control systems, **manipulating the data in the database can perform arbitrary actions on the control system**

Man-in-the Middle Attacks



Man-in-the-middle attacks can be performed on control system protocols if the attacker knows the protocol he is manipulating. **An attacker can modify packets in transit, providing both a full spoof of the operator HMI displays and full control of the control system (see Figure 16). By inserting commands into the command stream the attacker can issue arbitrary or targeted commands.** By modifying replies, the operator can be presented with a modified picture of the process.

Defending – DHS Recommended Practices



http://ics-cert.us-cert.gov/Recommended-Practice:
Defending ICS Against Cyberth...
sans.org
Recommended Practices | I...
Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ
Links
2:07 PM
5/7/2014

Recommended Practices

The recommended practices working group selects topics to be implemented in the recommended practices section. This page provides abstracts for existing recommended practices and links to the source documents. Additional supporting documents detailing a wide variety of control systems topics associated with cyber vulnerabilities and their mitigation have been developed and vetted by the working group for accuracy. These documents will be updated and topics added to address additional content and emerging issues.

- **Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies**
  Abstract
  Full document
- **Creating Cyber Forensics Plans for Control Systems**
  Abstract
  Full document
- **Developing an Industrial Control Systems Cybersecurity Incident Reponse Plan**
  Abstract
  Full document
- **Good Practice Guide for Firewall Deployment on SCADA and Process Control Networks**
  Abstract
  Full document
- **Recommended Practice Case Study: Cross-Site Scripting**
  Abstract

Five Key Countermeasures (1)

1. Security policies*. **Security policies*** should be developed for the control systems network and its individual components, but they should be ***reviewed periodically*** to incorporate the current threat environment, system functionality, and required level of security.

2. Blocking access to resources and services. This technique is generally employed on the ***network through the use of perimeter devices with access control lists*** such as firewalls or proxy servers. It can be enabled on the host via host-based firewalls and antivirus software.

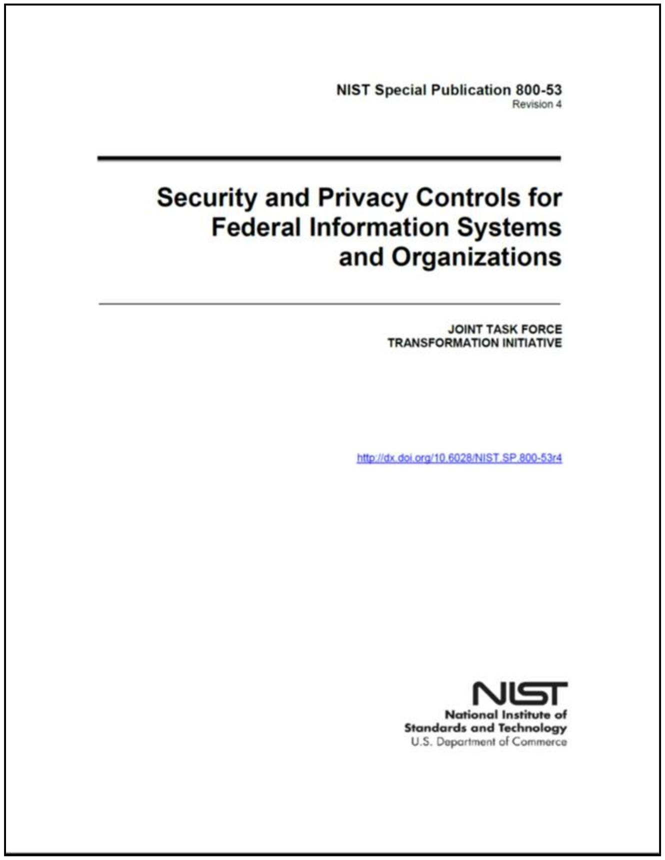
3. Detecting malicious activity. Detection activities of malicious activity can be networked or host-based and ***usually require regular monitoring of log files by experienced administrators***. IDS are the common means of identifying problems on a network, but can be deployed on individual hosts as well. Auditing and event logs should be enabled on individual hosts when possible.

Five Key Countermeasures (2)

4. Mitigating possible attacks. In many cases, vulnerability may have to be present because removal of the vulnerability may result in an inoperable or inefficient system. ***Mitigation allows administrators to control access to vulnerability in such a fashion that the vulnerability cannot be exploited***. Enabling technical workarounds, establishing filters, or running services and applications with specific configurations can often do this.

5. Fixing core problems. The resolution of ***core security problems almost always requires updating, upgrading, or patching the software vulnerability or removing the vulnerable application***. The software hole can reside in any of the three layers (networking, operating system, or application).

NIST SP 800-53 Rev 4 May 2013



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

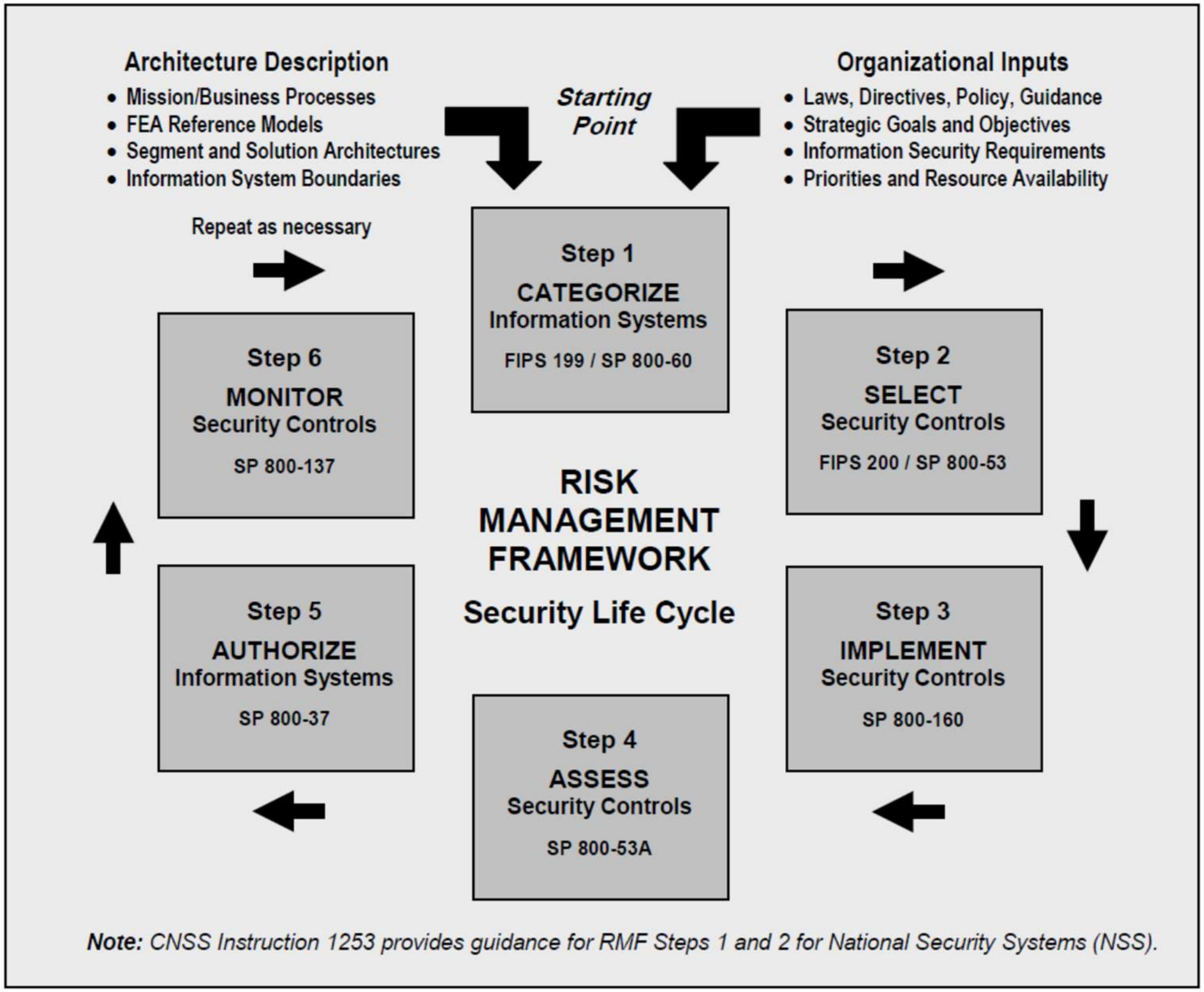
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a **process for selecting controls to protect organizational operations** (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a **diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).** The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.

NIST SP 800-53 Rev 4 May 2013



Architecture Description

- Mission/Business Processes
- FEA Reference Models
- Segment and Solution Architectures
- Information System Boundaries

Starting Point

Organizational Inputs

- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resource Availability

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53

Step 3
IMPLEMENT
Security Controls
SP 800-160

Step 4
ASSESS
Security Controls
SP 800-53A

Step 5
AUTHORIZE
Information Systems
SP 800-37

Step 6
MONITOR
Security Controls
SP 800-137

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

Note: *CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).*

FIGURE 2: RISK MANAGEMENT FRAMEWORK

NIST SP 800-82 Rev 2 May 2015

NIST Special Publication 800-82
Revision 1

Guide to Industrial Control Systems (ICS) Security

[illegible]

Keith Stouffer
Joe Falco
Karen Scarfone

[illegible]

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

800-82 Rev 2 - **Appendix G ICS Overlay uses the 800-53 security controls and adds Supplemental Guidance:**

“Instead of Screen Lock after 15 minutes of inactivity, use 2 person control”

A special acknowledgement to Lisa Kaiser, Department of Homeland Security, the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG), and Office of the Deputy Undersecretary of Defense for Installations and Environment, Business Enterprise Integration Directorate staff, **Daryl Haegley and Michael Chipley**, for their exceptional contributions to this publication.

Standards - NIST SP 800-82 R2 2015

2.5 Other Types of Control Systems

Although this guide provides guidance for securing ICS, other types of control systems share similar characteristics and many of the recommendations from this guide are applicable and could be used as a reference to protect such systems against cybersecurity threats. For example, although many building, transportation, medical, security and logistics systems use different protocols, ports and services and are configured and operate in different modes than ICS, they share similar characteristics to traditional ICS [18]. Examples of some of these systems and protocols include:

Other Types of Control Systems

- Advanced Metering Infrastructure
- Building Automation System
- Building Management Control System
- CCTV Surveillance System
- CO2 Monitoring
- Digital Signage Systems
- etc

Protocols/Ports and Services

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1628/29
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- ZigBee - Peer to Peer
- Bluetooth – Master/Slave

NIST SP 800-82 R2 Key Security Controls

Inventory

- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

Central Monitoring

- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

Test and Development Environment

- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

Critical Infrastructure

- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

Acquisition and Contracts

- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

NIST SP 800-53 and 800-82 Merged Ex 1

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.

NIST SP 800-53 and 800-82 Merged Ex 2

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at ***organization-defined acceptable levels with temperature and humidity levels within the facility where the IS resides at typically in the range of 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F***.; and

b. Monitors temperature and humidity levels ***organization-defined frequency***.

ICS Supplemental Guidance: Temperature and humidity controls are typically components of other ICS systems such as the HVAC, process, or lighting systems, or can be a standalone and unique ICS system. ICS can operate in extreme environments and both interior and exterior locations. For a specific ICS, the temperature and humidity design and operational parameters dictate the performance specifications. As ICS and IS become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity.

Key RMF Documents and Plans

Key RMF Documents/Plans (for commercial/private sector most now required by insurance)

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POAM)
- Information Systems Contingency and CONOPS Plan (ISCP)
- Event/Incident Communications Plan (EICP)
- Event/Incident Response Plan (EIRP)
- Security Audit Plan (SAP)

Obtain/create these plans in preparation to create the TTP Jump-Kit Rescue CD/USB

RMF Documents Using QUICX

Document Management

- □ Policy Management
- □ Risk Management Framework
- □ System Security Plans
- □ Cyber System Categorization
- □ Configuration Management
- □ Record Documents

Design and Construction

- □ Contract Management
- □ Permit Process
- □ Drawings and Specifications
- □ Submittals
- □ Requests for Information
- □ Change Management

QC & Commissioning

- □ Master Equipment List
- □ Location List
- □ Field Reporting
- □ Deliverables Tracking
- □ Inspections and Checklists
- □ Cyber Procedures
- □ Performance Testing
- □ Action Lists

Transition

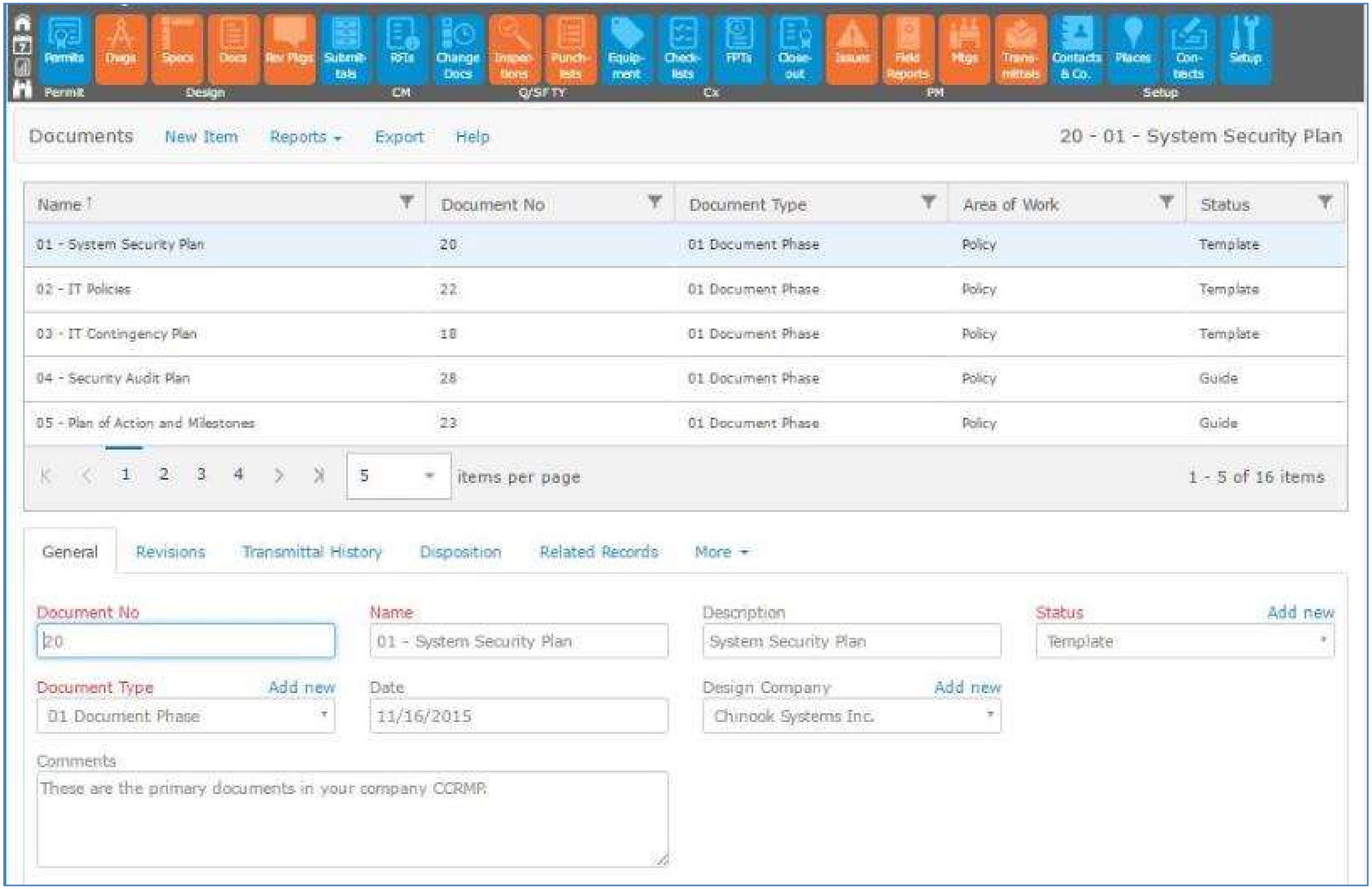
- □ Transition Management
- □ O&M Manuals
- □ Training Facilitation
- □ Warranty Certificates
- □ Spare Parts/Special Tools

Operations

- □ Life Cycle Cost Analysis
- □ Condition Assessments
- □ Building Controls Analytics
- □ Cyber Risk Assessments
- □ Cyber Continuous Monitoring

QUICX is a Facility Management and document management application that integrates facility equipment data, work orders, construction documents and specifications, geospatial, IT and OT network and component information

Typical Plans & Audit Logs Directory Using QUICX



20 - 01 - System Security Plan

Name ↑	Document No	Document Type	Area of Work	Status
01 - System Security Plan	20	01 Document Phase	Policy	Template
02 - IT Policies	22	01 Document Phase	Policy	Template
03 - IT Contingency Plan	18	01 Document Phase	Policy	Template
04 - Security Audit Plan	28	01 Document Phase	Policy	Guide
05 - Plan of Action and Milestones	23	01 Document Phase	Policy	Guide

1 2 3 4 — 5 items per page — 1 - 5 of 16 items

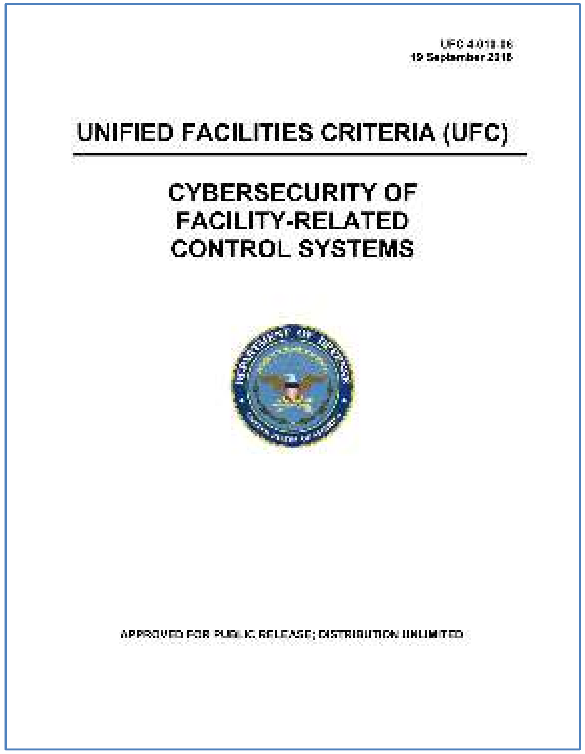
General | Revisions | Transmittal History | Disposition | Related Records | More

Document No: 20	Name: 01 - System Security Plan	Description: System Security Plan	Status (Add new): Template
Document Type (Add new): 01 Document Phase	Date: 11/16/2015	Design Company (Add new): Chinook Systems Inc.	

Comments: These are the primary documents in your company CCRMP.

An organization can use standard data drives, SharePoint, etc. to store the Plans and Audit Logs

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

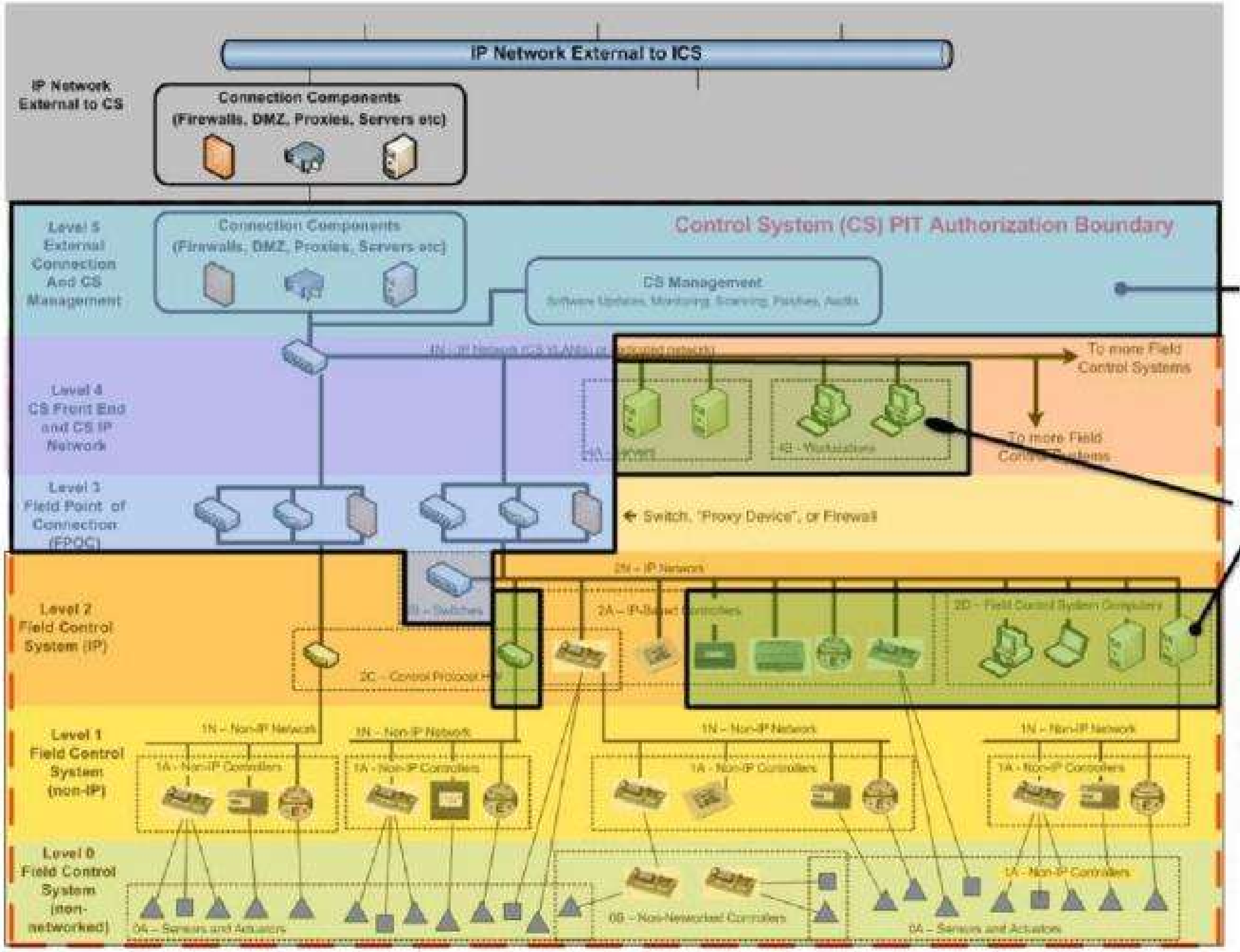
3-1.1 Five Steps for Cybersecurity Design. The five steps for cybersecurity design are:

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


IP Network External to ICS
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control System (CS) PIT Authorization Boundary
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (CS VLANs) or dedicated network
To more Field Control Systems
To more Field Control Systems
Level 4 CS Front End and CS IP Network
4A – Servers
4B – Workstations
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 Hub
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1A – Non-IP Controllers
1A – Non-IP Controllers
1A – Non-IP Controllers
1A – Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
1A – Non-IP Controllers
0A – Sensors and Actuators

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

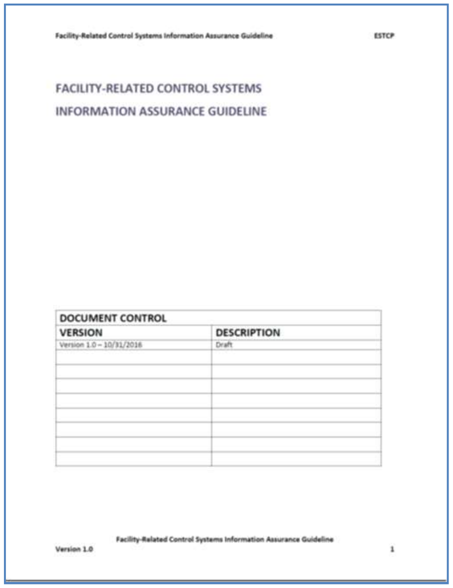
All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the FRCS-PE and NUMCS.

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 FRCS firmware
7. Hash all software and firmware
8. Hash the inventory files

Cybersecurity Guideline For FRCS



Facility-Related Control Systems Information Assurance Guideline ESTCP

FACILITY-RELATED CONTROL SYSTEMS
INFORMATION ASSURANCE GUIDELINE

DOCUMENT CONTROL	
VERSION	DESCRIPTION
Version 1.0 – 10/31/2016	Draft

Facility-Related Control Systems Information Assurance Guideline
Version 1.0 1

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

- Hybrid/Converged CS
- Project Roles and Responsibilities
- **Requirements For Subject Matter Experts**
- **Test And Development Environment and Tools**
- Required Submittals
- Applicable ESTCP FRCS Templates (FAT & SAT, PenTest)
- **Typical Sequence Of FRCS Design And Construction Activities**

Any organization can use for their FRCS

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

Cybersecurity Guideline For FRCS 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.

