Short Course - DoD Risk Management Framework (RMF) and Steps to Obtain Authority To Operate (ATO)

Michael Chipley PhD GICSP PMP LEED AP

ESTCP Cyber Support SME

December 2, 2021

3:00pm-4:30pm

SERDP • ESTCP SYMPOSIUM

2021 • Enhancing DoD's Mission Effectiveness

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

1500-1510 Why is the RMF Important for ESTCP Projects: Shodan Exploit Demo of Control Systems

1510-1520 Overview of the 6 Steps of the RMF for both IT and OT Systems

1520-1525 Introduction of Services and Agencies FRCS POC's, variations in ATO/eMASS procedures

1525-1530 Applying the RMF to ESTCP Demonstration Projects: Key Documents Needed to Get an ATO for an OT System

1530-1540 Defining the Platform Enclave and Authorization Boundary, Creating a Test and Development Environment, Continuous Monitoring/Auditing

1540-1550 Applying the RMF to Organization IT Systems: Protecting Controlled Unclassified Information & Cybersecurity Maturity Model Certification

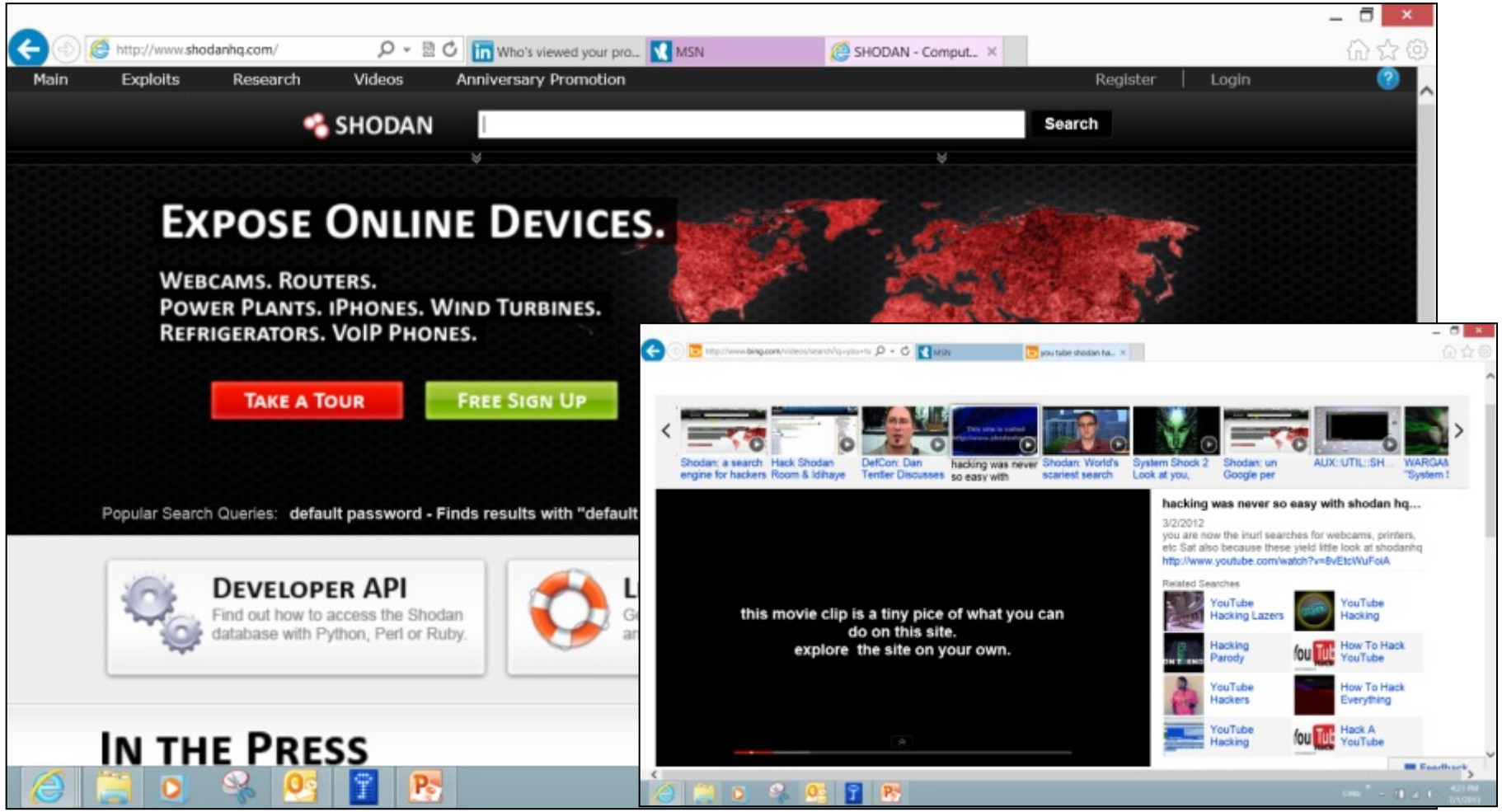
1550-1555 Advanced Control Systems Tactics, Techniques and Procedures: Detecting, Mitigating, Recovering and Reporting Events/Incidents

1555-1600 Open discussion, Lessons Learned, Best Practices

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

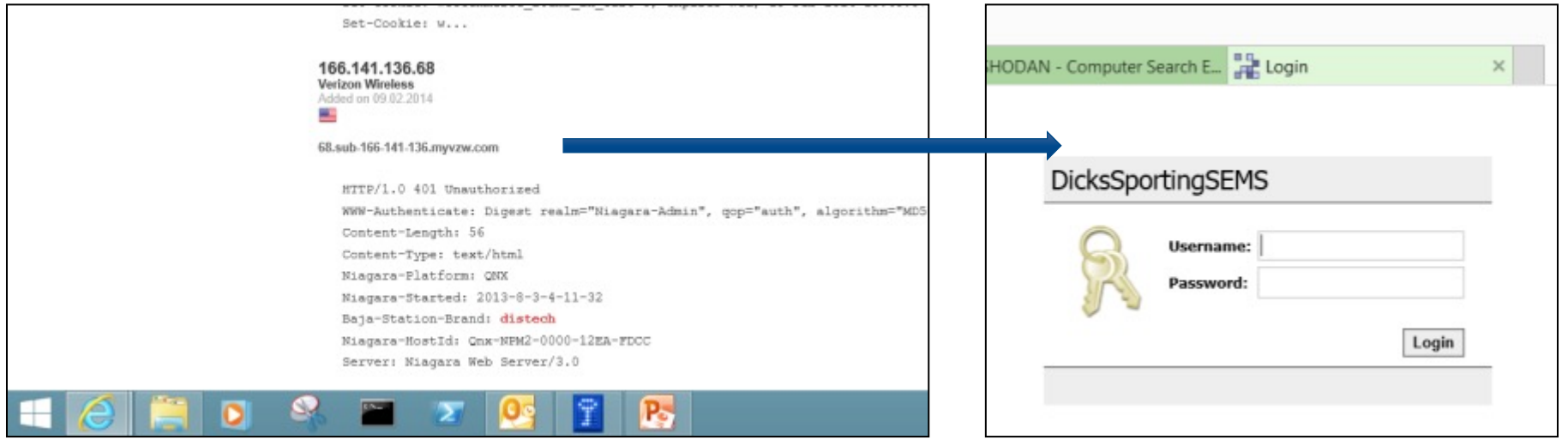
OT IP Based Controllers Are in Everything

Shodan



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

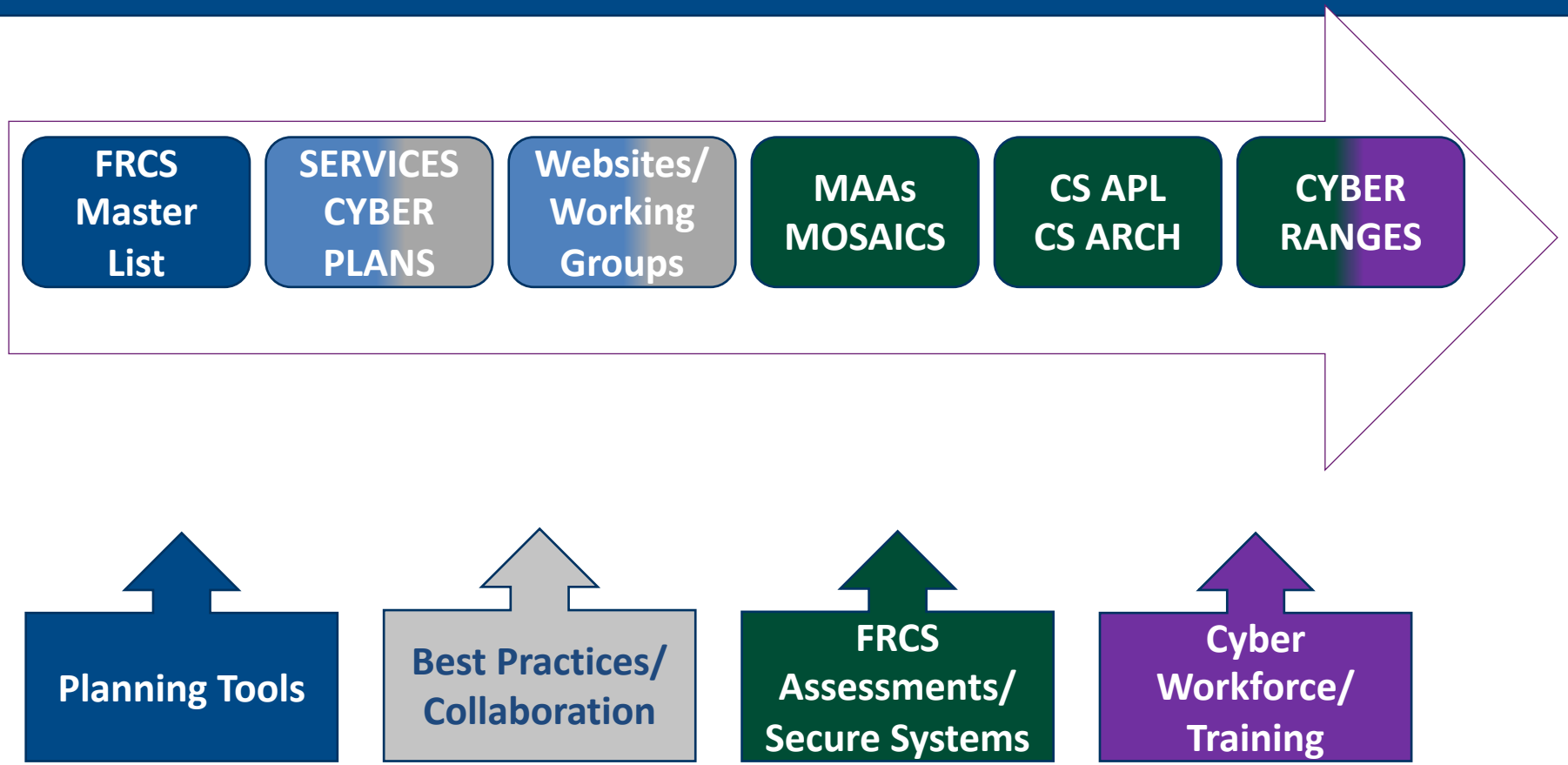
Shodan – Distech Search



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**

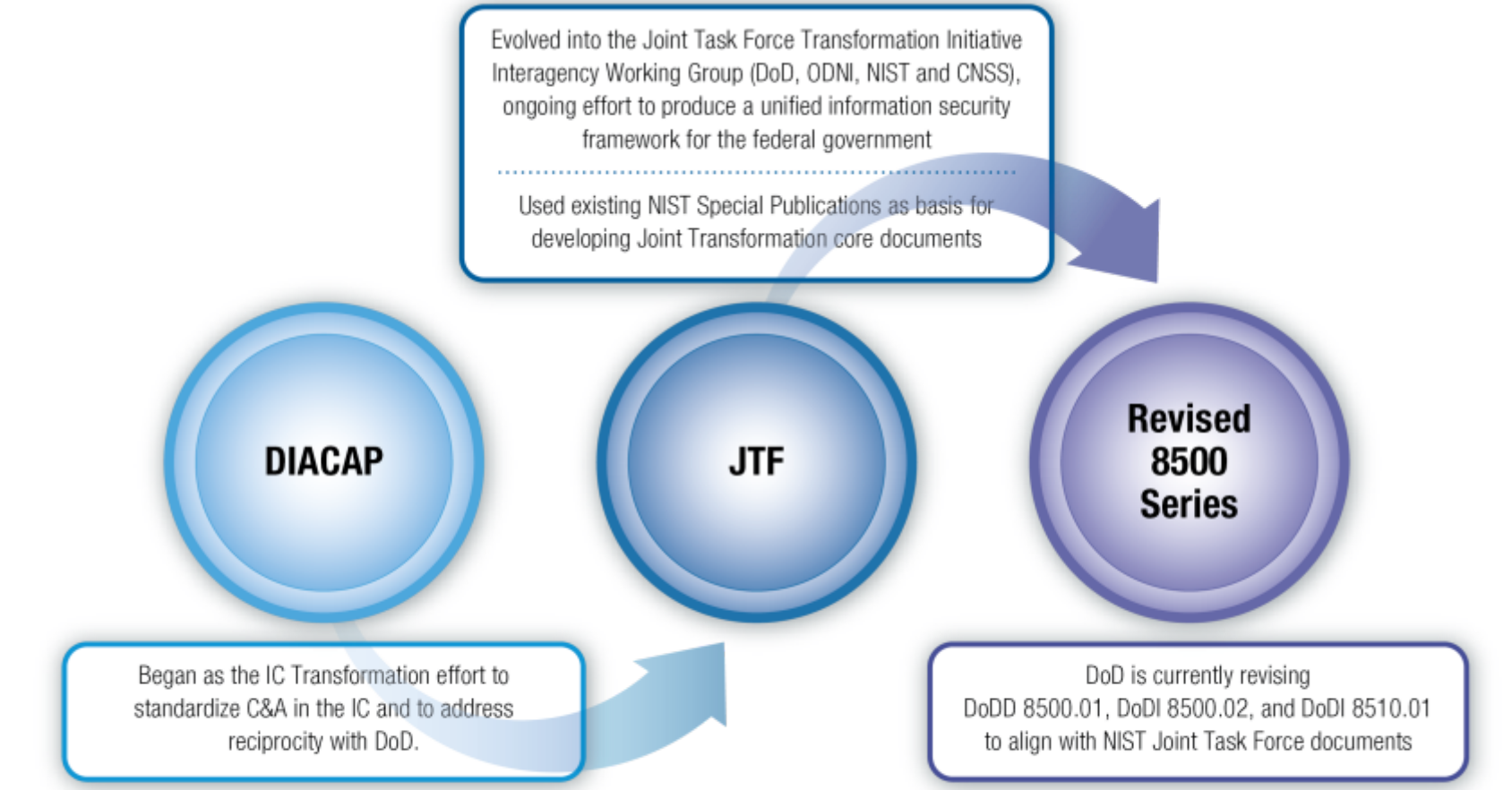
Overview of the 6 Steps of the RMF for both IT and OT Systems

ODASD(E) Cybersecurity Initiatives



Alignment with Federal, Industry Objectives

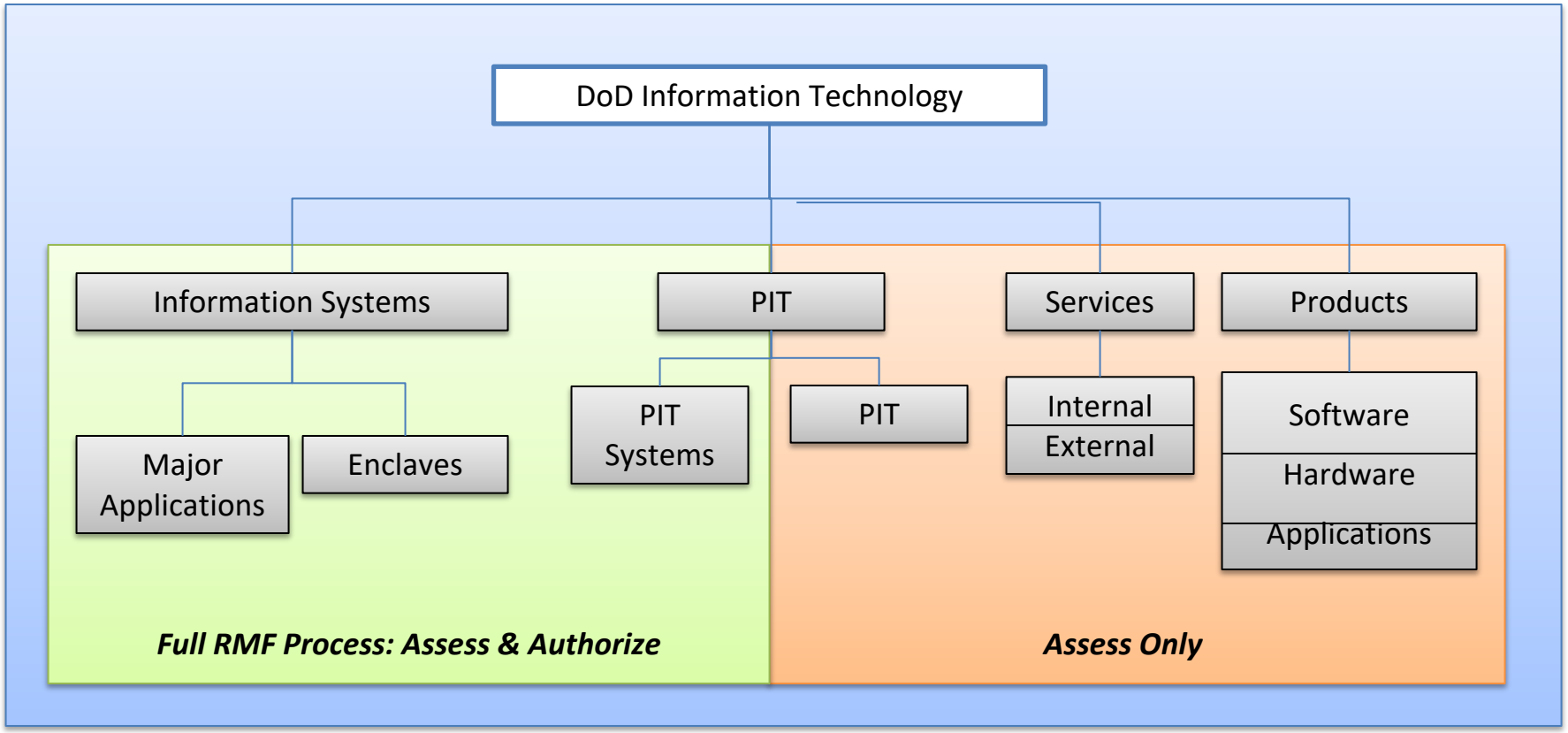
DoDI 8500.01 and 8510.01 Update



Transition Bottom Line – DoD will continue to follow the DoD 8500 series documentation for information assurance and risk management processes, procedures, and guidance

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

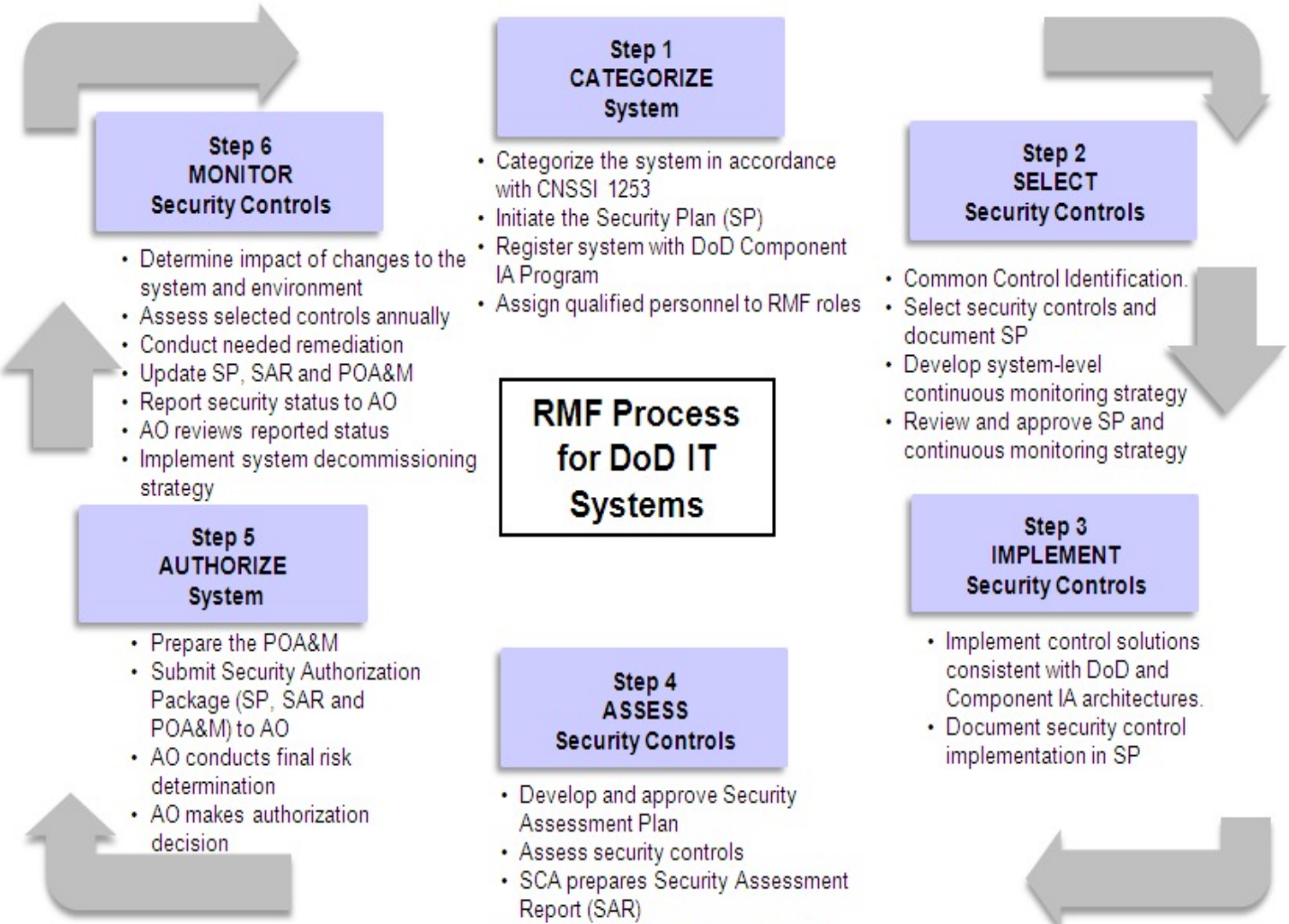
Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a **collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support.** PIT systems must be designated as such by the responsible 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

HBSS and Passive*

eMASS ATO's



CSET
FRCS
Overlay
ESTCP
RMF Tool

DoD Facility-Related Control Systems (FRCS)

Categories


Airfield Systems


Building Control System


Dam, Lock and Levee Systems


Electronic Security Systems


Environmental Monitoring


Fire & Life Safety

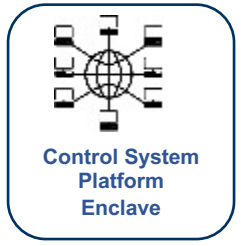

Pier Systems


Traffic Control Systems


Transportation & Fueling Systems


Utility Control Systems


Utility Monitoring & Control Systems


Control System Platform Enclave

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?

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

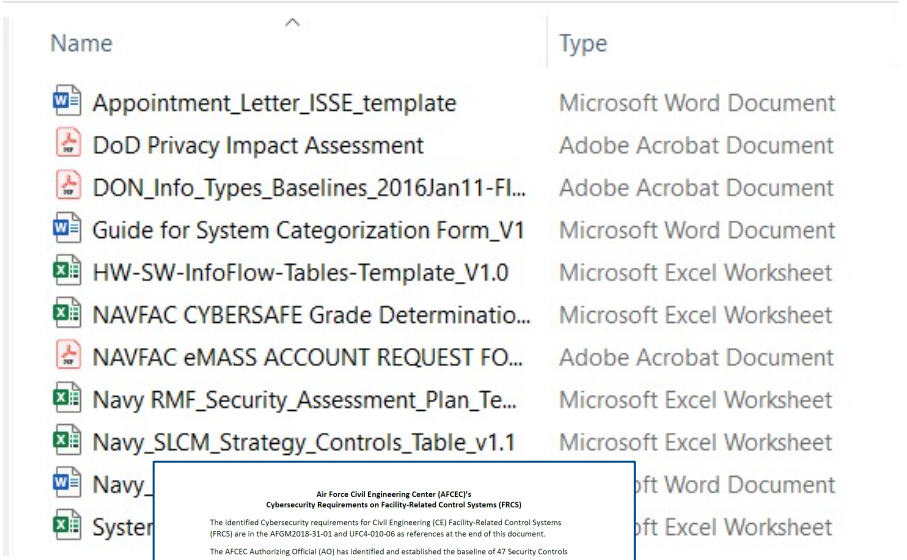
Army/IMCOM/ACTSIM/USACE

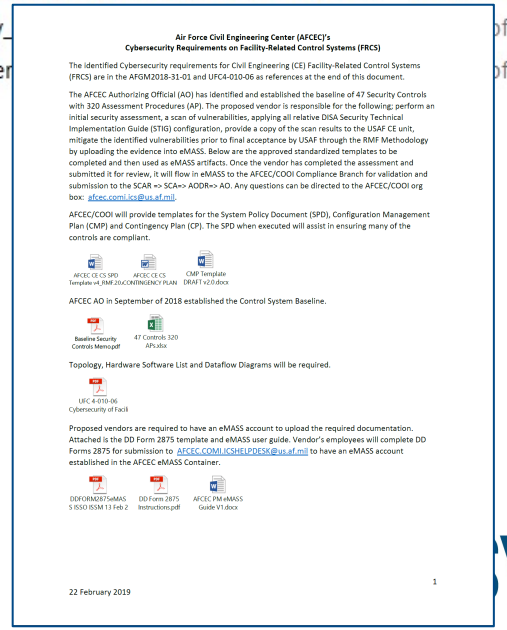
Navy/NAVFAC/CIO

Air Force/AFCEC

Defense Health Agency

Defense Logistics Agency




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 UFC4-010-06 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=> AODR=> AO. Any questions can be directed to the AFCEC/COOI org box: afcec.comi.ics@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 v4_RMF 2018
AFCEC CE CS CONTINGENCY PLAN
CMP Template DRAFT v2.0.docx

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

Baseline Security Controls Memo.pdf
47 Controls 320 APs.xlsx

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

UFC 4-010-06 Cybersecurity of Facili

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 Forms 2875 for submission to AFCEC.COMI.ICSHELPDESK@us.af.mil to have an eMASS account established in the AFCEC eMASS Container.

