

Navigating RMF

**Michael Chipley PhD GICSP PMP LEED AP
ESTCP Cyber Support SME**

December 5, 2019

8:30am-10:00am



Short Course Description

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). Most Installation Energy and Water ESTCP projects will be required to follow the RMF and, depending on the objectives of the demonstration, obtain an Authorization To Operate (ATO) on the DoD Information Network (DoDIN). The RMF Navigate RMF Short Course is geared to help ESTCP Investigators and Project Teams become familiar with the RMF process, understand the requirements and if/how they apply and learn about the available resources. The course reviews control system basics, protocols, how to use the NIST Risk Management Framework and the Cybersecurity of Facility-Related Control Systems Design Guidance, guidance on what tools and methods to use to inventory, diagram, identify, attack, defend, contain, eradicate and report a cyber event/incident.

Agenda

- 0830-0840 Why is the RMF Important for ESTCP Projects: Shodan Exploit Demo of Control Systems
- 0840-0850 Overview of the 6 Steps of the RMF for both IT and OT Systems
- 0850-0900 Introduction of Services and Agencies FRCS POC's, variations in ATO/eMASS procedures
- 0900-0910 Applying the RMF to ESTCP Demonstration Projects: Key Documents Needed to Get an ATO for an OT System
- 0910-0925 Defining the Platform Enclave and Authorization Boundary, Creating a Test and Development Environment, Continuous Monitoring/Auditing
- 0925-0935 Applying the RMF to Organization IT Systems: Protecting Controlled Unclassified Information
- 0935-0945 Advanced Control Systems Tactics, Techniques and Procedures: Detecting, Mitigating, Recovering and Reporting Events/Incidents
- 0945-1000 Open discussion, Lessons Learned, Best Practices

Why the RMF is Important for ESTCP Projects: Shodan Exploit Demo of Control Systems

OT IP Based Controllers Are in Everything

UNCLASSIFIED

Buildings



Weapon Platforms



Tactical



Electrical and HVAC



Nuclear



Medical



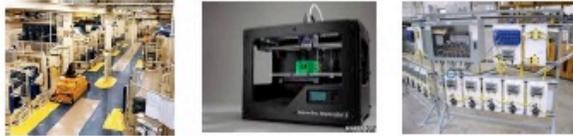
Controller



Electric Vehicles/Charging



Manufacturing

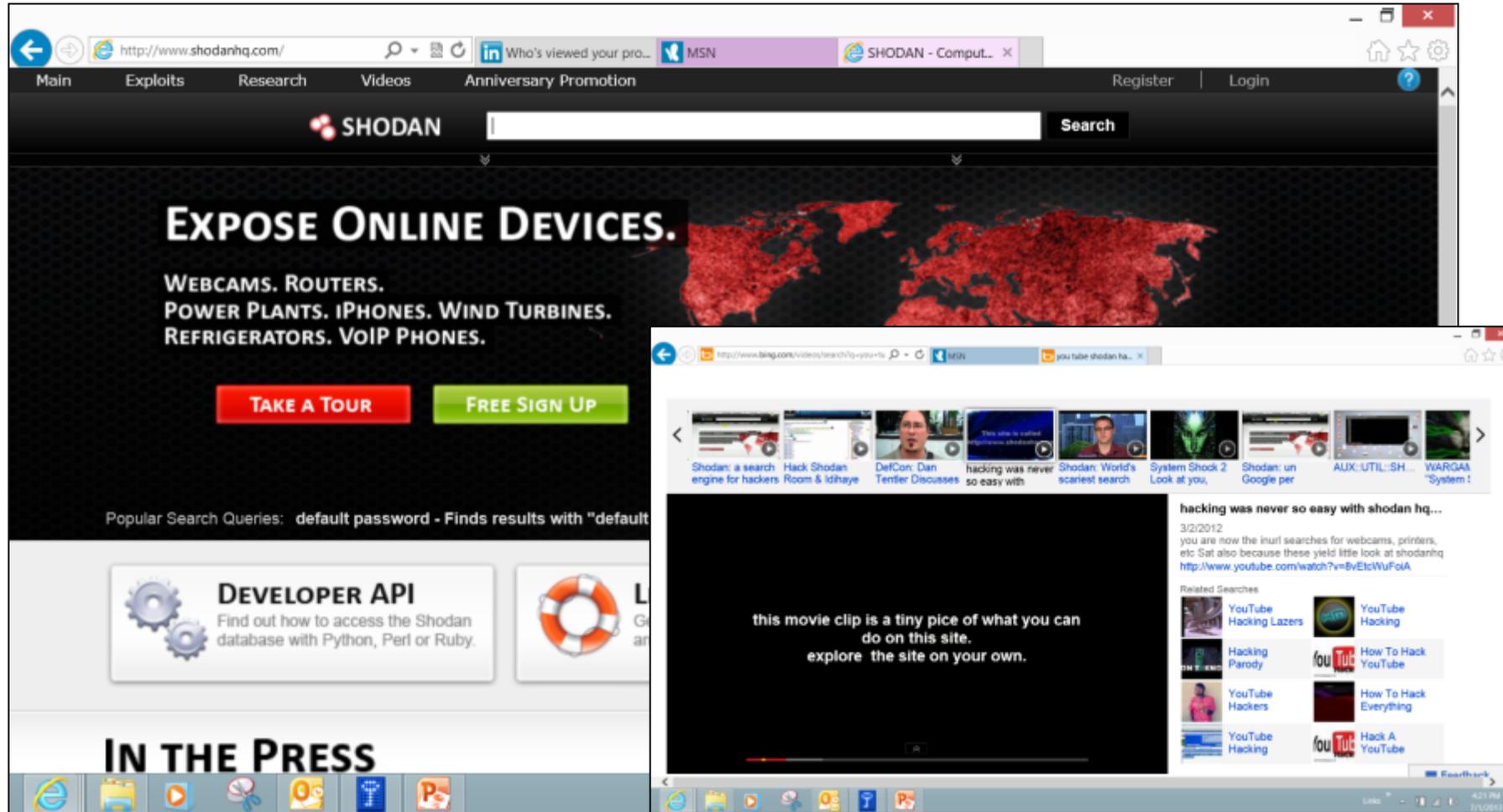


Pumps and Motors



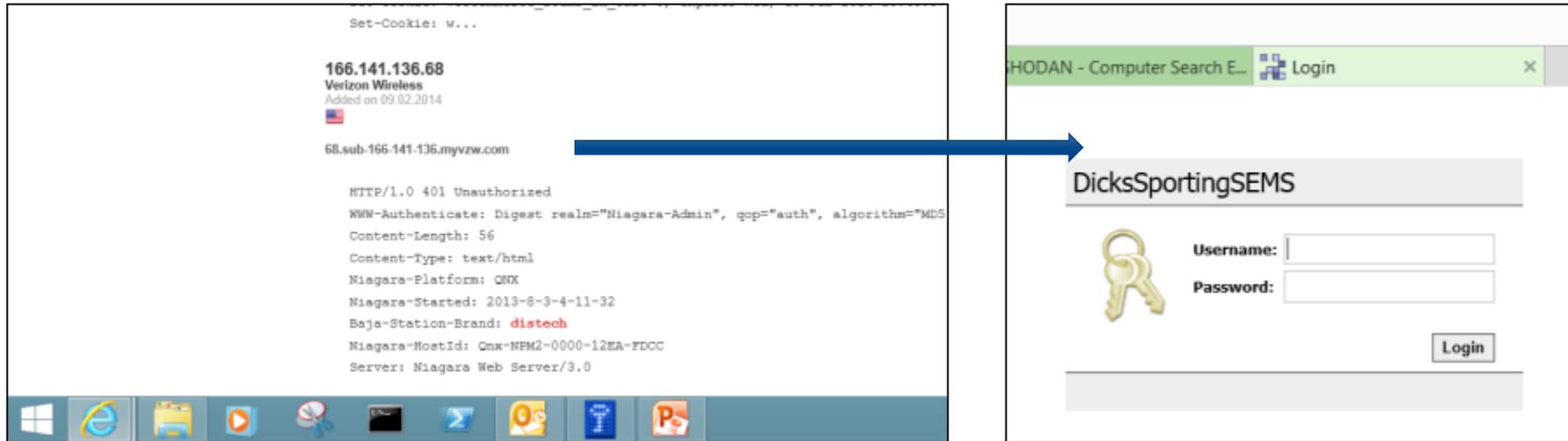
Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

Shodan



Shodan is to OT IP addresses as is Google is to text search

Shodan – Distech Search



HTTP/1.0 401 Unauthorized

WWW-Authenticate: Digest realm="**Niagara-Admin**", qop="auth", algorithm="**MD5**",
nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"

Content-Length: 56

Content-Type: text/html

Niagara-Platform: QNX

Niagara-Started: 2013-8-3-4-11-32

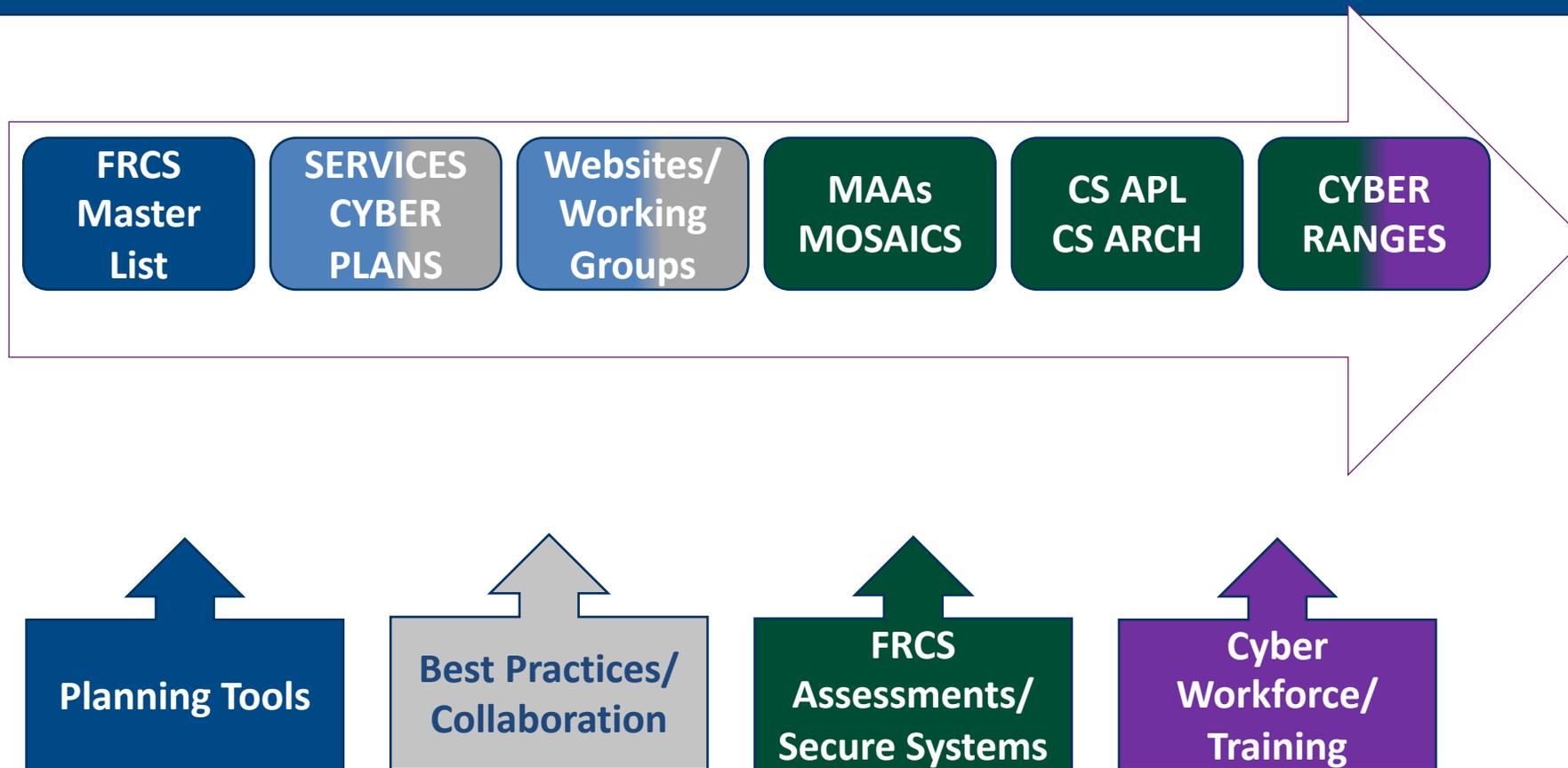
Baja-Station-Brand: **distech**

Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC

Server: **Niagara Web Server/3.0**

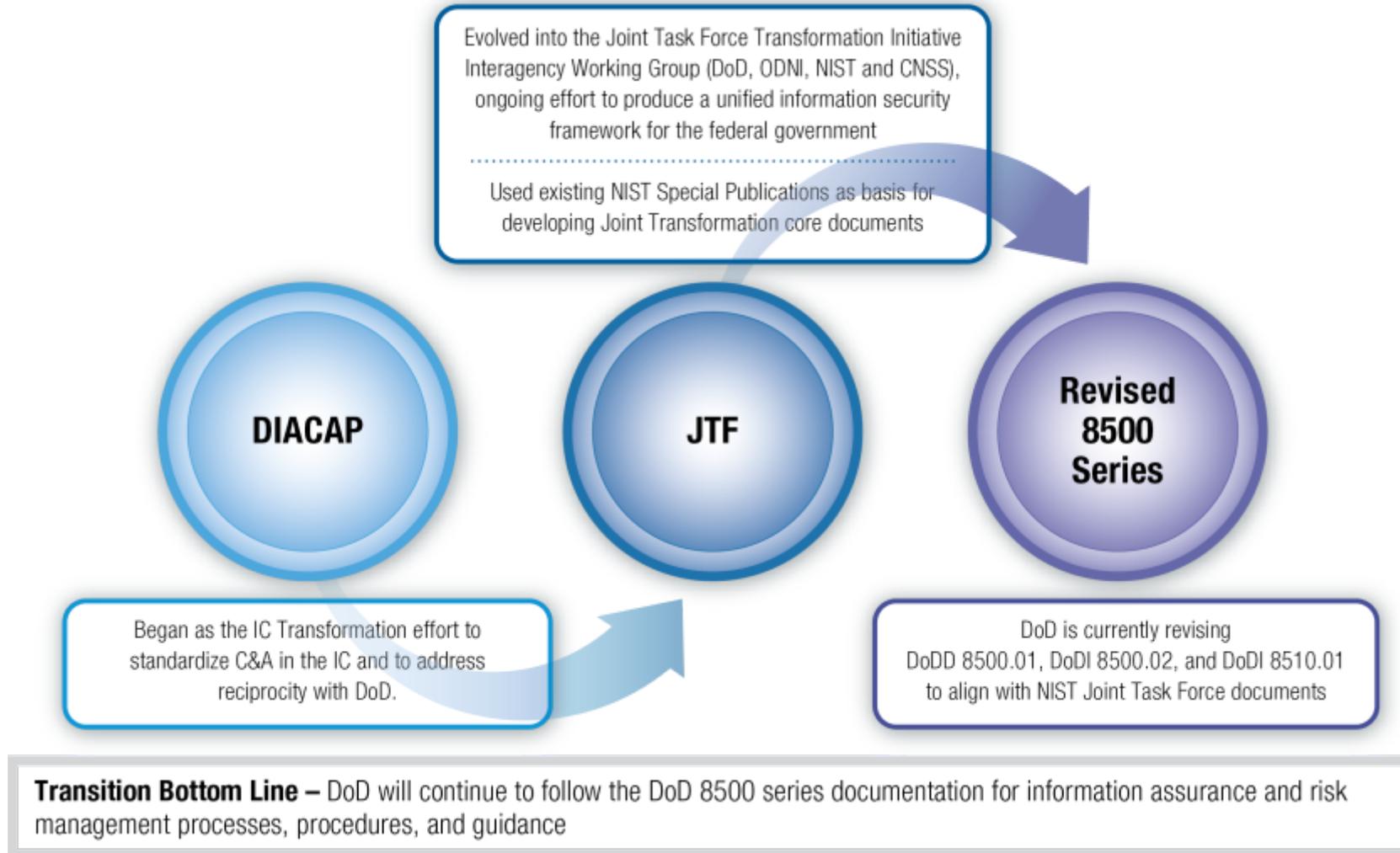
Overview of the 6 Steps of the RMF for both IT and OT Systems

ODASD(E) Cybersecurity Initiatives



Alignment with Federal, Industry Objectives

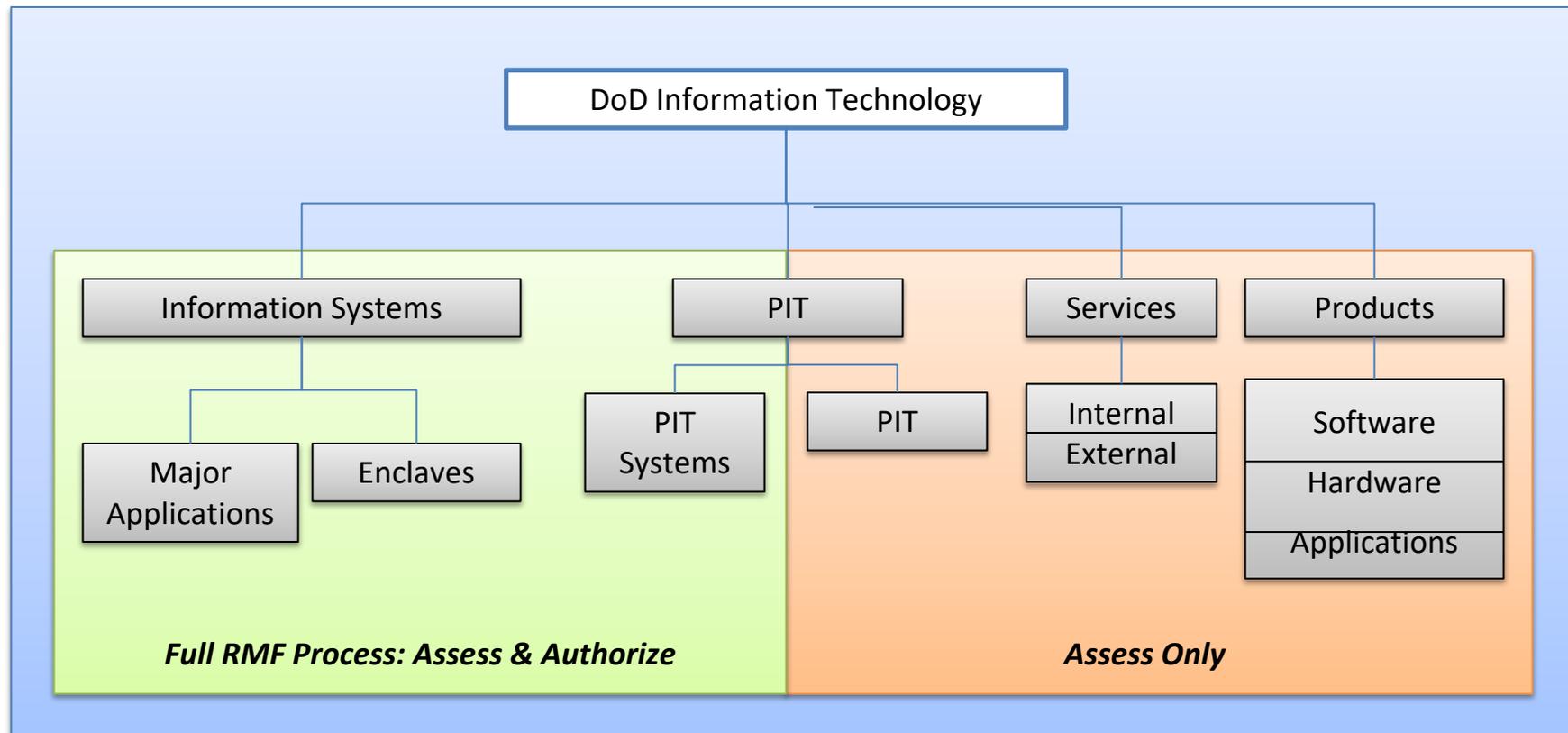
DoDI 8500.01 and 8510.01 Update



RMF for DoD IT

DoDI 8510.01 “Risk Management Framework for DoD IT”

- Provides clarity regarding what IT should undergo the RMF process and how



PIT = Platform IT, OT = Operational Technology (Proposed Alternate)

8500 PIT Cybersecurity Considerations

(2) PIT

(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (ah) for PIT cybersecurity requirements.

(b) Examples of platforms that may include PIT are: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), **buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering**, including associated data transport mechanisms (e.g., data links, dedicated networks).

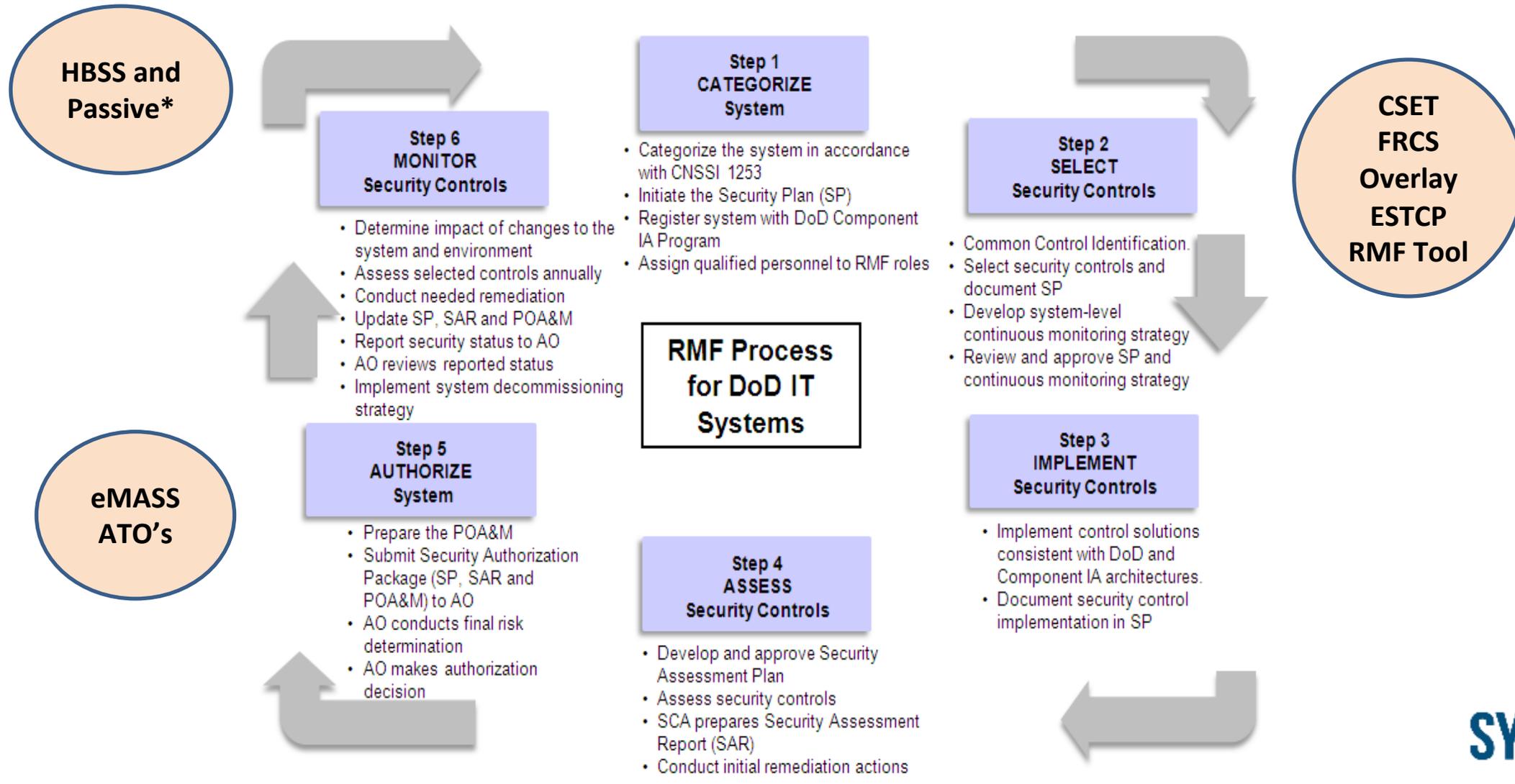
8500 PIT Systems

(d) PIT Systems

Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a **collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support.** PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

EI&E worked with CIO to adopt “Platform Enclaves” as the term for Facility-Related Control Systems (FRCS)

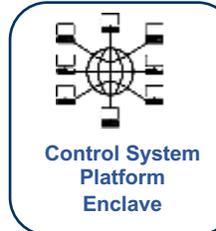
6 Steps of RMF for both IT and OT Systems



DoD Facility-Related Control Systems (FRCS)