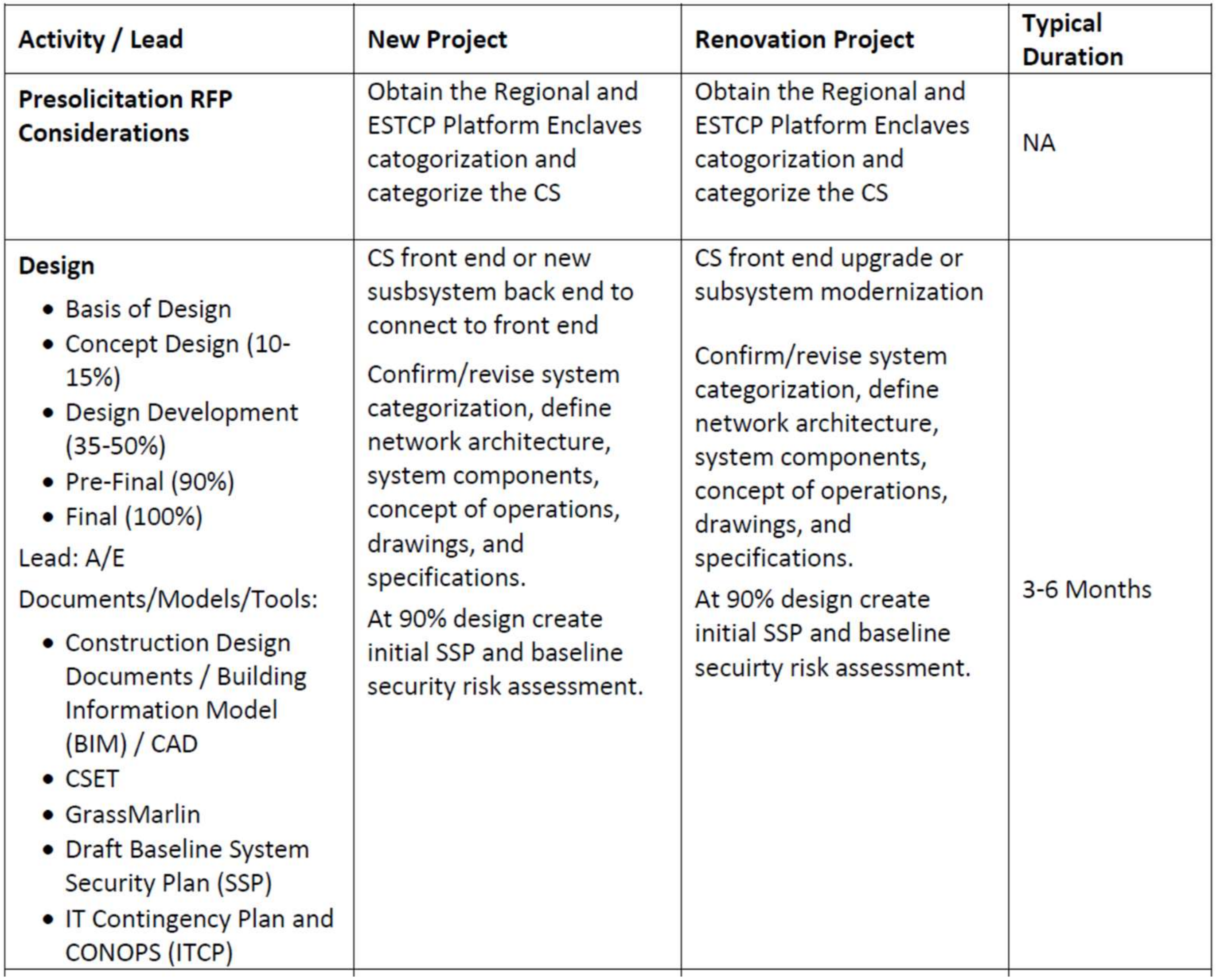
Cybersecurity Guideline For FRCS TDE

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.

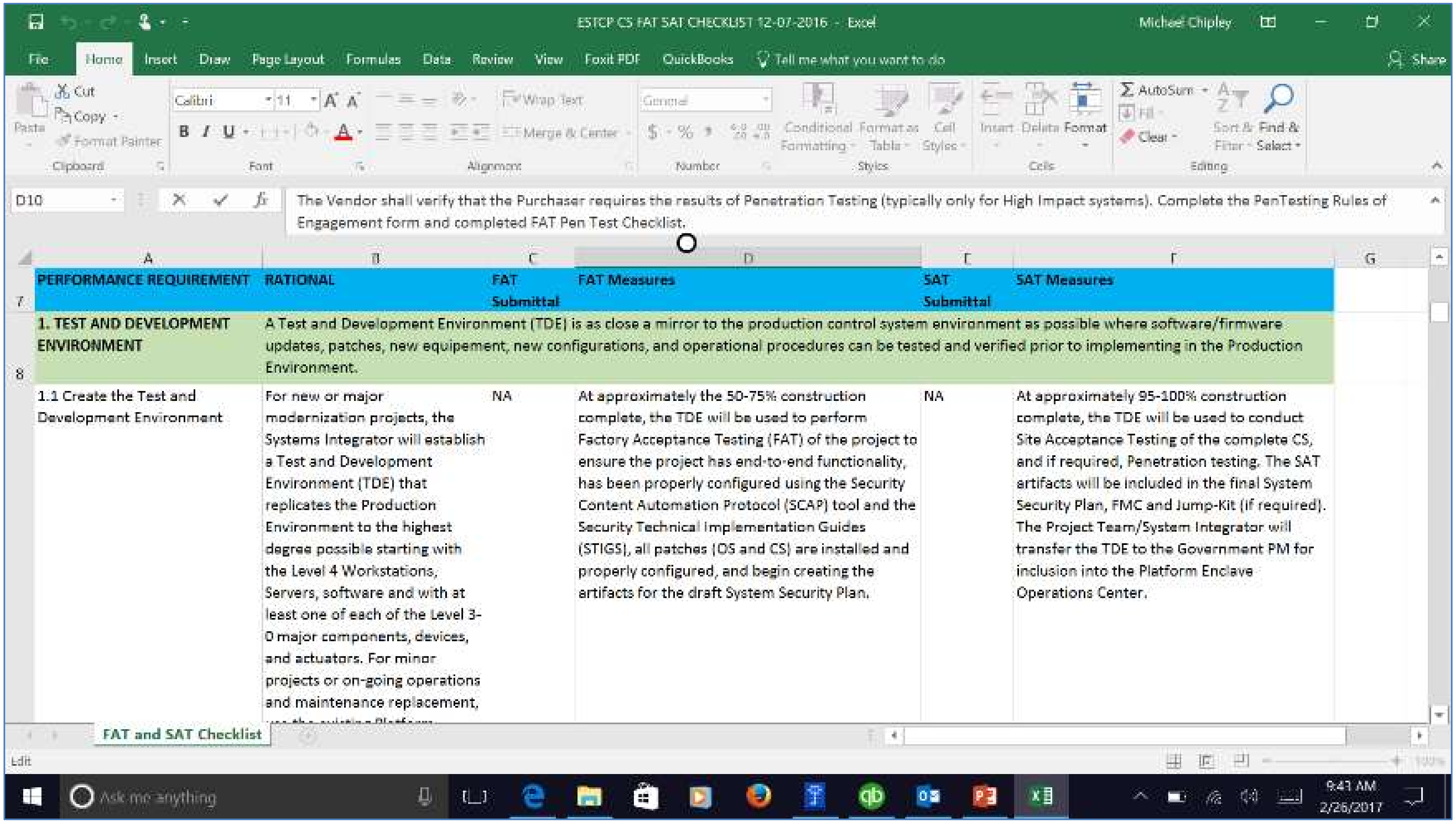
At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).

Cybersecurity Guideline For FRCS 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

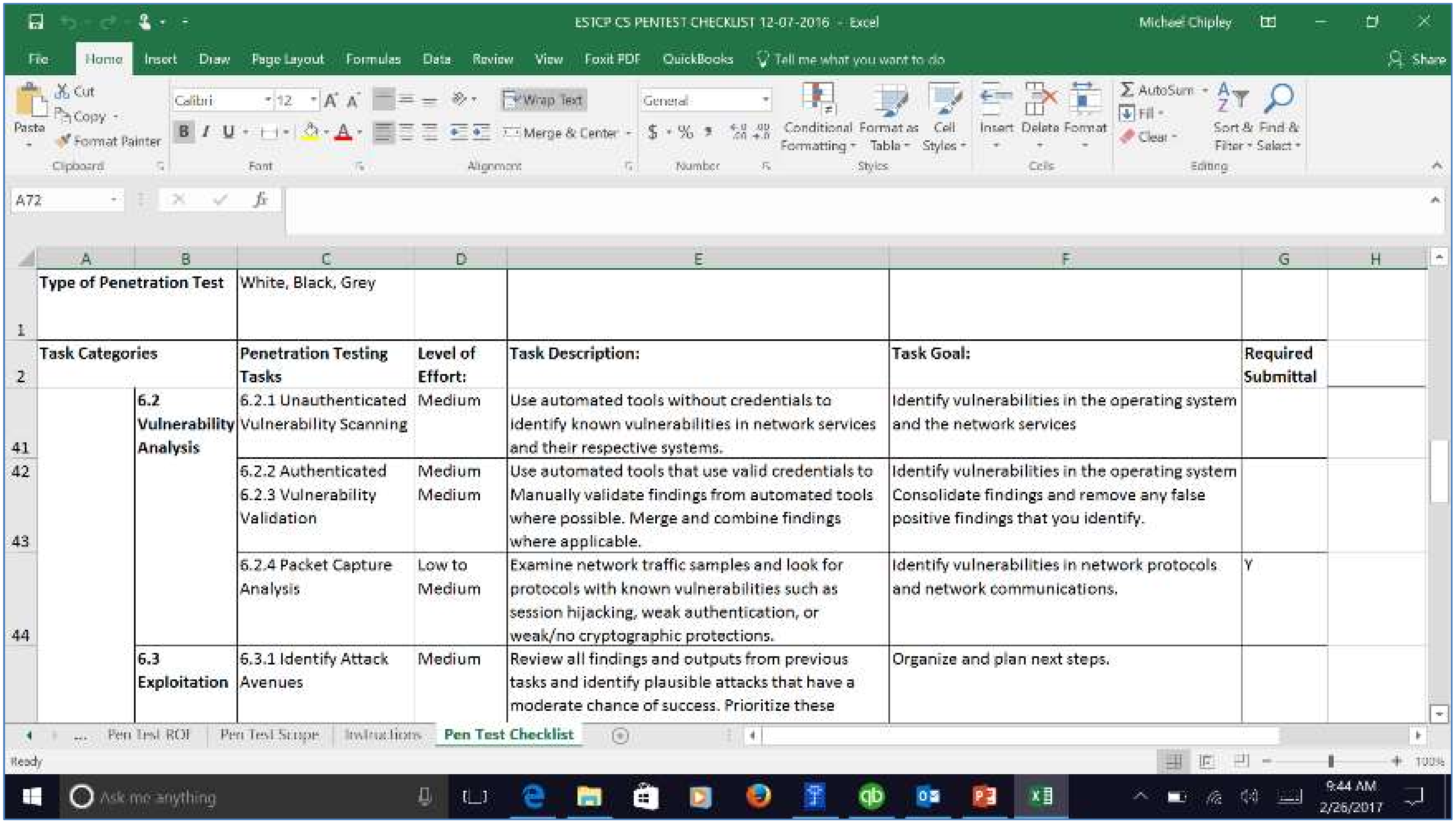
Cybersecurity Guideline For FRCS FAT/SAT



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, use the existing Platform	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 For FRCS 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.		

Tools

Information Gathering

- Google Search and Hacking
- Google Earth
- The Harvester
- Recon-NG
- Shodan
- Costar

Network Discovery and Monitoring

- Nmap
- Snort
- Kismet
- Nessus
- McAfee
- Sophia
- Bandolier
- SCAP
- Belarc
- Glasswire

Attack and Defend Tools

- Kali Linux (Backtrack)
- SamuraiSTFU
- Wireshark
- Gleg
- Windows PowerShell
- Windows Management Information Console
- Windows Enhanced Mitigation Tools
- Windows Sysinternals

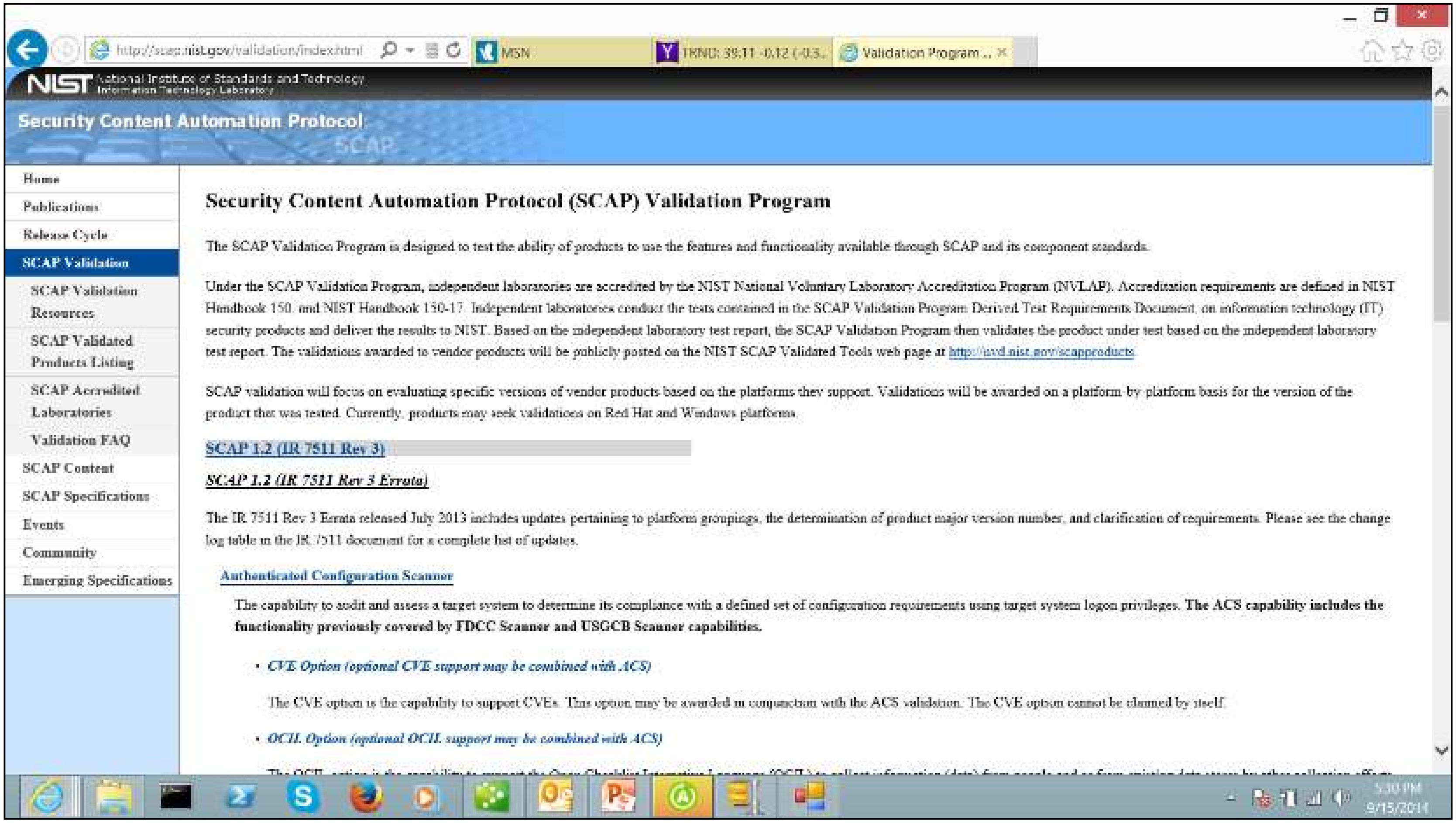
Assessment Tools

- DHS ICS-CERT Cyber Security Evaluation Tool (CSET)

Virtual Machines

- VM Player
- Windows Hypervisor

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.**

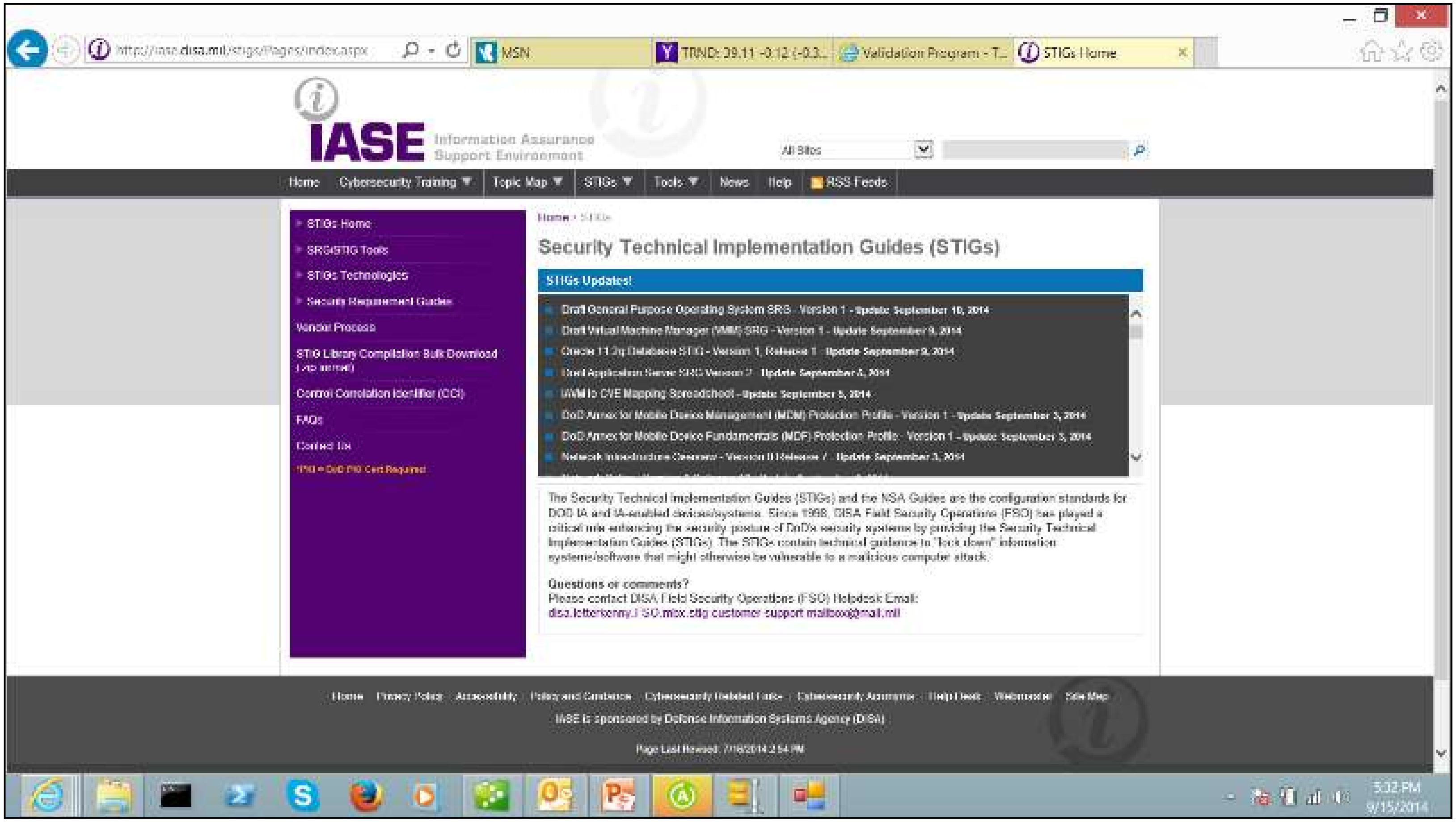
- *CVE Option (optional CVE support may be combined with ACS)*

  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


http://iase.disa.mil/stigs/Pages/index.aspx
MSN
TRND: 39.11 -0.12 (-0.3...
Validation Program - T...
STIGs Home
IASE Information Assurance Support Environment
All Sites
Home
Cybersecurity Training
Topic Map
STIGs
Tools
News
Help
RSS Feeds
STIGs Home
SRG/STIG Tools
STIGs Technologies
Security Requirement Guides
Vendor Process
STIG Library Compilation Bulk Download (.zip format)
Control Correlation Identifier (CCI)
FAQs
Contact Us
PKI = DoD PKI Cert Required
Home › STIGs
Home | Privacy Policy | Accessibility | Policy and Guidance | Cybersecurity Related Links | Cybersecurity Awareness | Help Desk | Webmaster | Site Map
5:32 PM
9/15/2014

Security Technical Implementation Guides (STIGs)

STIGs Updates!

- Draft General Purpose Operating System SRG - Version 1 - Update September 10, 2014
- Draft Virtual Machine Manager (VMM) SRG - Version 1 - Update September 9, 2014
- Oracle 11.2g Database STIG - Version 1, Release 1 - Update September 9, 2014
- Draft Application Server SRG Version 2 - Update September 5, 2014
- IAVM to CVE Mapping Spreadsheet - Update September 5, 2014
- DoD Annex for Mobile Device Management (MDM) Protection Profile - Version 1 - Update September 3, 2014
- DoD Annex for Mobile Device Fundamentals (MDF) Protection Profile - Version 1 - Update September 3, 2014
- Network Infrastructure Overview - Version 8 Release 7 - Update September 3, 2014

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

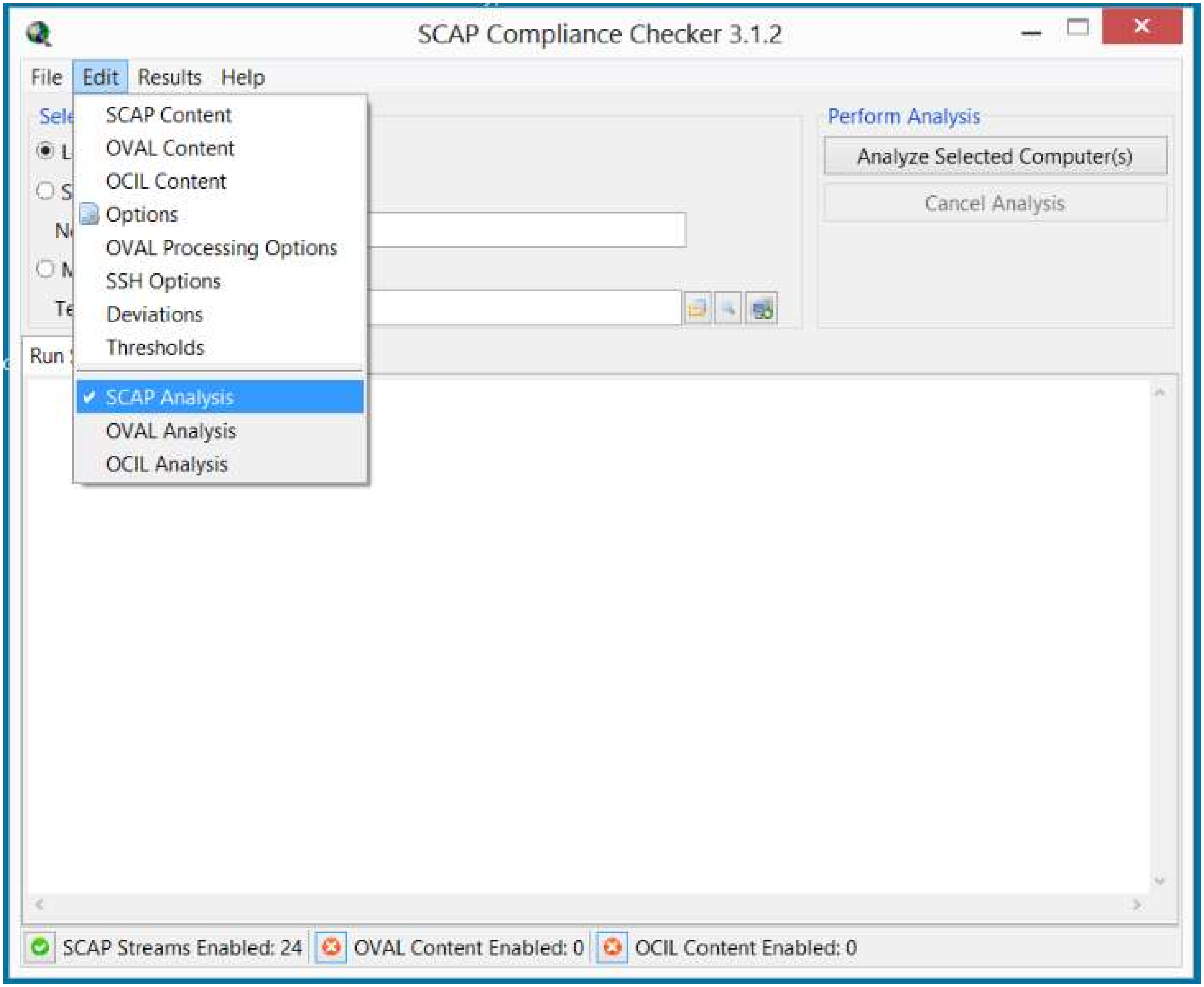
Questions or comments?
Please contact DISA Field Security Operations (FSO) Helpdesk Email:
disa.letterkenny.FSO.mbx.stig customer support mailbox@mail.mil

IASE is sponsored by Defense Information Systems Agency (DISA)

