RMF & eMASS Essentials

CyberProtex

CyberProtex

Introduction

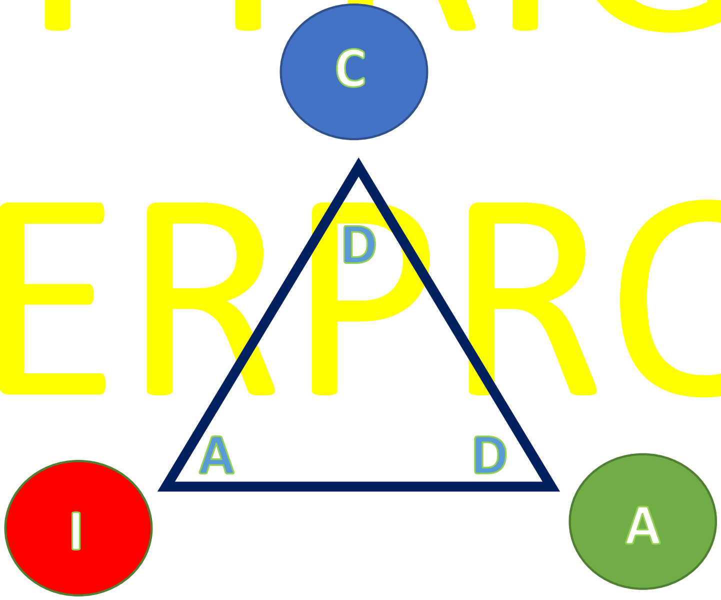
CyberProtex provides Cyber Security consulting solutions, training/ education, and innovative software development in the Tennessee Valley, and around the world via our online Institute. Serving businesses, government entities, the military, and educational institutions, Cyber Security professionals and students.

www.cyberprotex.com

Current Environment

Information Security

Author John Mariotti best surmised the current daily environment, “We worried for decades about WMDs – Weapons of Mass Destruction. Now it is time to worry about the new kind of WMDs – Weapons of Mass Disruption”



- Confidentiality
- Integrity
- Availability

- Disclosed
- Altered
- Denial/Destroyed

CyberProtex

Security Controls

Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets

Organizational Security Model

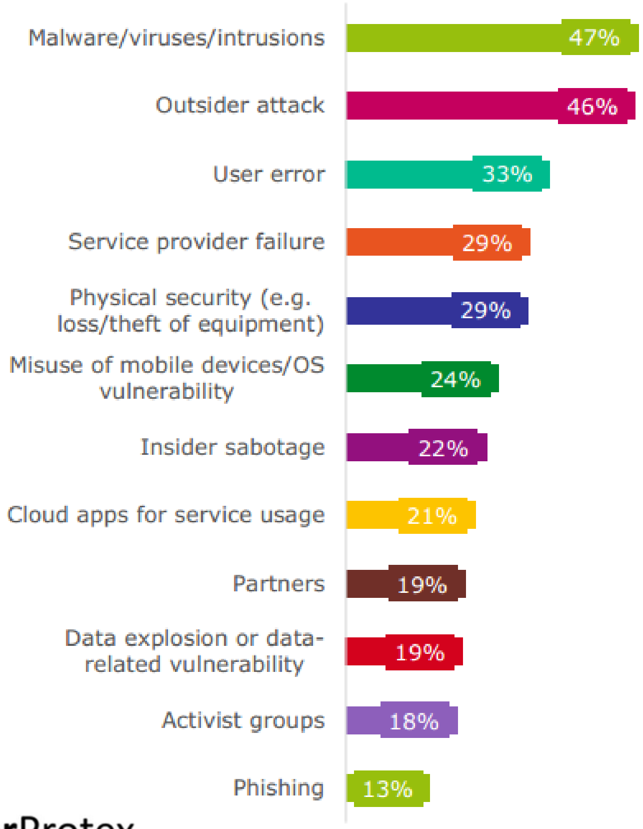
A comprehensive and effective security model has many integrated pieces.

What Does It All Mean

The National Institute of Standards and Technology (NIST) defines an incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

The Department of Homeland Security defines typical violations as the following:

- •Unauthorized access: attempts (either failed or successful) to gain unauthorized access to a system or sensitive data
- •Prevention of legitimate work from being conducted: disruption or denial of service
- •Use of the system for unauthorized processing or storing data
- •Unapproved modifications to the system hardware, firmware, or software characteristics



Possible Contributing Factors to Security Incident

DHS paints a broad scope in the description of the common security incidents. One article provides a statistical breakdown based upon 2015 survey results. The number one cause of incidents related to malware, viruses, and intrusions.

Image courtesy of: https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/

Managing Core Security

Cannot protect everything but we can have security measures in place to try

Managing Controls

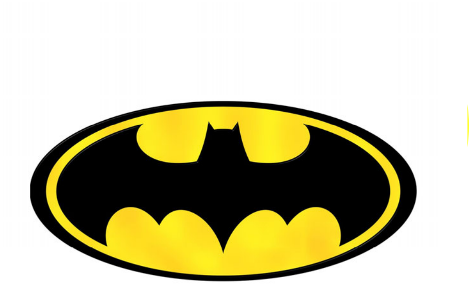
- Restrict Access
- Perform a Vulnerability Assessment
- Survey threats that can exploit vulnerabilities
- What are the impact of identified threats
- What can we do to try to mitigate these threats
- Train employees regularly about what measures are in place
- Automation

Understanding all of these components will help you provide the highest level of security possible

Risk assessment

- Since you can't protect yourself if you do not know what you are protecting against, a risk assessment must be performed
- A risk assessment answers 3 fundamental questions:
  - **Identify assets** - What I am trying to protect?
  - **Identify threats** - What do I need to protect against?
  - **Calculating risks** - How much time, effort & money am I willing to expend to obtain adequate protection?
- After risks are determined, you can then develop the policies & procedures needed to reduce the risks

What Makes Batman a Super Hero?



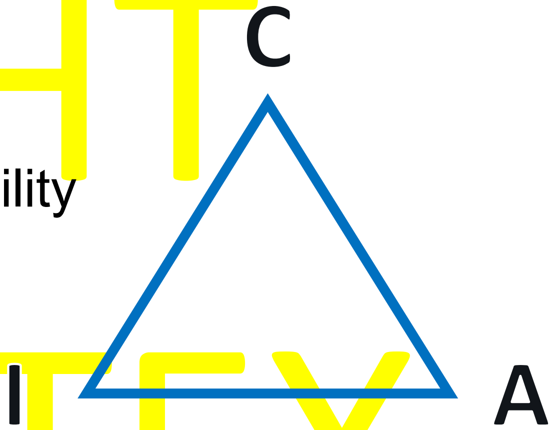
Tools for the cyber tool belt

- Logs
- Virtualization
- Networking Commands
- Nessus
- Wireshark
- Scripting

PRACTICAL EXERCISE
EASY AS ABC

Choose if the following Security Controls fall under

Confidentiality **I**ntegrity Or **A**vailability



Exercise:

1. Being able to access work accounts at home
2. A company requiring all emails to be sent with Digital Signature
3. All new Employees must sign a non disclosure agreement (NDA)
4. Employees must have an ID, pin, and fingerprint scan to enter the office
5. One company agreeing with another company to access each other's Databases

CyberProtex

Casterly Rock

PRACTICAL EXERCISE
“BEND THE KNEE”

What kind of controls would you put in place if you were in charge of security at Casterly Rock?

HINT:
Deter –
Delay –
Detect –
Assess –
Recovery –

CyberProtex

Come up with as many answers as you can.

eMASS Simulator

eMASS

- eMASS: Enterprise Mission Assurance Support Service
- eMASS is a government-owned, commercial off-the-shelf tool that will automate a broad range of services for comprehensive, fully-integrated information assurance (IA) management at the DoD Component level
- The objective is to provide a fully compliant tool that provides full support of the DoD 8500 series.
- Enterprise Mission Assurance Support Service (eMASS) is the Department of Defense's (DoD) recommended tool for information system Certification and Accreditation (C&A)
- eMASS provides the following functions:
  - Automating the C&A process
  - Management of workflow among users
  - Generating reports

eMASS

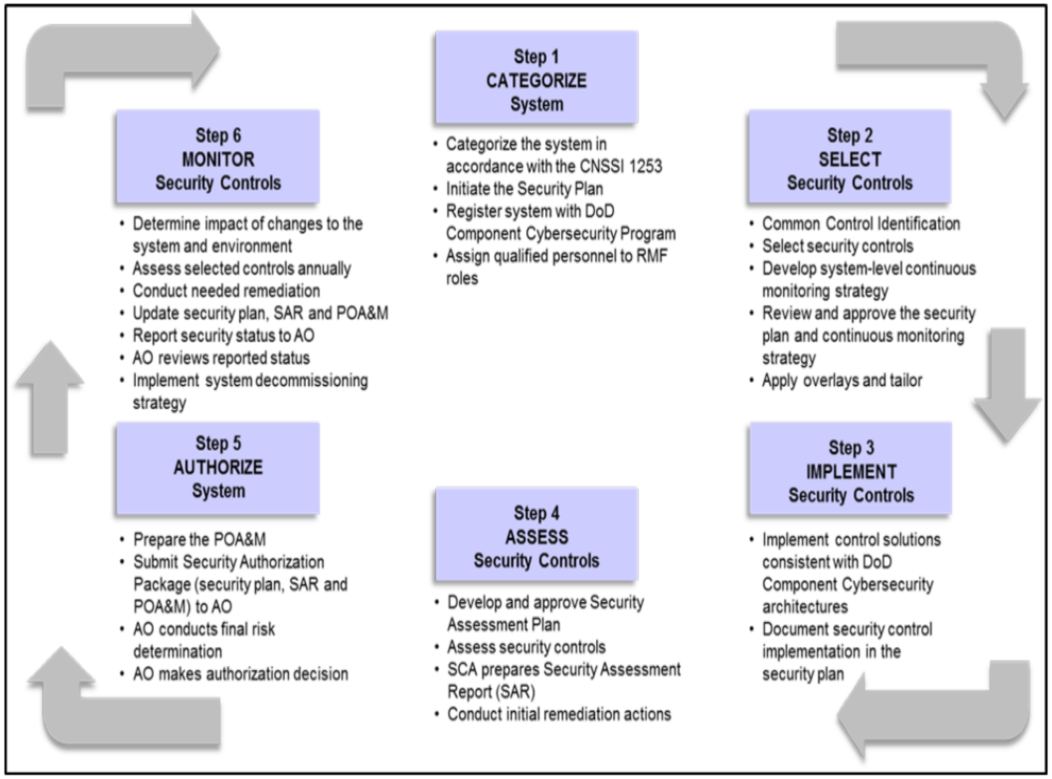
ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE

CyberProtex

* http://www.disa.mil/cybersecurity/certification-accreditation/emass

RMF

- RMF: Risk Management Framework
- RMF is the “unified information security framework for the entire federal government that is replacing the legacy Certification and Accreditation process within federal government departments and agencies, the Department of Defense, and the Intelligence Community (IC)”*
- NIST hosts numerous resources to help define the RMF risk management process which includes:**
  - ✓ Categorize Information Systems (IS)
  - ✓ Select Baseline Security Controls
  - ✓ Implement Security Controls
  - ✓ Assess Security Controls
  - ✓ Authorize IS Operations
  - ✓ Monitor Security Controls



Step 1 CATEGORIZE System
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls
- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4 ASSESS Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System
- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