DDFORM2875eMASS ISSO ISSM 13 Feb 2
DD Form 2875 Instructions.pdf
AFCEC PM eMASS Guide V1.docx

22 February 2019

1

Variations in ATO/eMASS procedures

Air Force Platform Enclave – COINE V2

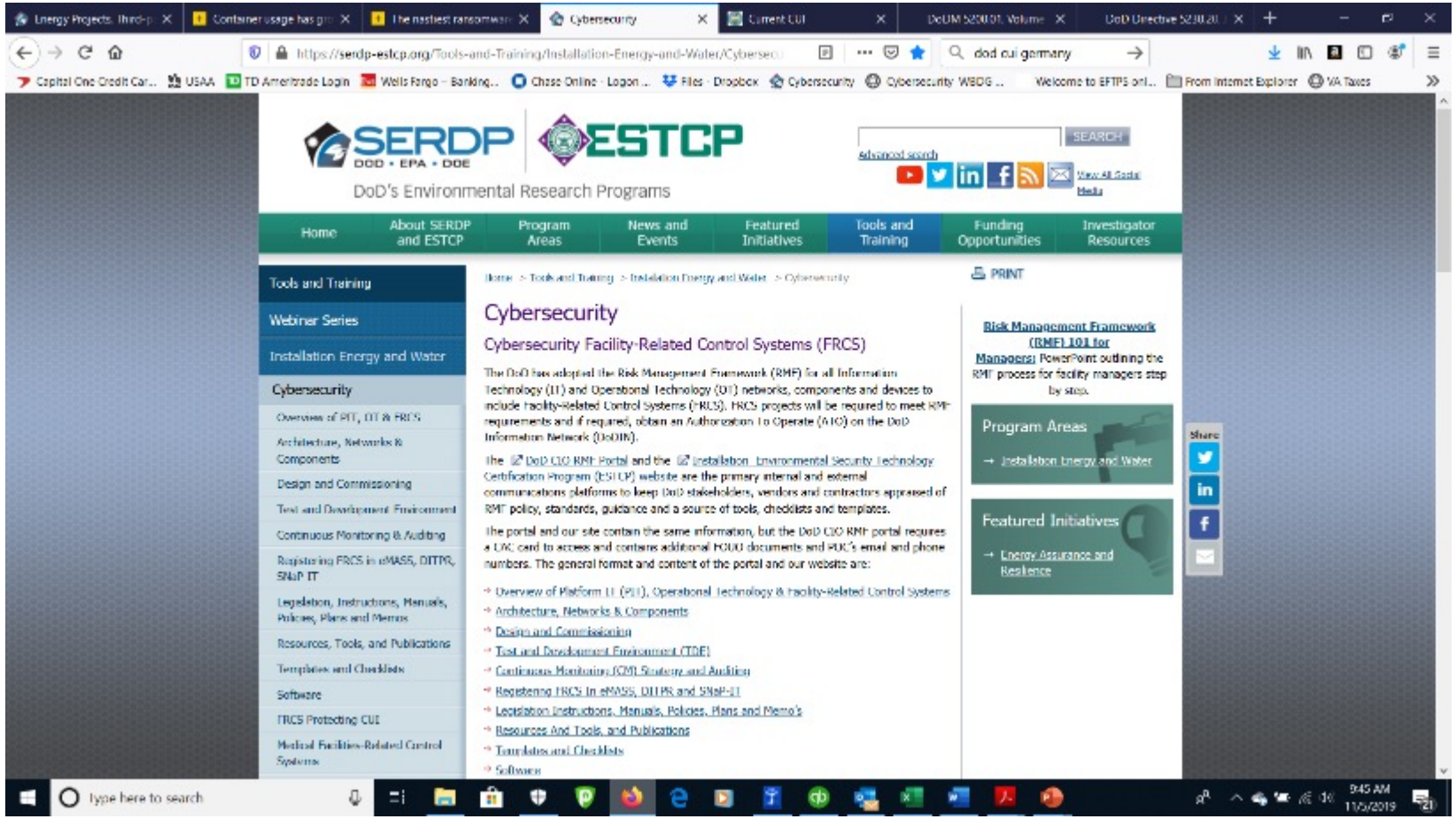
Navy Platform Enclave – PSNet V2

Army Platform Enclave – In development , interim SCPE

Defense Health Agency Platform Enclave - MedCOI

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

ESTCP RMF Cybersecurity Guidance and Templates



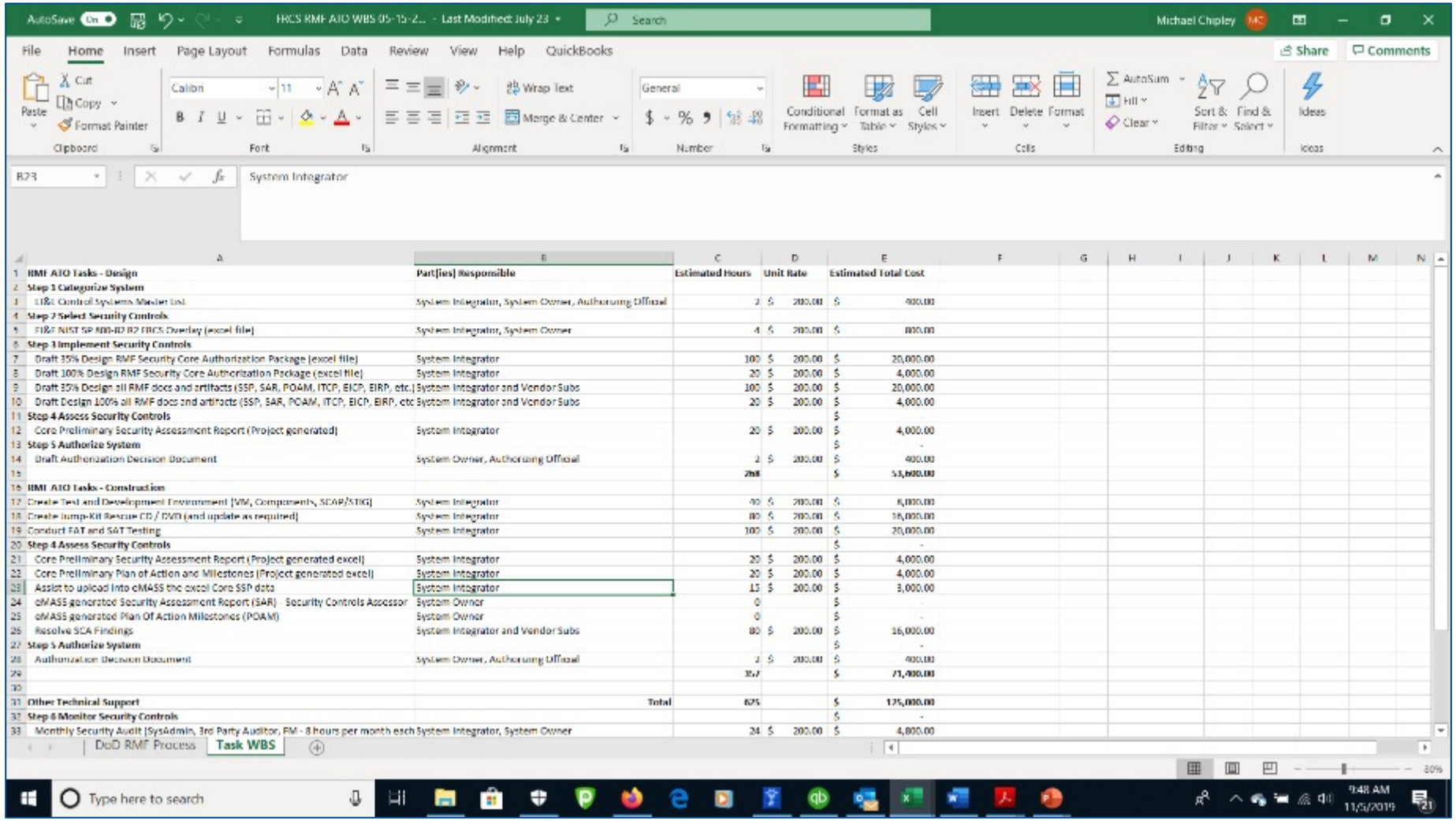
https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity

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)

RMF ATO Work Breakdown Structure (WBS)



RMF ATO Tasks - Design	Part[ies] Responsible	Estimated Hours	Unit Rate	Estimated Total Cost
Step 1 Categorize System				
Draft 35% Design RMF Security Core Authorization Package (excel file)	System Integrator	100	$ 200.00	$ 20,000.00
Draft 100% Design RMF Security Core Authorization Package (excel file)	System Integrator	20	$ 200.00	$ 4,000.00
Draft 35% Design all RMF docs and artifacts (SSP, SAR, POAM, ITCP, EICP, EIRP, etc.)	System Integrator and Vendor Subs	100	$ 200.00	$ 20,000.00
Draft Design 100% all RMF docs and artifacts (SSP, SAR, POAM, ITCP, EICP, EIRP, etc	System Integrator and Vendor Subs	20	$ 200.00	$ 4,000.00
Step 4 Assess Security Controls				$ -
Core Preliminary Security Assessment Report (Project generated)	System Integrator	20	$ 200.00	$ 4,000.00
Step 5 Authorize System				$ -
Draft Authorization Decision Document	System Owner, Authorizing Official	2	$ 200.00	$ 400.00
		268		$ 53,800.00
RMF ATO Tasks - Construction				
Create Test and Development Environment (VM, Components, SCAP/STIG)	System Integrator	40	$ 200.00	$ 8,000.00
Create Jump-Kit Rescue CD / DVD (and update as required)	System Integrator	80	$ 200.00	$ 16,000.00
Conduct FAT and SAT Testing	System Integrator	100	$ 200.00	$ 20,000.00
Step 4 Assess Security Controls				$ -
Core Preliminary Security Assessment Report (Project generated excel)	System Integrator	20	$ 200.00	$ 4,000.00
Core Preliminary Plan of Action and Milestones (Project generated excel)	System Integrator	20	$ 200.00	$ 4,000.00
Assist to upload into eMASS the excel Core SSP data	System Integrator	15	$ 200.00	$ 3,000.00
eMASS generated Security Assessment Report (SAR) - Security Controls Assessor	System Owner	0		$ -
eMASS generated Plan Of Action Milestones (POAM)	System Owner	0		$ -
Resolve SCA Findings	System Integrator and Vendor Subs	80	$ 200.00	$ 16,000.00
Step 5 Authorize System				$ -
Authorization Decision Document	System Owner, Authorizing Official	2	$ 200.00	$ 400.00
		357		$ 71,400.00
Other Technical Support	**Total**	625		$ 125,000.00
Step 6 Monitor Security Controls				$ -
Monthly Security Audit (SysAdmin, 3rd Party Auditor, PM - 8 hours per month each	System Integrator, System Owner	24	$ 200.00	$ 4,800.00

BLUF: Budget approx. $125K to prepare an FRCS RMF ATO package

(This cost is being validated by USACE Cyber Center of Expertise – most 1391's budget $250K to include SCA costs)

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

Standards – NIST SP 800-82 R2


NIST Special Publication 800-82
Revision 1

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Joe Falco
Karen Scarfone

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

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (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

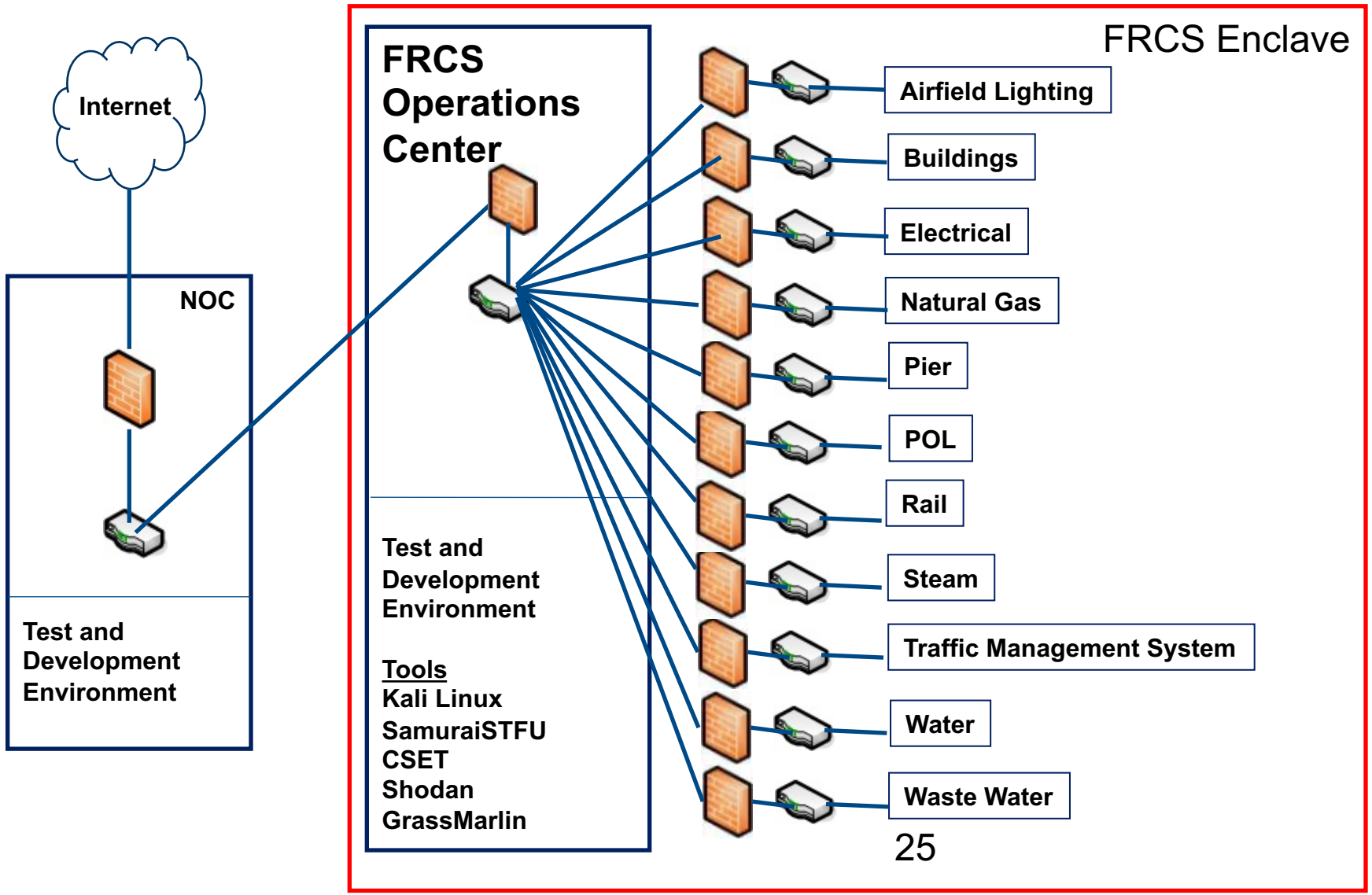
Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

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

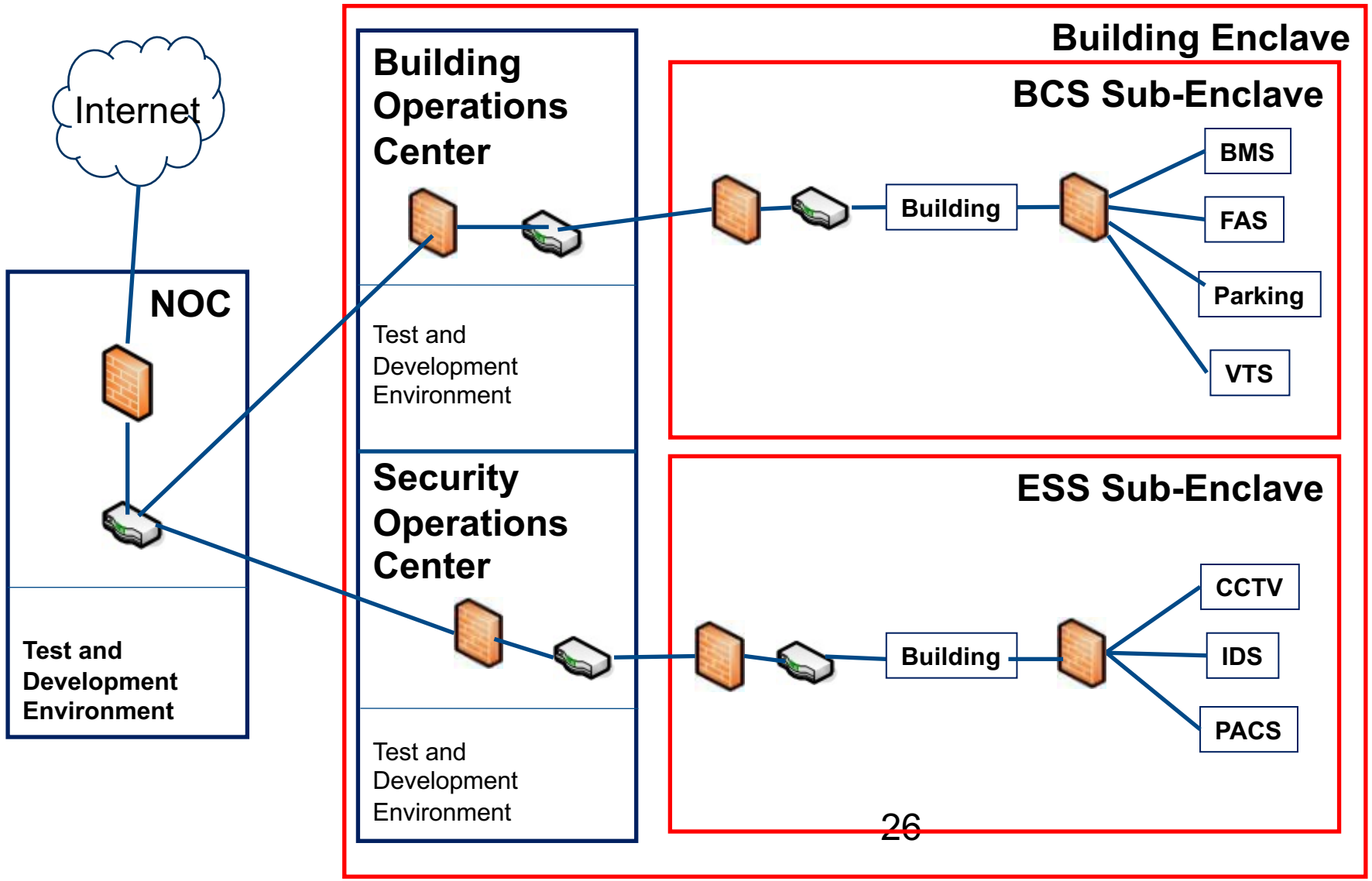
Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

FRCS Enclave and Numerous Sub-Enclaves



Hybrid FRCS and Security Enclaves



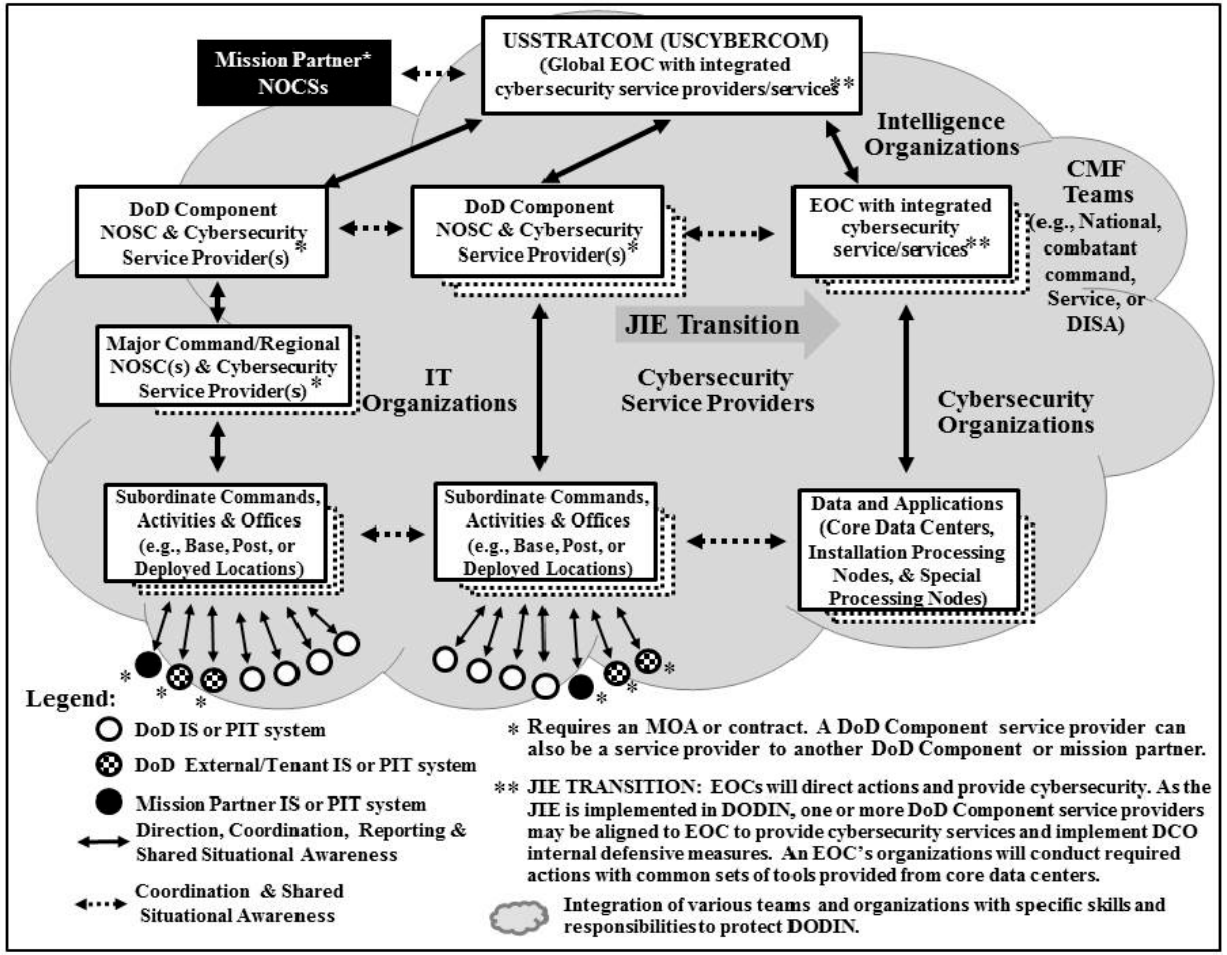
Installations and Environment
Real Property Installed Equipment

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)

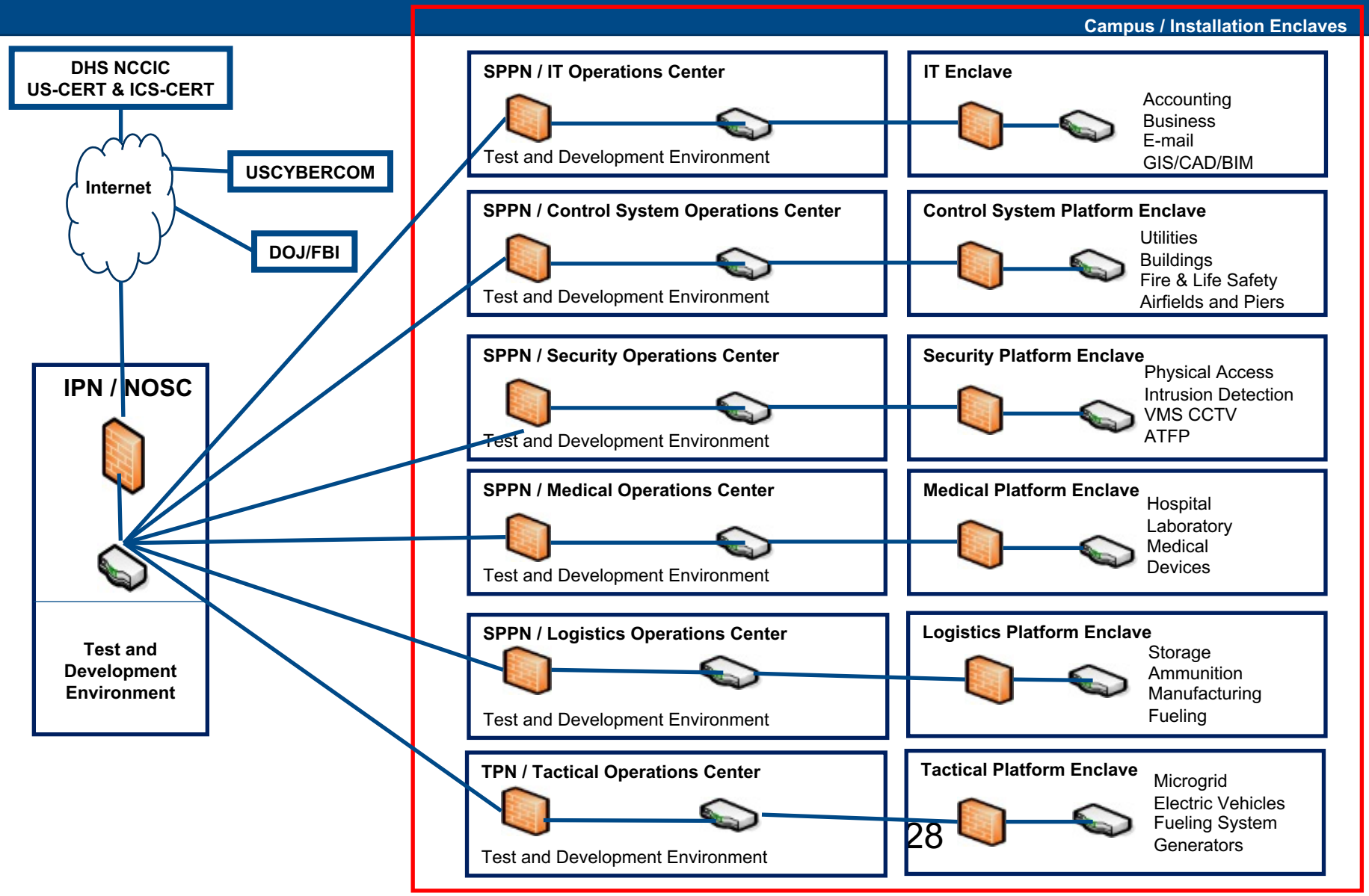
Figure 2. Notional View of Current and Future Integration of Cybersecurity Activities



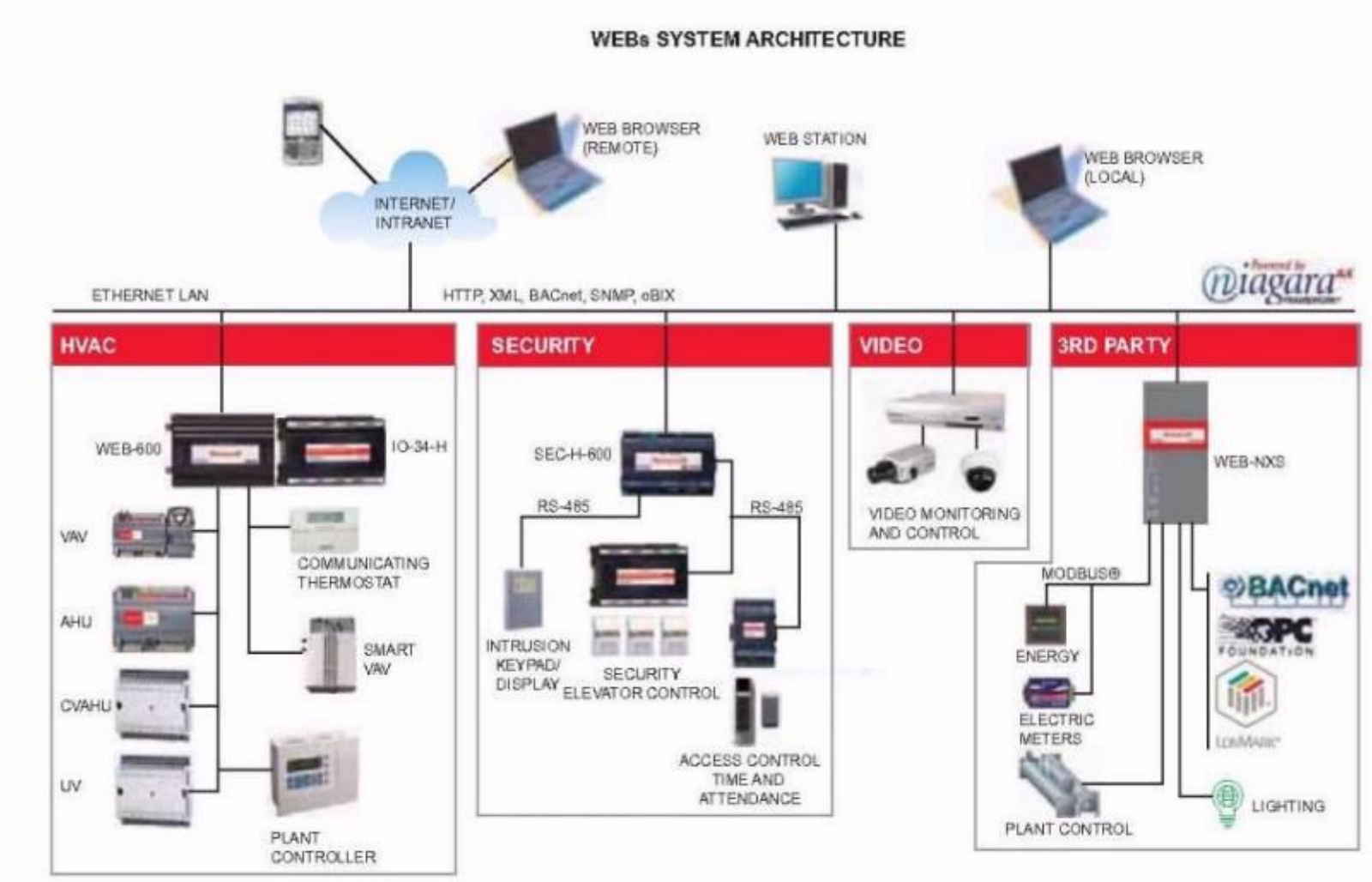
Gigabit Fiber, IPv6

- **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

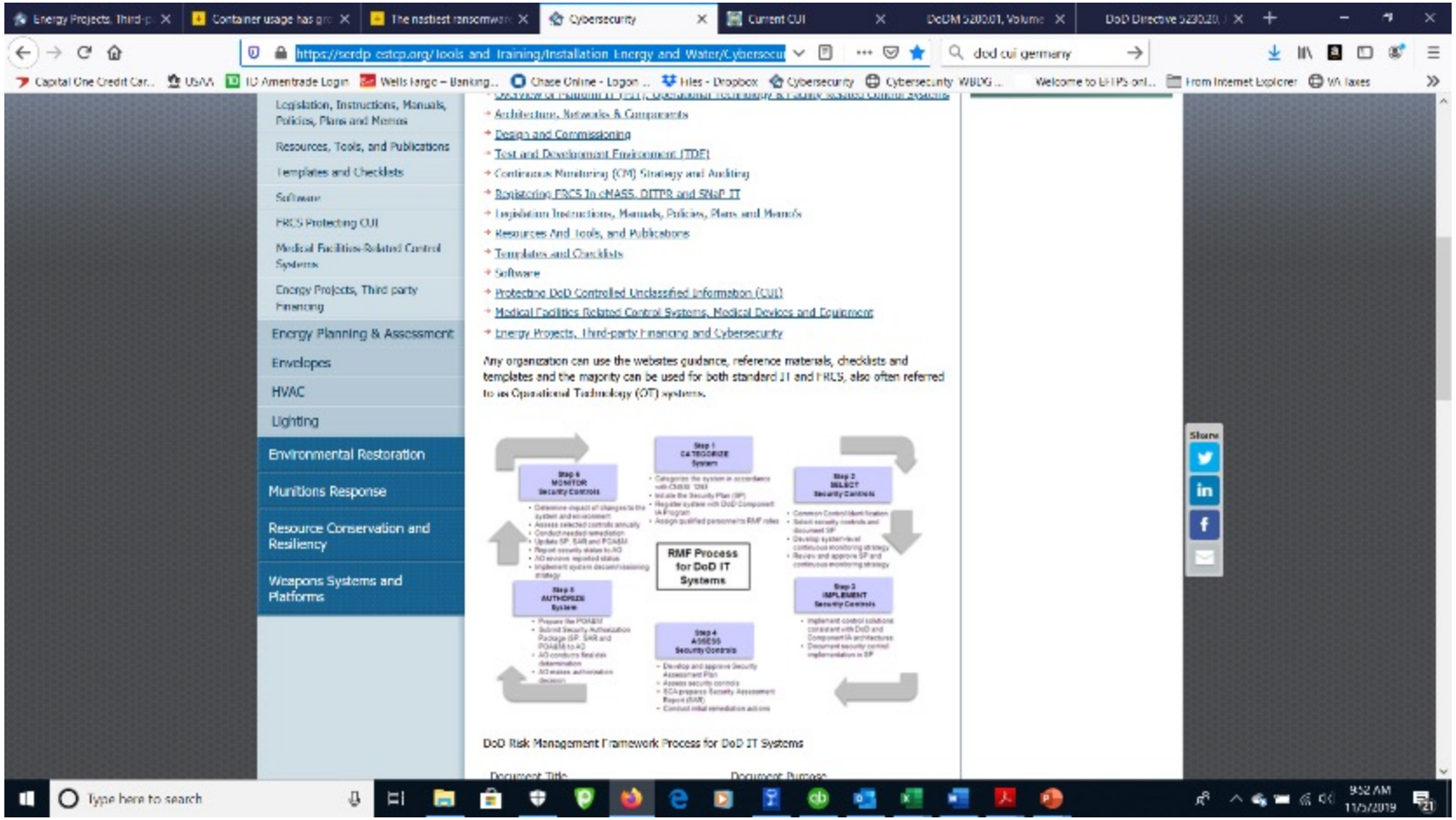
Open Control Systems Protocols

- Modbus: Master/Slave - Port 502
- BACnet: Peer to Peer - 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 NiagraAX/Fox
- Johnson Metasys N2
- OSISoft Pi System
- Many others…

ESTCP Cybersecurity Guidelines and Resources



Any organization can use for their FRCS

ESTCP 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.