Page Last Revised: 7/18/2014 2:54 PM

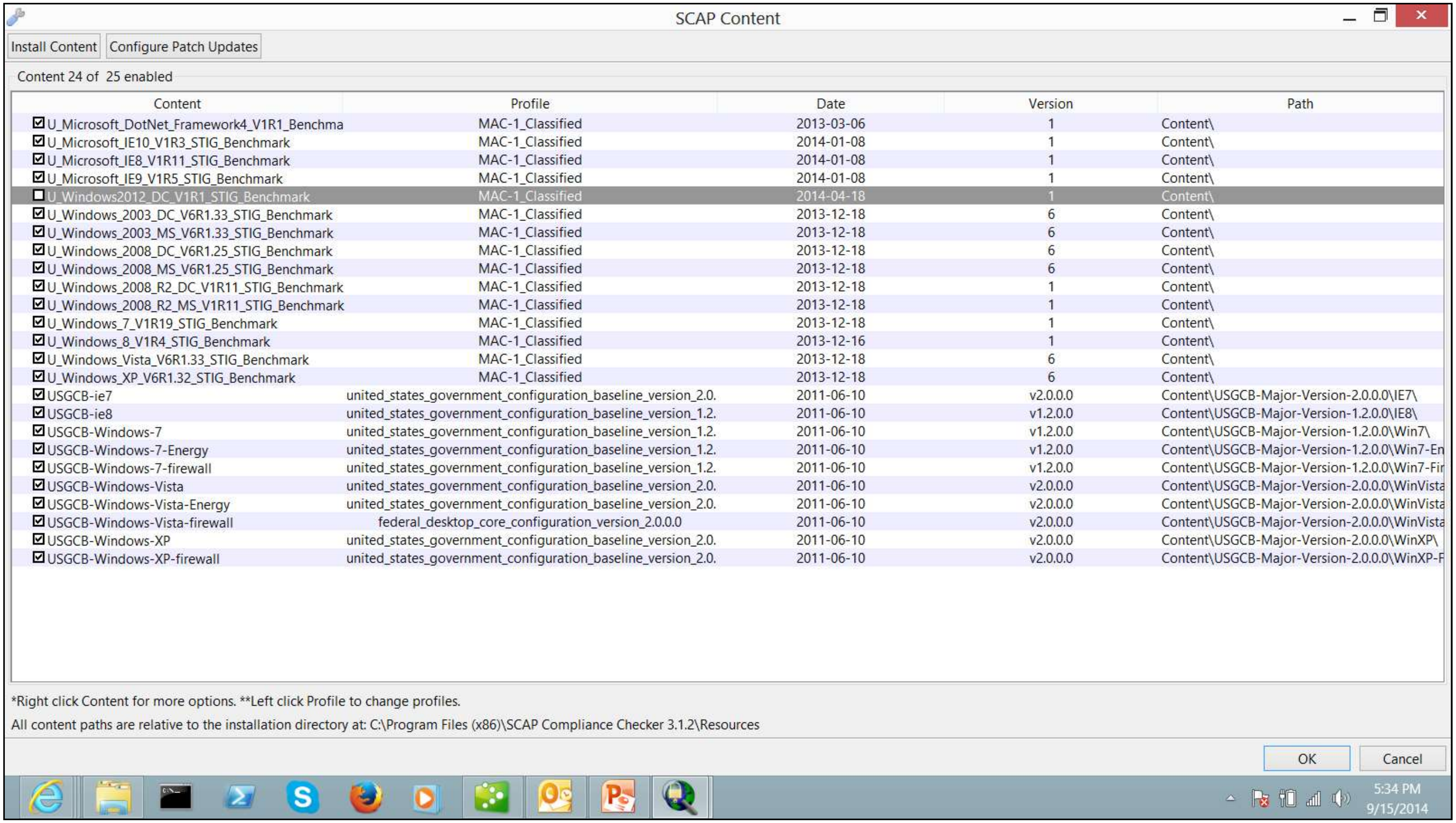
http://iase.disa.mil/stigs/Pages/index.aspx

DISA SCAP



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

DISA SCAP Contents



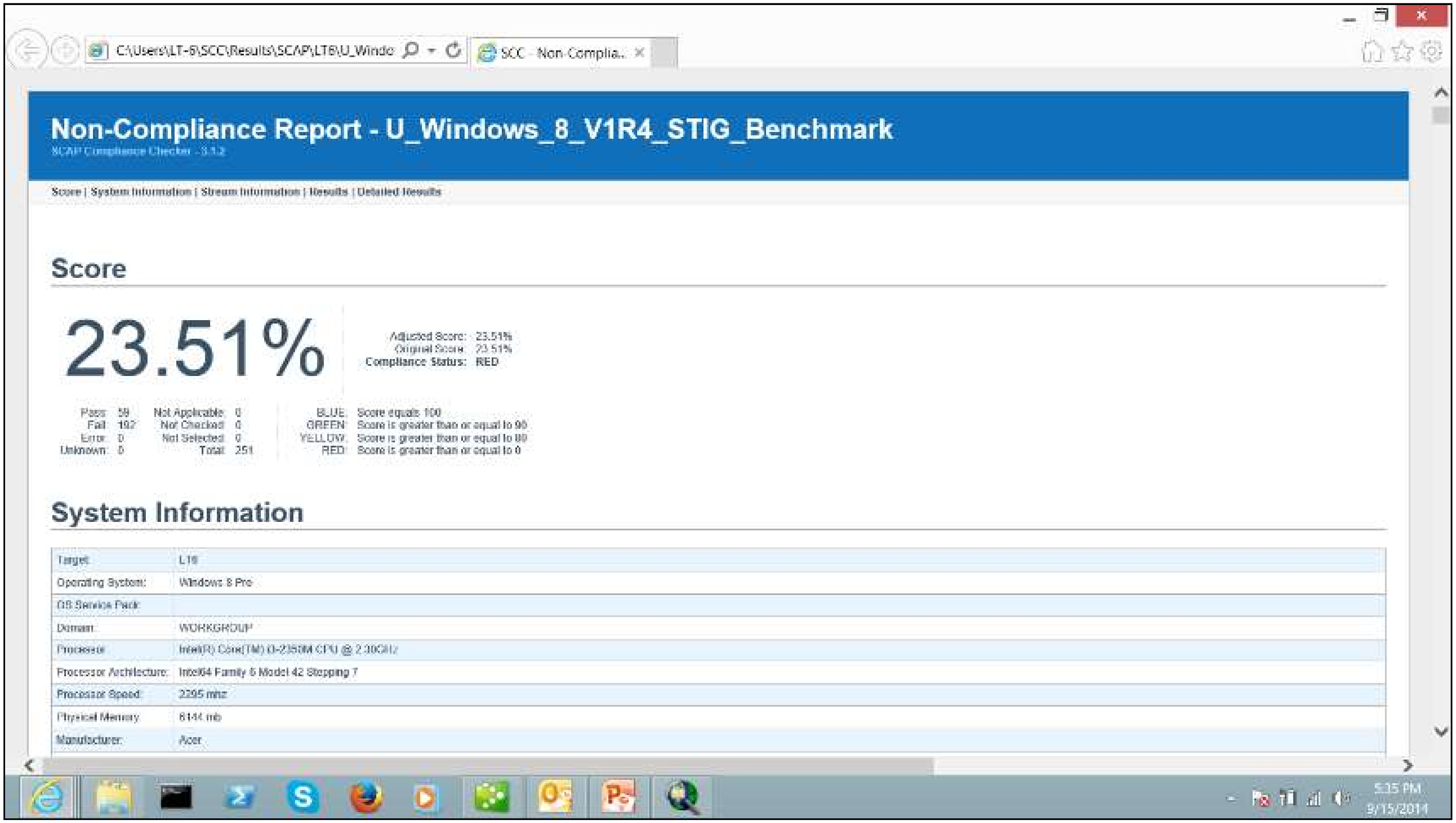
Content 24 of 25 enabled

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



Non-Compliance Report - U_Windows_8_V1R4_STIG_Benchmark

SCAP Compliance Checker - 3.1.2

Score | System Information | Stream Information | Results | Detailed Results

Score

23.51%

Adjusted Score:	23.51%
Original Score:	23.51%
Compliance Status:	RED

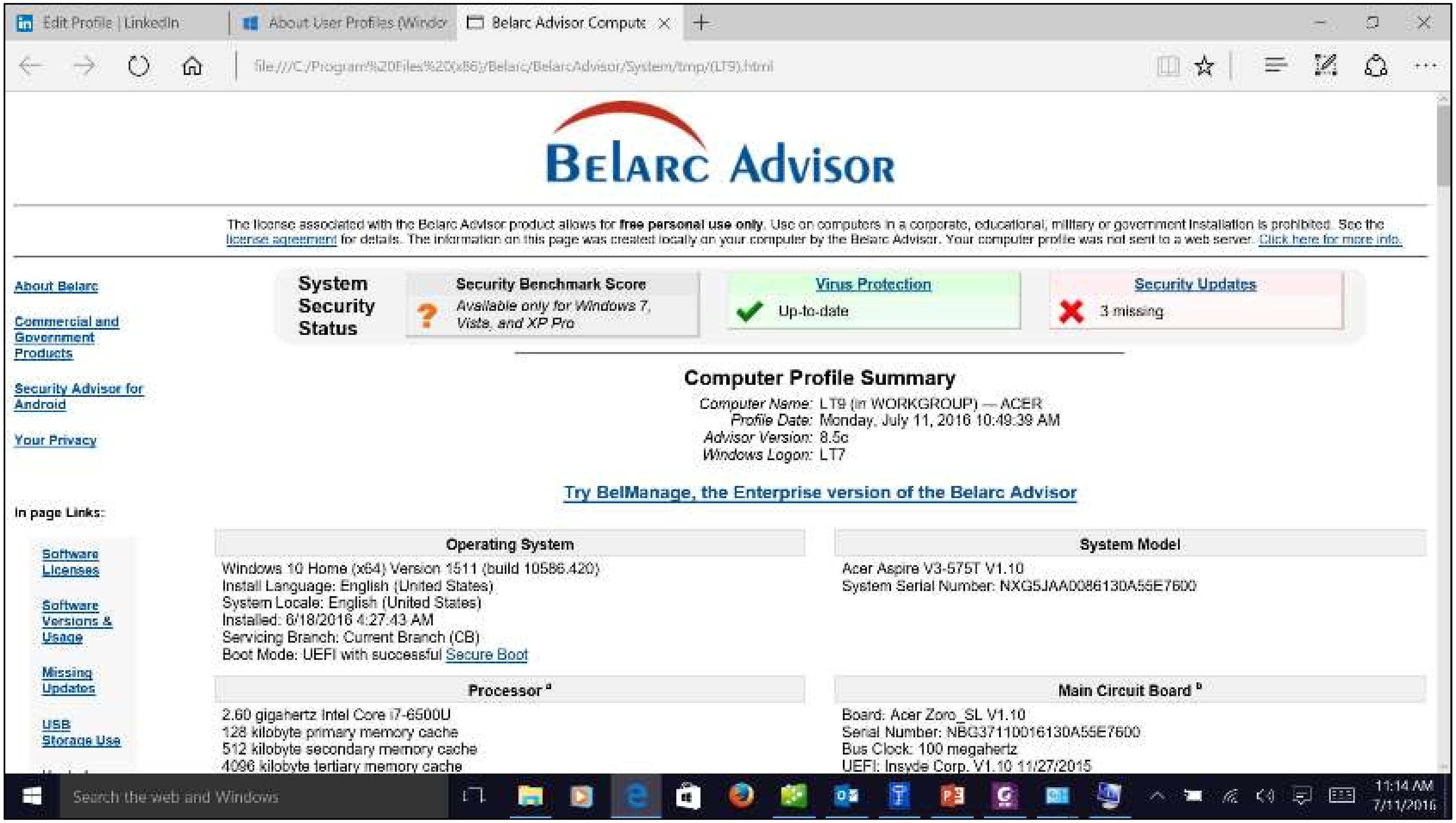
Pass:	59	Not Applicable:	0
Fail:	192	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Total:	251

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

System Information

Target:	L16
Operating System:	Windows 8 Pro
OS Service Pack:	
Domain:	WORKGROUP
Processor:	Intel(R) Core(TM) i3-2350M CPU @ 2.30GHz
Processor Architecture:	Intel64 Family 6 Model 42 Stepping 7
Processor Speed:	2295 mhz
Physical Memory:	6144 mb
Manufacturer:	Acer

Belarc Advisor


Edit Profile | LinkedIn
About User Profiles (Windo
Belarc Advisor Compute
file:///C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(LT9).html
Search the web and Windows
11:14 AM
7/11/2016

BELARC Advisor

The license associated with the Belarc Advisor product allows for **free personal use only**. Use on computers in a corporate, educational, military or government installation is prohibited. See the license agreement for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. Click here for more info.

About Belarc

Commercial and Government Products

Security Advisor for Android

Your Privacy

In page Links:

- Software Licenses
- Software Versions & Usage
- Missing Updates
- USB Storage Use

System Security Status	Security Benchmark Score	Virus Protection	Security Updates
	? *Available only for Windows 7, Vista, and XP Pro*	✓ Up-to-date	✗ 3 missing

Computer Profile Summary

Computer Name: LT9 (in WORKGROUP) — ACER
Profile Date: Monday, July 11, 2016 10:49:39 AM
Advisor Version: 8.5c
Windows Logon: LT7

Try BelManage, the Enterprise version of the Belarc Advisor

Operating System

Windows 10 Home (x64) Version 1511 (build 10586.420)
Install Language: English (United States)
System Locale: English (United States)
Installed: 6/18/2016 4:27:43 AM
Servicing Branch: Current Branch (CB)
Boot Mode: UEFI with successful Secure Boot

System Model

Acer Aspire V3-575T V1.10
System Serial Number: NXG5JAA0086130A55E7600

Processor [a]

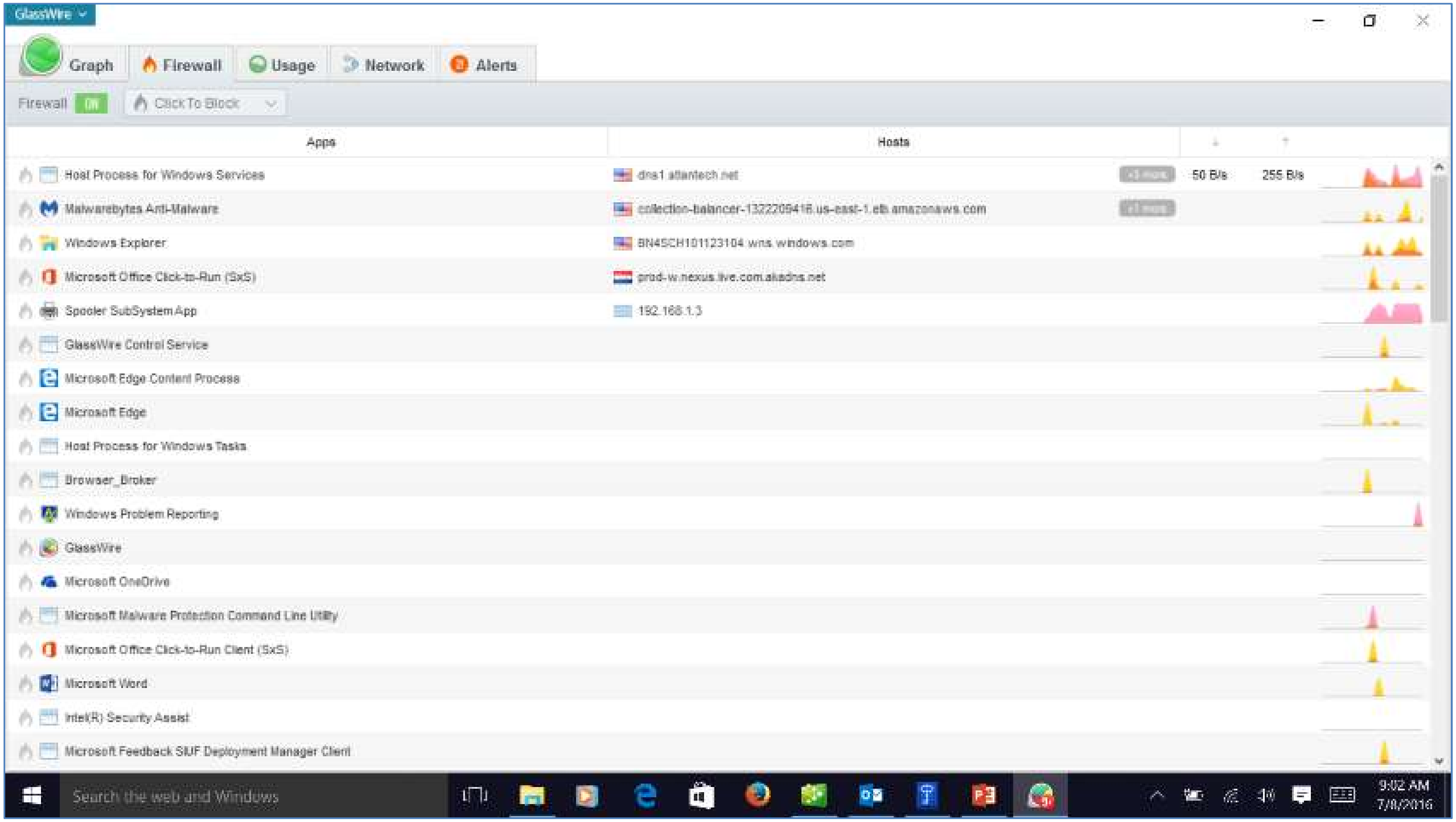
2.60 gigahertz Intel Core i7-6500U
128 kilobyte primary memory cache
512 kilobyte secondary memory cache
4096 kilobyte tertiary memory cache

Main Circuit Board [b]

Board: Acer Zoro_SL V1.10
Serial Number: NBG37110016130A55E7600
Bus Clock: 100 megahertz
UEFI: Insyde Corp. V1.10 11/27/2015

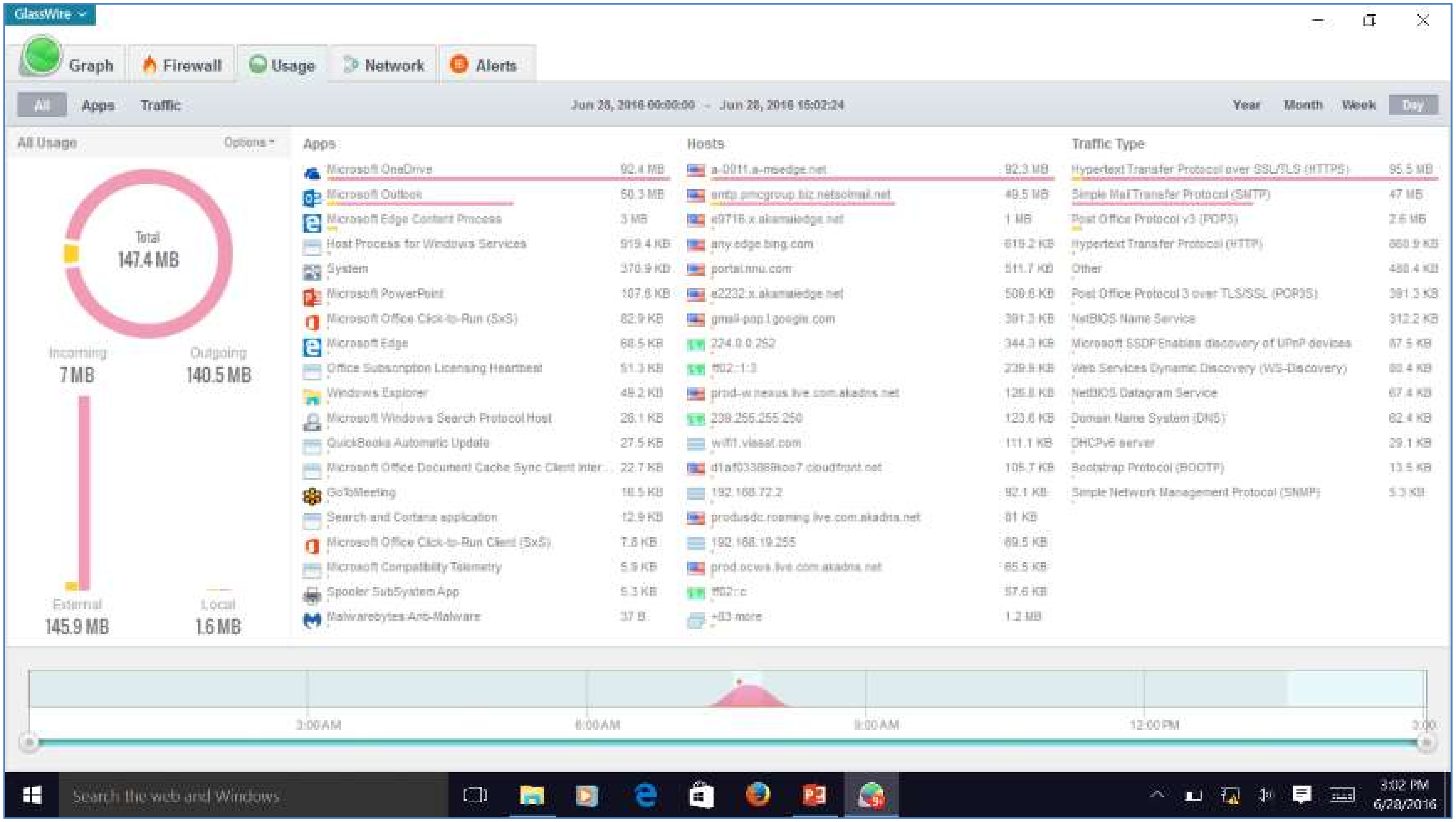
http://www.belarc.com/

Glasswire Firewall



Apps	Hosts		↓	↑
Host Process for Windows Services	dns1.atlantech.net	+1 more	50 B/s	255 B/s
Malwarebytes Anti-Malware	collection-balancer-1322209416.us-east-1.elb.amazonaws.com	+1 more		
Windows Explorer	BN4SCH101123104.wns.windows.com			
Microsoft Office Click-to-Run (SxS)	prod-w.nexus.live.com.akadns.net			
Spooler SubSystem App	192.168.1.3			
GlassWire Control Service				
Microsoft Edge Content Process				
Microsoft Edge				
Host Process for Windows Tasks				
Browser_Broker				
Windows Problem Reporting				
GlassWire				
Microsoft OneDrive				
Microsoft Malware Protection Command Line Utility				
Microsoft Office Click-to-Run Client (SxS)				
Microsoft Word				
Intel(R) Security Assist				
Microsoft Feedback SIUF Deployment Manager Client				

Glasswire Usage



Jun 28, 2016 00:00:00 - Jun 28, 2016 15:02:24

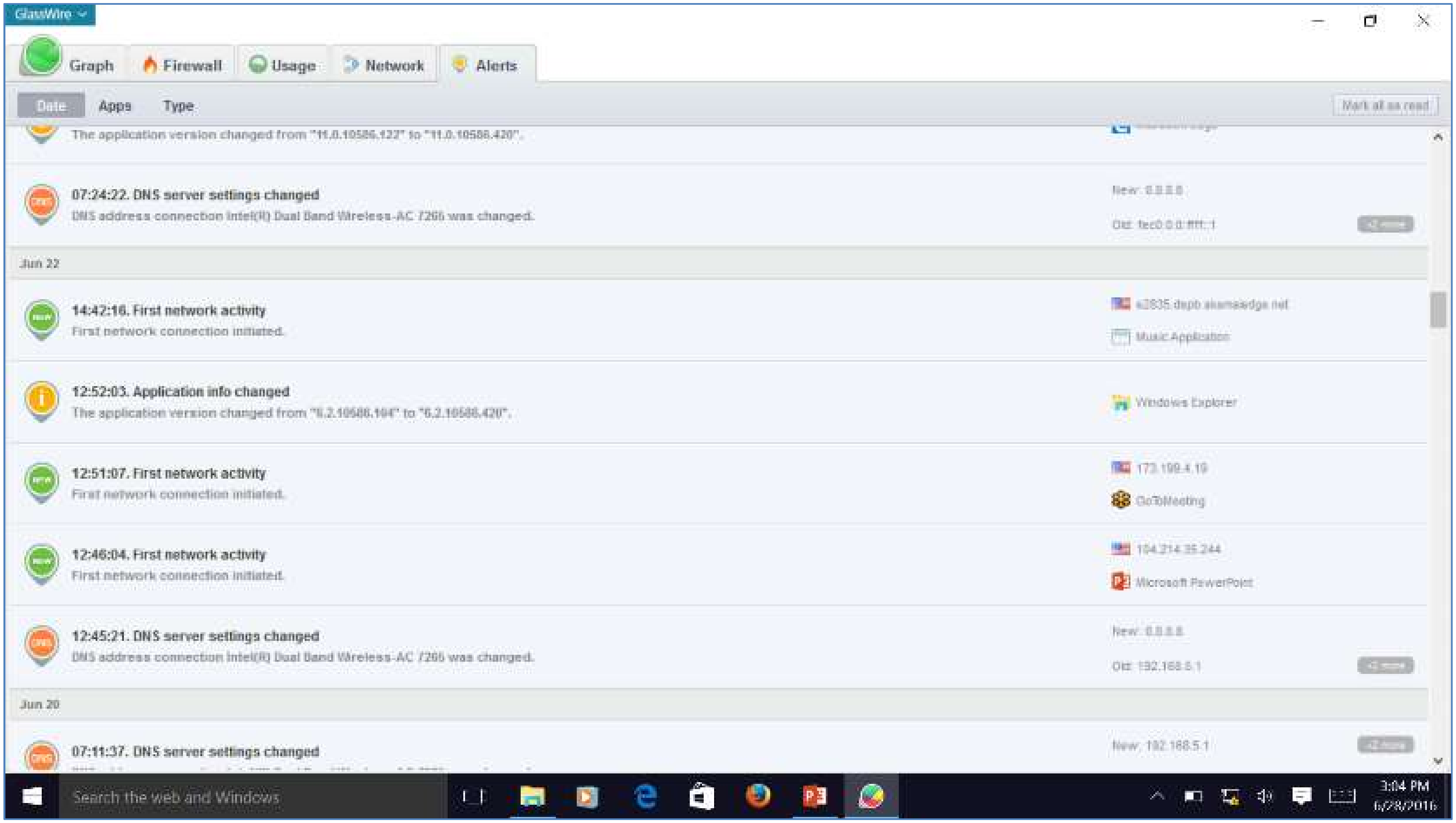
Apps	
Microsoft OneDrive	92.4 MB
Microsoft Outlook	50.3 MB
Microsoft Edge Content Process	3 MB
Host Process for Windows Services	919.4 KB
System	370.9 KB
Microsoft PowerPoint	107.6 KB
Microsoft Office Click-to-Run (SxS)	82.9 KB
Microsoft Edge	68.5 KB
Office Subscription Licensing Heartbeat	51.3 KB
Windows Explorer	49.2 KB
Microsoft Windows Search Protocol Host	28.1 KB
QuickBooks Automatic Update	27.5 KB
Microsoft Office Document Cache Sync Client Inter...	22.7 KB
GoToMeeting	18.5 KB
Search and Cortana application	12.9 KB
Microsoft Office Click-to-Run Client (SxS)	7.8 KB
Microsoft Compatibility Telemetry	5.9 KB
Spooler SubSystem App	5.3 KB
Malwarebytes Anti-Malware	37 B

Hosts	
a-0011.a-msedge.net	92.3 MB
smtp.pmcgroup.biz.netsolmail.net	49.5 MB
e9716.x.akamaiedge.net	1 MB
any.edge.bing.com	619.2 KB
portal.nnu.com	511.7 KB
e2232.x.akamaiedge.net	509.6 KB
gmail-pop.l.google.com	391.3 KB
224.0.0.252	344.3 KB
ff02::1:3	239.9 KB
prod-w.nexus.live.com.akadns.net	126.8 KB
239.255.255.250	123.6 KB
wifi1.viasat.com	111.1 KB
d1af033869koo7.cloudfront.net	105.7 KB
192.168.72.2	92.1 KB
produsdc.roaming.live.com.akadns.net	81 KB
192.168.19.255	69.5 KB
prod.ocws.live.com.akadns.net	65.5 KB
ff02::c	57.6 KB
+83 more	1.2 MB

Traffic Type	
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	95.5 MB
Simple Mail Transfer Protocol (SMTP)	47 MB
Post Office Protocol v3 (POP3)	2.6 MB
Hypertext Transfer Protocol (HTTP)	860.9 KB
Other	488.4 KB
Post Office Protocol 3 over TLS/SSL (POP3S)	391.3 KB
NetBIOS Name Service	312.2 KB
Microsoft SSDP Enables discovery of UPnP devices	87.5 KB
Web Services Dynamic Discovery (WS-Discovery)	80.4 KB
NetBIOS Datagram Service	67.4 KB
Domain Name System (DNS)	62.4 KB
DHCPv6 server	29.1 KB
Bootstrap Protocol (BOOTP)	13.5 KB
Simple Network Management Protocol (SNMP)	5.3 KB

Apps, Hosts and Traffic Type

Glasswire Alerts



The application version changed from "11.0.10586.122" to "11.0.10586.420".