CyberProtex

* https::/rmf.org
** http://csrc.nist.gov

Policy & Documentation

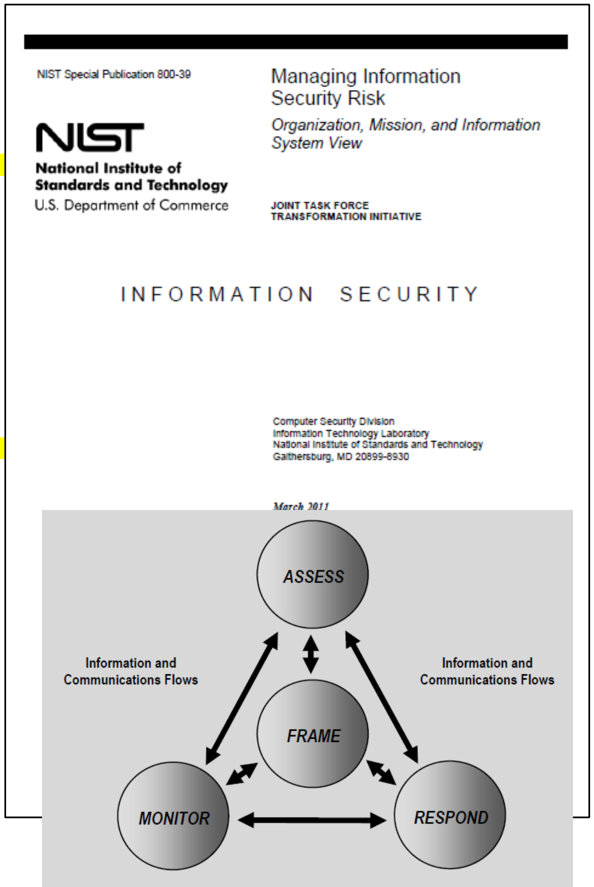
- In order to understand the objectives of the Risk Management Framework, it is important review and understand the existing documentation including:
  - ✓ DoDI 8500.01: Cybersecurity
  - ✓ DoDI 8510.01: Risk Management Framework for DoD Information Technology
  - ✓ NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems
  - ✓ NIST SP 800-39: Managing Information Security Risk
  - ✓ NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
  - ✓ NIST SP 800-71: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

CyberProtex

CyberProtex

NIST 800-39

- NIST SP 800-39: Managing Information Security Risk
- NIST SP 800-39 is the overarching document that defines the standards and guidelines developed by NIST in response to the Federal Information Security Management Act (FISMA)
- NIST SP 800-39 defines high-level risk management as:
  - ✓ Framing Risk
  - ✓ Assessing Risk
  - ✓ Risk Response
  - ✓ Risk Monitoring



NIST Special Publication 800-39

Managing Information Security Risk

Organization, Mission, and Information System View

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

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

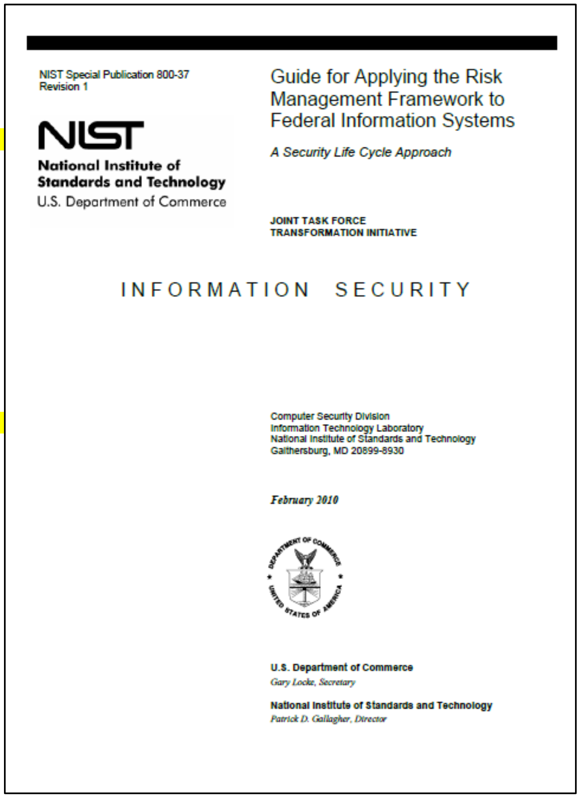
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

NIST SP 800-37

- NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems
- Further breaks down NIST SP 800-39 and defines the "process of applying the Risk Management Framework (RMF) to federal information systems"
  - ✓ Categorization of Information Systems
  - ✓ Select Security Controls
  - ✓ Implement Security Controls
  - ✓ Assess Security Controls
  - ✓ Authorize Information System
  - ✓ Monitor Security Controls
- Defines the "System Development Life Cycle"



NIST Special Publication 800-37
Revision 1

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

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

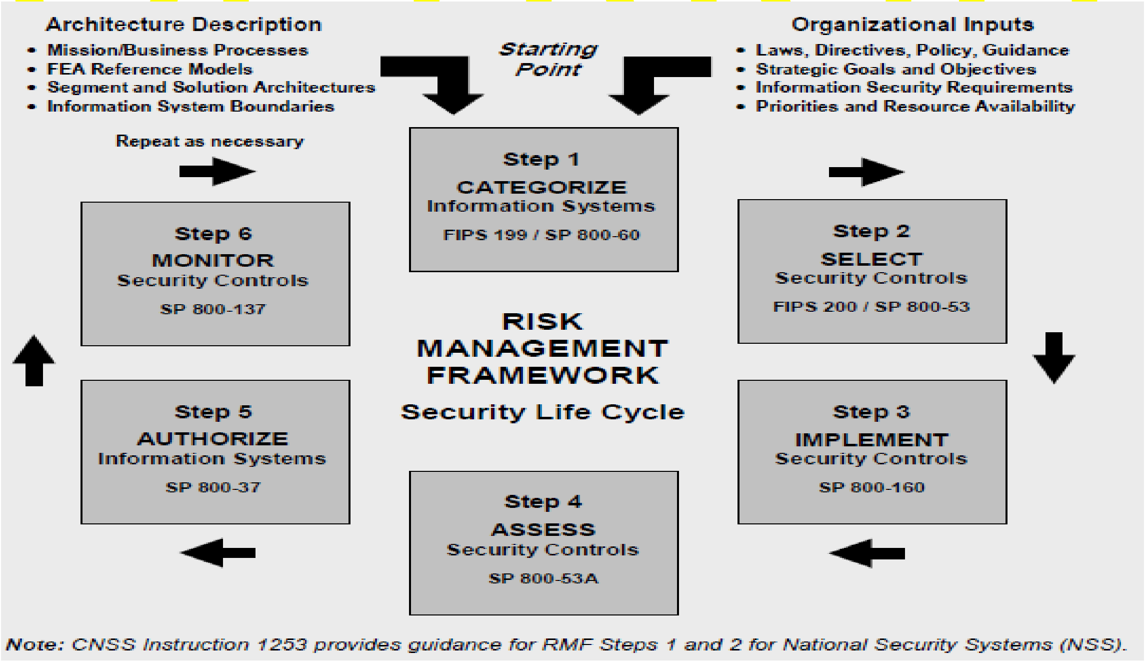
February 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

CyberProtex

NIST 800-37 – RMF Process

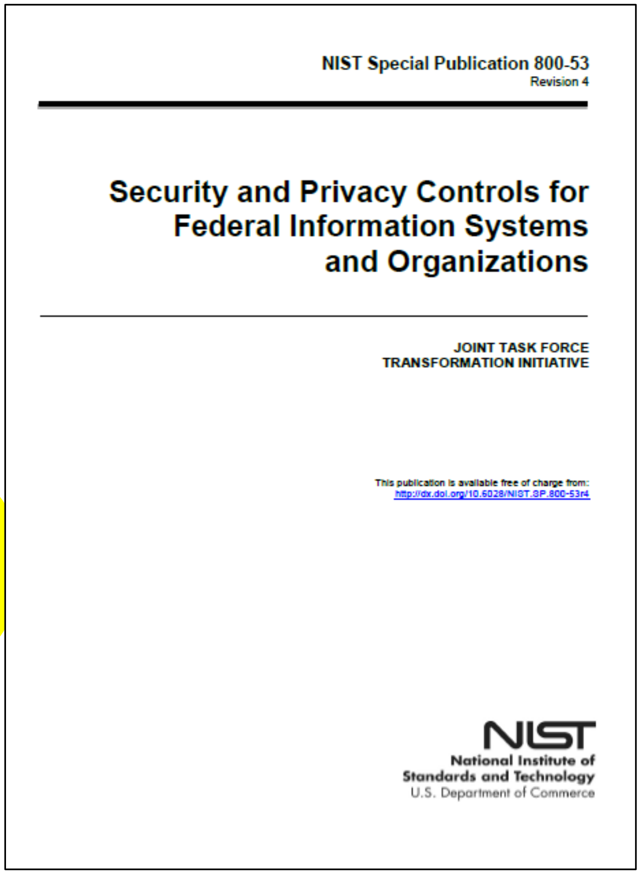


Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

CyberProtex

NIST 800-53

- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53 provides guidelines for selecting and specifying security controls for organizations and information systems
- Requirements for these controls are derived from FIPS Publication 200 titled ***Minimum Security Requirements for Federal Information and Information Systems***
- NIST SP 800-53 main focus on the selection of security controls



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

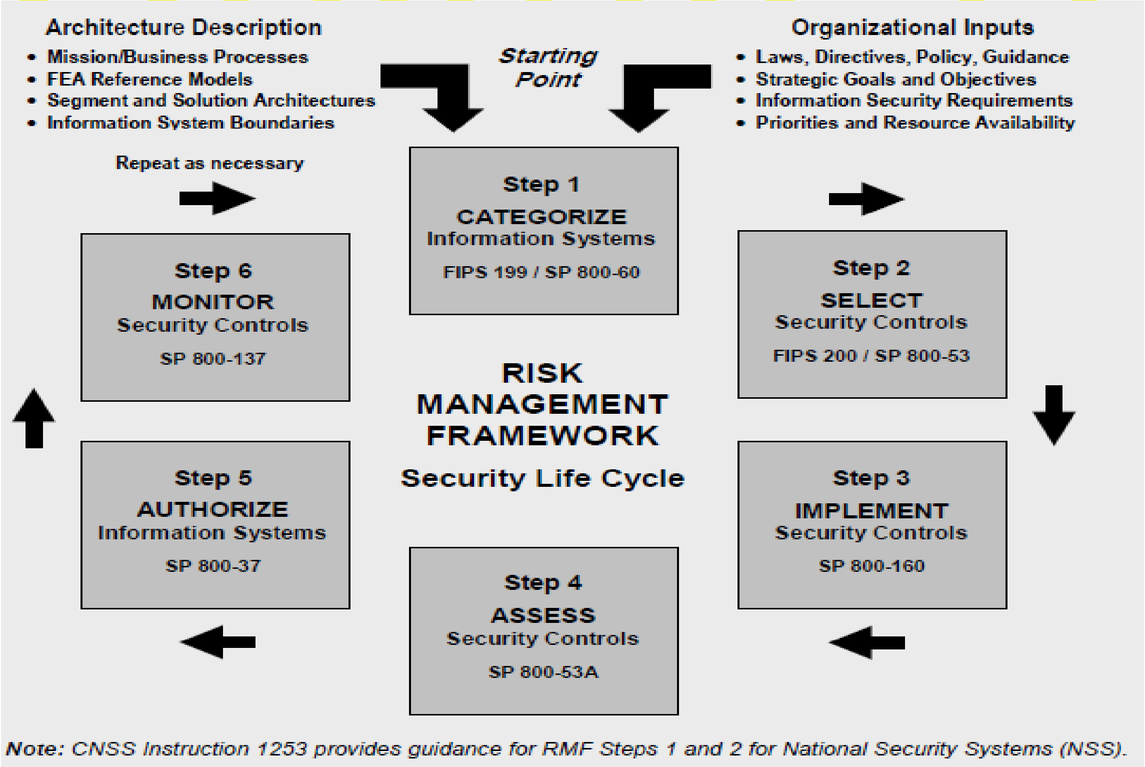
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