Categories

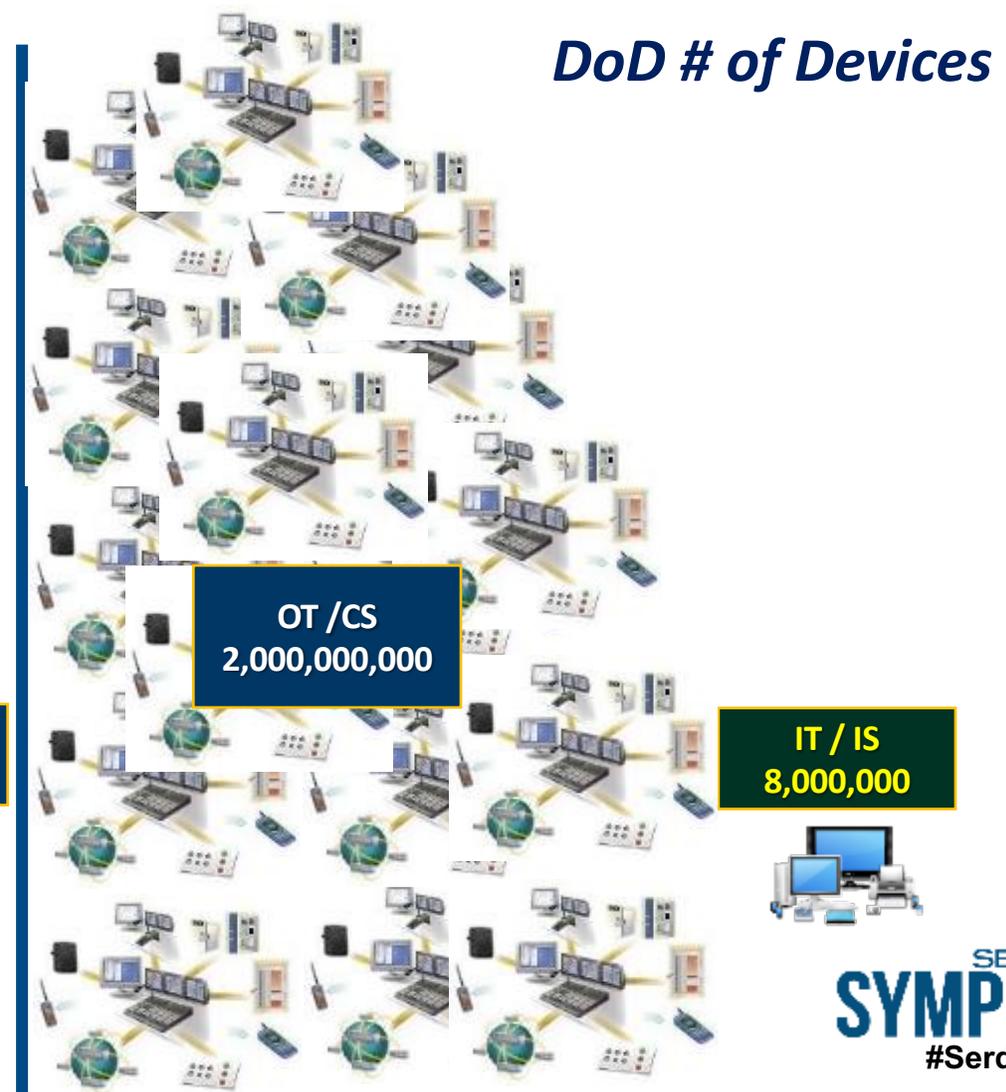
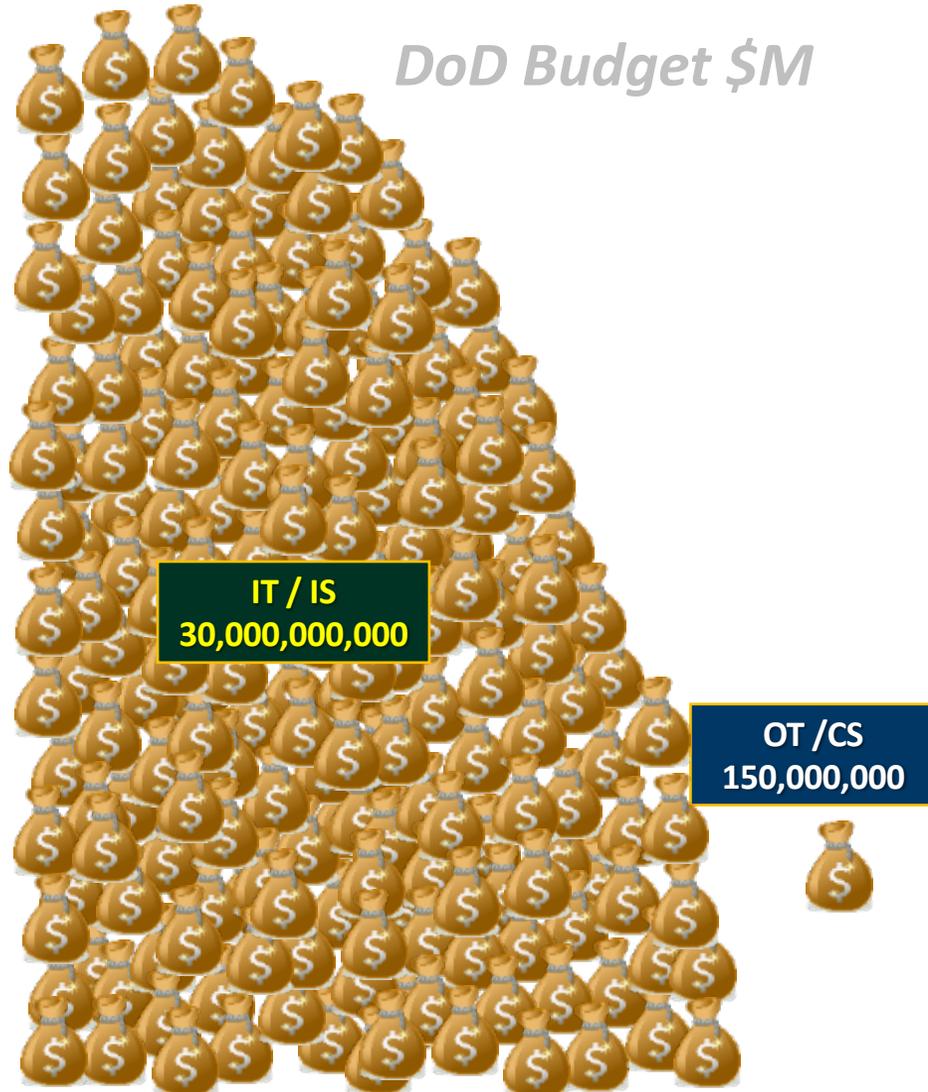
Systems



- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More...*

DoD Control Systems are just as vulnerable as industry, how do we protect them?

IT/IS Versus OT/CS Budgets and Devices



Introduction of Services and Agencies FRCS POC's, Variations in ATO/eMASS procedures

Introduction of Services and Agencies FRCS POC's

Introduction of Services and Agencies FRCS POC's

Army

Navy

Air Force

Defense Health Agency

Defense Logistics Agency

Variations in ATO/eMASS procedures

Air Force Platform Enclave - COINE

Navy Platform Enclave - PSNet

Marine Corps Platform Enclave

Defense Health Agency Platform Enclave - MedCOI

Name	Type
 Appointment_Letter_ISSE_template	Microsoft Word Document
 DoD Privacy Impact Assessment	Adobe Acrobat Document
 DON_Info_Types_Baselines_2016Jan11-Fl...	Adobe Acrobat Document
 Guide for System Categorization Form_V1	Microsoft Word Document
 HW-SW-InfoFlow-Tables-Template_V1.0	Microsoft Excel Spreadsheet
 NAVFAC CYBERSAFE Grade Determinatio...	Microsoft Excel Spreadsheet
 NAVFAC eMASS ACCOUNT REQUEST FO...	Adobe Acrobat Document
 Navy RMF_Security_Assessment_Plan_Te...	Microsoft Excel Spreadsheet
 Navy_SLCM_Strategy_Controls_Table_v1.1	Microsoft Excel Spreadsheet
 Navy_SLCM_Strategy_Guidance_v1.0	Microsoft Word Document
 System Categorization Form v1.2	Microsoft Excel Spreadsheet

**Air Force Civil Engineering Center (AFCEC)'s
Cybersecurity Requirements on Facility-Related Control Systems (FRCS)**

The identified Cybersecurity requirements for Civil Engineering (CE) Facility-Related Control Systems (FRCS) are in the AFGM2018-31-01 and UFG4-010-06 as references at the end of this document.

The AFCEC Authorizing Official (AO) has identified and established the baseline of 47 Security Controls with 320 Assessment Procedures (AP). The proposed vendor is responsible for the following: perform an initial security assessment, a scan of vulnerabilities, applying all relative DISA Security Technical Implementation Guide (STIG) configuration, provide a copy of the scan results to the USAF CE unit, mitigate the identified vulnerabilities prior to final acceptance by USAF through the RMF Methodology by uploading the evidence into eMASS. Below are the approved standardized templates to be completed and then used as eMASS artifacts. Once the vendor has completed the assessment and submitted it for review, it will flow in eMASS to the AFCEC/COOI Compliance Branch for validation and submission to the SCAR -> SCA -> ADDR -> AO. Any questions can be directed to the AFCEC/COOI.org box: afcec.comi.cs@us.af.mil.

AFCEC/COOI will provide templates for the System Policy Document (SPD), Configuration Management Plan (CMP) and Contingency Plan (CP). The SPD when executed will assist in ensuring many of the controls are compliant.



AFCEC CE CS SPD
Template v1.0



AFCEC CE CS
CMP Template
DRAFT v2.0.docx

AFCEC AO in September of 2018 established the Control System Baseline.



Baseline Security
Controls Manager



47 Controls 320
AP.xlsx

Topology, Hardware Software List and Dataflow Diagrams will be required.

UFG 4-010-06
Cybersecurity of Facilities

Proposed vendors are required to have an eMASS account to upload the required documentation. Attached is the DD Form 2875 template and eMASS user guide. Vendor's employees will complete DD Form 2875 for submission to AFCEC.COMI.KCSHELPPDS@us.af.mil to have an eMASS account established in the AFCEC eMASS Container.



DD FORM 2875
5 ISSO RSM 1314b-2



AFCEC FRCS
Instructions.pdf

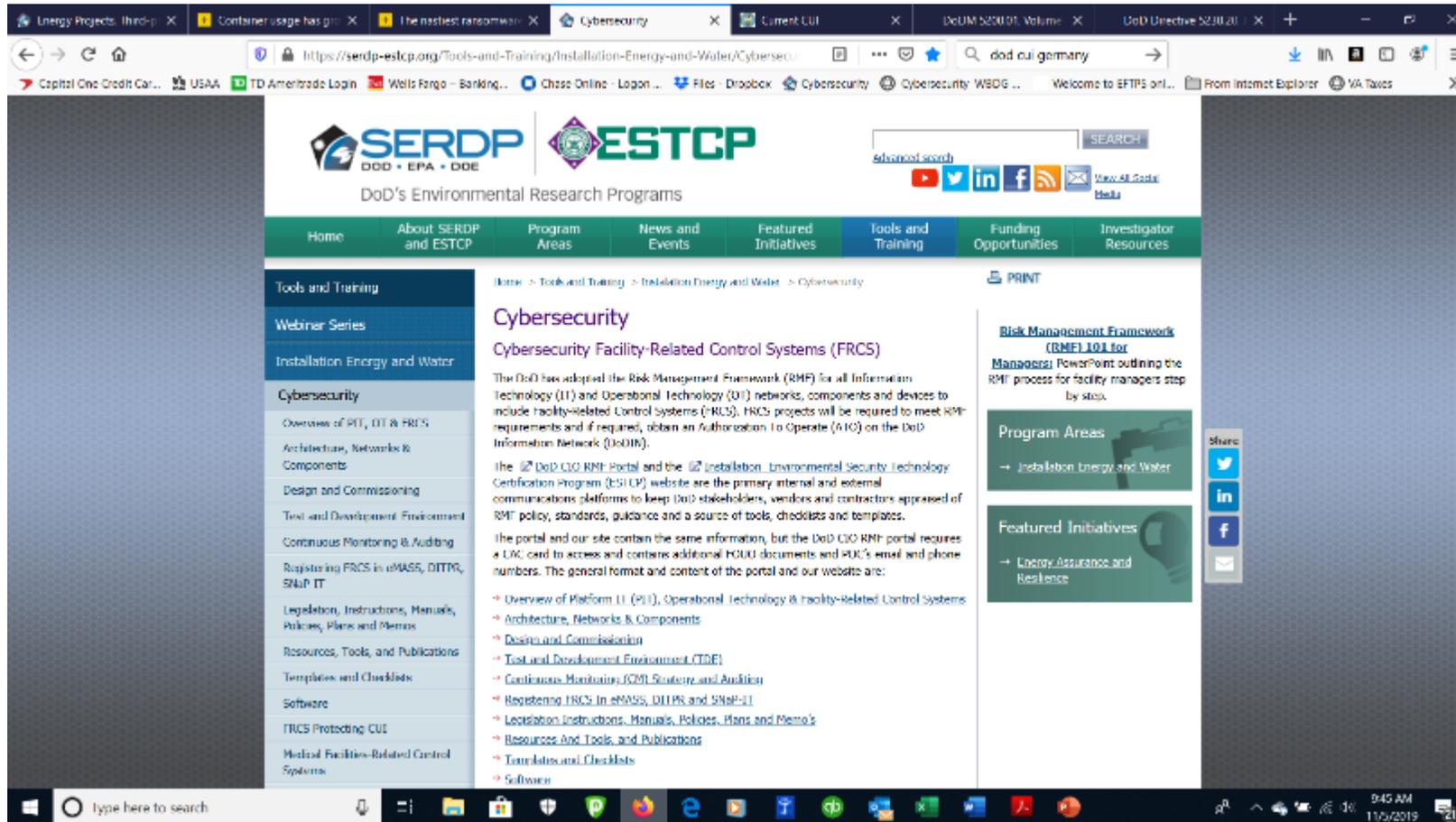


AFCEC FRCS
Guide V1.docx

22 February 2019

Applying the RMF to ESTCP Demonstration Projects: Key Documents Needed to Get an ATO for an OT System

ESTCP RMF Cybersecurity Guidance and Templates



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

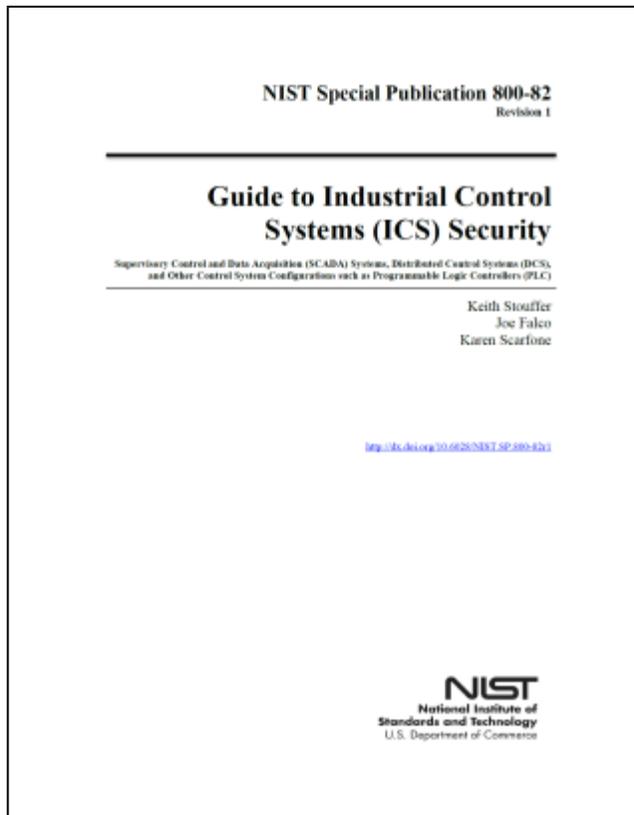
Applying the RMF to ESTCP Demonstration Projects

Key Documents Needed to Get an ATO for an FRCS OT System and recommended sequence of completion:

- **Event/Incident Communications Plan (EICP)** – use the modified FedRAMP template (ESTCP EICP Graphics)
- **Event/Incident Response Plan (EIRP)** – use the modified FedRAMP templates
 - CJCSM 6510.01B - Cyber Incident Handling Program 2012 – use the procedures outlined in the manual
 - US-CERT Incident Response Form – use the excel file template for a non-DoD data incident
- **Information Systems Contingency and CONOPS Plan (ISCP)** – use the modified FedRAMP template.
- Test and Development Environment (TDE)
- Factory Acceptance Testing/Site Acceptance Testing (FAT/SAT)
- Penetration Testing (For High Risk and others as required)
- **Security Audit Plan (SAP)** – use the modified NIST template
- **System Security Plan (SSP)** – recommend using the CSET tool/or Core Auth template NIST SP 800-53/800-82
- **Security Assessment Report (SAR)** – ESTCP does not require a SAR, however, many insurance companies or AO's may require a SAR. An organization can use the modified FedRAMP template.
- **Plan of Action & Milestones (POAM)** – use the modified FedRAMP and/or eMASS templates (GSA and DoD provided)

Defining the Platform Enclave and Authorization Boundary, Creating a Test and Development Environment, Continuous Monitoring/Auditing

Standards – NIST SP 800-82 R2



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 (DFRCS), 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 was released May 2015 – has 800-53 Rev 4 800+ controls,
Appendix G ICS Overlay

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

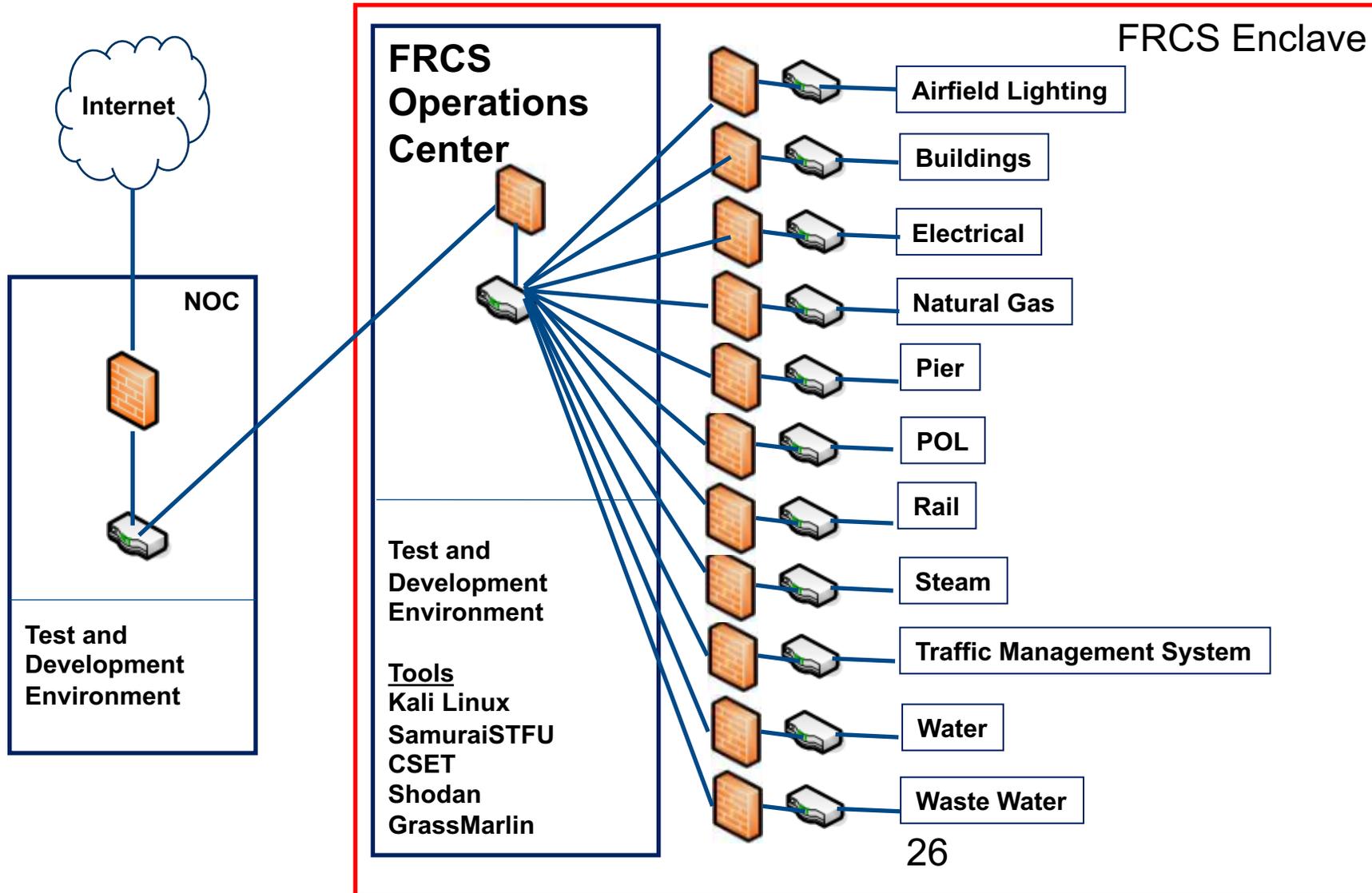
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity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

Acquisition and Contracts

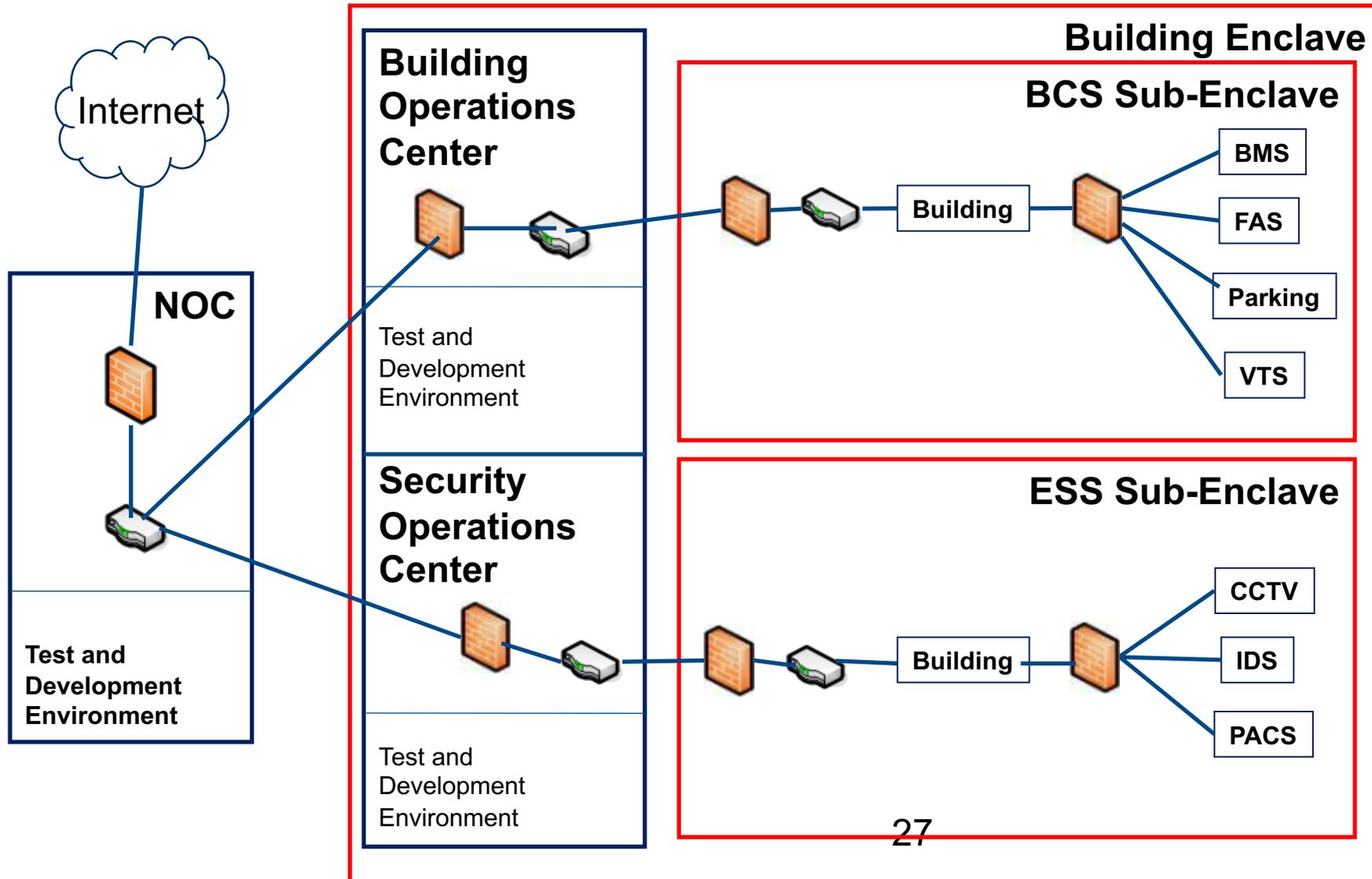
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection,
Outbound Detection

FRCS Enclave and Numerous Sub-Enclaves



Hybrid FRCS and Security Enclaves



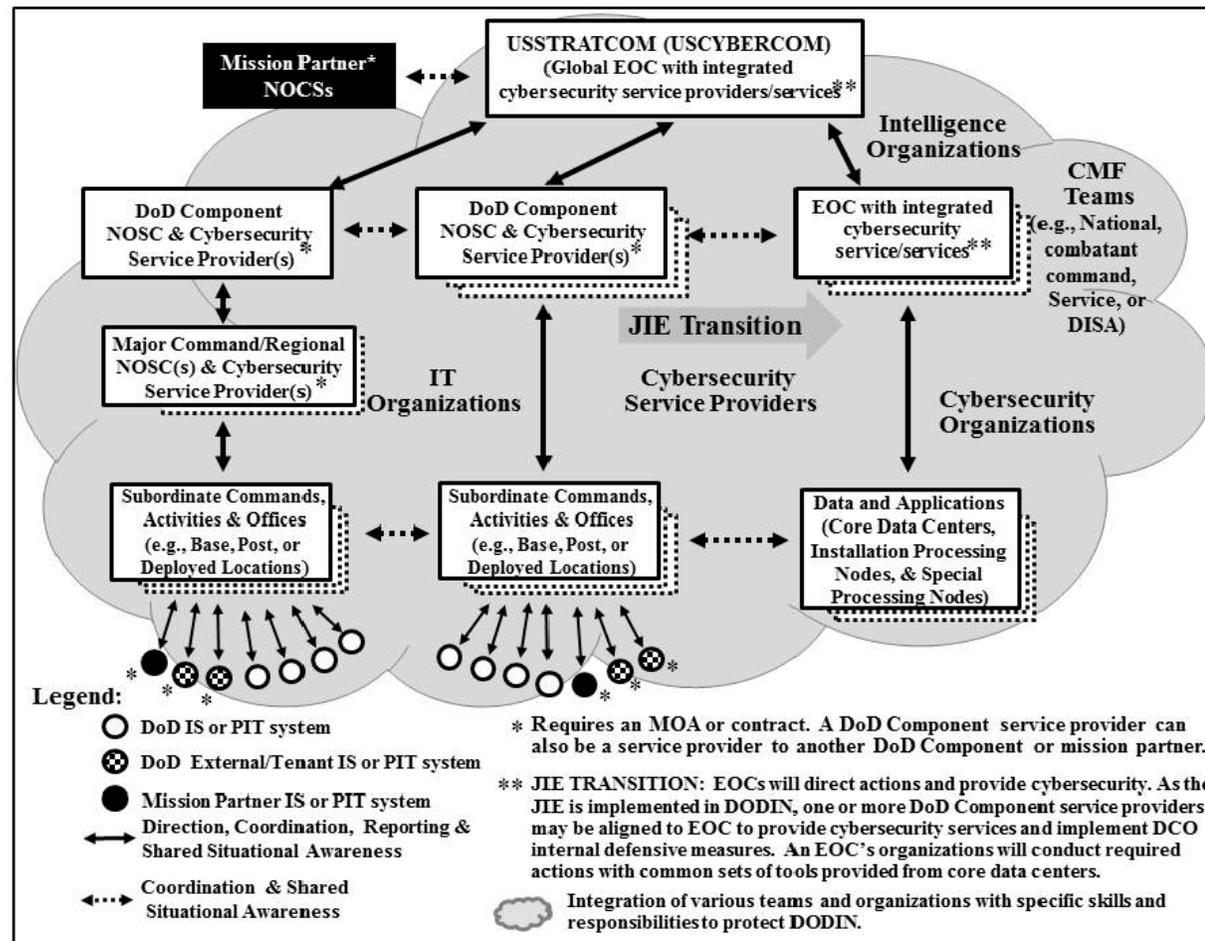
**Installations and Environment
Real Property Installed Equipment**

**NIST SP 800-53
and
NIST SP 800-82
Contains PII, HIPPA, PCI
FISMA**

**Director National Intelligence
Personal Property
FIACAM**

DODI 8530 – Joint Information Environment (JIE)

