

1



2

## BAI ACTIVITY

- RMF Fundamental Concepts Quiz
  - Refresh knowledge from yesterday's class
  - To prepare for our continued walk through the RMF steps



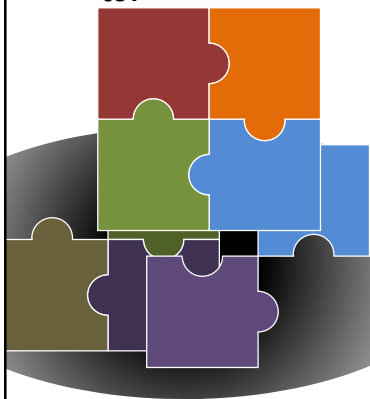
© 2024

3

3

## BAI Learning Goals

- This course has been designed to prepare you to be able to:



- ◆ Categorize the system
- ◆ Select and assign roles
- ◆ Select and tailor controls
- ◆ Plan an assessment
- ◆ Create a continuous monitoring plan
- ◆ Identify compliance testing tools
- ◆ Plan a successful project
- ◆ Find supporting resources

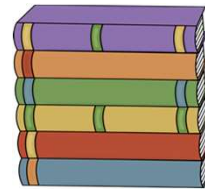
© 2024

4

4

## BAI Introduction to the Course Material

- Course Materials for the In-Depth students:
  - Course book onsite includes a hard-copy version of the slides
  - Online students receive three pdf files:
    - DB1-RMF for DoD IT In Depth Part 1
    - DB2-RMF for DoD IT In Depth Part 2
    - DB3-RMF for DoD IT In Depth Part 3
  - In Depth package for both onsite and online also includes "Participants Reference Guide" and "Participants Course Activities Guide"



© 2024

5

5

## BAI RMF Publications Library

Referenced Publications (i.e., NIST, CNSS, DoD, etc.) are available for download from the <https://rmf.org> website under RMF Resources/RMF Publications.

Laws/Executive Orders      FIPS Publications      NIST Special Publications      CNSS Publications      DoD Directives/Instructions



© 2024

<https://rmf.org/index.php/rmf-documents>

6

6

## BAI Course Format



© 2024

7

7

## BAI Primary Resources

- NIST:
  - NIST SP 800-37 R2 Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy
  - FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems
  - NIST SP 800-60 Volumes 1 & 2: Guide for Mapping Types of Information and Systems to Security Categories
- CNSSI:
  - CNSSI 1253 Security Categorization and Control Selection for National Security Systems
- DoD:
  - DoDI 8500.01 Cybersecurity
  - DoDI 8510.01 RMF for DoD IT
  - RMF Knowledge Service <https://rmfks.osd.mil>
  - eMASS

© 2024

8

8

## BAI Knowledge Service (KS)

- "Authoritative source" for RMF procedures and guidance, e.g.
  - Guidance on Life Cycle Steps
  - Assessment procedures
  - Security control overlays
- Maintained by RMF Technical Advisory Group (TAG)
- <https://rmfks.osd.mil>
  - Accessible by CAC, or ECA Certificate with approval of a DoD employee
- KS content is used throughout this course



© 2024

9

9

## BAI RMF Knowledge Service

The screenshot displays the RMF Knowledge Service website. At the top, the BAI logo is followed by "RMF Knowledge Service". Below this is a navigation bar with links: RMF Implementation, RMF for DoD Technology, Controls and Authorization, RMF Policy and Governance, Collaboration, and Help and Resources. A search bar is on the right. The main content area features the "RMF Process Wheel" with a circular diagram showing seven steps: CATEGORIZE, PREPARE, SELECT, IMPLEMENT, ASSESS, MONITOR, and REAUTHORIZE. To the left of the wheel is a text box explaining the RMF process. Below the wheel is a red box with the text: <https://rmfks.osd.mil> Requires CAC or ECA (With Sponsorship). At the bottom, there are links for RMF Knowledge Service, Security Controls Explorer, RMF Process Wheel, Recent Discussions, Most Viewed Pages, and Recent Site Changes.

<https://rmfks.osd.mil/>  
Requires CAC or ECA certificate

CAC holders must select email certificate


© 2024


10

10

## BAI eMASS: Enterprise Mission Assurance Support System

- Designed to provide full support for DoDI 8500 series
- Supports DoD's ongoing effort to automate services supporting IA management at DoD component level
  - Creates and maintains essential documentation (SP, SAR, POAM, supporting objects/artifacts)
  - Primary reporting for every system throughout System Development Life Cycle (SDLC)
  - Enterprise application, providing:
    - Workflow
    - Data repository
    - Documentation assistance for IS Assessment and Authorization





eMass has a significant learning curve. Training is mandatory!

© 2024 11

11

## BAI Knowledge Service Training

- Knowledge Service provides:
  - 24/7 access to latest RMF Policy and Guidance
  - Manual guidance for RMF implementation
  - Sample templates and examples for manual implementation
  - Updated policy or guidelines before eMASS
  - Discussion forums, FAQs and collaboration features
- eMASS provides:
  - An automated tool for the DoD user community
  - Ability to process workflow activities within RMF
  - Enterprise visibility, reporting and inheritance functions
  - Storage of documentation and artifacts to support assessment
  - Process to create Security Authorization Package
  - Capability to digitally sign system Authorization

© 2024 12

12

## BAI DoD Cyber Exchange (previously DISA IASE)

- Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) now moved to DoD Cyber Exchange
- Primary DoD source for RMF related: DISA STIGs/CCIs; Training; Cybersecurity Topics



### LIST OF TOPICS

Community Gold Standard (CGS)

Cross Domain Enterprise Service (CDES)

Cyber Sam

Cyber Workforce Management Program

(DoDD 8140.01 & DoD 8570.01-m)

Defense Collaboration Services (DCS)

DoD Cloud Computing Security

### LIST OF CYBER RESOURCES

About the DoD Cyber Exchange

Approved Products List (APL)

Conferences & Workshops

Cybersecurity Acronyms

DoD Cyber Exchange Public (<https://public.cyber.mil>)

or

DoD Cyber Exchange CAC Holder (<https://cyber.mil>)

© 2024

13

13

## BAI Can RMF be modified?

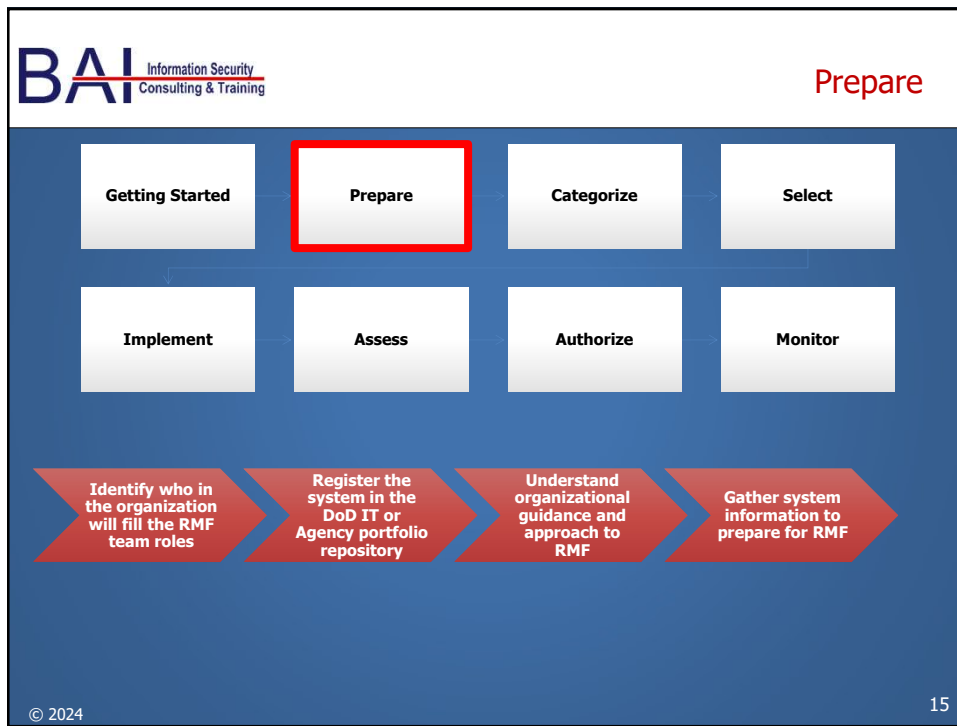
- Why to deviate from the RMF steps\*
  - To align to internal management and system development life cycle processes
  - To execute tasks more cost-effectively and efficiently
- Before an information system is placed into operation, the last step must be authorizing official's explicit acceptance of risk

\*NOTE: Generally, the RMF process steps are sequential.  
Tasks within each step may be suitable for altering.