CyberProtex

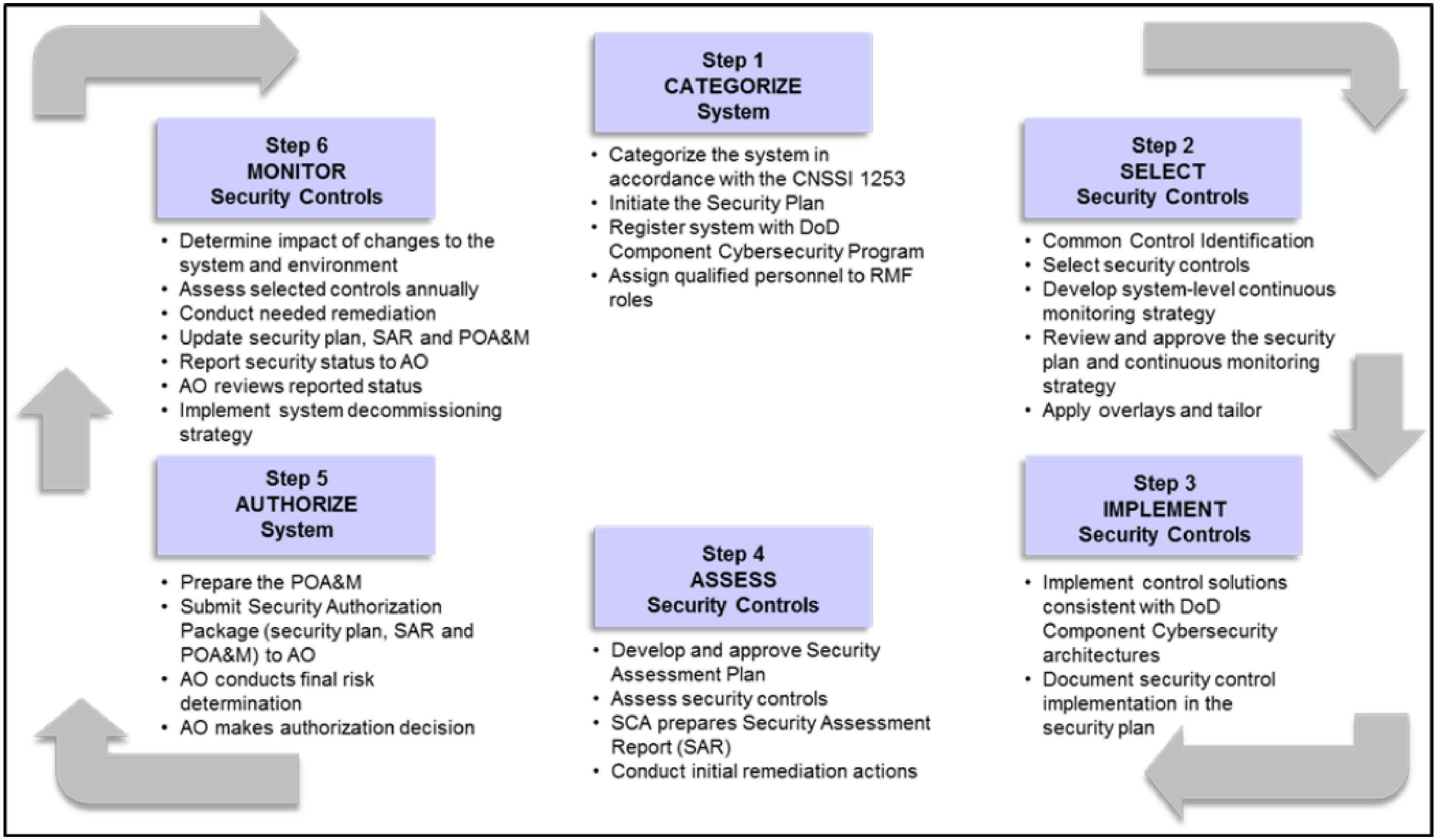
NIST 800-53 – Control Selection



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

DoDI 8510.01 – RMF Process

CyberProtex



Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

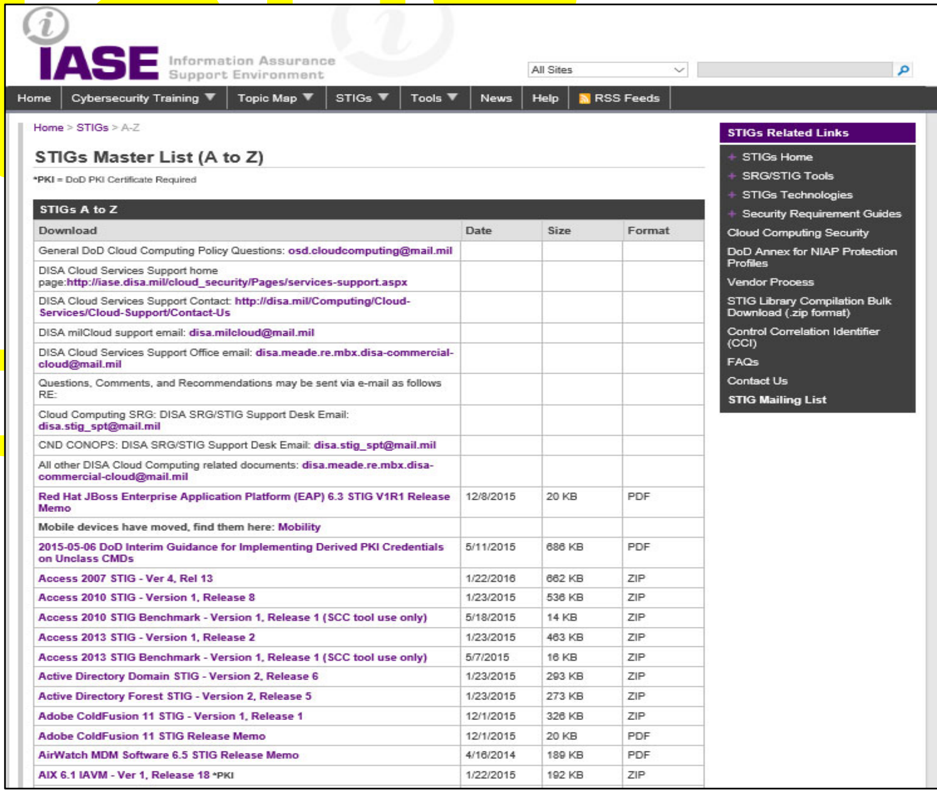
CyberProtex

STIG

- ➢STIG: Security Technical Implementation Guide
- ➢First implemented by DISA in 1998
- ➢STIGs provide the user community with configuration standards for DOD IA and IA-enabled devices/systems
- ➢These guide are applied to myriad of technologies and platforms including hardware, firmware, application, and cloud-based systems
- ➢STIGs are product-specific and document applicable DoD policies and security requirements and include best configuration practices
- ➢If STIGs are not developed for a particular system or application, organizations can substitute a Security Requirements Guide (SRG)

STIG Master List

- The DISA “STIG Master List” provides a repository of all current STIG resources available
- The first 2 steps of the RMF process requires proper categorization of a systems and selection of controls
- There may be cases when a STIG is not available for a current hardware, firmware, operating system, or application



STIGs Master List (A to Z)

*PKI = DoD PKI Certificate Required

STIGs A to Z

Download	Date	Size	Format
General DoD Cloud Computing Policy Questions: osd.cloudcomputing@mail.mil			
DISA Cloud Services Support home page:http://iase.disa.mil/cloud_security/Pages/services-support.aspx			
DISA Cloud Services Support Contact: http://disa.mil/Computing/Cloud-Services/Cloud-Support/Contact-Us			
DISA milCloud support email: disa.milcloud@mail.mil			
DISA Cloud Services Support Office email: disa.meade.re.mbx.disa-commercial-cloud@mail.mil			
Questions, Comments, and Recommendations may be sent via e-mail as follows RE:			
Cloud Computing SRG: DISA SRG/STIG Support Desk Email: disa.stig_spt@mail.mil			
CND CONOPS: DISA SRG/STIG Support Desk Email: disa.stig_spt@mail.mil			
All other DISA Cloud Computing related documents: disa.meade.re.mbx.disa-commercial-cloud@mail.mil			
Red Hat JBoss Enterprise Application Platform (EAP) 6.3 STIG V1R1 Release Memo	12/8/2015	20 KB	PDF
Mobile devices have moved, find them here: Mobility			
2015-05-06 DoD Interim Guidance for Implementing Derived PKI Credentials on Unclass CMDs	5/11/2015	686 KB	PDF
Access 2007 STIG - Ver 4, Rel 13	1/22/2016	662 KB	ZIP
Access 2010 STIG - Version 1, Release 8	1/23/2015	536 KB	ZIP
Access 2010 STIG Benchmark - Version 1, Release 1 (SCC tool use only)	5/18/2015	14 KB	ZIP
Access 2013 STIG - Version 1, Release 2	1/23/2015	463 KB	ZIP
Access 2013 STIG Benchmark - Version 1, Release 1 (SCC tool use only)	5/7/2015	16 KB	ZIP
Active Directory Domain STIG - Version 2, Release 6	1/23/2015	293 KB	ZIP
Active Directory Forest STIG - Version 2, Release 5	1/23/2015	273 KB	ZIP
Adobe ColdFusion 11 STIG - Version 1, Release 1	12/1/2015	326 KB	ZIP
Adobe ColdFusion 11 STIG Release Memo	12/1/2015	20 KB	PDF
AirWatch MDM Software 6.5 STIG Release Memo	4/16/2014	189 KB	PDF
AIX 6.1 IAVM - Ver 1, Release 18 *PKI	1/22/2015	192 KB	ZIP

SCAP

- SCAP: Security Compliance Application Protocol
- SCAP provides the following capabilities:
  - ✓ Policy Compliance Evaluation
  - ✓ Automated Vulnerability Assessment
- SCAP uses a number of open source resources for its checks including:
  - ✓ National Vulnerability Database
  - ✓ Common Vulnerabilities and Exposures
  - ✓ Common Vulnerability Scoring System
- Not every system has an automated SCAP process of identifying system vulnerabilities
- STIGViewer

CyberProtex

System Boundaries

- Challenges with Defining System Boundaries
- Establishing Information System Boundaries
- Boundaries for Complex Information Systems