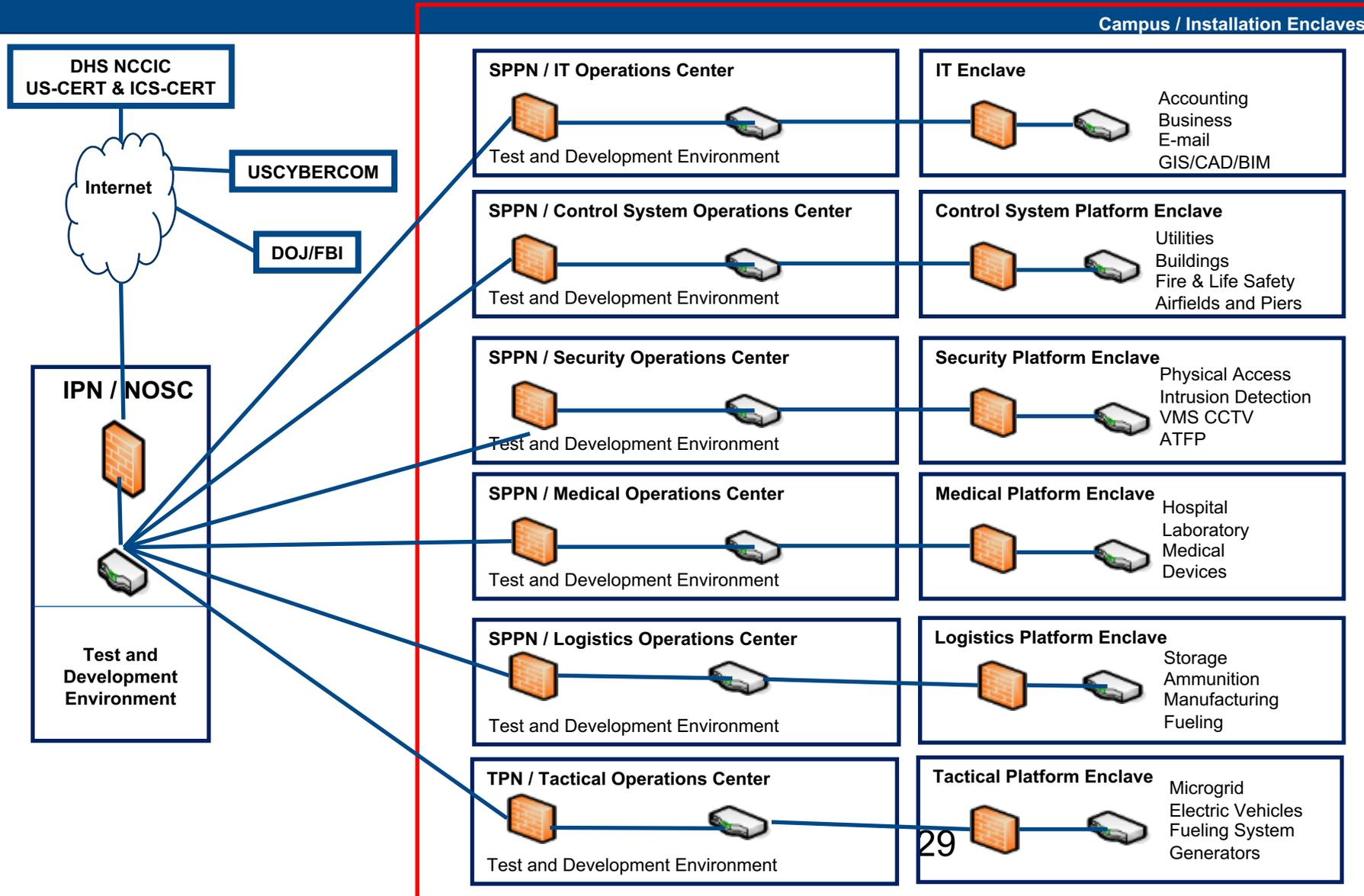
Figure 2. Notional View of Current and Future Integration of Cybersecurity Activities



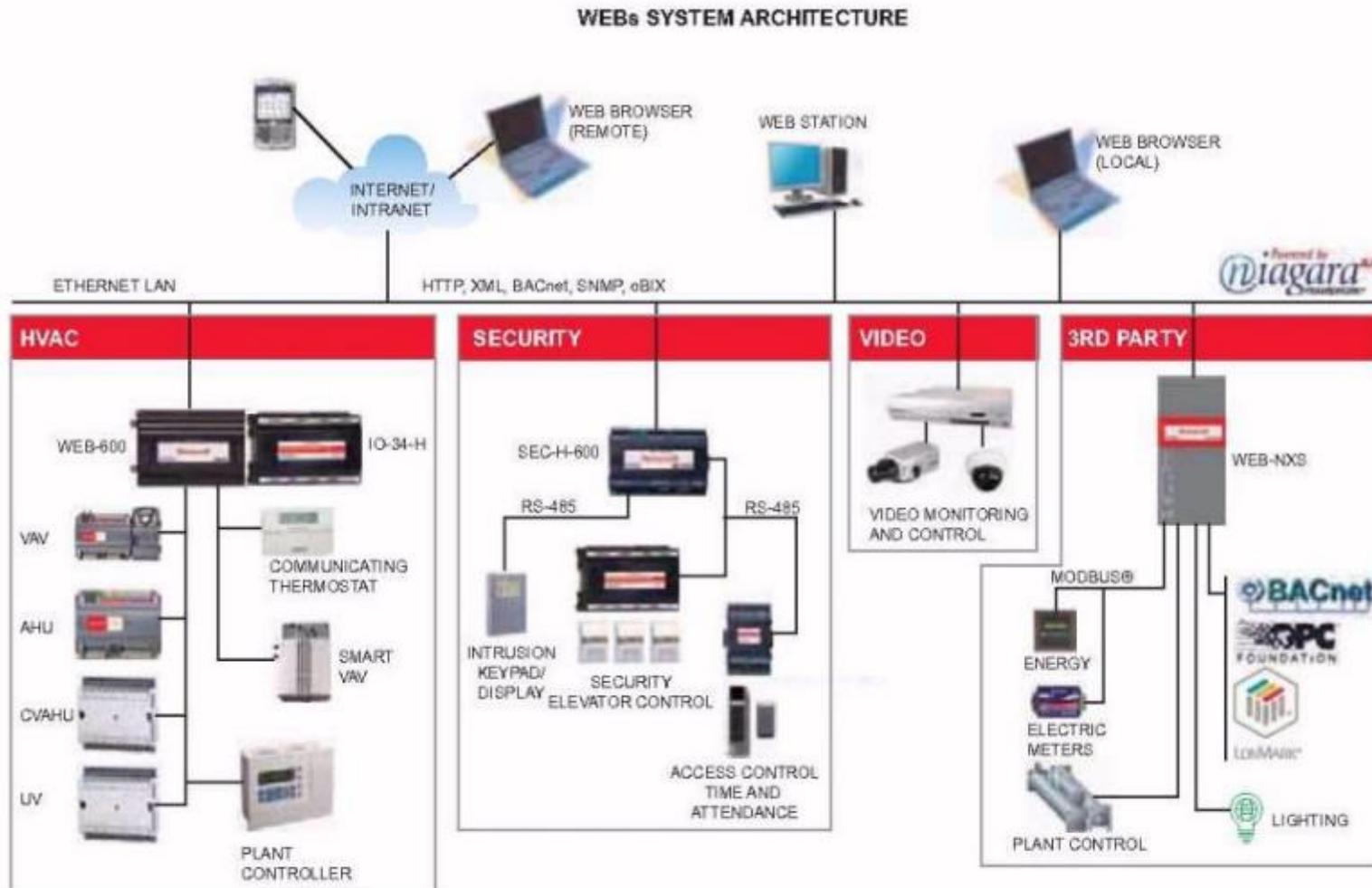
Gigabit Fiber, IPv6

- Network Operations Security Center
- Installations Processing Node (IPN)
- Special Purpose Processing Node (SPPN)
- Tactical Processing Node (TPN)

Notional JIE Control Systems



Tridium Architecture



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

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

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

Proprietary Control Systems Protocols

- Tridium NiagaraAX/Fox
- Johnson Metasys N2
- OSIsoft Pi System
- Many others...

ESTCP Cybersecurity Guidelines and Resources

The screenshot shows a web browser window with the URL <https://serdp-estcp.org/look-and-training/Installation-Energy-and-Water/Cybersecu>. The page features a left-hand navigation menu with categories such as "Legislation, Instructions, Manuals, Policies, Plans and Memos", "Resources, Tools, and Publications", "Software", "FRCS Protecting CUI", "Medical Facilities-Related Control Systems", "Energy Projects, Third-party Financing", "Energy Planning & Assessment", "Envelopes", "HVAC", "Lighting", "Environmental Restoration", "Munitions Response", "Resource Conservation and Resiliency", and "Weapons Systems and Platforms".

The main content area displays a list of links and a paragraph: "Any organization can use the website's guidance, reference materials, checklists and templates and the majority can be used for both standard IT and FRCS, also often referred to as Operational Technology (OT) systems."

Below the text is a circular diagram titled "DoD Risk Management Framework Process for DoD IT Systems". The diagram consists of six steps arranged in a circle, each with a brief description of its purpose:

- Step 1: CATEGORIZE System**: Categorize the system in accordance with OIGIS, DISA, and the Security Plan (SP).
- Step 2: SELECT Security Controls**: Common Control Dark Matter, Submit security controls and document SP, Develop system-level continuous monitoring strategy, Review and approve SP and continuous monitoring strategy.
- Step 3: AUTHENTICATE System**: Prepare the PDM&I, Submit Security Authorization Package (SAP), SAR and DDA&I to AD, AD confirms final risk determination, AD makes authorization decision.
- Step 4: ASSESS Security Controls**: Develop and approve Security Assessment Plan, Assess security controls, SA prepares Security Assessment Report (SAR), Conduct initial remediation actions.
- Step 5: MONITOR Security Controls**: Determine impact of changes to the system and environment, Assess selected controls annually, Conduct remediation, Update SP, SAR and PDM&I, Report security status to AD, AD reviews reported status, Implement system decommissioning strategy.
- Step 6: REPORT Security Controls**: Implement control solutions consistent with DoD and Component architecture, Document security control implementation in SP.

The diagram is titled "DoD Risk Management Framework Process for DoD IT Systems" and includes a "Document Title" and "Document Barcode" at the bottom.

Any organization can use for their FRCS

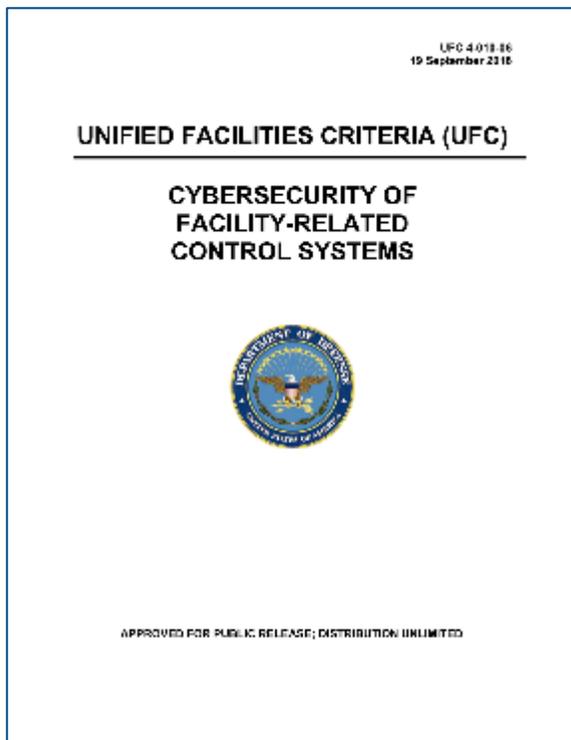
Cybersecurity Guideline SME's

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

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

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

DoD UFC 4-010-06 Cybersecurity



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

Step 1: Based on the organizational mission and details of the control system, the System Owner (SO) and Authorizing Official (AO) determine the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) for the control system.

Step 2: Use the impact levels to select the proper list of controls from NIST SP 800-82.

Step 3: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2.

Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.

Step 5: Include cybersecurity requirements in the project specifications and provide input to others as required.

DoD UFC 4-010-06 Platform Enclave

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

DoD UFC 4-010-06 Appendix D

UFC 4-010-06
19 September 2016

APPENDIX D PLATFORM ENCLAVE

D-1 PLATFORM ENCLAVE CONCEPT OVERVIEW

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

D-2 PLATFORM ENCLAVE USING TWO AUTHORIZATIONS

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

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

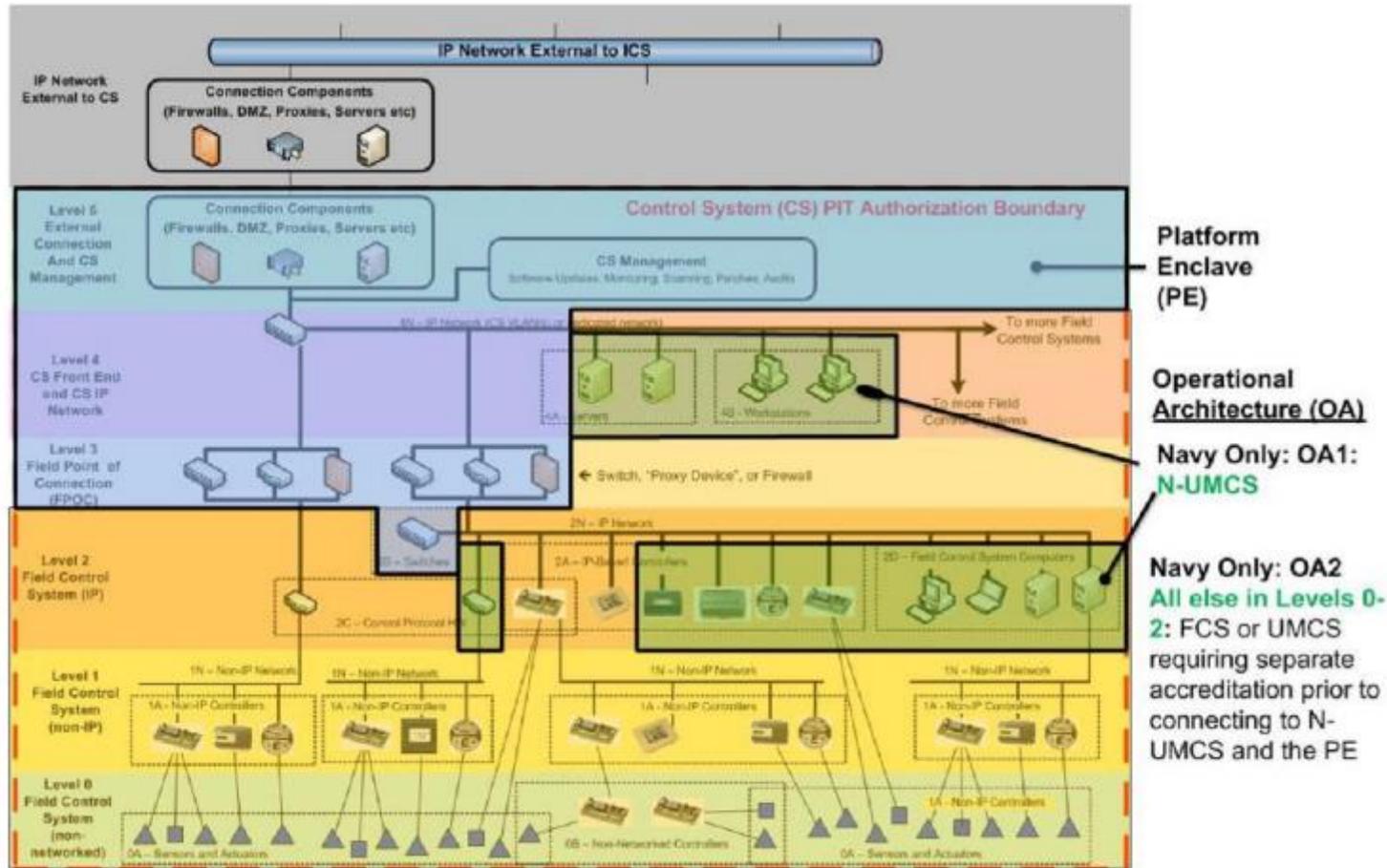
D-3 PLATFORM ENCLAVE BENEFITS

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

38

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

DoD UFC 4-010-06 Appendix D



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.

UFGS 25 05 11 Cybersecurity For FRCS

The screenshot shows a web browser window displaying the WBDG (Whole Building Design Guide) website. The URL in the address bar is <http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. The page features the WBDG logo, which is a green circular graphic with the text "WBDG a program of the National Institute of Building Sciences WHOLE BUILDING DESIGN GUIDE". Navigation links include "ABOUT", "SITE MAP", "CONTACT", "CREATE ACCOUNT", and "LOGIN". A search bar is located in the top right corner. Below the navigation bar, there are tabs for "DESIGN RECOMMENDATIONS", "PROJECT MANAGEMENT - O & M", "FEDERAL FACILITY CRITERIA", "CONTINUING EDUCATION", and "ADDITIONAL RESOURCES". The main content area displays the breadcrumb trail: "DEPARTMENT OF DEFENSE / UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS) / UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS". The title of the document is "UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS". The date is "11-01-2017", the division is "Division 25 - Integrated Automation", and the page count is "50". There are links to "View/Download" in PDF and ZIP formats. The Department of Defense seal is visible on the left. The Windows taskbar at the bottom shows the time as 7:45 AM on 5/29/2018.

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

UFGS 25 05 11 Schedules

The screenshot shows a Microsoft Excel spreadsheet titled "UFGS 25 05 11 Cybersecurity Schedules: 2017-09-07 - Last Saved 5/3/2018 8:45 AM". The spreadsheet is organized into sections with the following content:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Interconnection Schedule																		
2	Document connections between this control system and other systems.																		
3	Designer should generate this schedule as part of design. Designer should always provide the "Descriptive Purpose" and "Foreign Destination"; depending on the project, designer may provide																		
4	Contractor should complete the table, but may need outside input for the Network Address																		
5	Device ID should be a key to an entry in the <Inventory Table>																		
6	Network Address relates to the Transport Layer protocol and is typically the IP address.																		
7	Transport Layer protocol will typically be IP, provide if something other than IP.																		
8	Protocol is the application level protocol -- eg. SMTP, Lon.																		
9	Service might be a protocol-specific service -- eg BACnet Confirmed File Transfer																		
10																			
11	Network Communication Schedule																		
12	This documents connections within the control system.																		
13	This information may already be contained on other submittals, in which case those documents may be submitted instead.																		
14	(For HVAC installed IAW 23 09 00 it is contained on the Point Schedules.)																		
15																			
16	Wireless																		
17	Prior to using wireless, contractor must submit a Wireless Communication Request schedule with columns A - I filled out.																		
18	Govt. will Approve or Disapprove in column J. Approved devices may require post-installation testing.																		
19	For devices requiring post-installation testing, contractor shall attempt network connectivity at various points and document (Yes/No, Pass/Fail) whether network connectivity existed																		
20																			

The spreadsheet also shows a taskbar at the bottom with various application icons and a system tray displaying the time as 2:16 PM on 12/14/2018.

Create the Cyber Narrative/Design Analysis

Cybersecurity

Cybersecurity

Cybersecurity Requirements

CODES AND REFERENCES

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

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

1

FACILITY-RELATED CONTROL SYSTEMS

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

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

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

Assign Cyber Team

CYBERSECURITY TEAM PERSONNEL

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

Cyber Team Lead: GICSP or CISSP

Cyber System Administrator: MCSE, Security +

Cyber Commissioning: CEM, CISSP, CEH, CxA, DGCP

Cyber Auditing: CDFM, CFE, CISA, CPA

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

Assemble the Stakeholders

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

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

Cybersecurity Guideline Sequence

Activity / Lead	New Project	Renovation Project	Typical Duration
Presolicitation RFP Considerations	Obtain the Regional and ESTCP Platform Enclaves categorization and categorize the CS	Obtain the Regional and ESTCP Platform Enclaves categorization and categorize the CS	NA
Design <ul style="list-style-type: none"> • Basis of Design • Concept Design (10-15%) • Design Development (35-50%) • Pre-Final (90%) • Final (100%) Lead: A/E Documents/Models/Tools: <ul style="list-style-type: none"> • 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 subsystem 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 security risk assessment.	3-6 Months

Cybersecurity Guideline 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 FRCS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

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

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

Tools for the Test and Development Environment

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
- GrassMarlin

Attack and Defend Tools

- Kali Linux
- Control Things I/O
- Wireshark
- Gleg
- Windows PowerShell
- Windows Management Information Console
- Windows Sysinternals

Assessment Tools

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

Virtual Machines

- VM Player
- Windows Hypervisor
- Oracle VM Virtual Box

Facility Control Systems Ops Center

Facility Control Systems Operations Center (FCSOC)

Coordinate with all responsible organizations to determine the location of the FRCS servers, central monitoring and operational control/Human Machine Interface (HMI) operator's consoles, and the Test and Development Environment (TDE). The FCSOC can be within the campus or located on the installation at other Operations Centers (SOC, Fire Department, NETCOM Network Operations Security Center, etc.). Identify if the PE servers, workstations, laptops, switches, routers, etc. (all "traditional IT Front-End") will be GFE or if contactor procured and installed and turned over to government. **All PE assets capable of being hardened using the Security Technical Implementation Guides (STIGS), will be configured and checked using the Factory Acceptance Testing/Site Acceptance Testing (FAT/SAT) Checklist.** Determine if penetration testing, and what type, will be required; the ESS is recommended to have penetration testing (High Impact) per NIST SP 800-82. Complete the EI&E Penetration Testing Checklist.

RMF Cybersecurity SME Required

D3100 CYBERSECURITY

D310001 CYBERSECURITY SPECIALIST

Provide a dedicated Cybersecurity Specialist on the D/B team. The Cybersecurity Specialist is to be an individual or firm who is regularly and professionally engaged in the business of the applications, installation, and testing of the specified Cybersecurity and equipment required for this project. The Cybersecurity Specialist is to demonstrate experience in providing successful control system security protection within the past three years of similar scope and size. **The Cybersecurity Specialist is to design a system in accordance with contract requirements and ensure the design is fully implemented during construction.** Additionally the Cybersecurity Specialist is **responsible for creating the artifacts and documentation required to achieve RMF authorization.** Submit documentation for a minimum of three and a maximum of five successful control system installations for the Cybersecurity Specialist.

USACE UMCS V APPENDIX B CYBERSECURITY

1.0 Cybersecurity Requirements: **The contractor shall follow Unified Facility Criteria (UFC) 4-010-06 and Unified Facility Guide Specification (UFGS) 25 05 11, Cybersecurity of Facility-Related Control Systems.** UFC 4-010-06 defines the five steps to integrate cybersecurity into the FRCS Design as follows (see UFC 4-010-06 Chapter 3-1.1 Five Steps for Cybersecurity Design):

1.1 **The Contractor shall provide a cyber-secure system(s) with all applicable security artifacts and security engineering to meet the requirements of receiving an ATO accreditation decision via the DoD RMF.** The implementation of cybersecurity measures in relation to design and construction / installation of the system shall not impede the system's functional requirements. However, cybersecurity measures should be applied to the greatest extent possible and where compliance cannot be met, deviations from cybersecurity standards should be documented and appropriately justified. The expected duration for RMF Activities 1-5 stated below shall be approximately 12 months. The Contractor shall conduct and participate in RMF meetings as required by the PWS.

New Contract Language from Air Force

Upon completion of RMF Step 2, (at the 60% Design Phase Submittal, and all subsequent Design Phase Submittals) the **A-E shall provide the following as deliverables:**

a) Updated Draft Security Plan with security controls and CCIs determined in this step, along with other artifacts provided by the System Owner

b) Edited guide specifications to include UFGS 25 05 11 and other specification sections with affected control systems

c) **Cybersecurity section in the Design Analysis which includes:**

Overview and description of cybersecurity requirements for this project. Draft Security Plan . Interview with site personnel/occupants and resulting recommendations. Review of Master Plan (if any). Field survey data. Survey of existing data communication infrastructure . Proposed data communication system (include routers/switches). Existing front-end system protocol and interface requirements. Integration to existing system technical solution (if any). Network Architecture including the proposed network IP ports, protocols, and services associated with the facility related control system. Workstation/server. Preliminary system components

Cyber Commissioning

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

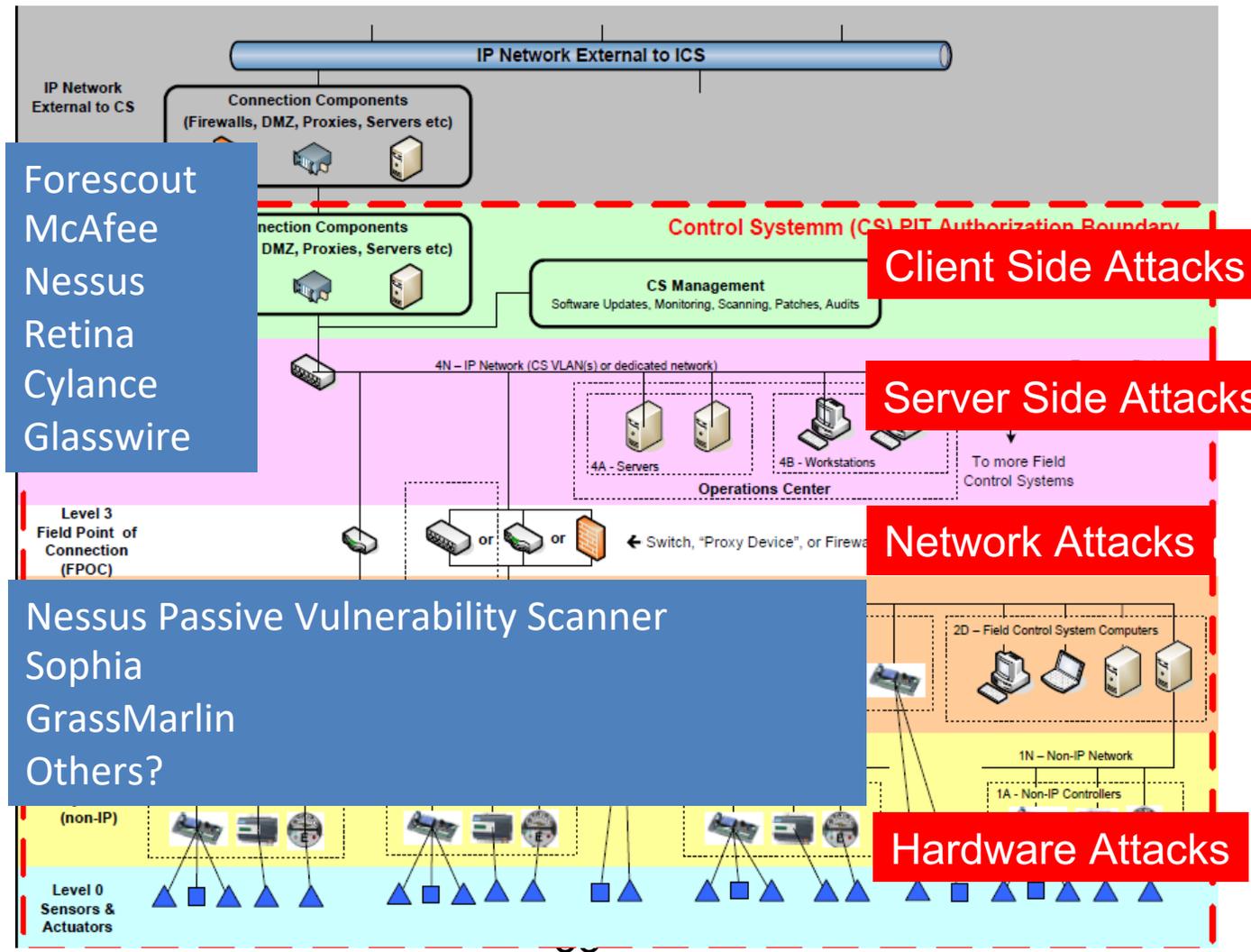
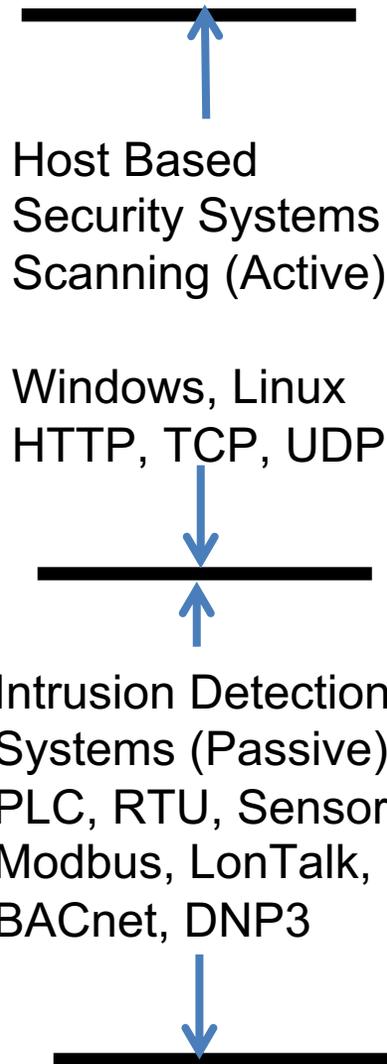
FRCS FAT and SAT Checklist - a checklist for FRCS to ensure the OS and vendor software, physical networks (firewalls, routers, devices, etc.) are properly hardened using the proper Security Technical Implementation Guides (STIGs) and configured to the JIE requirements. This will include the development, maintenance and turnover of the project Test and Development Environment at construction complete.