© 2024

14

14



15

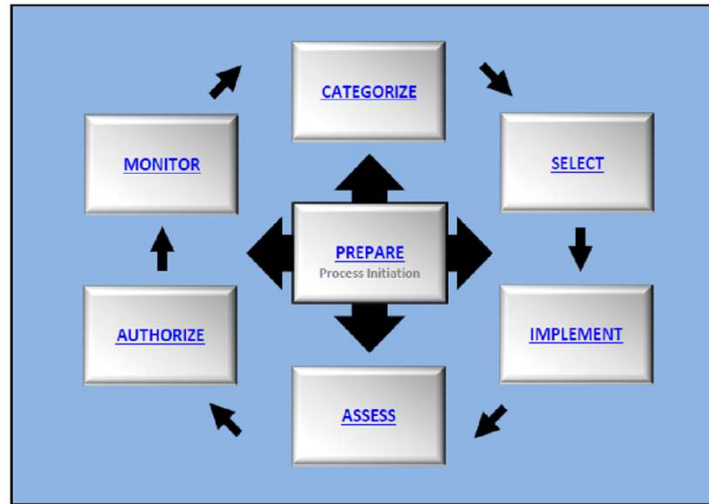


16



## BAI RMF Life Cycle

Addition of Preparation Step (NIST SP 800-37 R2):



© 2024

Source NISP SP 800-37 R2

17

17

## BAI Where We Are In the RMF for DoD Process



© 2024

Source: DoD Knowledge Service

18

18

## BAI Organization Preparation Requirements

- New Organizational Requirements cited in SP 800-37 R2
  1. Identify key roles in performing Risk Management Framework
  2. Determine an organization Risk Management Strategy with risk tolerance levels
  3. Complete organization-wide risk assessment
  4. Determine organizationally-tailored baselines and/or Cybersecurity Framework profiles (as needed)
  5. Identify organization-wide Common Controls
  6. Prioritize impact levels of organization systems
  7. Develop an organization-wide approach to continuous monitoring

© 2024

19

19

## BAI System Preparation - Gather Information

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>■ System General and Technical Description               <ul style="list-style-type: none"> <li>■ System Name &amp; Acronym</li> <li>■ New or Existing System?</li> <li>■ Where in the SDLC Process?</li> </ul> </li> <li>■ Key individuals and primary organizations involved in the process? In the Mission Area?               <ul style="list-style-type: none"> <li>■ Who ultimately approves the system for operations?</li> <li>■ Who supports the RMF process?</li> <li>■ RMF Primary Team Members</li> <li>■ Training; Orientation Meetings</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>■ Preliminary Artifacts               <ul style="list-style-type: none"> <li>■ Mission/Business Processes</li> <li>■ Organization's primary function?</li> <li>■ Information System Boundary</li> <li>■ What components need to be authorized? Hardware? Software?</li> <li>■ What interfaces exist with other systems?</li> <li>■ What types of information are being processed?</li> <li>■ Common Control Provider agreement</li> <li>■ Privacy Impact Assessment</li> <li>■ Previous Authorization</li> <li>■ Previous POA&amp;M</li> </ul> </li> </ul> |
|--|---|
- Apply Risk Assessment, e.g.
    - Information Security Requirements
    - Laws, Directives, Policy, Guidance
    - Threats, Vulnerabilities
    - Likelihood, Impact
- NIST SP 800-37 R2 adds a step called PREPARATION to gather information at both the Organizational and System levels.

© 2024

20

## BAI Where to Begin – Gain Agreement

- RMF success depends on System Requirements to be:
  - Complete
  - Accurate
  - Thorough
  - With buy-in and agreement from all the relevant stakeholders



© 2024

21

21

## BAI Organizational Preparation Develop Risk Management Strategy

- **Organization identifies assumptions as to how risk is assessed, responded to and monitored.**
  - Determine common terminology, frame of reference, risk assessment methodologies
  - Based on organization governance, culture and mission/business functions.
- **Organization identifies constraints on conduct of risk assessment, response and monitoring.**
  - Financial limitations
  - Legal or regulatory requirements
  - Contractual restraints
- **Organization identifies level of risk tolerance.**
  - Level of risk organization is willing to accept
  - Can affect AO acceptance of risk at system level
- **Organization identifies priorities and trade-offs**
  - Ex. Accepting short-term risk of degraded operations to achieve long-term goal
  - Can influence implementation of security controls

© 2024

(Resource NIST SP 800-39)




22

22

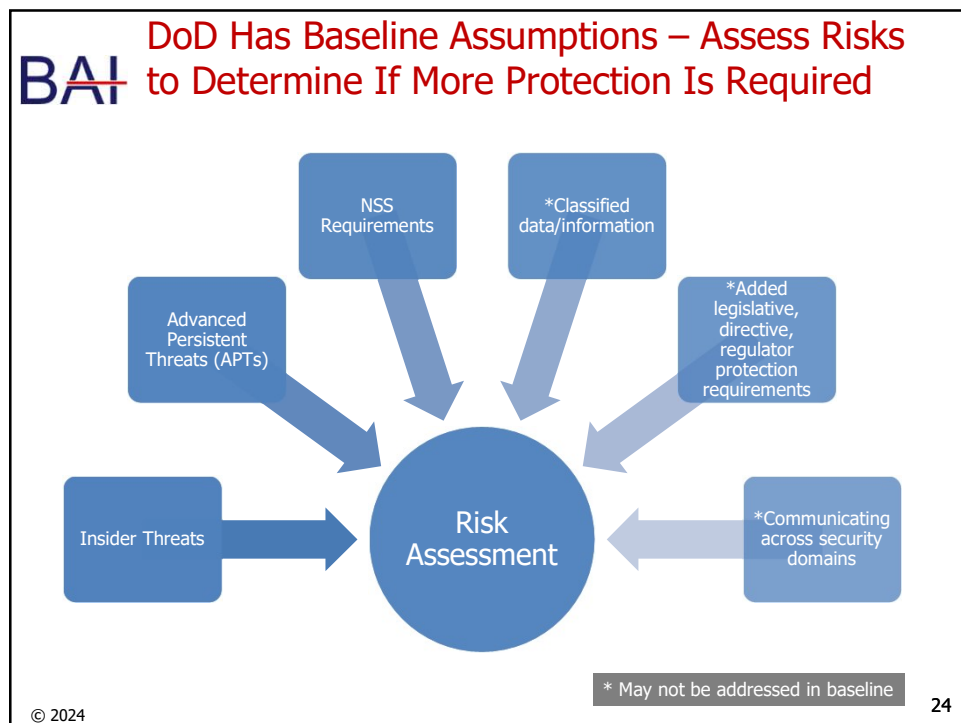
**BAI** **System Preparation**  
**Risk Assessment, Response and Monitoring**

- **Risk Assessment**
  - Identify threats & vulnerabilities
  - Determine likelihood, impact and risk (low, moderate, high)
  - Communicate risk to decision makers
- **Risk Response**
  - Identify courses of action to respond to risk
    - Accept risk based on situation and conditions; consider organizational risk tolerance level
    - Avoid risk by choosing to eliminate activity, process or technology causing risk
    - Mitigate risk via safeguard or countermeasure
    - Transfer or share risk by shifting liability or responsibility to another organization
  - Evaluate and implement alternative course of action
- **Risk Monitoring**
  - Identify risk monitoring strategy for organization to include purpose, type and frequency
  - Monitor on ongoing basis to address compliance, effectiveness and identify any changes

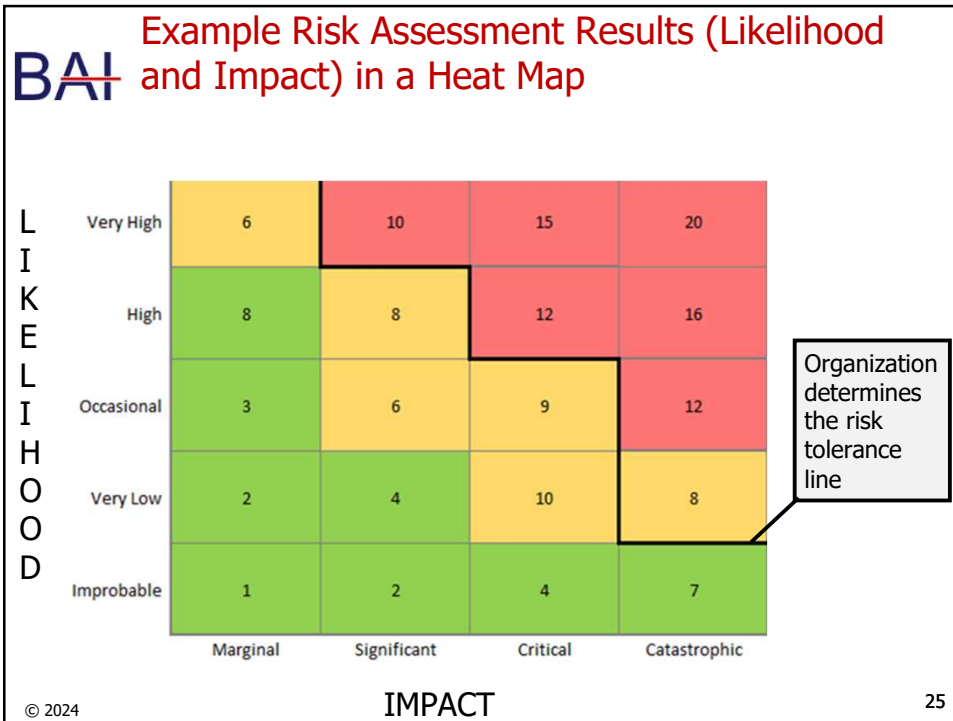
***Sounds like Risk Management Framework!***  
***More on risk to come as we explore the steps of RMF.***