07:24:22. DNS server settings changed
DNS address connection Intel(R) Dual Band Wireless-AC 7265 was changed.
New: 0.0.0.0
Old: fec0:0:0:ffff::1

Jun 22

14:42:16. First network activity
First network connection initiated.
e2835.dspb.akamaiedge.net
Music Application

12:52:03. Application info changed
The application version changed from "6.2.10586.104" to "6.2.10586.420".
Windows Explorer

12:51:07. First network activity
First network connection initiated.
173.199.4.19
GoToMeeting

12:46:04. First network activity
First network connection initiated.
104.214.35.244
Microsoft PowerPoint

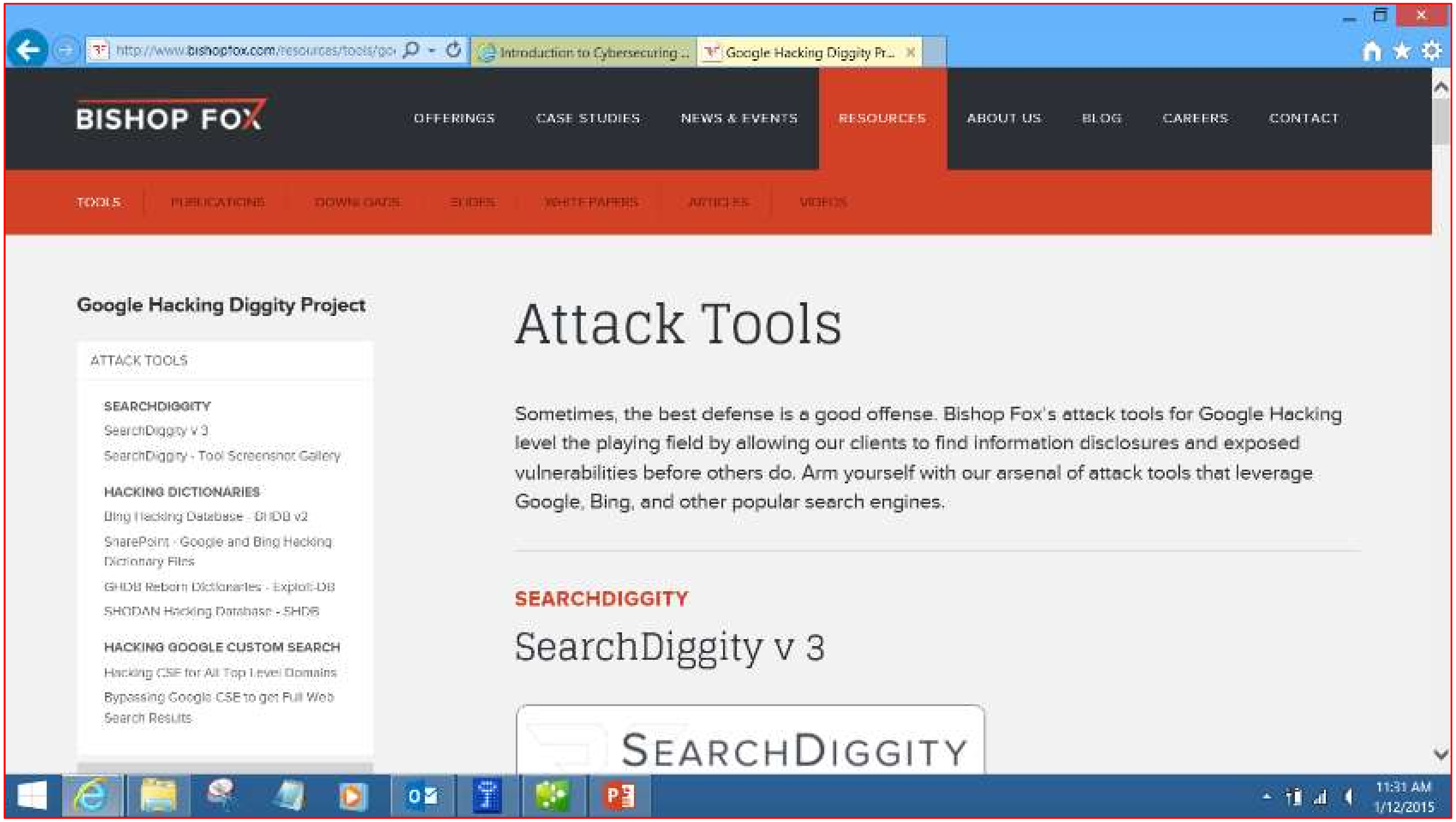
12:45:21. DNS server settings changed
DNS address connection Intel(R) Dual Band Wireless-AC 7265 was changed.
New: 0.0.0.0
Old: 192.168.5.1

Jun 20

07:11:37. DNS server settings changed
New: 192.168.5.1

DNS, Executable, Version

Google Hacking Diggity Project



Google Hacking Diggity Project

ATTACK TOOLS

SEARCHDIGGITY

SearchDiggity v 3

SearchDiggity - Tool Screenshot Gallery

HACKING DICTIONARIES

Bing Hacking Database - BHDB v2

SharePoint - Google and Bing Hacking Dictionary Files

GHDB Reborn Dictionaries - Exploit-DB

SHODAN Hacking Database - SHDB

HACKING GOOGLE CUSTOM SEARCH

Hacking CSE for All Top Level Domains

Bypassing Google CSE to get Full Web Search Results

Attack Tools

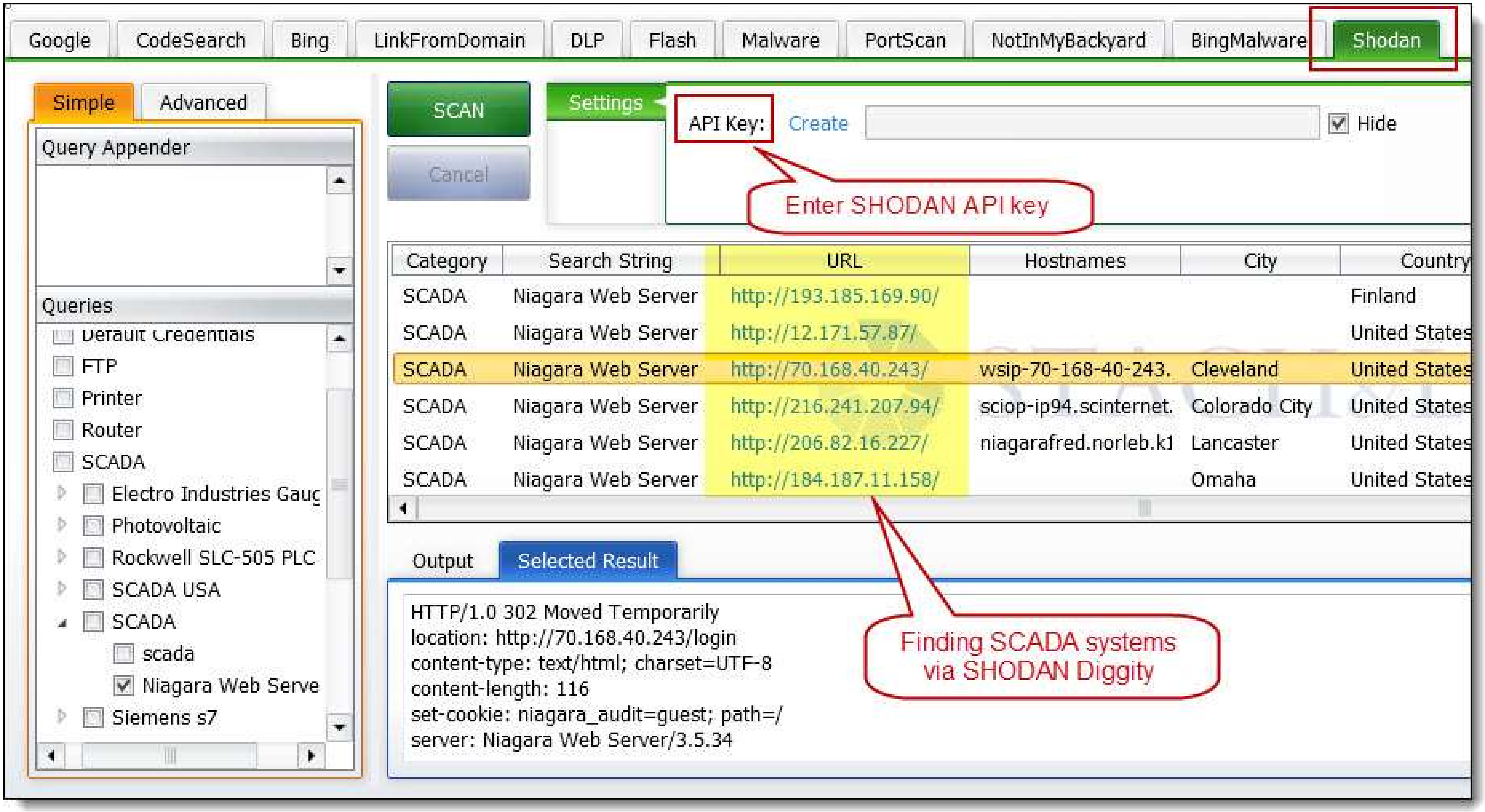
Sometimes, the best defense is a good offense. Bishop Fox's attack tools for Google Hacking level the playing field by allowing our clients to find information disclosures and exposed vulnerabilities before others do. Arm yourself with our arsenal of attack tools that leverage Google, Bing, and other popular search engines.

SEARCHDIGGITY

SearchDiggity v 3

http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/#searchdiggity

Google Hacking Diggity Project



☑ Hide

- □ Default Credentials
- □ FTP
- □ Printer
- □ Router
- □ SCADA
  - □ Electro Industries Gauc
  - □ Photovoltaic
  - □ Rockwell SLC-505 PLC
  - □ SCADA USA
  - □ SCADA
    - □ scada
    - ☑ Niagara Web Serve
  - □ Siemens s7

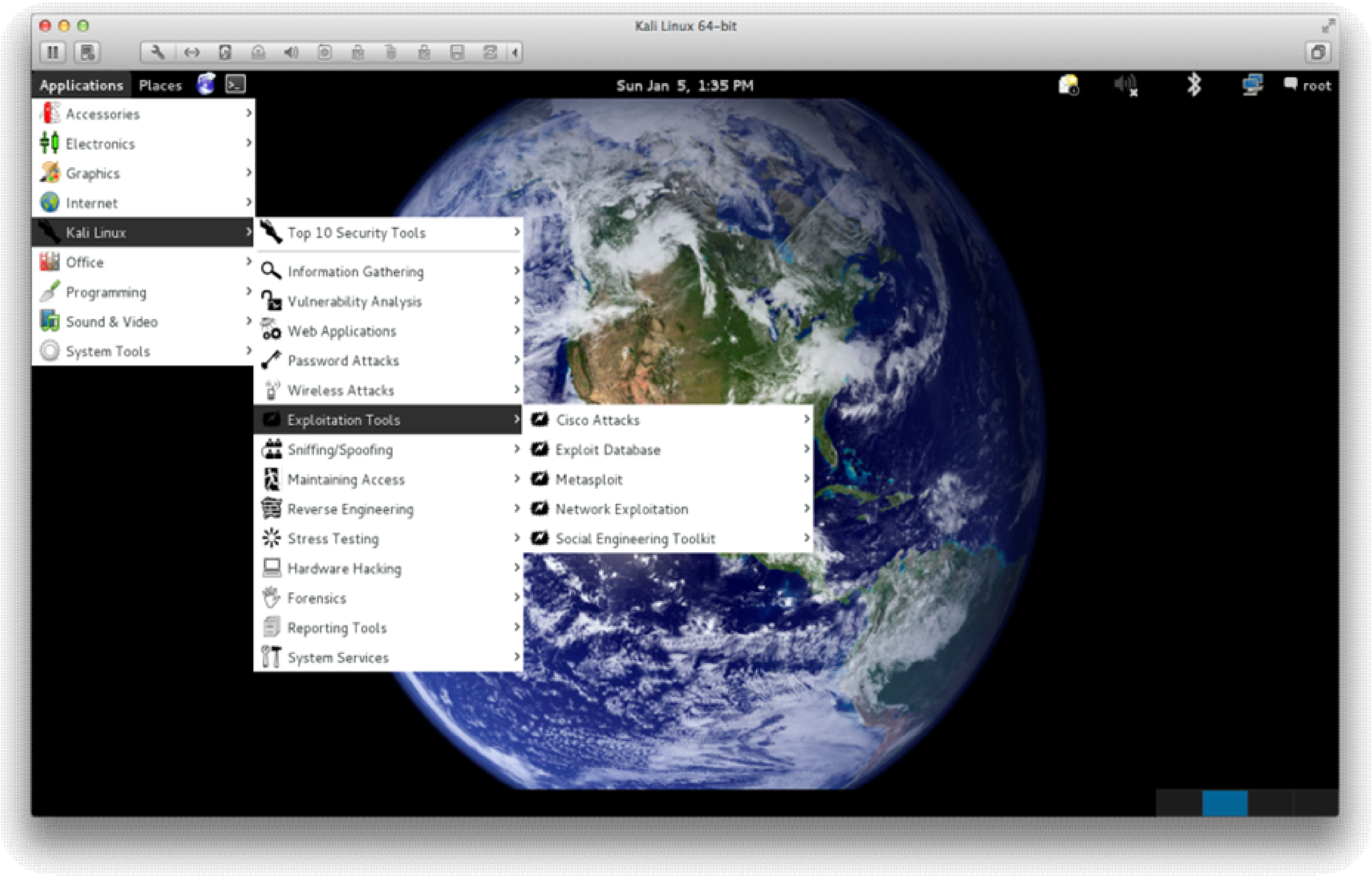
Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	http://206.82.16.227/	niagarafred.norleb.k1	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

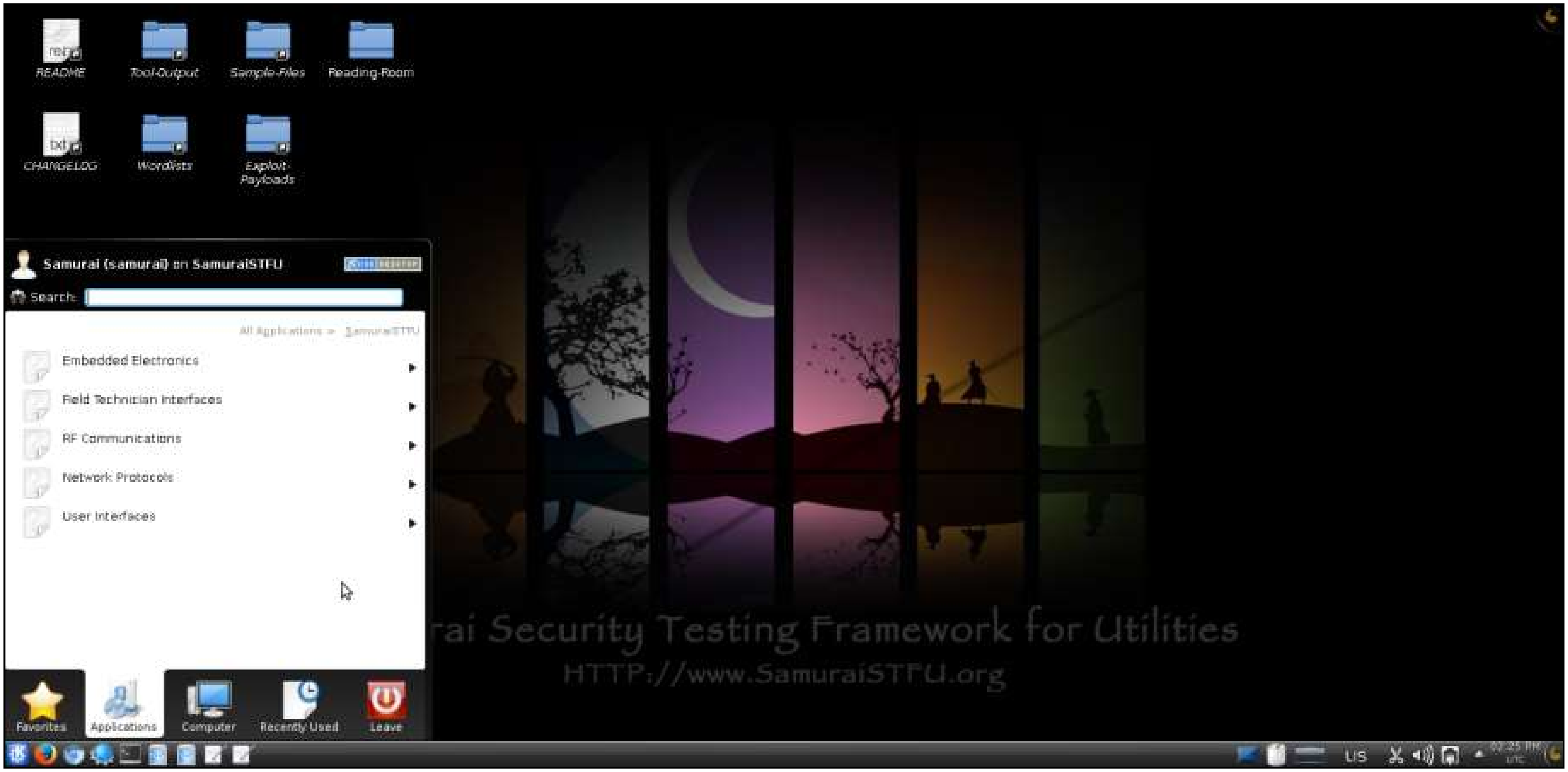
Enter SHODAN API key

Finding SCADA systems via SHODAN Diggity

Kali Linux Exploitation Tools



SamuraiSTFU Applications



Developed specifically for energy sector – EPRI NESCOR

SOPHIA

Sophia is a **passive, real time tool for inter-device communication discovery and monitoring** of the active elements in various types of modern control systems to include Supervisory Control and Data Acquisition (SCADA) systems.

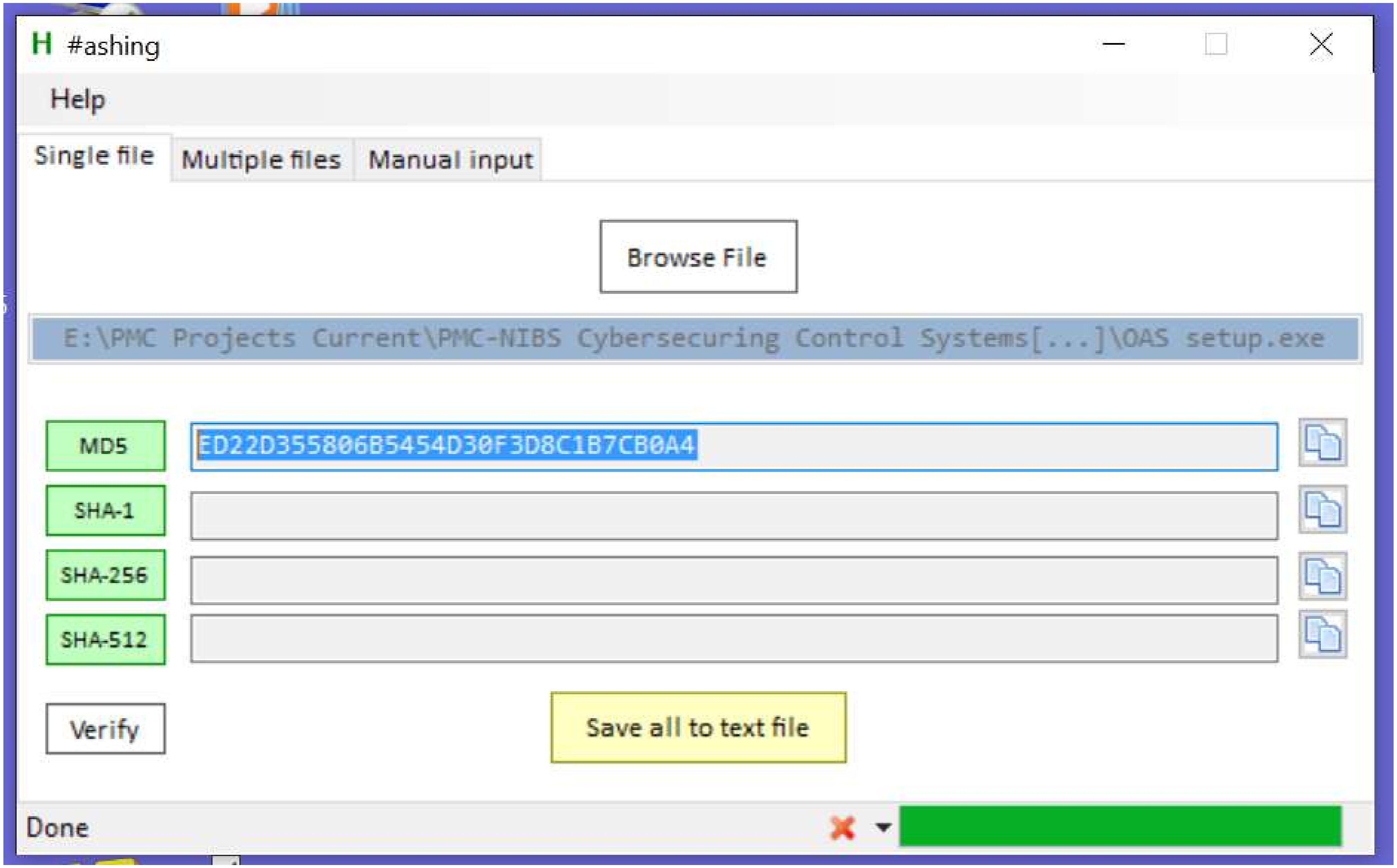
After the tool has been in place for a period of time, the user accepts this list as representative of the normal conversations expected from their ICS/SCADA and the list of conversations is established as a baseline fingerprint (whitelist) of accepted conversations.

Sophia monitors network traffic from which it extracts the source, destination, and port sets (conversations) between control system and networked components. These conversations are stored in real time to establish a list of conversations that are valid. Advanced three dimensional visualization tools provide users with an easy to understand interface to monitor expected communications and identify changes.