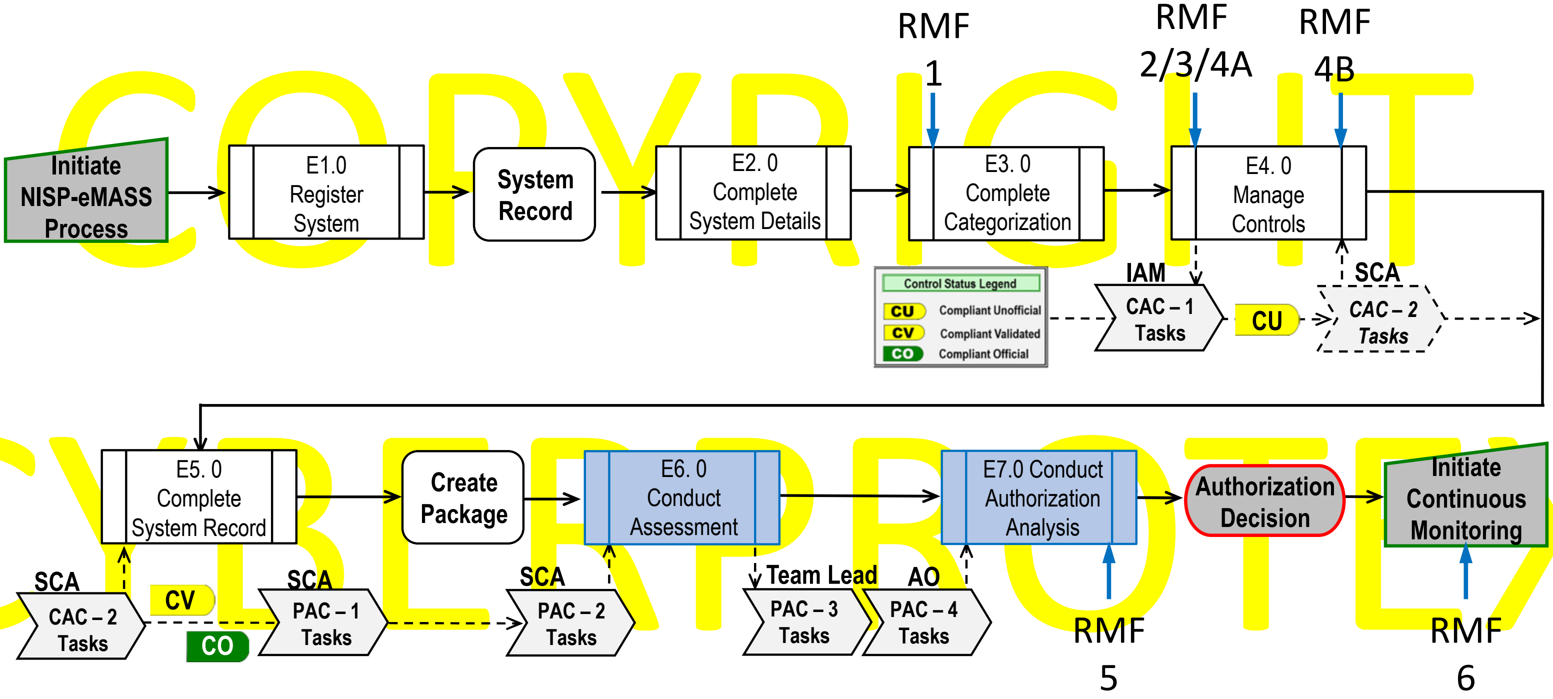
EMASS

CyberProtex

- ➢EMASS: Enterprise Mission Assurance Support Service
- ➢eMASS is a government-owned, commercial off-the-shelf tool that will automate a broad range of services for comprehensive, fully-integrated information assurance (IA) management at the DoD Component level
- ➢The objective is to provide a fully compliant tool that provides full support of the DoD 8500 series.
- ➢Enterprise Mission Assurance Support Service (eMASS) is the Department of Defense's (DoD) recommended tool for information system Certification and Accreditation (C&A)
- ➢eMASS provides the following functions:
  - ✓Automating the C&A process
  - ✓Management of workflow among users
  - ✓Generating reports

* http://www.disa.mil/cybersecurity/certification-accreditation/emass

eMASS Workflow w/ Embedded Approval & RMF Processes



Initiate NISP-eMASS Process

E1.0 Register System

System Record

E2. 0 Complete System Details

RMF 1

E3. 0 Complete Categorization

RMF 2/3/4A

RMF 4B

E4. 0 Manage Controls

IAM

CAC – 1 Tasks

CU

SCA

CAC – 2 Tasks

Control Status Legend	
CU	Compliant Unofficial
CV	Compliant Validated
CO	Compliant Official

E5. 0 Complete System Record

SCA

CAC – 2 Tasks

CV

CO

SCA

PAC – 1 Tasks

Create Package

SCA

PAC – 2 Tasks

E6. 0 Conduct Assessment

Team Lead

PAC – 3 Tasks

AO

PAC – 4 Tasks

E7.0 Conduct Authorization Analysis

RMF 5

Authorization Decision

Initiate Continuous Monitoring

RMF 6

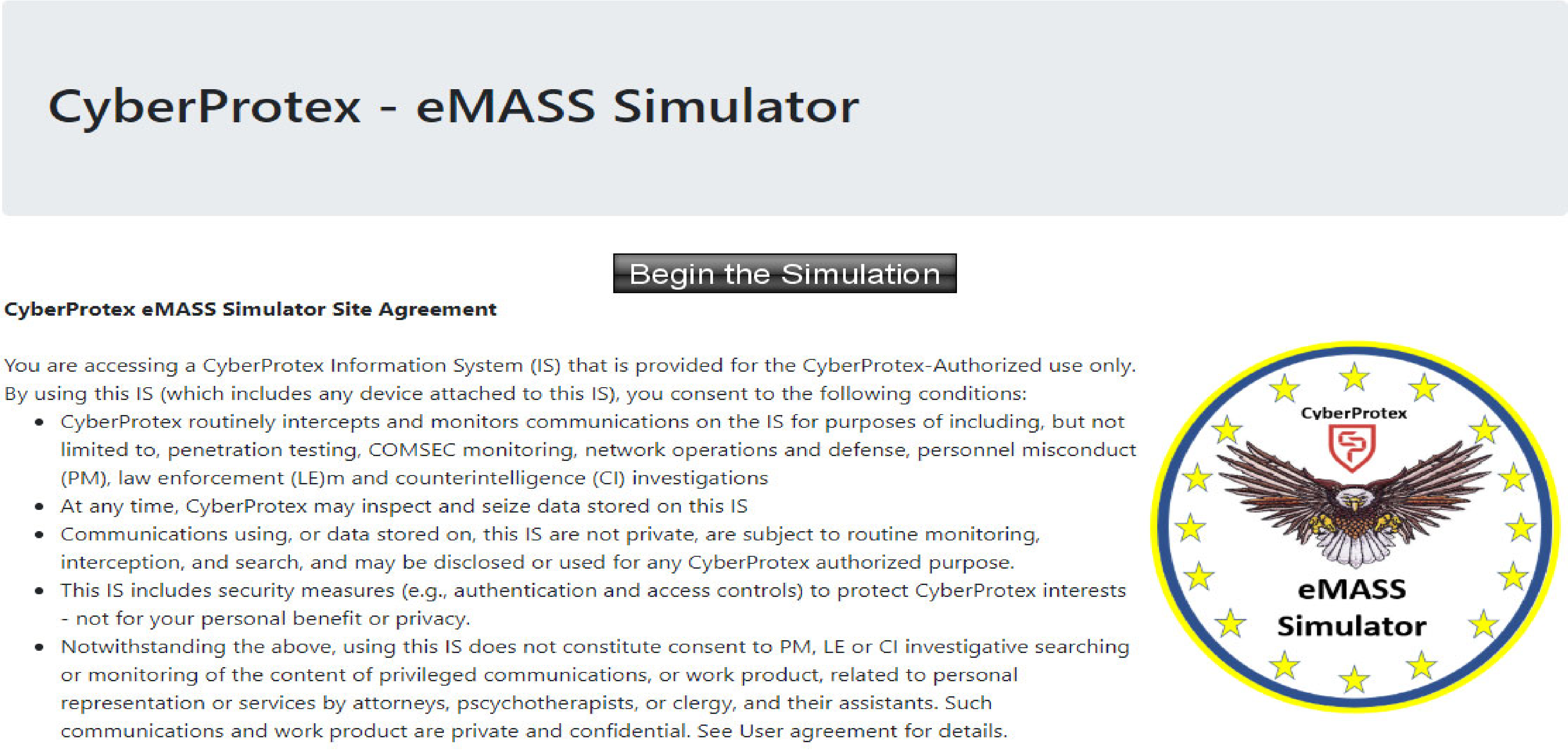
CyberProtex

eMASS in the RMF Steps and Actions

RMF Steps	eMASS Actions
1. CATEGORIZE (Industry)	▪ System Registration ▪ Assign Roles ▪ Input System Details
2. SELECT (Industry)	▪ Baseline Security Control Selection ▪ Overlay Selection ▪ Input of Additional System Details
3. IMPLEMENT (Industry)	Input of: ▪ Implementation Plan ▪ System-Level Continuous Monitoring (SLCM) Strategy
4. ASSESS (4a. Industry 4b. DSS)	▪ 4a. Self-Assessment of Security Controls ▪ 4a. Generation of Automated POA&M ▪ 4a. Review of finalized package ▪ 4a. Submission of Final Package to SCA -- ▪ 4b. Review and Validation of Security Controls within Finalized Package ▪ 4b. Document Weaknesses and/or Deficiencies in SAR ▪ 4b. Approve/Return Package for Rework ▪ 4b. Submission of Finalized Package to the Package Approval Chain (PAC)
5. AUTHORIZE (DSS)	▪ SCA Generates Security Assessment Report Executive Summary ▪ SCA Recommends Authorization Decision to AO -- ▪ AO Inputs Authorization Decision ▪ Automated Authorization Letter is Generated
6. MONITOR (Industry & DSS)	▪ Technical, Management, and Operational Security Controls are Assessed, Modified and Submitted for Approval According to Continuous Monitoring Strategy (CMS) ▪ POA&M Remediation/Mitigation Items are Updated, Reviewed and Submitted to SCA for Approval ▪ SCA Reviews Updated Security Controls and POA&M items in accordance to CMS

eMASS Lab Site Agreement

CyberProtex

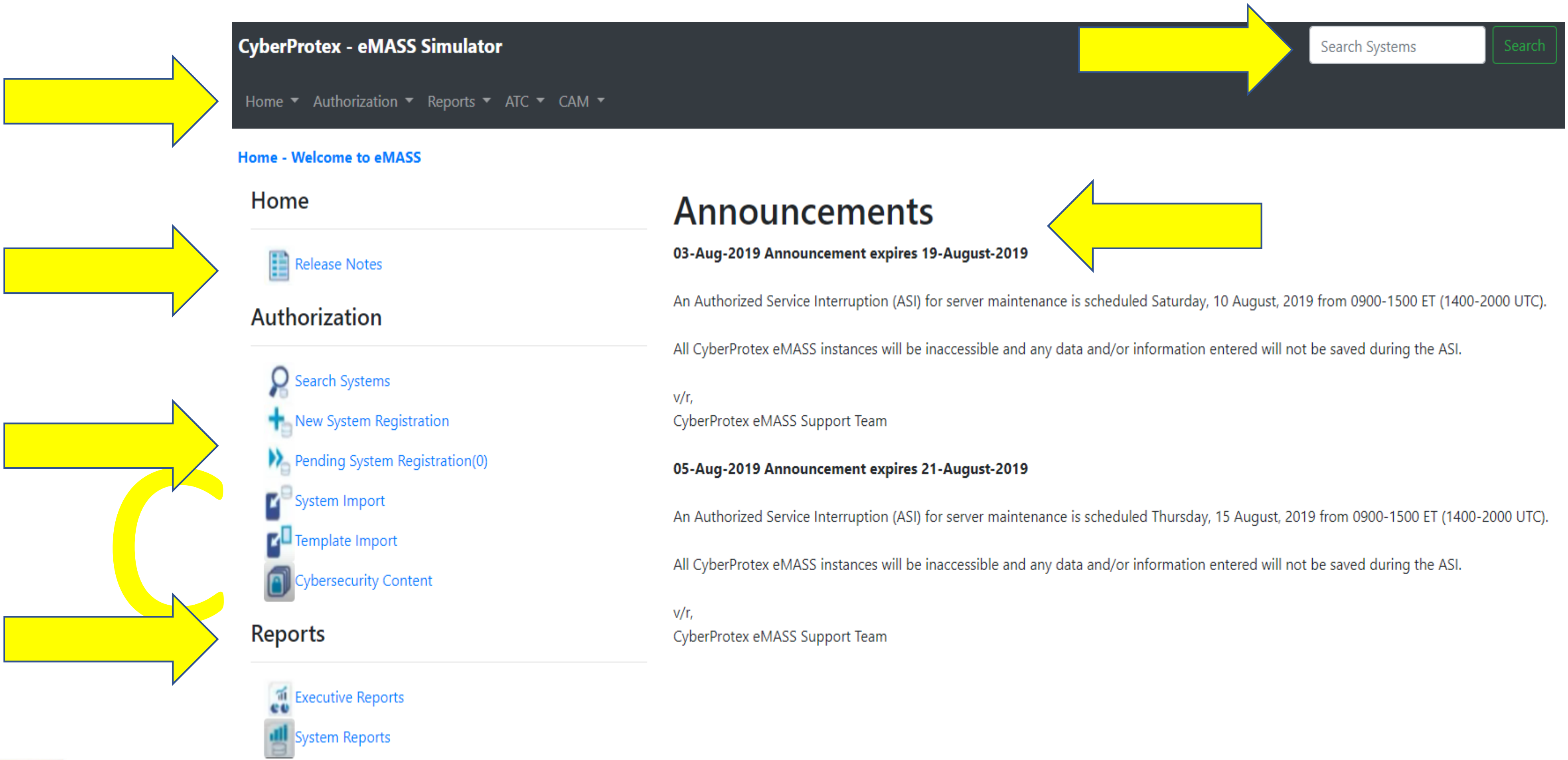


CyberProtex - eMASS Simulator

CyberProtex eMASS Simulator Site Agreement

You are accessing a CyberProtex Information System (IS) that is provided for the CyberProtex-Authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- CyberProtex routinely intercepts and monitors communications on the IS for purposes of including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE)m and counterintelligence (CI) investigations
- At any time, CyberProtex may inspect and seize data stored on this IS
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any CyberProtex authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect CyberProtex interests - not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, pscychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User agreement for details.



