
# DOD Cybersecurity Risk Management Framework And The Current Cybersecurity Environment


David C. Hall
Hall Associates LLC
dave.hall@hallassociateshsval.com

Provided to: AFCEA Meeting
Feb 9, 2016

# DOD Cybersecurity Risk Management Framework And The Current Cybersecurity Environment

The Department of Defense has adopted and is transitioning to a new Cybersecurity Risk Management Framework (RMF) methodology [RDIT] as the replacement for DIACAP. The direction for this transformation comes from the latest set of both DoD and Committee for National Security Systems (CNSS) document replacements for DoDD 8500.1, DoDI 8500.2, DoDI 8510.01, CNSSP 22, and CNSSI 1253.

The RDIT is supported and complimented through a suite of standards and guidelines: National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, 800-30, 800-39, 800-53, 800-53A, and 800-137. There are also several bills making their way through congress and numerous Presidential Executive Orders that pertain to cybersecurity. All of these are not being coordinated so we must determine how each affects each of us.

This brief will provide an overview of as many as I can fit into a short time frame and some links for additional research.

# What is the Risk Management Framework?

The Risk Management Framework (RMF) is the **unified information security framework for the entire federal government** that is replacing the legacy Certification and Accreditation (C&A) processes within federal government departments and agencies, the Department of Defense (DOD) and the Intelligence Community (IC).

RMF is an integral part of **the implementation of FISMA, the Federal Information Security Management Act, and is based on publications of the National Institute of Standards and Technology (NIST) and the Committee on National Security Systems (CNSS).**
DoDI 8500.01 replaces the former DoD Directive 8500.1 and defines DoD's policies for protecting and defending information and information technology, now officially dubbed "Cybersecurity" in place of "Information Assurance".

DoDI 8510.01 delineates the roles, responsibilities, and high-level life cycle process of the "Risk Management Framework (RMF) for DoD IT" as the replacement for DIACAP. Complete specification of security controls (requirements) and system categorization methodology, formerly published in DoD I 8500.2, are now provided by reference to the applicable NIST and CNSS publications (e.g., NIST SP 800-53 and CNSSI 1253).

# RMF in Federal Departments and Agencies

For several years now, most federal “civil” departments and agencies have been utilizing NIST methodology for Certification and Accreditation of their information systems. RMF is being implemented in these organizations by adoption of the most recent revisions to the key NIST publications:

- NIST SP 800-37 (Rev. 1) – RMF process
- NIST SP 800-53 (Rev. 4) – Security controls
- NIST SP 800-53A (Rev. 1) – Assessment methods

Federal departments and agencies also utilize NIST publications for guidance on development of:

- Security Plans (NIST SP 800-18 ),
- Risk Assessments NIST SP 800-30
- Contingency Plans (NIST SP 800-34 ), etc.

# RMF in the Intelligence Community (IC)

The IC is comprised of 16 organizations that are collectively involved in the Nation's intelligence gathering and analysis activities, under the overarching guidance of the Director of National Intelligence (DNI). Information systems that process intelligence information have traditionally undergone Certification and Accreditation (C&A) in accordance with Director of Central Intelligence Directive (DCID) 6/3.

In 2008, the DNI issued Intelligence Community Directive (ICD 503) , in which DCID 6/3 was "rescinded and replaced" by a process based on "standards, policies and guidelines approved by either or both NIST and CNSS". Thus began the transformation of the IC C&A program to RMF.

The RMF for Federal Agencies program covers the NIST and CNSS publications that form the basis of the new IC risk management process. Additionally, the RMF Resource Center is developing an ICD 503 Training program that specifically addresses transition of IC C&A from DCID 6/3 to RMF.