ACI TTP Fully-Mission Capable (FMC) Baseline - The FMC is a functional recovery point for the FRCS. Once this is defined, FRCS 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 FRCS. The Facility-Related Control Systems Inventory Spreadsheet is the initial FMC baseline.

FRCS Information Systems Contingency Plan (ISCP) – The ISCP and the FMC are used to perform disaster recovery and includes where back-ups are stored and the process to restore the FMC, the sequence of re-restart, assignment of personnel to the Roles and Responsibilities Table, and how to perform Functional and Validation Testing.

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

Continuous Monitoring (CM) and Attack Surfaces, Audit

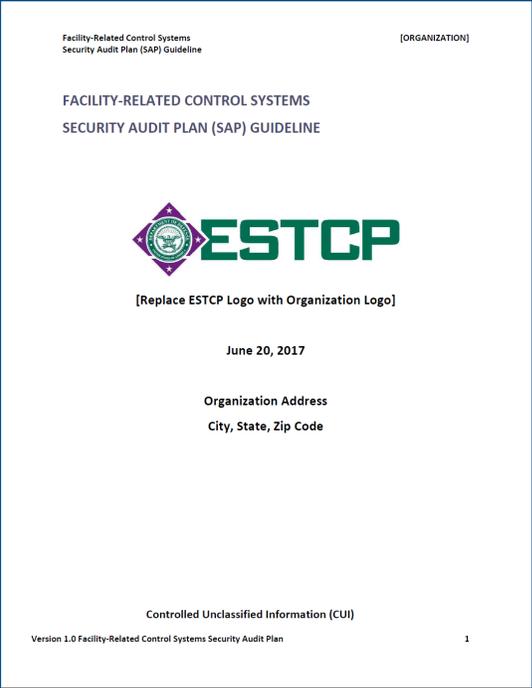


ForeScout
McAfee
Nessus
Retina
Cylance
Glasswire

Nessus Passive Vulnerability Scanner
Sophia
GrassMarlin
Others?

PI's/Project Teams may not get access to HBSS/ACAS, will need to use other CM tools (SCAP, Glasswire, Win Defender, Malwarebytes, TLS, etc.)

Security Audit Plan



Facility-Related Control Systems Security Audit Plan (SAP) Guideline [ORGANIZATION]

Step 1: Corporate IT Systems Admin Login Verification

- All system administrators log into the MS AD server console to validate credentials
- All system administrators log into the Office 365 server console to validate credentials
- All system administrators log into the firewalls and wireless access points to validate credentials
- All system administrators log into the corporate business servers to validate credentials
- All system administrators log into the corporate Electronic Security Systems servers to validate credentials

IT System	Name	Verified	
Active Directory		SysAdmin 1	No
Active Directory		SysAdmin 2	No
Remote Desktop Services (RDS 1)		SysAdmin 1	No
Remote Desktop Services (RDS 2)		SysAdmin 2	No
Server 1		SysAdmin 1	No
Server		SysAdmin 2	No
Office365		SysAdmin 1	No
Office365		SysAdmin 2	No

- 2.1 SYSTEM-LEVEL AUDIT TRAILS
- 2.2 APPLICATION-LEVEL AUDIT TRAIL
- 2.3 USER AUDIT TRAILS

PI's/Project Teams will need to perform audits of both IT and OT

NIST SCAP

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)***

The OCIL option is the capability to support the Open Checklist Interchange Language (OCIL) to collect information (data) from people and/or from existing data stores by other collection efforts.

PI's/Project Teams will use the DoD SCAP tool and the DoD STIGs to properly harden and configure the Level 4 servers, workstations and laptops

DISA STIGs – New Portal – Cyber Exchange

The screenshot shows the DoD Cyber Exchange Public website. The browser address bar displays <https://public.cyber.mil>. The page features a navigation menu with links for Topics, Training, PKI/PKE, SRGs/STIGs, Resources, and Help. A search bar and a "Login with CAC" button are also visible. The main content area is titled "ANNOUNCEMENTS" and contains four news items:

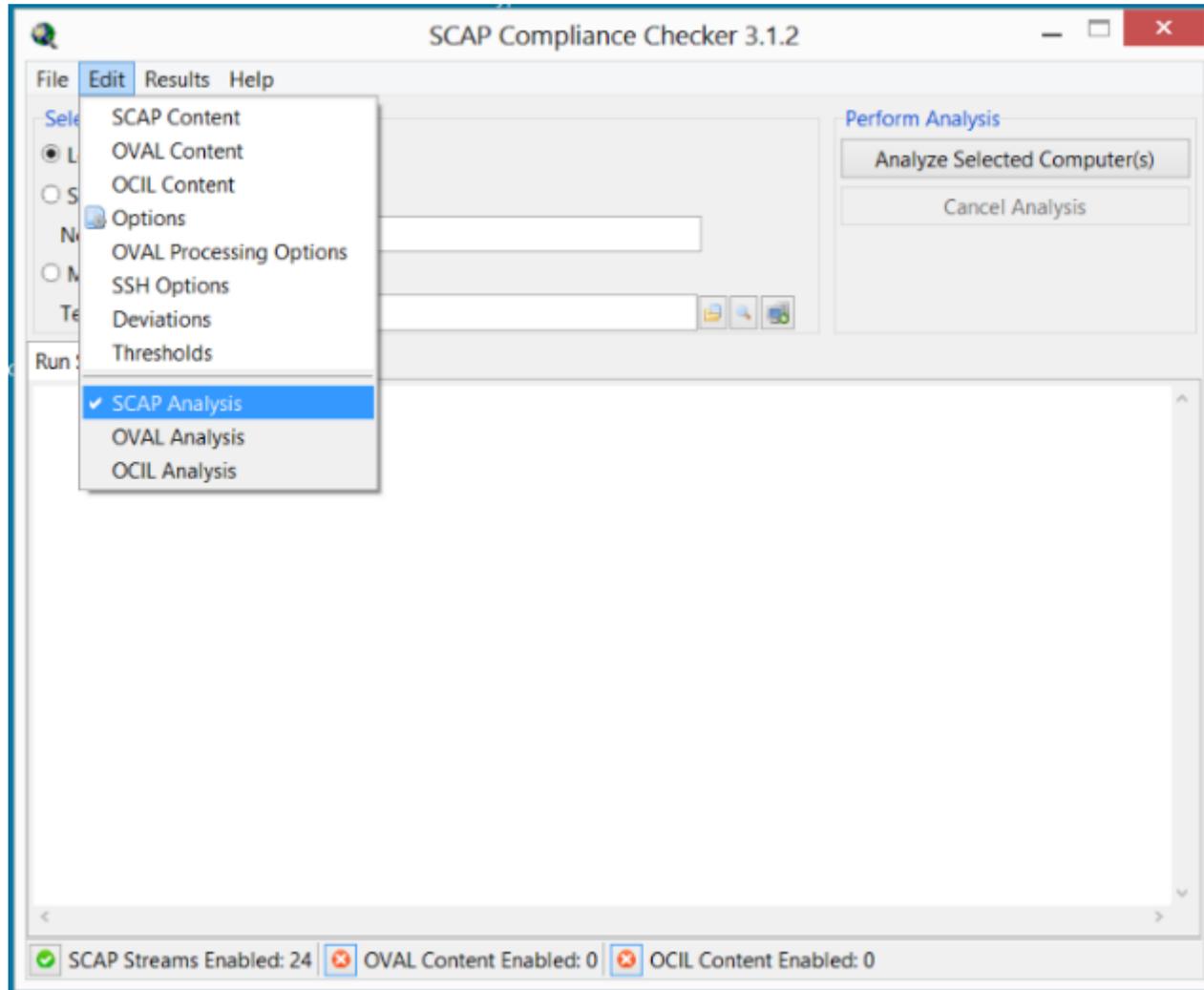
- DISA has released updates to the SRG/STIG Library Compilations**
These updates include the latest quarterly SRG/STIG update and newly released SRGs and STIGs published since the last quarterly update. Available at <https://public.cyber.mil/stigs/compilations/>
[+ Available here](#)
- Updated InstallRoot 5.5 installers**
InstallRoot 5.5 for Windows is now available for download on the DoD PKI website. This release adds support for new configuration file locations and support for Mozilla NSS cert19 and key4 database files used by newer versions of Firefox.
[+ Available here](#)
- Updated FBCA Cross-Certificate Remover v1.18**
This release incorporates two updated cross-certificates: DoD Interoperability Root CA 1 > DoD Root CA 2 and DoD CCEB Interoperability Root CA 2 > DoD Root CA 3.
[+ Available here](#)
- Required update for all users running Purebred Registration App 1.4 (or prior)**
Purebred Registration 1.4 (or prior) uses a now expired deployment profile that may prevent access to the keys from third party applications.
[+ Available here](#)

At the bottom of the page, there are three image thumbnails: a hand typing on a keyboard, a hand pointing at a network diagram, and a soldier in a field using a laptop.

Harden the OS, firewalls, switches, browsers, etc.

<https://public.cyber.mil/>

DISA SCAP Tool



PI's/Project Teams will be provided with the DoD SCAP tool

DISA SCAP Tool Contents

SCAP Content

Install Content | Configure Patch Updates

Content 24 of 25 enabled

Content	Profile	Date	Version	Path
<input checked="" type="checkbox"/> U_Microsoft_DotNet_Framework4_V1R1_Benchma	MAC-1_Classified	2013-03-06	1	Content\
<input checked="" type="checkbox"/> U_Microsoft_JE10_V1R3_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
<input checked="" type="checkbox"/> U_Microsoft_IE8_V1R11_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
<input checked="" type="checkbox"/> U_Microsoft_IE9_V1R5_STIG_Benchmark	MAC-1_Classified	2014-01-08	1	Content\
<input type="checkbox"/> U_Windows2012_DC_V1R1_STIG_Benchmark	MAC-1_Classified	2014-04-18	1	Content\
<input checked="" type="checkbox"/> U_Windows_2003_DC_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> U_Windows_2003_MS_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> U_Windows_2008_DC_V6R1.25_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> U_Windows_2008_MS_V6R1.25_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> U_Windows_2008_R2_DC_V1R11_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
<input checked="" type="checkbox"/> U_Windows_2008_R2_MS_V1R11_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
<input checked="" type="checkbox"/> U_Windows_7_V1R19_STIG_Benchmark	MAC-1_Classified	2013-12-18	1	Content\
<input checked="" type="checkbox"/> U_Windows_8_V1R4_STIG_Benchmark	MAC-1_Classified	2013-12-16	1	Content\
<input checked="" type="checkbox"/> U_Windows_Vista_V6R1.33_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> U_Windows_XP_V6R1.32_STIG_Benchmark	MAC-1_Classified	2013-12-18	6	Content\
<input checked="" type="checkbox"/> 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\
<input checked="" type="checkbox"/> 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\
<input checked="" type="checkbox"/> 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\
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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\
<input checked="" type="checkbox"/> 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

OK Cancel

Use the DoD STIG's, not the USGBC

DISA SCAP Tool Results

Summary Viewer
SCAP Compliance Checker - 5.0.2

2019-10-23_132442

Session: 2019-10-23_132442

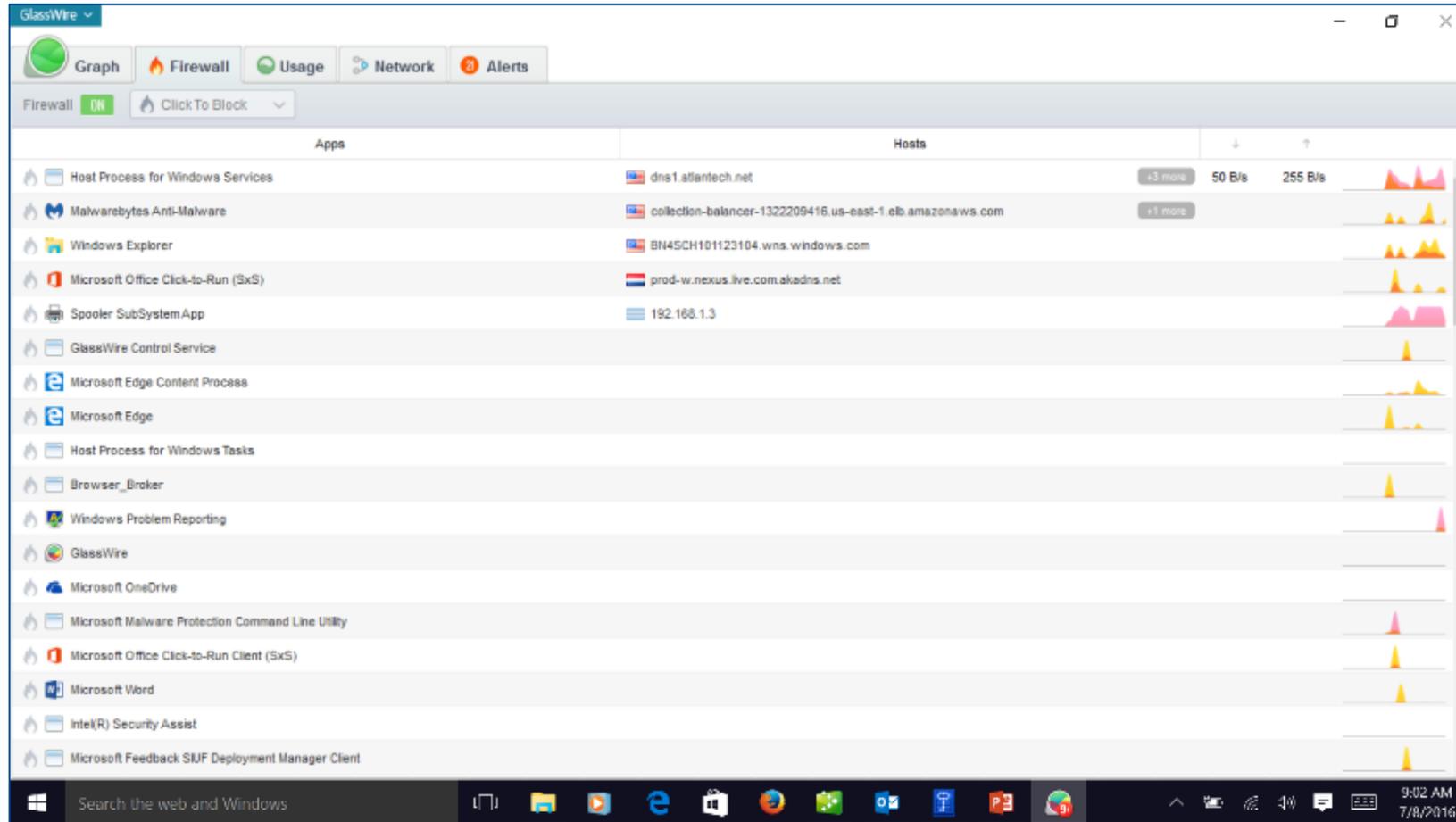
Stream	Host	Score	All Settings	Non-Compliance	NIST ARF	XCCDF Results	OVAL Results	OVAL Variables	OVAL CPE
E_11_STIG - v01.011	NORESCO	99.25	HTML	HTML	XML				
MS_Tot_Net_Framework - v01.004	NORESCO	100	HTML	HTML	N/A	XML	XML	XML	XML
Windows_Server_2016_STIG - v01.005	NORESCO	93.35	HTML	HTML	XML				

Showing 1 to 3 of 3 entries

SCAP Compliance Checker - 5.0.2 - SI/SAW Systems Center Atlanta

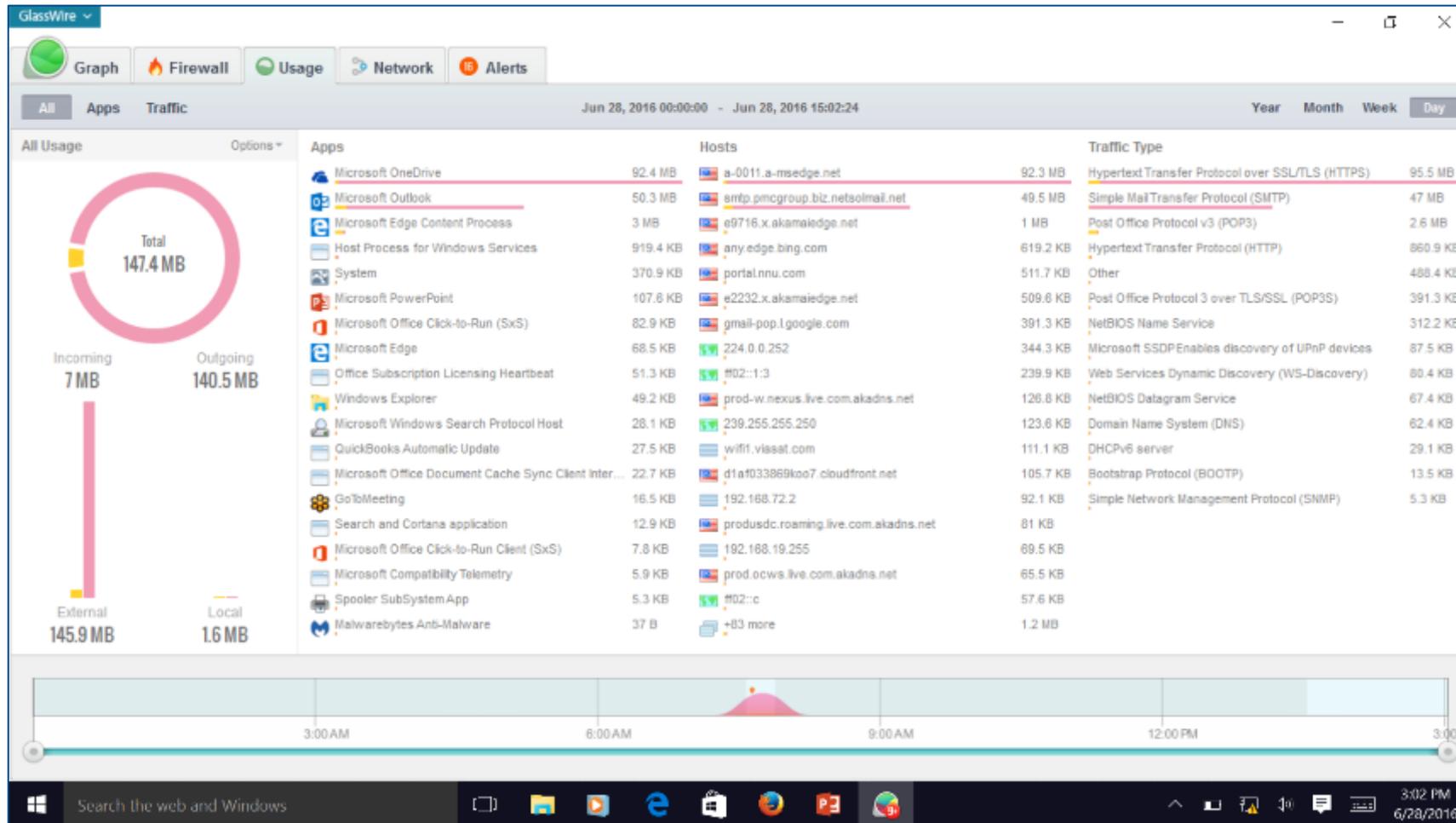
Maintain a score of 85 or better to demonstrate a properly hardened and configured system

Glasswire Firewall (IDS/IPS)



Glasswire can be used to simulate the HBSS/ACAS capability in the TDE

Glasswire Usage and Apps



Glasswire Alerts and Log's

The screenshot displays the GlassWire Alerts and Logs interface. At the top, there are navigation tabs for Graph, Firewall, Usage, Network, and Alerts. Below these, a table lists various alerts and logs. The table has columns for Date, Apps, and Type. A 'Mark all as read' button is located in the top right corner of the table area.

Date	Apps	Type
		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: 8.8.8.8 Old: fec0:0:0::fff::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: 8.8.8.8 Old: 192.168.5.1
Jun 20		
07:11:37		DNS server settings changed New: 192.168.5.1

Windows Log's

The screenshot displays the Windows Event Viewer interface with three overlapping windows:

- Top Window: Artifacts - Server System WinLog 10-08-2019**

Level	Date and Time	Source	Event ID	Task Category
Error	10/8/2019 12:36:46 PM	DistributedCOM	10016	None
Error	10/8/2019 12:25:23 PM	Disk	11	None
Error	10/8/2019 11:19:31 AM	DistributedCOM	10016	None
Error	10/8/2019 10:52:56 AM	Service Control Manager	7031	None
Error	10/8/2019 10:52:38 AM	Service Control Manager	7031	None
Error	10/8/2019 10:45:00 AM	DistributedCOM	10016	None
Error	10/8/2019 10:28:15 AM	DistributedCOM	10016	None
- Bottom-Left Window: Artifacts - Server Application WinLog 10-08-2019**

Level	Date and Time	Source	Event ID	Task Category
Error	10/8/2019 12:45:57 PM	Application Error	1000	Application Crashing Events
Error	10/8/2019 12:45:56 PM	.NET Runtime	1026	None
Error	10/8/2019 10:42:38 AM	RestartManager	10005	None
Error	10/8/2019 10:41:53 AM	RestartManager	10006	None

Event 1000, Application Error

General Details

Faulting application name: SQLServer2016-SSB-Eval.exe, version: 13.1805.4072.1, time stamp: 05b0f3c3d
 Faulting module name: KERNELBASE.dll, version: 10.0.14393.3085, time stamp: 0c5d1d7c96
 Exception code: 0ae0141132
 Fault offset: 0c000000000034c48
 Faulting process id: 0x1644
 Faulting application start time: 0d71d57df7d4a7a6
 Faulting application path: D:\Program (x64)\SQL\SQLServer2016-SSB-Eval.exe
 Faulting module path: C:\Windows\System32\KERNELBASE.dll
 Report id: a3c6846b-21d8-4350-9941-6f86a37c0e22
 Faulting package full name:
 Faulting package-relative application ID:

Log Name: Application
 Source: Application Error
 Event ID: 1000
 Level: Error
 User: N/A
 Op Code:
 More information: [Event Log Online Help](#)
- Bottom-Right Window: Artifacts - Server System WinLog 10-08-2019**

Event 10016, DistributedCOM

grant Local Activation permission for the COM Server application with CLSID
 from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission
 administrative tool.