Announcements

03-Aug-2019 Announcement expires 19-August-2019

An Authorized Service Interruption (ASI) for server maintenance is scheduled Saturday, 10 August, 2019 from 0900-1500 ET (1400-2000 UTC).

All CyberProtex eMASS instances will be inaccessible and any data and/or information entered will not be saved during the ASI.

v/r,
CyberProtex eMASS Support Team

05-Aug-2019 Announcement expires 21-August-2019

An Authorized Service Interruption (ASI) for server maintenance is scheduled Thursday, 15 August, 2019 from 0900-1500 ET (1400-2000 UTC).

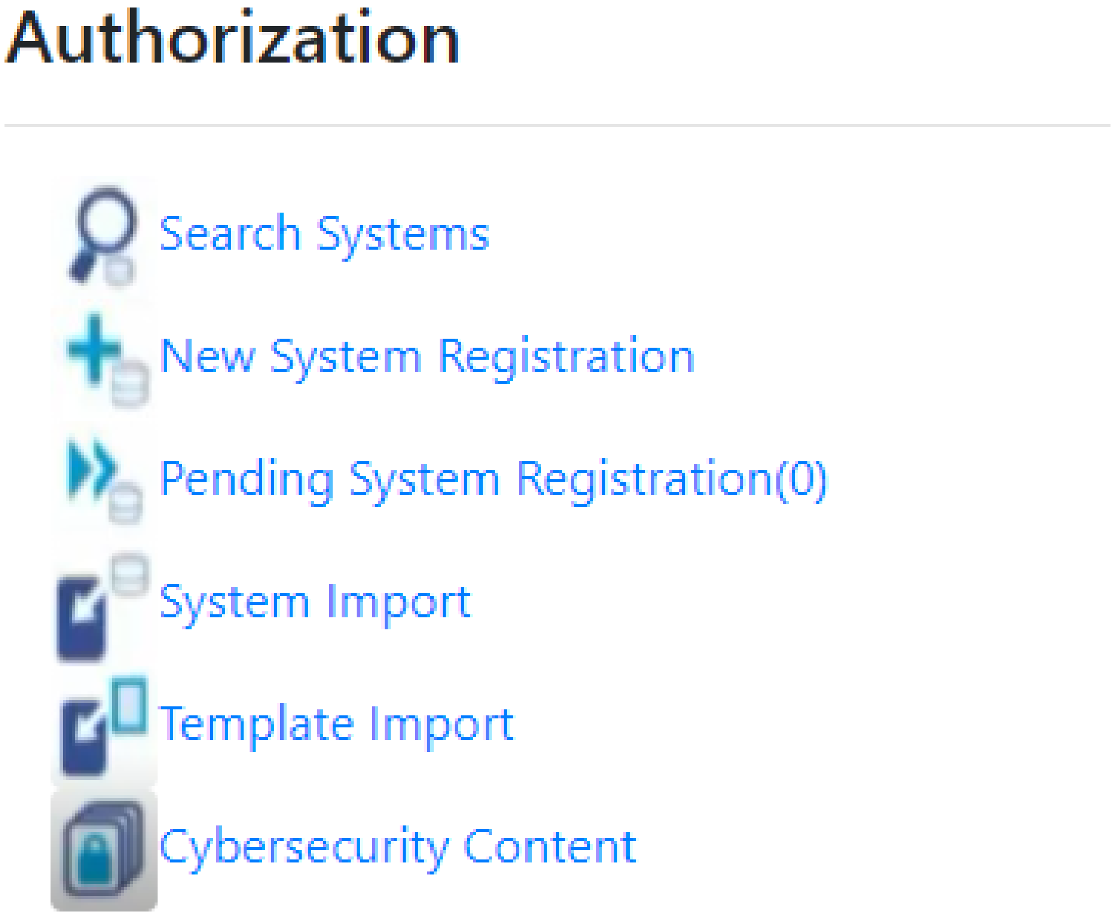
All CyberProtex eMASS instances will be inaccessible and any data and/or information entered will not be saved during the ASI.

v/r,
CyberProtex eMASS Support Team

CyberProtex

eMASS Lab

New System Registration



Authorization

- Search Systems
- New System Registration
- Pending System Registration(0)
- System Import
- Template Import
- Cybersecurity Content

SYSTEM CATEGORIZATION

Categorize the System

- Identify the information types
- Determine confidentiality, integrity, and availability values
- Determine potential impact on organizations and individuals
- Categorize information types
- Categorize information system
- Document categorization in the Security Plan (SP)
- Perform Privacy Threshold Analysis and Privacy Impact Assessment

Describe the Information System (Including the Security Authorization Boundaries)

Practical Exercise - Prepping for eMASS System Overview – MOUS

- The Software Engineering Directorate (SED) is engineering a next generation subsystem they call the Miniature Operational Unmanned System or “MOUS”. The MOUS is a system made up of a hardware and software solution for the Army Aviation Tactical Precision Fires. The MOUS provides functionality for the Unmanned Aircraft Systems (UAS) via a Linux microcontroller installed on large drone with secure radios communicating with a Ground Station Software (GSS).

- The main software component is the platforms’ GSS which is delivered via an Windows 10 operating system for extreme flexibility and mobility to the warfighter. The Windows 10 GSS controls the MOUS – UAS and sends information to a Windows 2016 Server Domain Controller. The MOUS delivers data to other applications used for flight performance modeling, test, and diagnostics. The Army’s MOUS enables an environment to provide the warfighter the capability to sneak up on the enemy and attack unnoticed. Collectively, many MOUS working in concert creates a “Secure Swarm” of drones. This scenario is a system of systems. If this system is successful, it will become a program of record. Thus, we will anticipate a need to register the system needing to be "Assessed and Authorized".

- The Information System Owner, Mr. Herman Sherman thinks that this is a Platform IT System. Since it has been approved, Post Milestone A of technology development in the system life cycle. The system is not considered a National Security System and is certainly not a Financial Management System. There are no Reciprocity Systems included in this development. We will need to begin to collect information with anticipation of entering it into eMASS. We will release version 1.0 into eMASS and need it evaluated.

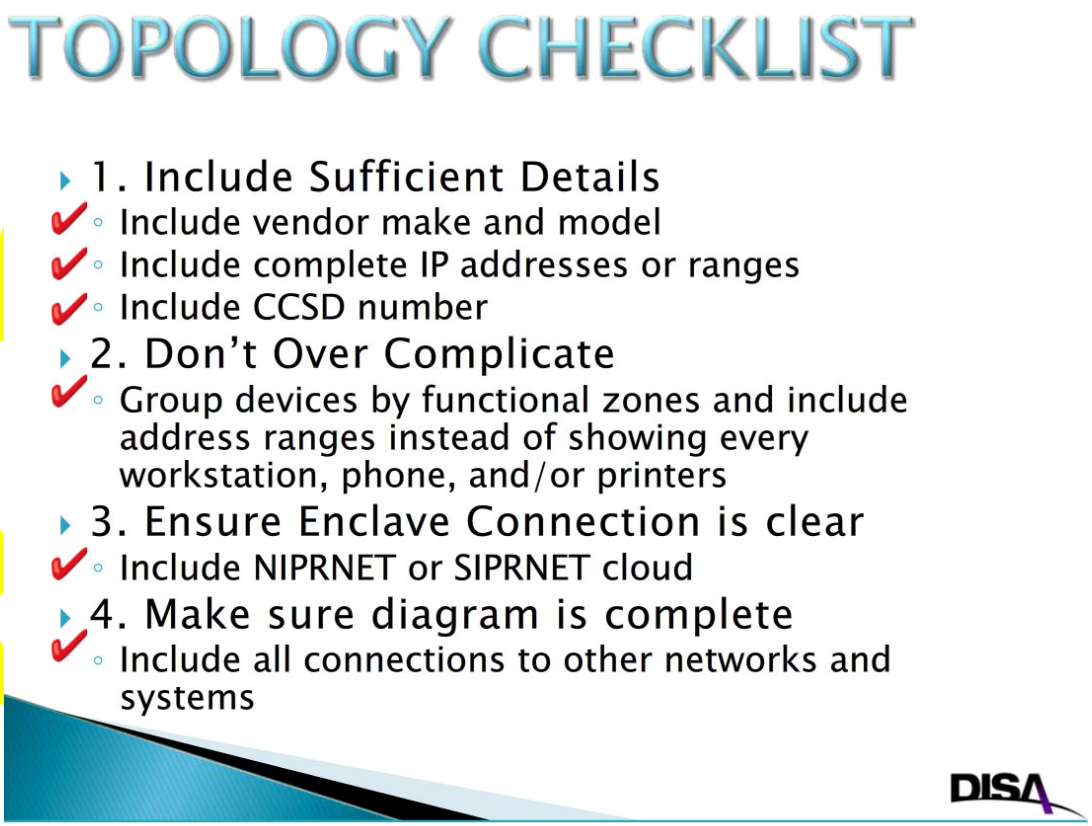
CyberProtex

Worksheet: MOUS
Draw a quick MOUS Topology and Boundaries

CyberProtex

System Boundaries

- Challenges with Defining System Boundaries
- Establishing Information System Boundaries
- Boundaries for Complex Information Systems