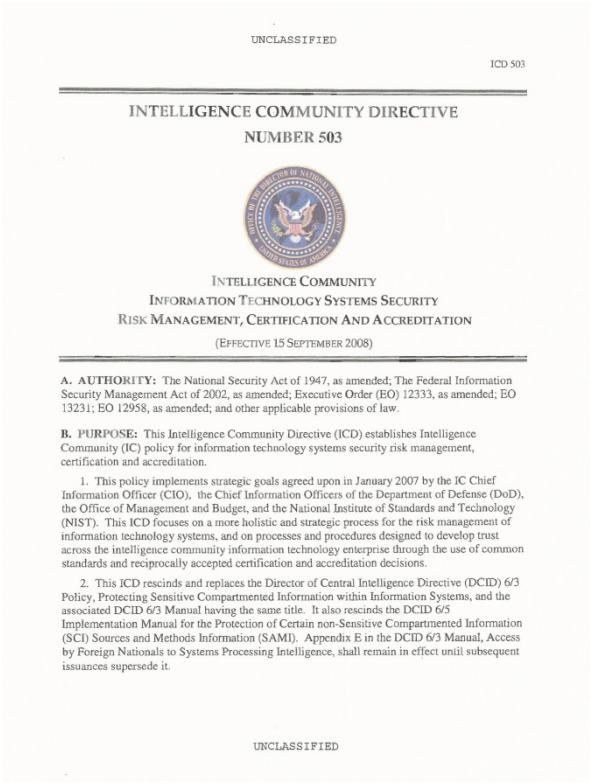
**IC Agencies**

- Central Intelligence Agency (CIA)
- Defense Intelligence Agency (DIA)
- US Air Force Intelligence
- US Army Intelligence
- US Coast Guard Intelligence
- US Marine Corps Intelligence
- US Navy Intelligence
- Department of Energy Office of Intelligence & Counterintelligence
- Department of Homeland Security Office of Intelligence & Analysis
- Department of State Bureau of Intelligence & Research (INR)
- Department of Treasury Office of Intelligence & Analysis (OIA)
- Drug Enforcement Administration Office of National Security Intelligence (NN)
- Federal Bureau of Investigation National Security Branch (NSB)
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency/Central Security Service (NSA/CSS)

# INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY SYSTEMS SECURITY RISK MANAGEMENT, CERTIFICATION AND ACCREDITATION

PURPOSE: This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation.

This policy implements strategic goals agreed upon in January 2007 by the IC Chief Information Officer (CIO), the Chief Information Officers of the Department of Defense (DoD), the Office of Management and Budget, and the National Institute of Standards and Technology (NIST). This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.



UNCLASSIFIED

ICD 503

INTELLIGENCE COMMUNITY DIRECTIVE
NUMBER 503

INTELLIGENCE COMMUNITY
INFORMATION TECHNOLOGY SYSTEMS SECURITY
RISK MANAGEMENT, CERTIFICATION AND ACCREDITATION

(EFFECTIVE 15 SEPTEMBER 2008)

**A. AUTHORITY:** The National Security Act of 1947, as amended; The Federal Information Security Management Act of 2002, as amended; Executive Order (EO) 12333, as amended; EO 13231; EO 12958, as amended; and other applicable provisions of law.

**B. PURPOSE:** This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation.

1. This policy implements strategic goals agreed upon in January 2007 by the IC Chief Information Officer (CIO), the Chief Information Officers of the Department of Defense (DoD), the Office of Management and Budget, and the National Institute of Standards and Technology (NIST). This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.

2. This ICD rescinds and replaces the Director of Central Intelligence Directive (DCID) 6/3 Policy, Protecting Sensitive Compartmented Information within Information Systems, and the associated DCID 6/3 Manual having the same title. It also rescinds the DCID 6/5 Implementation Manual for the Protection of Certain non-Sensitive Compartmented Information (SCI) Sources and Methods Information (SAMI). Appendix E in the DCID 6/3 Manual, Access by Foreign Nationals to Systems Processing Intelligence, shall remain in effect until subsequent issuances supersede it.