© 2024  23

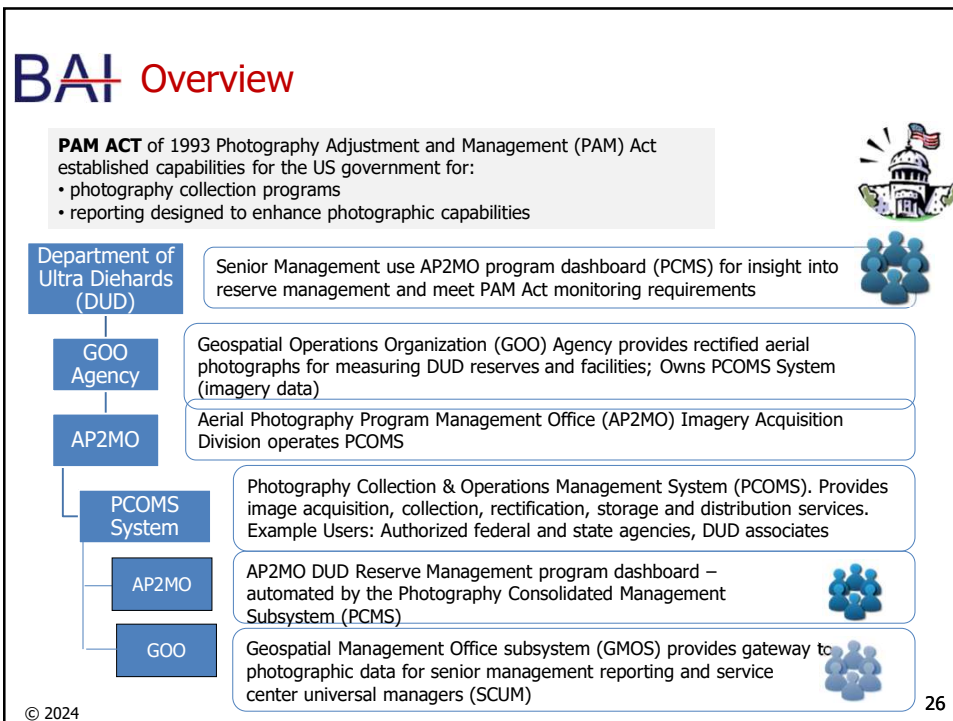
23



24



25



26

## BAI Informal Risk Assessment Activity

- Purpose of risk assessment activity:
  - Ensure a common understanding about risk assessment
  - Establish risk assessment as an essential element of risk management:
    - Decision-making
    - Prioritization
    - Risk reporting



© 2024

27

27



28

## BAI Identify Key Roles and Responsibilities

- Government Contracting Officer Representative (COR)\*
- Contractor Project Manager\*
- Information System Owner (ISO)/Program Manager (PM)
- Information System Security Manager (ISSM)
- Information System Security Officer (ISSO)
- Information Systems Security Architect/Engineer (ISSA/ISSE)
- Senior Information Security Officer (SISO)
- Authorizing Official (AO)
- Security Control Assessor (SCA)
- User Representative (UR)
- **Extended team - building relationships will help with control implementations**
  - Developers
  - System Administrators
  - Network Administrators
  - Database Administrators
  - Application Administrators
  - Personnel Security Officer
  - Facilities Management and Security Personnel
  - Operational Security/Physical Security
  - Training Officer

\*Roles unique to contractor developed systems

© 2024

29

29

## BAI Personnel Considerations DoD Cyber Workforce Framework

- Assign qualified personnel to RMF roles and document in the Security Plan.
- Requirements for cybersecurity personnel:
  - Qualification standards per DoDD 8140.01 Cyberspace Workforce Management, October 2020
- DoD Cyber Workforce Framework (DCWF) now available to identify cyber personnel categories and work roles
  - DoDI 8140.02, December 2021
- DoDM 8140.03 published February 2023

© 2024

30

30

## BAI Former DoDD 8570.01 Versus DoDD 8140 series

### DoDD 8570.01

- DoD Directive 8570.01 Information Assurance Training, Certification and Workforce Management
- Enterprise-wide requirements for training, qualifying, and managing DoD IA workforce
- Accompanying manual DoD 8570-M provided supporting detail

### DoDD 8140.01

- Partially implemented August 2015 – Final publication, Cyberspace Workforce Management, October 2020
- Includes NICE framework categories/tasks

### DoDM 8140.03

- Cyberspace Workforce Qualification and Management Program
- Published February 2023

### DoDI 8140.02

- Identification, Tracking, and Reporting of Cyberspace Workforce Requirements
- Published December 2021

© 2024

31

31

## BAI National Initiative for Cybersecurity Education (NICE) Framework

 <p style="text-align: center;"><b>DoD DIRECTIVE 8140.01</b> <b>CYBERSPACE WORKFORCE MANAGEMENT</b></p> <hr/> <p><b>Originating Component:</b> Office of the DoD Chief Information Officer</p> <p><b>Effective:</b> October 5, 2020</p> <p><b>Releasability:</b> Cleared for public release. Available on the Directives Division Website at <a href="https://www.esd.whs.mil/DD/">https://www.esd.whs.mil/DD/</a>.</p> <p><b>Revises and Cancels:</b> DoD Directive 8140.01, "Cyber", August 11, 2015, as amended</p>	 <p style="text-align: center;"><b>DoD INSTRUCTION 8140.02</b> <b>IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS</b></p> <hr/> <p><b>Originating Component:</b> Office of the DoD Chief Information Officer</p> <p><b>Effective:</b> December 21, 2021</p> <p><b>Releasability:</b> Cleared for public release. Available on the Directives Division Website at <a href="https://www.esd.whs.mil/DD/">https://www.esd.whs.mil/DD/</a>.</p> <p><b>Approved by:</b> E. Fletcher, Performing the Duties of the DoD Chief Information Officer</p>
 <p style="text-align: center;"><b>DoD MANUAL 8140.03</b> <b>CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM</b></p> <hr/> <p><b>Originating Component:</b> Office of the DoD Chief Information Officer</p> <p><b>Effective:</b> February 15, 2023</p> <p><b>Releasability:</b> Cleared for public release. Available on the Directives Division Website at <a href="https://www.esd.whs.mil/DD/">https://www.esd.whs.mil/DD/</a>.</p> <p><b>Incorporates and Cancels:</b> DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2015, as amended</p> <p><b>Approved by:</b> Julius B. Shannon, DoD Chief Information Officer</p>	


© 2024

32

32



## BAI NICE: 7 Categories – 32 Specialty Areas

Analyze (AN)	Threat Analysis (TWA)	Exploitation Analysis (EXP)	All-Source Analysis (ASA)	Targets (TGT)	Language Analysis (LNG)		
Collect and Operate (CO)	Collection Operations (CLO)	Cyber Operational Planning (COP)	Workforce Elements				
Investigate (IN)	Cyber Investigation (INV)	Digital Forensics (FOR)	Work Roles				
			Knowledge, Skills, Abilities and Tasks				
Operate and Maintain (OM)	Data Administration (DTA)	Knowledge Management (KMG)	Customer Service and Technical Support (STS)	Network Services (NET)	Systems Administration (ADM)	Systems Analysis (ANA)	
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Training, Education, and Awareness (TEA)	Cybersecurity Management (MGT)	Strategic Planning and Policy (SPP)	Executive Cyber Leadership (EXL)	Program /Project Management (PMA) and Acquisition	
Protect and Defend (PR)	Cybersecurity Defense Analysis (CDA)	Cybersecurity Defense Infrastructure Support (INF)	Incident Response (CIR)	Vulnerability Assessment and Management (VAM)			
Securely Provision (SP)	Risk Management (RSK)	Software Development (DEV)	Systems Architecture (ARC)	Technology R&D (TRD)	Systems Requirements Planning (SRP)	Test and Evaluation (TST)	Systems Development (SYS)

© 2024

33

33

## BAI DoD Cyber Workforce Framework (DCWF)



**FRAMEWORK**

**Cyber Workforce Navigation**

- Overview
- DoD Cyber Workforce
- Cyber Workforce Strategies
- DoD Cyber Workforce Framework (DCWF)
- Cyber Workforce Management
- Federal Cybersecurity Workforce Assessment Act (FCWAA)
- Cyber Excepted Service Personnel System (CES)
- Chief Digital and AI Officer (CDAO)
- College of Information and Cyberspace (CIC)
- Cyber Scholarship Program (CySP)
- Cyber Information Technology Exchange Program (CITEP)
- Info For DoD Participants
- Info For Industry Participants
- Useful Resources
- Resources
- Contact Us

**The DoD Cyber Workforce Framework (DCWF)**

Cyberspace is a warfighting domain that continues to evolve in terms of threat and complexity. As a result, the cyber workforce must also evolve to address the challenges posed by our adversaries and meet strategic mission requirements. A part of this requires reshaping our understanding of the cyber workforce to include all personnel who build, secure, operate, defend, and protect United States cyber resources; conduct cyber-related intelligence activities; and enable current and future cyber operations.

The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCTCS). It has a hierarchical structure with seven broad categories, 33 specialty areas, and 54 work roles. Each work role contains a definition, as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions. Work roles vary in terms of breadth (requirements spanning multiple sets of functions) and depth (requirements focused on a related set of functions).

The DCWF will facilitate uniform identification, tracking, and reporting required by the Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015. It will also be used to develop qualification requirements for cyber work roles that will be outlined in DoD Manual 8140. Finally, the DCWF can also be used to support a number of other DoD-wide workforce management and planning activities. For example, it can be used to facilitate supply and demand analyses, develop targeted recruitment and retention strategies, develop horizontal and vertical career paths, and standardize development of civilian position descriptions. As such, the DCWF serves as an important building block for a capable and ready cyber workforce.

To increase understanding and use of the DCWF, the DoD CIO collaborated with DISA to create the DCWF Tool, an interactive online tool for stakeholders to identify, organize, and manage the tasks and KSAs of the cyberspace workforce in accordance with the DoD policy.

© 2024

<https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx>

34

34

## BAI Sample Work Role Qualification Matrix

DoDM 8140.03, February 15, 2023

Figure 1: Sample Work Role Qualification Matrix

		Proficiency Levels		
		Basic	Intermediate	Advanced
Foundational Qualification Options – Demonstration of knowledge	Education	Option OR	Option OR	Option OR
	Training	Option OR	Option OR	Option OR
	Personnel Certification	Option	Option	Option
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification – Demonstration of Capability	On-the-Job Qualification	Always Required	Always Required	Always Required
	Environment Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Current with technology, hostile actor tactics	Continuous Professional Development	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.