TOPOLOGY CHECKLIST

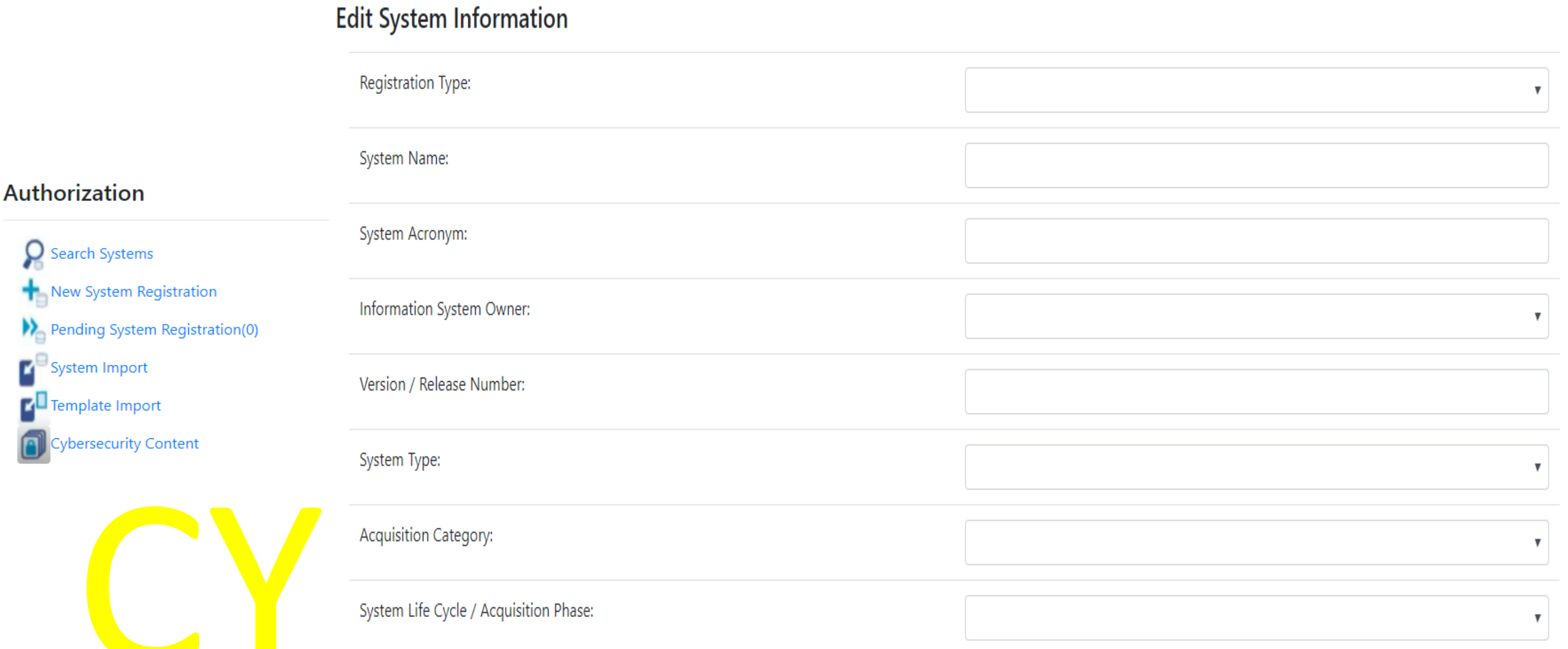
- 1. Include Sufficient Details
  - ✓ Include vendor make and model
  - ✓ Include complete IP addresses or ranges
  - ✓ Include CCSD number
- 2. Don’t Over Complicate
  - ✓ Group devices by functional zones and include address ranges instead of showing every workstation, phone, and/or printers
- 3. Ensure Enclave Connection is clear
  - ✓ Include NIPRNET or SIPRNET cloud
- 4. Make sure diagram is complete
  - ✓ Include all connections to other networks and systems

CyberProtex

System Overview – MOUS – Worksheet

In the space provided below, enter the appropriate information based off the system overview of the MOUS.

Registration Type:	
System Name:	
System Acronym:	
Information System Owner:	
Version / Release Number:	
System Type:	
Acquisition Category:	
System Life Cycle / Acquisition Phase:	
National Security System:	
Financial Management System:	
Reciprocity System:	
System Description:	



Edit System Information

Registration Type: ▾

System Name:

System Acronym:

Information System Owner: ▾

Version / Release Number:

System Type: ▾

Acquisition Category: ▾

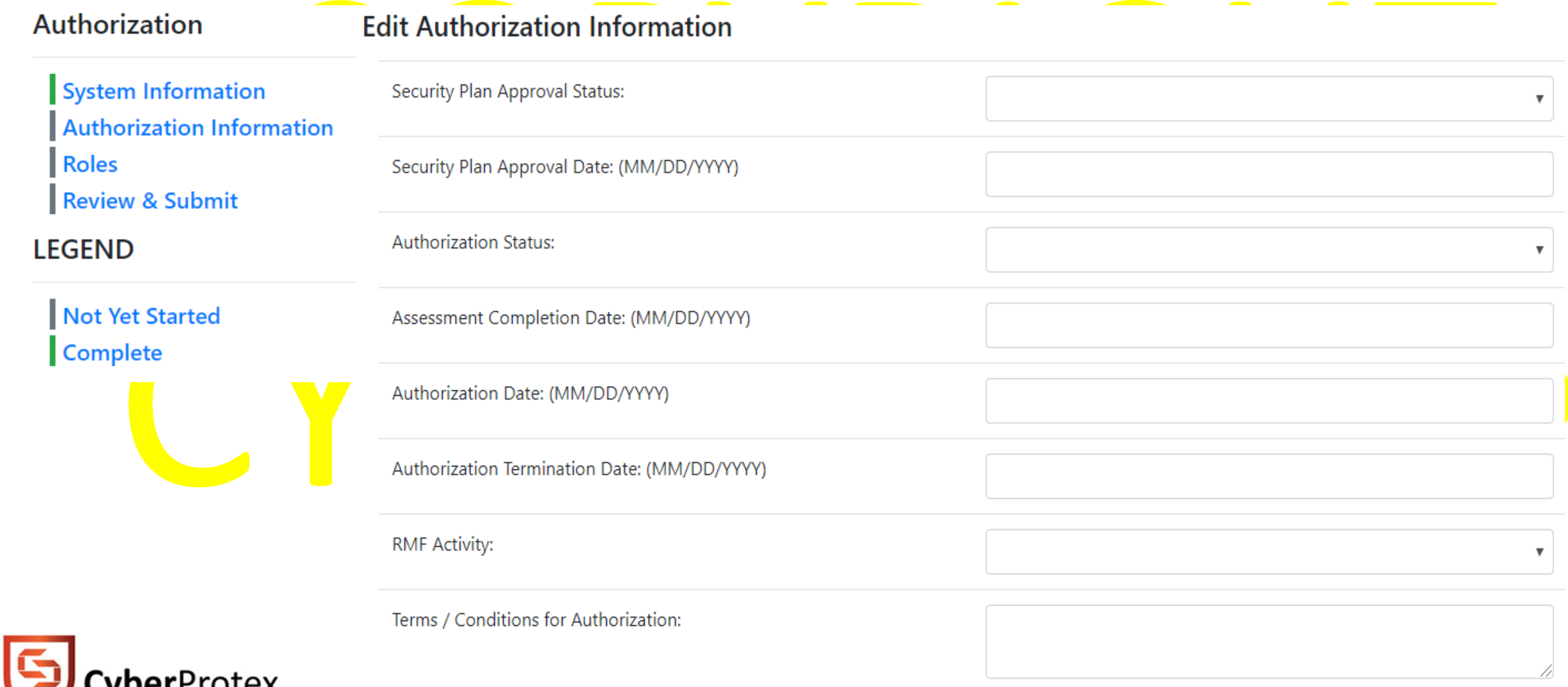
System Life Cycle / Acquisition Phase: ▾

eMASS Lab

Enter New System Registration

CyberProtex

eMASS Lab - Registering Systems
Entering Authorization Information



Authorization

- 🟩 System Information
- ▮ Authorization Information
- ▮ Roles
- ▮ Review & Submit

LEGEND

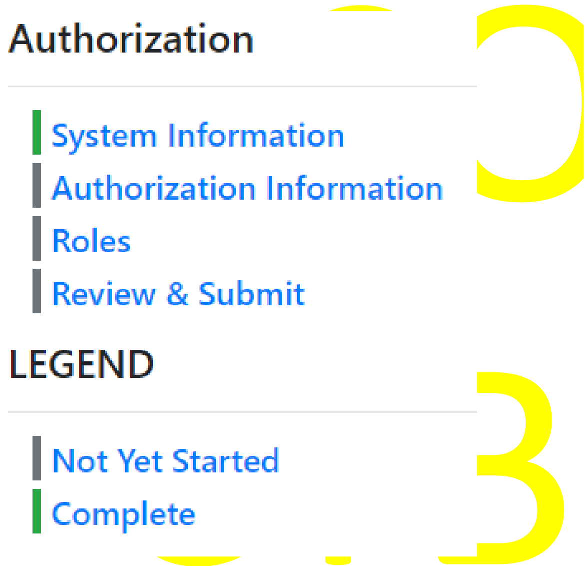
- ▮ Not Yet Started
- 🟩 Complete

Edit Authorization Information

Security Plan Approval Status:	▾
Security Plan Approval Date: (MM/DD/YYYY)	
Authorization Status:	▾
Assessment Completion Date: (MM/DD/YYYY)	
Authorization Date: (MM/DD/YYYY)	
Authorization Termination Date: (MM/DD/YYYY)	
RMF Activity:	▾
Terms / Conditions for Authorization:	

CyberProtex

eMASS Lab - Registering Systems
Entering Authorization Information - Roles

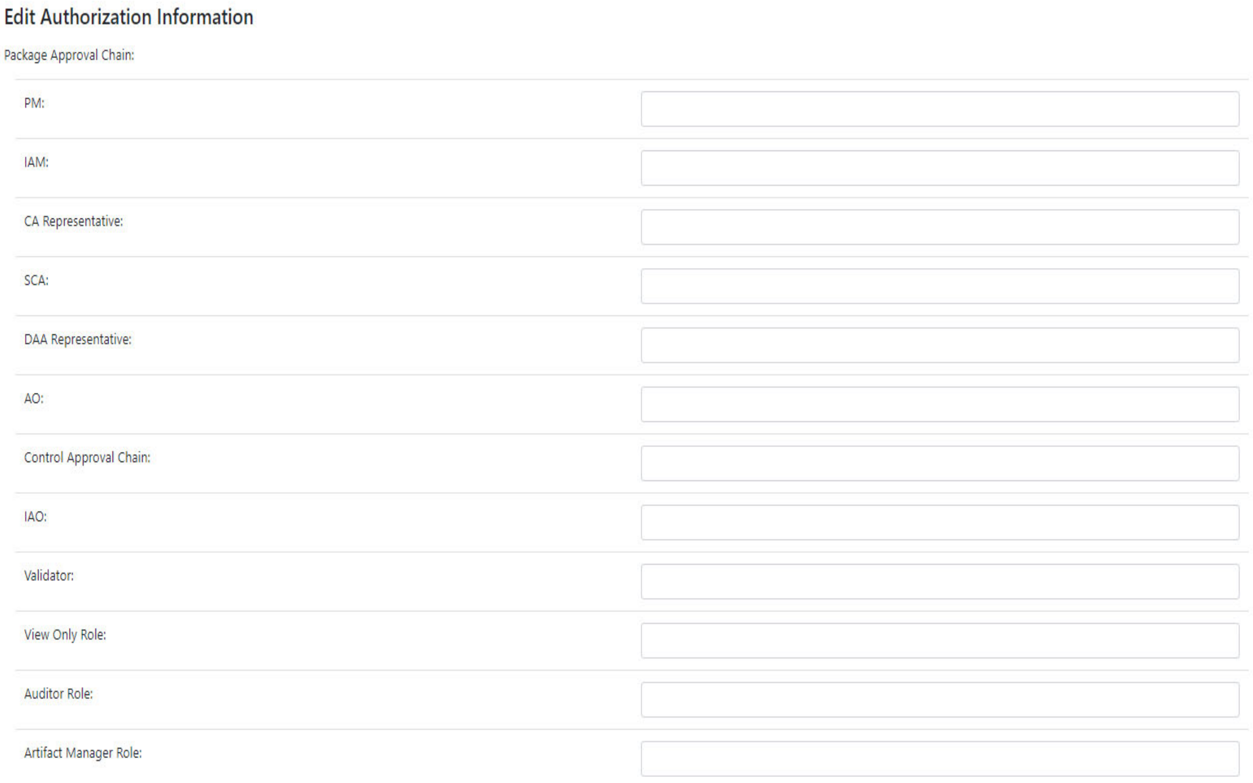


Authorization

🟩 System Information
▨ Authorization Information
▨ Roles
▨ Review & Submit

LEGEND

▨ Not Yet Started
🟩 Complete



Edit Authorization Information

Package Approval Chain:

PM:

IAM:

CA Representative:

SCA:

DAA Representative:

AO:

Control Approval Chain:

IAO:

Validator:

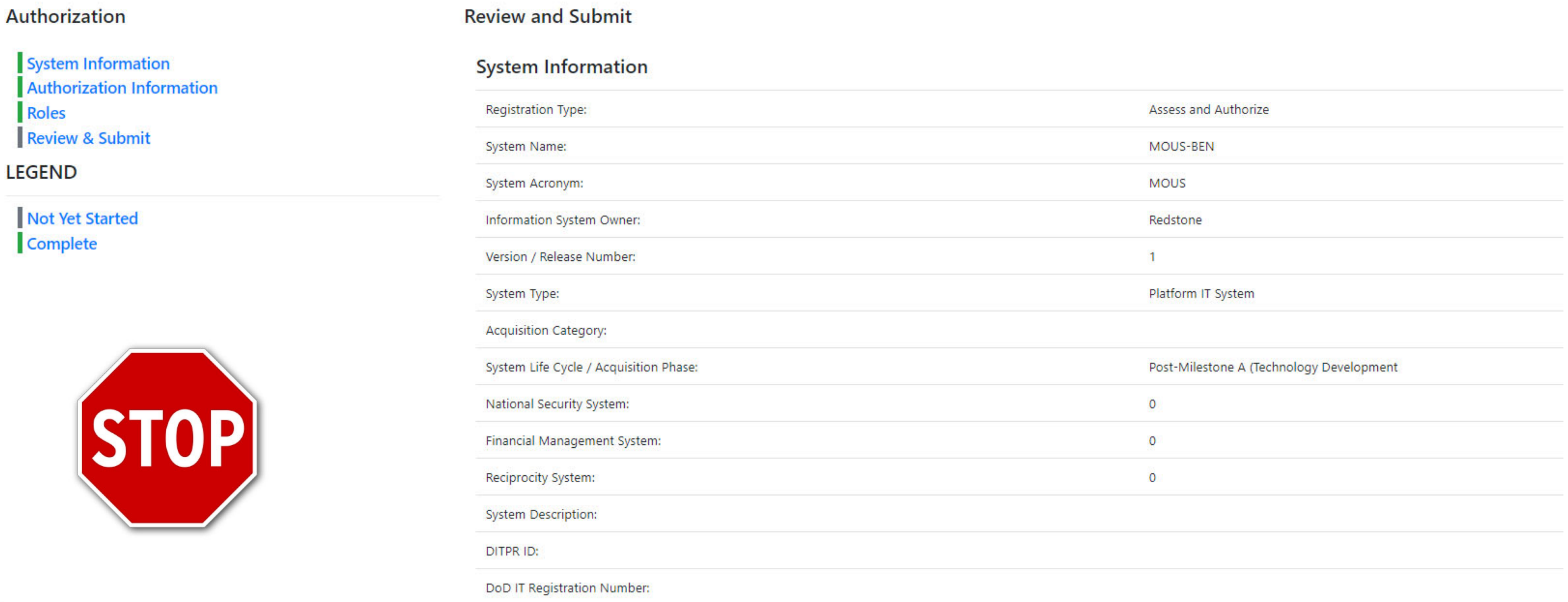
View Only Role:

Auditor Role:

Artifact Manager Role:

CyberProtex

eMASS Lab - System Categorization - Review and Submit



Authorization

- 🟩 System Information
- 🟩 Authorization Information
- 🟩 Roles
- ▮ Review & Submit

LEGEND

- ▮ Not Yet Started
- 🟩 Complete

STOP

Review and Submit

System Information

Registration Type:	Assess and Authorize
System Name:	MOUS-BEN
System Acronym:	MOUS
Information System Owner:	Redstone
Version / Release Number:	1
System Type:	Platform IT System
Acquisition Category:	
System Life Cycle / Acquisition Phase:	Post-Milestone A (Technology Development
National Security System:	0
Financial Management System:	0
Reciprocity System:	0
System Description:	
DITPR ID:	
DoD IT Registration Number:	

CyberProtex

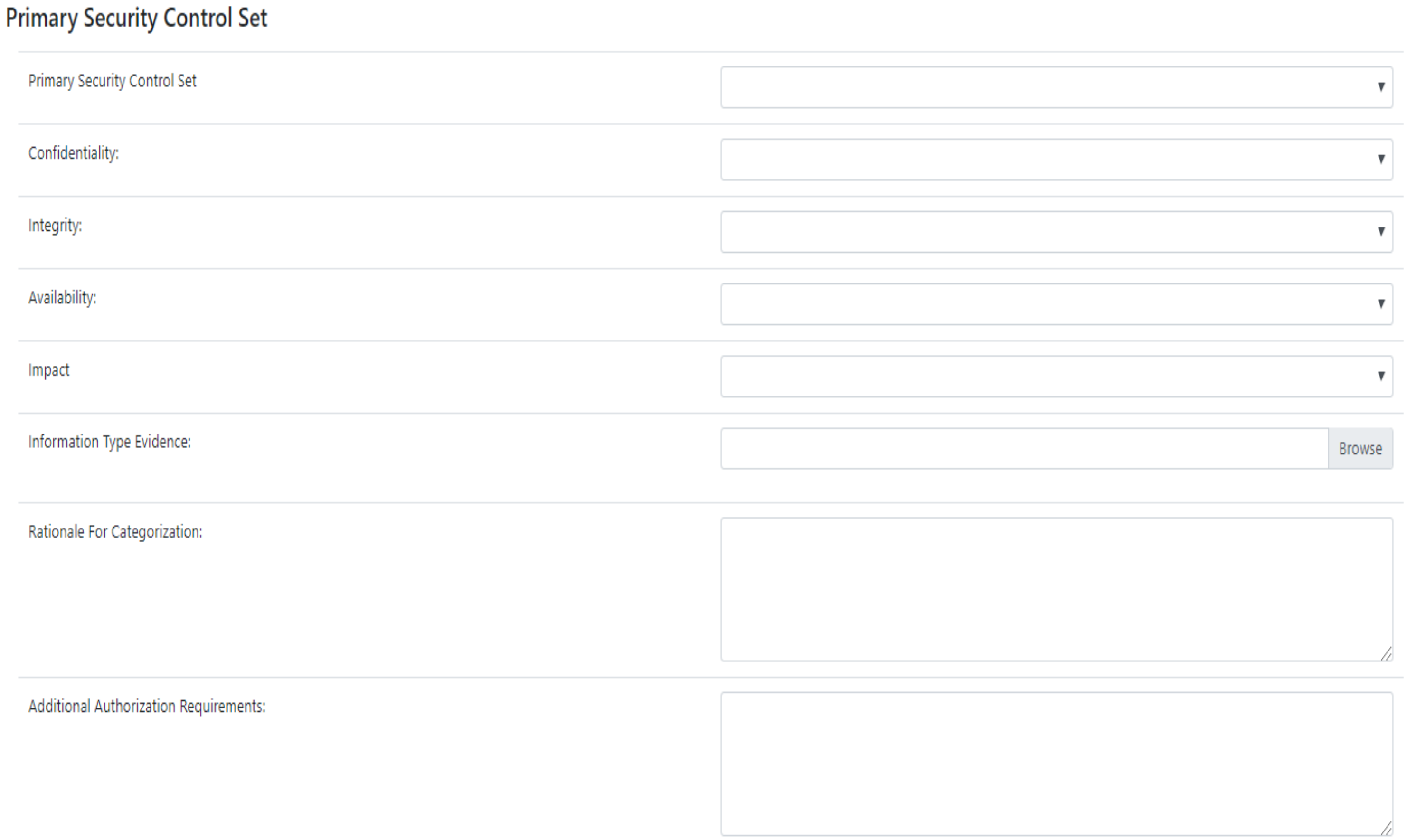
Selecting Security Controls

- Security Controls Build-Out
- Identify and Document Common (Inheritable) Controls
- Select, Tailor, and Document Security Controls
- Develop Security Control Monitoring Strategy
- Review and Approve SP
- Assign Baseline Controls in eMASS

eMASS Lab - Applying Categorization and Baseline Controls

Categorization Options

- Control Selection
- Overlays
- Manage Security Controls



Primary Security Control Set

Primary Security Control Set	▾
Confidentiality:	▾
Integrity:	▾
Availability:	▾
Impact	▾
Information Type Evidence:	Browse
Rationale For Categorization:	
Additional Authorization Requirements:	

Implementing Security Controls

- **Administrative, technical, and physical controls should work in a synergistic manner to protect a system's assets**
- Security Control Implementation
- Implement Selected Security Controls
- Document Security Control Implementation

CyberProtex

Managing Controls - Core Security

Cannot protect everything …. but we can have security measures in place to try

Managing Controls

- Restrict Access
- Perform a Security Assessment
- Survey threats that can exploit vulnerabilities
- What are the impact of identified threats
- What can we do to try to mitigate these threats
- Train employees regularly about what measures are in place
- Automation

CyberProtex

Understanding all of these components will help you provide the highest level of security possible

Managing Controls - STIGS

- STIG: Security Technical Implementation Guide
- First implemented by DISA in 1998
- STIGs provide the user community with configuration standards for DOD IA and IA-enabled devices/systems
- These guide are applied to myriad of technologies and platforms including hardware, firmware, application, and cloud-based systems
- STIGs are product-specific and document applicable DoD policies and security requirements and include best configuration practices
- If STIGs are not developed for a particular system or application, organizations can substitute a Security Requirements Guide (SRG)

Managing Controls - SCC

- SCAP: Security Compliance Application Protocol
- SCAP provides the following capabilities:
  - Policy Compliance Evaluation
  - Automated Vulnerability Assessment
- SCAP uses a number of open source resources for its checks including:
  - National Vulnerability Database
  - Common Vulnerabilities and Exposures
  - Common Vulnerability Scoring System
- Not every system has an automated SCAP process of identifying system vulnerabilities
- STIGViewer

CyberProtex

Practical Exercise
Manual Controls Implementation

Control	Brief Description	Estimate
AC-2(5)	Account Management | Inactivity Logout	
AC-7	Unsuccessful Login Attempts	
AC-17(2)	Remote Access | Protection of Confidentiality/ Integrity Using Encryption	
AT-1	Security Awareness And Training Policy And Procedures	
AT-2	Security Awareness Training	
AT-2(2)	Security Awareness Training | Insider Threat	
AU-12(1)	Audit Generation | System-Wide/ Time-Correlated Audit Trail	
CM-3	Configuration Change Control	
CM-8	Information System Component Inventory	
IA-2(4)	Identification And Authentication (Organizational Users) | Local Access to Non-Privileged Accounts	
IR-6	Incident Reporting	
MA-3(2)	Maintenance Tools | Inspect Media	
PM-4	Plan of Action and Milestones Process	
	TOTAL	

CyberProtex

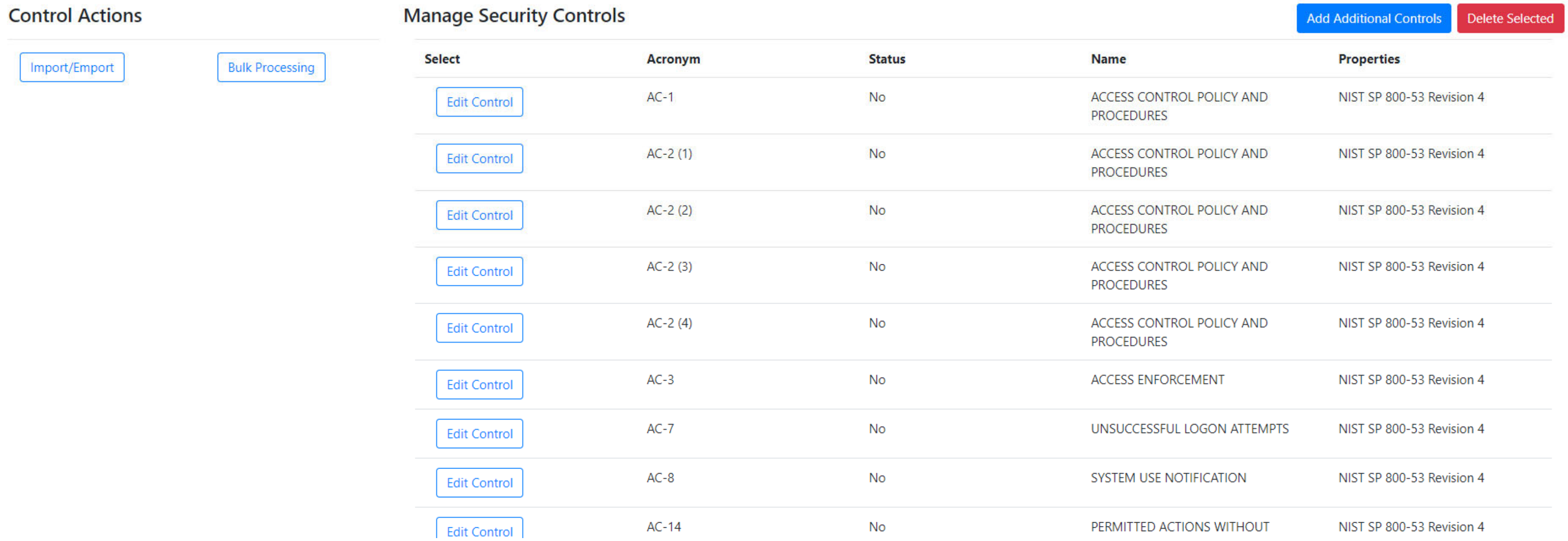
Work with a partner to come up with an estimate and be prepared to pitch it.
What tool(s) would you use?