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

Create the Cyber Narrative/Design Analysis

Cybersecurity

Cybersecurity Requirements

CODES AND REFERENCES

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

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

FACILITY-RELATED CONTROL SYSTEMS

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

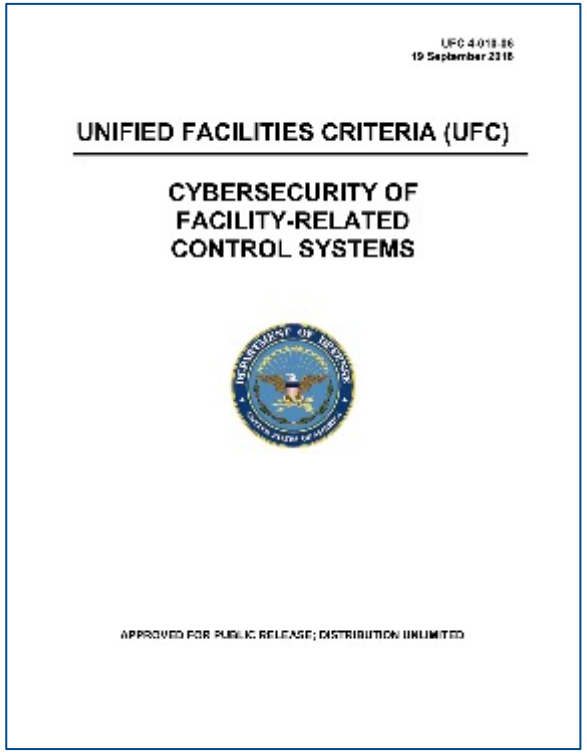
The PROJECT cyber design needs to include, but is not limited to, the following FRCS:

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

Cybersecurity Guideline Sequence

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

DoD UFC 4-010-06 Cybersecurity


UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

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

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

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

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

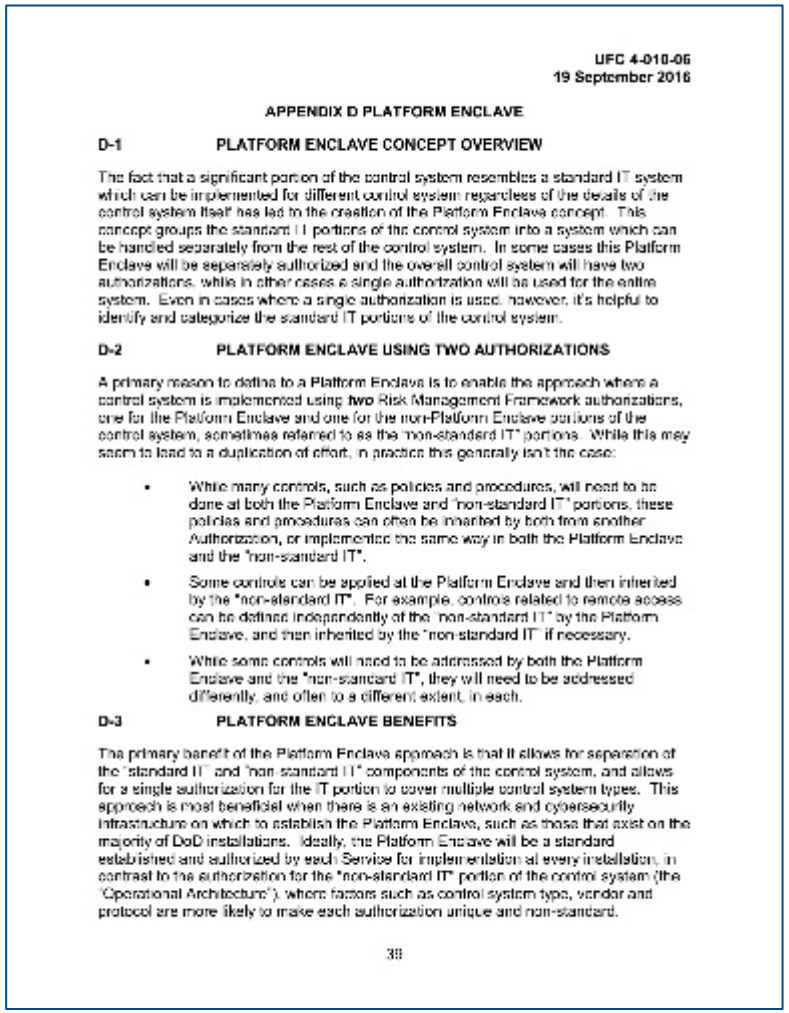
Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.

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

DoD UFC 4-010-06 Platform Enclave

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

DoD UFC 4-010-06 Appendix D



UFC 4-010-06
19 September 2016

APPENDIX D PLATFORM ENCLAVE

D-1 PLATFORM ENCLAVE CONCEPT OVERVIEW

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

D-2 PLATFORM ENCLAVE USING TWO AUTHORIZATIONS

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

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

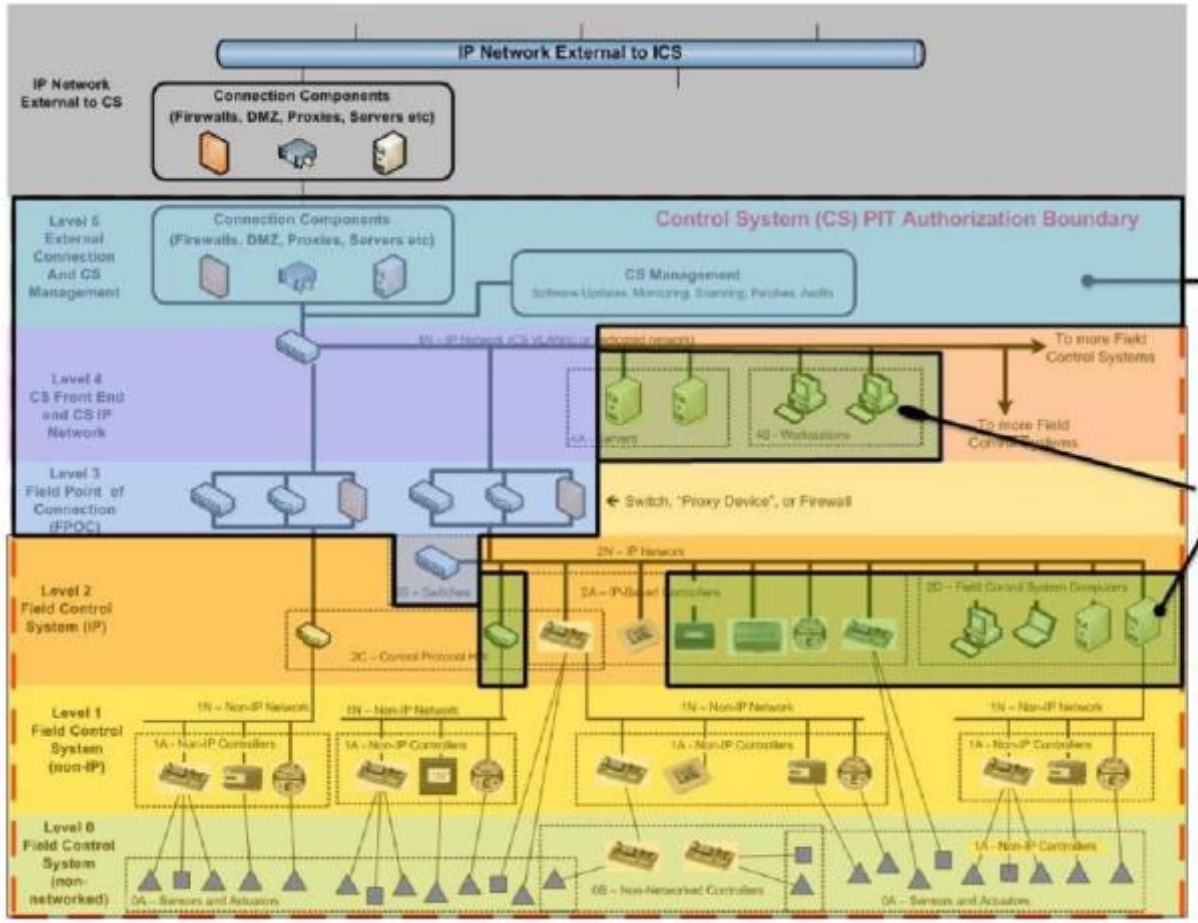
D-3 PLATFORM ENCLAVE BENEFITS

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

38

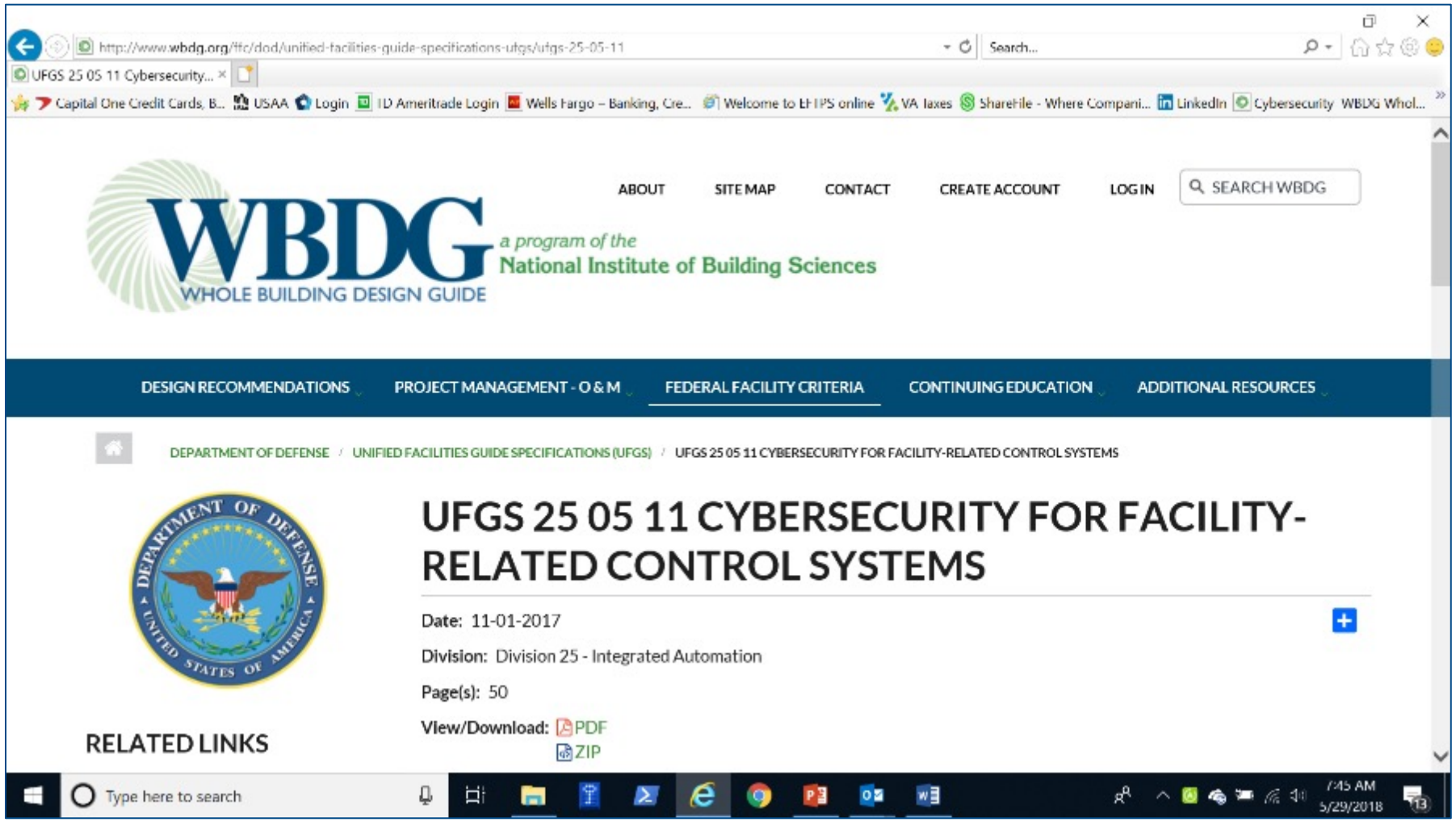
Platform Enclave: The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system, or is mostly implemented at the Platform Enclave but also needed within the field control system (in which case the CCI is also in the “Designer” category). 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



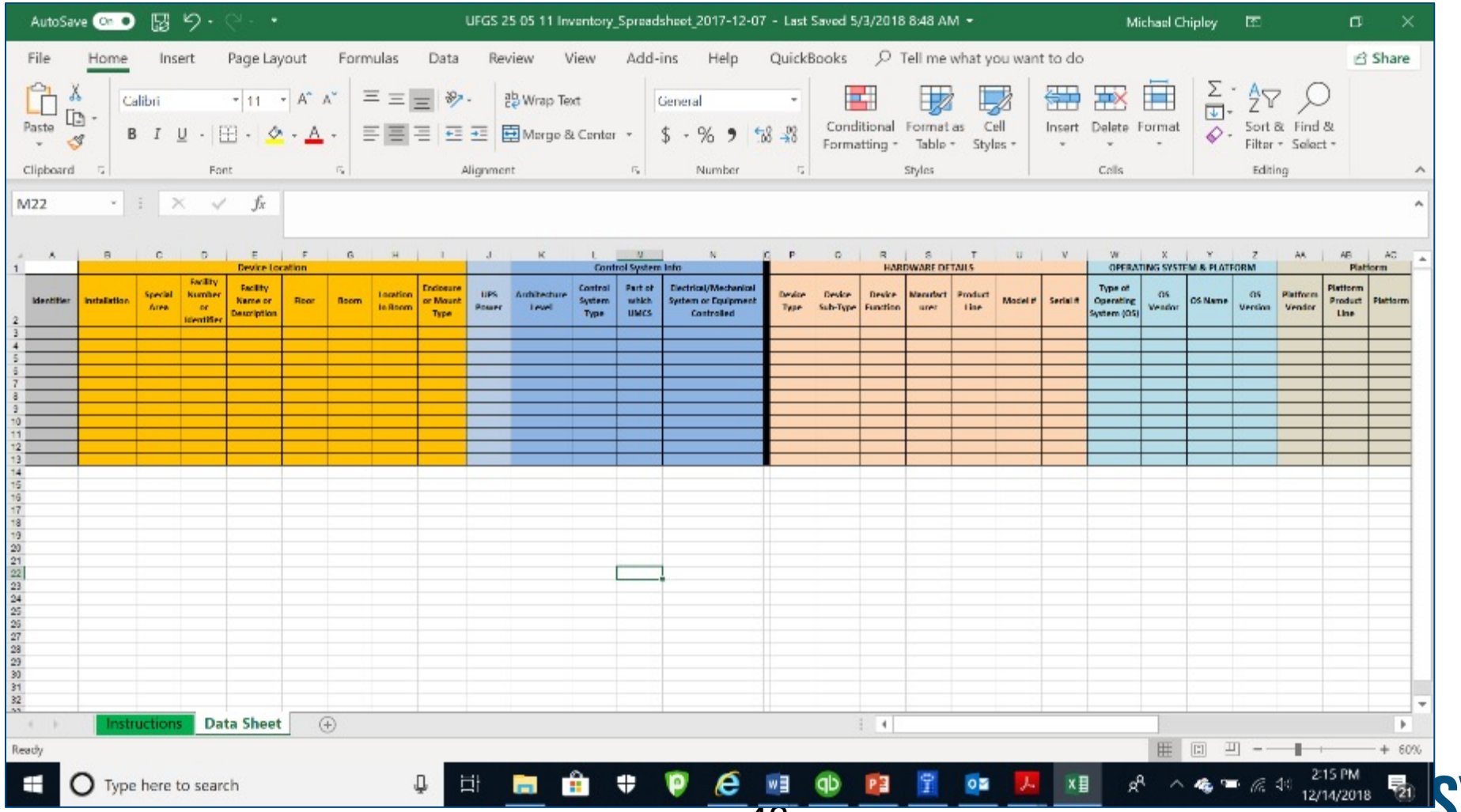
All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the FRCS-PE and NUMCS.

UFGS 25 05 11 Cybersecurity For FRCS



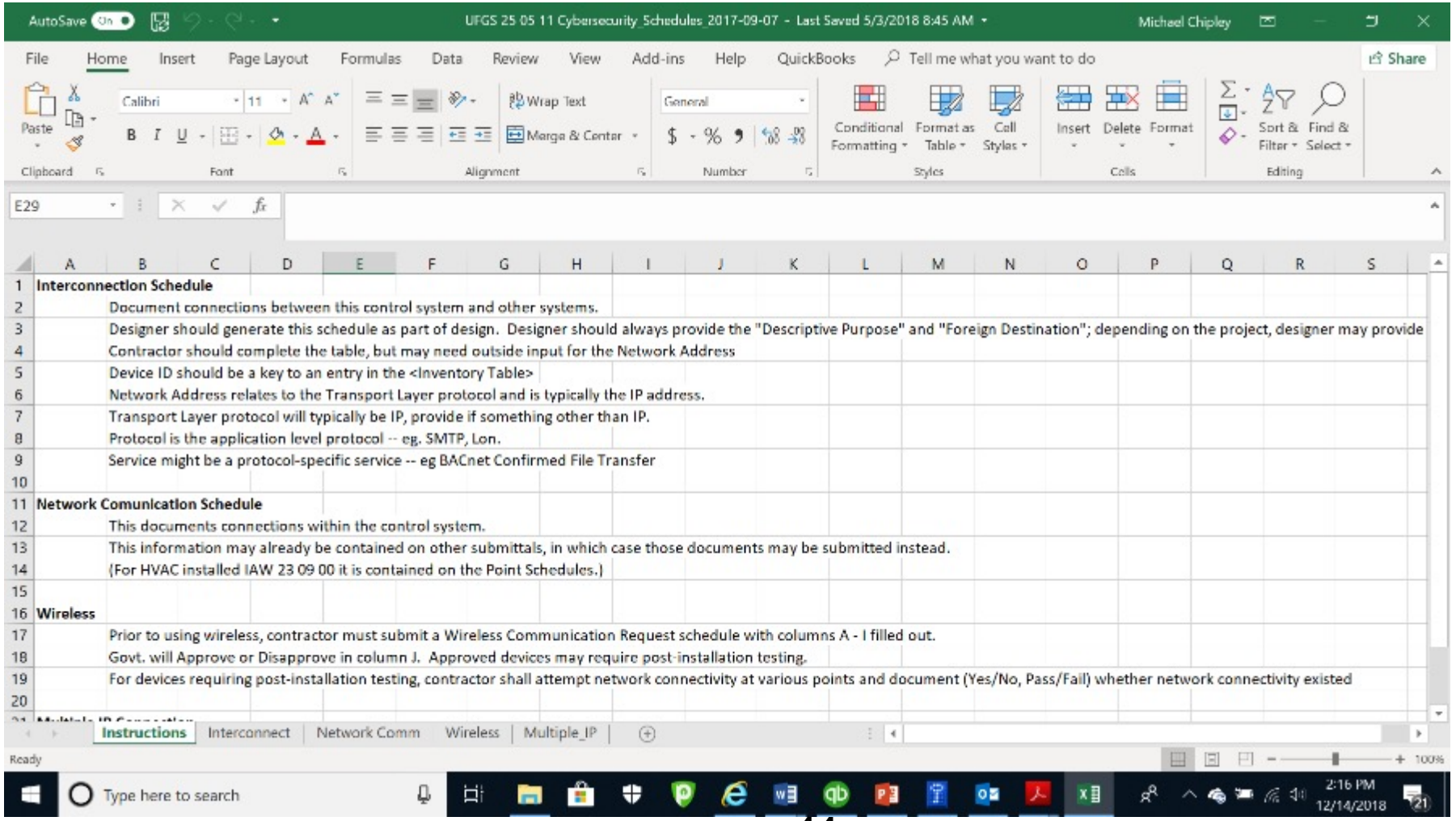
http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

UFGS 25 05 11 Inventory



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

UFGS 25 05 11 Schedules



	A	B
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 Comunication 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		

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

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.

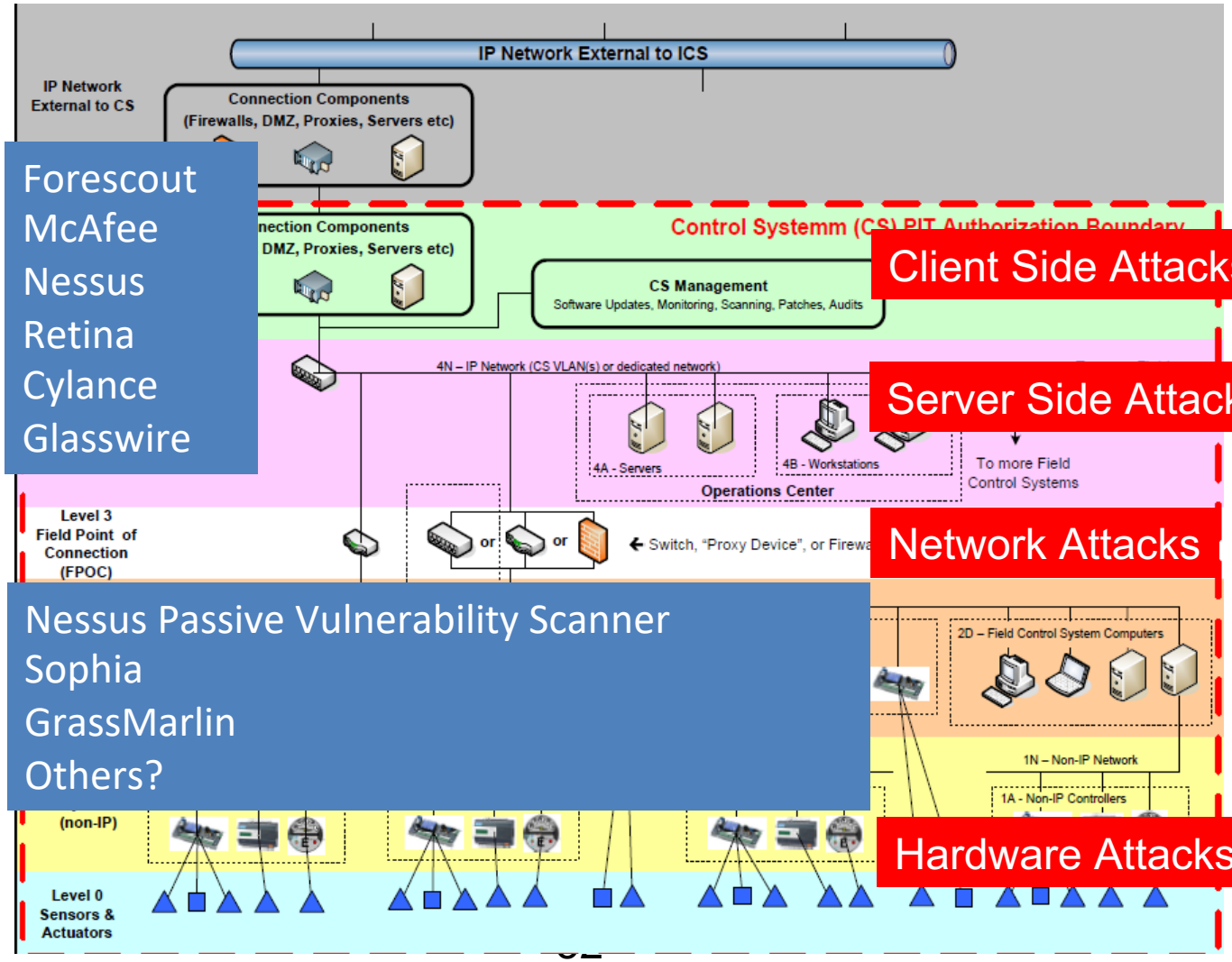
System Security Plan (SSP) – Use the DoD Core Authorization Package to develop a Preliminary SSP.

Continuous Monitoring (CM) and Attack Surfaces, Audit

Host Based Security Systems Scanning (Active)

Windows, Linux HTTP, TCP, UDP

Intrusion Detection Systems (Passive) PLC, RTU, Sensor Modbus, LonTalk, BACnet, DNP3



Forescout
McAfee
Nessus
Retina
Cylance
Glasswire

Client Side Attacks

Server Side Attacks

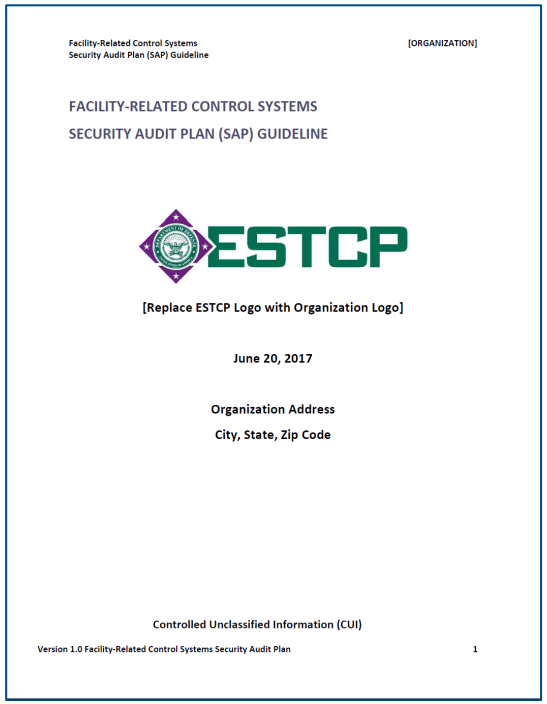
Network Attacks

Nessus Passive Vulnerability Scanner
Sophia
GrassMarlin
Others?

Hardware Attacks

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]

FACILITY-RELATED CONTROL SYSTEMS
SECURITY AUDIT PLAN (SAP) GUIDELINE

[Replace ESTCP Logo with Organization Logo]

June 20, 2017

Organization Address
City, State, Zip Code

Controlled Unclassified Information (CUI)

Version 1.0 Facility-Related Control Systems Security Audit Plan 1

2.1 SYSTEM-LEVEL AUDIT TRAILS

2.2 APPLICATION-LEVEL AUDIT TRAIL

2.3 USER AUDIT TRAILS

.