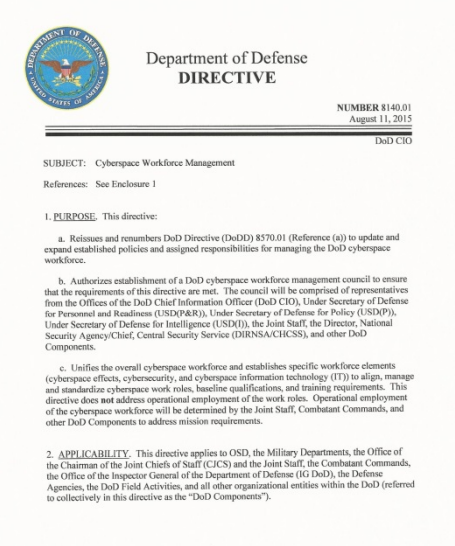
UNCLASSIFIED

# What is the DoD Risk Management Framework?

DoDI 8500.01 replaces the former DoD Directive 8500.1 and defines DoD's policies for protecting and defending information and information technology, now officially dubbed "Cybersecurity" in place of "Information Assurance".

DoDI 8510.01 delineates the roles, responsibilities, and high-level life cycle process of the "Risk Management Framework (RMF) for DoD IT" as the replacement for DIACAP. Complete specification of security controls (requirements) and system categorization methodology, formerly published in DoD I 8500.2, are now provided by reference to the applicable NIST and CNSS publications (e.g., NIST SP 800-53 and CNSSI 1253).

DoDD 8140.01 reissues and renumbers DoD Directive (DoDD) 8570.01 (Reference (a)) to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.



Department of Defense
**DIRECTIVE**

**NUMBER** 8140.01
August 11, 2015
DoD CIO

SUBJECT: Cyberspace Workforce Management

References: See Enclosure 1

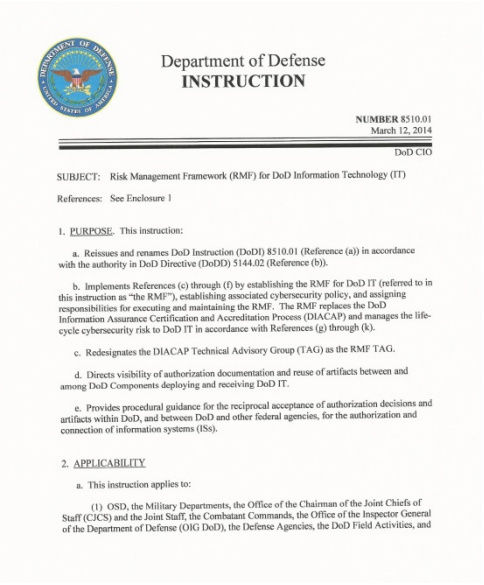
1. PURPOSE. This directive:

a. Reissues and renumbers DoD Directive (DoDD) 8570.01 (Reference (a)) to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.

b. Authorizes establishment of a DoD cyberspace workforce management council to ensure that the requirements of this directive are met. The council will be comprised of representatives from the Offices of the DoD Chief Information Officer (DoD CIO), Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Under Secretary of Defense for Policy (USD(P)), Under Secretary of Defense for Intelligence (USD(I)), the Joint Staff, the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), and other DoD Components.

c. Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does **not** address operational employment of the work roles. Operational employment of the cyberspace workforce will be determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.

2. APPLICABILITY. This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the "DoD Components").



Department of Defense
**INSTRUCTION**

**NUMBER** 8510.01
March 12, 2014
DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

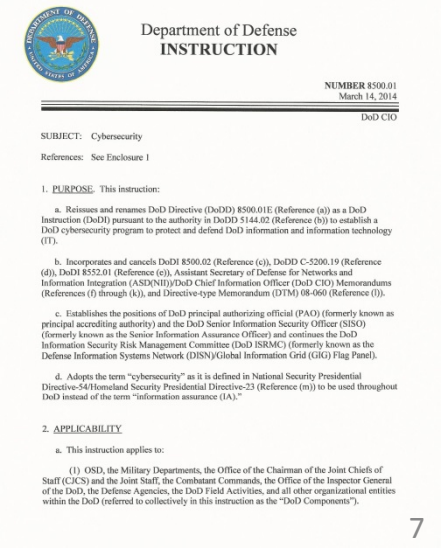
d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and



Department of Defense
**INSTRUCTION**

**NUMBER** 8500.01
March 14, 2014
DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference (d)), DoDI 8552.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (k)), and Directive-type Memorandum (DTM) 08-060 (Reference (l)).

c. Establishes the positions of DoD principal authorizing official (PAO) (formerly known as principal accrediting authority) and the DoD Senior Information Security Officer (SISO) (formerly known as the Senior Information Assurance Officer) and continues the DoD Information Security Risk Management Committee (DoD ISRMC) (formerly known as the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel).