Logged: 10/8/2019 12:36:46 PM
 Task Category: None
 Keywords: Classic
 Computer: NORESKO

AV/MW Reports

Antivirus Health

Client Antivirus Health



Healthy

Average Definition File Age

5 days

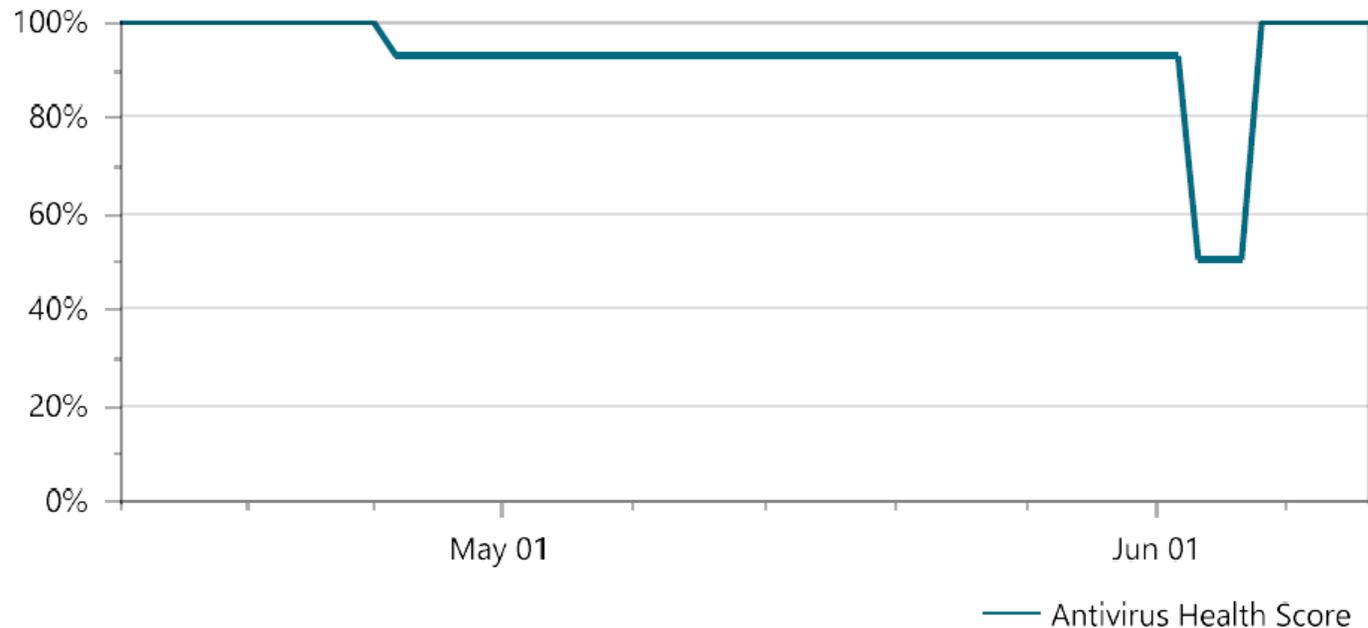
Total Managed Assets

2 server(s) / 5 workstation(s)

Total At-Risk Assets

0 server(s) / 0 workstation(s)

Antivirus Health History



Patch Reports

Patch Compliance

Patch Compliance



91.18%

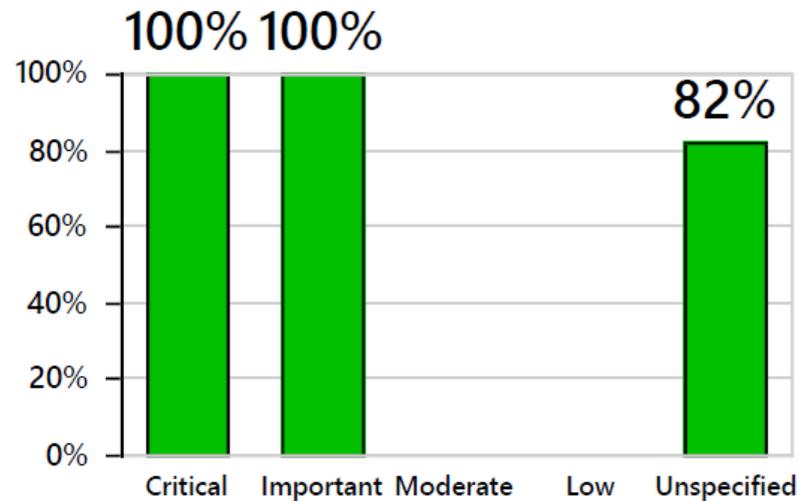
Patch Compliance Calculation

31 Installed / 34 Approved

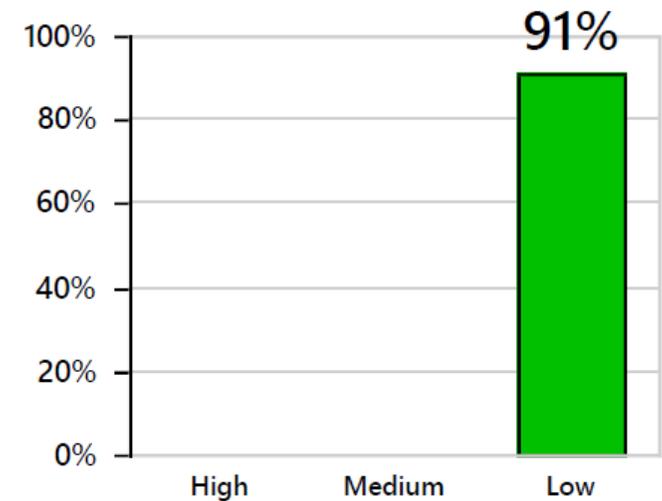
Total Managed Windows Assets

2 Servers / 5 Workstations

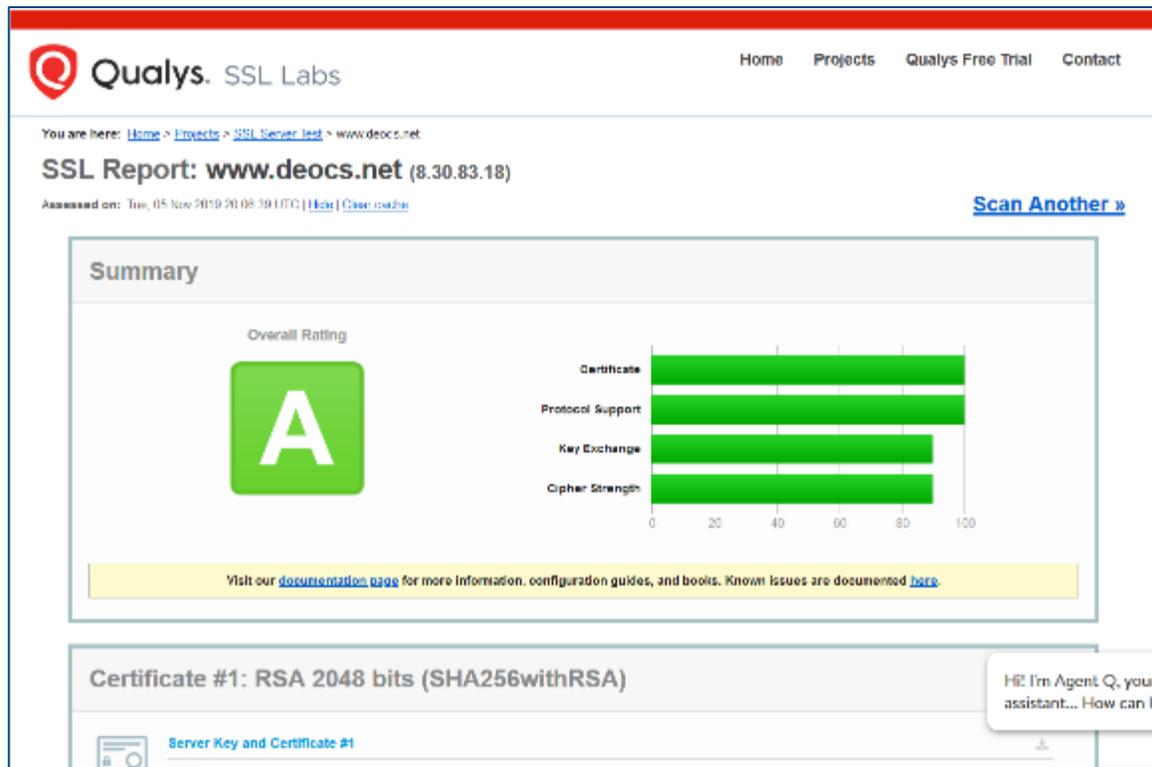
Compliance by Severity



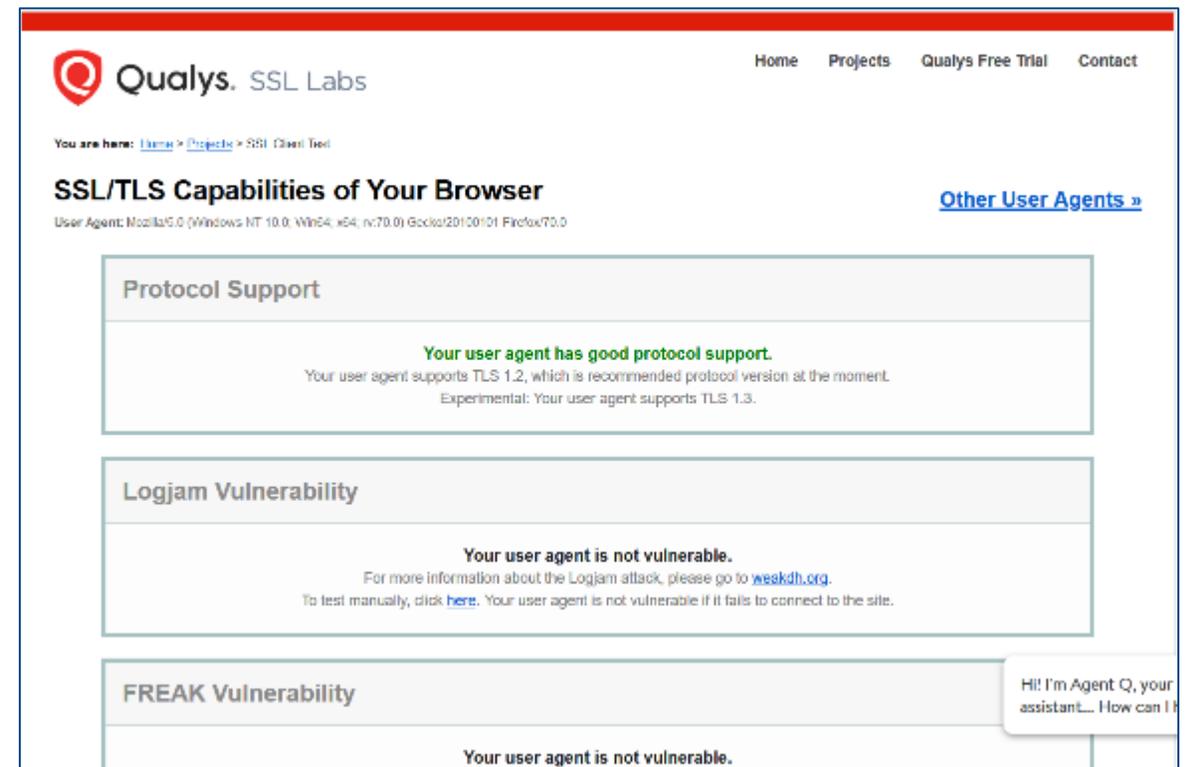
Compliance by CVSS



TLS Reports

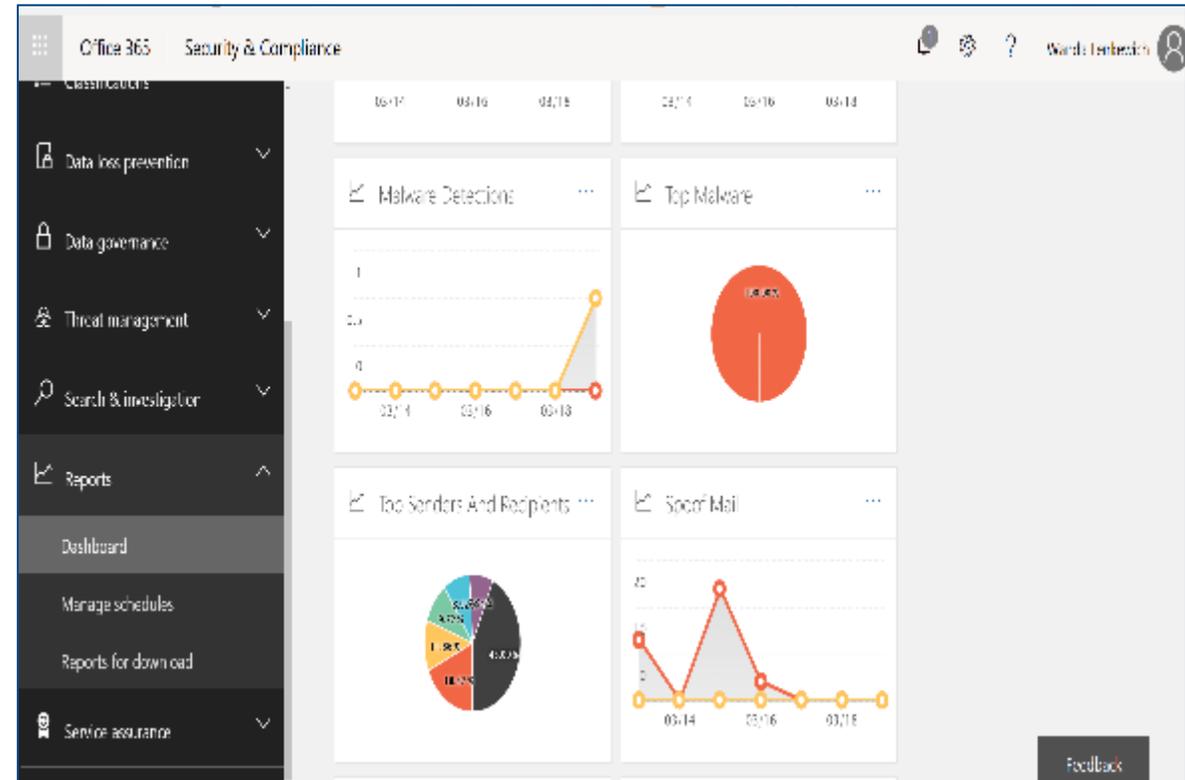
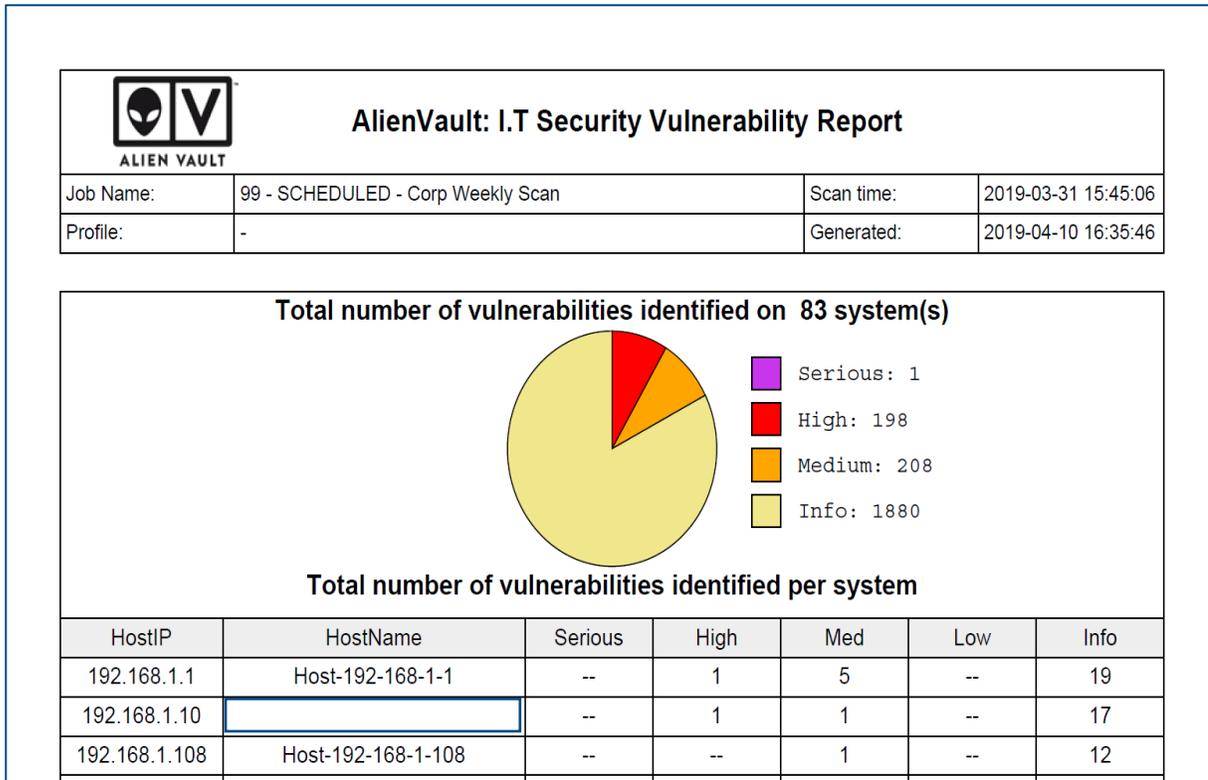


Server Test

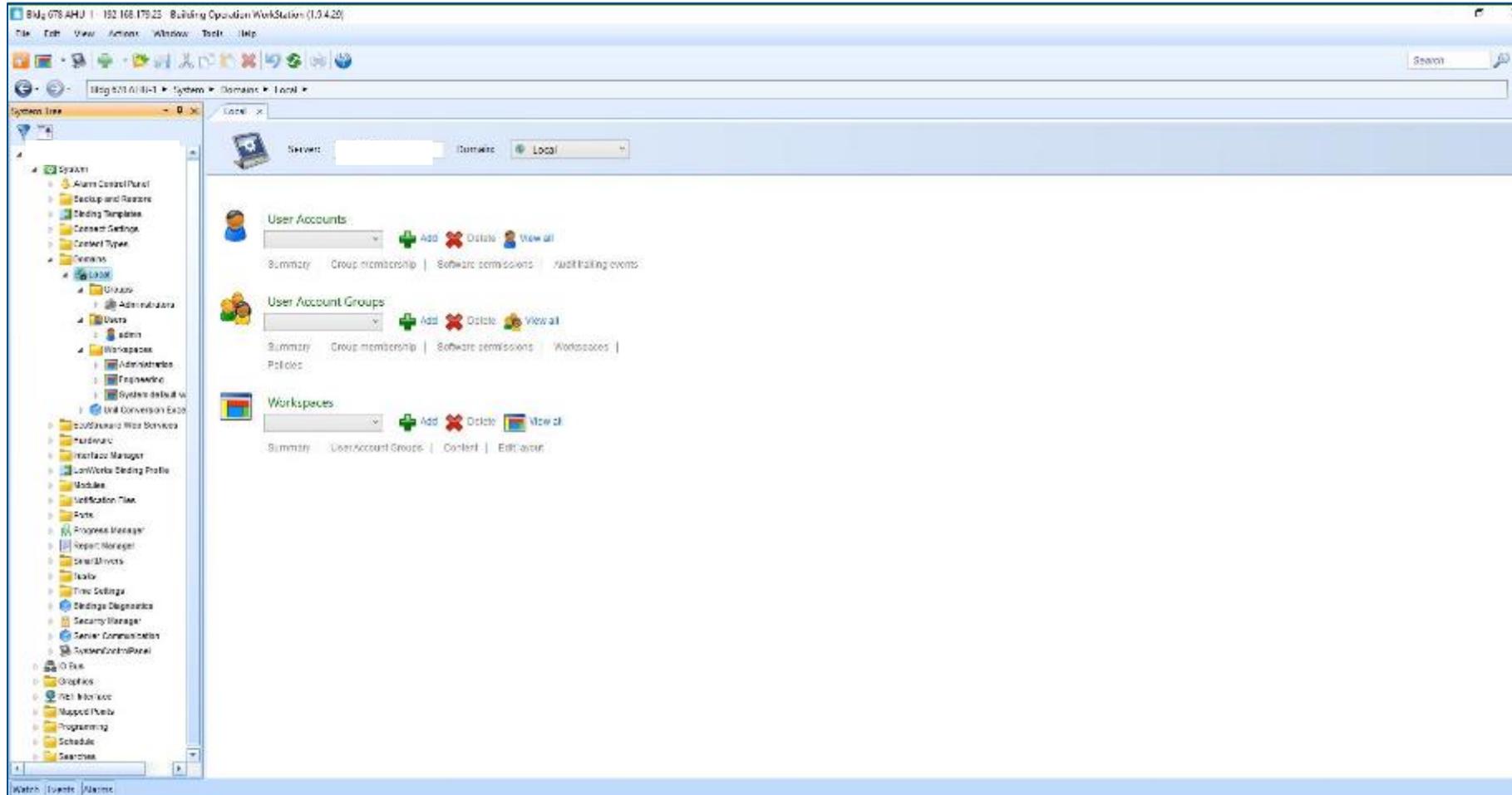


Client Browser Test

SEIM Reports



User Accounts Reports



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

DHS CSET



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

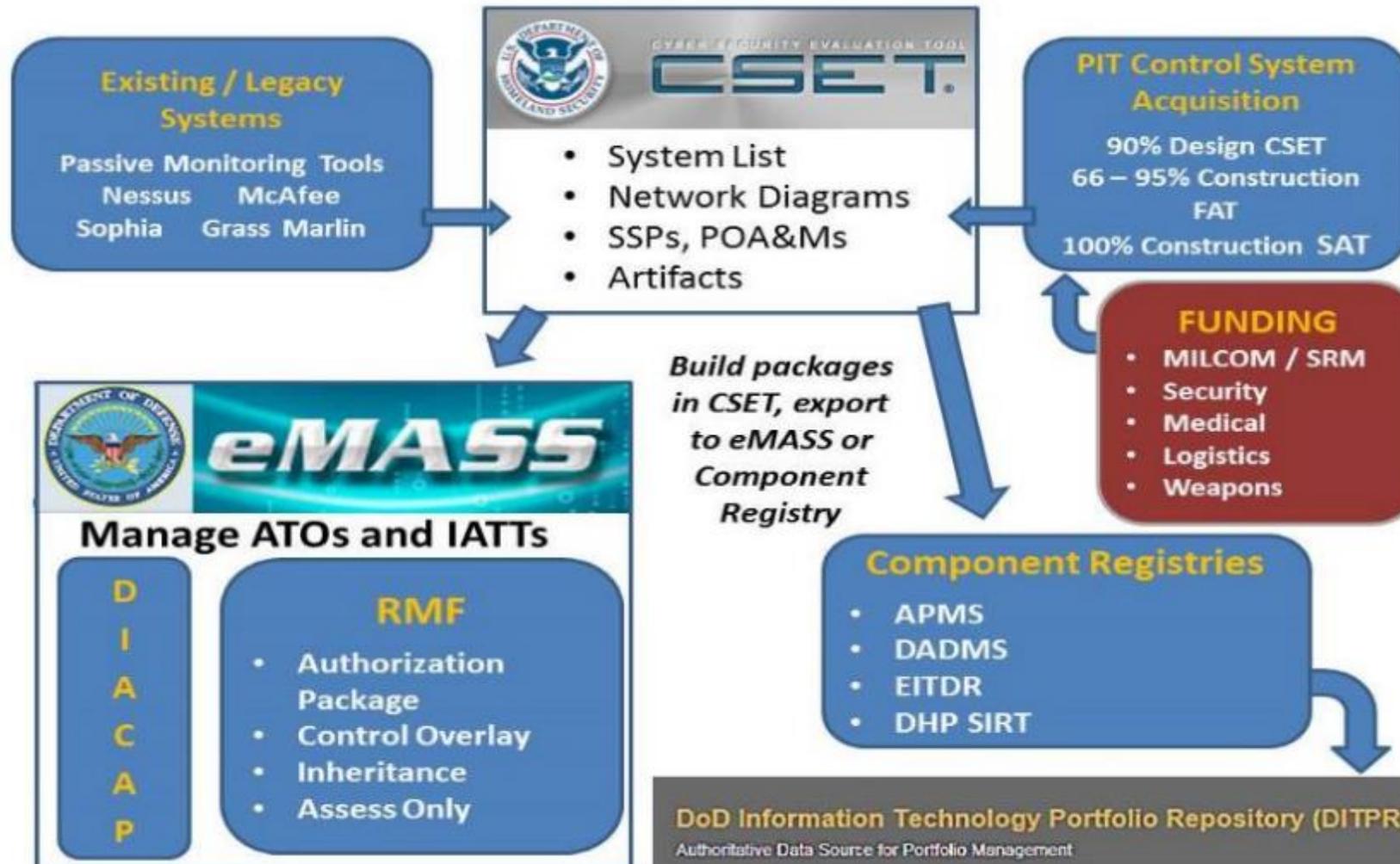


CSET Download:

<https://www.us-cert.gov/ics/Downloading-and-Installing-CSET>

<https://github.com/cisagov/cset#cset-901>

CSET and eMASS Relationship



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

CSET Process

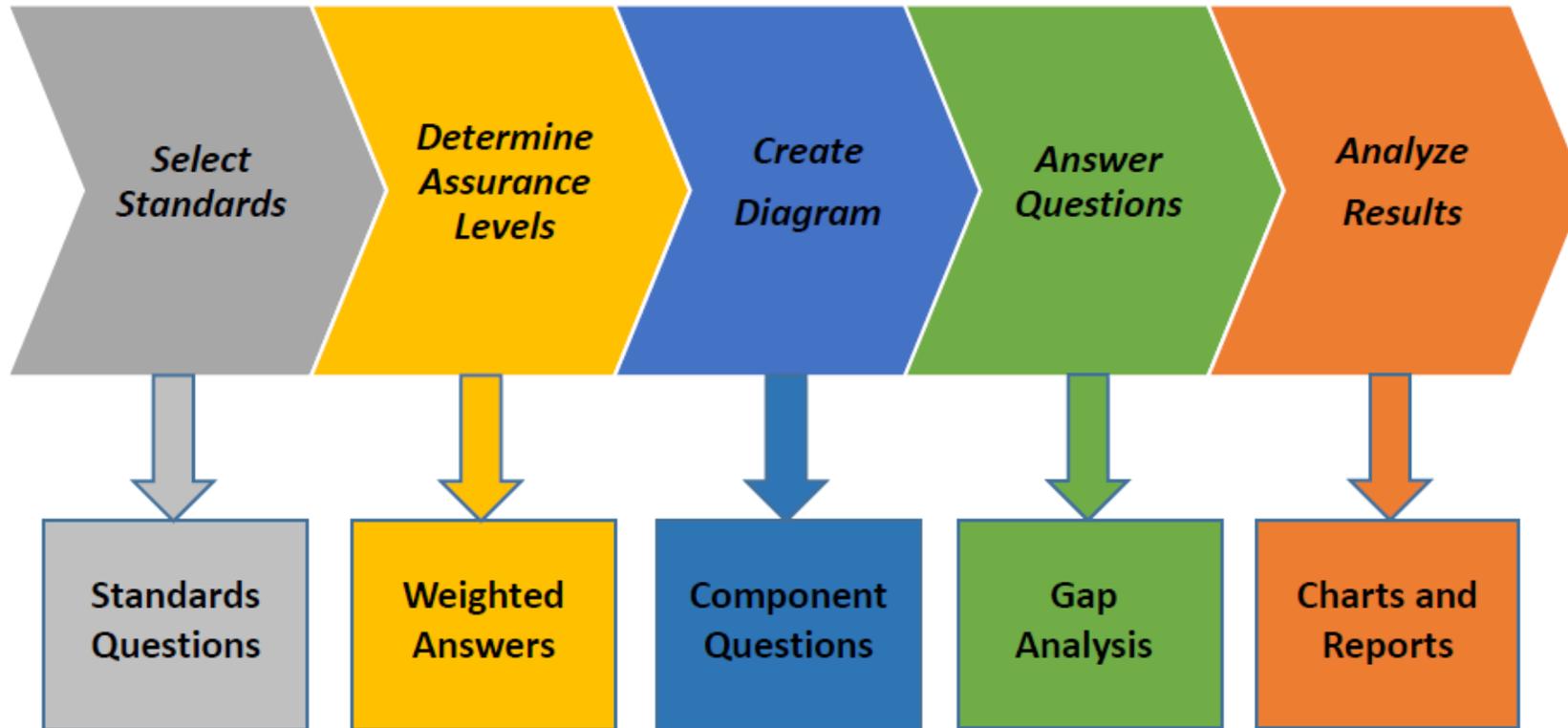
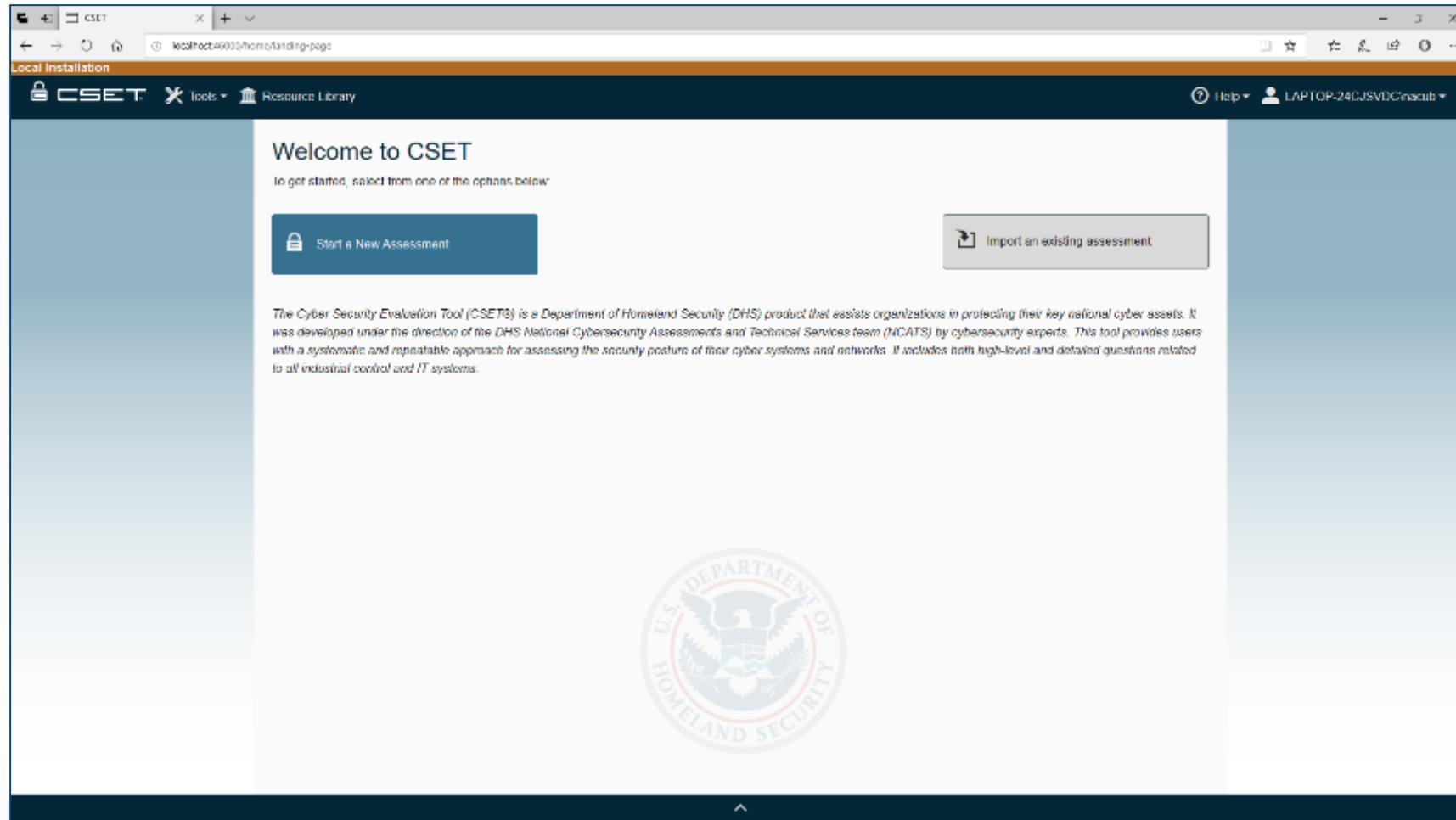
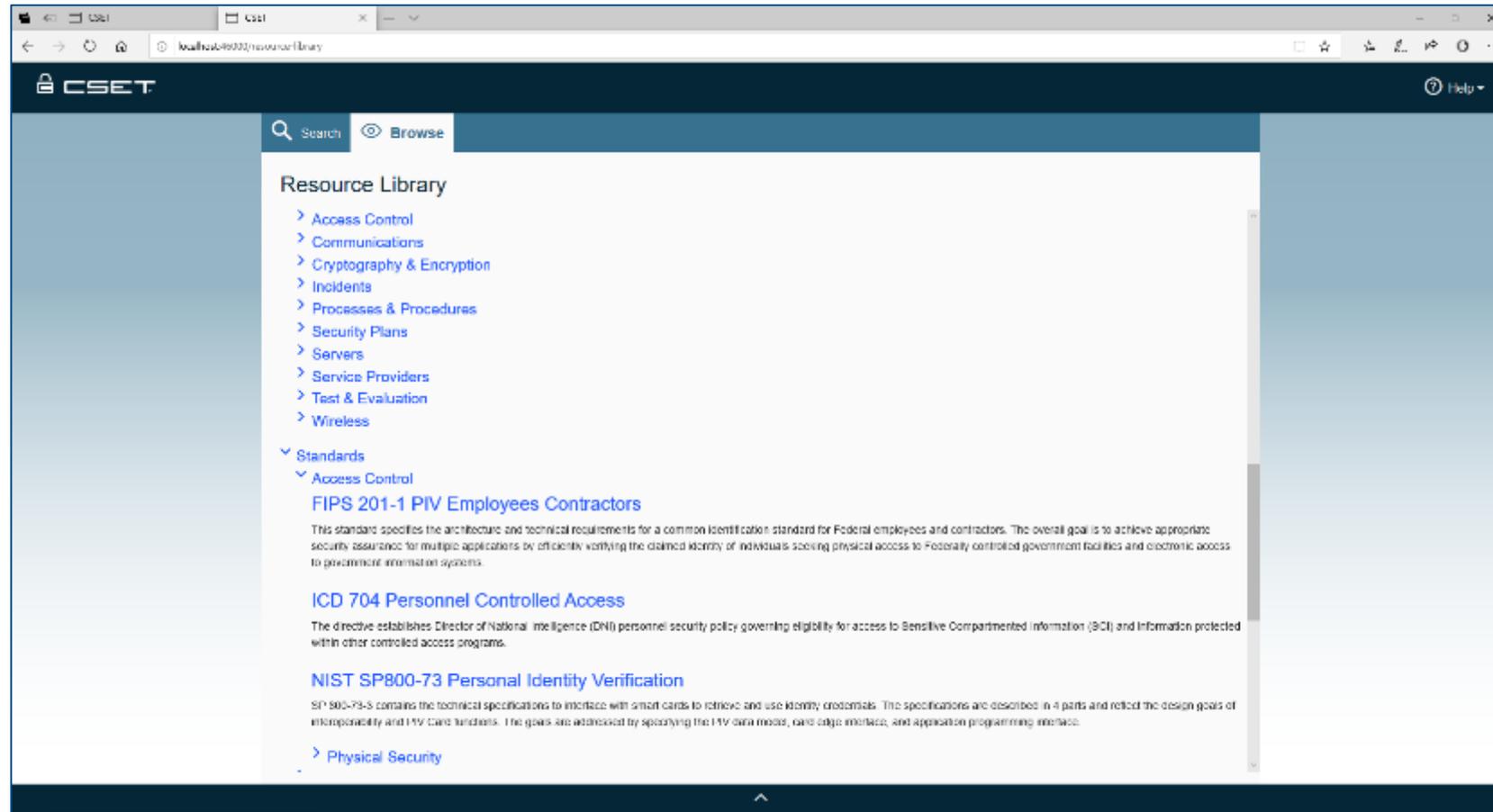


Figure 3-1. CSET process.

CSET Start



Resource Library



The screenshot shows a web browser window displaying the CSET Resource Library. The browser's address bar shows the URL `malhub4900/resource-library`. The CSET logo is in the top left, and a 'Help' icon is in the top right. Below the logo, there are 'Search' and 'Browse' buttons. The main content area is titled 'Resource Library' and contains a list of categories with expandable arrows:

- > Access Control
- > Communications
- > Cryptography & Encryption
- > Incidents
- > Processes & Procedures
- > Security Plans
- > Servers
- > Service Providers
- > Test & Evaluation
- > Wireless
- ▼ Standards
 - ▼ Access Control
 - [FIPS 201-1 PIV Employees Contractors](#)

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.
 - [ICD 704 Personnel Controlled Access](#)

The directive establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs.
 - [NIST SP800-73 Personal Identity Verification](#)

SP 800-73-3 contains the technical specifications to interface with smart cards to retrieve and use identity credentials. The specifications are described in 4 parts and reflect the design goals of interoperability and PIV card functions. The goals are addressed by specifying the PIV data model, card edge interface, and application programming interface.
 - > Physical Security

Home and Site Information

The screenshot shows a web browser window with the URL `localhost:45002/assessment/3/prepare/info`. The page title is "Local Installation" and the CSET logo is visible in the top left. The navigation bar includes "Tools" and "Resource Library". The main content area is titled "Assessment Information" and is divided into two sections: "Details" and "Contacts".

Assessment Information

Details

Assessment Name * Assessment Date

Facility Name

City Or Site Name State/Province/Region

Contacts

LAPTOP-24CJSVDCinacub Assessment Owner
LAPTOP-24CJSVDCinacub@myorg.org
Administrator

First Name Last Name

Email

Role

Sector and Demographic Information

The screenshot displays a web browser window with the URL `localhost:4000/assessment/3/prepare/info`. The page is titled "Local Installation" and features a navigation bar with "CSET", "Tools", and "Resource Library". The main content area is divided into a left sidebar and a central form. The sidebar contains a back arrow and three menu items: "Assessment Information", "Security Assurance Level (SAL)", and "Cybersecurity Standards Selection". The central form is titled "Prepare" and includes tabs for "Questions" and "Results".

The form contains the following fields and options:

- First Name:** Michael
- Last Name:** Chipley
- Email:** mchipley@pmcbiz.com
- Role:** User (selected), Administrator
- Buttons:** Save, Cancel
- + Add Contact:** A button to add a new contact.
- Demographics:**
 - Sector:** Government Facilities Sector
 - Industry:** Local Governments
 - What is the gross value of the asset you are trying to protect?:** < \$10,000,000
 - What is the relative expected effort for this assessment?:** Large (3+ days)
- Buttons:** Next

Security Assurance Level Selection

The screenshot shows a web browser window with the URL `localhost:40013/assessment/5/prepare/sal`. The page title is "Local Installation" and the browser shows "CSET" and "tools" in the address bar. The user is logged in as "LAPTOP-24CJ5VDCGnaut". The main content area is titled "Security Assurance Level (SAL)" and includes the following sections:

- Prepare** (selected), Questions, Results
- Security Assurance Level (SAL)**
 - The Security Assurance Level or SAL 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.
 - Current Security Assurance Level**

Overall	Confidentiality	Integrity	Availability
High	High	High	High
 - Choose one of the three SAL methodologies below to determine the correct level for your assessment:
 - Simple (selected)
 - General Risk Based
 - NIST-60 / FIPS-180
 - Overall SAL**
 - Low
 - Moderate
 - High (selected)
 - Very High
 - Confidentiality**

This value relates to the importance of protecting information from unauthorized access. The more important it is that unauthorized users do not have access to the information the higher your SAL level.

 - Low
 - Moderate
 - High (selected)
 - Very High
 - Integrity**

This value relates to the importance of the accuracy of information. The more important it is that information is kept consistent, accurate, and only changed by those authorized the higher your SAL level.

 - Low
 - Moderate
 - High (selected)
 - Very High
 - Availability**

FIPS 199 SAL Guidance

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](#)

CIA Values Based on Selected Information Types

Check applicable information types.

Type	C	I	A
<input type="checkbox"/> Air Transportation : D.11.3	LOW	LOW	LOW
<input type="checkbox"/> Asset and Liability Management : C.3.2.1	LOW	LOW	LOW
<input type="checkbox"/> Budget Execution : C.2.3.5	LOW	LOW	LOW
<input type="checkbox"/> Budget Formulation : C.2.3.1	LOW	LOW	LOW
<input type="checkbox"/> Budgeting & Performance Integration : C.2.3.8	LOW	LOW	LOW
<input type="checkbox"/> Capital Planning : C.2.3.2	LOW	LOW	LOW

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

The screenshot shows the CSET web application interface. At the top, there are navigation tabs for 'Prepare', 'Questions', and 'Results'. Below these, four summary boxes show 'Overall', 'Confidentiality', 'Integrity', and 'Availability', all set to 'High'. The main section is titled 'CIA Values Based on Selected Information Types' and includes a sub-instruction: 'Check applicable information types.' Below this is a table with columns for 'Type', 'C', 'I', and 'A'. Each row represents an information type with a checkbox and corresponding CIA values.

Type	C	I	A
<input type="checkbox"/> Air Transportation : D.11.3	LOW	LOW	LOW
<input type="checkbox"/> Asset and Liability Management : C.3.2.1	LOW	LOW	LOW
<input type="checkbox"/> Budget Execution : C.2.3.5	LOW	LOW	LOW
<input type="checkbox"/> Budget Formulation : C.2.3.1	LOW	LOW	LOW
<input type="checkbox"/> Budgeting & Performance Integration : C.2.3.8	LOW	LOW	LOW
<input type="checkbox"/> Capital Planning : C.2.3.2	LOW	LOW	LOW
<input type="checkbox"/> Collections & Receivables : C.3.2.6	LOW	MOD	LOW
<input type="checkbox"/> Contingency Planning : C.2.4.1	MOD	MOD	MOD
<input type="checkbox"/> Continuity of Operations : C.2.4.2	MOD	MOD	MOD
<input type="checkbox"/> Cost Accounting/Performance Measurement : C.3.2.7	LOW	MOD	LOW
<input type="checkbox"/> Customer Services : C.2.6.1	LOW	LOW	LOW
<input type="checkbox"/> Disaster Preparedness & Planning : D.4.2	LOW	LOW	LOW
<input type="checkbox"/> Emergency Response : D.4.4	LOW	HIGH	HIGH

FIPS 199 SAL Answer Questions

Local Installation

CSET Tools Resource Library Help LAPTOP-24CJSVDCinacub

Prepare Questions Results

Overall	Confidentiality	Integrity	Availability
High	High	High	High

Answer Questions

- Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems? Yes No
- Does/could access to this system result in some form of access to other more sensitive or critical systems (e.g., over a network)? Yes No
- 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? Yes No
- 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? Yes No
- 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? Yes No
- Does the mission served by the system, or the information that the system processes, affect the security of critical infrastructures and key resources? Yes No
- Does the system store, communicate, or process any privacy act information? Yes No
- Does the systems store, communicate, or process any trade secrets information? Yes No

Determine Special Factors

Confidentiality Special Factor

FIPS 199 SAL Special Factors

The screenshot shows a web browser window with the URL `localhost:4000/assessments/3/prepare/sal`. The page is titled "Local Installation" and features the CSET logo and navigation links for "Tools" and "Resource Library". The main content area is titled "Prepare" and includes a progress bar with "Prepare", "Questions", and "Results" tabs. Below the progress bar, there are four summary boxes for "Overall", "Confidentiality", "Integrity", and "Availability", all showing a "High" rating. The form contains two questions with "Yes/No" radio buttons:

- Does the system store, communicate, or process any privacy act information?
- Does the systems store, communicate, or process any trade secrets information?

Below these questions is a section titled "Determine Special Factors" with three text input fields for "Confidentiality Special Factor", "Integrity Special Factor", and "Availability Special Factor". At the bottom of the form are "Back" and "Next" buttons.

Cybersecurity Standard Selection

The screenshot shows a web browser window displaying the CSET Cybersecurity Standards Selection page. The browser address bar shows the URL: `localhost:9000/assessment/5/prepare/standards`. The page header includes the CSET logo, navigation links for Tools and Resource Library, and a user profile for LAPTOP-24CJ5VDCInacub. The main content area is titled "Cybersecurity Standards Selection" and includes instructions: "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." Below this, there is a link: "I want to do a basic assessment instead". Two buttons, "Requirements" (1030) and "Questions" (1061), are visible. The list of standards is categorized into: Chemical, Oil, and Natural Gas; DoDI and CNSSI; Electrical; Financial; and General. Each standard has a checkbox and a dropdown arrow.

Cybersecurity Standards 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.
[I want to do a basic assessment instead](#)

Requirements: 1030 Questions: 1061

Chemical, Oil, and Natural Gas

- CFATS Risk Based Performance Standards Guide 8 Cyber
- CIS Controls Version 6
- INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- TSA Pipeline Security Guidelines April 2011

DoDI and CNSSI

- CNSSI No. 1253 Baseline V2 March 27, 2014
- DoD Instruction 8510.01

Electrical

- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NERC CIP-002 through CIP-011 Rev 5
- NERC CIP-002 through CIP-014 Rev 6
- NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1
- NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1 Rev 1

Financial

- Payment Card Industry (PCI) Data Security Standard

General

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.

Create a network diagram

< Back Continue >>

Ask me anything 11:46 AM 10/3/2016

CSET 8.1 Network Diagrams

The screenshot displays the CSET 8.1 Network Diagrams software interface. The window title is "Diagram Tool". The interface includes a ribbon menu with tabs for "Home" and "Format". The ribbon contains various icons for actions such as "Clear Diagram", "Templates", "Layers", "Analyze Network", "Diagram Inventory", "Preview/Print", "Settings" (with a "Default SAL" dropdown set to "High"), "Export as Image", "Import Diagram", "Export Diagram", "Import Visio", "Export Visio", "Grass", and "Marlin Import". A "Help" icon is also present.

On the left side, there is a "Stencils" and "Symbols" panel. The "Stencils" panel lists categories: ICS, IT, Radio, Medical, General, Zone, and Shapes. The "Symbols" panel lists various network components: Configuration Server, DCS, EWS, FFP, Historian, HMI, IED, MTU, PLC, RTU, SIS, Terminal Server, and Unidirectional.

The main workspace shows a network diagram on a grid background. The diagram is divided into two main sections: a yellow-shaded area on the left and a light blue-shaded area on the right. The yellow area contains a "Domain" network with a central "Domain Controller" and various servers and workstations. The light blue area contains a "Security Control System (SCS)" network with a central "SCS Controller" and various sensors and devices. A "Save and Close" button is visible in the bottom right corner of the workspace.

The Windows taskbar at the bottom shows the system tray with the time "11:58 AM" and date "10/3/2016".

Diagram – Tools, Templates, Inventory

The screenshot displays the CSET Diagram Tool software interface. The title bar reads "CSET Diagram Tool". The ribbon menu includes "Home" and "Format" tabs. The "Home" tab contains icons for "Clear Diagram", "Templates", "Layers", "Analyze Network", "Diagram Inventory", "Preview/Print", "Settings", "Export as Image", "Import Diagram", "Export Diagram", "Import Visio", "Export Visio", "Grass", and "Marlin Import". The "Settings" section shows "Default SAL" set to "High". The "Import/Export" section includes "Import Diagram", "Export Diagram", "Import Visio", and "Export Visio". The "Help" section has a question mark icon.

A "Manage Templates..." dropdown menu is open on the left, listing various system templates: Building Access Control, DCS, Electric, HVAC, Hydro, Medical, Nuclear, Oil & Gas 1, Oil & Gas 2, PCS, Radio, SCADA, Traffic Control, Waste Water Treatment Plant, and Water Plant System.

The main workspace shows a network diagram on a grid background. The diagram is divided into two main sections: a yellow-shaded area on the left and a light blue-shaded area on the right. The yellow area contains a "Dependent Line" diagram with components like "Mobile Device", "VTS-01", "VTS-02", "VTS-03", "VTS-04", "VTS-05", "VTS-06", "VTS-07", "VTS-08", "VTS-09", "VTS-10", "VTS-11", "VTS-12", "VTS-13", "VTS-14", "VTS-15", "VTS-16", "VTS-17", "VTS-18", "VTS-19", "VTS-20", "VTS-21", "VTS-22", "VTS-23", "VTS-24", "VTS-25", "VTS-26", "VTS-27", "VTS-28", "VTS-29", "VTS-30", "VTS-31", "VTS-32", "VTS-33", "VTS-34", "VTS-35", "VTS-36", "VTS-37", "VTS-38", "VTS-39", "VTS-40", "VTS-41", "VTS-42", "VTS-43", "VTS-44", "VTS-45", "VTS-46", "VTS-47", "VTS-48", "VTS-49", "VTS-50", "VTS-51", "VTS-52", "VTS-53", "VTS-54", "VTS-55", "VTS-56", "VTS-57", "VTS-58", "VTS-59", "VTS-60", "VTS-61", "VTS-62", "VTS-63", "VTS-64", "VTS-65", "VTS-66", "VTS-67", "VTS-68", "VTS-69", "VTS-70", "VTS-71", "VTS-72", "VTS-73", "VTS-74", "VTS-75", "VTS-76", "VTS-77", "VTS-78", "VTS-79", "VTS-80", "VTS-81", "VTS-82", "VTS-83", "VTS-84", "VTS-85", "VTS-86", "VTS-87", "VTS-88", "VTS-89", "VTS-90", "VTS-91", "VTS-92", "VTS-93", "VTS-94", "VTS-95", "VTS-96", "VTS-97", "VTS-98", "VTS-99", "VTS-100". The light blue area contains a "Building Control System (BACS) - BACS" diagram with components like "BACS-01", "BACS-02", "BACS-03", "BACS-04", "BACS-05", "BACS-06", "BACS-07", "BACS-08", "BACS-09", "BACS-10", "BACS-11", "BACS-12", "BACS-13", "BACS-14", "BACS-15", "BACS-16", "BACS-17", "BACS-18", "BACS-19", "BACS-20", "BACS-21", "BACS-22", "BACS-23", "BACS-24", "BACS-25", "BACS-26", "BACS-27", "BACS-28", "BACS-29", "BACS-30", "BACS-31", "BACS-32", "BACS-33", "BACS-34", "BACS-35", "BACS-36", "BACS-37", "BACS-38", "BACS-39", "BACS-40", "BACS-41", "BACS-42", "BACS-43", "BACS-44", "BACS-45", "BACS-46", "BACS-47", "BACS-48", "BACS-49", "BACS-50", "BACS-51", "BACS-52", "BACS-53", "BACS-54", "BACS-55", "BACS-56", "BACS-57", "BACS-58", "BACS-59", "BACS-60", "BACS-61", "BACS-62", "BACS-63", "BACS-64", "BACS-65", "BACS-66", "BACS-67", "BACS-68", "BACS-69", "BACS-70", "BACS-71", "BACS-72", "BACS-73", "BACS-74", "BACS-75", "BACS-76", "BACS-77", "BACS-78", "BACS-79", "BACS-80", "BACS-81", "BACS-82", "BACS-83", "BACS-84", "BACS-85", "BACS-86", "BACS-87", "BACS-88", "BACS-89", "BACS-90", "BACS-91", "BACS-92", "BACS-93", "BACS-94", "BACS-95", "BACS-96", "BACS-97", "BACS-98", "BACS-99", "BACS-100".

A "Save and Close" button is visible in the bottom right corner of the diagram area. The Windows taskbar at the bottom shows the time as 12:00 PM on 10/3/2016.