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

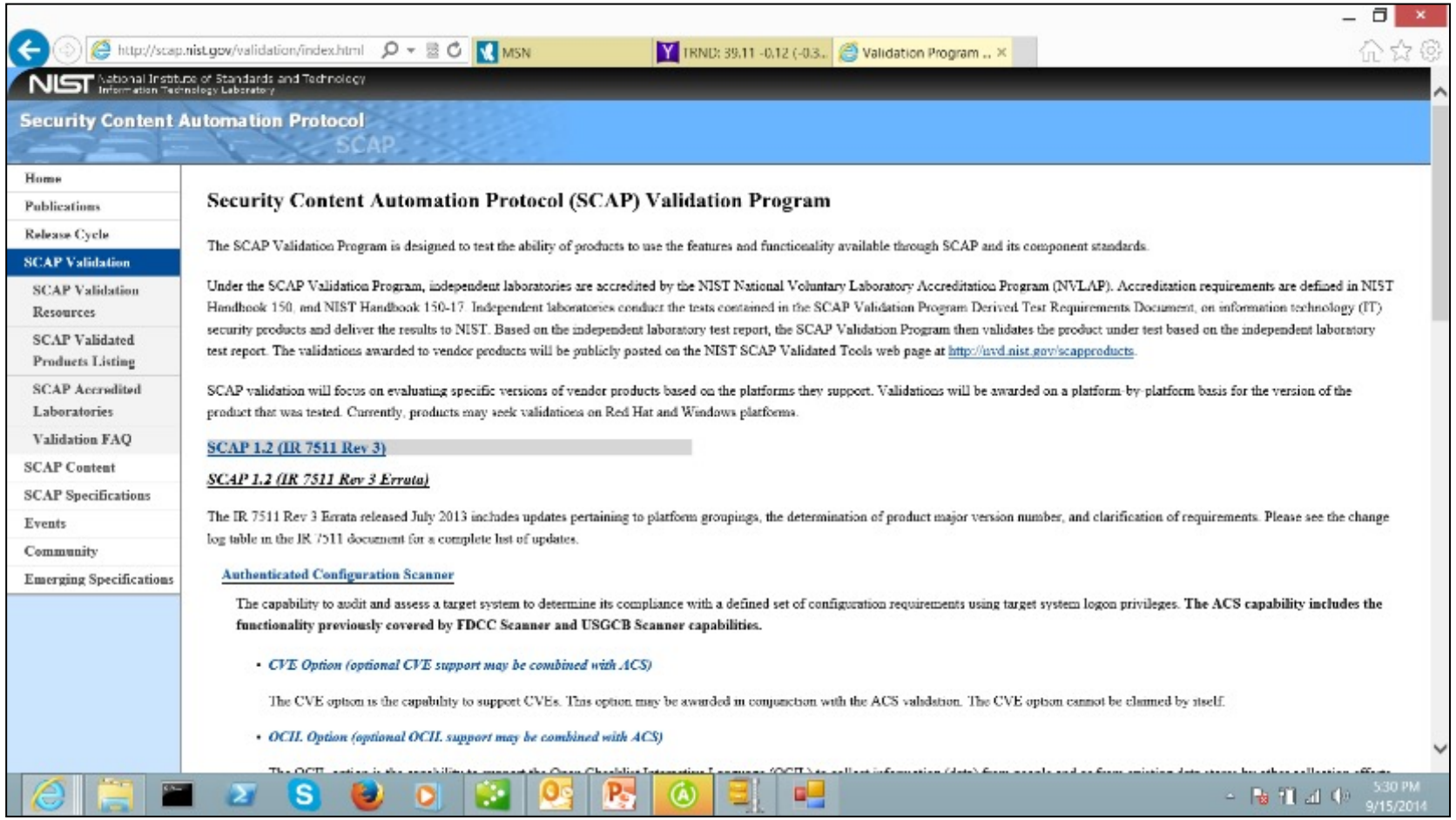
Step 1: Corporate IT Systems Admin Login Verification

- 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

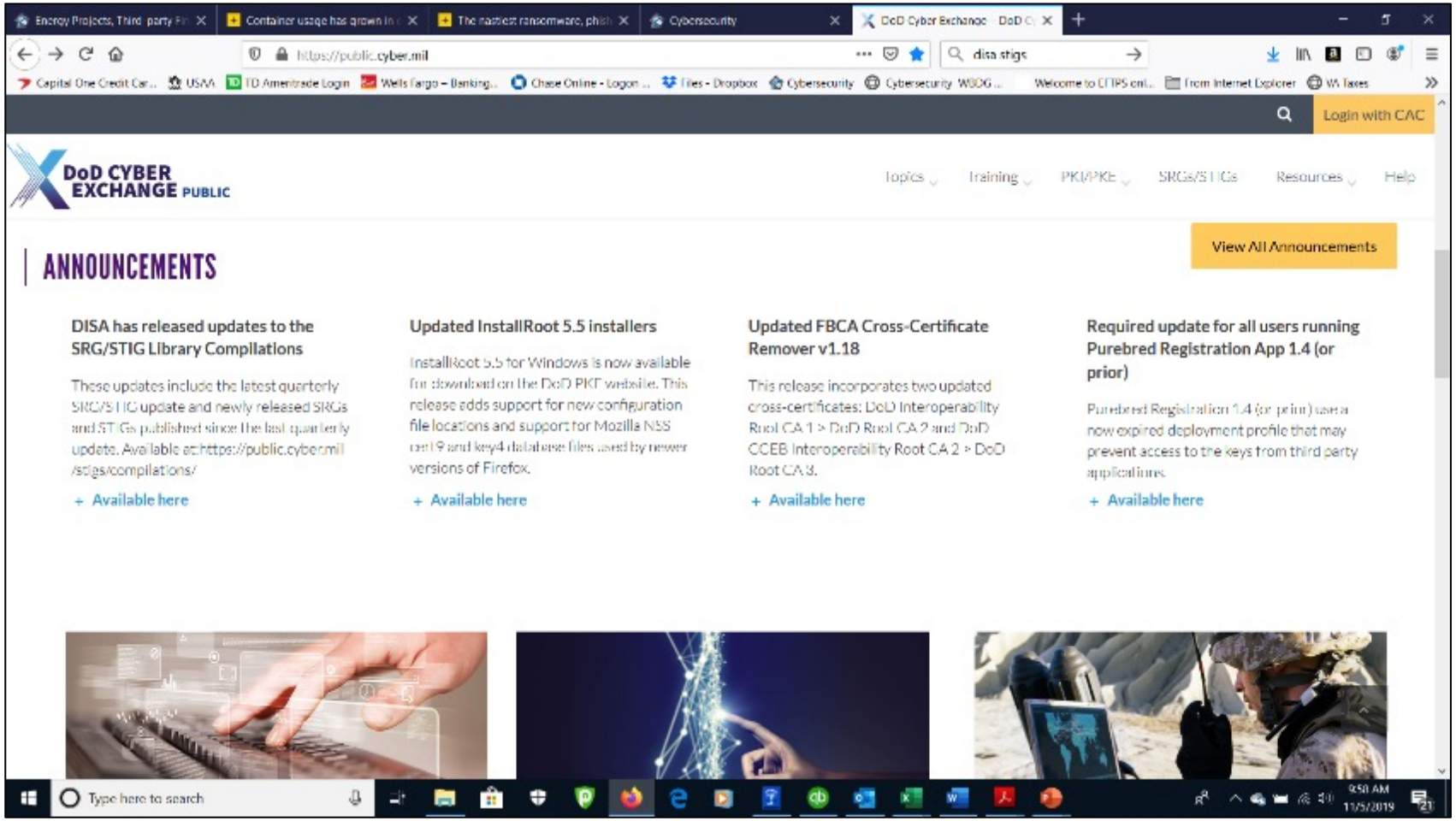
PI's/Project Teams will need to perform audits of both IT and OT

NIST SCAP



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

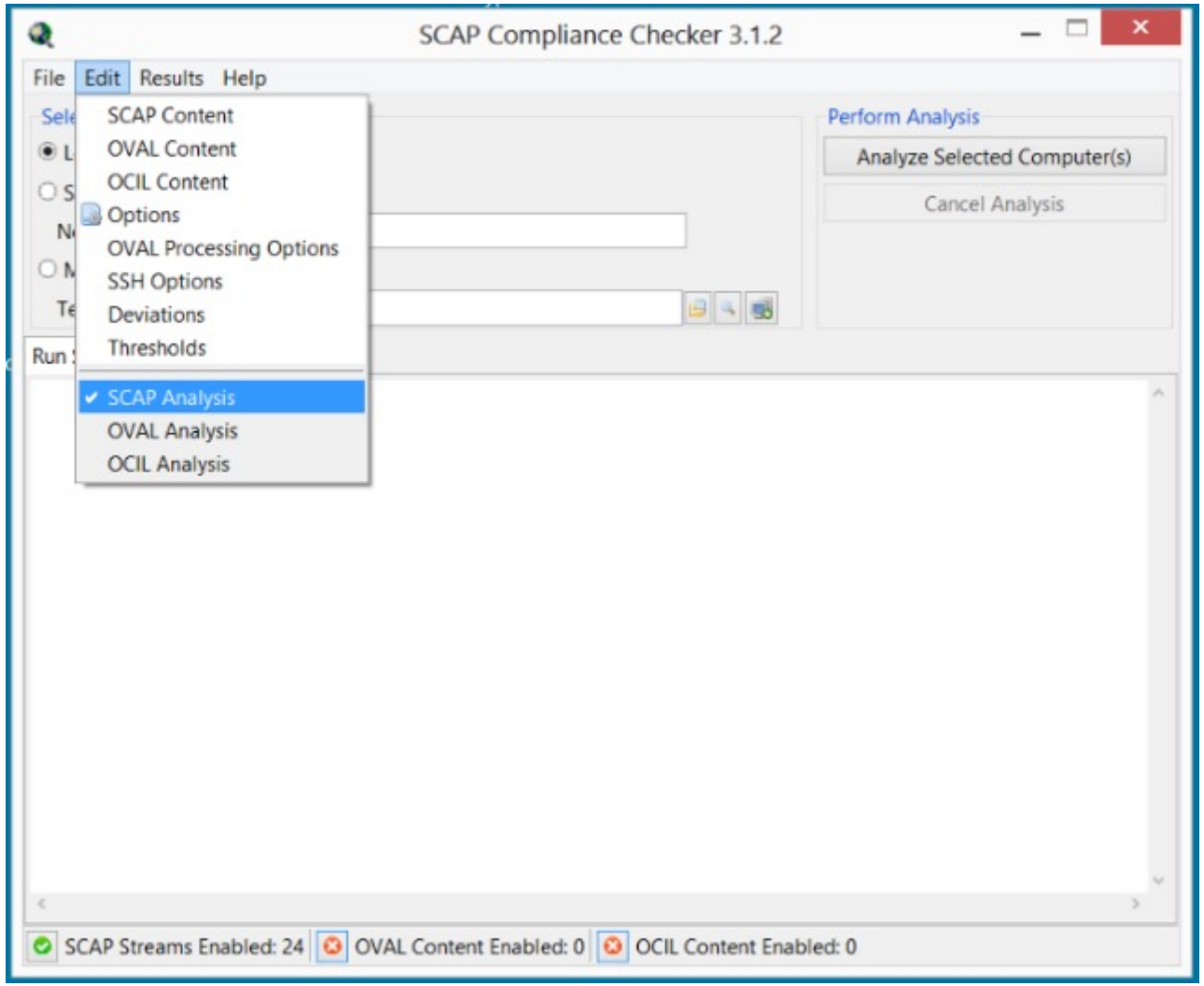
DISA STIGs – New Portal – Cyber Exchange



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

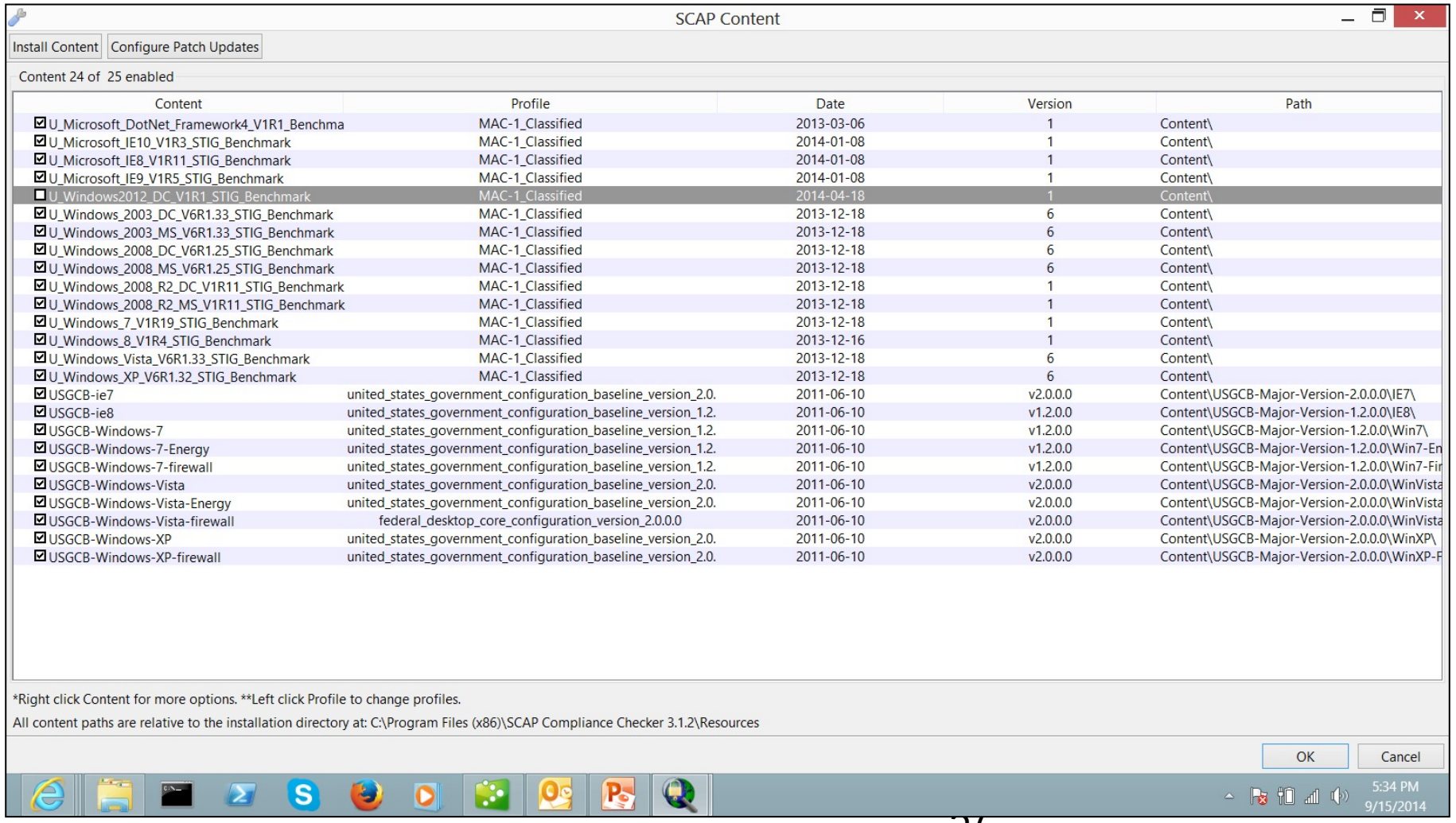
https://public.cyber.mil/

DISA SCAP Tool



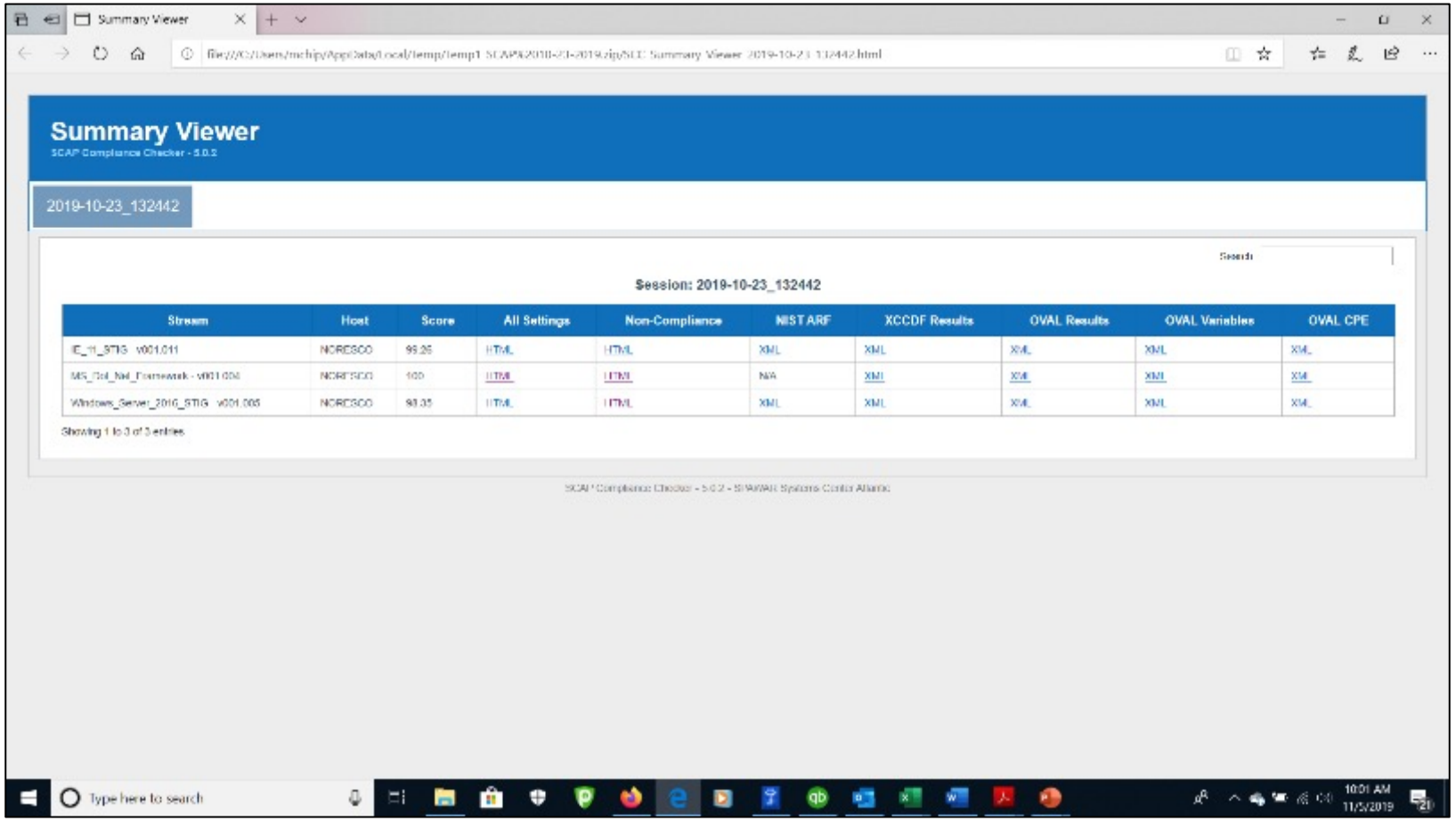
PI's/Project Teams will be provided with the DoD SCAP tool

DISA SCAP Tool Contents



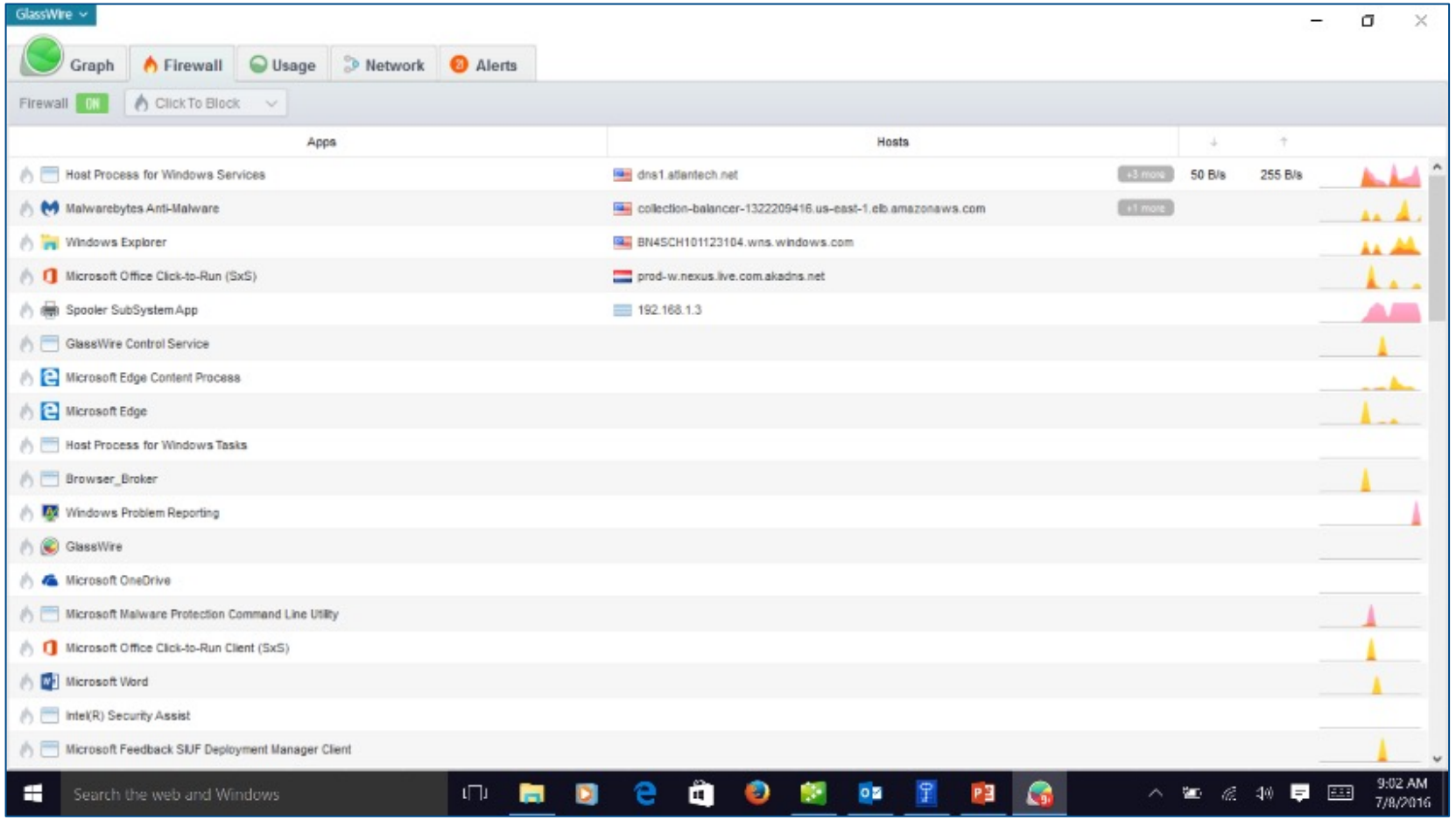
Use the DoD STIG's, not the USGBC

DISA SCAP Tool Results



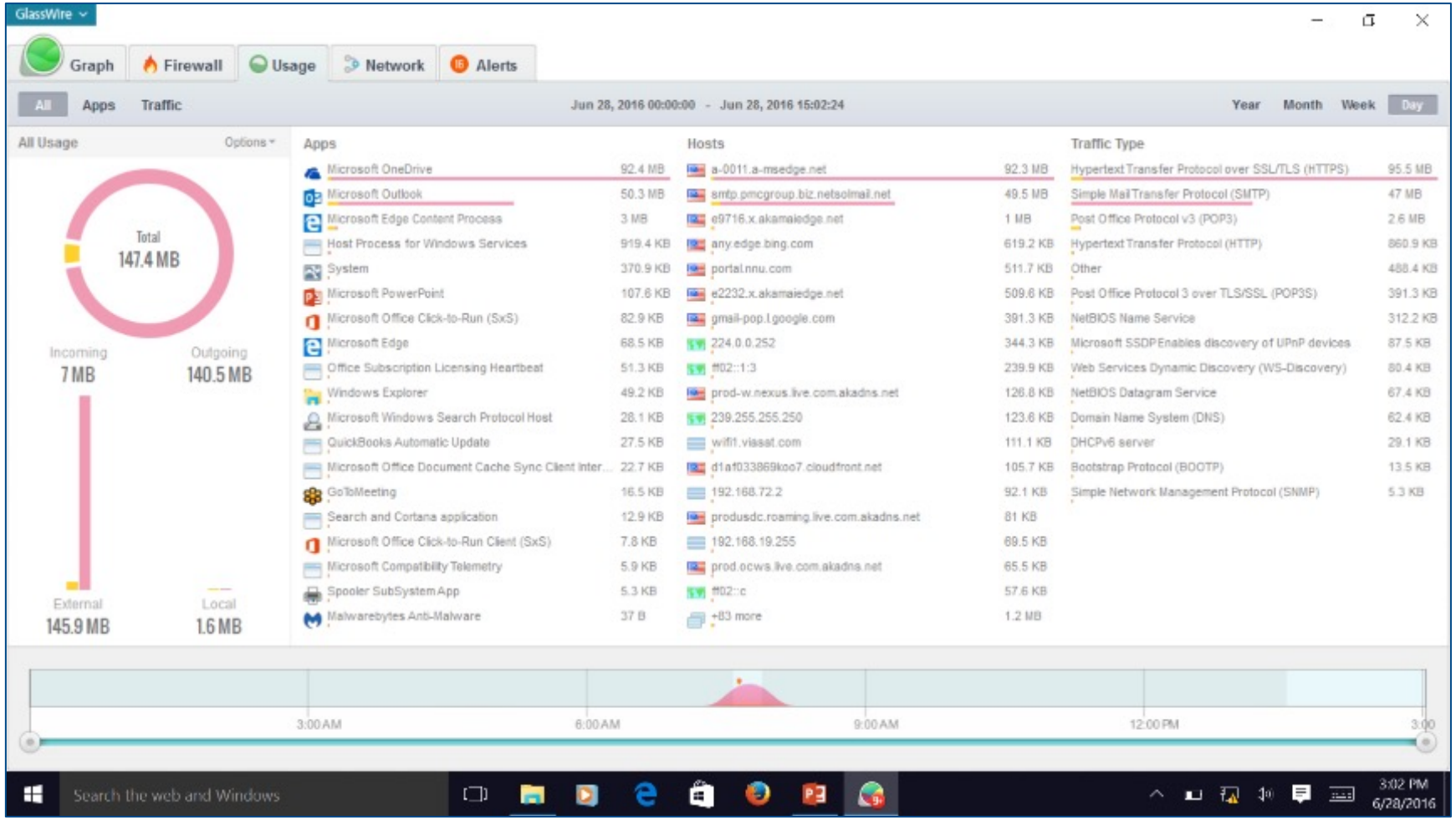
Maintain a score of 85 or better to demonstrate a properly hardened and configured system

Glasswire Firewall (IDS/IPS)