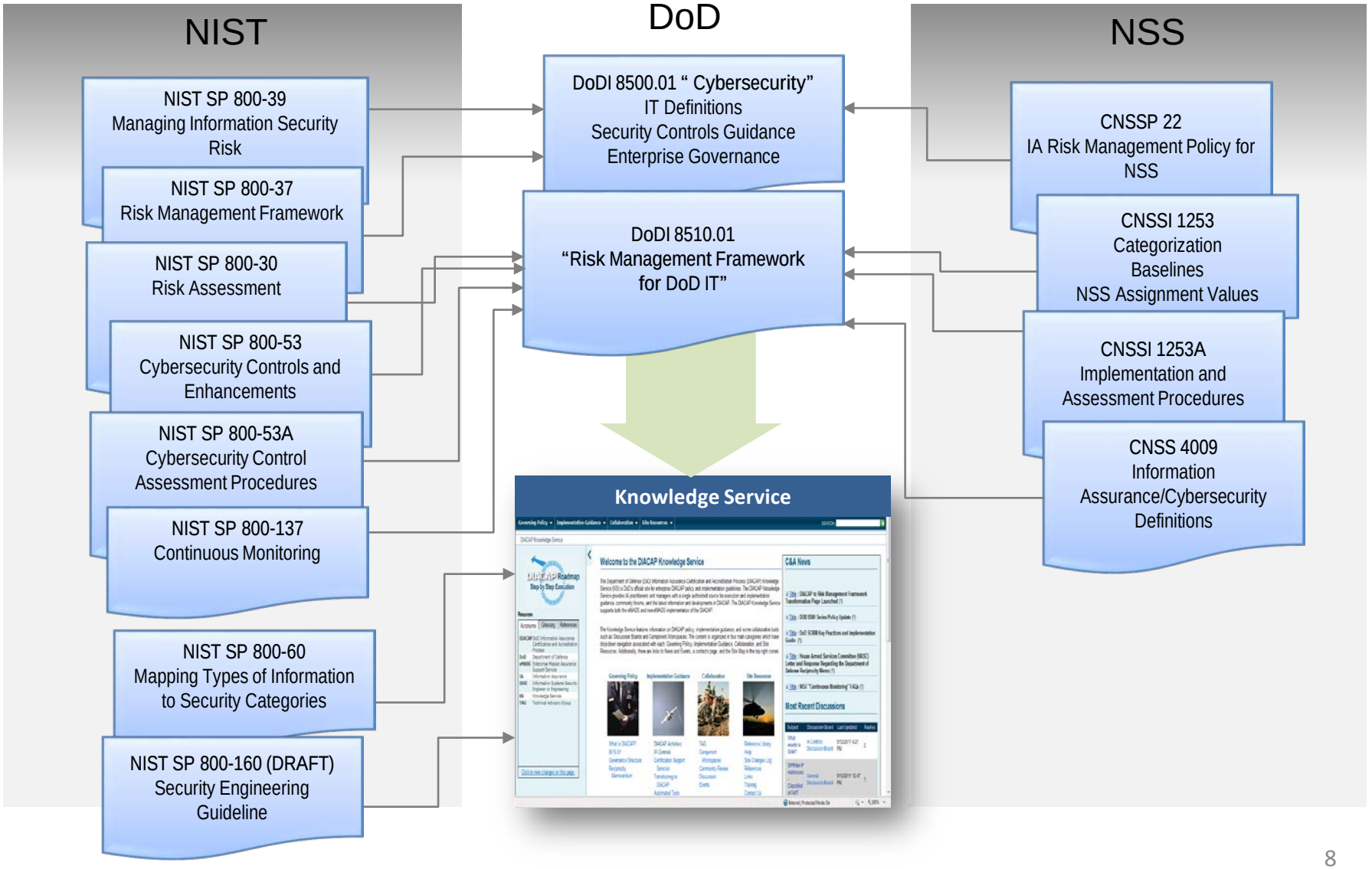
d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term "information assurance (IA)."