© 2024

35

35

## BAI ISSM Matrix – DoD 8140 Certifications and Education (<https://cyber.mil>)

(722) Information Systems Security Manager					
		Basic	Intermediate	Advanced	NOTES
Foundational Qualification Options	Education	Associate degree or higher from an accredited college or university	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	When Education is listed, recommend an accredited Computer Science, Cyber Security, Information Technology, Software Engineering, Information Systems, or Computer Engineering degree; or a degree in a Mathematics or Engineering field.
	Training	OR Offerings listed in DoD 8140 Training Repository	OR Offerings listed in DoD 8140 Training Repository	OR Offerings listed in DoD 8140 Training Repository	
	Personnel Certification	GSEC or Security+	CAP or CASP+ or CCISO or CCSP or CISM or CISSP or Cloud+ or SSCP	CISSP-ISSMP or GSLC	See the Certification Index tab at the end of this document for certification vendor information.
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative	Refer to Section 3 of the DoD 8140 Manual for more information.
Residential Qualification	On-the-Job Qualification	Always Required	Always Required	Always Required	Individuals must demonstrate capability to perform their duties in their resident environment.
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion	
Annual Maintenance	Continuous Professional Development	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	

© 2024

Source: DoD 8140 Cyberspace Training Repository

36

36

## BAI Artifacts Resulting from Preparation

- System Description/CONOPS/System Boundary drawing
- System Architecture drawing (to include cloud if applicable)
- Data Flows/Ports and Protocols (if applicable)
- Hardware/Software Inventory (if applicable)
- Interconnecting Systems/Sub-systems (chart or drawing)
- Privacy Impact Assessment (DoD form DD 2930)
- Any current ATO or ATO w/Conditions

© 2024

37

37

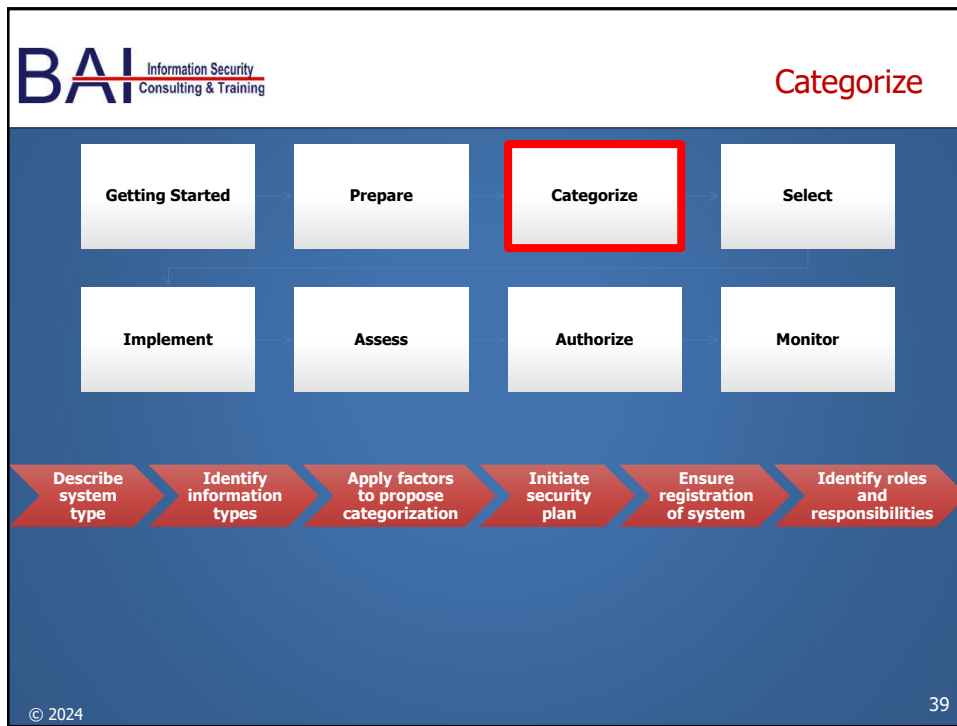
## BAI Artifacts Resulting from Preparation

- Any current Plan of Action & Milestones (POA&M)
- Waivers or unique/approved requirements
- Common Control Provider Agreements (MOA, SLA, Contract)
- Risk Assessment Report (threats, vulnerabilities)
- Contact Information for System Stakeholders
- Contact Information for RMF Lead/Primary RMF Team
- Contact Information for Extended Team

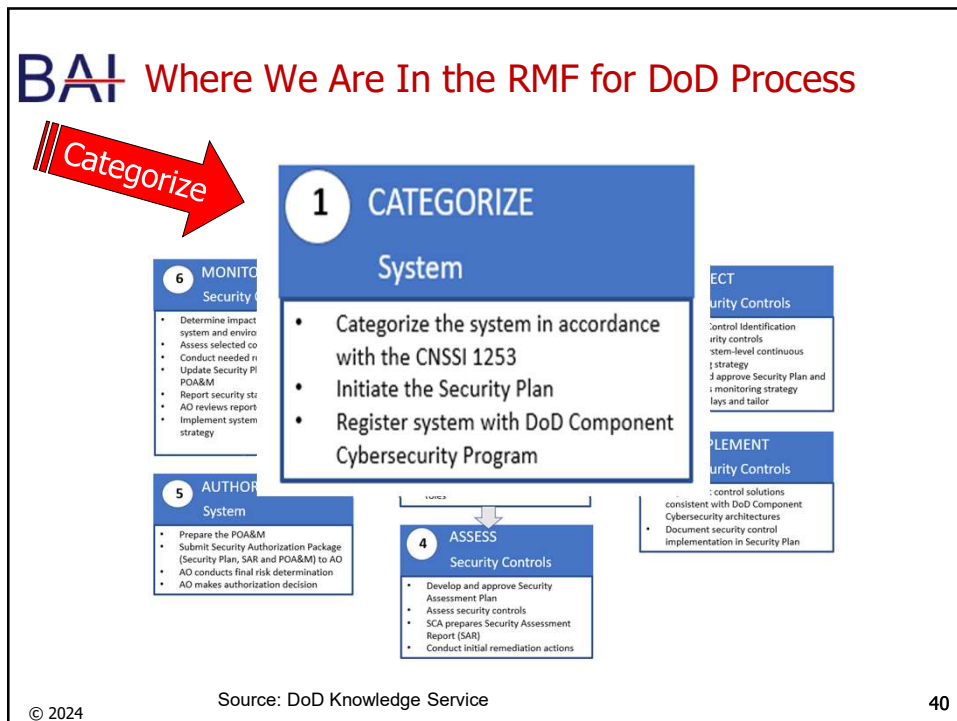
© 2024

38

38



39



40

**BAI** System Categorization (DIACAP vs. RMF)

	MAC	CL
DIACAP	I	Classified
	I	Sensitive
	I	Public
	II	Classified
	II	Sensitive
	II	Public
	III	Classified
	III	Sensitive
	III	Public

	Confidentiality	Integrity	Availability
RMF	High	High	High
	High	High	Moderate
	High	High	Low
	High	Moderate	High
	High	Moderate	Moderate
	High	Moderate	Low
	High	Low	High
	High	Low	Moderate
	High	Low	Low
	Moderate	High	High
	Moderate	High	Moderate
	Moderate	High	Low
	Moderate	Moderate	High
	Moderate	Moderate	Moderate
	Moderate	Moderate	Low
	Moderate	Low	High
	Moderate	Low	Moderate
	Moderate	Low	Low
	Low	High	High
	Low	High	Moderate
	Low	High	Low
	Low	Moderate	High
	Low	Moderate	Moderate
	Low	Moderate	Low
Low	Low	High	
Low	Low	Moderate	
Low	Low	Low	

© 2024

41

**BAI** Initiate Security Plan

**Plan Contains**

- Security categorization results
- Information system description (including system boundary)
- Requirement's overview
- Qualified personnel by:
  - Role
  - Name
  - Contact information

Next: Categorize the System

**Guidance**

- DoD:
  - Knowledge Service
  - eMASS
- Federal "civil" agencies
  - NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems

Note: The NIST SP 800-18 contains a template that can be used by the Federal "civil" community to build their Security Plan. It does not contain all elements required for the DoD Community.

© 2024

42

## BAI Categorize the System

### NIST SP 800-60

#### Volume 1 – Guidelines

- Security categorization process overview
- Security objectives and corresponding security impact levels (per FIPS 199)
- Security categorization terms and definitions (per FIPS 199)

### NIST SP 800-60

#### Volume 2 – Reference

- Provisional security impact level assignments & rationale by information type
  - Appendix C: Management and support information
  - Appendix D: Mission-based information (mission information and services delivery mechanisms)

© 2024

43

43

## BAI Impact Values Based on Information Types: Processed, Stored, Transmitted

### E.g., Application data elements

- First and last names
- Home and work addresses
- Work phone
- SSN
- Bank account number
- Federal Gov't Building Management Procedures
- Federal Funds Payments
- In-house Software Maintenance Procedures
- Border Patrol Procedures & Schedules

### E.g., IT related data elements

- System configurations
- System and security event logs
- Password hash (Windows-based system) files
- Intrusion monitoring and auditing
- Network performance and health

© 2024

Course Guide: NIST SP 800-60 V2 (Information types)



44

44

## BAI Determine Impact

### C.2.3.5 Budget Execution Information Type

Budget Execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The recommended provisional security categorization for budget execution information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget execution information on the ability of responsible agencies to manage day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The effects of loss of confidentiality of most budget execution information are unlikely to pose the threat of serious harm to agency assets, personnel or operations.