After the fingerprint is accepted, Sophia continues to monitor and capture conversations and generates an alarm on any conversation that is not a part of the system fingerprint. The user then analyzes the alarm with three choices:

- Add it to the white-list (fingerprint) – the conversation is valid.
- Add it to the black-list – not required for system operation, always alarm.
- Or do nothing and leave it on the ‘to be evaluated gray-list’

Software / Firmware Inventory Hash

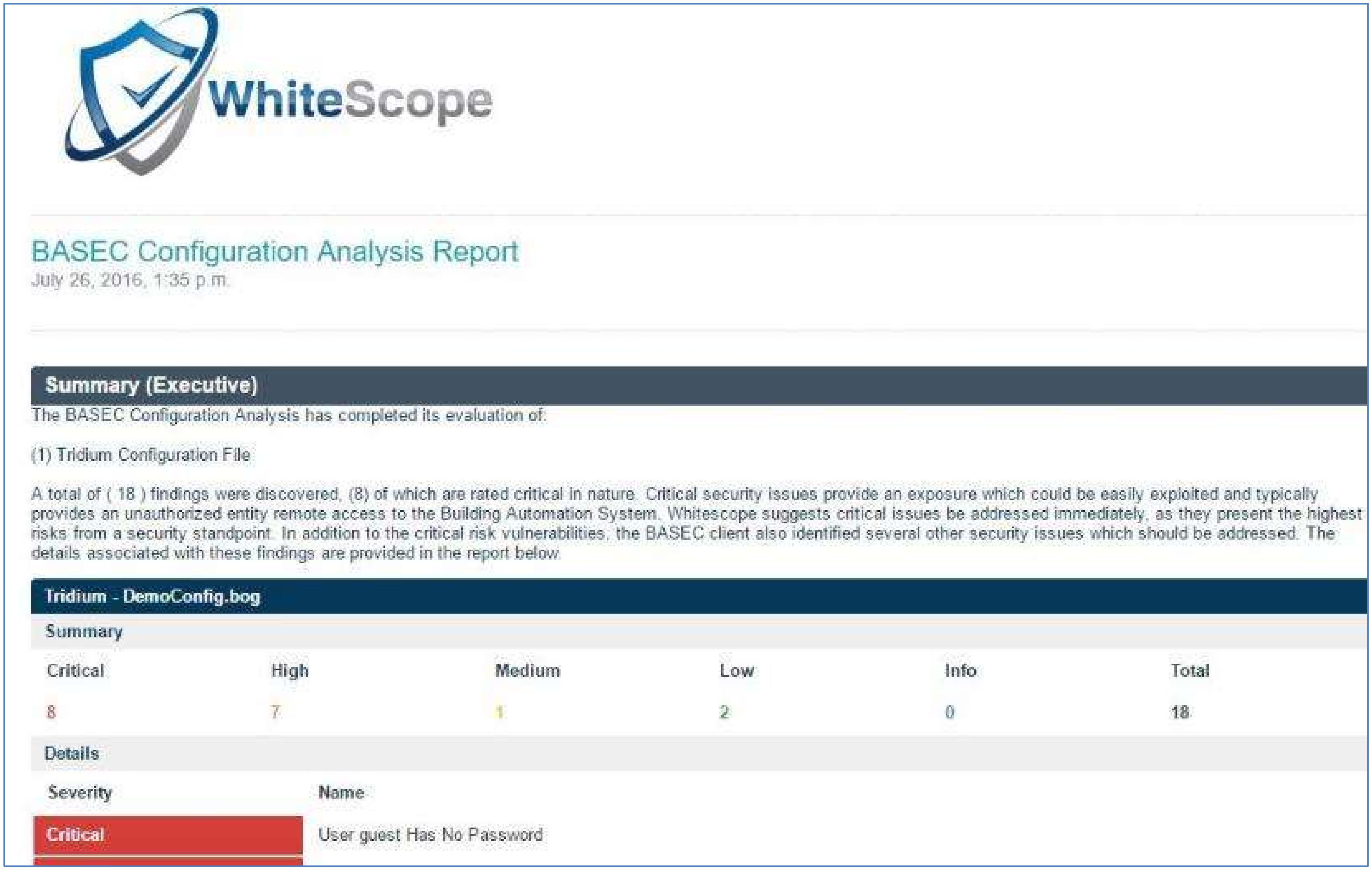


E:\PMC Projects Current\PMC-NIBS Cybersecuring Control Systems[...]\OAS setup.exe

MD5	ED22D355806B5454D30F3D8C1B7CB0A4
SHA-1	
SHA-256	
SHA-512	

Done

WhiteScope Configuration Analysis



BASEC Configuration Analysis Report

July 26, 2016, 1:35 p.m.

Summary (Executive)

The BASEC Configuration Analysis has completed its evaluation of:

(1) Tridium Configuration File

A total of (18) findings were discovered, (8) of which are rated critical in nature. Critical security issues provide an exposure which could be easily exploited and typically provides an unauthorized entity remote access to the Building Automation System. Whitescope suggests critical issues be addressed immediately, as they present the highest risks from a security standpoint. In addition to the critical risk vulnerabilities, the BASEC client also identified several other security issues which should be addressed. The details associated with these findings are provided in the report below.

Tridium - DemoConfig.bog

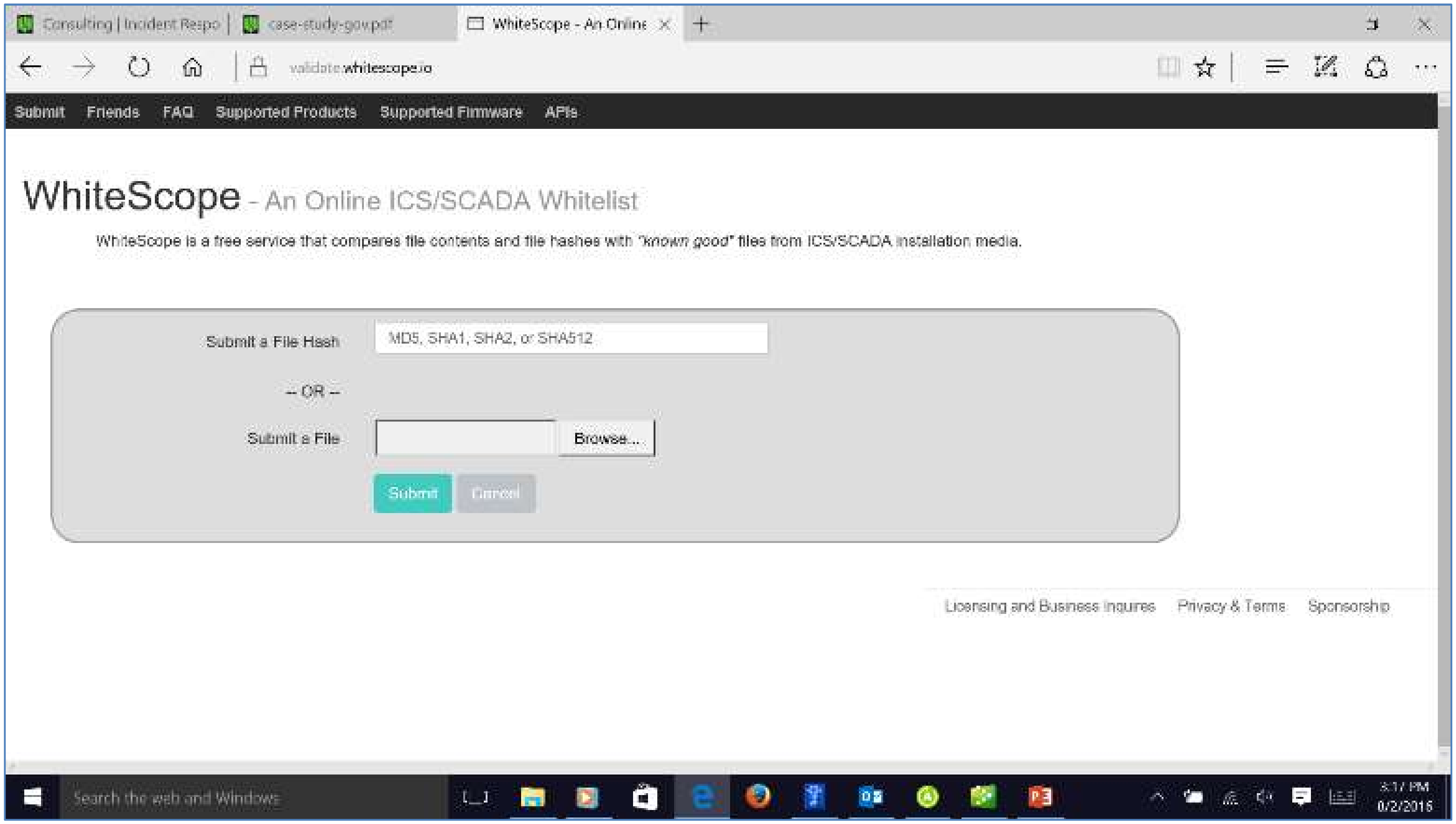
Summary

Critical	High	Medium	Low	Info	Total
8	7	1	2	0	18

Details

Severity	Name
Critical	User guest Has No Password

WhiteScope Whitelist Products



WhiteScope - An Online ICS/SCADA Whitelist

WhiteScope is a free service that compares file contents and file hashes with *"known good"* files from ICS/SCADA installation media.

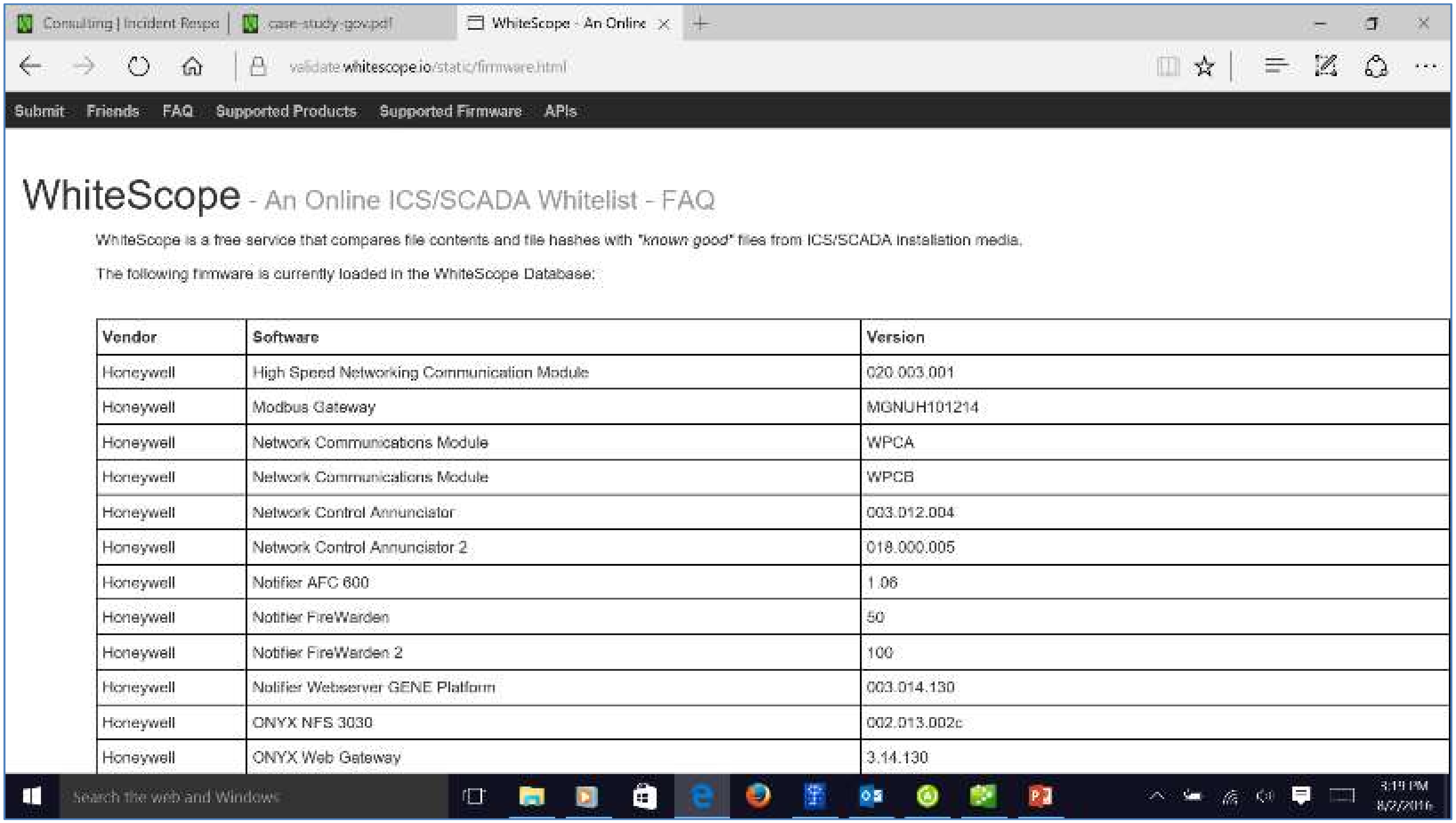
Submit a File Hash: MD5, SHA1, SHA2, or SHA512

-- OR --

Submit a File

https://validate.whitescope.io/

WhiteScope Whitelist Firmware



WhiteScope - An Online ICS/SCADA Whitelist - FAQ

WhiteScope is a free service that compares file contents and file hashes with *"known good"* files from ICS/SCADA installation media.

The following firmware is currently loaded in the WhiteScope Database:

Vendor	Software	Version
Honeywell	High Speed Networking Communication Module	020.003.001
Honeywell	Modbus Gateway	MGNUH101214
Honeywell	Network Communications Module	WPCA
Honeywell	Network Communications Module	WPCB
Honeywell	Network Control Annunciator	003.012.004
Honeywell	Network Control Annunciator 2	018.000.005
Honeywell	Notifier AFC 600	1.06
Honeywell	Notifier FireWarden	50
Honeywell	Notifier FireWarden 2	100
Honeywell	Notifier Webserver GENE Platform	003.014.130
Honeywell	ONYX NFS 3030	002.013.002c
Honeywell	ONYX Web Gateway	3.14.130

https://validate.whitescope.io/static/firmware.html

DHS CSET

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

CSET®

CYBER SECURITY EVALUATION TOOL

Version 8.0

Homeland Security

NCCIC / ICS-CERT

CSET Download:

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

CSET Process

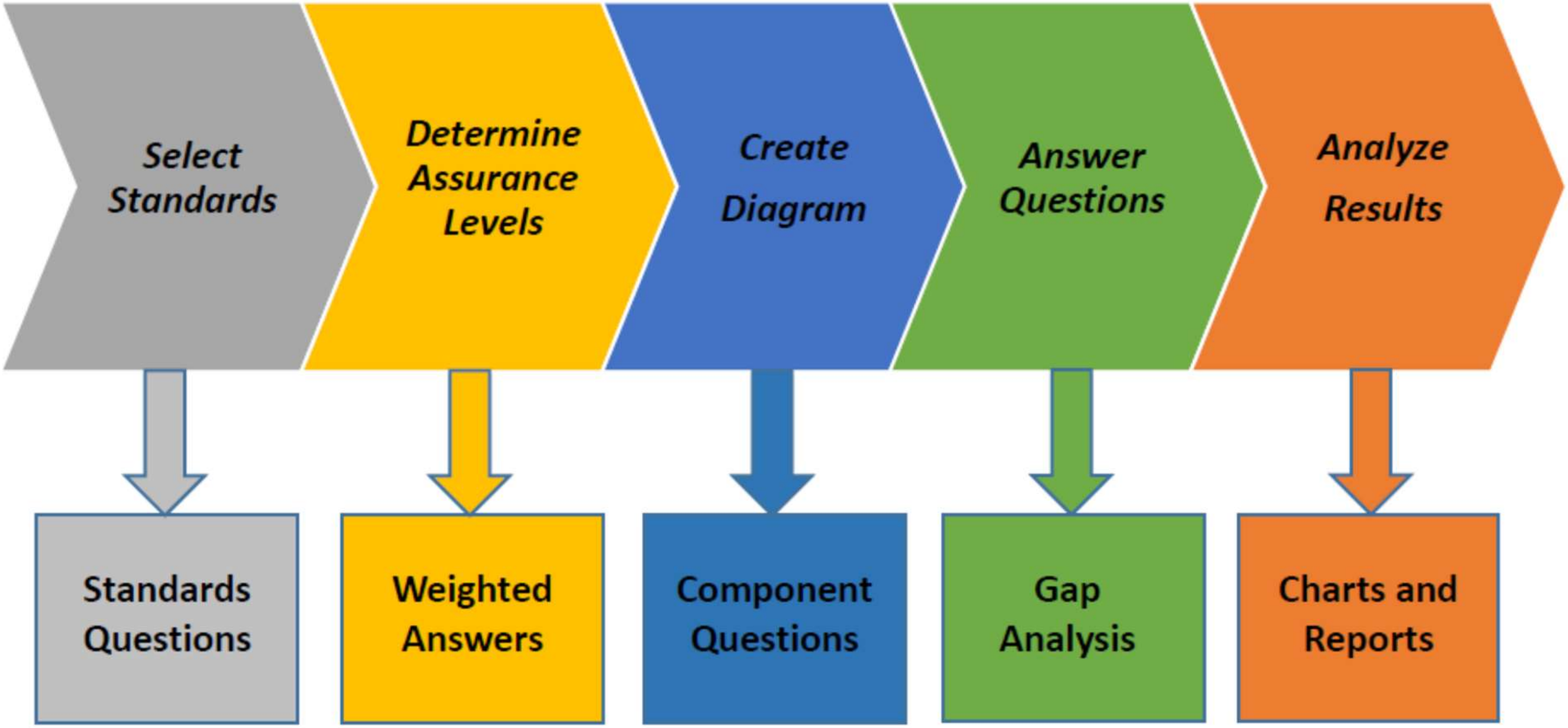
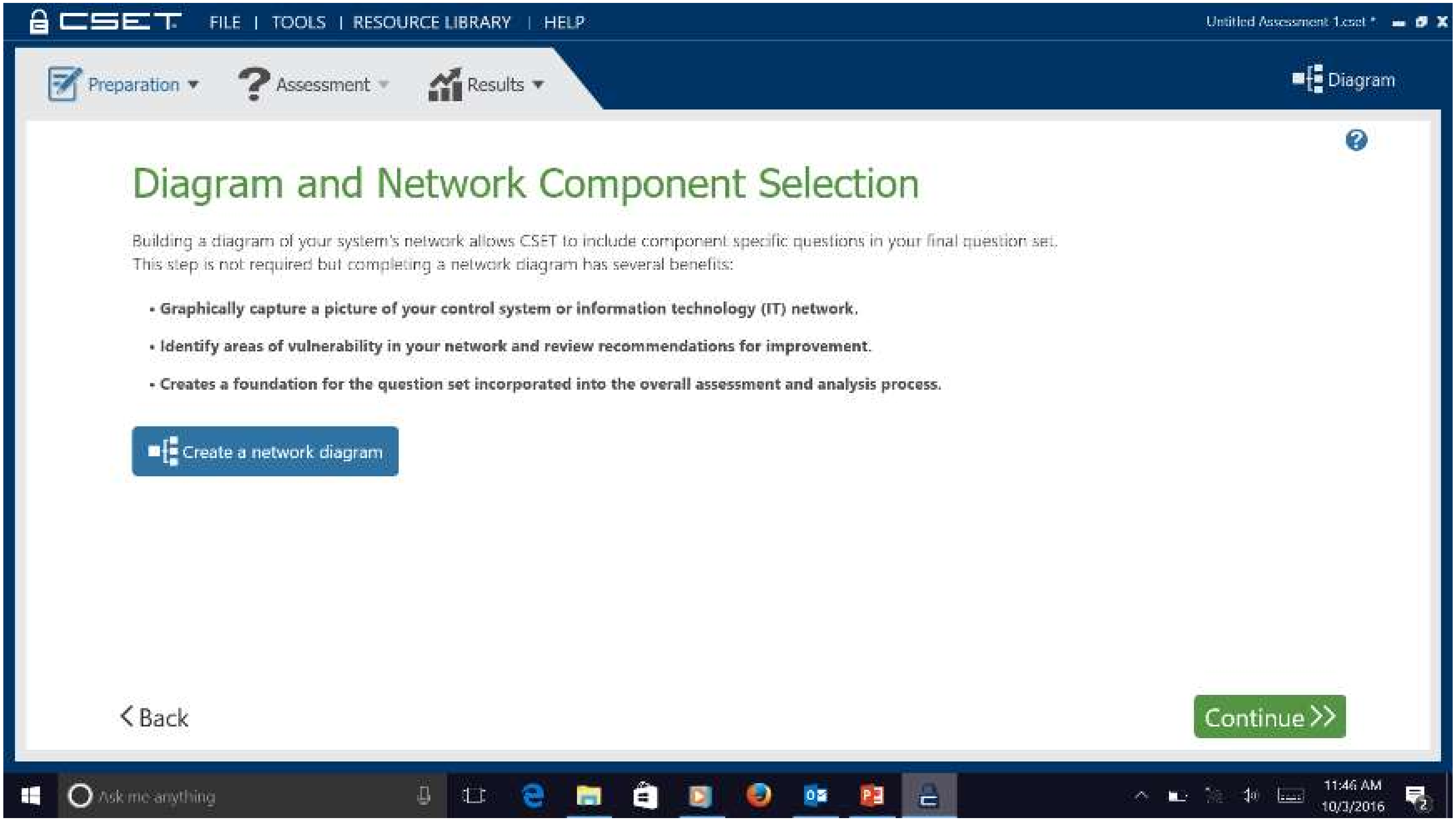


Figure 3-1. CSET process.

Design and Network Component Selection



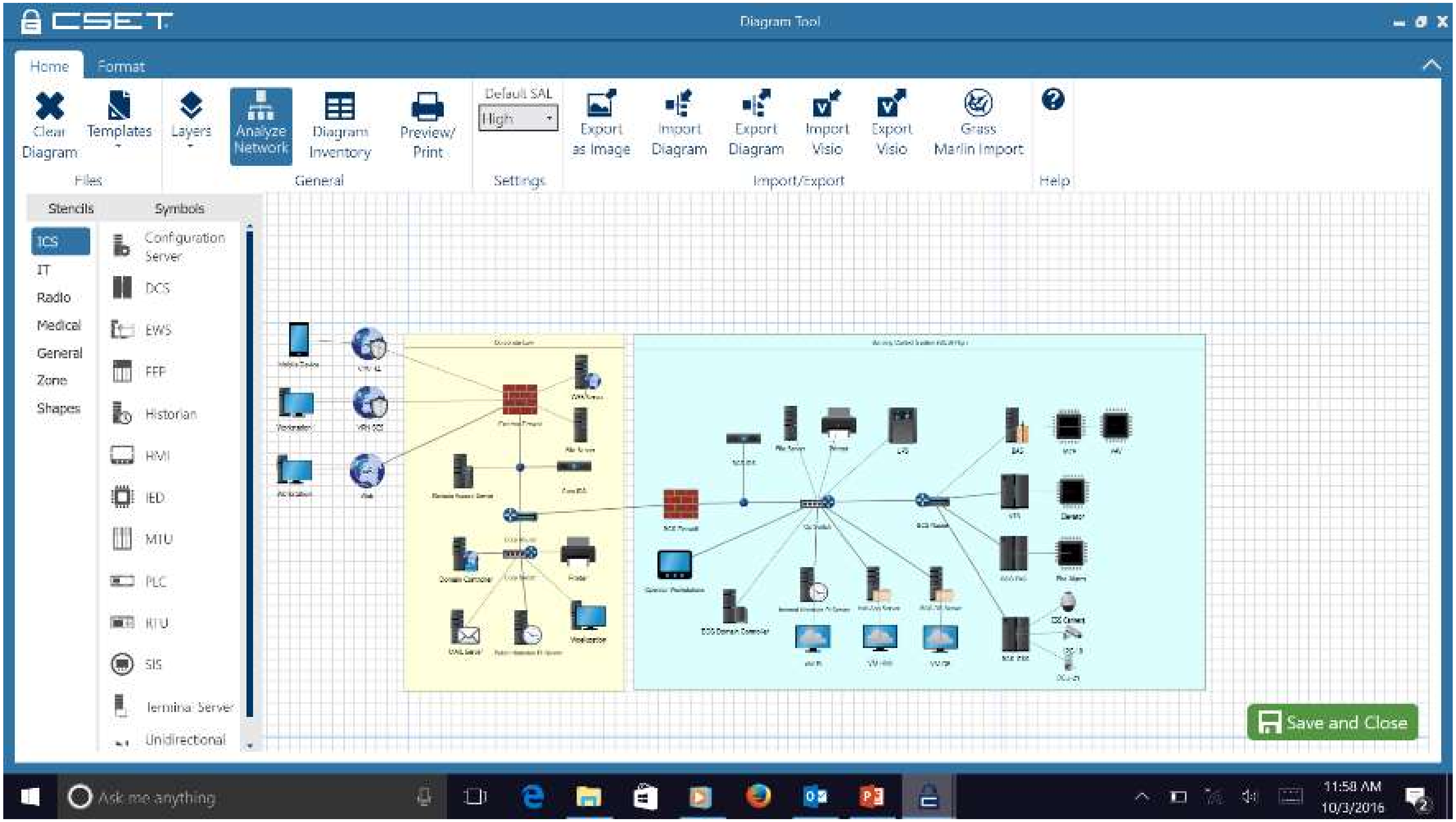
CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset *
Preparation
Assessment
Results
Diagram