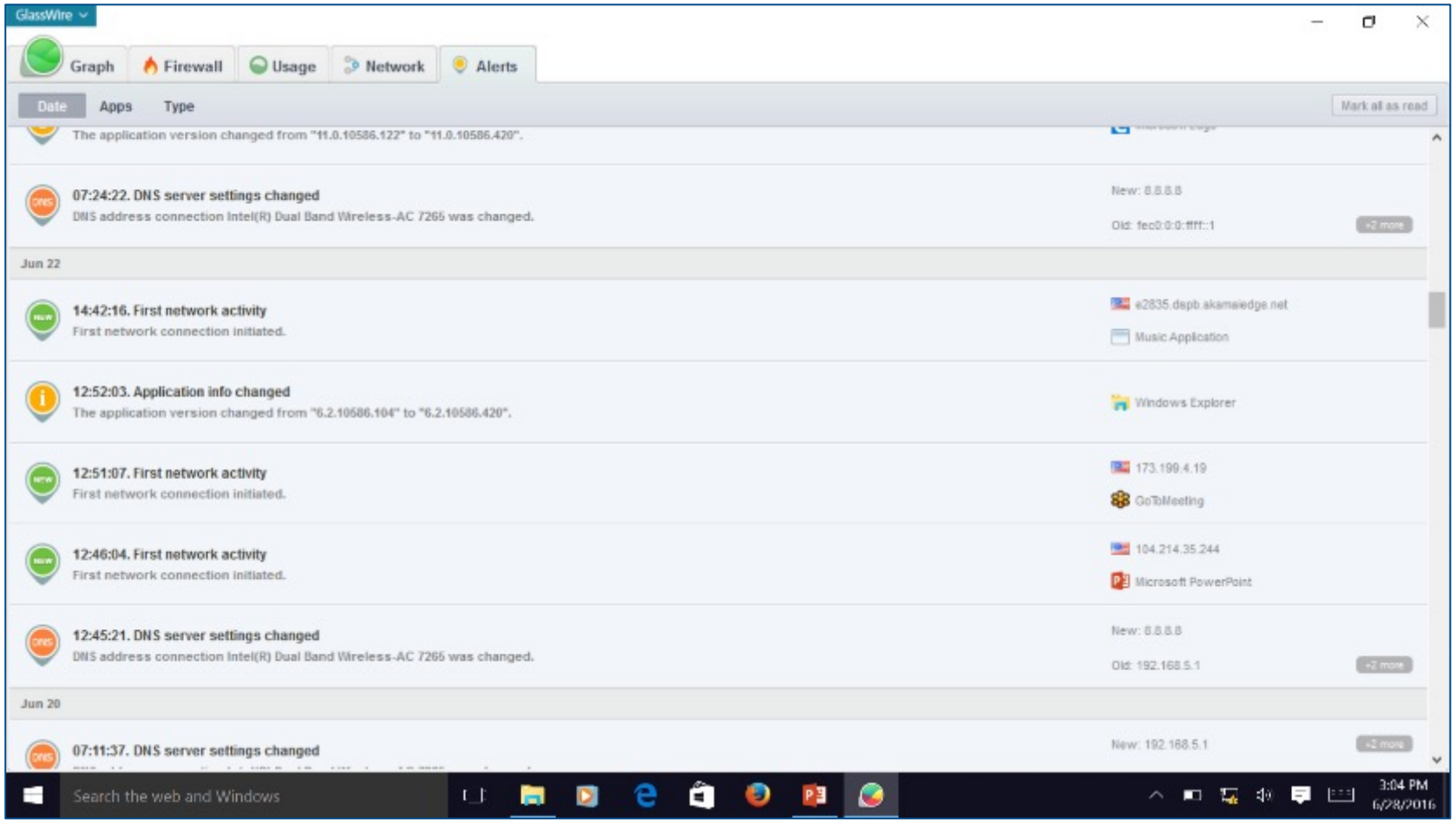


Glasswire can be used to simulate the HBSS/ACAS capability in the TDE

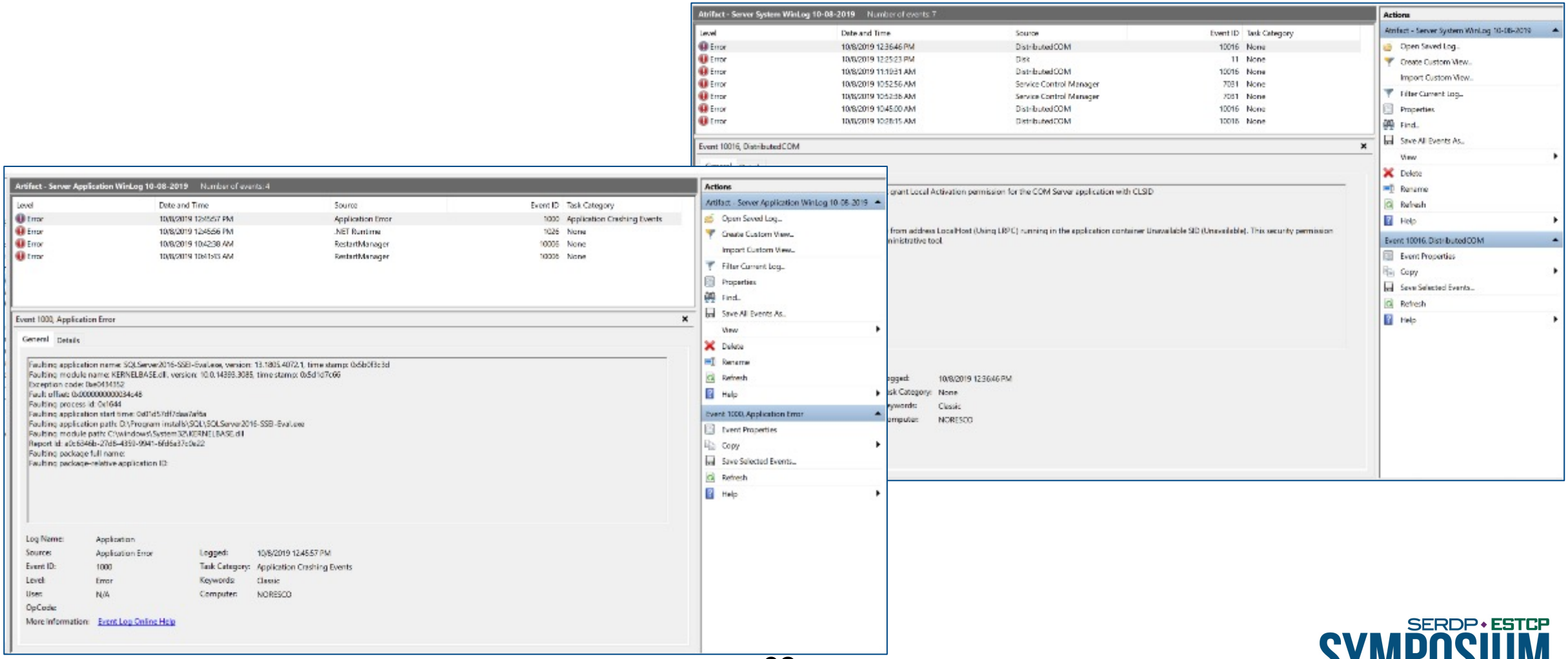
Glasswire Usage and Apps



Glasswire Alerts and Log's



Windows Log's



AV/MW Reports

Antivirus Health

Client Antivirus Health

Healthy

Average Definition File Age

5 days

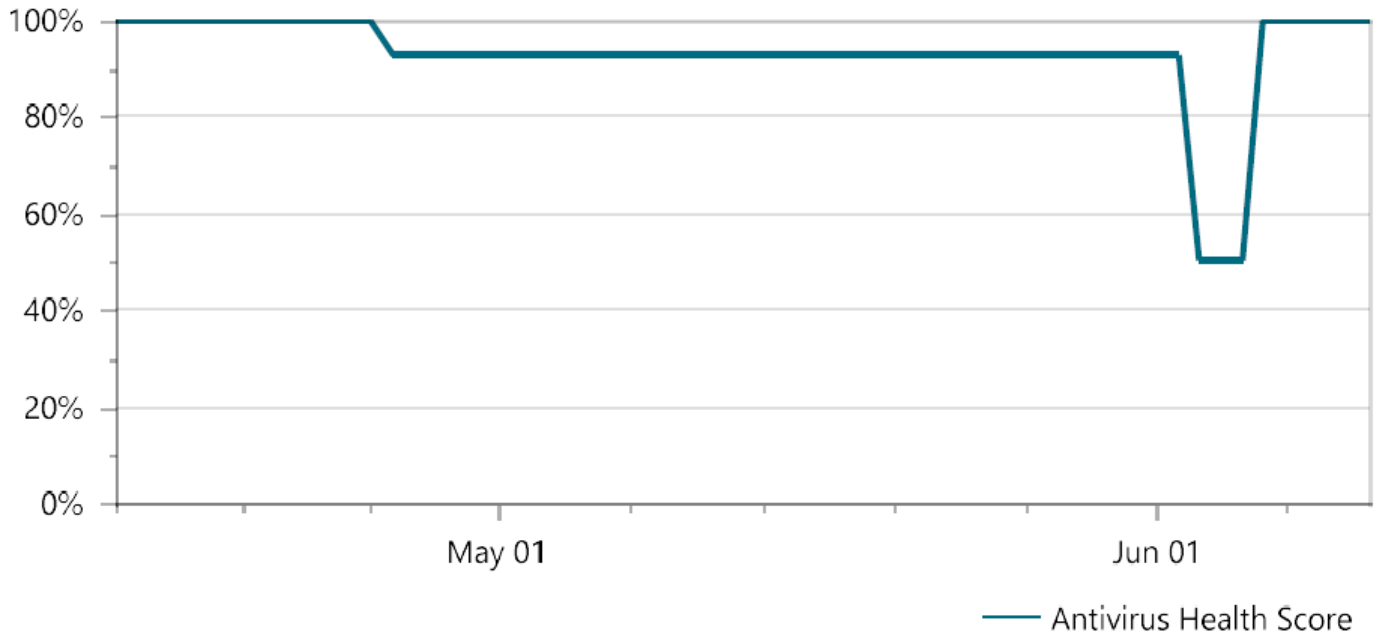
Total Managed Assets

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%

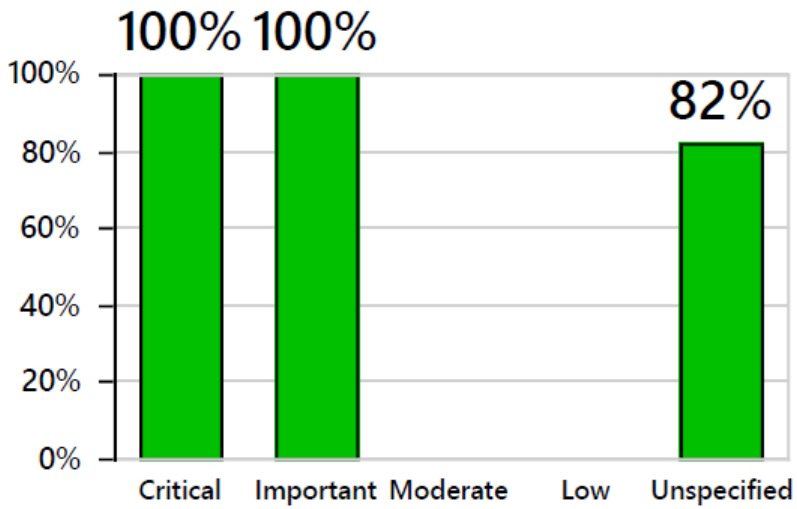
Patch Compliance Calculation

31 Installed / 34 Approved

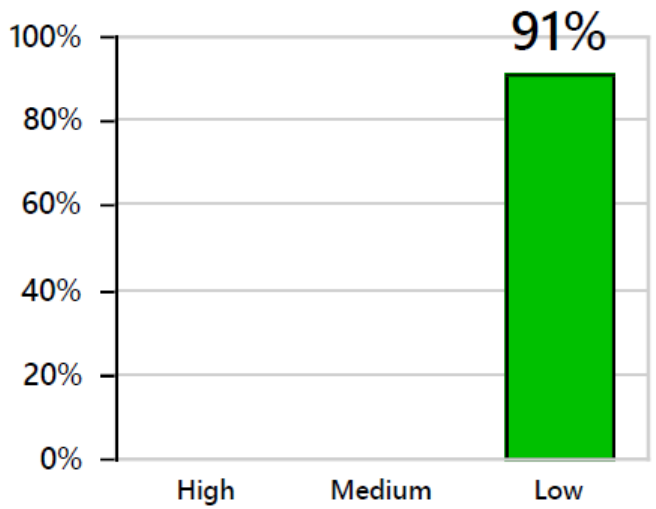
Total Managed Windows Assets

2 Servers / 5 Workstations

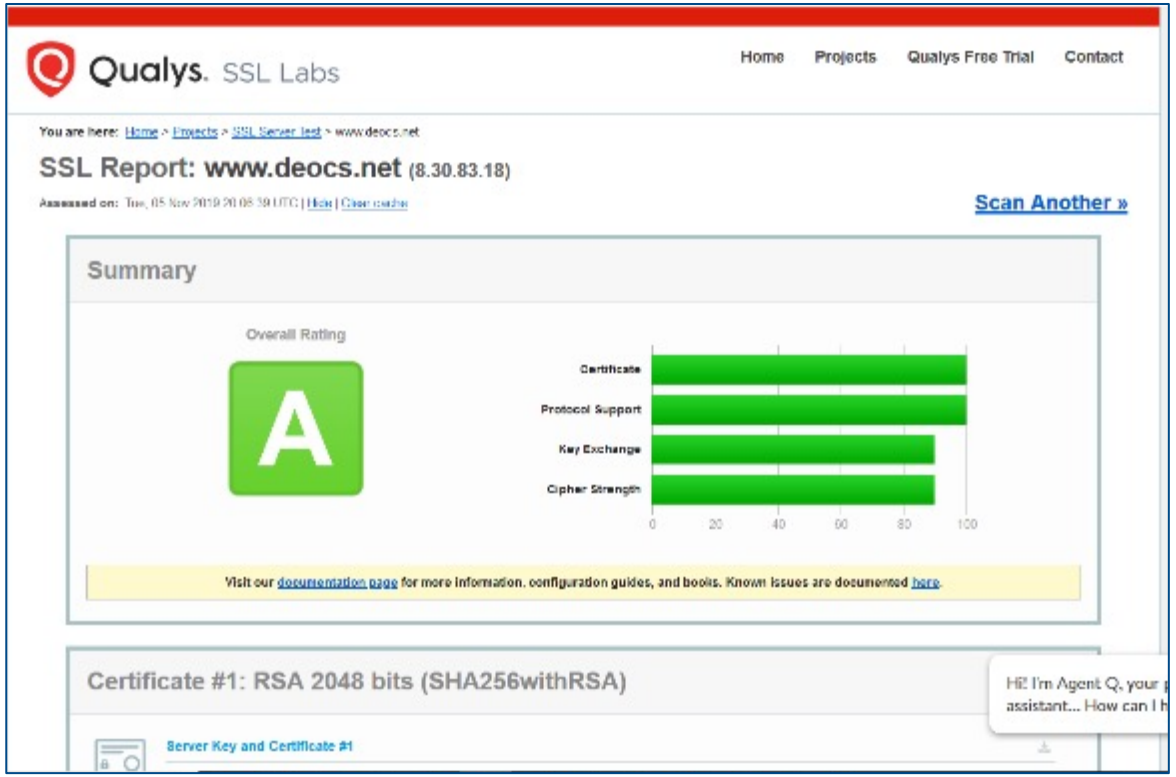
Compliance by Severity



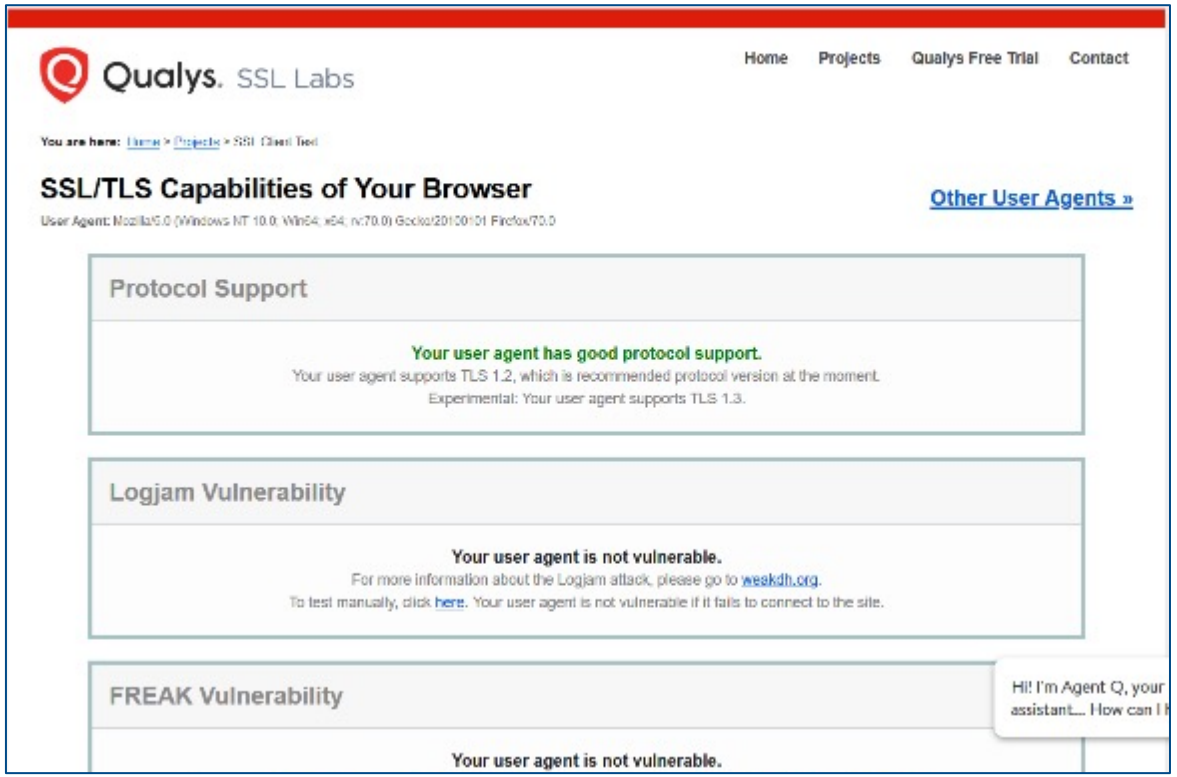
Compliance by CVSS



TLS Reports



Server Test



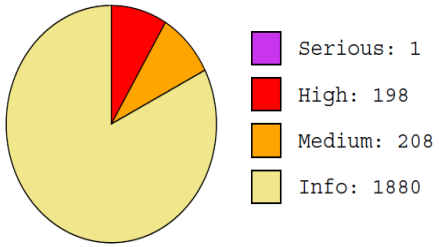
Client Browser Test

SEIM Reports

AlienVault: I.T Security Vulnerability Report

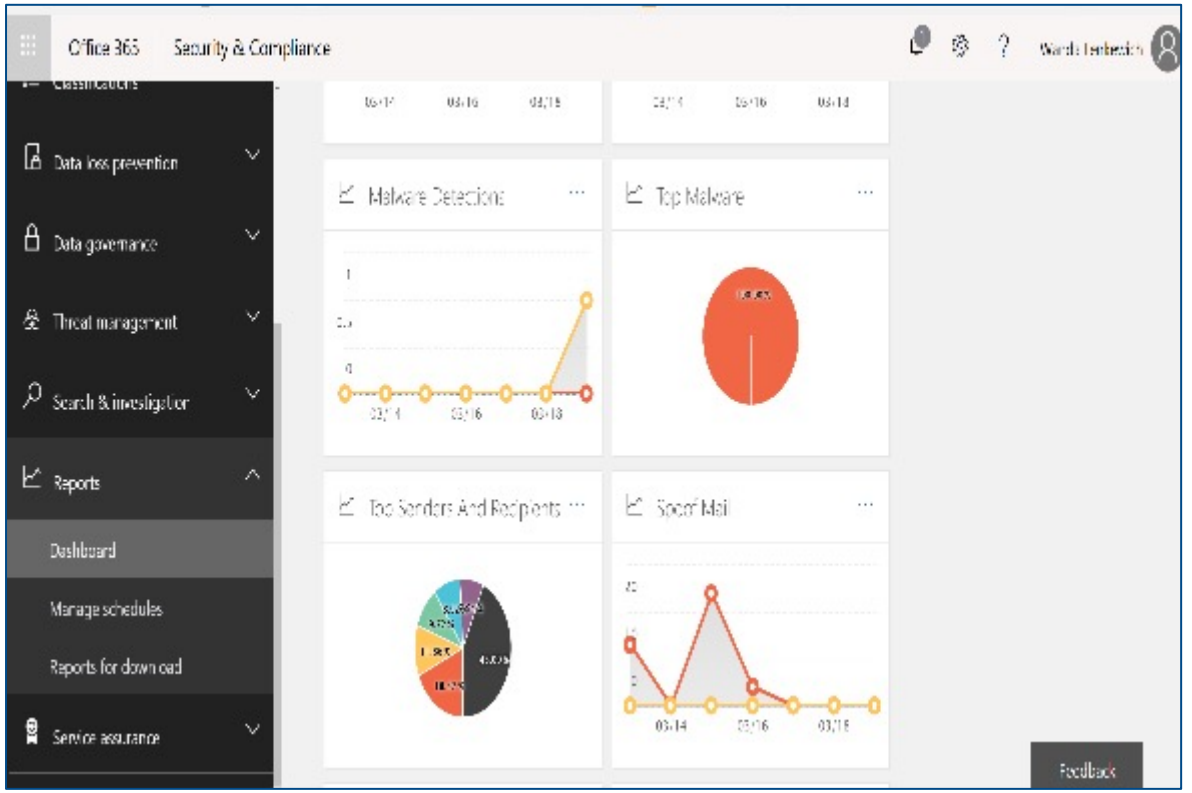
Job Name:	99 - SCHEDULED - Corp Weekly Scan	Scan time:	2019-03-31 15:45:06
Profile:	-	Generated:	2019-04-10 16:35:46

Total number of vulnerabilities identified on 83 system(s)

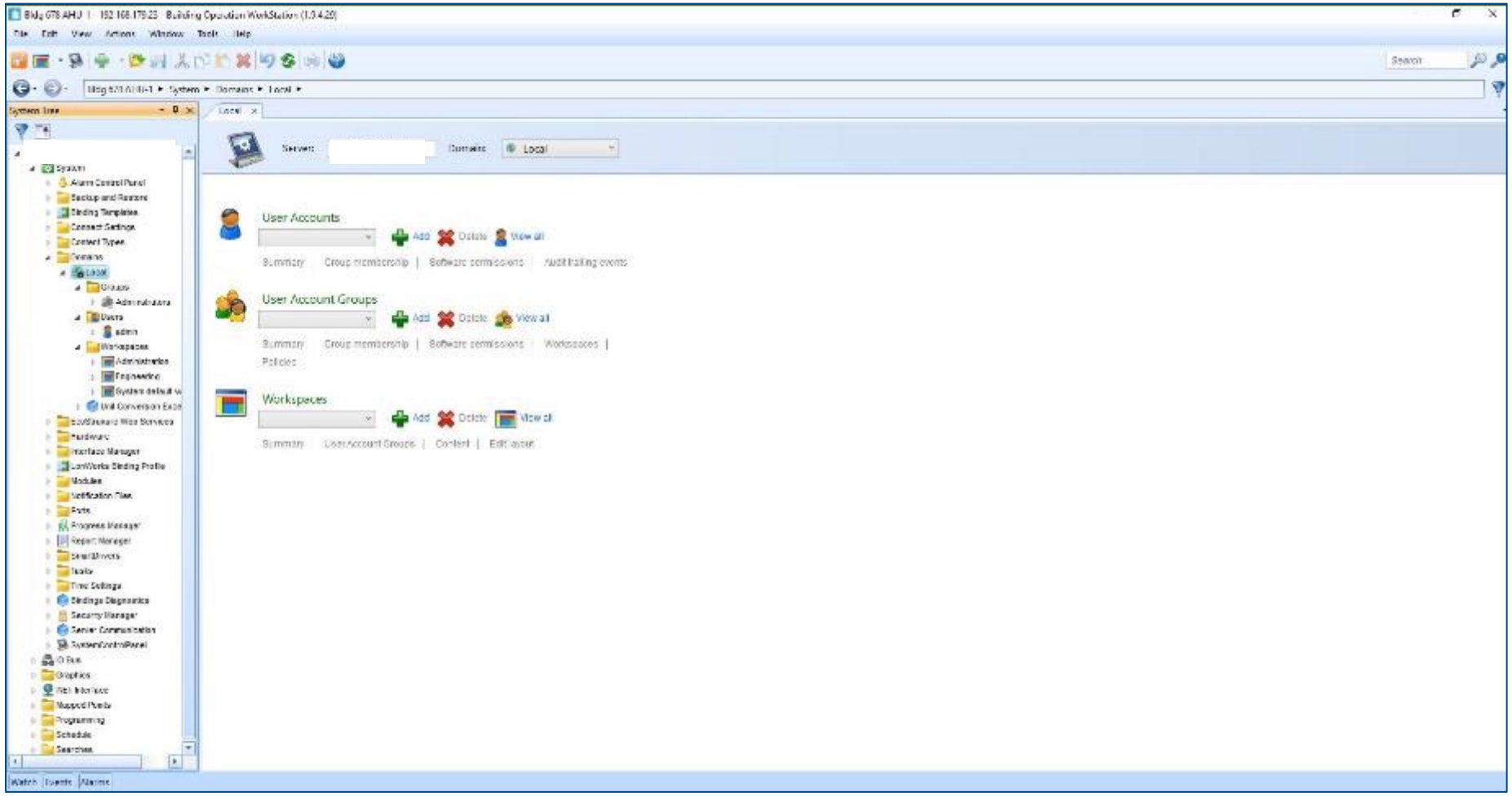


Total number of vulnerabilities identified per system

HostIP	HostName	Serious	High	Med	Low	Info
192.168.1.1	Host-192-168-1-1	--	1	5	--	19
192.168.1.10		--	1	1	--	17
192.168.1.108	Host-192-168-1-108	--	--	1	--	12



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

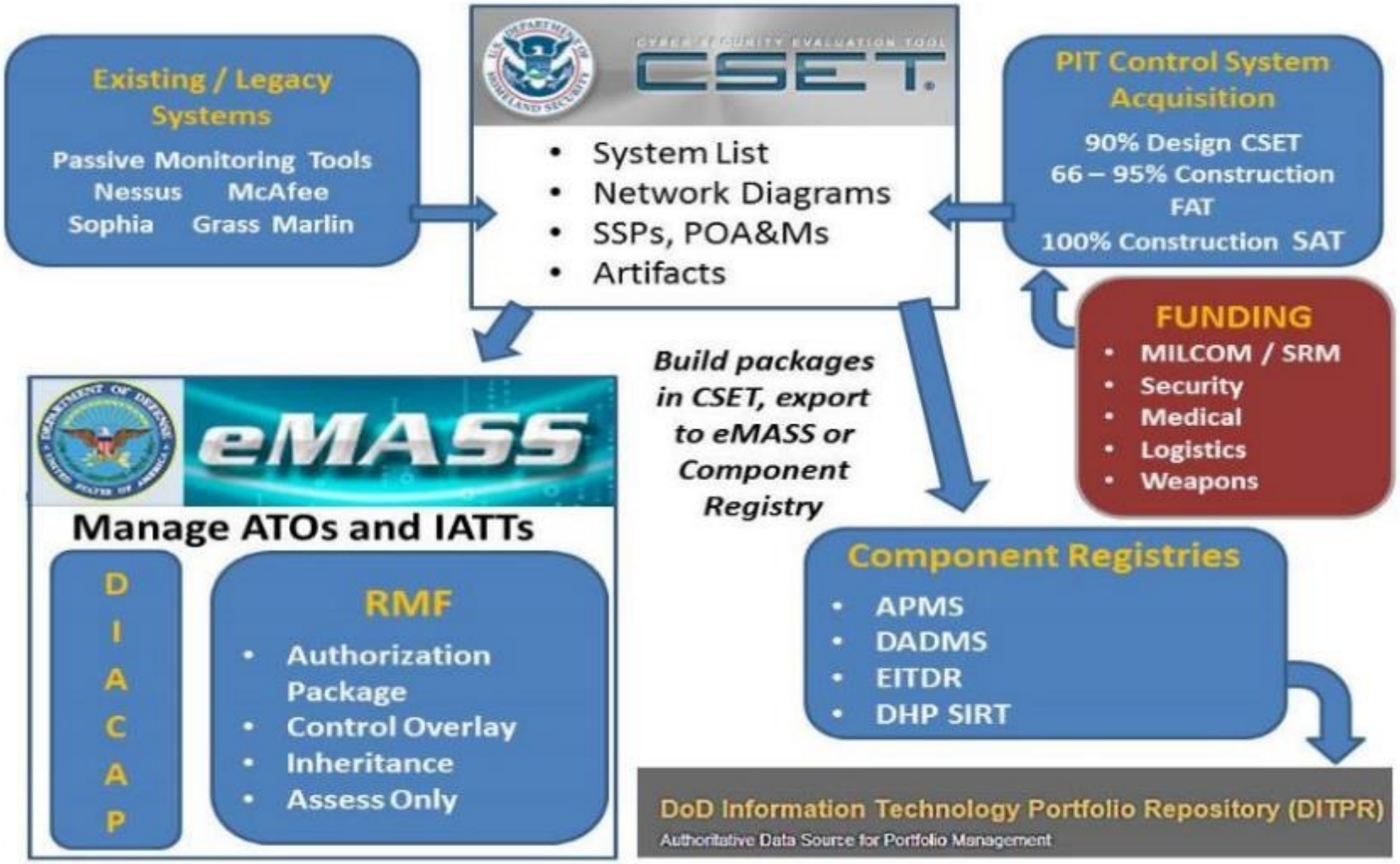
CYBER SECURITY EVALUATION TOOL
CSET®

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

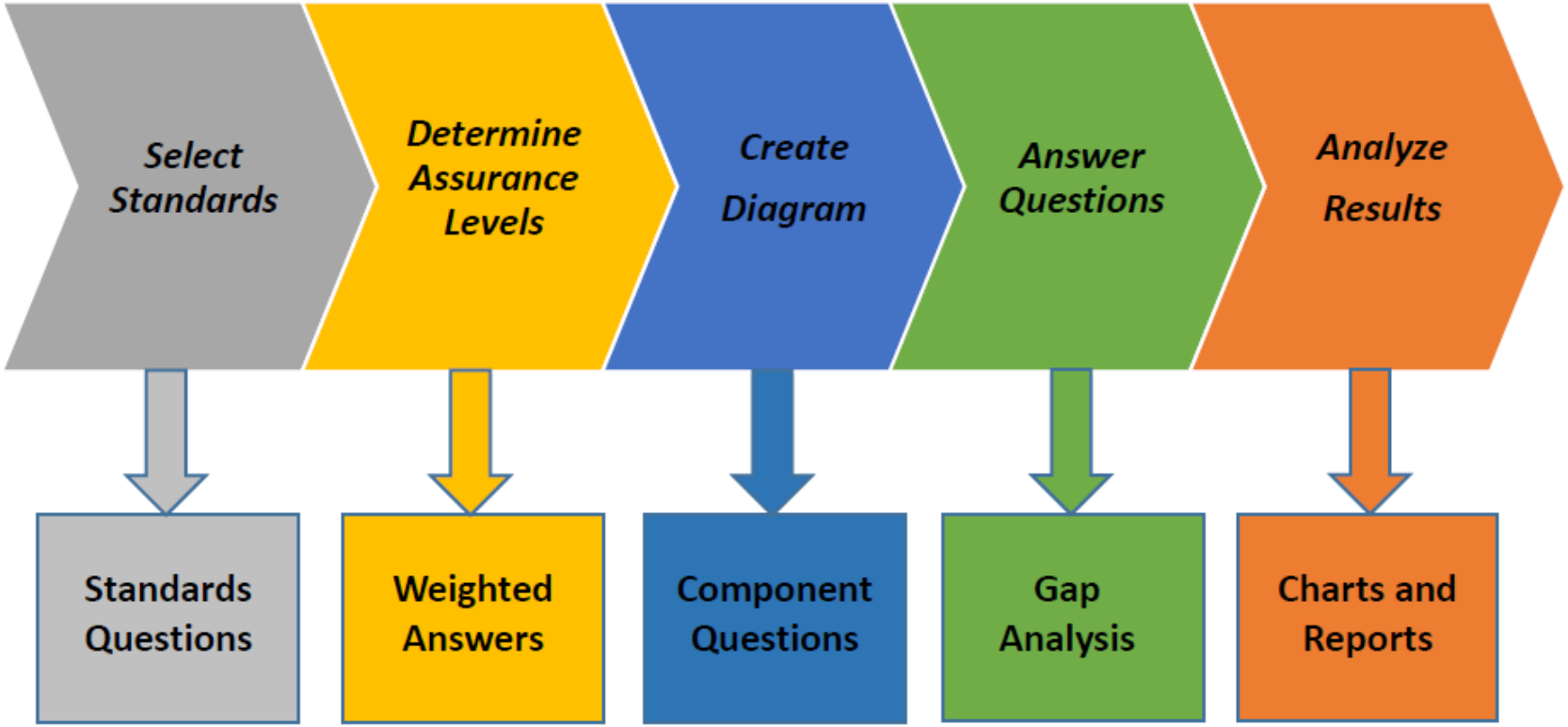


Figure 3-1. CSET process.

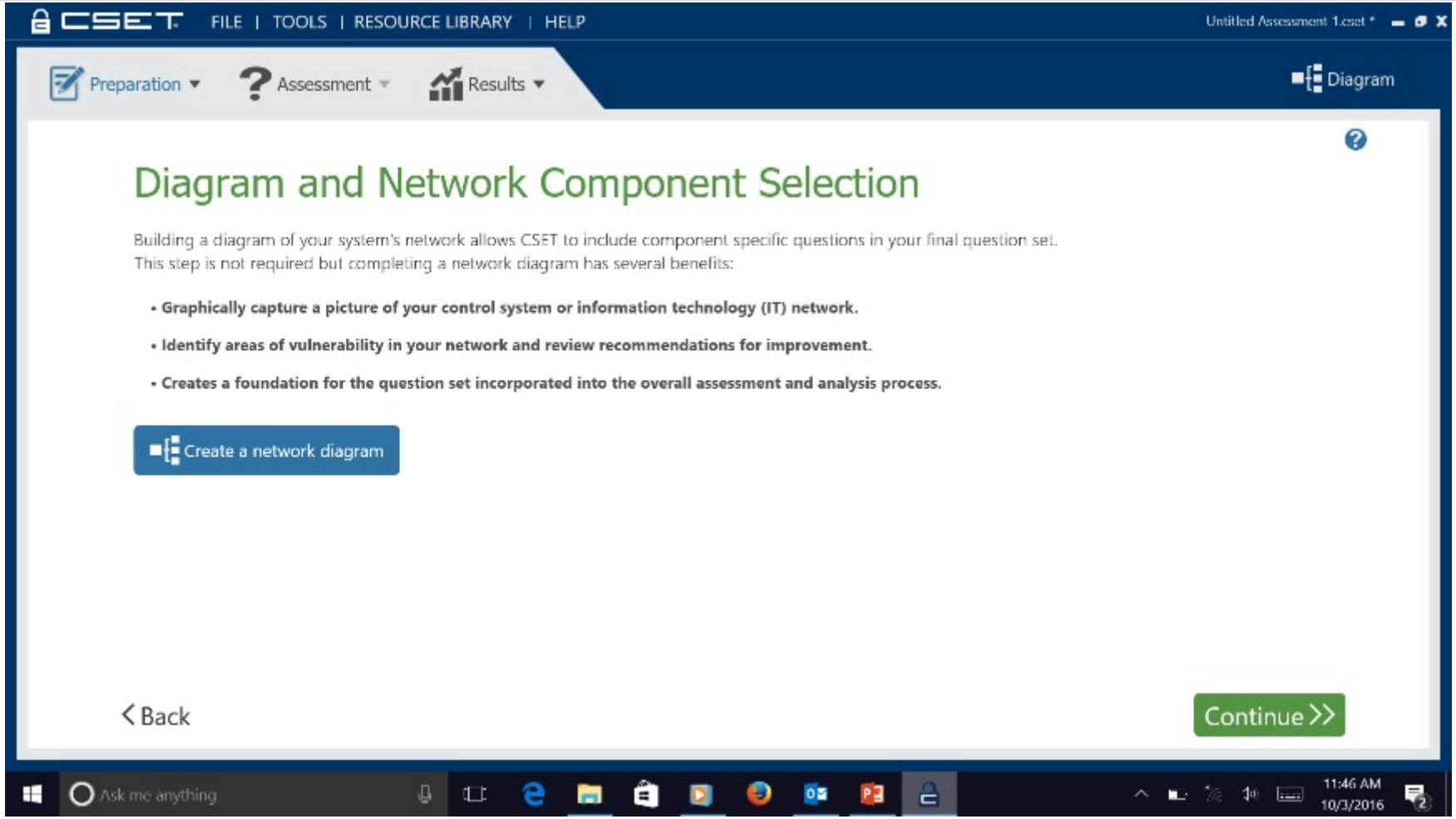
FIPS 199 SAL Impact Levels

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.