**Special Factors Affecting Confidentiality Impact Determination:** The effects of loss of confidentiality of budget execution information can violate privacy regulations, reveal information proprietary to private institutions, and reveal procurement-sensitive information. In aggregate, budget execution information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from *moderate to high*. Public release of sensitive budget execution information can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

© 2024

45

45

## BAI FIPS 199 Impact Values for DoD

### Per CNSSI 1253, Section 3.1:

For Moderate and High potential impact, append "...**exceeding mission expectations**" to the sentence in FIPS 199.

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Availability</b> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

© 2024

46

46



## BAI Information Types

- Example: Human Resource Management
- See Course Guide

<i>Human Resource Management</i>			
HR Strategy	Low	Low	Low
Staff Acquisition	Low	Low	Low
Organization and Position Management	Low	Low	Low
Compensation Management	Low	Low	Low
Benefits Management	Low	Low	Low
Employee Performance Management	Low	Low	Low
Employee Relations	Low	Low	Low
Labor Relations	Low	Low	Low
Separation Management	Low	Low	Low
Human Resources Development	Low	Low	Low

Source: NIST SP 800-60 V2, Appendix C



© 2024

47

47

## BAI Select Provisional Impact Levels (2 of 2)

- Mission information types
- NIST SP 800-60, V2 APPENDIX D, Table D2
- See Course Guide

**Table D-2: Security Categorization of Mission Information**

	Confidentiality	Integrity	Availability
<i>Defense &amp; National Security</i>	<b>Nat'l Security</b>	<b>Nat'l Security</b>	<b>Nat'l Security</b>
<i>Homeland Security</i>			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	High	High	High
Catastrophic Defense	High	High	High
Executive Functions of the EOP <sup>23</sup>	High	Moderate	High
<i>Intelligence Operations</i> <sup>24</sup>	High	High	High
<i>Disaster Management</i>			
Disaster Monitoring and Prediction	Low	High	High
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low
Emergency Response	Low	High	High

© 2024

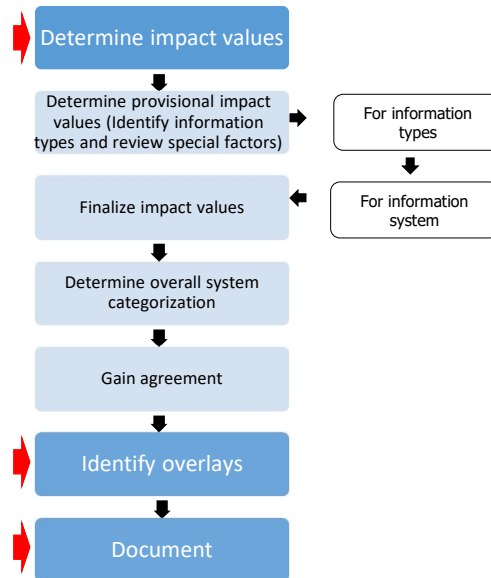
48

48



## BAI Categorize Process Overview

- Red arrows point to the major steps:
  - Determine impact values
  - Identify overlays
  - Document the process
- Overlays promote reciprocity of systems and security controls
- CNSSI 1253 process identifies overlays in Categorize – and applies them during Step 2 - Select.



© 2024

49

49

## BAI Impact Values Based on Information Type

- Define data classification, protection, and processing requirements
- Review information types in NIST SP 800-60 V2, e.g.
  - Privacy
  - Medical, etc.
- Information Owner (IO) is responsible

**Next:** Impact values based on:

- Management & support information type, and/or
- Mission information type

© 2024

50

50

**BAI** Review/Adjust/Finalize "Information Type" Impact Levels

- Review provisional impact levels based on (Guidance in NIST SP 800-60 V1):
  - Organization
  - Environment
  - Mission
  - Use
  - Data Sharing
- Review and adjust security objective impact levels (NIST SP 800-60 V2, Appendices C and D "Special Factors")
- Document adjustments and provide the rationale or justification for the adjustments

```

graph TD
    A[Determine impact values] --> B[Determine provisional impact values  
(Identify information types and review special factors)]
    C[For information types] --> B
    D[For information system] --> B
    B --> E[Finalize impact values]
    E --> F[Determine overall system categorisation]
    F --> G[Gain agreement]
    G --> H[Identify overlays]
    H --> I[Document]
  
```

© 2024 51

51

**BAI** Finalize Impact Levels

- Review/Adjust/Finalize system security category impact levels
- Factors that may raise system impact level higher than security objective impact
  - Confidentiality
    - PII, Reference NIST SP 800-122, Guide to Protecting Personally Identifiable Information (PII)
  - Integrity
    - Time Sensitivity/criticality – Weather data in terminal approach during aircraft landing
    - Extenuating Circumstances – Critical process flows or security capabilities
  - Availability
    - Number of other systems reliant on its operation
    - Overall cost of replacement
  - Recommended: Refer to the business impact analysis
  - Process reference NIST SP 800-60 V1, 4.4.2

© 2024 52

52



## Summary: Categorize in DoD Requires Three Impact Values

- Systems are categorized as High, Moderate or Low for each of the three security objectives (C-I-A)
- Process:
  - Analyze the system and determine each of the "information types" processed or stored
  - For each information type:
    - Use NIST SP 800-60 to obtain an initial categorization
    - Adjust the categorization to account for "special factors"
  - For each security objective:
    - Select the highest categorization level among all the information types

Info Type	C	I	A
Disaster Prediction	L	H	H
Disaster Planning	L	L	L
Emergency Response	L	H	H

System Categorization is:  
Confidentiality: LOW  
Integrity: HIGH  
Availability: HIGH

© 2024

53

53



## NSS All DoD versus non-NSS (non-DoD)

- NSS + all DoD systems
  - CNSSI 1253 methodology (comparable to FIPS 199)
  - Separate categorization levels:
    - Confidentiality (C)
    - Integrity (I)
    - Availability (A)
    - Each is discrete
    - Table D1 cross-references to 800-53 for C, I, and A
  - Additional factors may affect Confidentiality categorization
  - Overlays supplement security
- non-NSS (non-DoD)
  - FIPS 199 and NIST SP 800-53
  - Single categorization level (High, Moderate, Low) for each system
  - Single overall categorization

CNSSI 1253 Table D1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management / Automated System Account Management	X	X		X	X				
AC-2(2)	Account Management / Removal of Temporary / Emergency Accounts	X	X		X	X				

© 2024

54

54

## BAI System Categorization of non-NSS

- For categorization of non-NSS in Federal "civil" sector, agencies can also use FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- The process is similar to the analysis using NIST SP 800-60- just selecting the highest categorization level among the three security objectives

Info Type	C	I	A
Disaster Prediction	L	H	H
Disaster Planning	L	L	L
Emergency Response	L	H	H

→ System Categorization is: HIGH

© 2024

55

55

## BAI Understand your System Type

- Assess and Authorize versus Assess only:
  - Full RMF "Assess and Authorize" process:
    - Major Application
    - Enclave
    - Platform IT (PIT) Systems:
  - Assess only to determine risk
    - Products/Services/Minor Applications: Should already be part of an existing boundary
    - PIT: Risk should be minimal due to limited scope of application

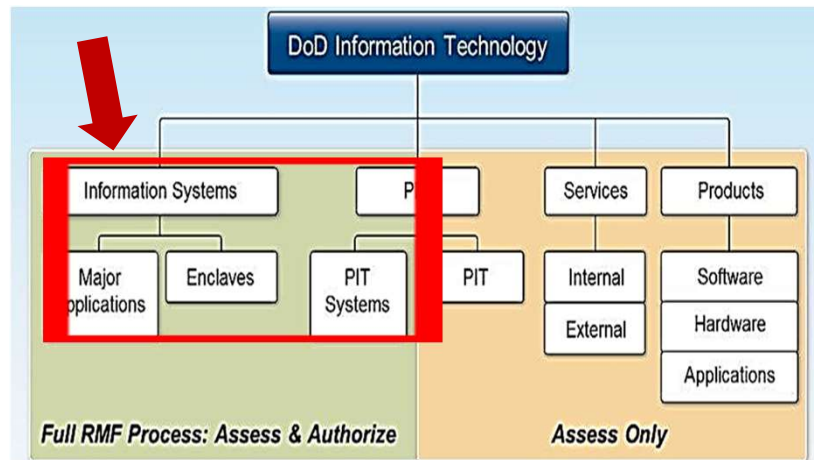
© 2024

56

56

## BAI Must be Assessed and Authorized

- Full RMF process required



© 2024

57

57

## BAI PIT Systems & Major Applications

### Platform Information Technology (PIT) System

- A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. (*DoDI 8500.01, Cybersecurity, 14 March 2014*)
- Special Purpose System; e.g., Weapons Systems or Medical System
- May be standalone—not connected to the DoD Network
- Often higher impact level on integrity or availability
- Unique requirements and security controls

© 2024

58

58

## BAI PIT Systems & Major Applications

Major Application (MA) (May support a mission program or have acquisition products or deliverables)

- "A major application means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate." (*OMB Circular A-130 Appendix III*)
- Owns and administers servers (e.g., software updates, maintain DB, web interface)
- Develops and maintains application
- Servers may be in Enclave and rely on Enclave for communications or other services
- Global workstations may access the application—but may not be part of the boundary
- Data sensitivity may increase cybersecurity risk