Diagram and Network Component Selection

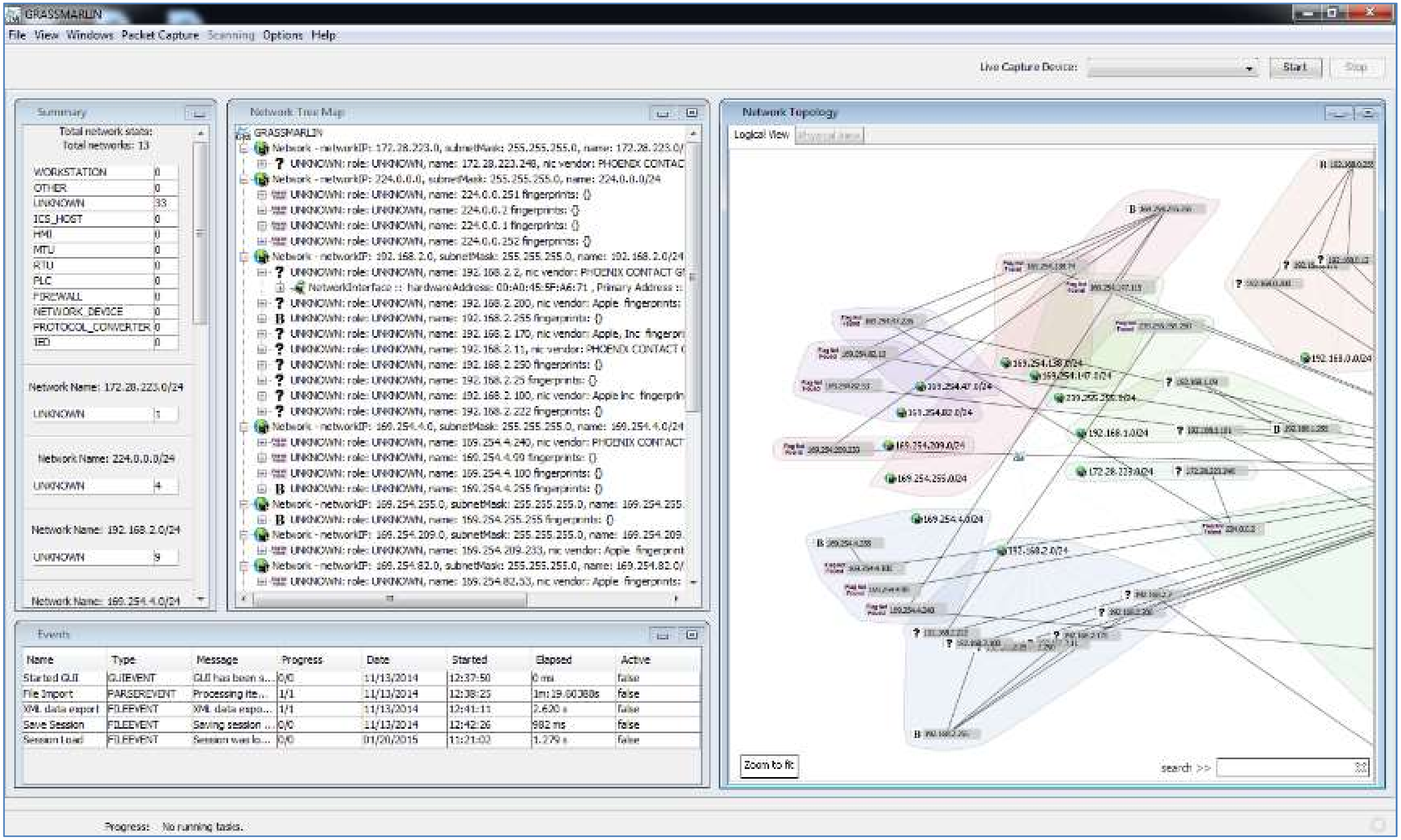
Building a diagram of your system's network allows CSET to include component specific questions in your final question set. This step is not required but completing a network diagram has several benefits:

- **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



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

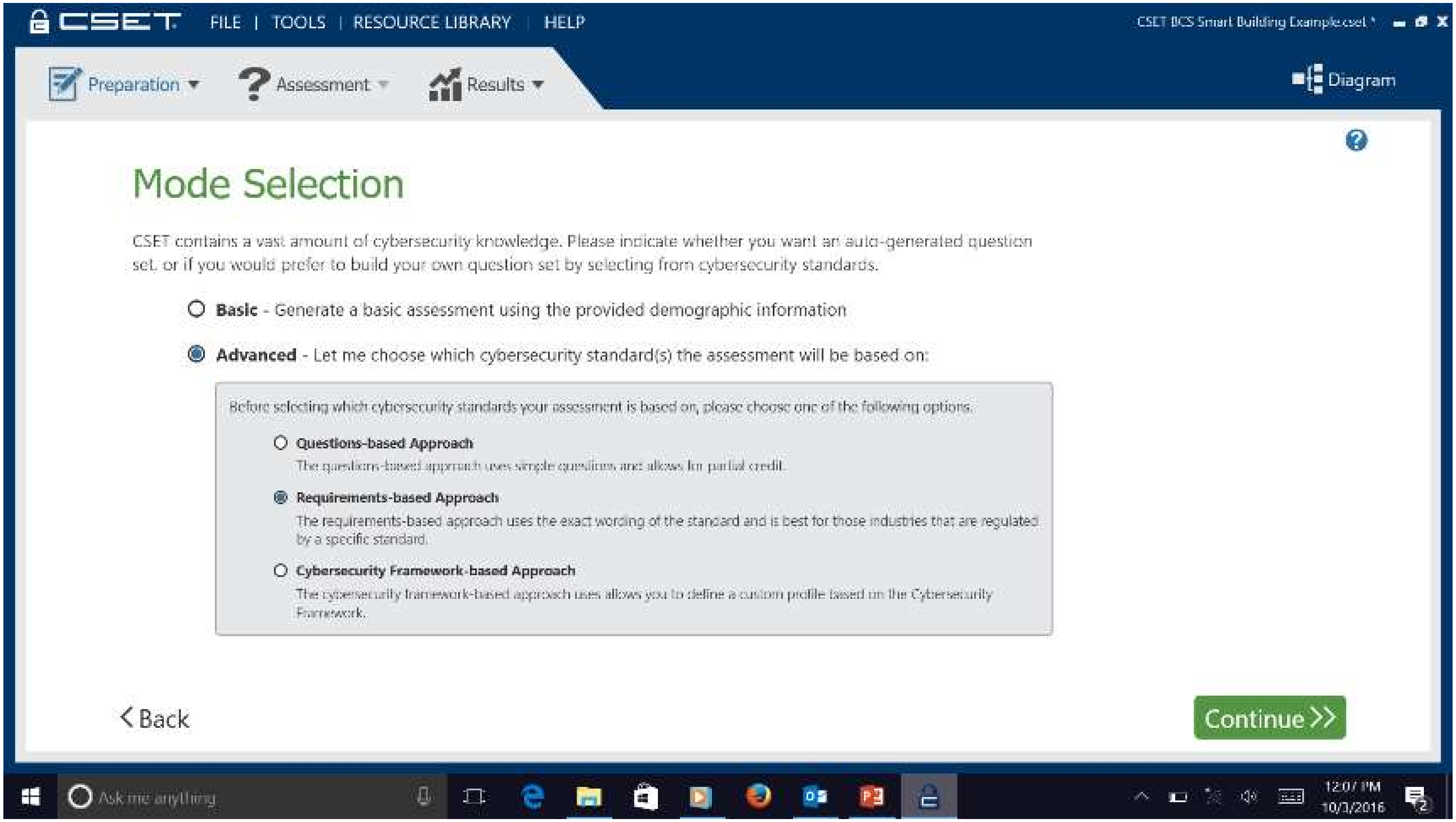
```
GRASSMARLIN
  Network - networkIP: 172.28.223.0, subnetMask: 255.255.255.0, name: 172.28.223.0/
    ? UNKNOWN: role: UNKNOWN, name: 172.28.223.248, nic vendor: PHOENIX CONTAC
  Network - networkIP: 224.0.0.0, subnetMask: 255.255.255.0, name: 224.0.0.0/24
    UNKNOWN: role: UNKNOWN, name: 224.0.0.251 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 G
      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.

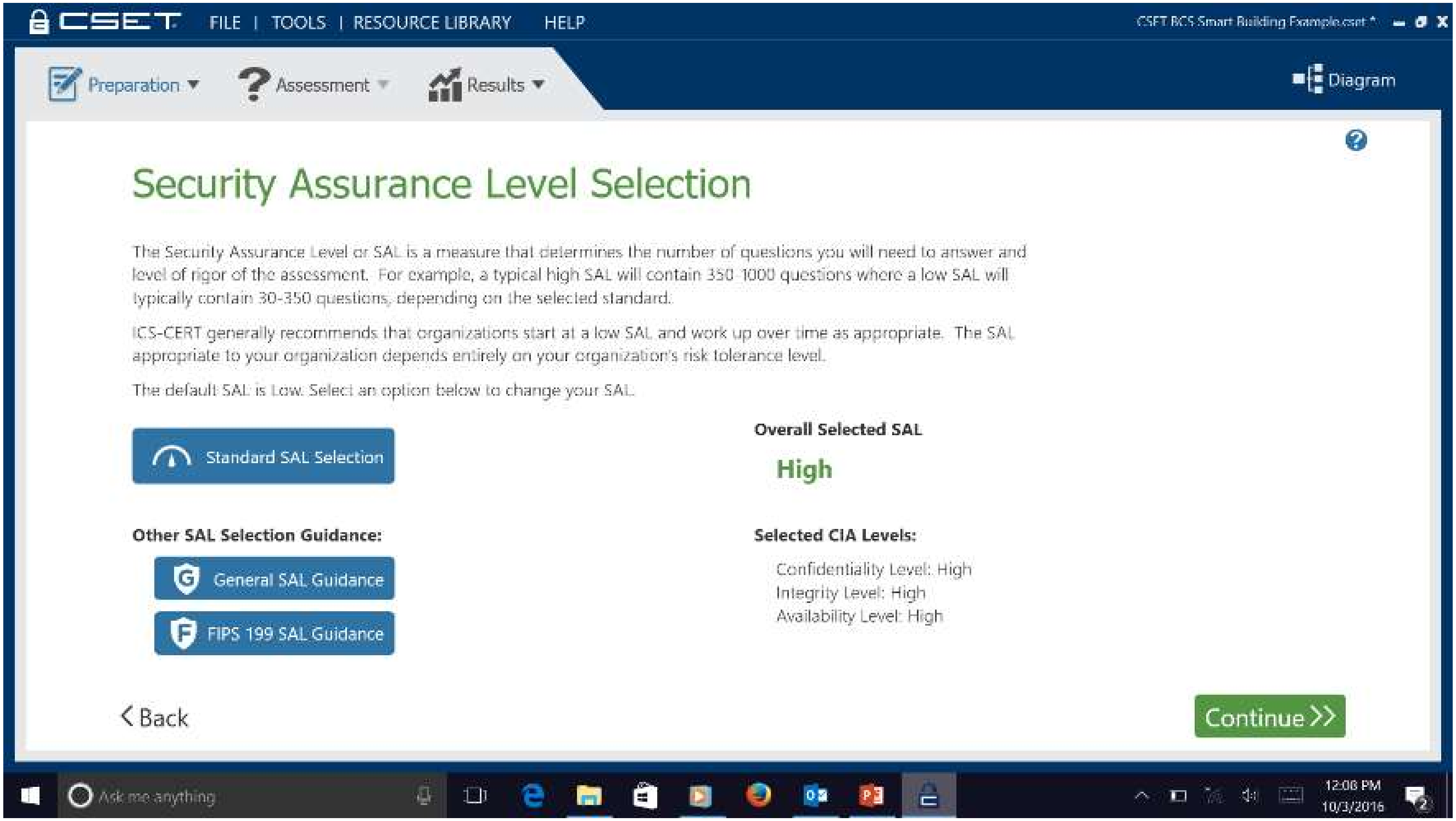
● **Requirements-based Approach**
The requirements-based approach uses the exact wording of the standard and is best for those industries that are regulated by a specific standard.

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

< Back

Continue >>

Security Assurance Level Selection



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

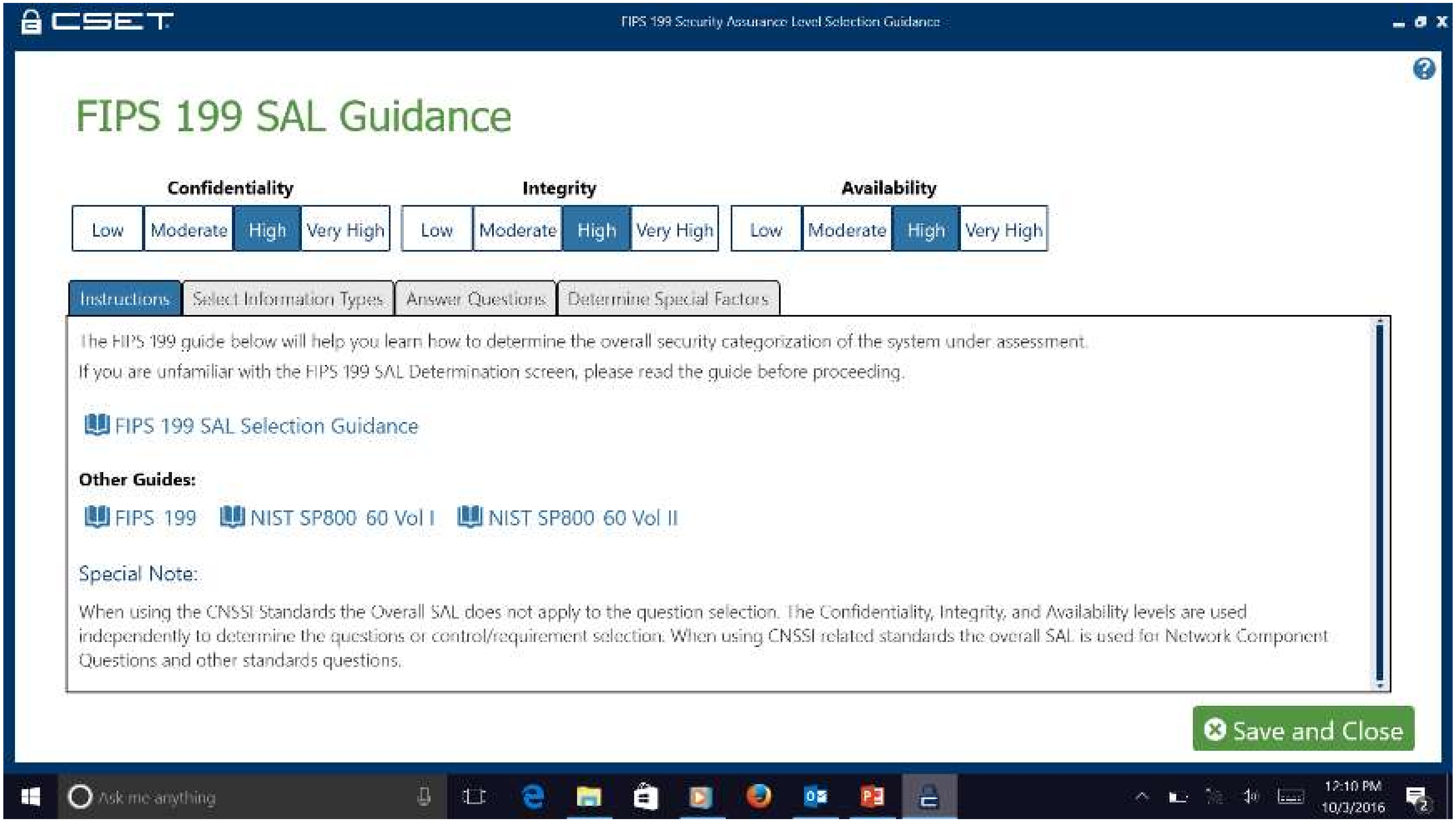
High

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 Low Moderate [✓ High] Very High

Integrity Low Moderate [✓ High] Very High

Availability 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.

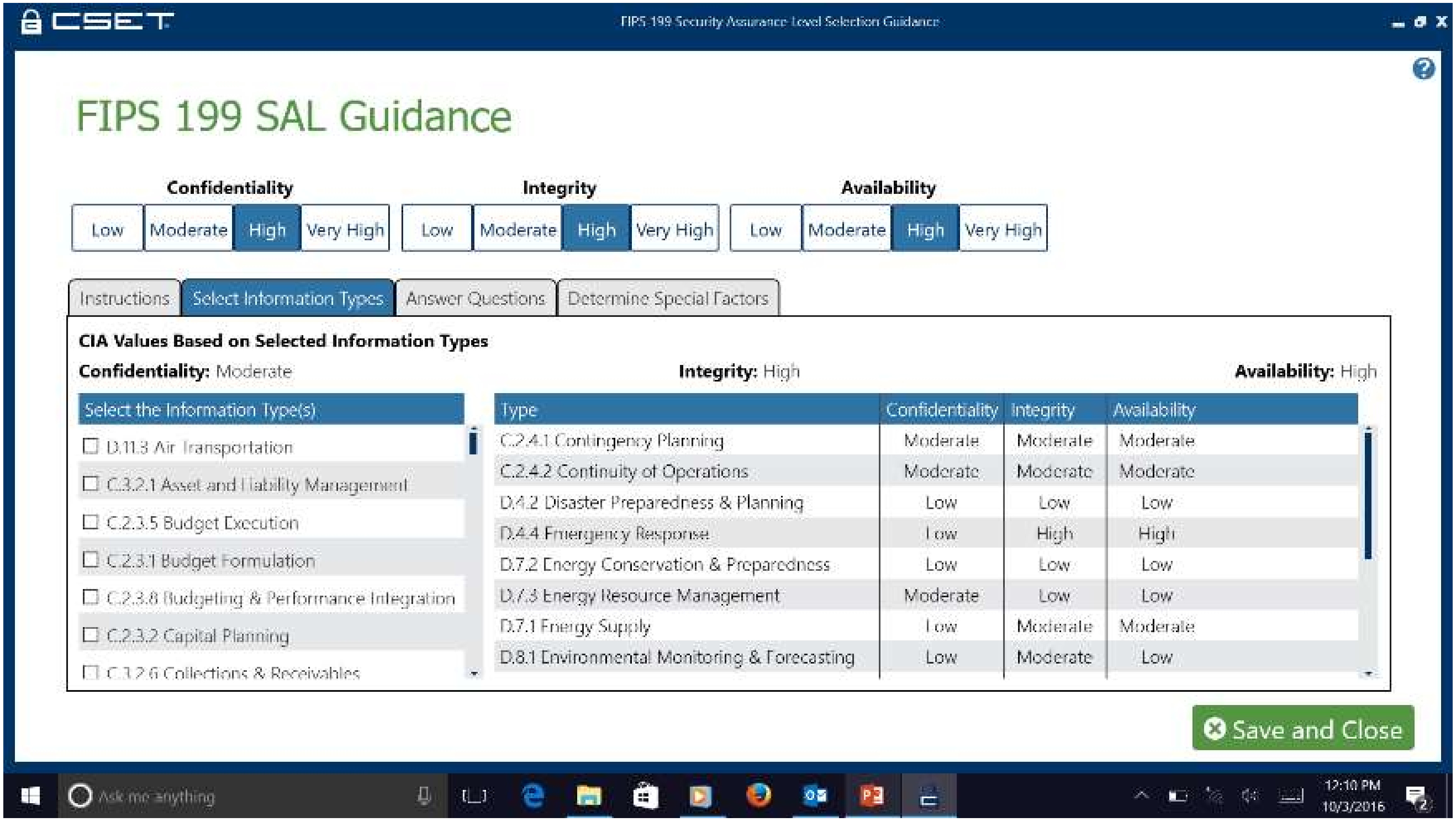
FIPS 199 SAL Impact Levels

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



FIPS 199 SAL Guidance

Confidentiality				Integrity				Availability			
Low	Moderate	**High**	Very High	Low	Moderate	**High**	Very High	Low	Moderate	**High**	Very High

CIA Values Based on Selected Information Types

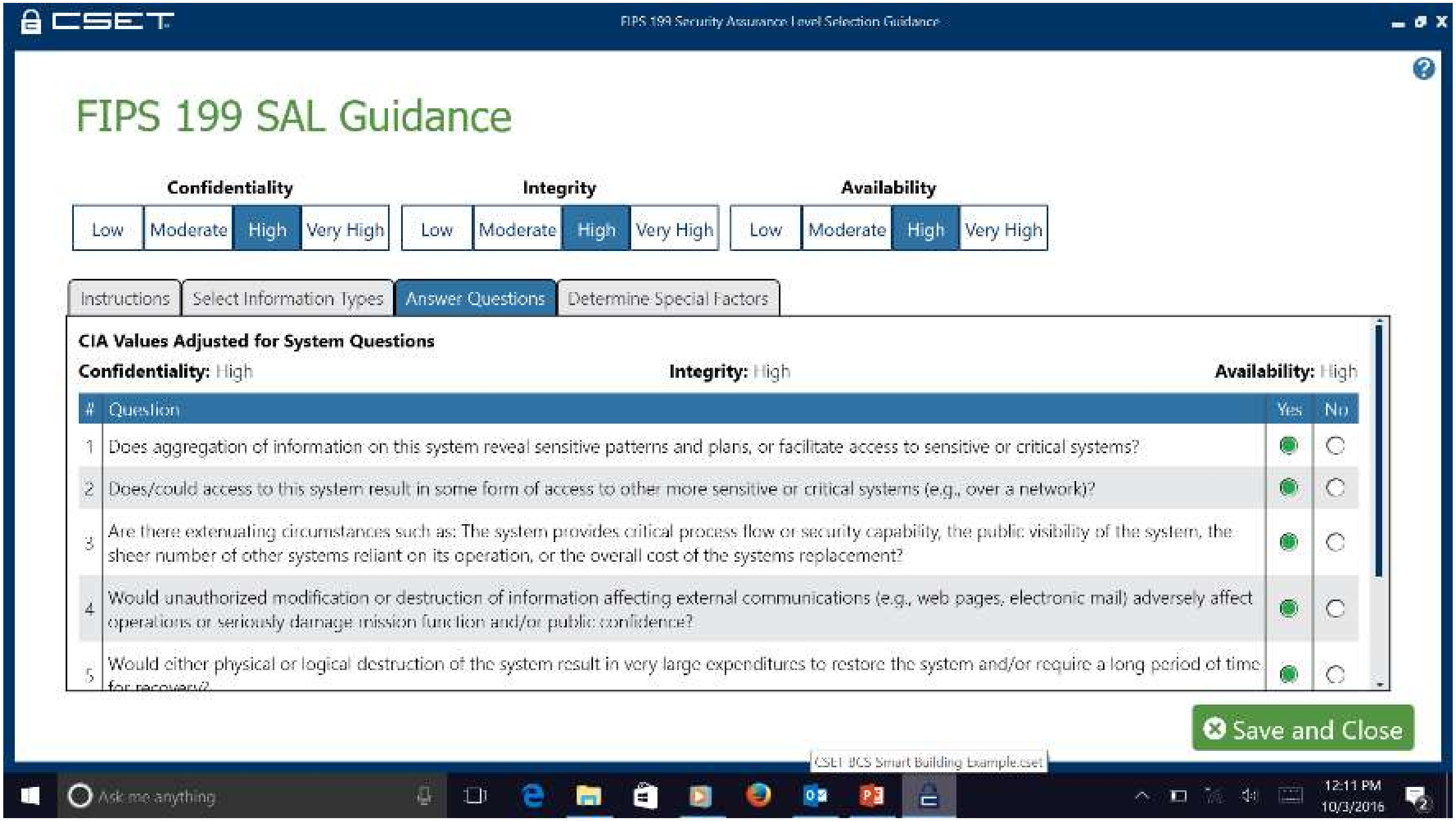
Confidentiality: Moderate **Integrity:** High **Availability:** High

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
Instructions
Select Information Types
Answer Questions
Determine Special Factors
Save and Close
CSET BCS Smart Building Example.cset
Ask me anything
12:11 PM
10/3/2016

FIPS 199 SAL Guidance

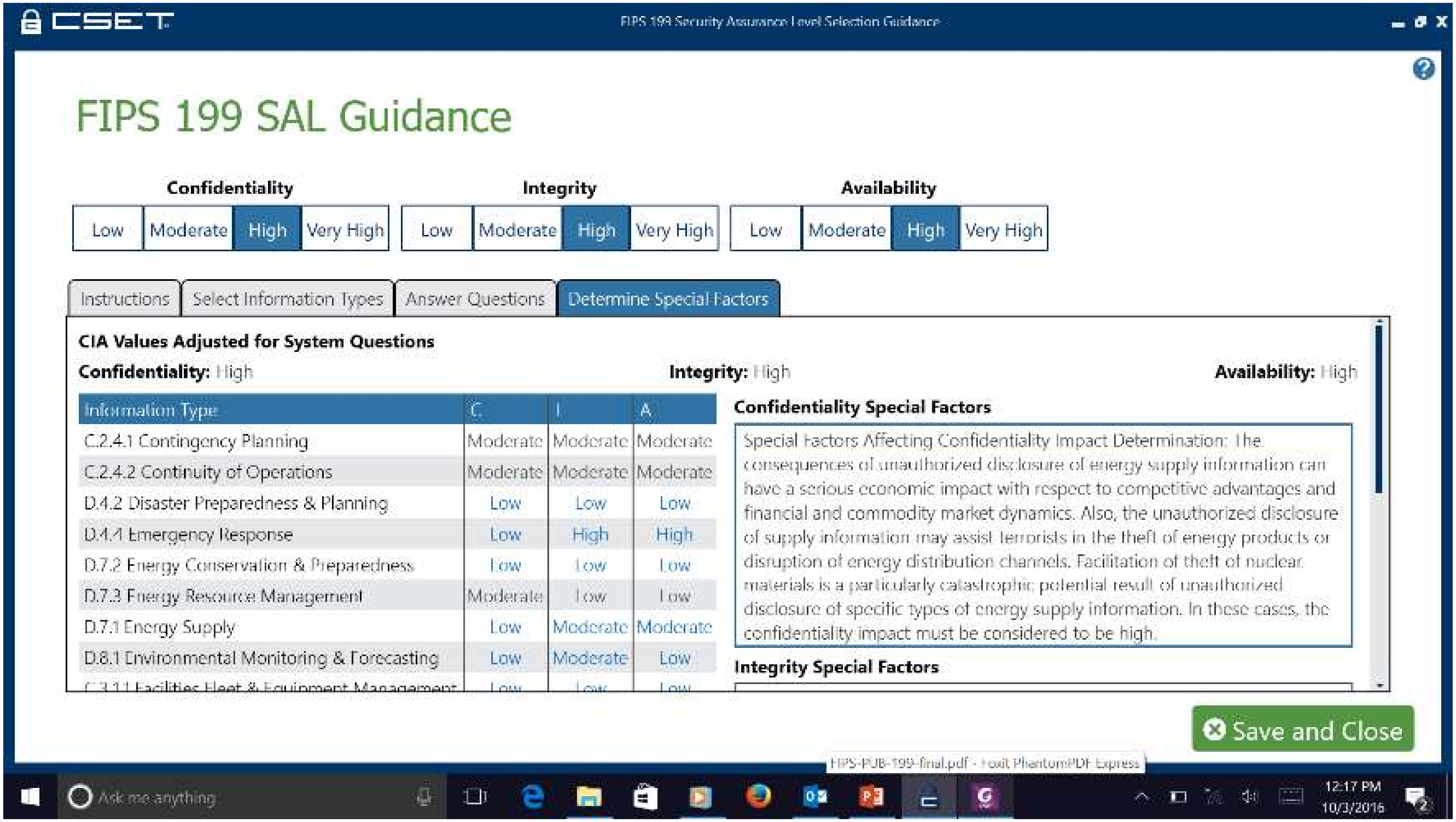
Confidentiality	Integrity	Availability
Low / Moderate / [✓ High] / Very High	Low / Moderate / [✓ High] / Very High	Low / Moderate / [✓ High] / Very High

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


CSET
FIPS 199 Security Assurance Level Selection Guidance
Save and Close
FIPS-PUB-199-final.pdf - Foxit PhantomPDF Express
Ask me anything
12:17 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

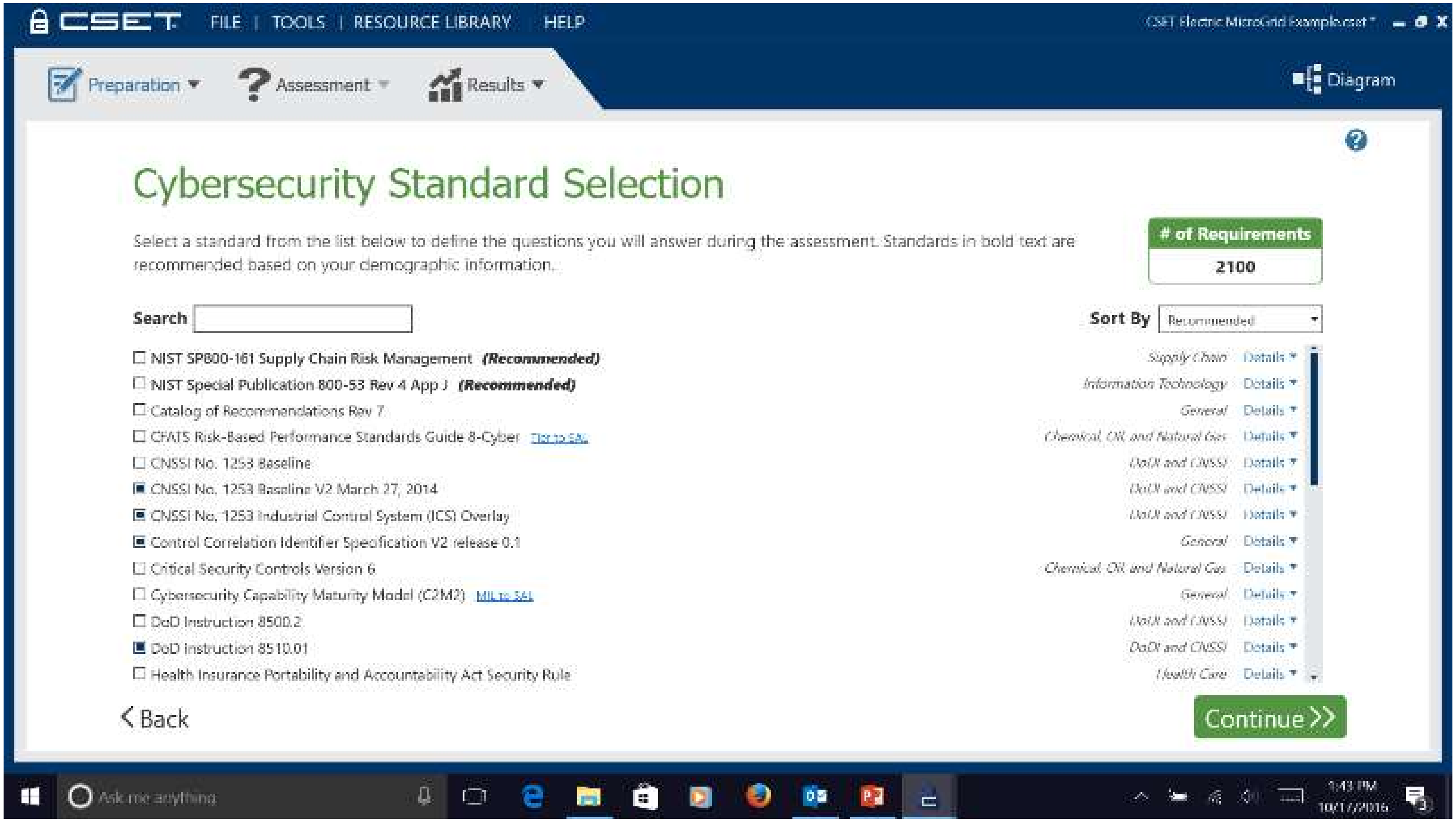
Information Type	C	I	A
C.2.4.1 Contingency Planning	Moderate	Moderate	Moderate
C.2.4.2 Continuity of Operations	Moderate	Moderate	Moderate
D.4.2 Disaster Preparedness & Planning	Low	Low	Low
D.4.4 Emergency Response	Low	High	High
D.7.2 Energy Conservation & Preparedness	Low	Low	Low
D.7.3 Energy Resource 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

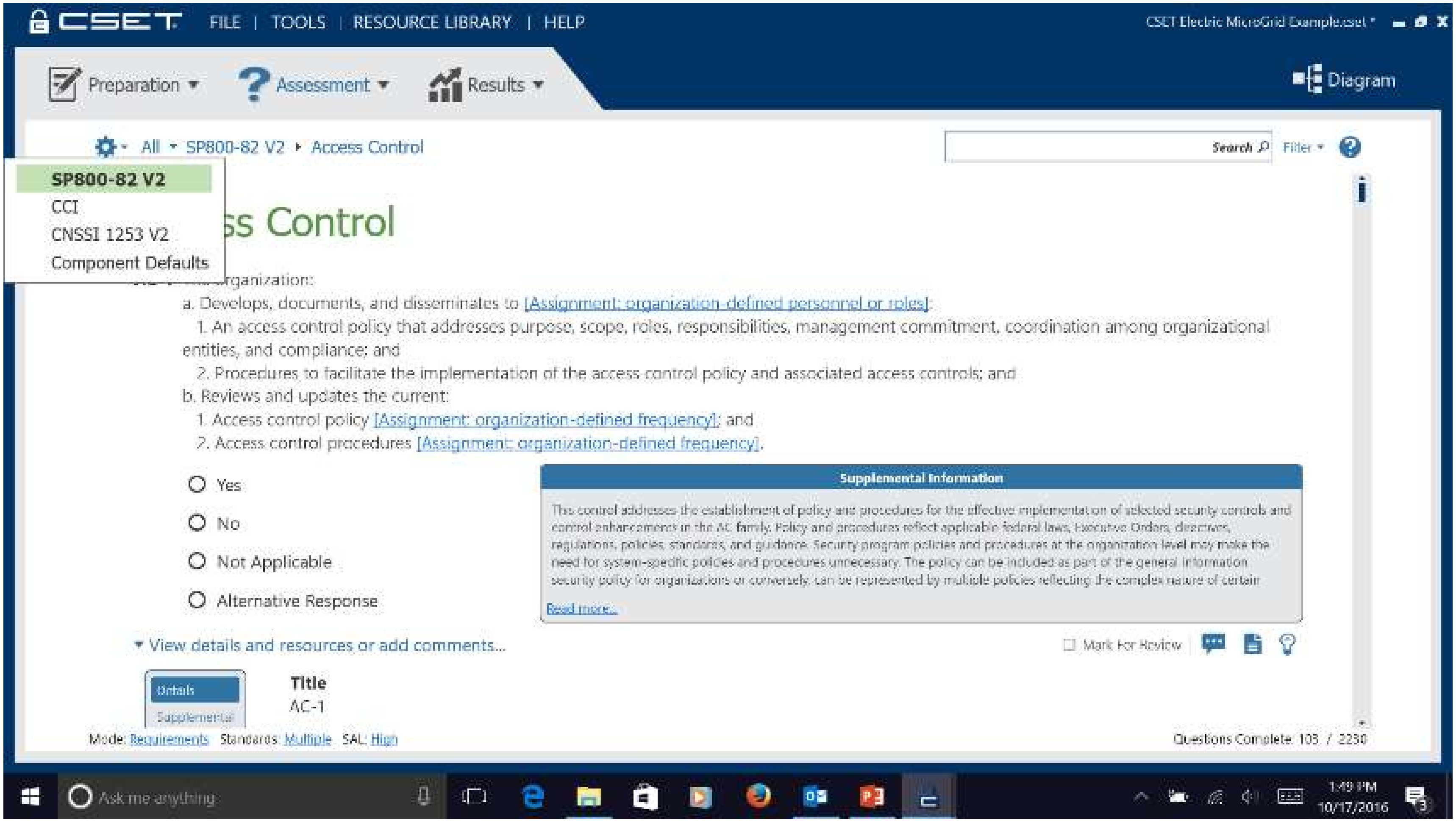
Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

# of Requirements
2100

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 ▾

Questions – Family, Detail, Info



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...

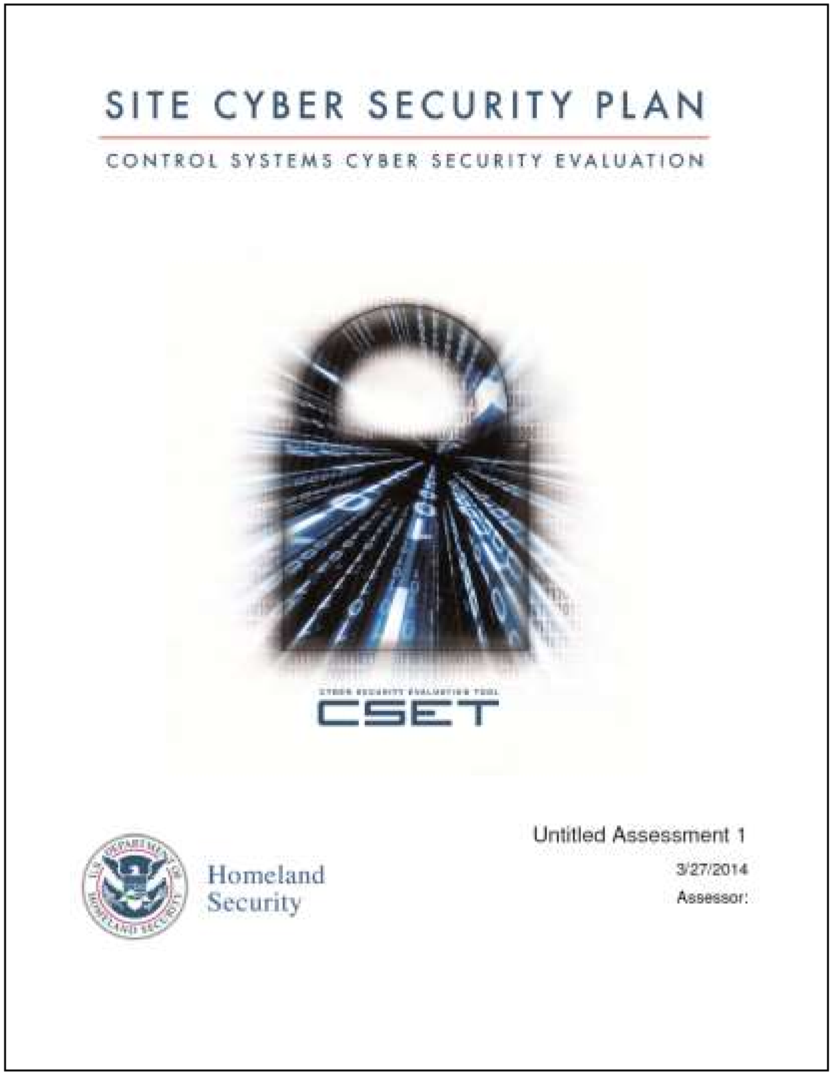
□ Mark For Review

Title
AC-1

Mode: Requirements Standards: Multiple SAL: High

Questions Complete: 103 / 2230

System Security Plan



SITE CYBER SECURITY PLAN

CONTROL SYSTEMS CYBER SECURITY EVALUATION

CYBER SECURITY EVALUATION TOOL

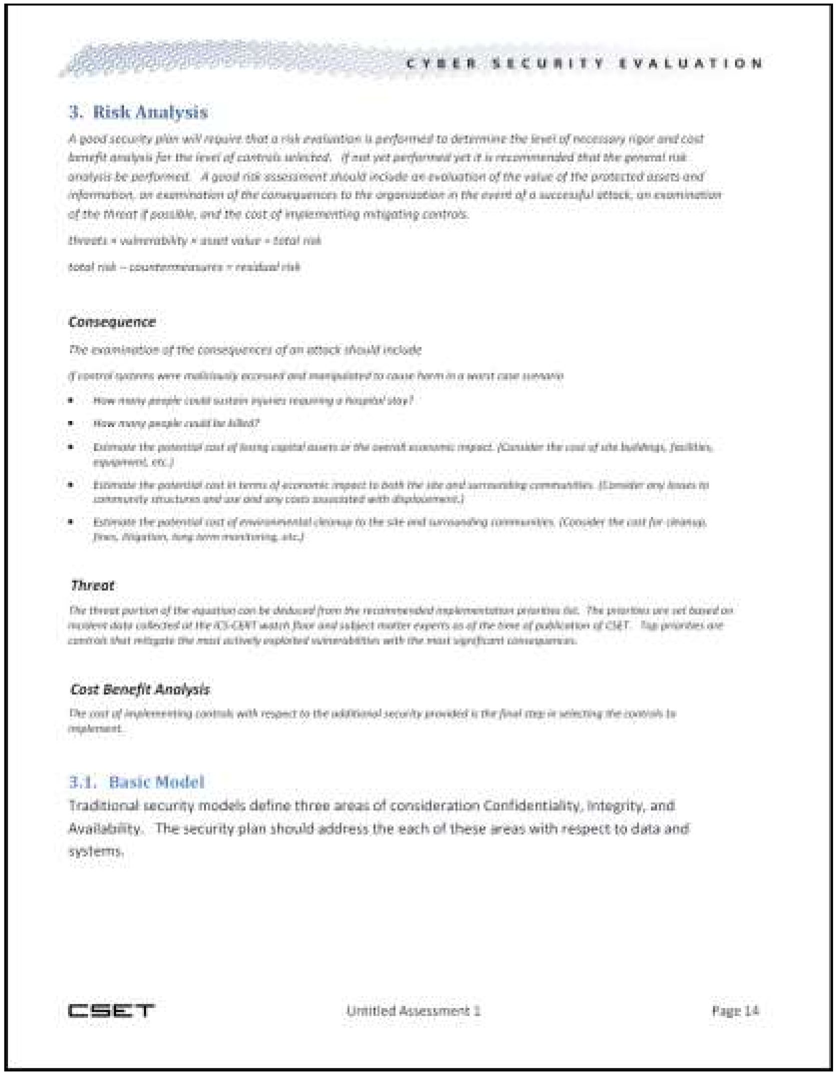
CSET

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.

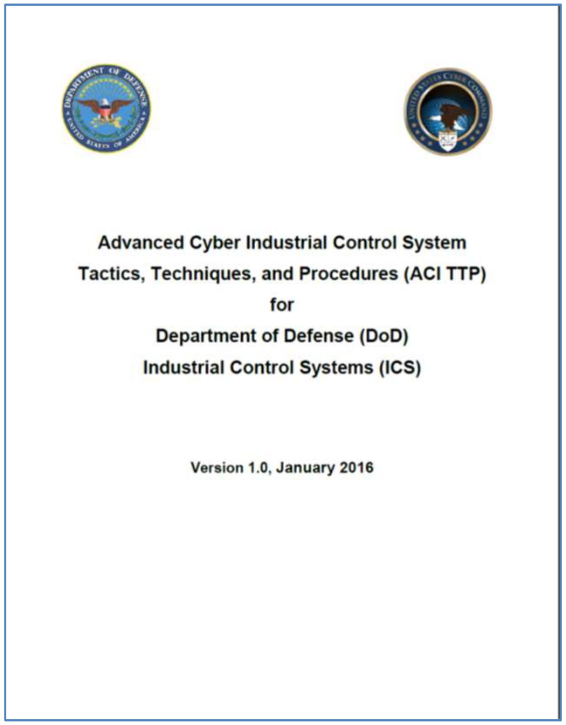
3.1. Basic Model

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

ACI 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)

- ***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***

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.

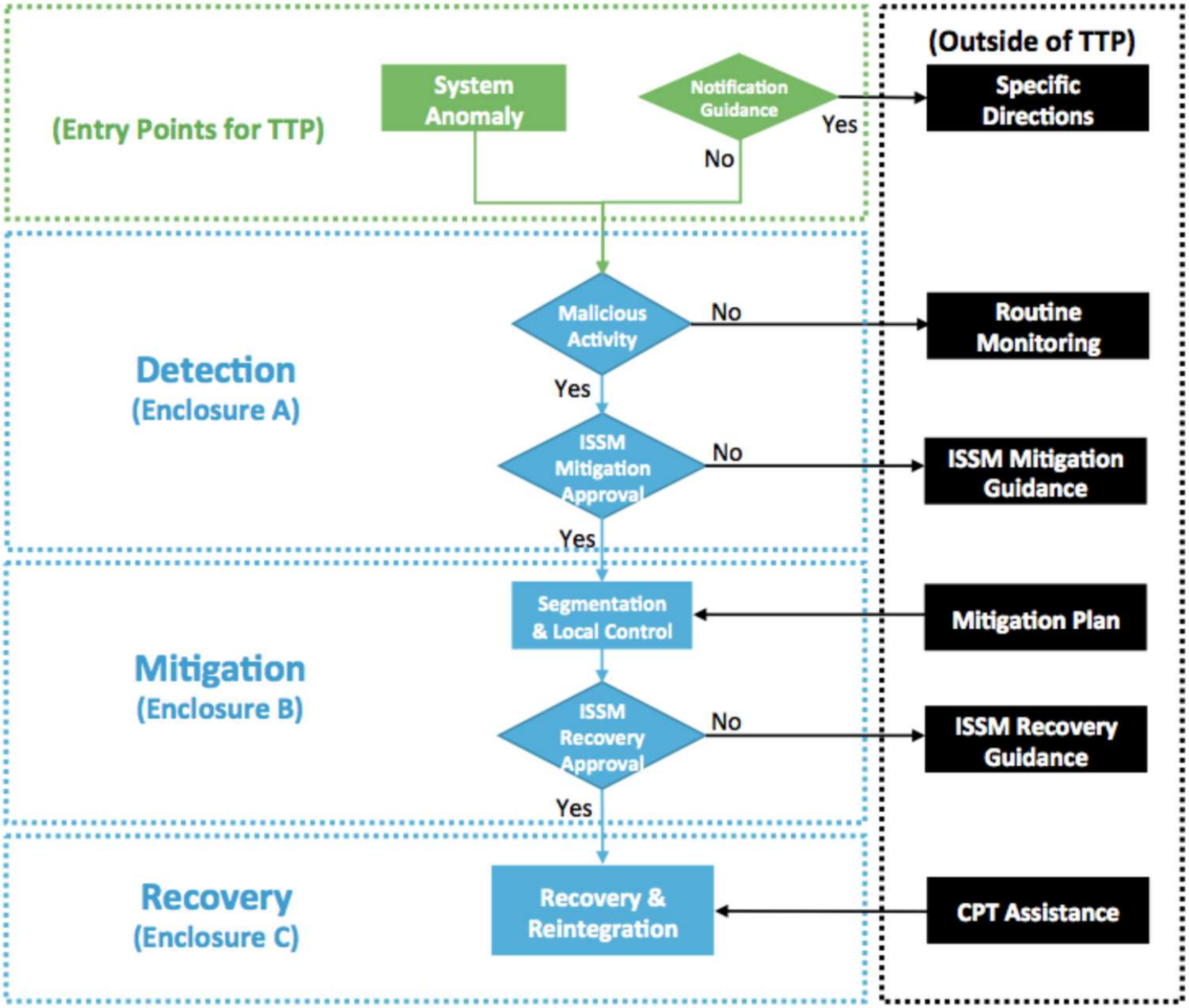
Before the ACI TTP are adopted, ICS and IT managers should establish what a FMC network is as it pertains to their specific installations and missions. The ACI TTP defines FMC as a functional recovery point for both the ICS and the SCADA. Once this is defined, ICS and IT managers should capture the FMC 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.**