Making Compliant Controls
Update Controls with Appropriate Information

Control	Brief Description	Estimate
AC-2(5)	Account Management | Inactivity Logout	
AC-7	Unsuccessful Login Attempts	
AC-17(2)	Remote Access | Protection of Confidentiality/ Integrity Using Encryption	
AT-1	Security Awareness And Training Policy And Procedures	
AT-2	Security Awareness Training	
AT-2(2)	Security Awareness Training | Insider Threat	
AU-12(1)	Audit Generation | System-Wide/ Time-Correlated Audit Trail	
CM-3	Configuration Change Control	
CM-8	Information System Component Inventory	
IA-2(4)	Identification And Authentication (Organizational Users) | Local Access to Non-Privileged Accounts	
IR-6	Incident Reporting	
MA-3(2)	Maintenance Tools | Inspect Media	
PM-4	Plan of Action and Milestones Process	
	TOTAL	

CyberProtex

eMASS Lab - Managing Security Controls



Select	Acronym	Status	Name	Properties
Edit Control	AC-1	No	ACCESS CONTROL POLICY AND PROCEDURES	NIST SP 800-53 Revision 4
Edit Control	AC-2 (1)	No	ACCESS CONTROL POLICY AND PROCEDURES	NIST SP 800-53 Revision 4
Edit Control	AC-2 (2)	No	ACCESS CONTROL POLICY AND PROCEDURES	NIST SP 800-53 Revision 4
Edit Control	AC-2 (3)	No	ACCESS CONTROL POLICY AND PROCEDURES	NIST SP 800-53 Revision 4
Edit Control	AC-2 (4)	No	ACCESS CONTROL POLICY AND PROCEDURES	NIST SP 800-53 Revision 4
Edit Control	AC-3	No	ACCESS ENFORCEMENT	NIST SP 800-53 Revision 4
Edit Control	AC-7	No	UNSUCCESSFUL LOGON ATTEMPTS	NIST SP 800-53 Revision 4
Edit Control	AC-8	No	SYSTEM USE NOTIFICATION	NIST SP 800-53 Revision 4
Edit Control	AC-14	No	PERMITTED ACTIONS WITHOUT	NIST SP 800-53 Revision 4

CyberProtex

Assess Security Controls - Risk assessment

- Since you can’t protect yourself if you do not know what you are protecting against, a risk assessment must be performed
- A risk assessment answers 3 fundamental questions:
  - **Identify assets** - What I am trying to protect?
  - **Identify threats** - What do I need to protect against?
  - **Calculating risks** - How much time, effort & money am I willing to expend to obtain adequate protection?
- After risks are determined, you can then develop the policies & procedures needed to reduce the risks

CyberProtex

Practical Exercise – Assess Security Controls SCA-V

SCENARIO

You have been asked to perform a SCA-V / Vulnerability assessment on the MOUS system. Before you can provide a quote, there are certain things that we need to know. What are they? Work with a partner to come up with a version for the SCA-V / Vulnerability assessment and be prepared to pitch it.

What tool(s) would you use?
How long would it take?
How many people are needed?
How much to charge customer?

Timeline

Prepare for Security Control Assessment

Develop Security Control Assessment Plan

Assess Security Control Effectiveness

Develop Initial Security Assessment Report (SAR)

Security Plan Artifacts

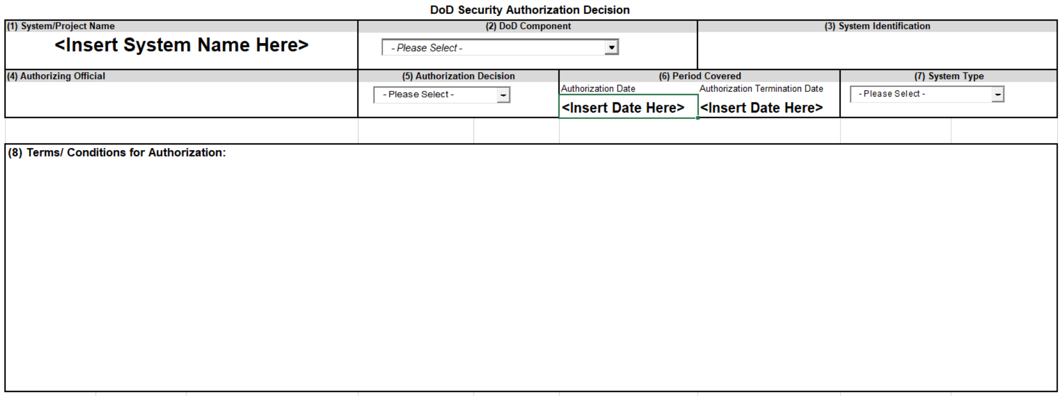
This information may include but is not limited to the list below:

- System Description Statement
- Configuration Management Plan
- Disaster Recovery Plan
- Continuity of Operations
- Contingency Plan
- Incidence Response Plan
- Risk Assessment Report
- Plan of Action and Milestones (POAM)
- System Architecture / Topology / Data Flow
- Configuration Validation Checklist
- Security Classification Guide
- System Configuration Guide
- Hardware Inventory List (use the CIO/G-6 template)
- Software Inventory List (use the CIO/G-6 template)
- Physical Security Plan
- Personnel Security Plan
- Information Assurance Vulnerability Management (IAVM) Process
- Patch Management Process, Connection Approval / System Approval documentation s) Ports, Protocols, and Services (PPS) List
- Active Directory (AD) Documentation

Authorize System

- Authorization Decision Doc
- SP
- SAR
- POA&M

CyberProtex

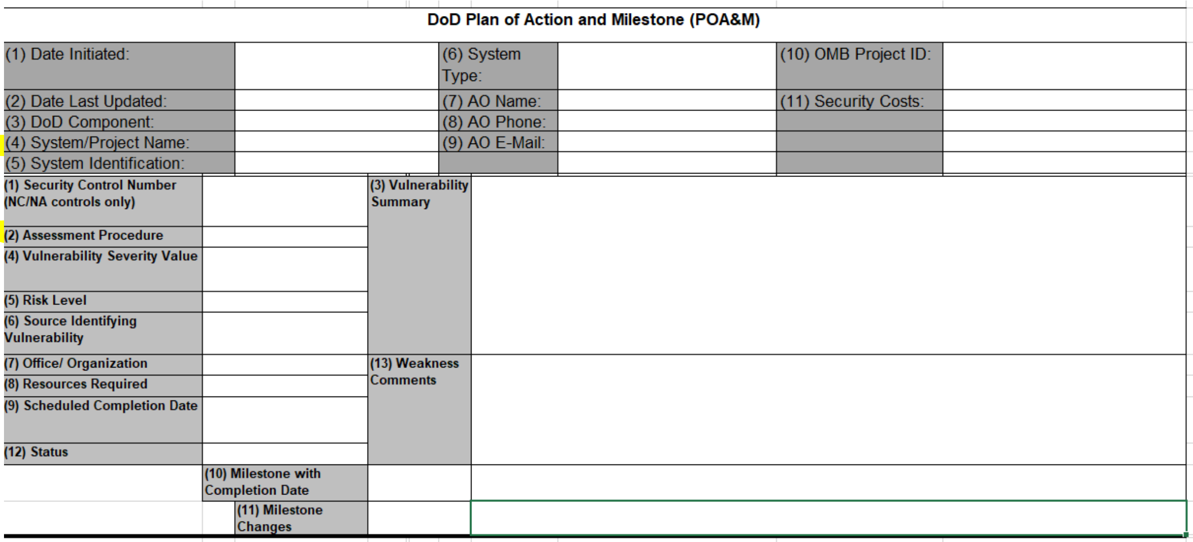


DoD Security Authorization Decision

(1) System/Project Name	(2) DoD Component	(3) System Identification
<Insert System Name Here>	- Please Select -	

(4) Authorizing Official	(5) Authorization Decision	(6) Period Covered		(7) System Type
		Authorization Date	Authorization Termination Date	
	- Please Select -	<Insert Date Here>	<Insert Date Here>	- Please Select -

(8) Terms/ Conditions for Authorization:



DoD Plan of Action and Milestone (POA&M)

(1) Date Initiated:		(6) System Type:		(10) OMB Project ID:	
(2) Date Last Updated:		(7) AO Name:		(11) Security Costs:	
(3) DoD Component:		(8) AO Phone:			
(4) System/Project Name:		(9) AO E-Mail:			
(5) System Identification:					

(1) Security Control Number (NC/NA controls only)		(3) Vulnerability Summary	
(2) Assessment Procedure			
(4) Vulnerability Severity Value			
(5) Risk Level			
(6) Source Identifying Vulnerability			
(7) Office/ Organization		(13) Weakness Comments	
(8) Resources Required			
(9) Scheduled Completion Date			
(12) Status			
	(10) Milestone with Completion Date		
	(11) Milestone Changes		

Continuous Monitoring

Everyday Tools to Make Life Easier

T5529 :.$:$225=9 ?5; :5 &8/4+ :5+):.)8?5;8(/96$8$:) ($:$ 9):9 $4(92/′) $4((/′) :.)3 /4 $ =$? :.$:8)<)$29 /49/+. :9 =/:. :.) 2)$9:6599/&2))**58:nT.8)$: .;4:/4+ ′$4 /4<52<) $ 3 $99/<) $3 5;4:5* /4*583 $:/54q95 = ./2) /: /9 $.;3 $4i 2)( )**58:q?5;y22′)8:$/42? 4))(953) ′53 6;:)8 $99/9:$4′) :5 3 $1) :.) :$91 3 58) 3 4+)$&2)

- Know your landscape
- System commands
- Wireshark – real time capture and analysis
- Log analysis
- File integrity
- Scripts

CyberProtex

Continuous Monitoring – Practice Security

Current Environment

- Information Assurance Vulnerability Management (IAVM) Process

- Patch Management Process, Connection Approval / System Approval documentation s) Ports, Protocols, and Services (PPS) List

CyberProtex

Questions????

- Check out our automated RMF Compliance Software the Vulnerability Genius ™

Ben McGee

bmcgee@cyberprotex.com

256.401.7072

cyberprotex.com