© 2024

59

59

## BAI Enclave

Enclave

- "A Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location." (*CNSSI 4009, National Information Assurance (IA) Glossary, 26 April 2010*)
- Has a physical environment
- Provides networking capability, cabling, firewalls, internet, IDS
- Offers basic services, e.g., email
- Usually a Common Controls provider, often for a fee

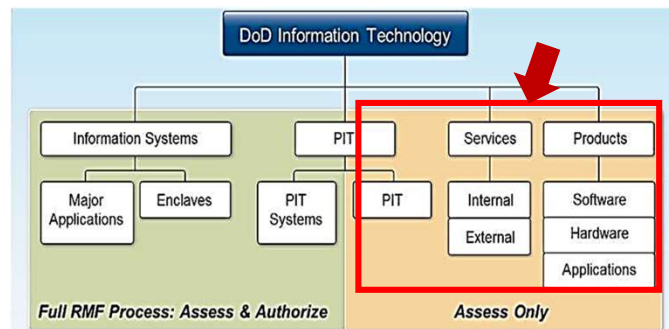
© 2024

60

60

## BAI Assess Only

- "IT below the System level"



© 2024

61

61

## BAI PIT, IT Service, IT Product

### Platform Information Technology (PIT)

- IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. (*DoDI 8500.01*)
- (Example: Radiology system, X-Ray machine)

### IT Service

- A capability provided to one or more DoD entities by an internal or external provider based on the use of information technology and that supports a DoD mission or business process. An IT Service consists of a combination of people, processes, and technology (*DoDI 8500.01*)
- (Example: Internal or External Services that support an IT system (sometimes contracted))

### IT Product

- Individual IT hardware or software items. Products can be commercial, or government provided and include, but are not limited to, operating systems, office productivity software, firewalls, and routers. (*DoDI 8500.01*)
- (Example: Commercial off-the-shelf (COTS) software or hardware)

© 2024

62

62

## BAI Describe the System

- Typical information: scope, components, and boundary
  - System description, name, DoD component identifier (often the DITPR ID), acronym, location
  - Technical Description (hardware, software, application inventories, version or release number, subsystems, cross domain requirements, etc.)
  - System type:
    - IS major application
    - IS enclave (discussion to follow)
    - Platform IT system
  - System Acquisition Phase
  - Categorization, including Information Types
  - Inventory and Configuration Management Systems
- Responsible Organization
- Roles and responsibilities, Points of Contact (PoC)

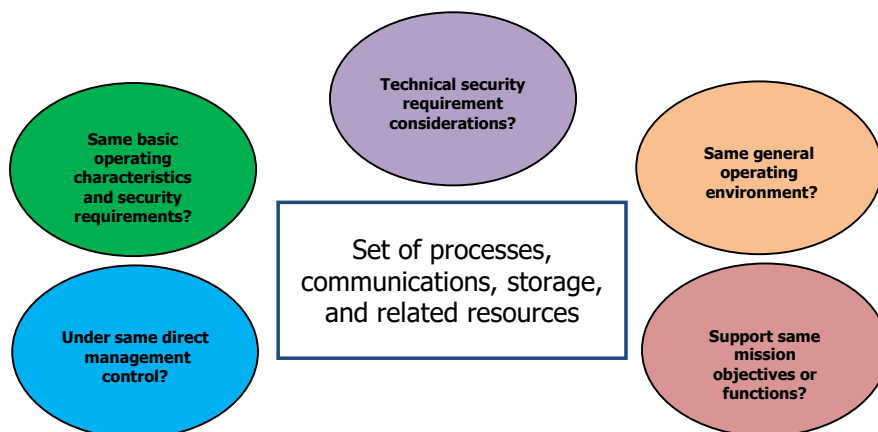
© 2024



63

63

## BAI System Boundary Considerations



© 2024



64

64



## BAI What You Need to Determine Before You Can Propose a Boundary

- Responsible organization - What is under direct management control and in scope of organization boundaries
- Where system resides – physical and environmental
- Any hardware, software, applications, databases, including any logical interfaces – “hooks” from the application to the host, databases, etc.
- Any interconnections through ports, protocols, services with physical and logical interfaces
- System Description
- Technical Description (Hardware, Software, Applications, etc.)
- Information System Type (IS, PIT, etc.)
- System Components and Boundary
- Inventory and Configuration Management system: Compare with the system diagram
- Available resources, e.g., budget, personnel, tools, and timeline

© 2024



65

65

## BAI Boundaries – Understanding Enclaves – per DoDI 8500.01

- Enclaves always assume the highest security category of the ISs that they host and derive their security needs from those systems.
- Enclaves provide standard cybersecurity, such as:
  - boundary defense
  - incident detection and response, and
  - key management
- Enclaves deliver common applications, e.g., office automation and electronic mail.
- May be specific to an organization or a mission
- The computing environments may be organized by physical proximity or by function independent of location.
- Examples enclaves:
  - local area networks and the applications they host
  - Backbone networks
  - Data processing centers.


© 2024

66

66

**BAI** Where to Find Information to Help Define Boundaries

- Existing System
  - System Contract
  - System CONOPS
  - Organizational and system risk assessments
  - Previous system and authorization documentation
- New System
  - System Contract
  - System CONOPS
  - System RFP/RFO/RFI
  - Organizational and system risk assessments
  - Architecture description
    - Mission/Business Processes
    - Federal Enterprise Architecture (FEA) Reference Models
    - Segment Solution Architectures
- Where to Look - Documentation
  - Hardware/Software Inventories
  - System & Network Diagrams
  - System Interface Documentation
  - System Data Flow Diagrams
  - Physical Plant (Datacenter, Building) Floor Plans
  - Memorandum of Understanding, Memorandum of Agreement
  - System Interconnect Agreements
  - Standard Operating Procedures (SOP)



© 2024 67

67

**BAI** Common Mistakes in Setting the System Boundary

- Scope (too small or too big) may impact:
  - Cost
  - Risk
  - Complexity
  - Scope (system components)
- Jurisdictional issues
  - Systems overlap
  - "Gaps" remain
- Consider how these fit into your boundary:
  - Applications
  - Dynamic Subsystems
  - External Systems

© 2024 68

68

## BAI PCOMS Boundary

- Remember the PCOMS System Description?
- Let's figure out the PCOMS boundary.

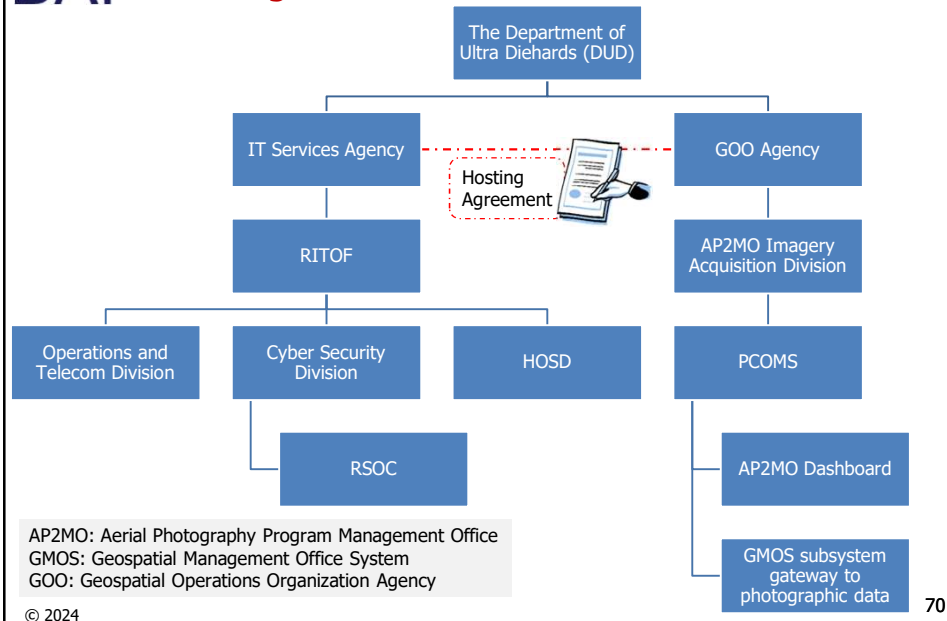
© 2024



69

69

## BAI DUD Organization



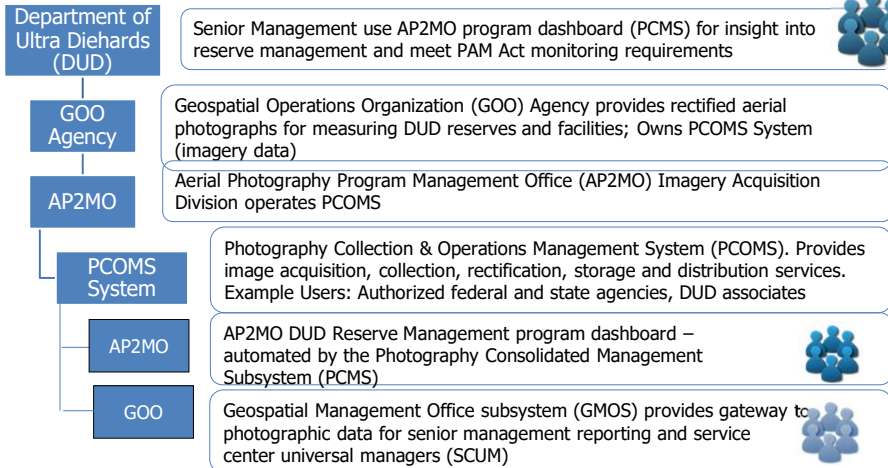
70

70

## BAI Overview

**PAM ACT** of 1993 Photography Adjustment and Management (PAM) Act established capabilities for the US government for:

- photography collection programs
- reporting designed to enhance photographic capabilities