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.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.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.

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.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

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.

b. Key Components

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

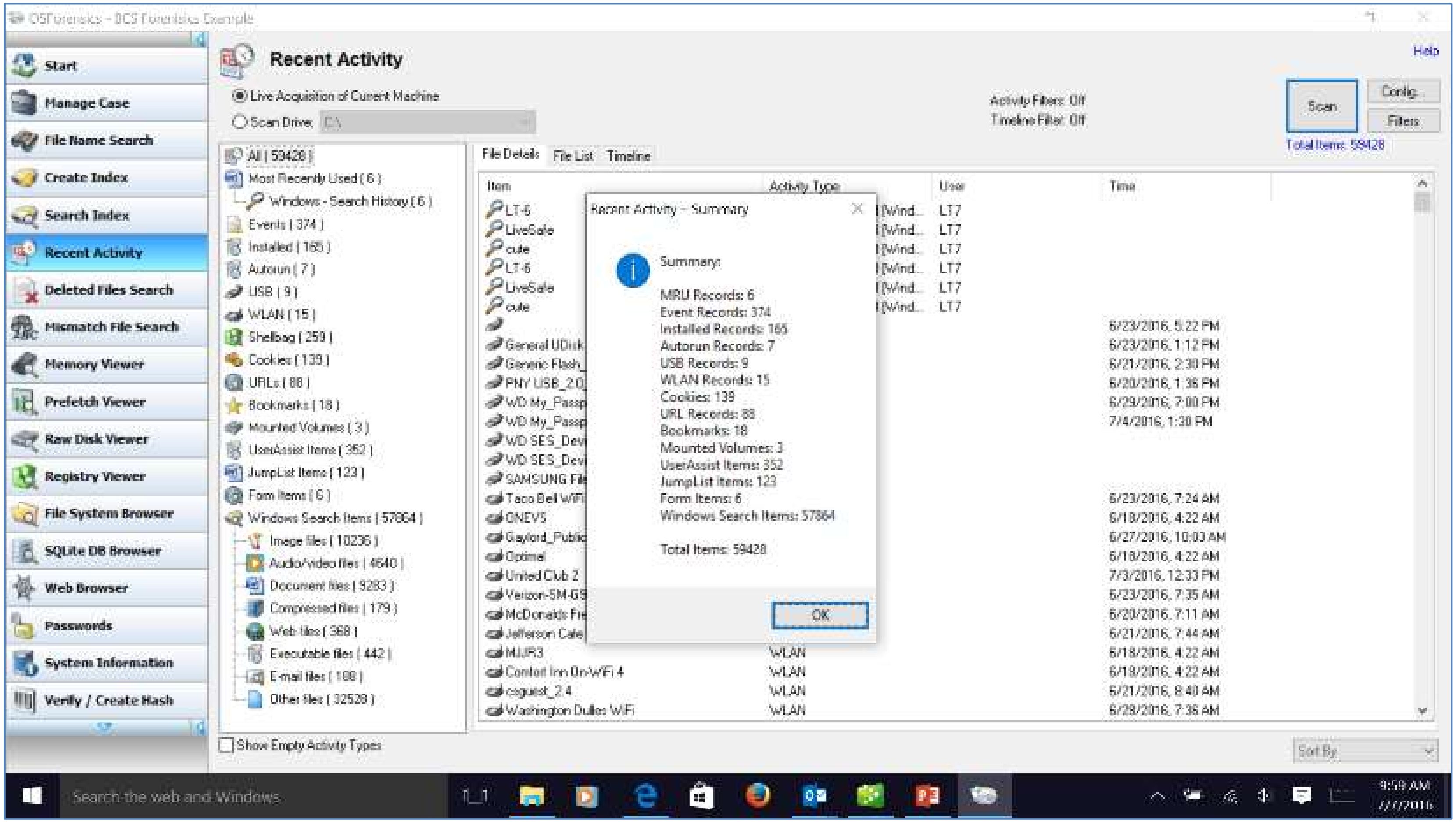
c. Prerequisites
(1) Administrative tools for acquisition
(2) Storage devices to capture and transport evidence

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 [108]
  - 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

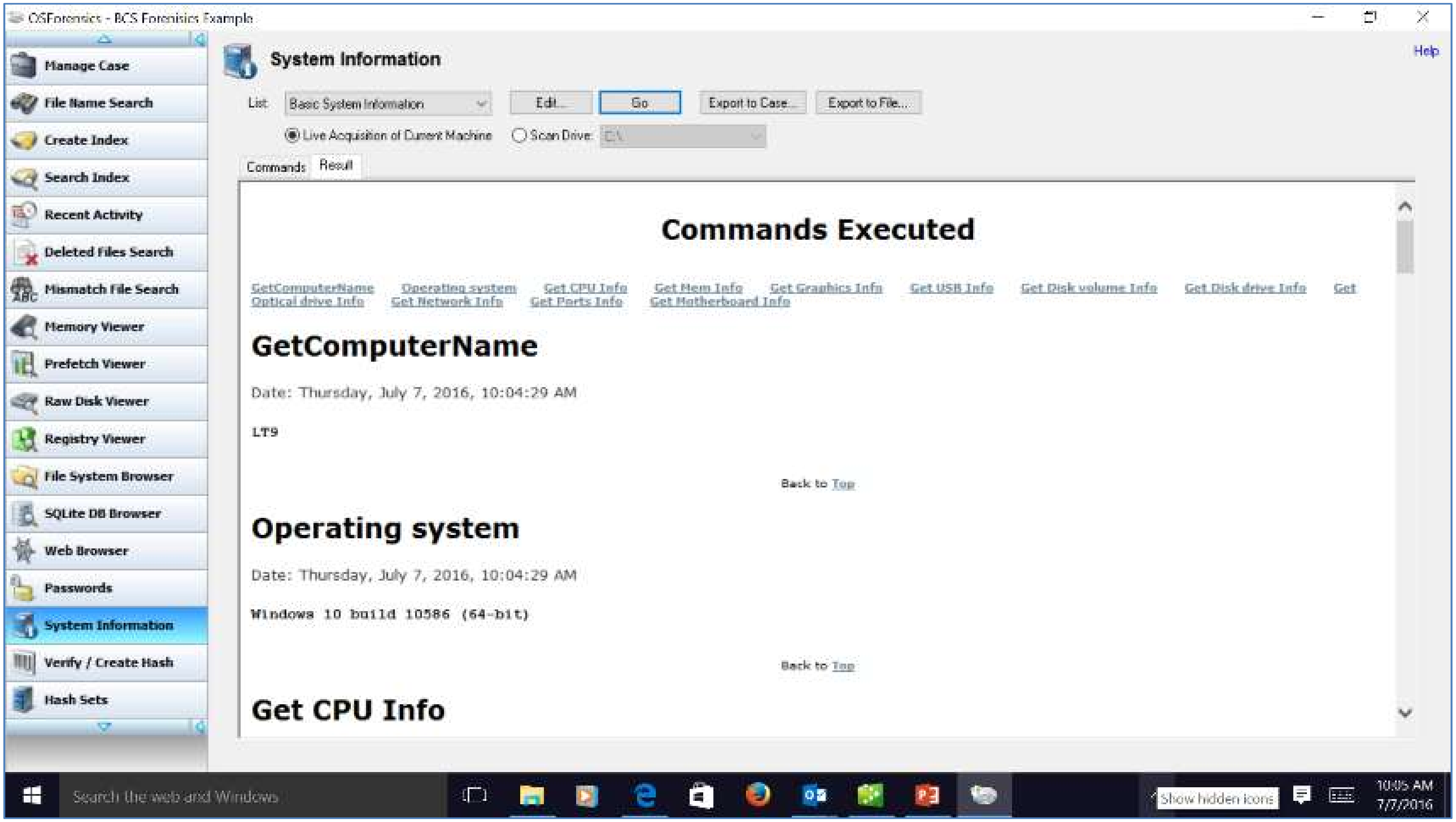
Summary:

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



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

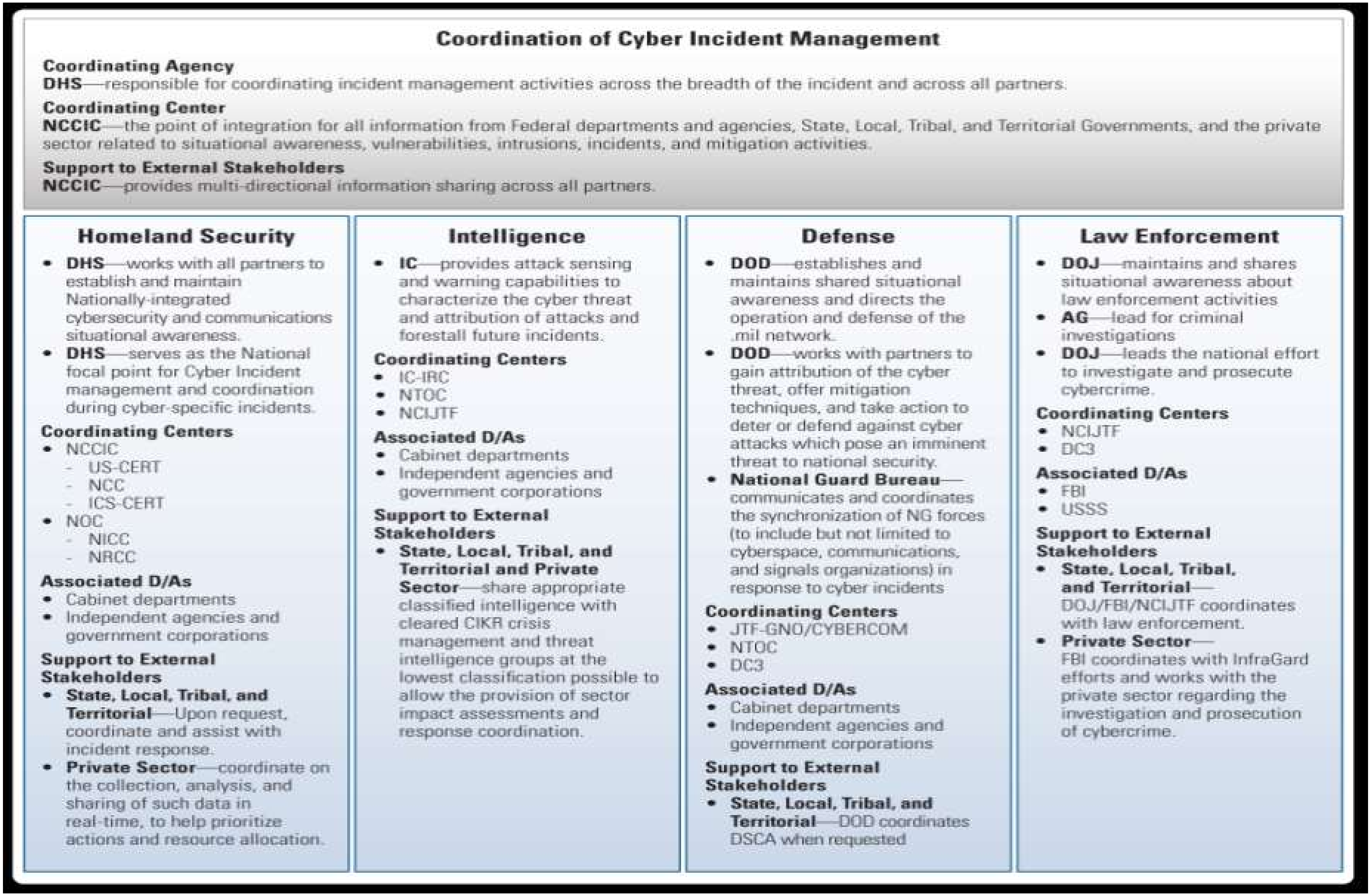
Date: Thursday, July 7, 2016, 10:04:29 AM

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

Back to Top

Get CPU Info

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

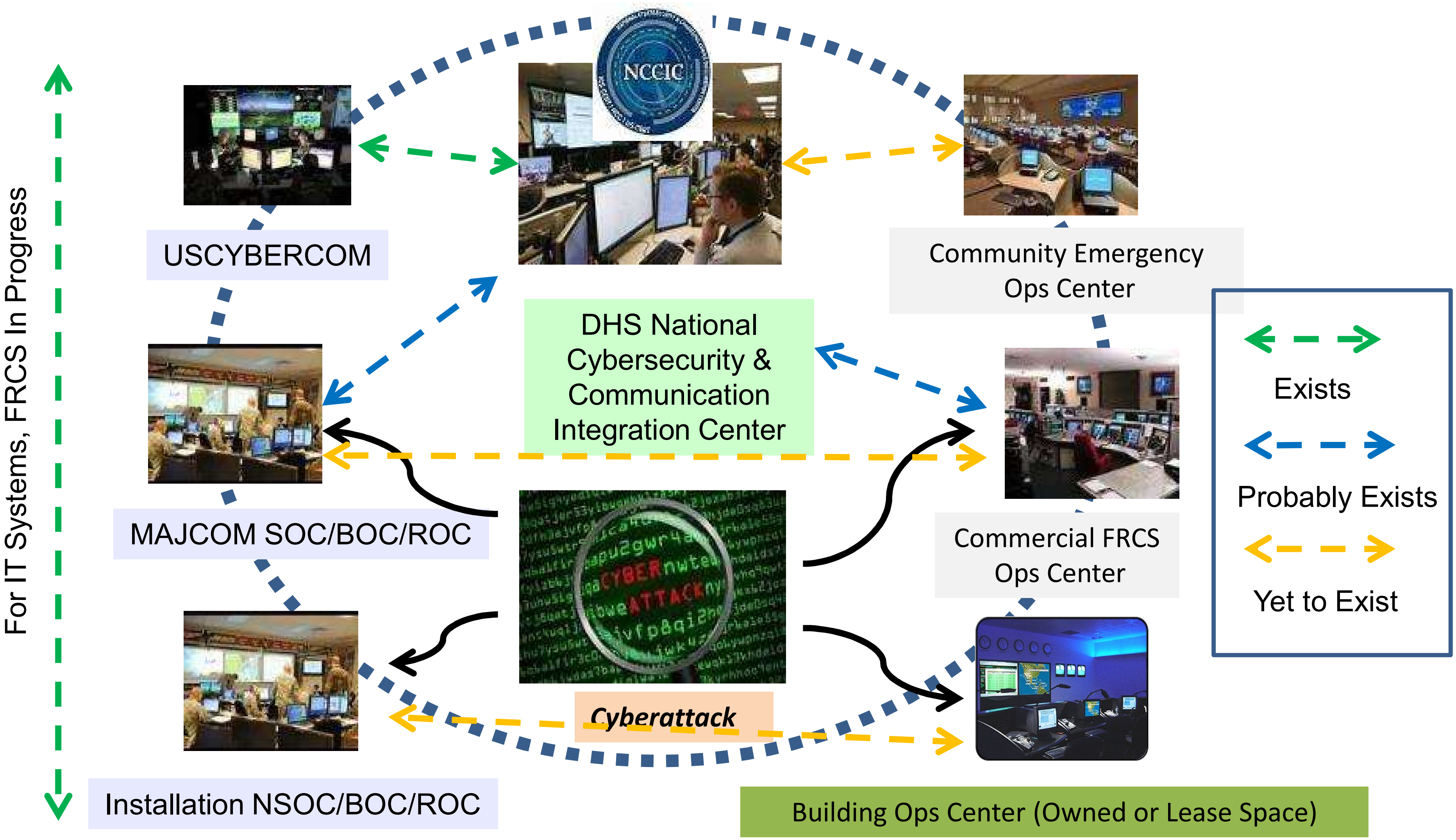
- FBI
- USSS

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



For IT Systems, FRCS In Progress

USCYBERCOM

DHS National Cybersecurity & Communication Integration Center

Community Emergency Ops Center

MAJCOM SOC/BOC/ROC

Commercial FRCS Ops Center

Cyberattack

Installation NSOC/BOC/ROC

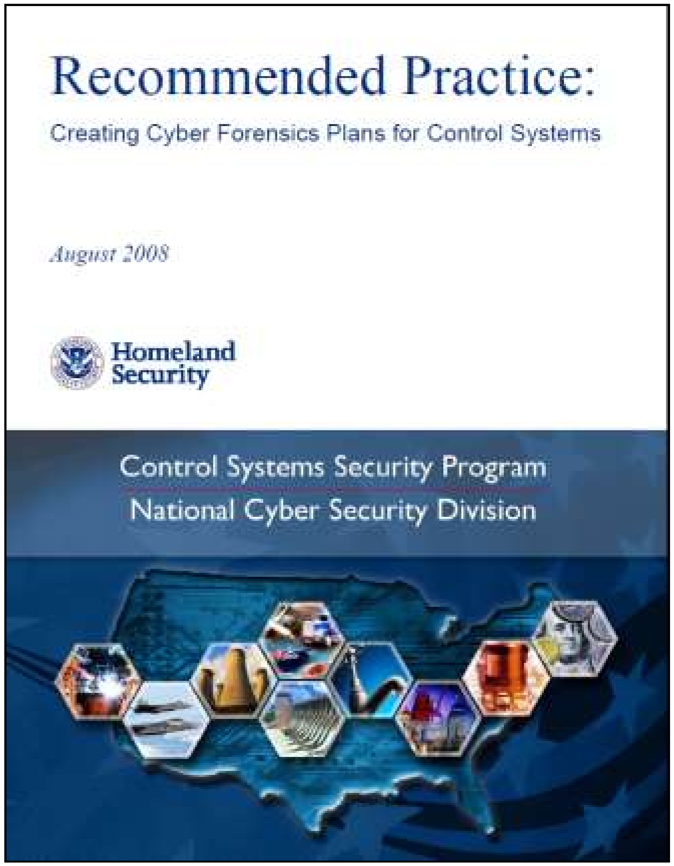
Building Ops Center (Owned or Lease Space)

🟩 Exists

🟦 Probably Exists

🟨 Yet to Exist

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

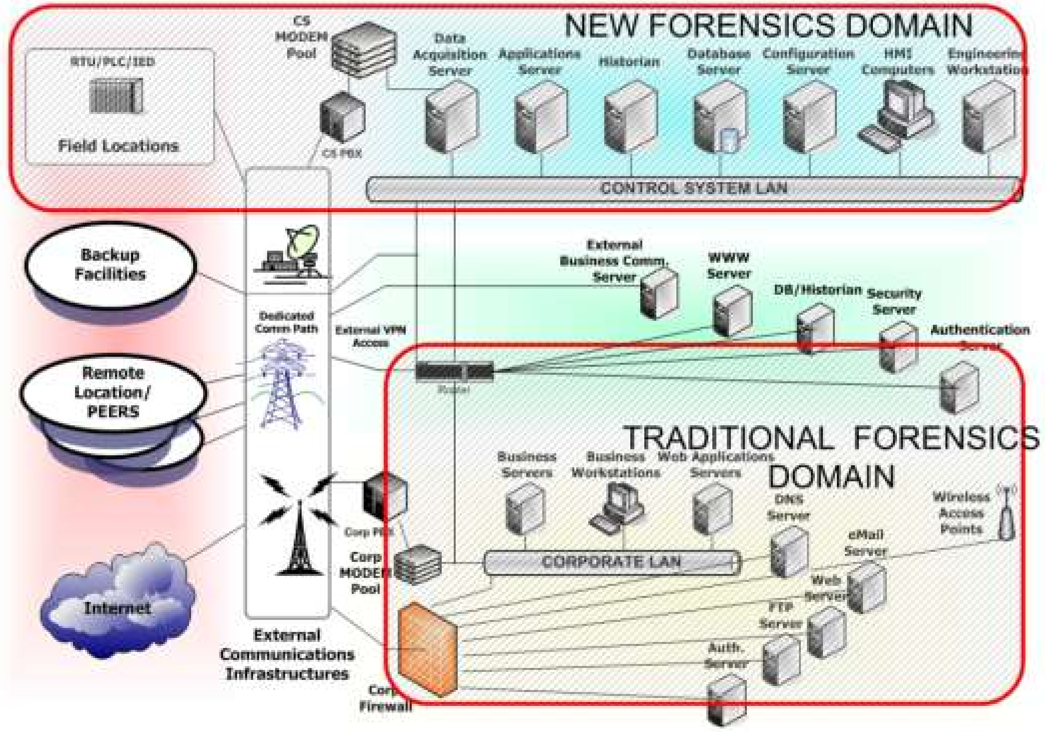
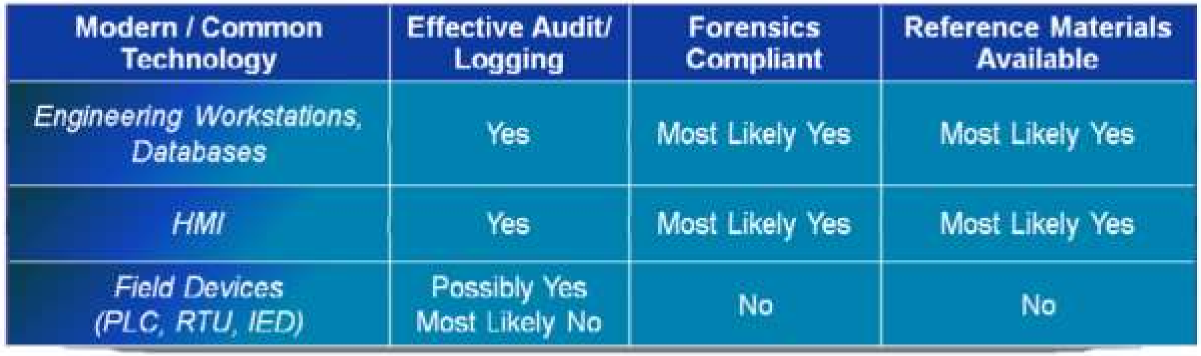


Figure 1. Control systems forensics domain and CSSP reference architecture.[9]



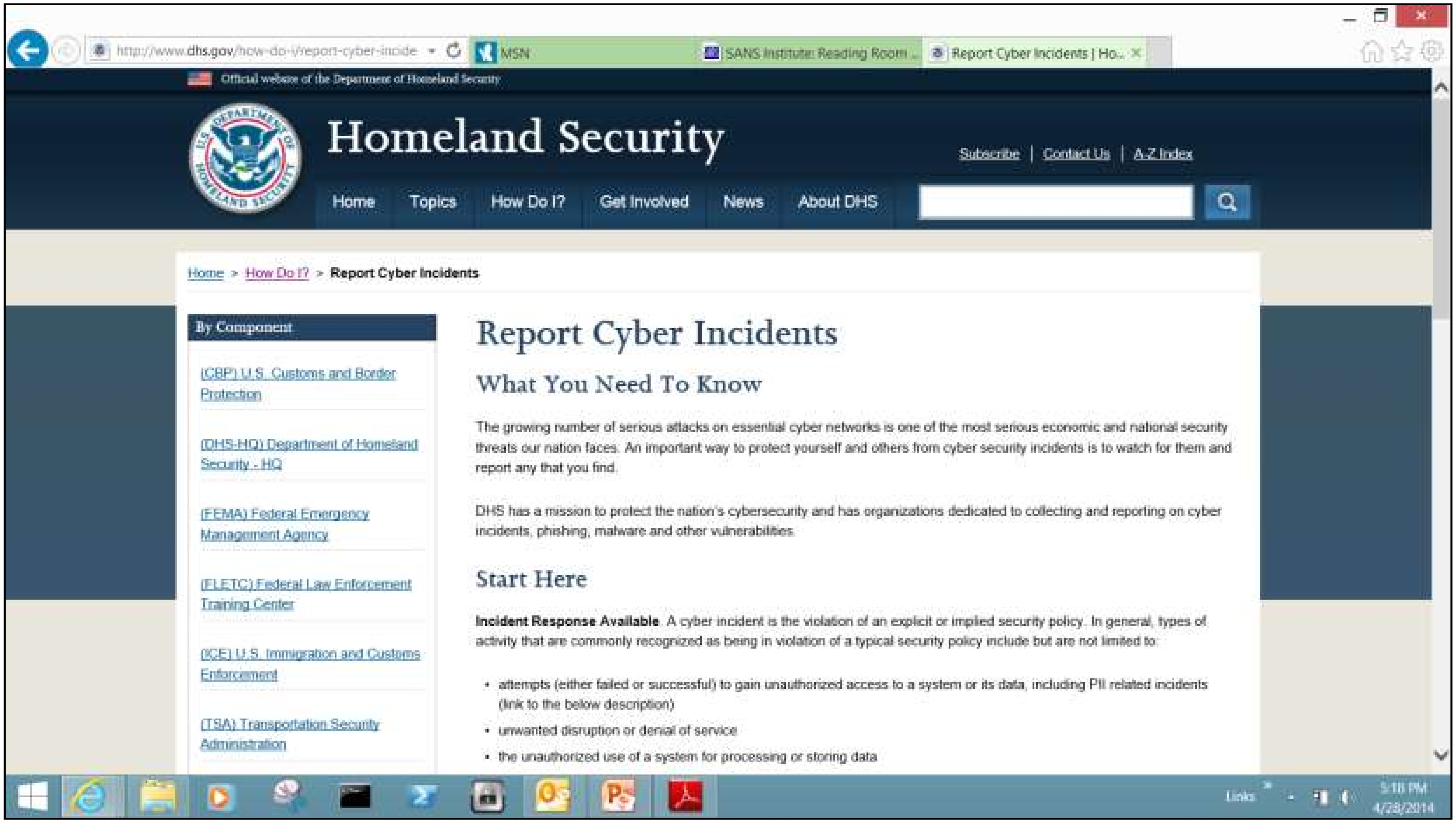
Modern / Common Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases	Yes	Most Likely Yes	Most Likely Yes
HMI	Yes	Most Likely Yes	Most Likely Yes
Field Devices (PLC, RTU, IED)	Possibly Yes Most Likely No	No	No

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

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
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

Home > How Do I? > Report Cyber Incidents

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.

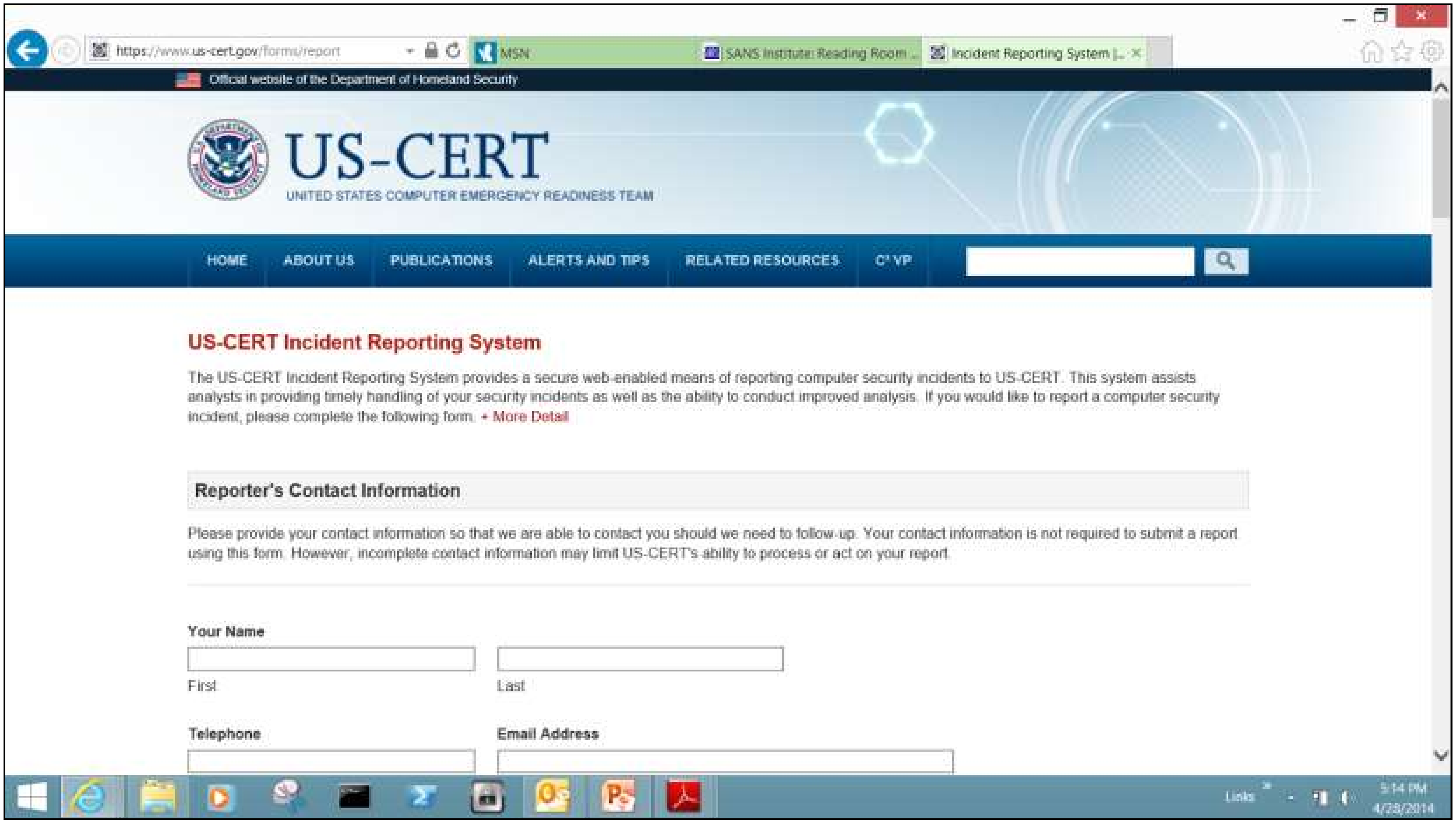
Start Here

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

Cybersecuring Control Systems Workshop

The Cybersecuring Control Systems Workshop is geared to help architects, engineers, contractors, owners, facility managers, maintenance engineers, physical security specialists, information assurance professionals—essentially anyone involved with implementing cybersecurity in the Control System (CS) life cycle—to learn the best practice techniques to better protect their CS. The workshop provides a combination of classroom learning modules to teach control system basics, protocols, how to use the NIST Risk Management Framework and the Cybersecurity of Facility-Related Control Systems Design Guidance, and hands-on laboratory exercises using tools and methods to inventory, diagram, identify, attack, defend, contain, eradicate and report a cyber event/incident. This includes understanding and practicing hacker and defender techniques for footprinting, scanning and enumeration, exploitation, and post exploitation clean up and maintain persistence. Attendees will see how hackers use exploit tools to gain entrance into the control system, pivot through the network, establish beacon command and control channels, modify logs to mask presence, and exfiltrate data. Attendees will also learn how to use the Advanced Control System Tactics, Techniques, and Procedures (TTPs) developed by the U.S. Cyber Command (USCYBERCOM) to create a Recovery Jump-Kit to find and eradicate malware and exploits using tools such as MalwareBytes, Microsoft Internals Suite, and OSForensics to perform data collection for forensics.

http://www.pmcgroup.biz/services/cybersecurityworkshops.html

QUESTIONS

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

Eric Nickel
Director Technical Solutions
Cell: 703-589-7849
E-mail: enickel@chinooksystems.com