SIAGOVSUMMIT

Connecting Government, Security and Technology

June 27 – 28, 2018 | Washington, D.C. | #siagov18

SIAGOVSUMMIT

Understanding the RMF Process for DOD Information Technology

Damon Lam
SPAWAR

Hank Osborne
SPAWAR

SPAWAR
Systems Center
ATLANTIC

Space and Naval Warfare Systems Center Atlantic

Risk Management Framework (RMF)

Presented to:
SIA GovSummit

Hank Osborne
and
Damon Lam

SSC Atlantic is part of the Naval Research & Development Establishment (NR&DE)

What is Risk Management Framework (RMF)

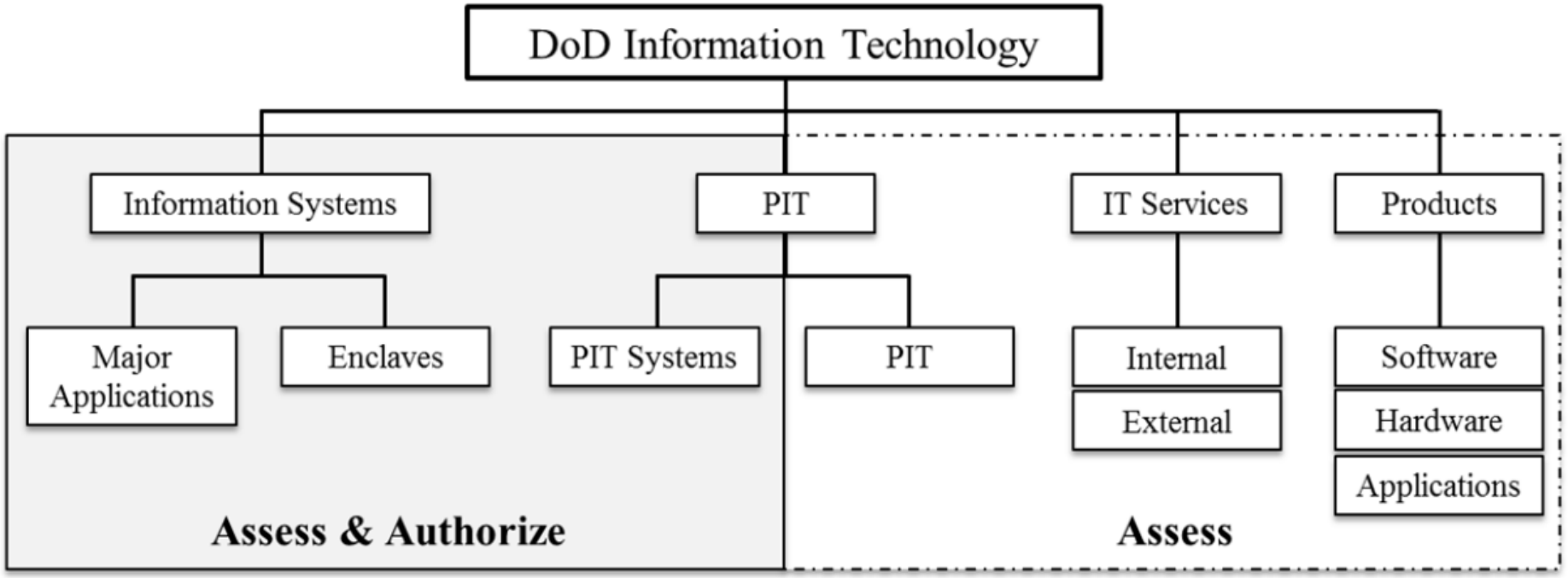
- **What is RMF?**
  - New authorization process that requires DoD Information Systems (IS) and Platform Information Technology (PIT) systems to assess their Cybersecurity risks
    - Replaces DIACAP
    - Emphasizes Continuous Monitoring in lieu of compliance checks

- **Goals of RMF**
  - Base authorization decisions on the acceptance of risk and not the management of vulnerabilities
  - Perform risk assessment throughout SDLC
  - Improve understanding of risks to systems and missions
- **Allows systems to potentially inherit security control implementation**
- **Security control selection and implementation occurs as part of the SDLC**
- **Uses continuous monitoring to support risk management decisions and maintain organizational risk tolerance at acceptable levels**