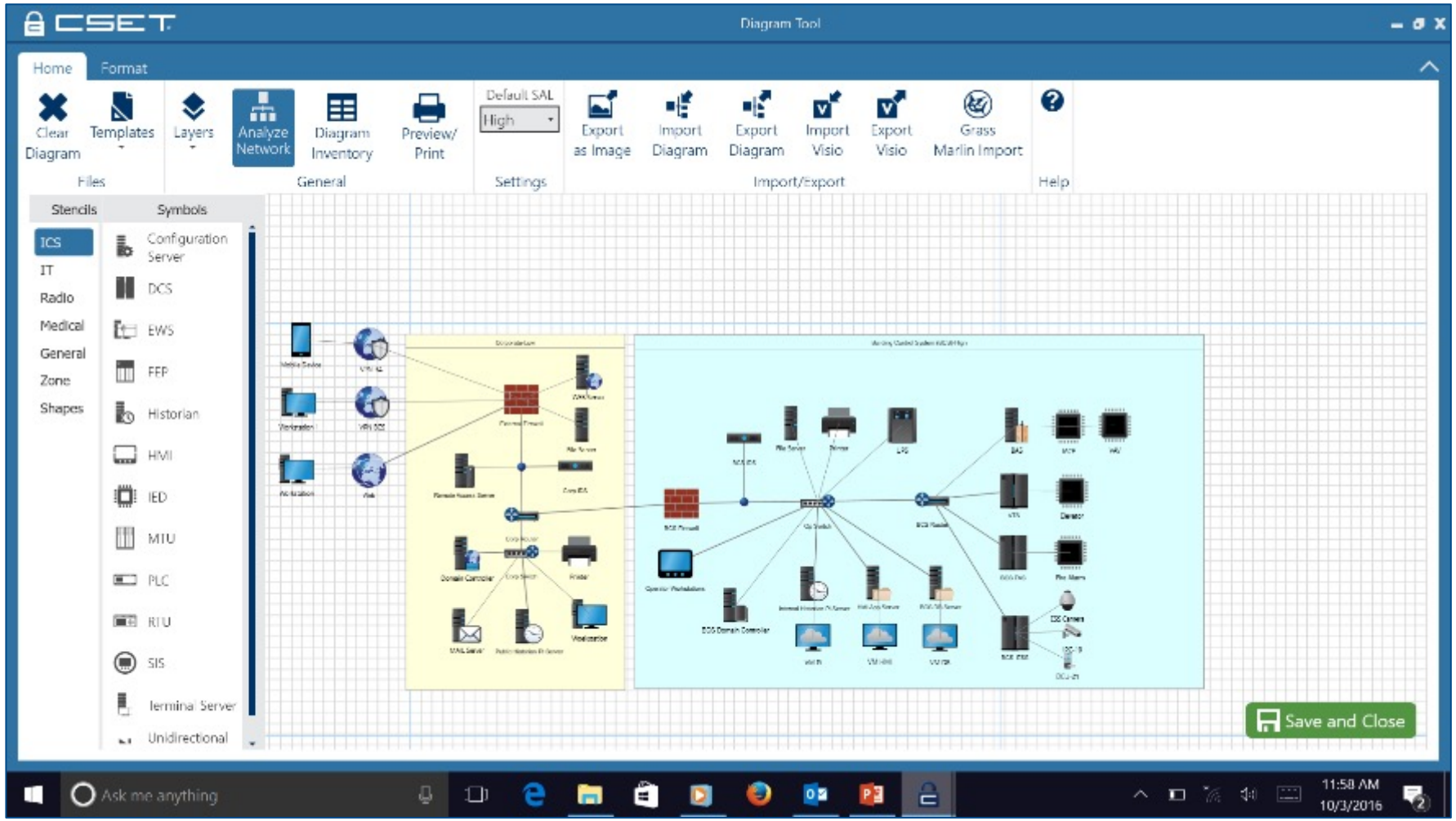
The *potential impact* is **MODERATE** if—
– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
AMPLIFICATION: A serious adverse effect means that, for example, the loss of 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.

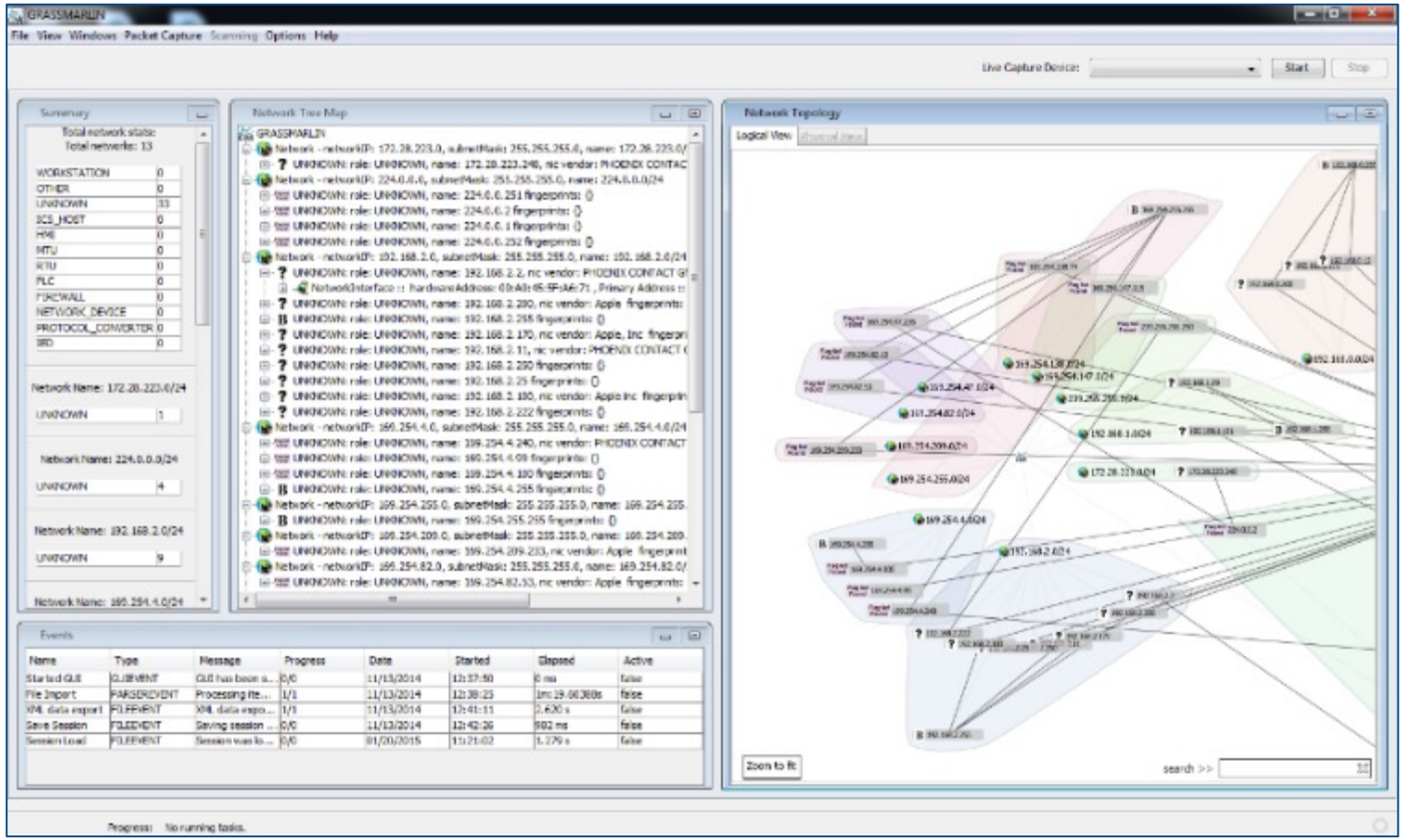
Design and Network Component Selection



CSET 8.1 Network Diagrams



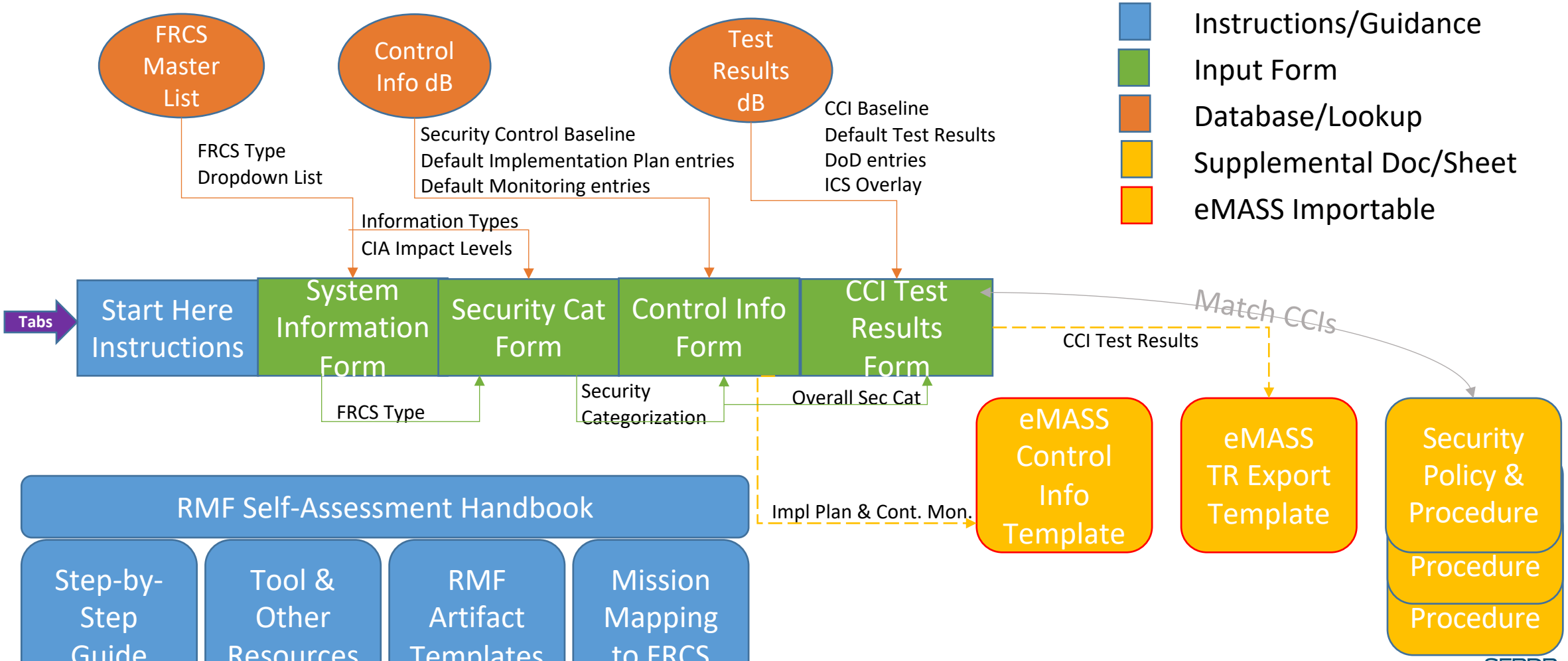
GrassMarlin Plug-In for CSET



Working with other products to get Visio import templates

SERDP • ESTCP SYMPOSIUM
#SerdpEstcp2021

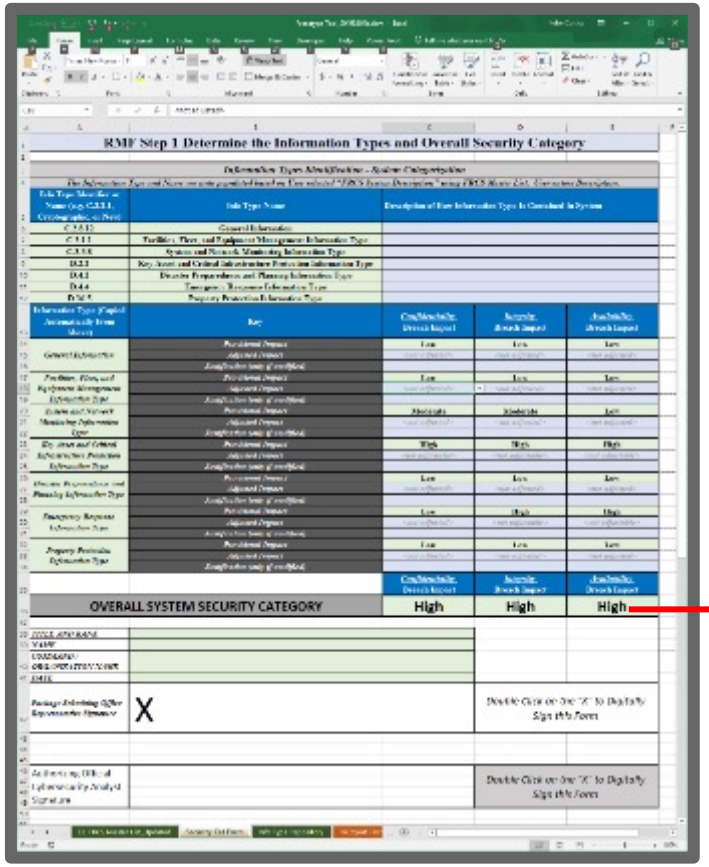
ESTCP FRCS RMF Tool



ESTCP FRCS RMF Tool

Step 3
Implement Controls

CCI Test Results Form


RMF Step 1 Determine the Information Types and Overall Security Category

Info Type Identifier	Info Type Name	Description of How Information Type Is Contained In System
C.3.4.1	Facilities, Fleet, and Equipment Management Information Type	
C.3.5.8	Systems and Network Monitoring Information Type	
D.2.2	Key Asset and Critical Infrastructure Protection Information Type	
D.4.1	Disaster Preparedness and Planning Information Type	
D.4.4	Transport Restoration Information Type	
D.5.1	Property Protection Information Type	

Information Type Provisional Security Impact Level Selected	Key	Confidentiality (Severity/Impact of Breach)	Integrity (Severity/Impact of Breach)	Availability (Severity/Impact of Breach)
		Low	Low	Low
		Low	Low	Low
		Moderate	Moderate	Low
		High	High	High
		Low	Low	Low
		Low	High	High
		Low	Low	Low
	OVERALL SYSTEM SECURITY CATEGORY	High	High	High

X

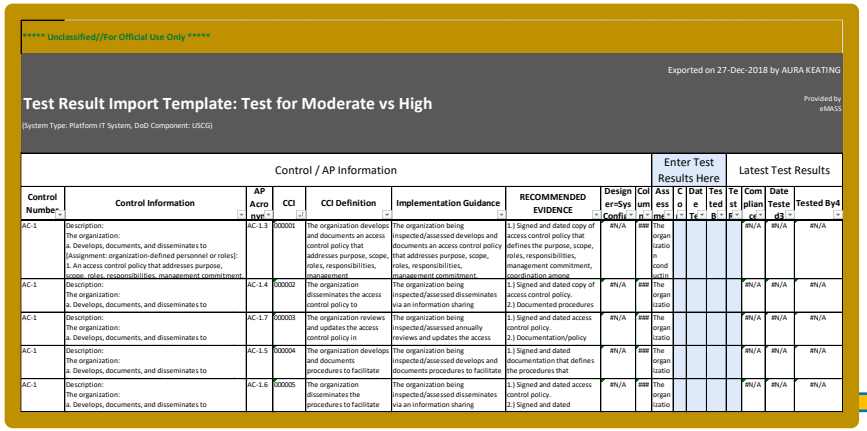
Double Click on the "X" to Digitally Sign this Form

Double Click on the "X" to Digitally Sign this Form

NIST 800-82
800-82 ICS
Overlay

DoD-level Policies

UFC 4-010-


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

Exported on 27-Dec-2018 by AURA KEATING

Test Result Import Template: Test for Moderate vs High

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

Provided by eMASS

Control / AP Information									Enter Test Results Here				Latest Test Results			
Control Number	Control Information	AP Acronym	CCI	CCI Definition	Implementation Guidance	RECOMMENDED EVIDENCE	Designer=System Configuration	Column	Assessment	Comment	Date Tested	Tested By	Compliance	Date Tested	Tested By4
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment	AC-1.3	000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among	1.) Signed and dated copy of access control policy that defines the purpose, scope, roles, responsibilities, management commitment, coordination among	#N/A	###	The organization conducting				#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.4	000002	The organization disseminates the access control policy to	The organization being inspected/assessed disseminates via an information sharing	1.) Signed and dated copy of access control policy. 2.) Documented procedures	#N/A	###	The organizatio				#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.7	000003	The organization reviews and updates the access control policy in	The organization being inspected/assessed annually reviews and updates the access	1.) Signed and dated access control policy. 2.) Documentation/policy	#N/A	###	The organizatio				#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.5	000004	The organization develops and documents procedures to facilitate	The organization being inspected/assessed develops and documents procedures to facilitate	1.) Signed and dated documentation that defines the procedures that	#N/A	###	The organizatio				#N/A	#N/A	#N/A
AC-1	Description: The organization: a. Develops, documents, and disseminates to	AC-1.6	000005	The organization disseminates the procedures to facilitate	The organization being inspected/assessed disseminates via an information sharing	1.) Signed and dated access control policy. 2.) Signed and dated	#N/A	###	The organizatio				#N/A	#N/A	#N/A

eMASS Import of Test Results

Test Result Export Form

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

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

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.

DFARS Technical Information

- Technical data or computer software as defined in DFARS Clause 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in the solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
- **The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.**
- **Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.**

Applying the RMF to Organization IT Systems - CUI

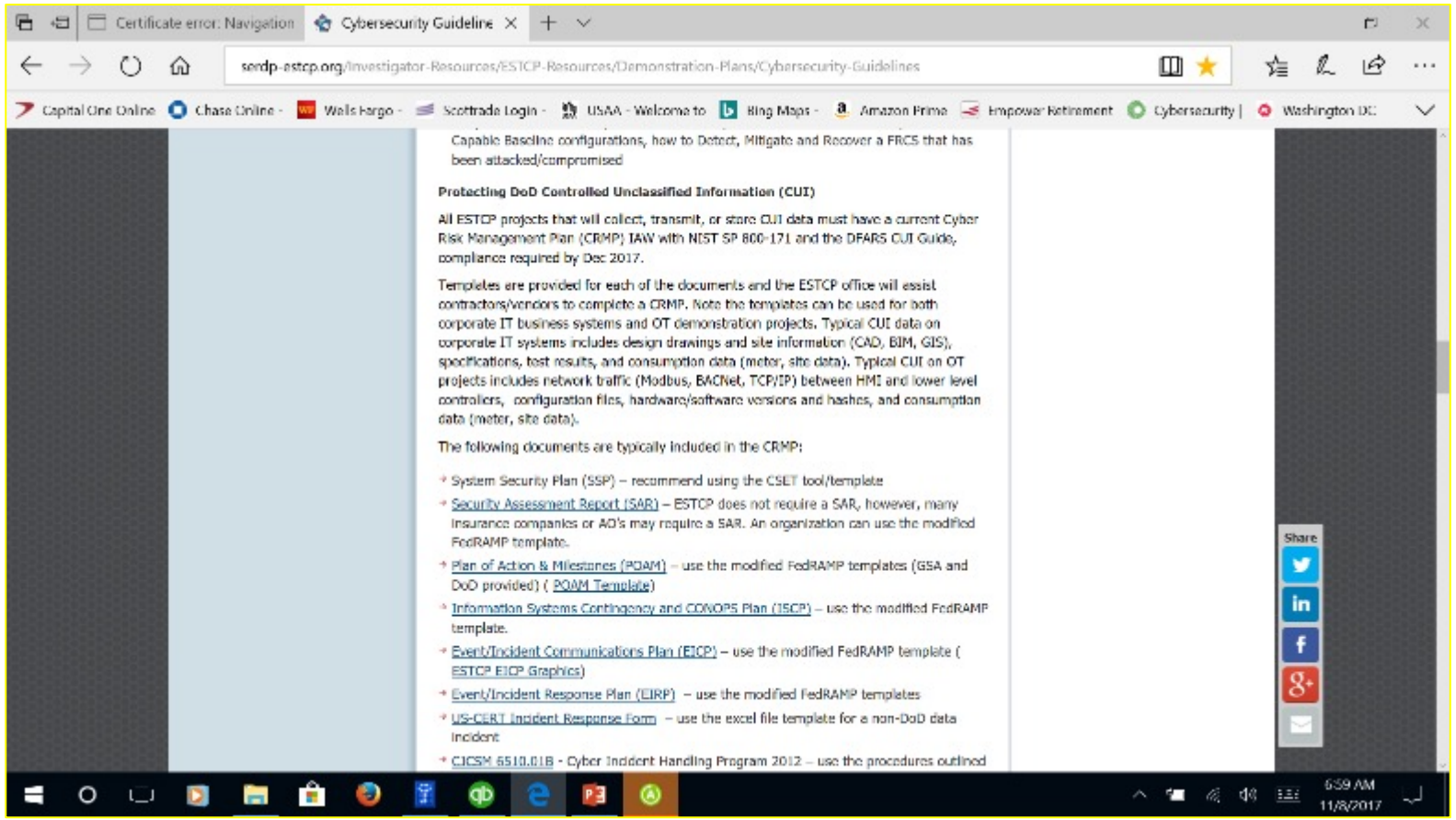
Protecting Controlled Unclassified Information

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).

Applying the RMF to Organization IT Systems - CUI

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



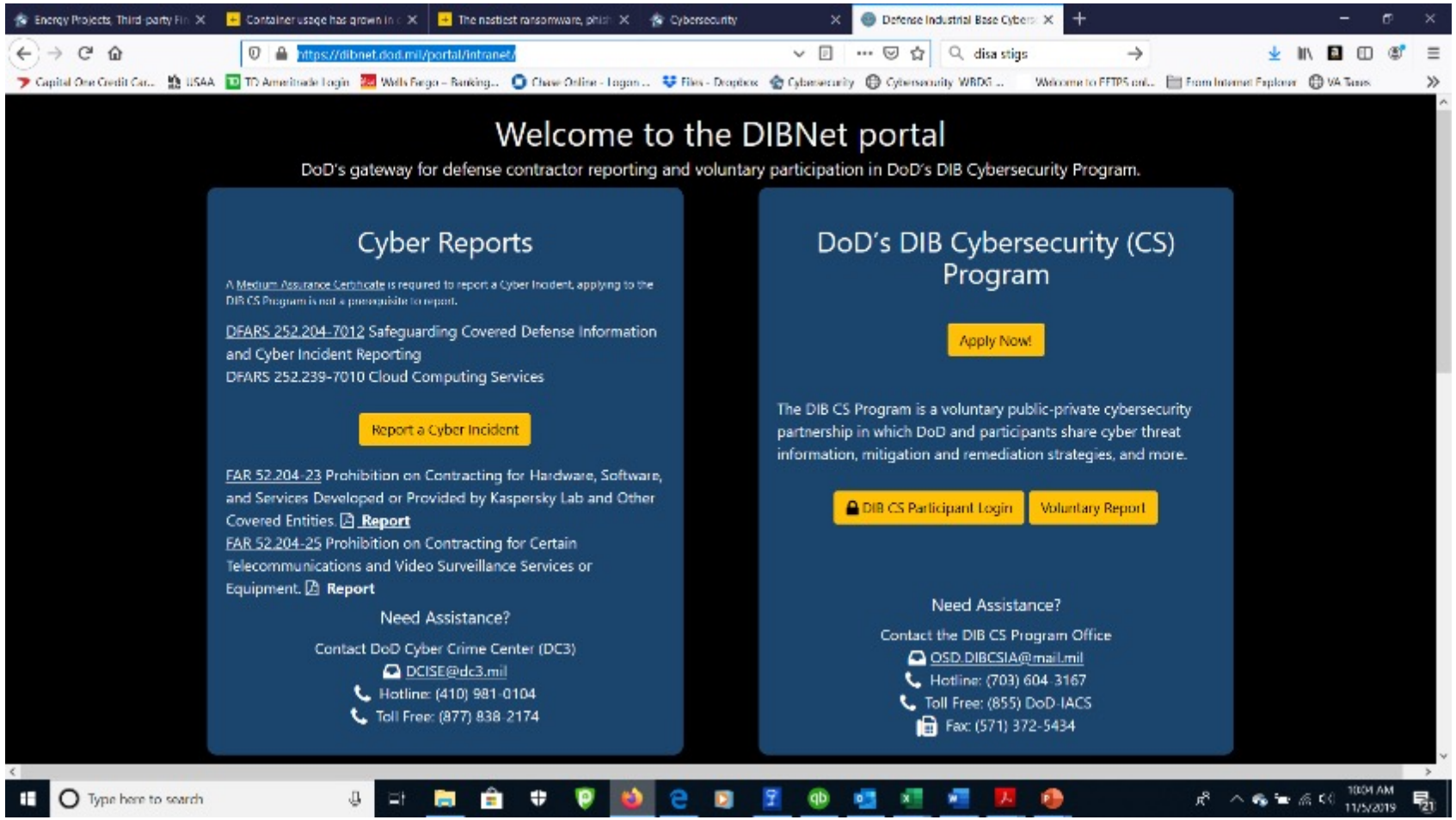
DFARS Guide 2015 Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement – This guidance is intended for stakeholders charged with protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s) covered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

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)

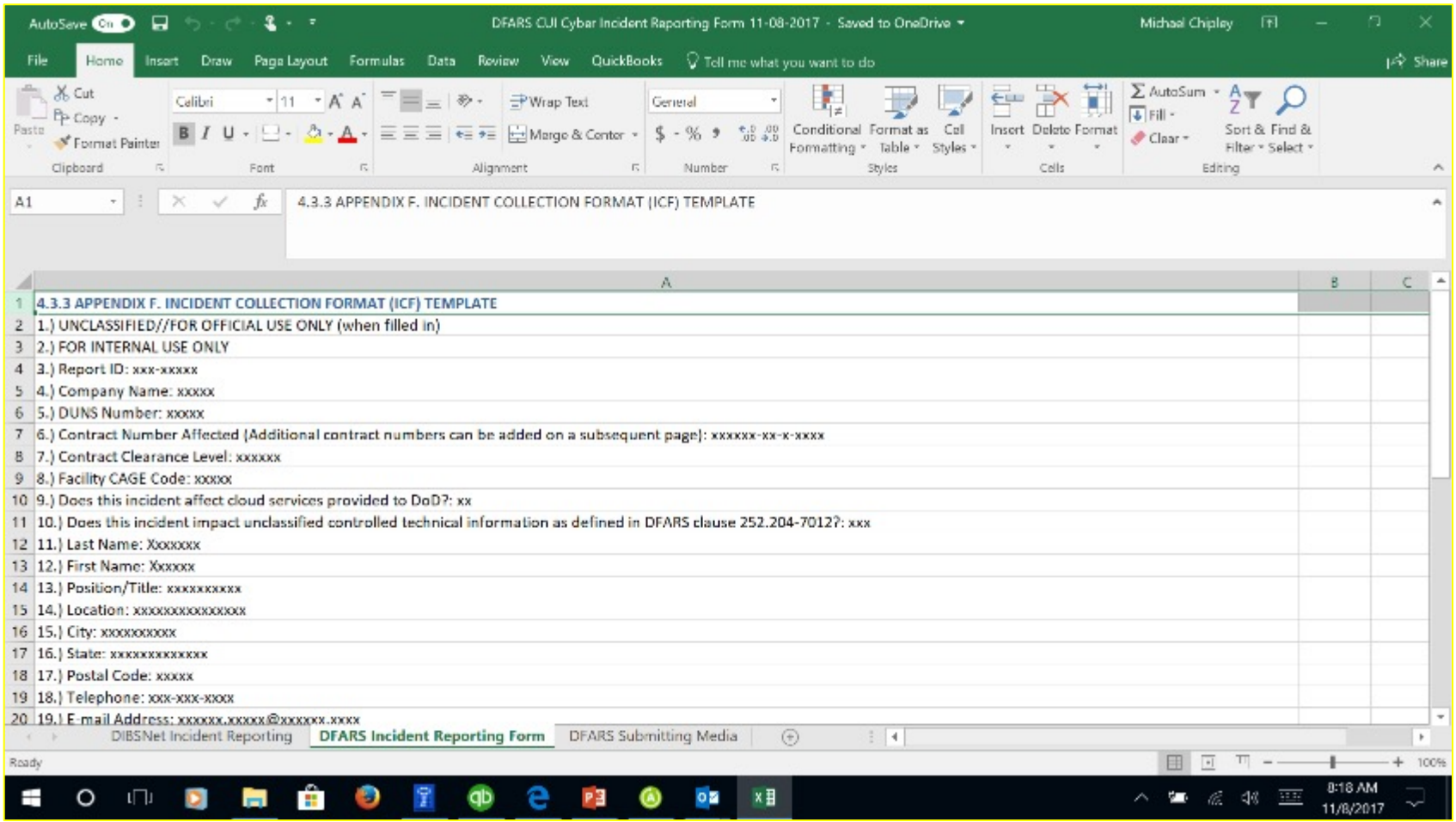
DIBNet Portal to Report Cyber CUI Incidents (CAC Required)



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

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.



DFARS CMMC Interim Rule Nov 30, 2020

Federal Register /Vol. 85, No. 189 /Tuesday, September 29, 2020 /Rules and Regulations **61505**

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS–2020–0034]

RIN 0750–AJ81

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DATES: Effective November 30, 2020.

Comments on the interim rule should be submitted in writing to the address shown below on or before November 30, 2020, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019–D041, using any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Search for ''DFARS Case 2019–D041''. Select ''Comment Now'' and follow the instructions provided to submit a comment. Please include ''DFARS Case 2019–D041'' on any attached documents.
- *Email: osd.dfars@mail.mil.* Include DFARS Case 2019–D041 in the subject line of the message.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571–372–6104.

SUPPLEMENTARY INFORMATION:

I. Background

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. As part of multiple lines of effort focused on the security and resiliency of the Defense Industrial Base (DIB) sector, the Department is working with industry to enhance the protection of unclassified information within the supply chain. Toward this end, DoD has developed the following assessment methodology and framework to assess contractor implementation of cybersecurity requirements, both of which are being implemented by this rule: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The NIST SP 800–171 DoD Assessment and CMMC assessments will not duplicate efforts from each assessment, or any other DoD assessment, except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

A. NIST SP 800–171 DoD Assessment Methodology

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, except for acquisitions solely for commercially available off-the-shelf (COTS) items. The clause requires contractors to apply the security requirements of NIST SP 800–171 to ''covered contractor information systems,'' as defined in the clause, that are not part of an IT service or system operated on behalf of the Government. The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204–7012. More information on the NIST SP 800–171 DoD Assessment Methodology is available at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

The Assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The results of Assessments are documented in the Supplier Performance Risk System (SPRS) at *https://www.sprs.csd.disa.mil/* to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (*i.e.,* not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

B. Cybersecurity Maturity Model Certification Framework

Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC levels and the associated sets of processes and practices are cumulative. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204–21, Basic Safeguarding of Covered

Contractor Information Systems, and the security requirements for CUI specified in NIST SP 800–171 per DFARS clause 252.204–7012. Furthermore, the CMMC model includes an additional five processes and 61 practices across Levels 2–5 that demonstrate a progression of cybersecurity maturity.

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. CMMC assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs). Upon completion of a CMMC assessment, a company is awarded a certification by an independent CMMC Accreditation Body (AB) at the appropriate CMMC level (as described in the CMMC model). The certification level is documented in SPRS to enable the verification of an offeror's certification level and currency (*i.e.* not more than three years old) prior to contract award. Additional information on CMMC and a copy of the CMMC model can be found at *https://www.acq.osd.mil/cmmc/index.html.*

DoD is implementing a phased rollout of CMMC. Until September 30, 2025, the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment.

CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. Contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (*i.e.* not older than three years) certification for the required CMMC level. Furthermore, CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

II. Discussion and Analysis

A. NIST SP 800–171 DoD Assessment Methodology

This rule amends DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting, to implement the NIST SP 800–171 DoD Assessment Methodology. The new coverage in the subpart directs contracting officers to verify in SPRS that an offeror has a current NIST SP 800–171 DoD Assessment on record, prior to contract award, if the offeror is required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012. The contracting officer is also directed to include a new DFARS provision 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, and a new DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in solicitations and contracts including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

The new DFARS provision 252.204–7019 advises offerors required to implement the NIST SP 800–171 standards of the requirement to have a current (not older than three years) NIST SP 800–171 DoD Assessment on record in order to be considered for award. The provision requires offerors to ensure the results of any applicable current Assessments are posted in SPRS and provides offerors with additional information on conducting and submitting an Assessment when a current one is not posted in SPRS.

The new DFARS clause 252.204–7020 requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments. The clause also provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments.

B. Cybersecurity Maturity Model Certification

This rule adds a new DFARS subpart, Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC), to specify the policy and procedures for awarding a contract, or exercising an option on a contract, that includes the requirement for a CMMC certification. Specifically, this subpart directs contracting officers to verify in SPRS that the apparently successful offeror's or contractor's CMMC certification is current and meets the required level prior to making the award.

A new DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments.

The Department took into consideration the timing of the requirement to achieve a CMMC level certification in the development of this rule, weighing the benefits and risks associated with requiring CMMC level certification: (1) At time of proposal or offer submission; (2) at time of award;

DFARS Case 2019–D041

SERDP • ESTCP SYMPOSIUM

#SerdpEstcp2021

Implementing the New DFARS 7012

The top five NAICS code industries expected to be impacted by this rule are as follows: **541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services.** These NAICS codes are the same as the DoD Assessment NAICS codes and were selected based on a review of NAICS codes associated with awards that include the clause at FAR 52.204–21 or DFARS 252.204–7012.

1. DoD Assessment Methodology

To comply with NIST SP 800–171 a company must (1) implement 110 security requirements on their covered contractor information systems; or (2) document in a ‘‘system security plan’’ and ‘‘plans of action’’ those requirements that are not yet implemented and when the requirements will be implemented. All offerors that are required to implement NIST SP 800–171 on covered contractor information systems pursuant to DFARS clause 252.204–7012, **will be required to complete a Basic Assessment and upload the resulting score to the Supplier Risk Management System (SPRS),** DoD’s authoritative source for supplier and product performance information.

Guidance for Assessing Compliance

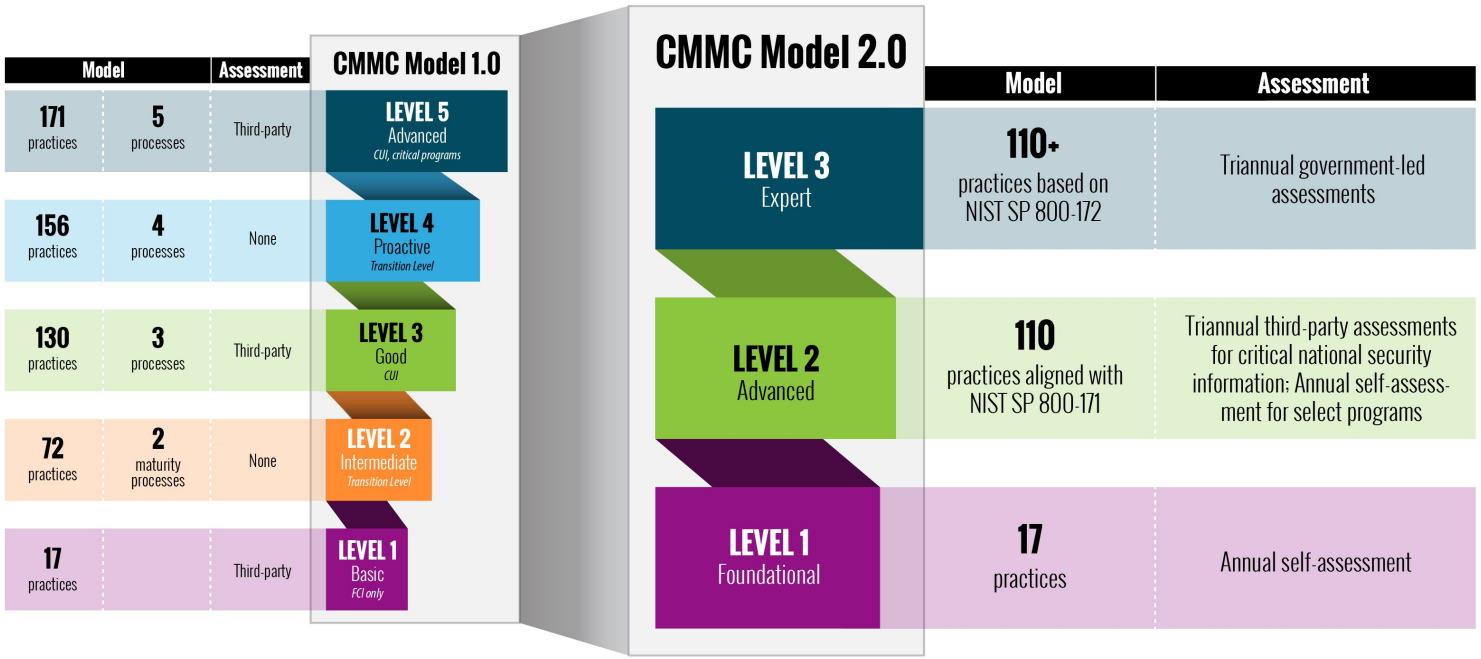
November 6, 2018

GUIDANCE FOR ASSESSING COMPLIANCE OF AND ENHANCING PROTECTIONS FOR A CONTRACTOR'S INTERNAL UNCLASSIFIED INFORMATION SYSYEM

(REQUIRES NEGOTIATION OF TERMS/COSTS ON A CONTRACT-BY-CONTRACT BASIS)

	OBJECTIVE	SOLICITATION	SOURCE SELECTION	CONTRACT
Pre-Award (Solicitation and Source Selection)				
1	Contractor 'self-attests' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171 (Status Quo with DFARS 252.204-7008)	Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012		Section I: • DFARS Clause 252.204-7012
2	Require enhanced cybersecurity measures in addition to the security requirements in NIST SP 800-171 to safeguard information stored on the contractor's internal unclassified information system	Section C: • Include Statement of Work referencing DoD approved list of enhanced security requirements Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012 Section L: • Describe contractor implementation of additional requirements Section M: • Detail specifics of how additional requirements will be evaluated	Evaluate offeror's proposed implementation of protections required in addition to NIST SP 800-171 in accordance with the specifics of how additional requirements will be evaluated as documented in Section M	Section C: • Include Statement of Work referencing a DoD approved list of enhanced security requirements Section I: • DFARS Clause 252.204-7012

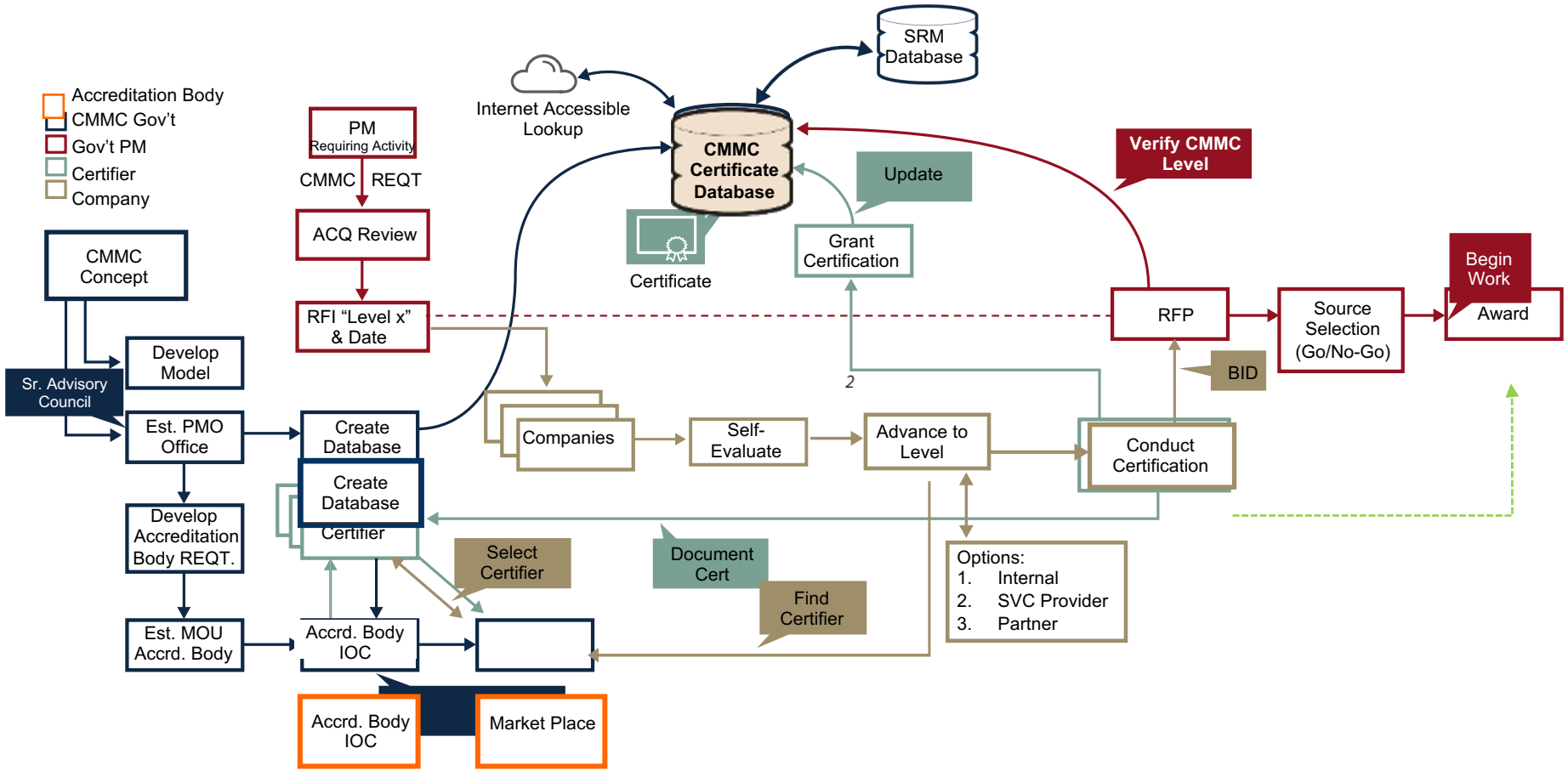
CMMC 2.0 – Nov 2021



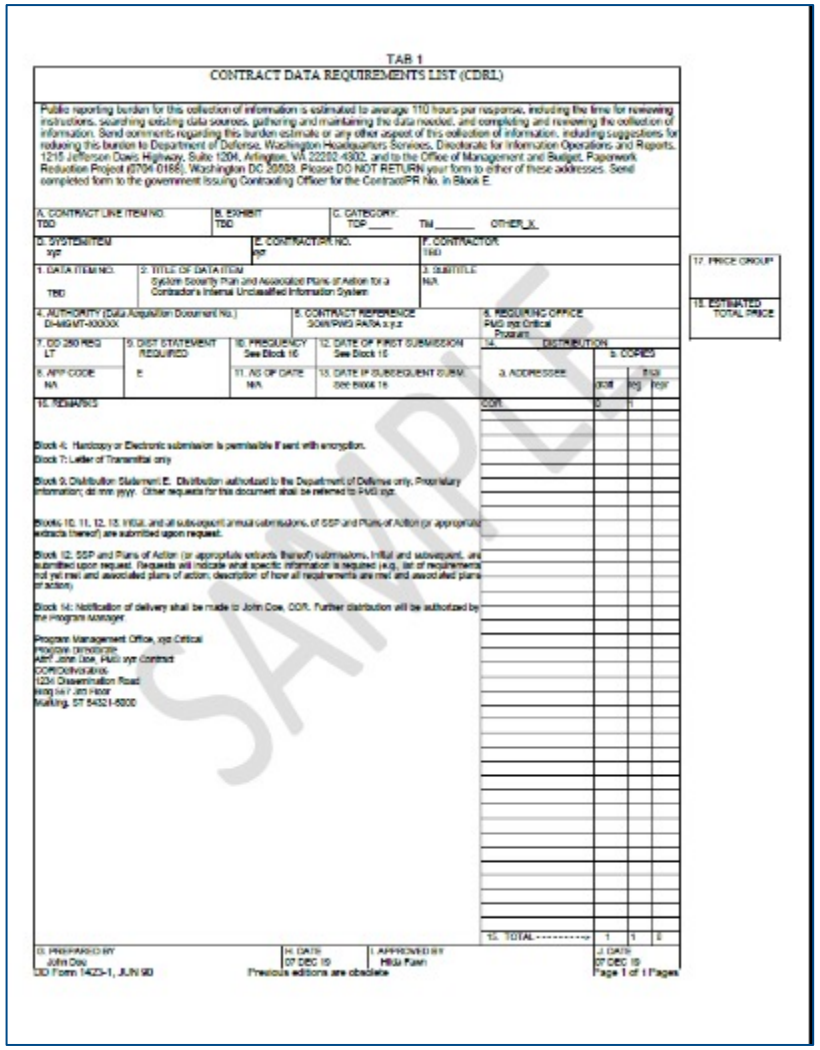
b) allow companies associated with the new Level 1 (Foundational) and some Level 2 (Advanced) acquisition programs to perform self-assessments rather than third-party assessments

Spirit of collaboration: Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification

CMMC Implementation Flow



Contract Data Requirements



TAB 1

CONTRACT DATA REQUIREMENTS LIST (CDRL)

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed form to the government Issuing Contracting Officer for the Contract/PR No. in Block E.

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
TBD	TBD	TDP ____ TM _____ OTHER X

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
xyz	xyz	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
TBD	System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System	N/A

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-MGMT-XXXXX	SOW/PWS PARA x.y.z	PMO xyz Critical Program

7. DD 250 REQ	8. DIST STATEMENT REQUIRED	9. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
LT	E	See Block 16	See Block 16	a. ADDRESSEE

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBM
N/A	N/A	See Block 16

b. COPIES	Draft	Reg	Final
COR	0	1	

16. REMARKS

Block 4: Hardcopy or Electronic submission is permissible if sent with encryption.

Block 7: Letter of Transmittal only

Block 9: Distribution Statement E. Distribution authorized to the Department of Defense only; Proprietary information; dd mm yyyy. Other requests for this document shall be referred to PMO xyz.

Blocks 10, 11, 12, 13: Initial and all subsequent annual submissions, of SSP and Plans of Action (or appropriate extracts thereof) are submitted upon request.

Block 12: SSP and Plans of Action (or appropriate extracts thereof) submissions, initial and subsequent, are submitted upon request. Requests will indicate what specific information is required (e.g., list of requirements not yet met and associated plans of action; description of how all requirements are met and associated plans of action)

Block 14: Notification of delivery shall be made to John Doe, COR. Further distribution will be authorized by the Program Manager

Program Management Office, xyz Critical
Program Developer
Attn: John Doe, PMO xyz Contract
COR/Divisions
1234 Dissemination Road
Bldg 567 Jim Floor
Mailing, ST 54321-6000

15. TOTAL ---------- 1 1 0

10. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
John Doe	07 DEC 19	Mike Fawn	07 DEC 19

DD Form 1423-1, JUN 90 Previous editions are obsolete Page 1 of 1 Pages

17. PRICE GROUP

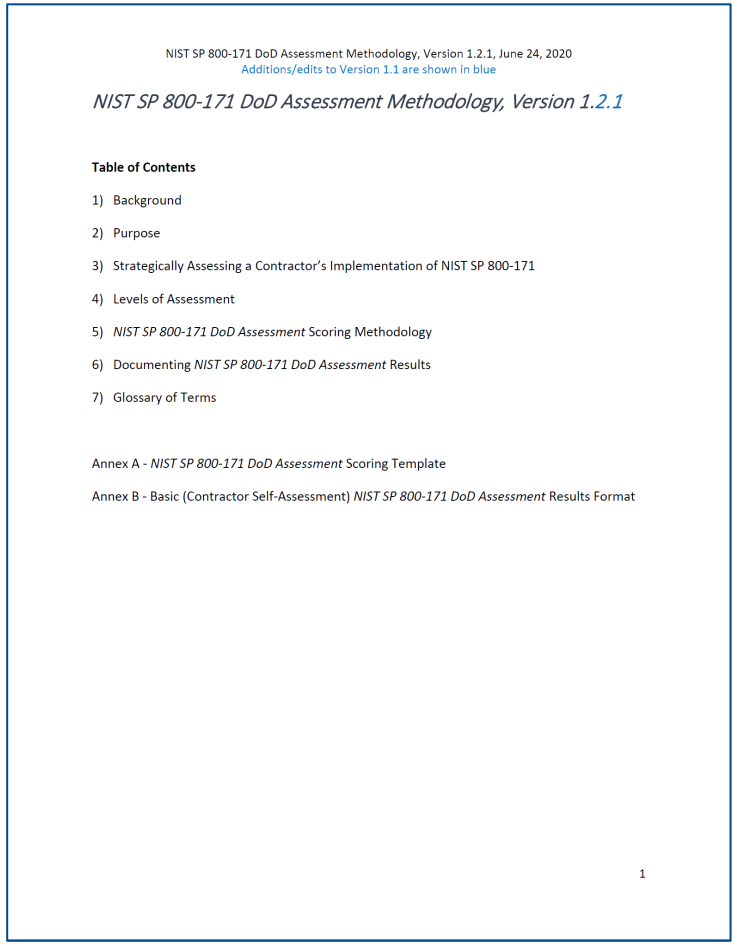
18. ESTIMATED TOTAL PRICE

SAMPLE

Blocks 10, 11, 12, 13: Initial, and all subsequent annual submissions, of SSP and Plans of Action (or appropriate extracts thereof) are submitted **upon request**.

Block 12: SSP and Plans of Action (or appropriate extracts thereof) submissions, initial and subsequent, are submitted upon request. Requests will indicate what specific information is required (e.g., list of requirements not yet met and associated plans of action; description of how all requirements are met and associated plans of action)

DOD Assessment Methodology



NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020
Additions/edits to Version 1.1 are shown in blue

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1

Table of Contents

1) Background
2) Purpose
3) Strategically Assessing a Contractor's Implementation of NIST SP 800-171
4) Levels of Assessment
5) *NIST SP 800-171 DoD Assessment* Scoring Methodology
6) Documenting *NIST SP 800-171 DoD Assessment* Results
7) Glossary of Terms

Annex A - *NIST SP 800-171 DoD Assessment* Scoring Template

Annex B - Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment* Results Format

1

Conduct of the NIST SP 800-171 DoD Assessment will result in a score reflecting the net effect of security requirements not yet implemented. **If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements.** For each security requirement not met, the associated value is subtracted from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

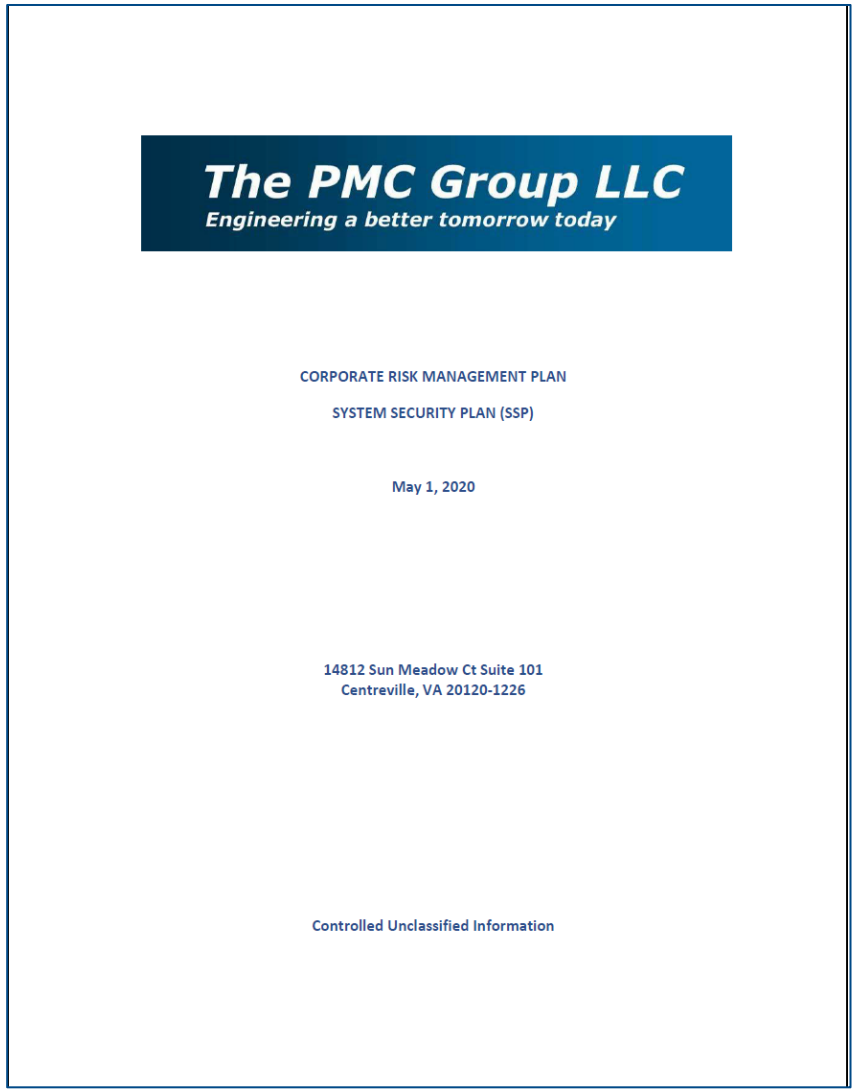
DOD Assessment Methodology

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020
Additions/edits to Version 1.1 are shown in blue

Annex A - *NIST SP 800-171 DoD Assessment* **Scoring Template**

- The following template illustrates the scoring methodology described in Section 5. If all requirements are met, a score of 110 is awarded. For each requirement not met, the associated value is subtracted from 110. Consistency results from the fact that the assessments are based on what is not yet implemented, or document that all requirements have been met.
- It is important to note an assessment is about the extent to which the company has implemented the requirements. It is not a value judgement about the specific approach to implementing – in other words, all solutions that meet the requirements are acceptable. This is not an assessment of one solution compared to another.
- Scoring for Basic, Medium, and High *NIST SP 800-171 DoD Assessments* is the same.
- While NIST does not prioritize requirements in terms of impact, certain requirements do have more impact than others. In this scoring methodology security requirements are weighted based on their effect on the information system and DoD CUI created on or transiting that system.

System Security Plan (SSP)



The PMC Group LLC
Engineering a better tomorrow today

CORPORATE RISK MANAGEMENT PLAN

SYSTEM SECURITY PLAN (SSP)

May 1, 2020

14812 Sun Meadow Ct Suite 101
Centreville, VA 20120-1226

Controlled Unclassified Information

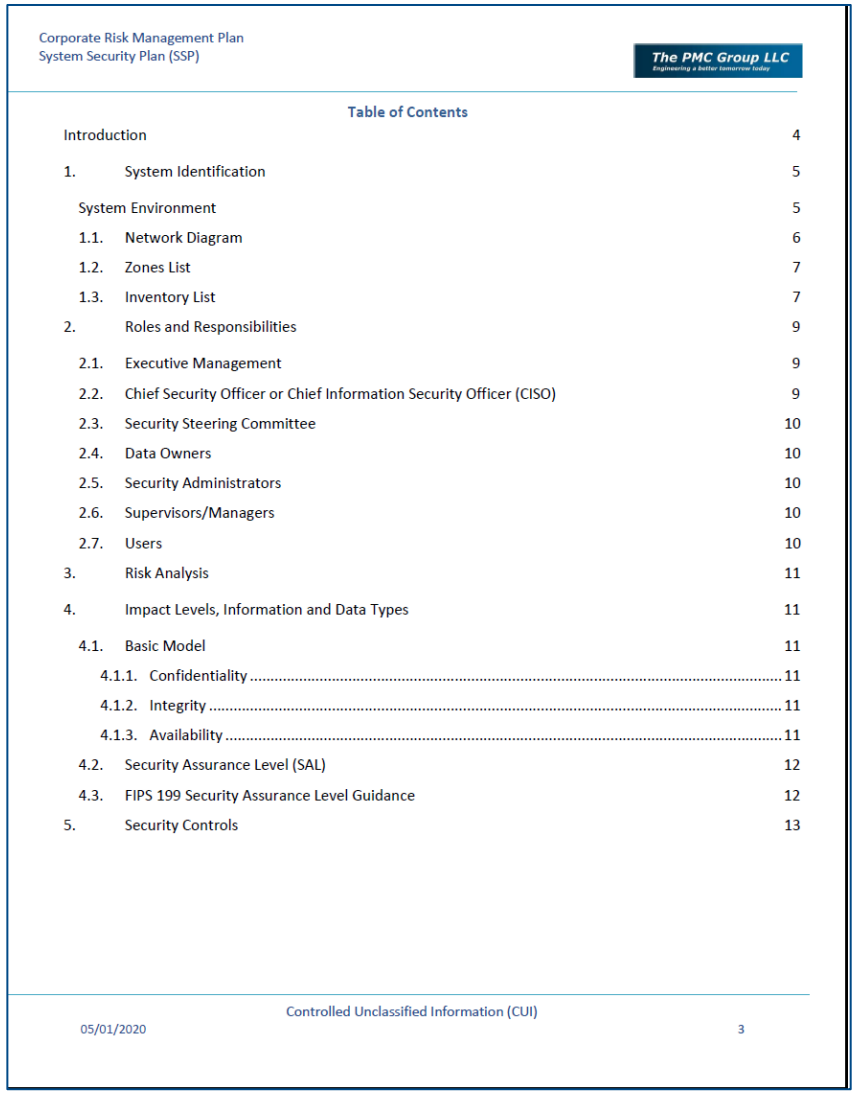
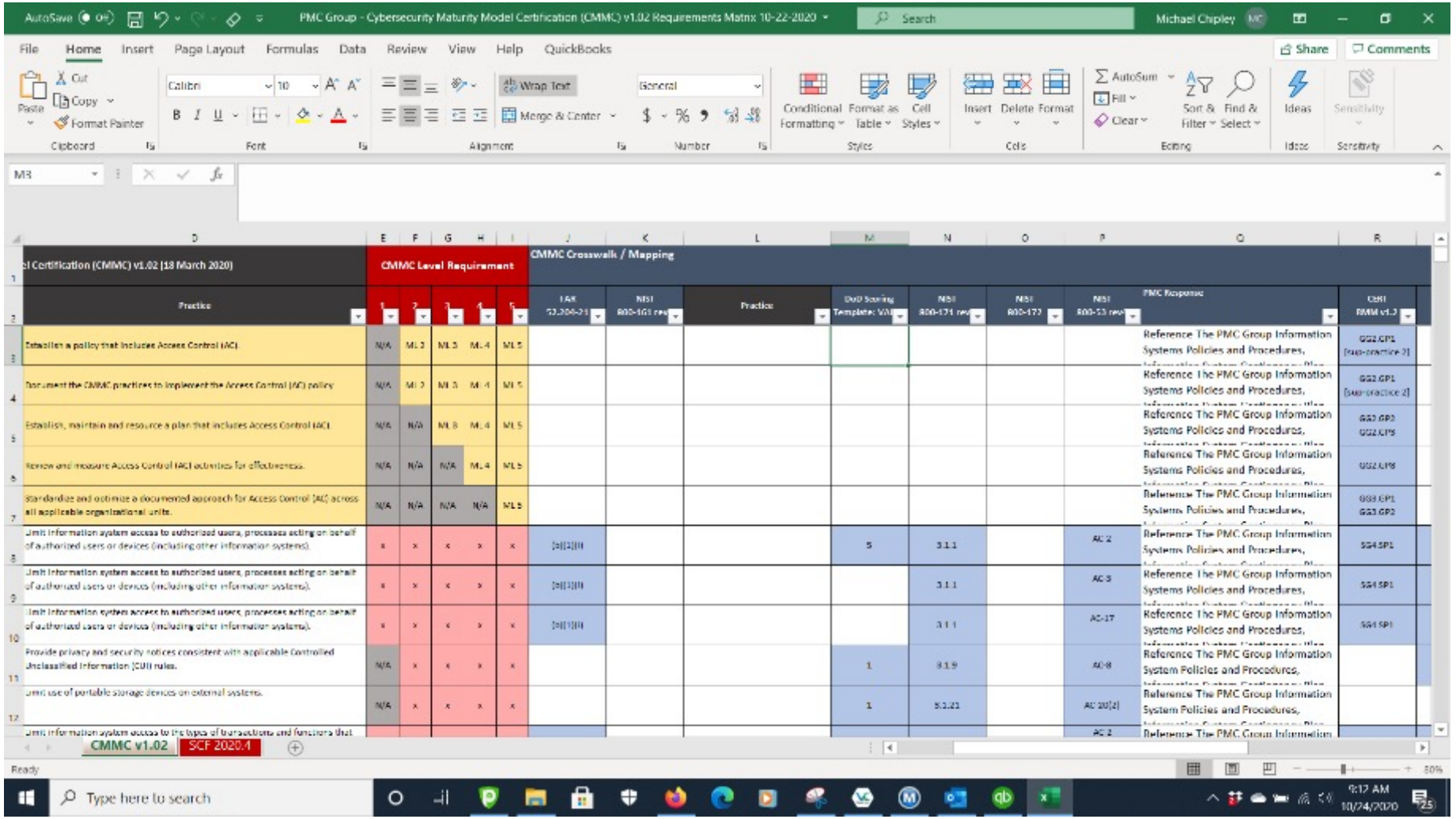


Table of Contents

Introduction 4
1. System Identification 5
System Environment 5
1.1. Network Diagram 6
1.2. Zones List 7
1.3. Inventory List 7
2. Roles and Responsibilities 9
2.1. Executive Management 9
2.2. Chief Security Officer or Chief Information Security Officer (CISO) 9
2.3. Security Steering Committee 10
2.4. Data Owners 10
2.5. Security Administrators 10
2.6. Supervisors/Managers 10
2.7. Users 10
3. Risk Analysis 11
4. Impact Levels, Information and Data Types 11
4.1. Basic Model 11
4.1.1. Confidentiality 11
4.1.2. Integrity 11
4.1.3. Availability 11
4.2. Security Assurance Level (SAL) 12
4.3. FIPS 199 Security Assurance Level Guidance 12
5. Security Controls 13