© 2024

71

71

## BAI RMF Boundaries Require Detail

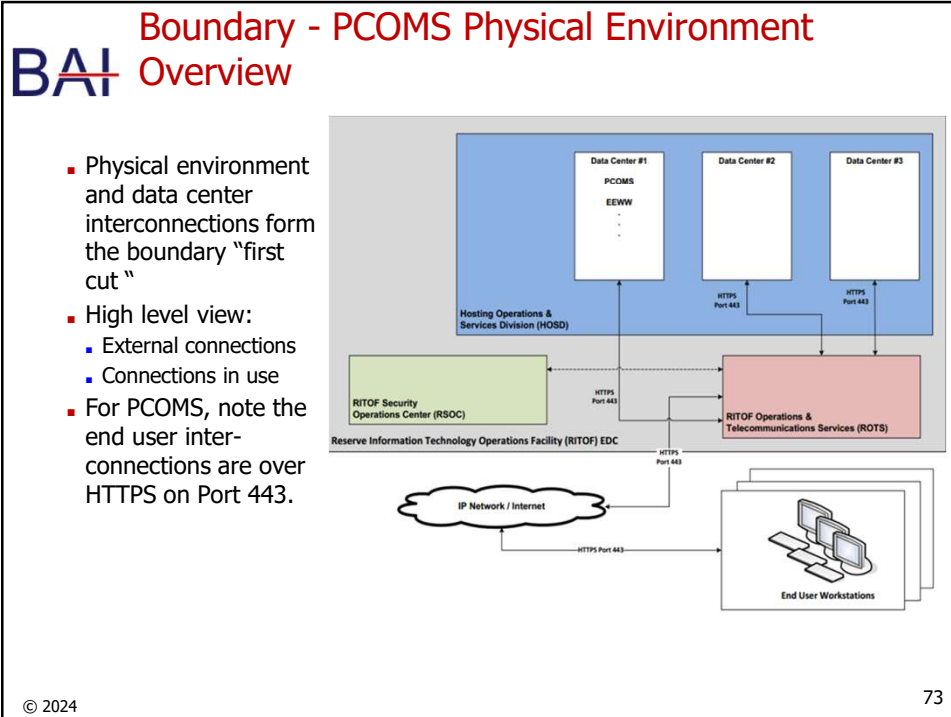
- What is within the scope of organizational responsibilities
- Where does the system reside in the facility or physical environment.
  - Where RITOF and HOSD are located
  - Data centers #1, #2 and #3, RSOC, etc., and what might be in each room
- Hardware, software, applications, database(s)
  - Application and its subsystems
  - The hardware, software, and database(s)
  - Any other component identified in the system inventory.
- An information flow diagram would also help. It depicts interactions among:
  - Operating system
  - Database
  - Application
  - Different ports, protocols, etc.
- Vendor documentation and Service Level Agreements (SLA's) may describe interfaces, e.g., ports and services in use.

© 2024

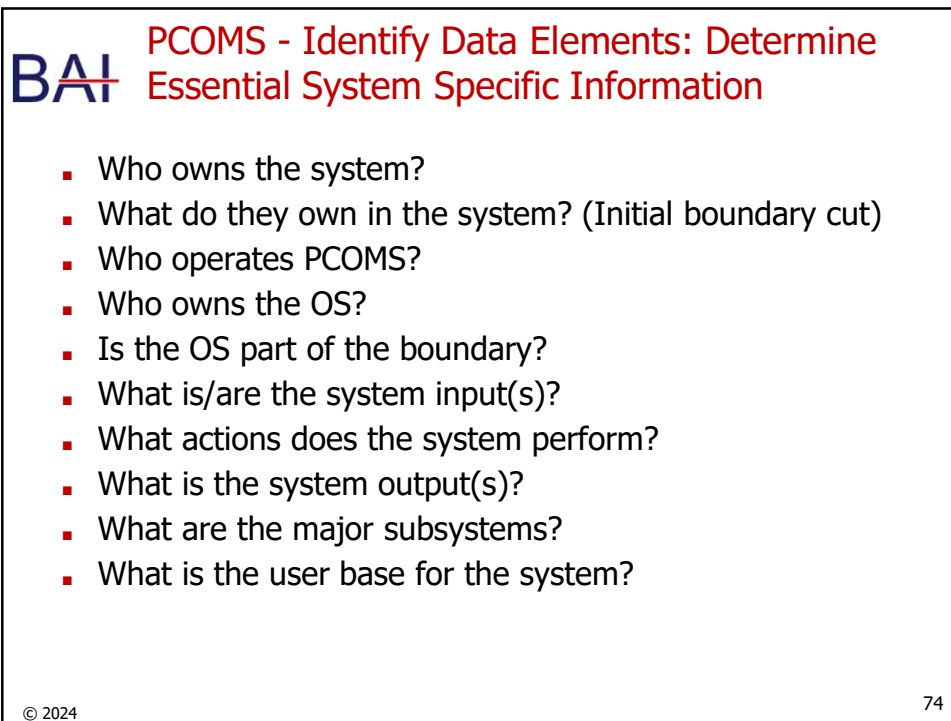
▪ For PCOMS, Active Directory is owned and managed by HOSD.

72

72



73



74



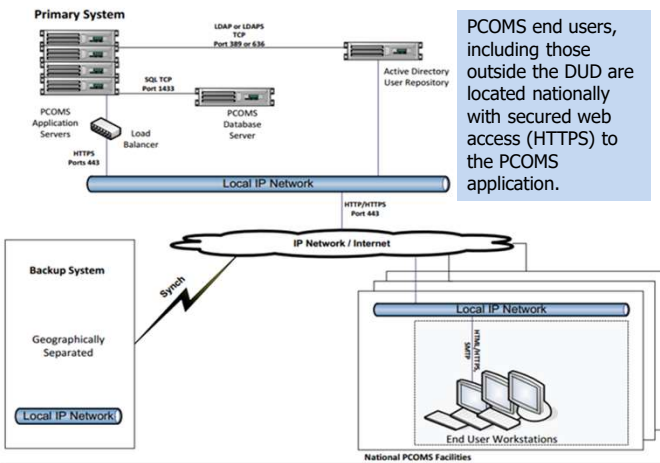
## Boundary Considerations – PCOMS Systems and Interconnections

HOSD hosts PCOMS (Linux and Microsoft Windows data center.) Hosting agreement provides Enterprise Active Directory (EAD), security, network, and monitoring services.

AP2MO management responsible for all:

- Hardware
- Operating systems
- Databases
- Installation
- Administration
- Authorization
- Acquisition/purchasing and maintenance of PCOMS application and sub-components.

Photography Collection & Operations Management System (PCOMS) – Ports & Protocols



PCOMS end users, including those outside the DUD are located nationally with secured web access (HTTPS) to the PCOMS application.

© 2024

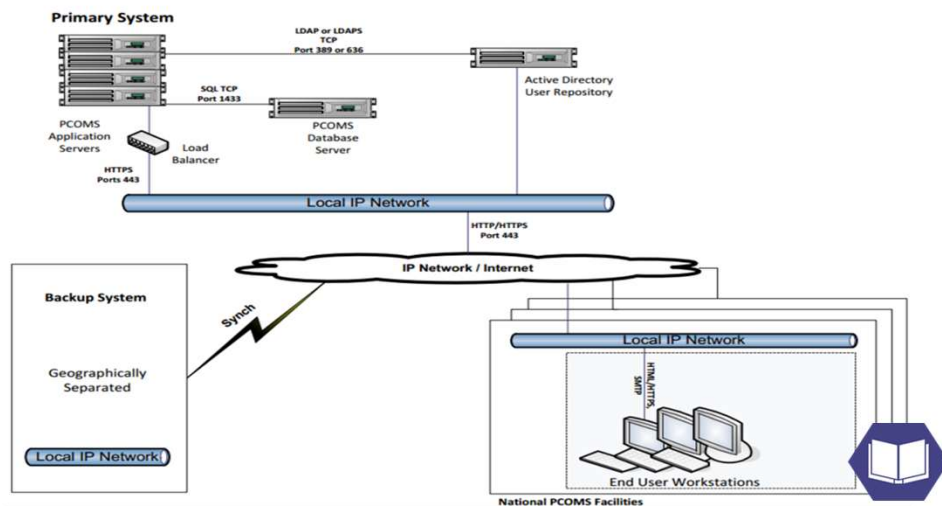
75

75



## PCOMS Systems and Interconnections

Photography Collection & Operations Management System (PCOMS) – Ports & Protocols



© 2024

76

76

## BAI Preparing to Identify Information Types for PCOMS

- Once you have a sense for the boundary...
- Identify applicable information types that are representative of data that the system has:
  - Transmitted
  - Input
  - Stored
  - Processed, and/or
  - Output

© 2024

77

77

## BAI PCOMS Information Type Analysis

- The 1993 Photography Adjustment and Management (PAM) Act established capabilities for the US government for:
  - Photography collection programs
  - Established monitoring and reporting requirements designed to enhance photographic capabilities for the US government
- Information type:
  - C.2.1.3 – Program Monitoring Information Type (L, L, L) Program Monitoring involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies. The impact levels should be commensurate with the impact levels of the programs that are being monitored.