Reference: DoDI 8510.01, Change 2; July 28, 2017

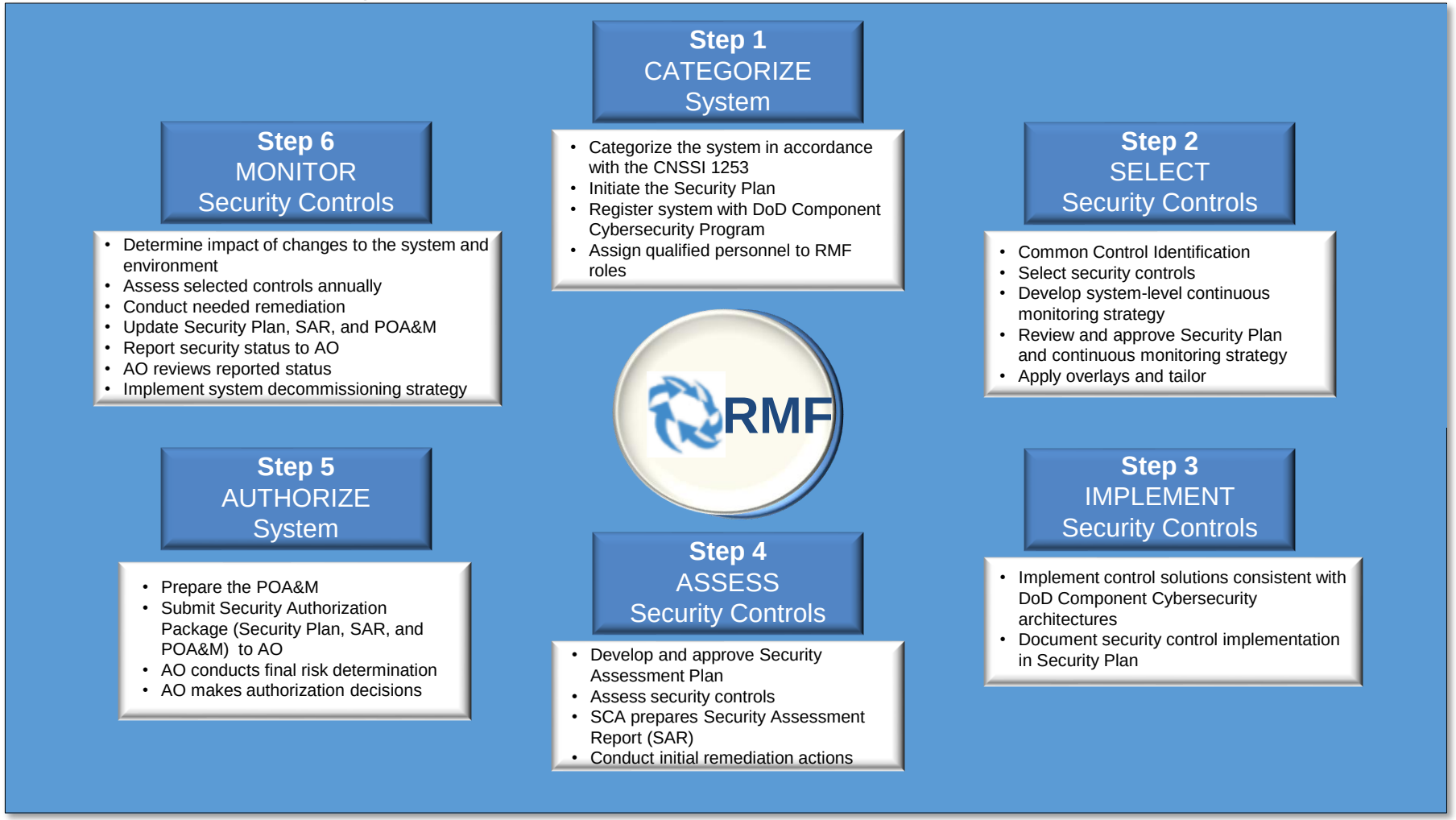
Does RMF Apply to My Systems?

Figure 2. DoD Information Technology



Reference: DoDI 8500.01

DoD RMF Steps



Reference: DoDI 8510.01; May 24, 2016; Figure 3

DoD Control Baseline Example

Table D-1: 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			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions			X			X			
AC-2(12)	Account Management | Account Monitoring /	+	+	X	+	+	X			

Reference: CNSSI 1253

Control Example

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

Reference: NIST 800-53r4

DoD RMF Resources

- DoDI 8510.01, Change 2, July 28, 2017, Pages 9-39
- NIST SP 800-53r4, Chapter 2, Pages 7-27
- CNSSI 1253, Pages 1-7
- DoDI 8500.01, Pages 1-5

SPAWAR
Systems Center
ATLANTIC

We deliver Information Warfare capabilities

Enabling Warfighters to secure America and promote global freedom



SSC Atlantic is part of the Naval Research & Development Establishment (NR&DE)

Web: http://www.public.navy.mil/spawar/Atlantic Facebook: http://www.facebook.com/spaceandnavalwarfaresystemscommand
Twitter: http://twitter.com/SPAWARHQ Employment opportunities: www.USAJOBS.gov
SPAWAR Small Business: http://www.public.navy.mil/spawar/Pages/SmallBusiness.aspx
SPAWAR Contract Directorate Office: https://e-commerce.sscno.nmci.navy.mil