SSP CMMC Security Controls Matrix

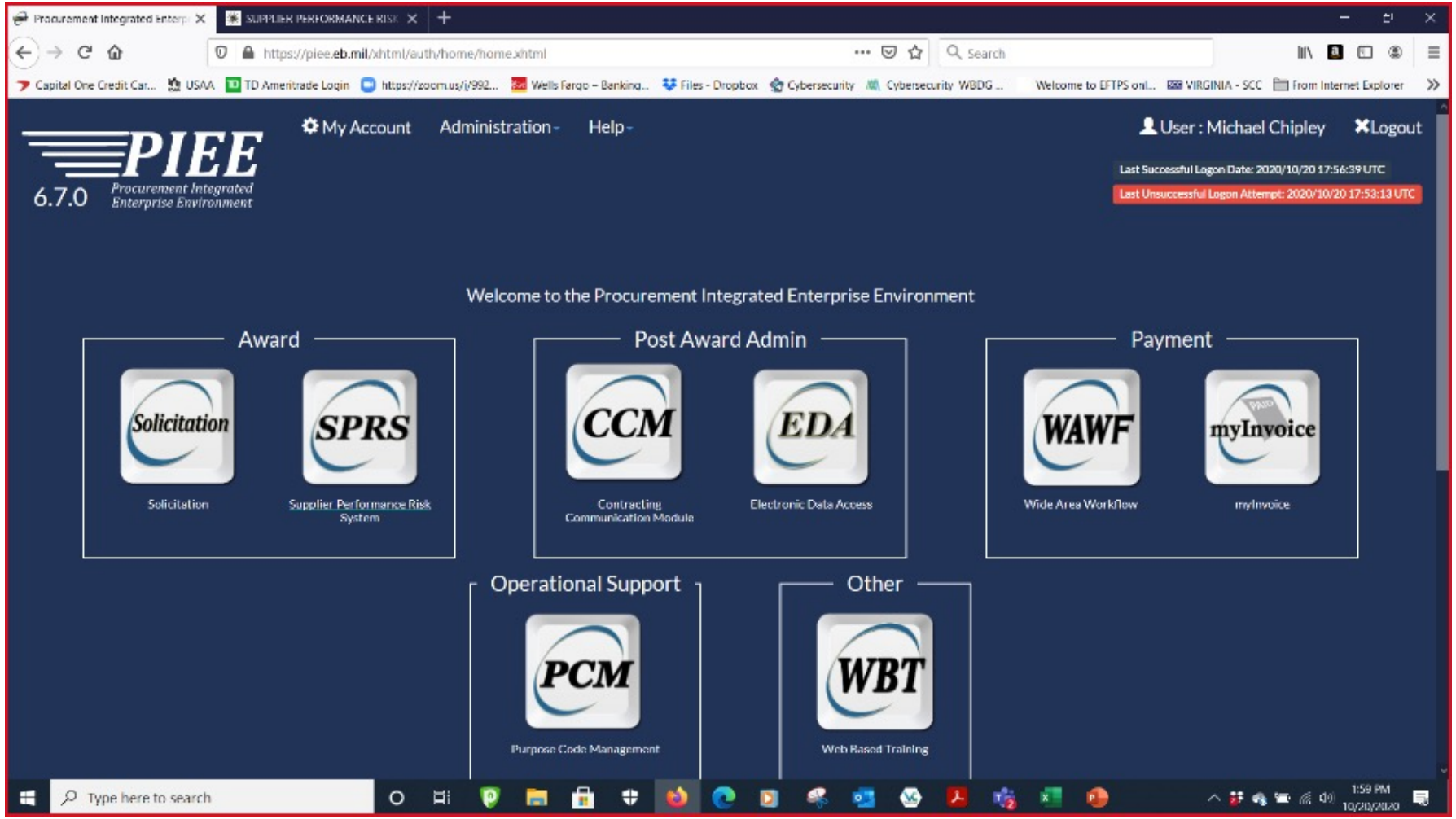


Implementing the New DFARS 7012

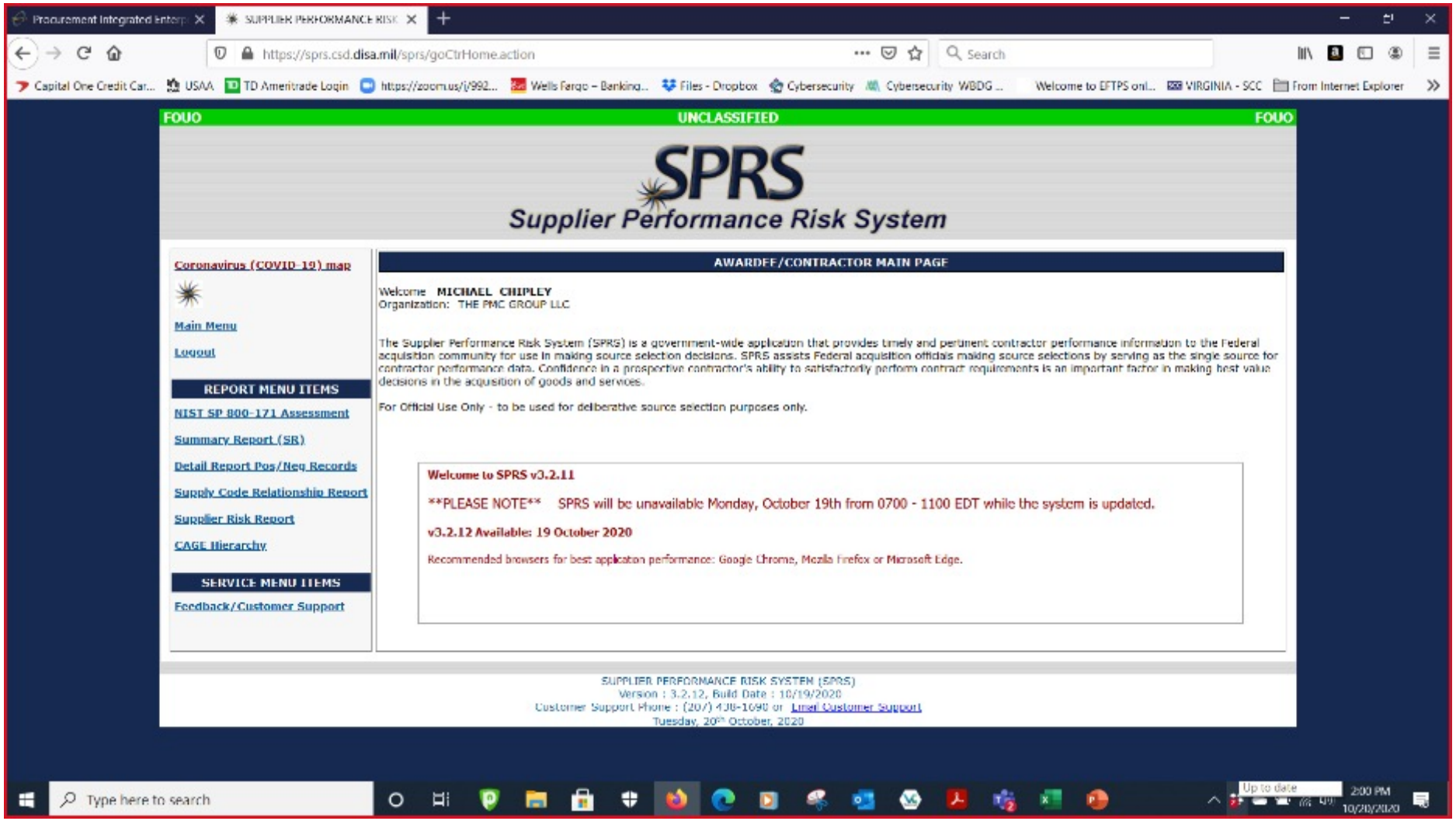
Implementing the new DFARS 7012 Requirements

1. If you do not have a PIEE account, you will need to create the account and have Systems Administrator rights, call 866-618-5988
2. Call the PIEE Help Desk to have the Supplier Performance Reporting System (SPRS) added to your account, add as a System Administrator
3. **Input score of 110 and date of completion**

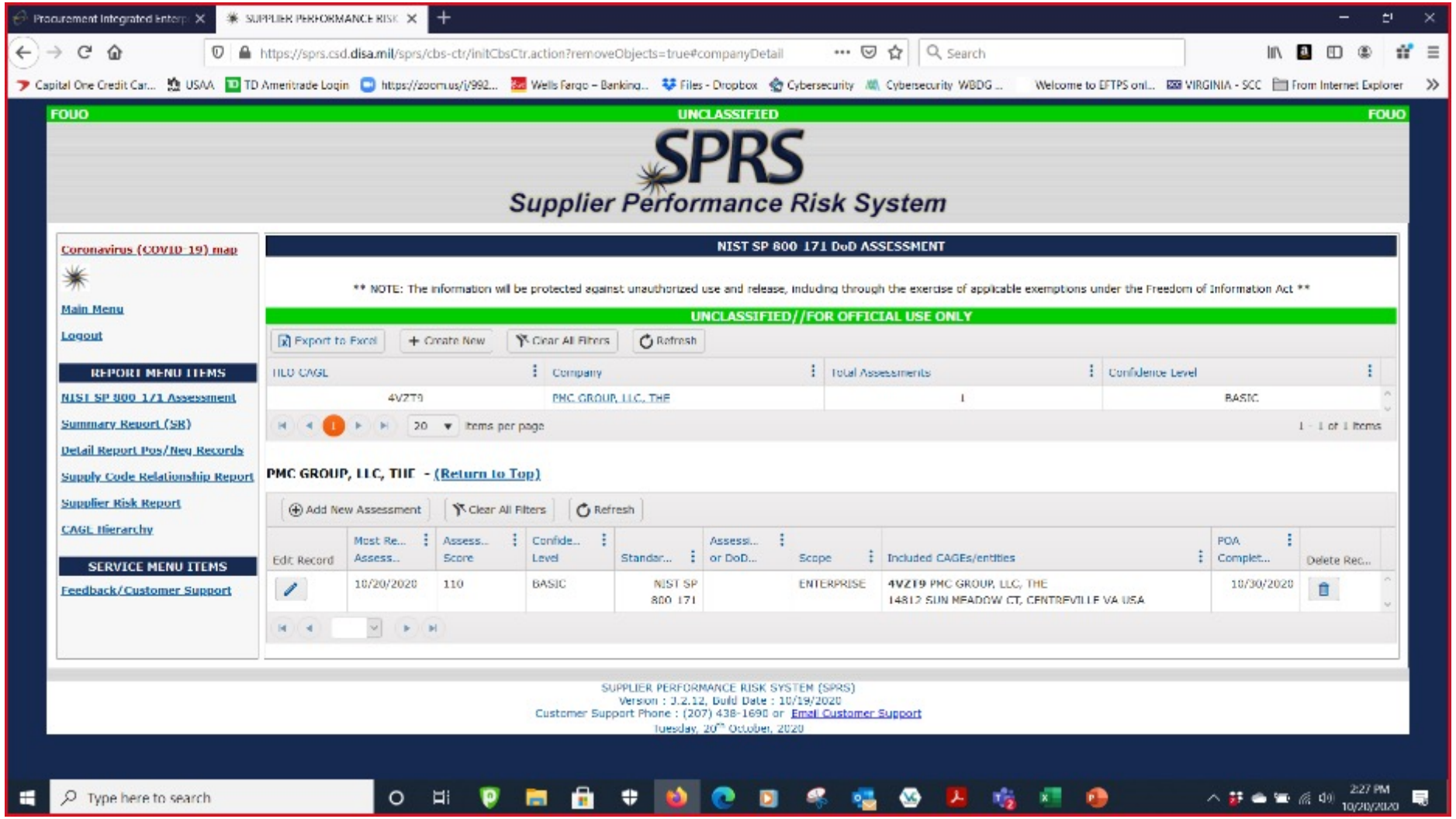
DOD PIEE Portal



DOD SPRS Portal

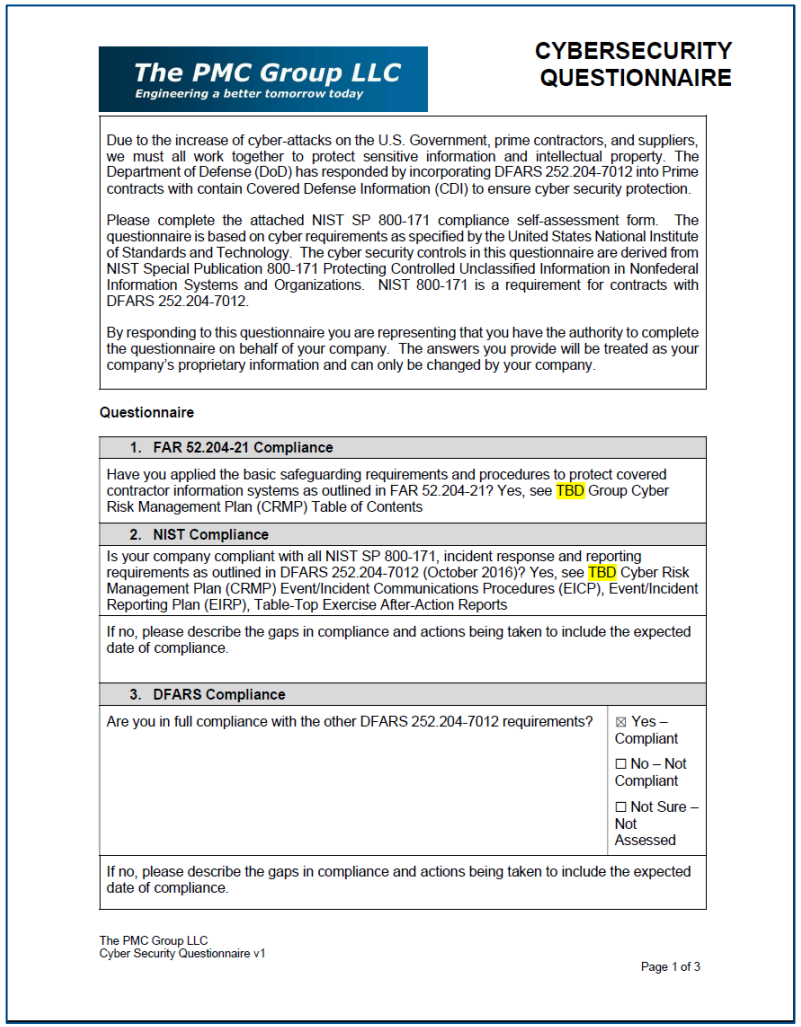


SPRS NIST SP 800-171 Basic Complete



SERDP • ESTCP SYMPOSIUM
#SerdpEstcp2021

Security Questionnaire and Self-Attest Letter



The PMC Group LLC
Engineering a better tomorrow today

CYBERSECURITY QUESTIONNAIRE

Due to the increase of cyber-attacks on the U.S. Government, prime contractors, and suppliers, we must all work together to protect sensitive information and intellectual property. The Department of Defense (DoD) has responded by incorporating DFARS 252.204-7012 into Prime contracts with contain Covered Defense Information (CDI) to ensure cyber security protection.

Please complete the attached NIST SP 800-171 compliance self-assessment form. The questionnaire is based on cyber requirements as specified by the United States National Institute of Standards and Technology. The cyber security controls in this questionnaire are derived from NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST 800-171 is a requirement for contracts with DFARS 252.204-7012.

By responding to this questionnaire you are representing that you have the authority to complete the questionnaire on behalf of your company. The answers you provide will be treated as your company's proprietary information and can only be changed by your company.

Questionnaire

1. FAR 52.204-21 Compliance	
Have you applied the basic safeguarding requirements and procedures to protect covered contractor information systems as outlined in FAR 52.204-21? Yes, see TBD Group Cyber Risk Management Plan (CRMP) Table of Contents	
2. NIST Compliance	
Is your company compliant with all NIST SP 800-171, incident response and reporting requirements as outlined in DFARS 252.204-7012 (October 2016)? Yes, see TBD Cyber Risk Management Plan (CRMP) Event/Incident Communications Procedures (EICP), Event/Incident Reporting Plan (EIRP), Table-Top Exercise After-Action Reports	
If no, please describe the gaps in compliance and actions being taken to include the expected date of compliance.	
3. DFARS Compliance	
Are you in full compliance with the other DFARS 252.204-7012 requirements?	☒ Yes – Compliant ☐ No – Not Compliant ☐ Not Sure – Not Assessed
If no, please describe the gaps in compliance and actions being taken to include the expected date of compliance.	

The PMC Group LLC
Cyber Security Questionnaire v1

Page 1 of 3

The PMC Group LLC
Engineering a better tomorrow today

DoD CUI SELF-ATTESTATION LETTER DECLARATION OF CONFORMITY

The PMC Group LLC
14812 Sun Meadow Ct
Suite 101
Centreville, VA 20120-1226

Dear TBD Contracting Office:

The PMC Group LLC has reviewed *NIST Special Publication 800-171* and based on the evidence provided in the supporting documents attached, has determined that The PMC Group LLC corporate IT systems meet the DoD DFARS 7012 Cyber Risk Management Plan (CRMP) requirements. The following documents are included in The PMC Group LLC CRMP:

- *Corporate Risk Management Plans*
- *Corporate All-Hazards Risk Management Plan*
- *Corporate All-Hazards Risk Management Plan Excel Scoring Matrix*
- *DoD DFARS Controlled Unclassified Information 2015*
- *Corporate Information Systems Plans and Procedures (ISPP)*
  - *Roles and Responsibilities*
  - *Information Security Program Management*
  - *Acceptable Encryption*
  - *Account Management*
  - *Audit Policy*
  - *Awareness and Training*
  - *Configuration Management*
  - *Email Policy*
  - *Information Sensitivity*
  - *Password Construction*
  - *Password Protection*
  - *Penetration Testing*
  - *Remote Access*
  - *Software Installation*
  - *Vulnerability Management*
  - *Wireless Communication*
  - *Wireless Communication Standard*
  - *Workstation Security*
- *Corporate System Security Plan (SSP)*
- *Corporate Plan Of Action and Milestones (POAM)*
- *Corporate Information Systems Contingency Plan / CONOPS (ISCP)*
- *Corporate Event/Incident Communication Plan (EICP)*
- *Corporate Event/Incident Response Plan (EIRP)*
- *Corporate Security Audit Plan (SAP)*

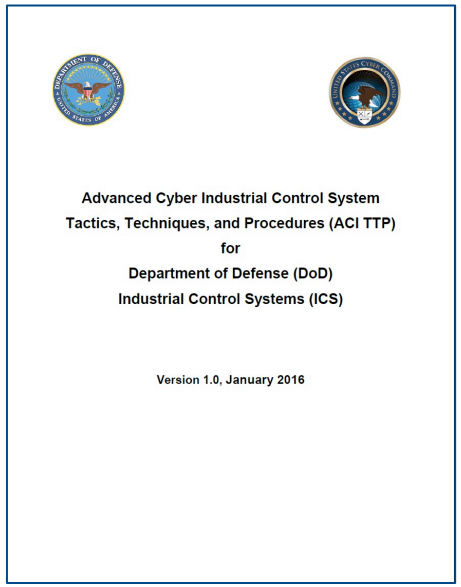
1 of 2

Flow Down to Subcontractors

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.**


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

Version 1.0, January 2016

3. How to Use These TTP

This ACI TTP is divided into essentially four sections:

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

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 [ORGANICATION NAME] with a cc copy to the ESCTP office

ACI TTP Threat-Response Procedures

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

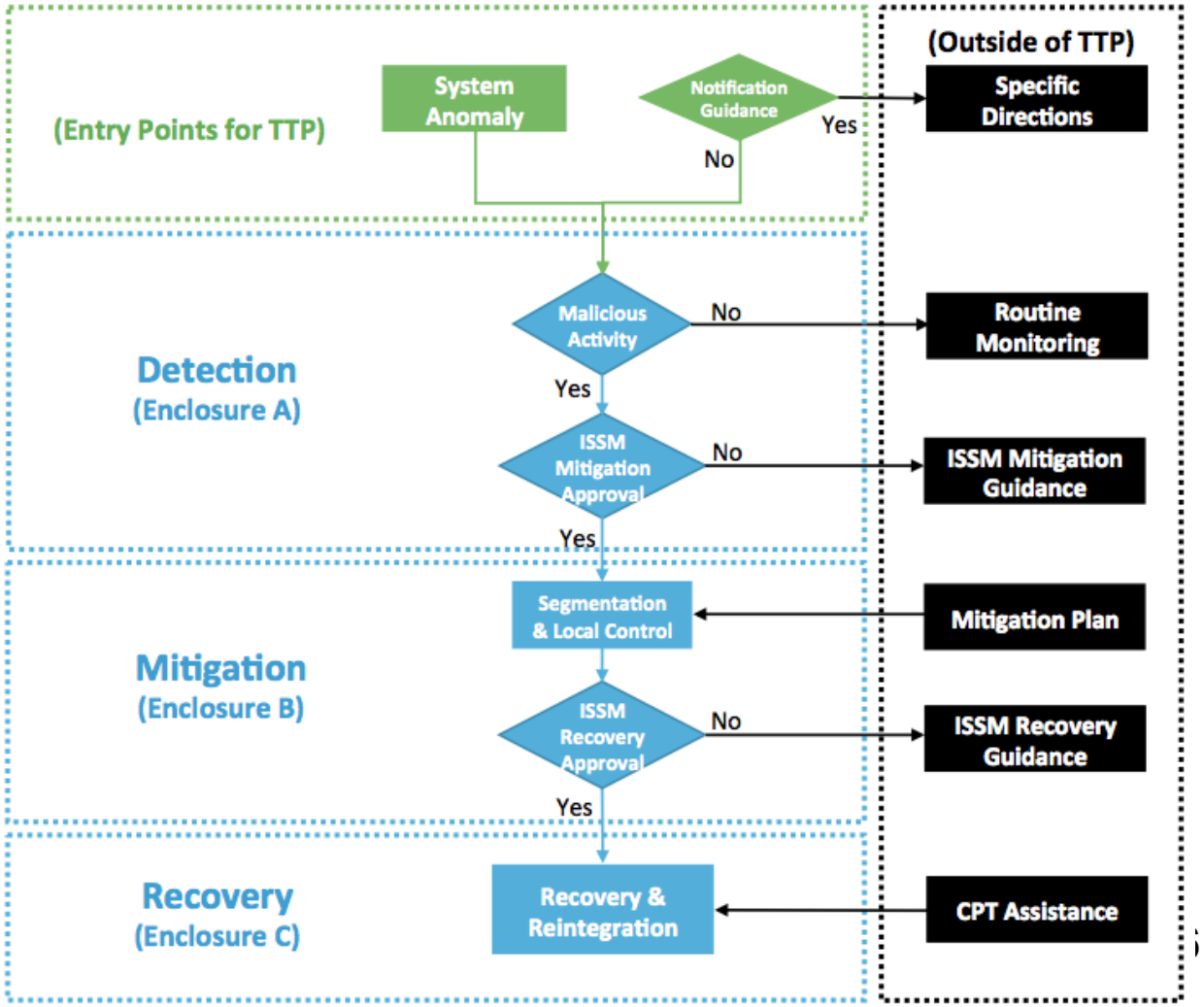
Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general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

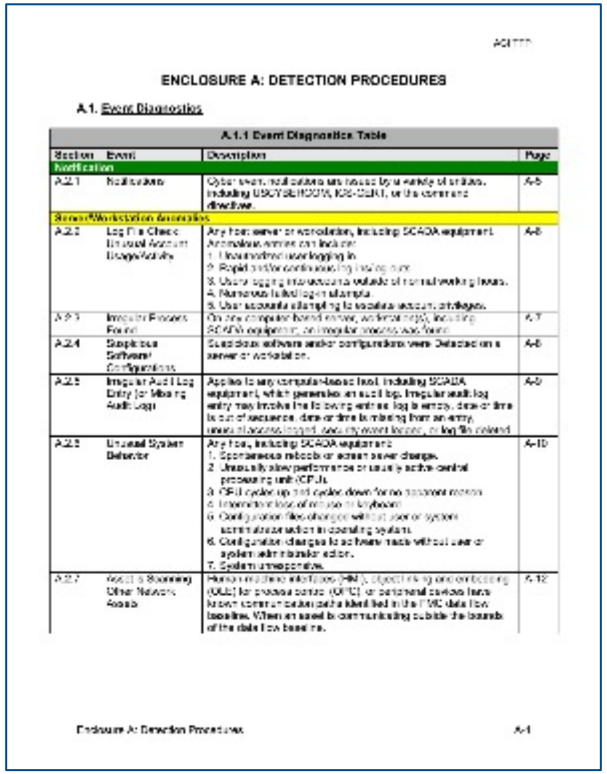
- Incident Notifications List: document contact information for command's Information Assurance Manager
- Document stakeholders who could be affected by a Cyber attack on ICS
- Establish notification procedures with chain of command

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

Design and Construction Sequence TTP Jump-Kit Rescue CD

ENCLOSURE A: DETECTION PROCEDURES


ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostics Table

Section	Event	Description	Page
Notification			
A.2.1	Notifications		A-5
Server/Workstation Anomalies			

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

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

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

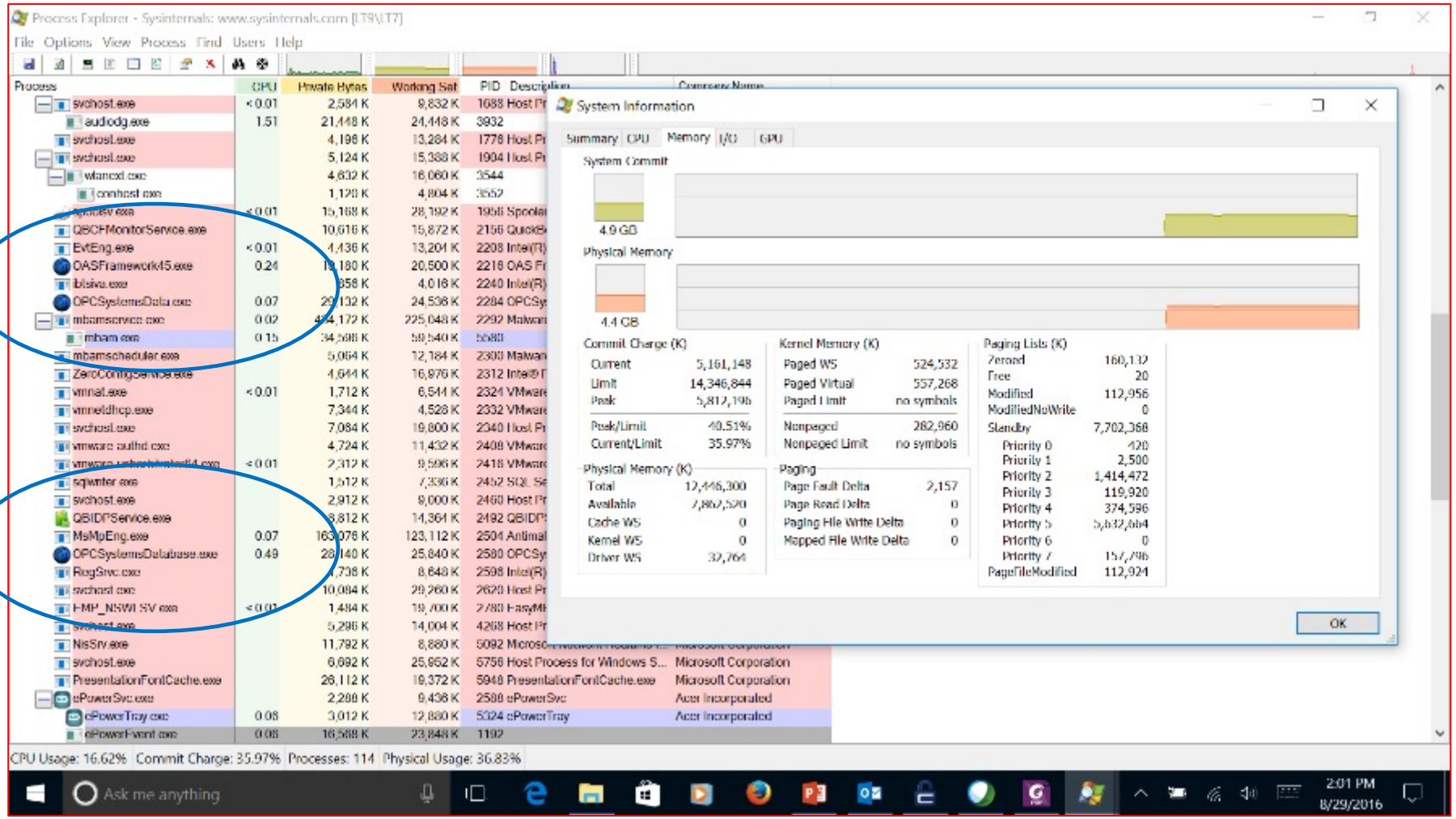
DETECTION PROCEDURES SERVER EXAMPLE 1

A.3.2.1 Server/Workstation Process Check

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

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

DETECTION PROCEDURES SERVER EXAMPLE 1



ENCLOSURE I: CYBER SEVERITY LEVELS

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6 CJCSM 6510.01B
DISTRIBUTION: A, B, C, JEL, S 10 July 2012

CYBER INCIDENT HANDLING PROGRAM

References: See Enclosure H.

1. 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.

2. Cancellation. CJCSM 6510.01A, 24 June 2009, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)," is canceled.

3. 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).

4. Procedures. See Enclosures A through G.

5. Summary of Changes

a. 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).

b. Updates manual based on Unified Command Plan (UCP) Change 1, 12 September 2011.

6. 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.

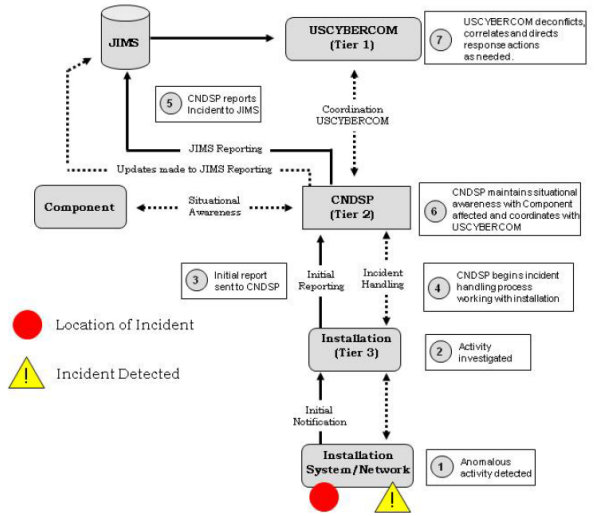


Figure C-C-2. Cyber Event Detected by Installation

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