© 2024

78

78

## BAI PCOMS Information Type Analysis

- Geospatial Operations Organization (GOO) has been involved in acquisition, use, and distribution of aerial photography for more than 35 years for Department of Ultra Diehards (DUD) and other authorized users.
- GOO mission: provide rectified aerial photographs for accurately measuring DUD Reserves and facilities.
- PCOMS supports GOO mission through acquisition, collection, rectification, storage and distribution of imagery data.
- PCOMS is designated as an authoritative source for imagery data
- Recipients include:
  - DUD/GOO/AP2MO users;
  - Authorized federal and state agencies; and
  - Other approved users and associates.
- INFORMATION TYPE
  - C.2.6.2 – Official Information Dissemination Information Type (L, L, L); Official Information Dissemination includes all efforts to provide official government information to external stakeholders through the use of various types of media, such as video, paper, web, etc.

© 2024



79

79

## BAI PCOMS Information Type Analysis

- AP2MO management is responsible for all hardware, operating systems, databases, installation, administration, authorization, purchasing and maintenance of the PCOMS application and all sub-components.
- INFORMATION TYPE
  - C.3.5.4 – IT Infrastructure Information Type (L, L, L) IT infrastructure maintenance involves the planning, design, implementation, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, network access rules and implementing files and/or switch setting, hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes. The impact levels associated with IT infrastructure maintenance information are primarily a function of the information processed in and through that infrastructure.

© 2024

80

80



## BAI PCOMS Information Type Analysis

- The Aerial Photography Program Management Office (AP2MO), through PCOMS management and operations, provides:
  - Imagery acquisition;
  - Rectification;
  - Inspection;
  - Distribution; and
  - Archiving services.
- INFORMATION TYPE(S)
  - C.3.5.7 – Information Management Information Type (L, M, L)  
Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management.

© 2024

81

81

## BAI PCOMS Information Type Analysis

- GOO mission: Provide rectified and annotated aerial photographs for accurately measuring Dept. of Ultra Diehard (DUD) Reserves and facilities.
- Images that are properly delineated and annotated with Reserve boundaries and acreage serve as the basic record of each Reserve's land use along with conservation information for legally mandated monitoring and reporting requirements of the PAM Act.
- INFORMATION TYPE
  - D.6.2 – Conservation, Marine and Land Management Information Type (L, L, L)  
Conservation, Marine and Land Management involves the responsibilities of surveying, maintaining, and operating public lands and monuments, as well as activities devoted to ensuring the preservation of land, water, wildlife, and natural resources, both domestically and internationally. It also includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.).

© 2024



82

82

## BAI PCOMS Categorization Determination

### ■ PCOMS Information Types

- C.2.1.3 – Program Monitoring Information Type (L, L, L)
- C.2.6.2 – Official Information Dissemination Information Type (L, L, L)  
A moderate integrity value could be selected since PCOMS is described as the authoritative source for the photographic data.
- C.3.5.4 – IT Infrastructure Information Type (L, L, L)
- C.3.5.7 – Information Management Information Type (L, M, L)
- D.6.2 – Conservation, Marine and Land Management Info Type (L, L, L)

### ■ PCOMS Overall Categorization

- The categorization values for the PCOMS based on the NIST 800-60 would be: **Low, Moderate, Low**
- Does this need to be categorized at a higher level? Can you justify the change?

© 2024

83

83

## BAI System Categorization Activity

- ACTIVITY: Review the System Description for the Location Inventory Management Baseline Operations (LIMBO) system and develop a System Categorization



© 2024

84

84

## BAI Register the System

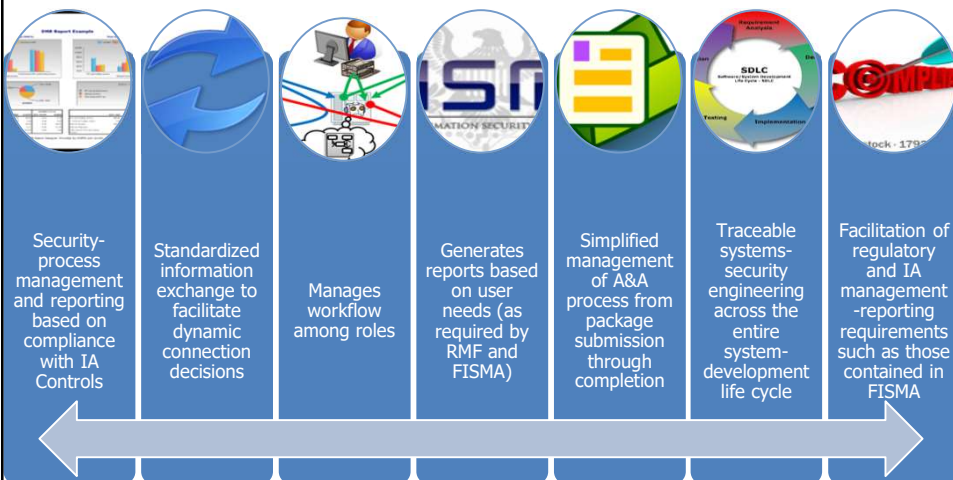
- All systems must be registered with the DoD Component Cybersecurity Program
- Establishes information system and governing organization relationship
  - Provides management and tracking capability
  - Notifies governing organization of new system
  - Identifies information system (with subsystems) in the system inventory
  - Identifies system with DoD mission (i.e., Warfighting, Enterprise, Business, and Defense Intelligence)
  - Tracks FISMA compliance of system

© 2024

85

85

## BAI eMASS Supports Project Planning



Access to eMASS requires a DoD eMASS training certificate from the <https://cyber.mil> website (CAC required).

© 2024

86

86

## BAI eMASS Registration

- Allows organizations management/tracking capability
- Establishes information system and governing organization relationship:
  - Notifies governing organization of new system
  - Identifies information system with Common Control provider
  - Provides workflow and approvals throughout the RMF process
- The organization determines the level of detail provided in the security plan
- The level of detail is typically commensurate with the security categorization of the information system

© 2024

87

87

## BAI eMASS System Registration System Information – Information Types

The screenshot displays the 'eMASS System Registration' interface, specifically the 'System Information – Information Types' section. The interface is divided into a sidebar and a main content area. The sidebar on the left contains navigation links for 'System', 'Controls', 'Assets', and 'POA&M'. The main content area is titled 'Information Types' and features an 'Information Types Listing' section. This section includes a search bar with the text 'Supply Chain Management' and a 'Search' button. Below the search bar, there is a list of information types: 'Goods Acquisition', 'Inventory Control', 'Logistics Management', and 'Services Acquisition'. To the right of the listing, there is a 'Recommended Categorization' section showing 'Confidentiality', 'Integrity', and 'Availability' levels (Moderate, Moderate, Low). Below this, there are sections for 'Selected Information Types (2)' with 'Help Desk Services' and 'Security Management' categories, each with dropdowns for 'Confidentiality', 'Integrity', and 'Availability'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Note: Information Types is an optional module during new system registration. It is not mandatory at this time.

Note: Certain eMASS instances have custom organizational information types available for application.

© 2024

88

88

## eMASS System Registration System Information – Information Types

**BAI** eMASS System Registration  
System Information – Information Types

© 2024

89

89

## eMASS System Registration System Information – Information Types

**BAI** eMASS System Registration  
System Information – Information Types

© 2024

90

90

## BAI RMF Planning Tips

- Steps are equally important
- Control granularity renders DIACAP not a comparable work effort
- Some steps considerably more time/effort than others



© 2024

91

91

## BAI Categorize Project Planning



### Supporting Roles

- Risk Executive (Function)
- AO or AODR
- CIO, SISO, ISSM, ISSO
- Operational Personnel (Administrators, etc.)

### Resources Required

- Role Holders to Provide System Information
- Qualified Security Personnel
- Tool(s) to Document Categorization and Registration Information (eMASS, APMS, etc.)



### Timeframe

- Days to weeks depending on personnel availability

© 2024

92

92

## BAI Categorize Guidance

- DoDI 8500.01 - Cybersecurity
- DoDI 8510.01 - RMF for DoD IT
- CNSSI 1253 - System Categorization and Security Control Selection
- NIST SP 800-37 R2 - RMF Process
- NIST SP 800-60 V 1 & 2 Categorization

© 2024

93

93

## BAI Artifacts Resulting from Categorization

- System Categorization artifact signed
- Finalized System Description
- Finalized System Boundary
- Cybersecurity Portfolio (FISMA) System Record
- eMASS System Record (initiated)

© 2024

94

94

## BAI Categorize Summary Tasks and Responsibilities

### Step 1: CATEGORIZE

RMF Tasks	Per DoD KS Primary Responsibility	Per DoD KS Stakeholders
Categorize the system in accordance with the CNSSI 1253	IO, ISO, Mission Owner(s)	AO, AODR CIO, ISSM, PM/SM SISO
Initiate the Security Plan	Information System Owner	AO, AODR CIO, ISSM, PM/SM SISO
Register system with DoD	ISO, PM/SM	ISSM

© 2024

95

95

## BAI Review Questions

1. What are the major steps in doing the categorization for your system?
2. What do you need to have in place or agreed upon before you start to categorize the information and the system?
3. What documentation will you use to help you follow the process to categorize the system?
4. What guidance is unique to NSS, and DoD as opposed to only using NIST guidance?
5. What would you do to prepare for defining your system boundary?
6. What information can you use regarding transition to RMF that helps convey the change in scope?



© 2024

96

96



## BAI Review Questions

1. Who are the key players at this stage? Is there anyone who has a newer role that you might not have incorporated in the same way previously?
2. What factors might affect provisional impact levels?
3. Can a system be categorized as containing both Management and Support Information types as well as Mission Information Types?
4. Can Overlays be applied to any NSS baseline?
5. Must Contractor Owned/Contractor Operated (COCO) Systems be categorized and registered?



© 2024

97

97



End of Section 1

NEXT: "Select"

© 2024

98

98