Diagram – Zones, Layers

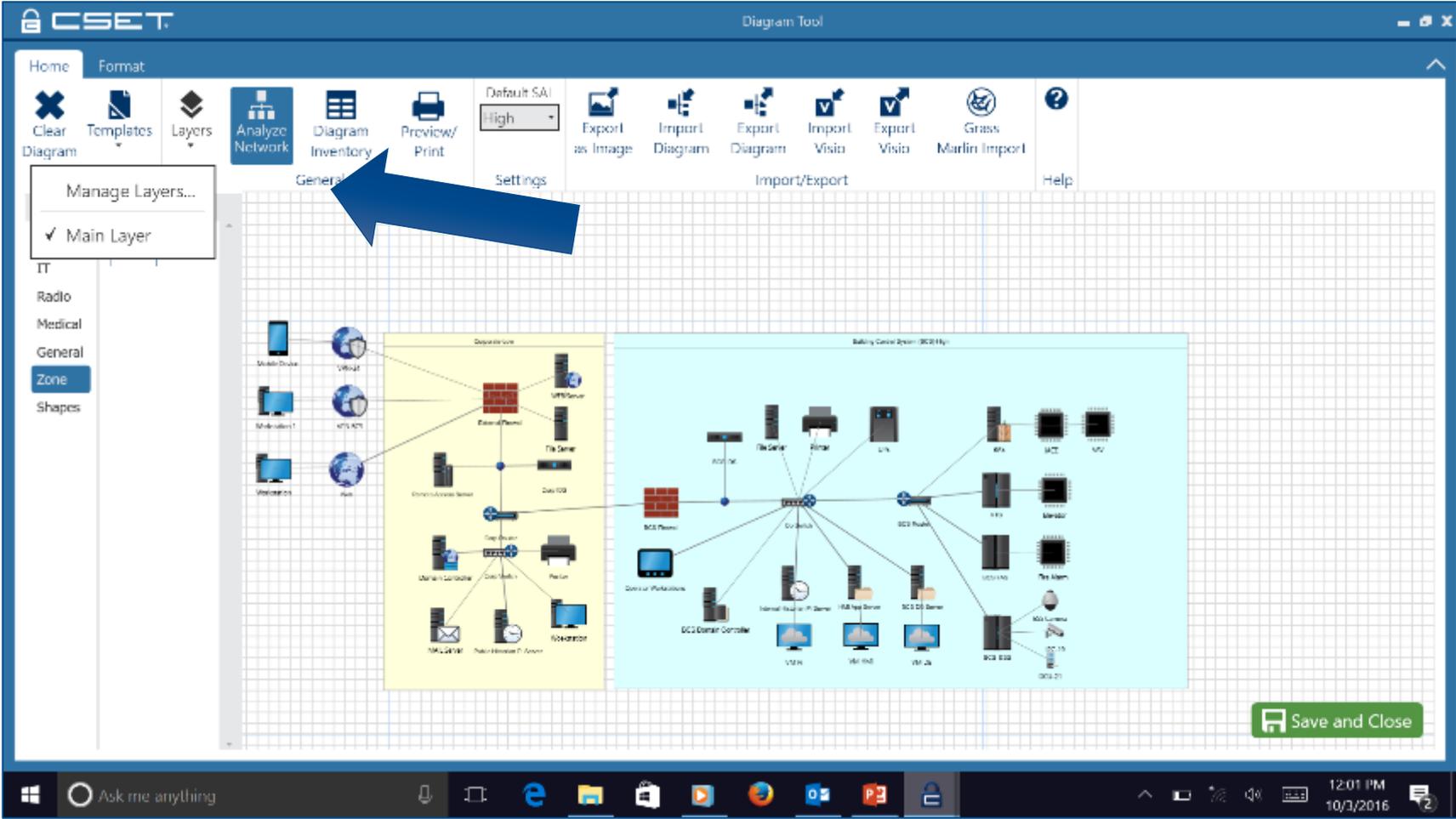
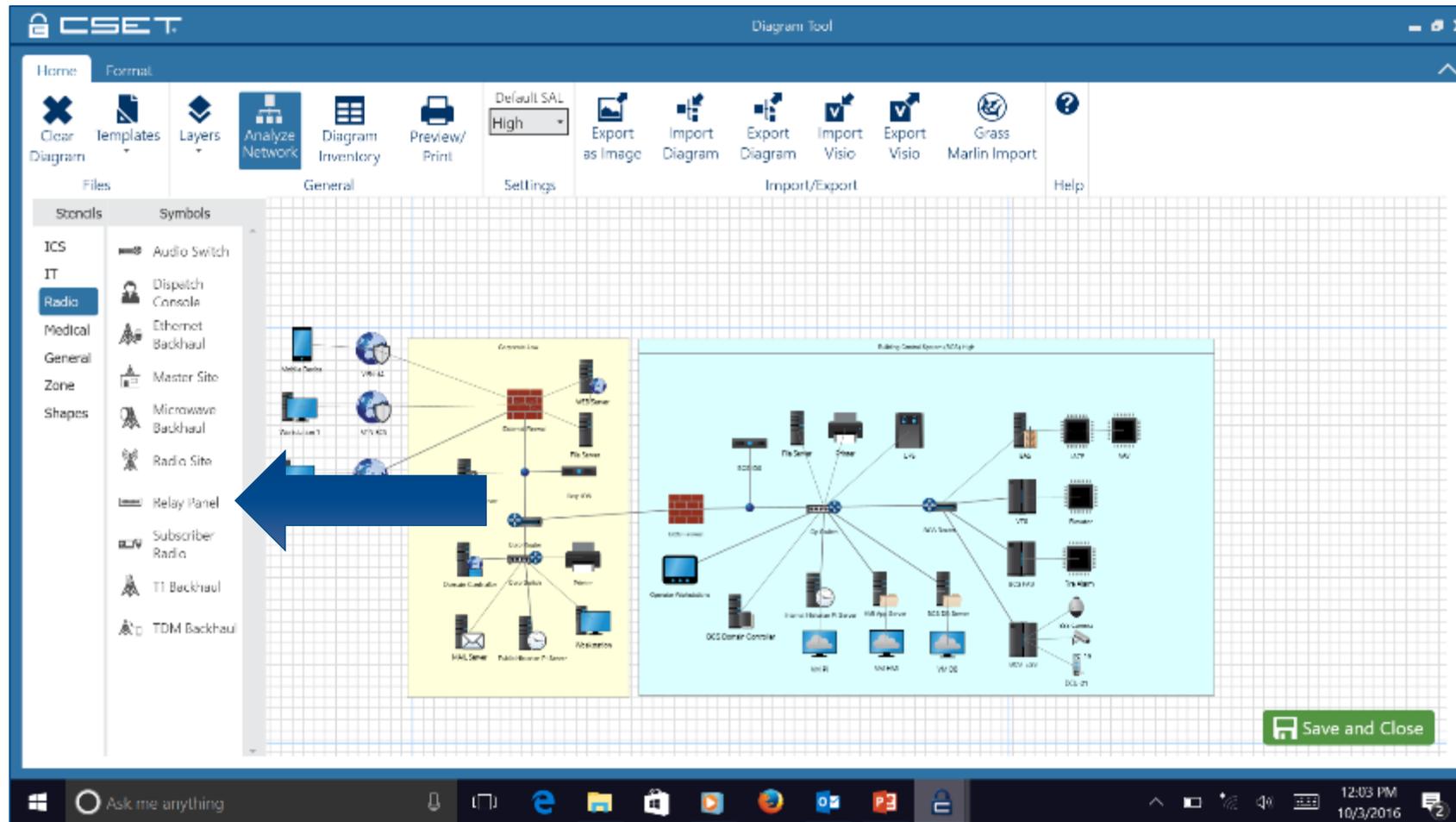
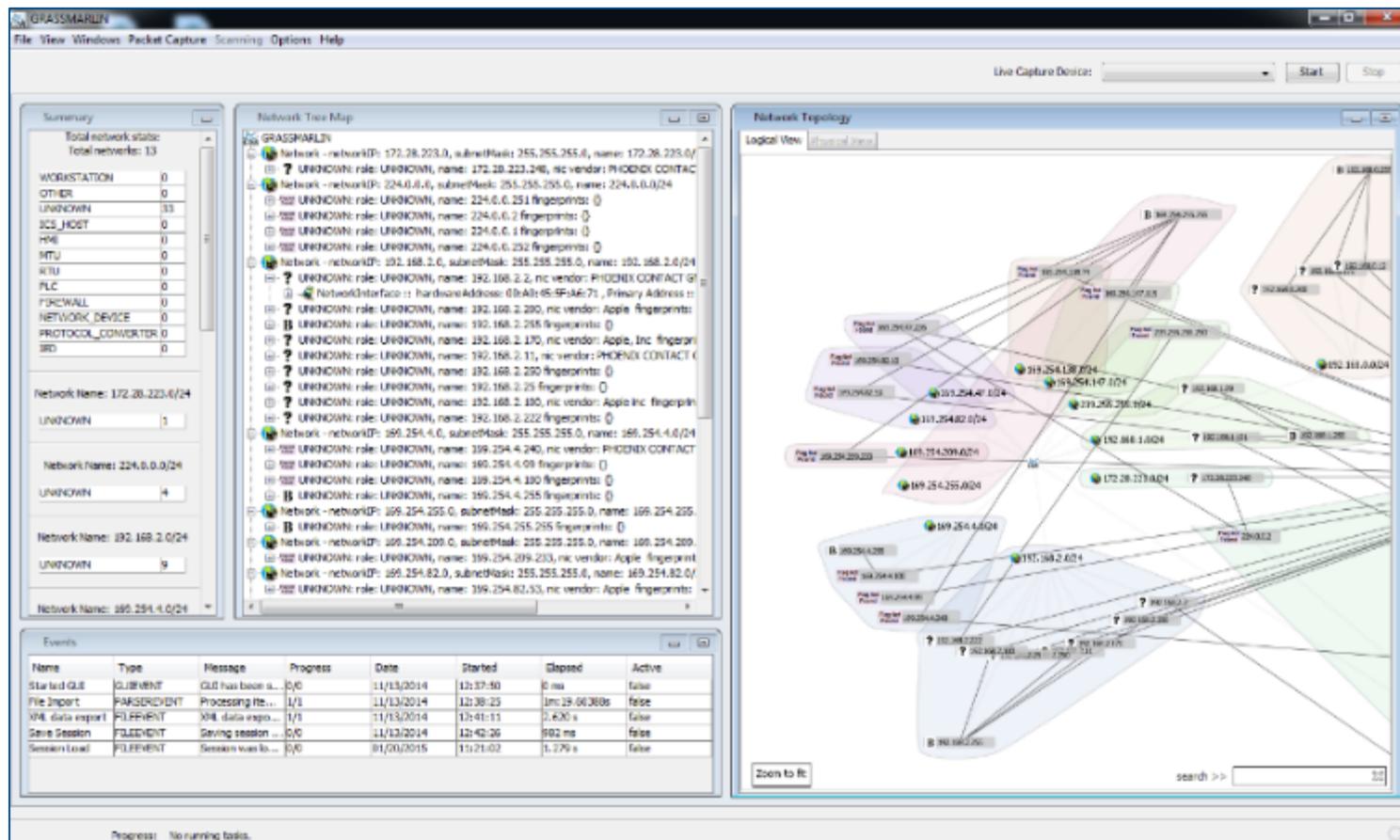


Diagram – Components



GrassMarlin Plug-In



Working with other products to get Visio import templates

Mode Selection

Local Installation

CSET Tools Resource Library Help LAPTOP-24CJSVDCnrcub

Prepare Questions Results

Cybersecurity Standards 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 information.

[I want to do a basic assessment instead.](#)

Requirements Questions 1081

Chemical, Oil, and Natural Gas

- CTATS Risk Based Performance Standards Guide 8 Cyber
- CIS Controls Version 8
- INSAV Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- TSA Pipeline Security Guidelines April 2011

DoDI and CNSSI

- CNSSI No. 1253 Baseline V2 March 27, 2014
- DoD Instruction 8510.01

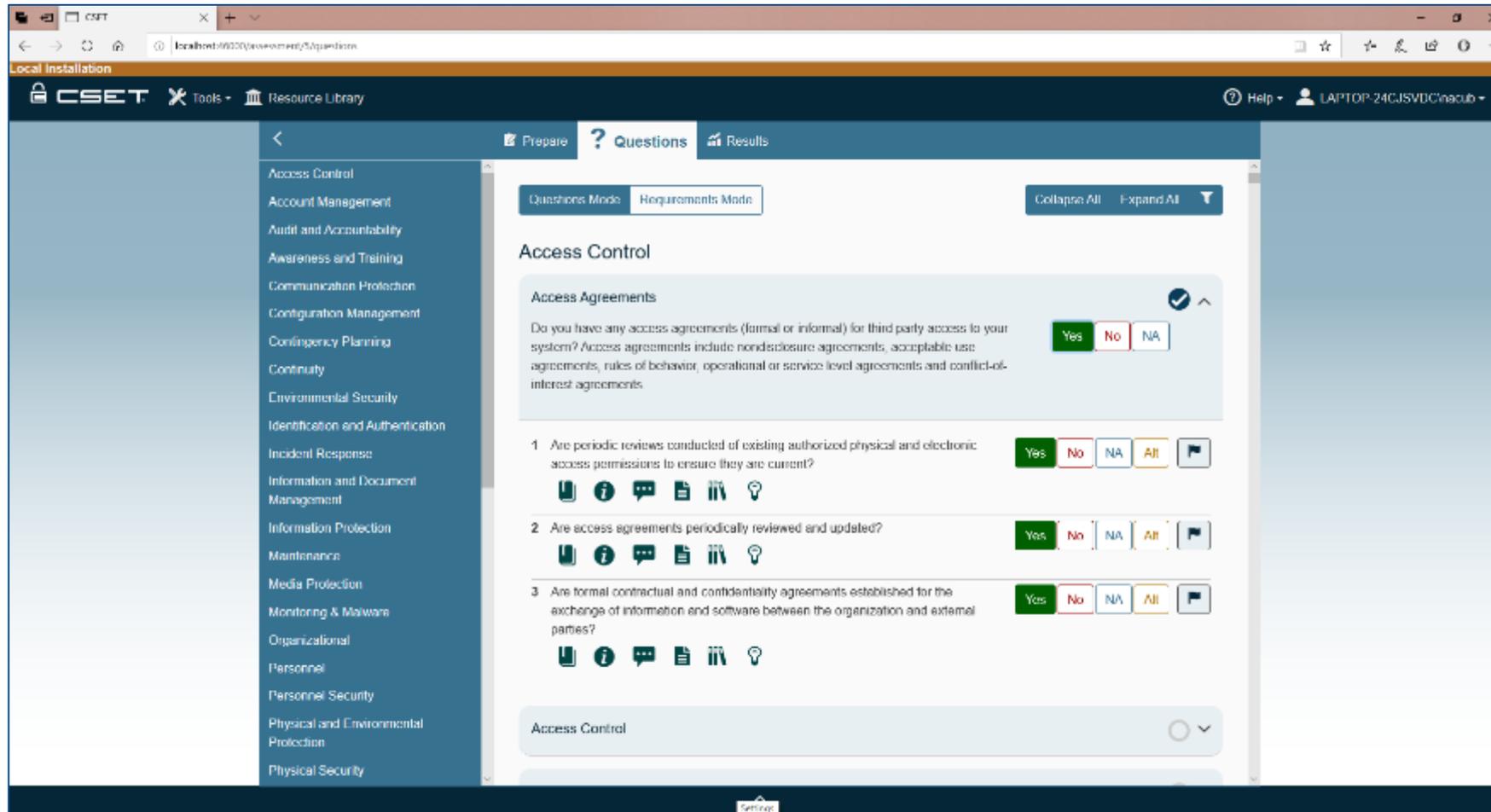
Electrical

- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NERC CIP 002 through CIP 011 Rev 5
- NERC CIP-002 through CIP-014 Rev 8
- NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol. 1
- NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol. 1 Rev 1

Financial

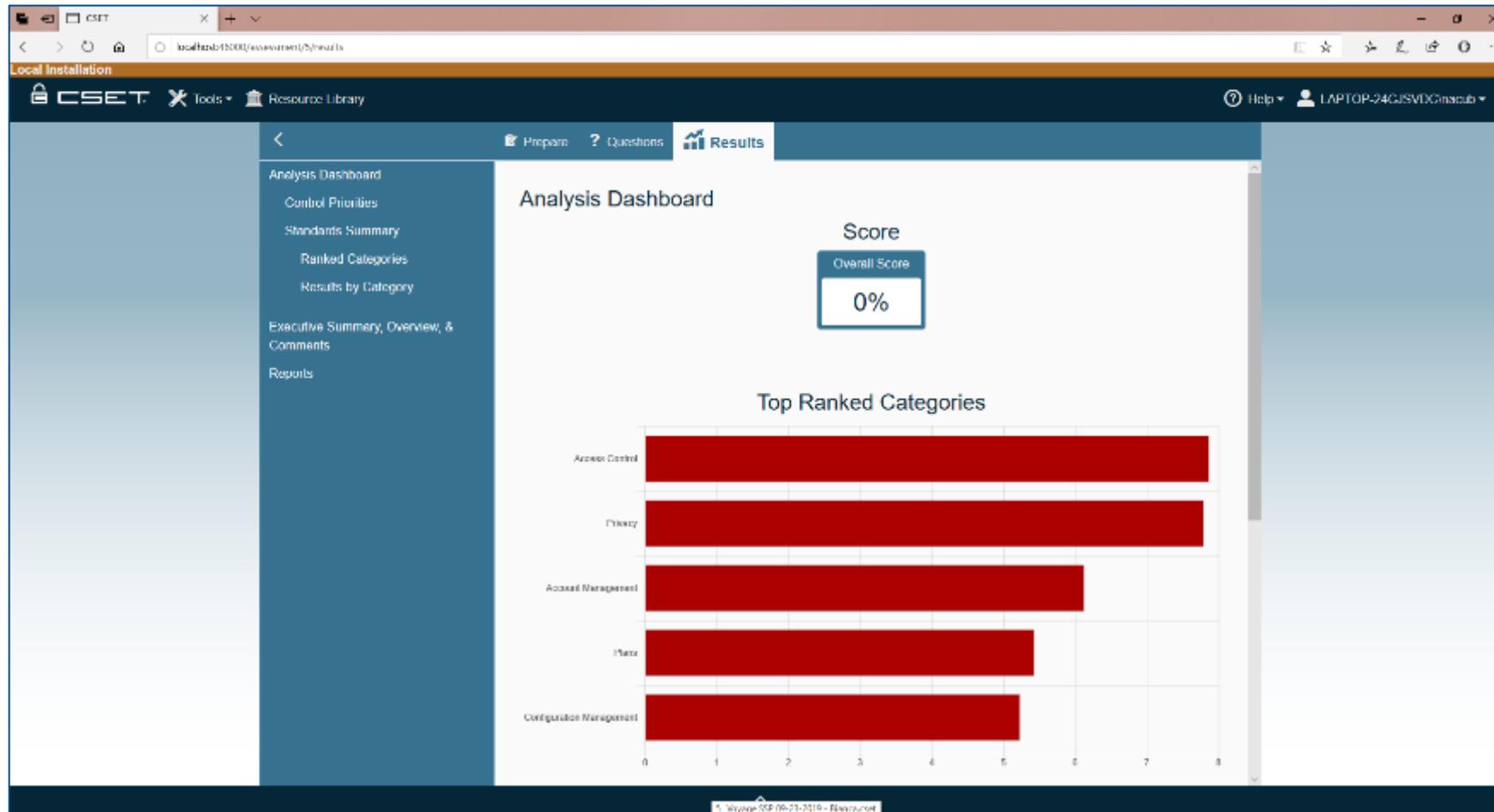
- Payment Card Industry (PCI) Data Security Standard

Questions – Family, Detail, Info



The screenshot displays the CSET assessment interface in a web browser. The browser address bar shows the URL `localhost:60300/assessment/5/questions`. The interface includes a navigation menu on the left with categories such as Access Control, Account Management, Audit and Accountability, Awareness and Training, Communication Protection, Configuration Management, Contingency Planning, Continuity, Environmental Security, Identification and Authentication, Incident Response, Information and Document Management, Information Protection, Maintenance, Media Protection, Monitoring & Malware, Organizational, Personnel, Personnel Security, Physical and Environmental Protection, and Physical Security. The main content area is titled 'Access Control' and features a 'Questions Mode' tab. It contains three questions with response buttons for 'Yes', 'No', 'NA', and 'All'. The first question is 'Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.' The second question is 'Are periodic reviews conducted of existing authorized physical and electronic access permissions to ensure they are current?'. The third question is 'Are access agreements periodically reviewed and updated?'. The fourth question is 'Are formal contractual and confidentiality agreements established for the exchange of information and software between the organization and external parties?'. The interface also includes a 'Collapse All' button and a 'Settings' icon at the bottom.

Analysis - Dashboard



Report Builder

localhost:49000/assessment/5/results/reports

Local Installation

CSET Tools Resource Library Help LAPTOP-24GJ5V1C Guest

Prepare Questions Results

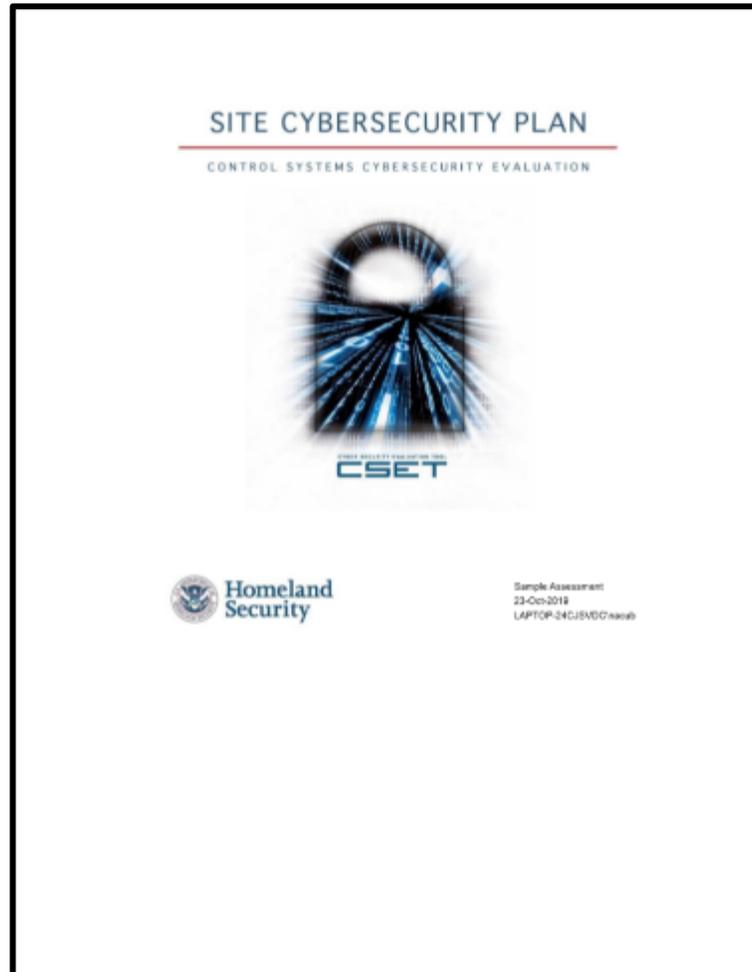
Report Builder

Create your final reports. You can add descriptions, comments, and an executive summary to your reports. You can also specify comments and descriptive text.

- Executive Summary
- Site Summary Report
- Site Cybersecurity Plan
- Site Detail Report
- Observations Test-Out Streets

Back

System Security Plan



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. It is recommended that a 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 (possibilities), and the cost of implementing mitigating controls.

Assets + vulnerability = asset value = total risk
threat risk - control measures = residual risk

Consequence

The examination of the consequences of an attack should include:

- How many people could sustain injuries requiring a hospital stay?
- How many people could be killed?
- What is the substantial cost of losing capital assets or the overall economic impact? (Consider the cost of site buildings, facilities, equipment, etc.)
- What is the substantial cost in terms of economic impact to both the site and surrounding communities? (Consider any losses to community structures and any costs associated with displacement.)
- What is the substantial cost of employee effort clean-up to the site and surrounding communities? (Consider the cost for cleanup, remediation, long term monitoring, etc.)

Threat

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

Cost Benefit Analysis

The cost of implementing controls will depend to the additional security provided to be the 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 each of these areas with respect to data and systems.

3.1.1 Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

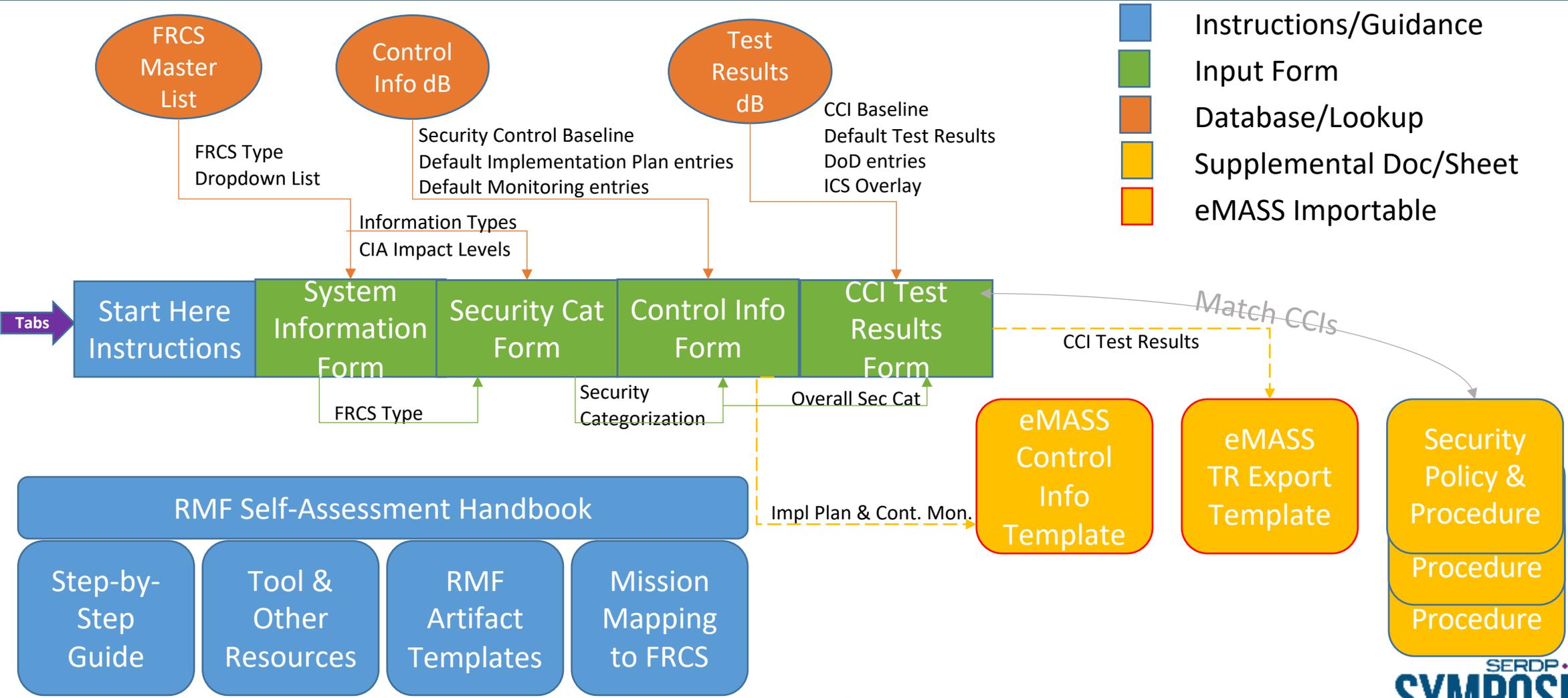
3.1.2 Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life cycle. This means that data cannot be modified in an unauthorized or unintended manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing. Integrity is violated when a message is subtly modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

3.1.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

ESTCP FRCS RMF Tool – Coming Soon!



ESTCP FRCS RMF Tool

Step 3
Implement Controls

CCI Test Results Form

Information Type Name (e.g., C.I.1.1, C.I.1.2, etc.)	Info Type Name	Description of How Information Type is Classified in System	Confidentiality Impact	Integrity Impact	Availability Impact
C.I.1.1	Confidential Information	...	Low	Low	Low
C.I.1.2	Restricted Information	...	Low	Low	Low
C.I.1.3	System and Network Management Information	...	Low	Low	Low
C.I.1.4	Non-System and Network Management Information	...	Low	Low	Low
C.I.1.5	Executive Personnel and Planning Information	...	Low	Low	Low
C.I.1.6	Personnel Information	...	Low	Low	Low
C.I.1.7	Financial Information	...	Low	Low	Low
C.I.1.8	Operational Information	...	Low	Low	Low
C.I.1.9	Logistics Information	...	Low	Low	Low
C.I.1.10	Legal Information	...	Low	Low	Low
C.I.1.11	Regulatory Information	...	Low	Low	Low
C.I.1.12	Proprietary Information	...	Low	Low	Low
C.I.1.13	Other Information	...	Low	Low	Low
OVERALL SYSTEM SECURITY CATEGORY			High	High	High

NIST 800-82
800-82 ICS
Overlay

DoD-level
Policies

UFC
4-010-

Control Number	Control Information	AP Acro	CCI	CCI Definition	Implementation Guidance	RECOMMENDED EVIDENCE	Design Conf	Col	Ass	o	l	e	Te	g	Te	Com	Date Tested	Tested By
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles); b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	AC-1.3	00001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	The organization being inspected/used develops and documents an access control policy that defines the purpose, scope, roles, responsibilities, management commitments, and authorized access.	1) Signed and dated copy of access control policy that defines the purpose, scope, roles, responsibilities, management commitments, and authorized access.	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles); b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	AC-1.4	00002	The organization reviews and updates the access control policy in accordance with the organization's information security program.	The organization being inspected/used reviews and updates the access control policy in accordance with the organization's information security program.	1) Signed and dated copy of access control policy. 2) Documentation/policy.	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles); b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	AC-1.7	00003	The organization reviews and updates the access control policy in accordance with the organization's information security program.	The organization being inspected/used reviews and updates the access control policy in accordance with the organization's information security program.	1) Signed and dated access control policy. 2) Documentation/policy.	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles); b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	AC-1.5	00004	The organization develops and documents procedures to facilitate the dissemination of information.	The organization being inspected/used develops and documents procedures to facilitate the dissemination of information.	1) Signed and dated access control policy. 2) Signed and dated documentation that defines the procedures that facilitate the dissemination of information.	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles); b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, management objectives, and authorized access.	AC-1.6	00005	The organization disseminates the access control policy to the organization's personnel and contractors.	The organization being inspected/used disseminates the access control policy to the organization's personnel and contractors.	1) Signed and dated access control policy. 2) Signed and dated documentation that defines the procedures that facilitate the dissemination of information.	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A	IN/A

eMASS
Import
of Test
Results

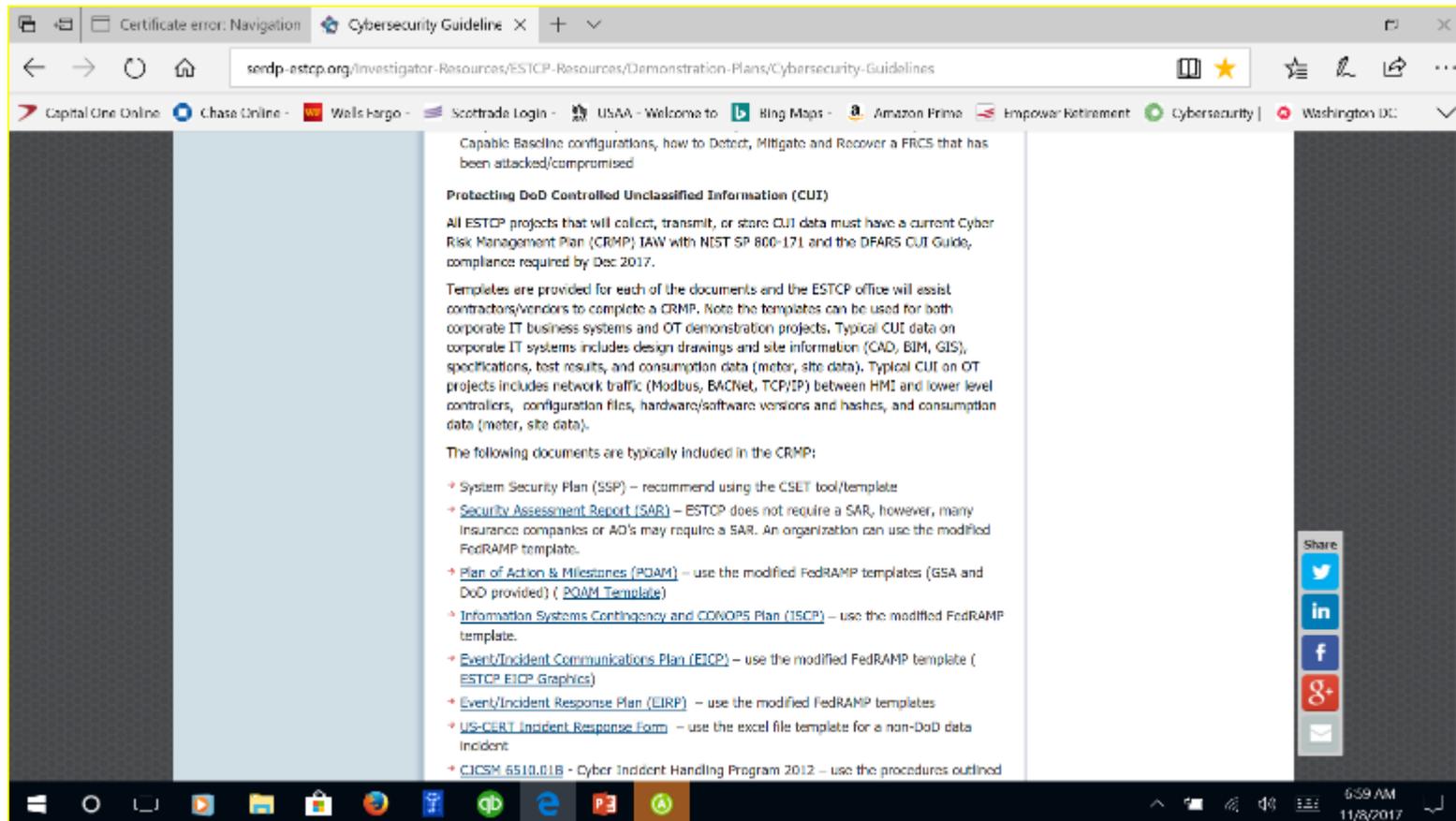
Test Result Export Form

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

Applying the RMF to Organization IT Systems: Protecting Controlled Unclassified Information (CUI)

Applying the RMF to Organization IT Systems - CUI

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



DFARS Guide 2015 Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement – This guidance is intended for stakeholders charged with protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s) covered by DFARS 252-204-7012 (Safeguarding Unclassified Controlled Technical Information).

Applying the RMF to Organization IT Systems - CUI

Protecting Controlled Unclassified Information

All ESTCP projects that will collect, transmit, or store CUI data must have a current Cyber Risk Management Plan (CRMP) IAW with NIST SP 800-171 and the DFARS CUI Guide, compliance required by Dec 2017. Templates are provided for each of the documents and the ESTCP office will assist contractors/vendors to complete a CRMP. **Note the templates can be used for both corporate IT business systems and OT demonstration projects.** Typical CUI data on corporate IT systems includes design drawings and site information (CAD, BIM, GIS), specifications, test results, and consumption data (meter, site data). Typical CUI on OT projects includes network traffic (Modbus, BACNet, TCP/IP) between HMI and lower level controllers, configuration files, hardware/software versions and hashes, and consumption data (meter, site data).

Protecting Controlled Unclassified Information (CUI)

The following documents are typically included in the CRMP and recommended sequence of completion:

- **Event/Incident Communications Plan (EICP)** – use the modified FedRAMP template and the ESTCP EICP Graphics
- **Event/Incident Response Plan (EIRP)** – use the modified FedRAMP templates
 - US-CERT Incident Response Form – use the excel file template for a non-DoD data incident
 - CJCSM 6510.01B - Cyber Incident Handling Program 2012 – use the procedures outlined in the manual
 - DFARS Incident Response Form – use the excel file template for a DoD data incident and the DBNet portal
- **Information Systems Contingency and CONOPS Plan (ISCP)** – use the modified FedRAMP template.
- **Security Audit Plan (SAP)** – use the modified NIST template
- **System Security Plan (SSP)** – recommend using the CSET tool/template NIST SP 800-171
- **Security Assessment Report (SAR)** – ESTCP does not require a SAR, however, many insurance companies or AO's may require a SAR. An organization can use the modified FedRAMP template.
- **Plan of Action & Milestones (POAM)** – use the modified FedRAMP templates (GSA and DoD provided)

Protecting Controlled Unclassified Information (CUI)

DFARS Guide 2015 Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement – This guidance is intended for stakeholders charged with protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s) covered by DFARS 252-204-7012 (Safeguarding Unclassified Controlled Technical Information). CTI is technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This guide will assist stakeholders in carrying out their responsibilities should a defense contractor report a compromise on a contract that contains unclassified CTI.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting – This is the DFARS Contract clause an investigator should look for in their contract/subcontract. If the ESTCP contract does not include this clause, contact the ESTCP office so a modification can be issued.

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations - The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

DIBNet Portal to Report Cyber CUI Incidents (CAC Required)

The screenshot shows a web browser window with the URL <https://dibnet.dod.mil/portal/intranet/>. The page title is "Welcome to the DIBNet portal" and the subtitle is "DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program." The page is divided into two main sections:

- Cyber Reports:** This section includes a "Report a Cyber Incident" button and lists reporting requirements such as "A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report." It also lists specific FAR regulations: FAR 252.204-7012, FAR 252.239-7010, FAR 52.204-23, and FAR 52.204-25.
- DoD's DIB Cybersecurity (CS) Program:** This section includes an "Apply Now!" button and a "Voluntary Report" button. It describes the program as a voluntary public-private cybersecurity partnership.

Both sections provide contact information for assistance, including email addresses (DCISE@dc3.mil, OSD.DIBCSIA@mail.mil) and phone numbers (Hotline: (410) 981-0104, Toll Free: (855) DoD-IACS, Fax: (571) 372-5434).

<https://dibnet.dod.mil/portal/intranet/>

102

DFARS Incident Reporting Form (72 Hours)

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident.

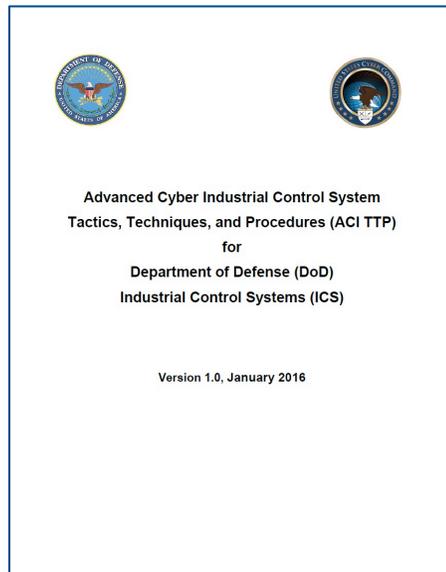
The screenshot shows a Microsoft Excel spreadsheet titled "DFARS CUI Cyber Incident Reporting Form 11-08-2017". The spreadsheet is a template for an incident collection format (ICF) and contains the following items:

- 4.3.3 APPENDIX F. INCIDENT COLLECTION FORMAT (ICF) TEMPLATE
- 1.) UNCLASSIFIED//FOR OFFICIAL USE ONLY (when filled in)
- 2.) FOR INTERNAL USE ONLY
- 3.) Report ID: xxx-xxxxx
- 4.) Company Name: xxxxxx
- 5.) DUNS Number: xxxxxx
- 6.) Contract Number Affected (Additional contract numbers can be added on a subsequent page): xxxxxx-xx-x-xxxx
- 7.) Contract Clearance Level: xxxxxx
- 8.) Facility CAGE Code: xxxxxx
- 9.) Does this incident affect cloud services provided to DoD?: xx
- 10.) Does this incident impact unclassified controlled technical information as defined in DFARS clause 252.204-7012?: xxx
- 11.) Last Name: Xxxxxxx
- 12.) First Name: Xxxxxxx
- 13.) Position/Title: xxxxxxxxxxxx
- 14.) Location: xxxxxxxxxxxxxxxxx
- 15.) City: xxxxxxxxxxxx
- 16.) State: xxxxxxxxxxxxxxxxx
- 17.) Postal Code: xxxxxx
- 18.) Telephone: xxx-xxx-xxxx
- 19.1 E-mail Address: xxxxxxxx.xxxxxx@xxxxxx-xxxx

Advanced Control Systems Tactics, Techniques and Procedures: Detecting, Mitigating, Recovering and Reporting Events/Incidents

ACT TTP for DoD ICS

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



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)

ACT TTP for DoD ICS

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

Information Technology (IT) Systems – Organization, 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), MS Sysinternals, OS Forensics, Malwarebytes, Kali, Control Things I/O, etc.

- Segment and VLAN organization IT and FRCS OT demonstration 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
- Practice with the TTP's

All PI's/Project Teams will need to have a Table-Top exercise and use the EICP and EIRP as a DFARS incident (use the DFARS IR form), include an email with DFARS Exercise/Exercise/Exercise [ORGANIZATION NAME] with a cc copy to the ESCTP office

ACI TTP Threat-Response Procedures

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

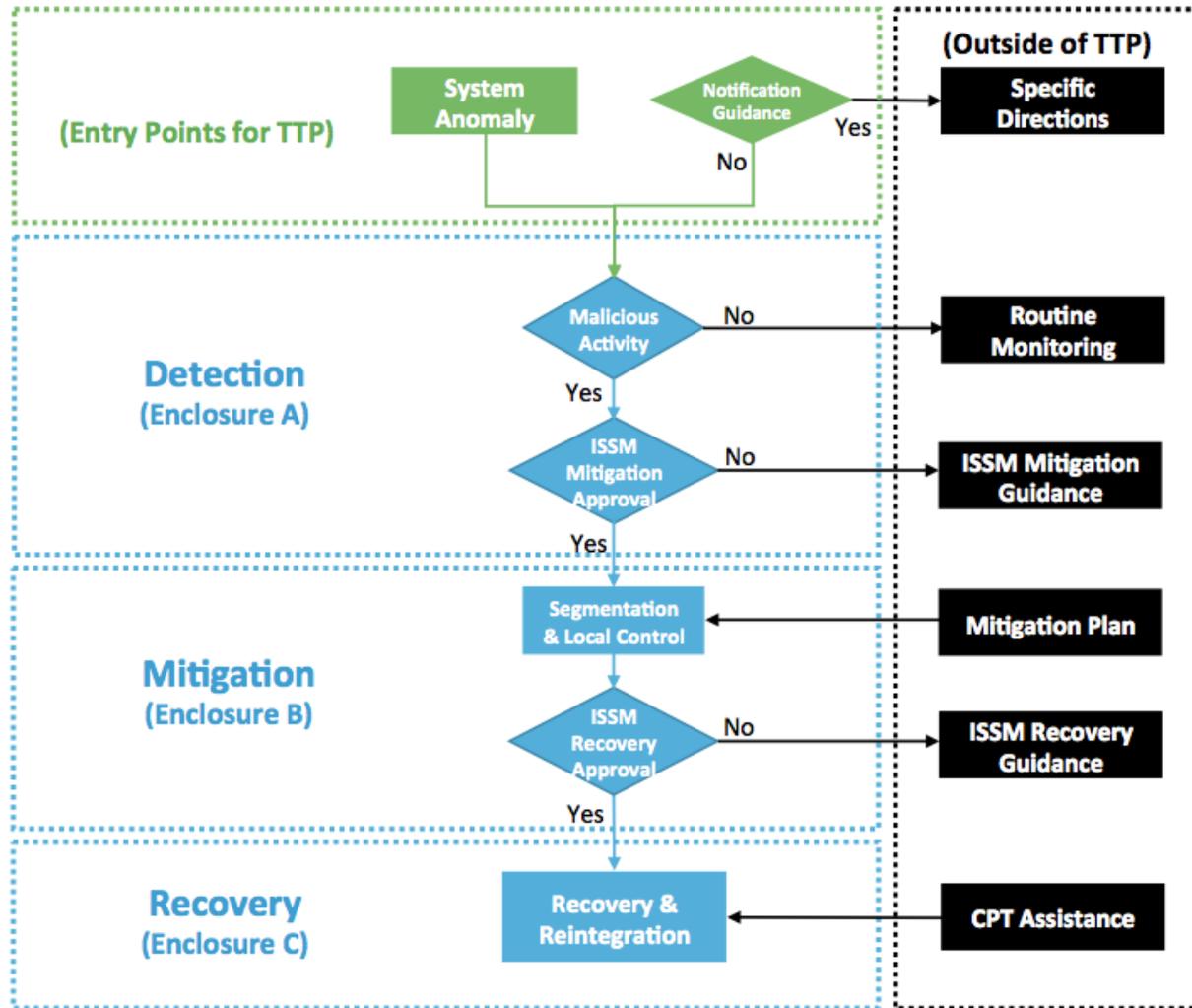
Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general 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.

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.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.1. 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.1. 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

FRCS Cybersecurity Guidance with the TTP's

Activity / Lead	New Project	Renovation Project	Typical Duration
Conduct testing on initial build Lead: construction/system integrator Documents/Models/Tools: <ul style="list-style-type: none"> • Kali Linux • SamuraiSTFU 	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	2 – 4 weeks
Construction - conduct pilot implementation deployment Lead: construction/system integrator Documents/Models/Tools: <ul style="list-style-type: none"> • Kali Linux • SamuraiSTFU • OIT IT Repository • Penetration Testing Scope, ROE, Checklist (if required) • Jump-Kit Rescue CD 	Pilot implementation of FRCS solution on a small subset of user base to evaluate solution against real-world requirements. Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Varies with size of deployment (number of facilities and interconnections)

Design and Construction Sequence TTP Jump-Kit Rescue CD

ENCLOSURE A: DETECTION PROCEDURES

A01177

ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostic Table			
Section	Event	Description	Page
Notification			
A.2.1	Unauthorized Access	Cyber event, not caused by a failure of a ICS, including USCYBERCOM, ICS-CERT, or the command structure	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any form, server or workstation, including SCADA equipment, that includes events and logs on: 1. Unusual or frequent logins 2. Rapid or too consecutive logins 3. User logging into accounts outside of normal working hours 4. Unusual or failed logins attempts 5. User accounts attempting to acquire access privileges	A-6
A.2.3	Irregular Process Found	On any computer based device, workstation, including SCADA equipment, an irregular process was found	A-7
A.2.4	Suspicious Software/Configurations	SCADA software under configuration was detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (Or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the log being written, slow or time based of occurrence, data or time being missing from an entry, unusual changes, rapid security event losses, or log file corruption	A-9
A.2.6	Unusual System Behavior	Any ICS, including SCADA equipment: 1. Unexplained reboot or system power change. 2. Unusually slow performance or unusually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Unexplained loss of user or system. 5. Unusually rapid device or system security event loss or system shutdown in operating systems. 6. Configuration changes to software made without user or system administrator. 7. System unresponsive.	A-10
A.2.7	Asset Is Scanning Other Network Assets	Hardware or software (H/W, S/W) operating and connecting (O/C) for protocol control (O/C) or operational system (O/S) to scan or connect to a network asset identified in the ICS data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

Enclosure A: Detection Procedures A-1

Notification

A.2.1 Notifications

Server/Workstation Anomalies

A.2. Event Diagnostic Procedures

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

A.2.3 Server/Workstation: Irregular Process Found

A.2.4 Server/Workstation: Suspicious Software/Configurations

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

A.2.6 Server/Workstation: Unusual System Behavior

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

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

DETECTION PROCEDURES SERVER EXAMPLE 1

A.1.1 Event Diagnostics Table			
Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log-ins/log-outs. 3. Users logging into accounts outside of normal working hours. 4. Numerous failed log-in attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment. 1. Spontaneous reboots or screen saver change. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

DETECTION PROCEDURES SERVER EXAMPLE 1

A.2.3 Server/Workstation: Irregular Process Found	
<ul style="list-style-type: none">• Functional Area: IT or ICS• Description: On any computer-based server, workstation, including SCADA equipment, an irregular process was found	
Step	Procedures
Investigation	<ol style="list-style-type: none">1. DETERMINE if the new process belongs to an authorized installation:<ol style="list-style-type: none">a. New software was installed on to the system?b. Was maintenance performed on the system, and if the new process was installed during that maintenance?c. Is the new process a result of a patch update?
No Action Required	<ol style="list-style-type: none">2. If the new process belongs to an authorized installation:<ol style="list-style-type: none">a. DOCUMENT the Severity Level as None (0) in the Security Log.b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none">3. If the new process does not belong to an authorized installation:<ol style="list-style-type: none">a. DOCUMENT in Security Log.b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check associated with server or workstation you are investigating and EXECUTE the Integrity checks. Recommended Checks:<ul style="list-style-type: none">A.3.2.1 Server/Workstation Process CheckA.3.2.2 Server/Workstation Log ReviewA.3.2.4 Server/Workstation Communications CheckA.3.2.16 Peripherals Integrity CheckA.3.2.9 Controller Integrity CheckA.3.2.13 Server/Workstation Rootkit Check4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

DETECTION PROCEDURES SERVER EXAMPLE 1

A.3.2.1 Server/Workstation Process Check	
<ul style="list-style-type: none">• Who should do this check: The organization or individual responsible for the server or workstation• What is needed for this check:<ol style="list-style-type: none">1. FMC data flow chart2. FMC baseline topology3. FMC baseline authorized process and tasks4. FMC baseline software list5. FMC baseline system information	
Step	Procedures
1.	If the machine is responsive , EXECUTE steps a and b below. Once completed, RETURN to this section, and resume with Step 2. <ol style="list-style-type: none">a. Section: A.3.2.2 Server/Workstation Log Review.b. Section: A.3.2.3 Unauthorized User Account Activity. If the machine is not responsive , GO TO Section A.3.2.5 <i>Server/Workstation Unresponsive Check</i> .
2.	If Procedures A.3.2.2 or A.3.2.3 do not result in a Severity Level of High (3) , CONTINUE to step 3.
3.	Process Check: LAUNCH SysInternals: CHECK for processes that do not appear legitimate. This can include (but is not limited to) processes that: <ol style="list-style-type: none">a. Have no icon or name.b. Have no descriptive or company name.c. Are unsigned Microsoft images.d. Reside in the Windows directory.e. Include strange uniform resource locators (URLs) in their strings.f. Communicating with unknown IP address (use FMC data flow diagram to compare).g. Host suspicious dynamic link library (DLL) or services (hiding as a DLL instead of a process).h. LOOK for "packed" processes which are highlighted in purple.
4.	If an anomalous process was found: <ol style="list-style-type: none">a. DOCUMENT details of the event in Security Log.b. CONTACT system administrator responsible for the machine or the command ISSM.<ol style="list-style-type: none">(1) REPORT suspicious process.(2) REQUEST assistance in determining if the process is malicious (process may be undocumented but normal).(3) If the process is not malicious, DOCUMENT in Security Log, and EXECUTE A.3.2.4 Server/Workstation Communications Check.(4) If the process is malicious, DOCUMENT the Severity Level of High (3) in the Security log.c. GO TO section A.2.29 Action Step.
5.	If an anomalous process was not found: <ol style="list-style-type: none">a. DOCUMENT the Severity Level as None (0).b. RETURN to the previous diagnostic procedure and continue with <i>Recommended Checks</i>.

DETECTION PROCEDURES SERVER EXAMPLE 1

Process Explorer - Sysinternals: www.sysinternals.com [T9\T7]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description
svchost.exe	< 0.01	2,584 K	8,832 K	1688	Host Pr...
audodg.exe	1.51	21,448 K	24,448 K	3932	
svchost.exe		4,196 K	13,264 K	1778	Host Pr...
svchost.exe		5,124 K	15,368 K	1904	Host Pr...
wlanext.exe		4,632 K	16,060 K	3544	
conhost.exe		1,120 K	4,804 K	3552	
spoolsv.exe	< 0.01	15,188 K	28,192 K	1988	Spooler
QBCFMonitorService.exe		10,616 K	15,872 K	2156	QuickB...
EvtEng.exe	< 0.01	4,436 K	13,204 K	2208	Inter(R)
OASFramework15.exe	0.24	18,180 K	20,500 K	2218	OAS Fr...
lsisrv.exe		358 K	4,016 K	2240	Inter(R)
OPCSysData.exe	0.07	29,132 K	24,536 K	2294	OPCSy...
mbamservice.exe	0.02	454,172 K	225,048 K	2292	Malwar...
mbam.exe	0.15	34,588 K	59,540 K	5880	
mbamscheduler.exe		5,064 K	12,184 K	2300	Malwar...
ZeroConfigService.exe		4,644 K	16,976 K	2312	Inter(R)
vmtoolsd.exe	< 0.01	1,712 K	6,514 K	2324	VMware
vmtoolsd.hcp.exe		7,344 K	4,528 K	2332	VMware
svchost.exe		7,084 K	19,000 K	2340	Host Pr...
vmware-authd.exe		4,724 K	11,432 K	2408	VMware
vmtoolsd.vtoolsd.exe	< 0.01	2,312 K	9,508 K	2416	VMware
sqlwriter.exe		1,512 K	7,336 K	2452	SQL S...
svchost.exe		2,912 K	9,000 K	2460	Host Pr...
QBIDPService.exe		8,812 K	14,364 K	2492	QBIDP...
MsmqEng.exe	0.07	163,076 K	123,112 K	2504	Antimal...
OPCSysDatabase.exe	0.49	28,140 K	25,840 K	2580	OPCSy...
RegSvc.exe		1,738 K	8,648 K	2598	Inter(R)
svchost.exe		10,084 K	29,260 K	2620	Host Pr...
FMF_NSWI_SV.exe	< 0.01	1,484 K	19,700 K	2780	Fasym...
svchost.exe		5,296 K	14,004 K	4268	Host Pr...
NisSrv.exe		11,782 K	8,880 K	5092	Microso...
svchost.exe		6,682 K	25,952 K	5756	Host Process for Windows S...
PresentationFontCache.exe		26,112 K	19,372 K	5948	PresentationFontCache.exe
ePowerSvc.exe		2,288 K	9,436 K	2588	ePowerSvc
ePowerTray.exe	0.08	3,012 K	12,880 K	5324	ePowerTray
ePowerFront.exe	0.08	16,588 K	23,848 K	1192	

System Information

Summary CPU Memory I/O GPU

System Commit: 4.9 GB

Physical Memory: 4.4 GB

Commit Charge (K)	Kernel Memory (K)	Paging Lists (K)
Current: 5,161,148	Paged WS: 524,532	Zeroed: 160,132
Limit: 14,346,844	Paged Virtual: 557,268	Free: 20
Peak: 5,812,196	Paged Limit: no symbols	Modified: 112,956
Peak/Limit: 40.51%	Nonpaged: 282,960	ModifiedNoWrite: 0
Current/Limit: 35.97%	Nonpaged Limit: no symbols	Standby: 7,702,368

Physical Memory (K)

Physical Memory (K)	Paging
Total: 12,446,300	Page Fault Delta: 2,157
Available: 7,867,520	Page Read Delta: 0
Cache WS: 0	Paging File Write Delta: 0
Kernel WS: 0	Mapped File Write Delta: 0
Driver WS: 32,764	

System Information OK

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

Ask me anything 2:01 PM 8/29/2016

ENCLOSURE I: CYBER SEVERITY LEVELS



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6
DISTRIBUTION: A, B, C, JEL, S

CJCSM 6510.01B
10 July 2012

CYBER INCIDENT HANDLING PROGRAM

References: See Enclosure H.

- Purpose.** This manual describes the Department of Defense (DoD) Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions.
- Cancellation.** CJCSM 6510.01A, 24 June 2009, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)," is canceled.
- Applicability.** This manual applies to the Joint Staff and to Combatant Commands, Services, Defense agencies, DoD field activities, and joint and combatant activities (hereafter referred to as CC/S/A/FAs).
- Procedures.** See Enclosures A through G.
- Summary of Changes**
 - Updates manual to include the new mission, processes, and procedures of U.S. Cyber Command (USCYBERCOM), the subunified command of U.S. Strategic Command (USSTRATCOM).
 - Updates manual based on Unified Command Plan (UCP) Change 1, 12 September 2011.
- Releasability.** This manual is approved for public release; distribution is unlimited. DoD components (to include the Combatant Commands), other federal agencies, and the public may obtain copies of this manual through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

CJCSM 6510.01B CYBER INCIDENT HANDLING PROGRAM
(3) This enclosure provides requirements and methodology for establishing, operating, and maintaining a robust DoD cyber incident handling capability for routine response to events and incidents within the Department of Defense. Additional guidance for cyber incident handling for a crisis or in case of active hostilities will be issued by USCYBERCOM as required.

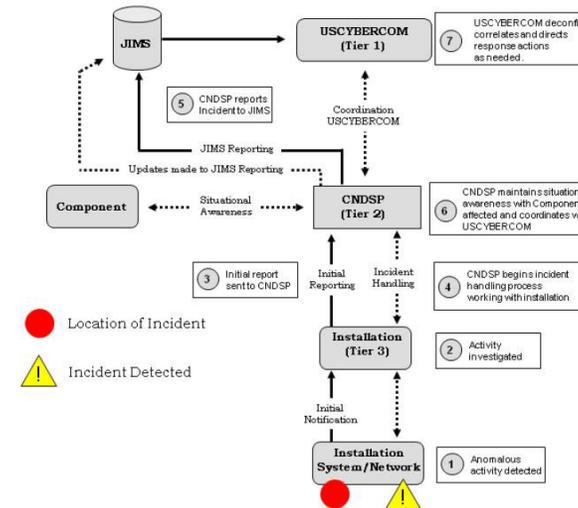


Figure C-C-2. Cyber Event Detected by Installation

ENCLOSURE I: CYBER SEVERITY LEVELS

I.2. Cyber Severity Levels Overview

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

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

Table I-1: Incident Severity Levels

ENCLOSURE I: CYBER SEVERITY LEVELS

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

Table I-3: Malicious Actions Table

The ESTCP EIRP has the CYBERCOM forms

BLUF: ESTCP will provide SME's to assist the PI's/Project Teams complete RMF packages!!

Open discussion, Lessons Learned, Best Practices

QUESTIONS



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