2. APPLICABILITY

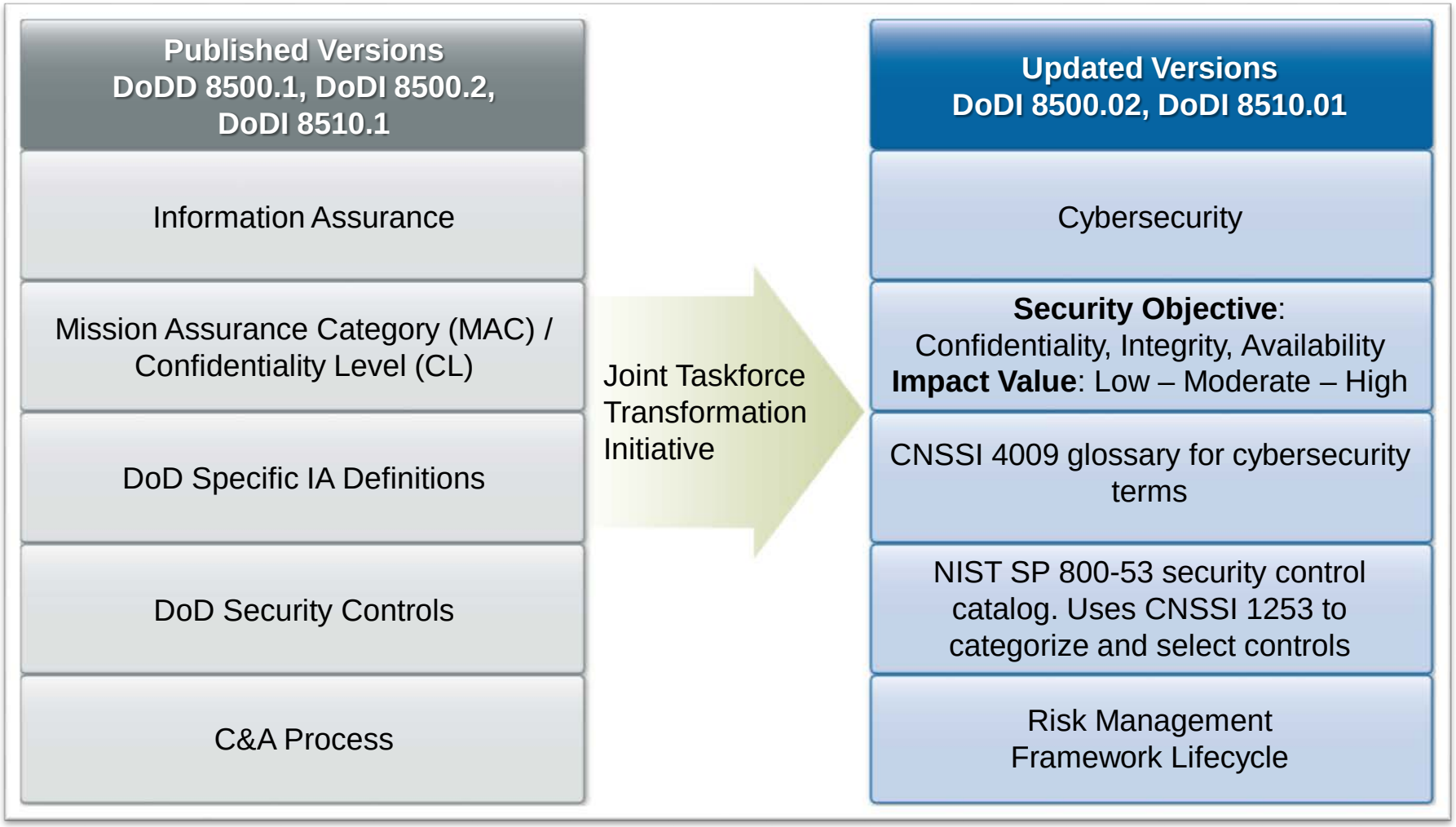
a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

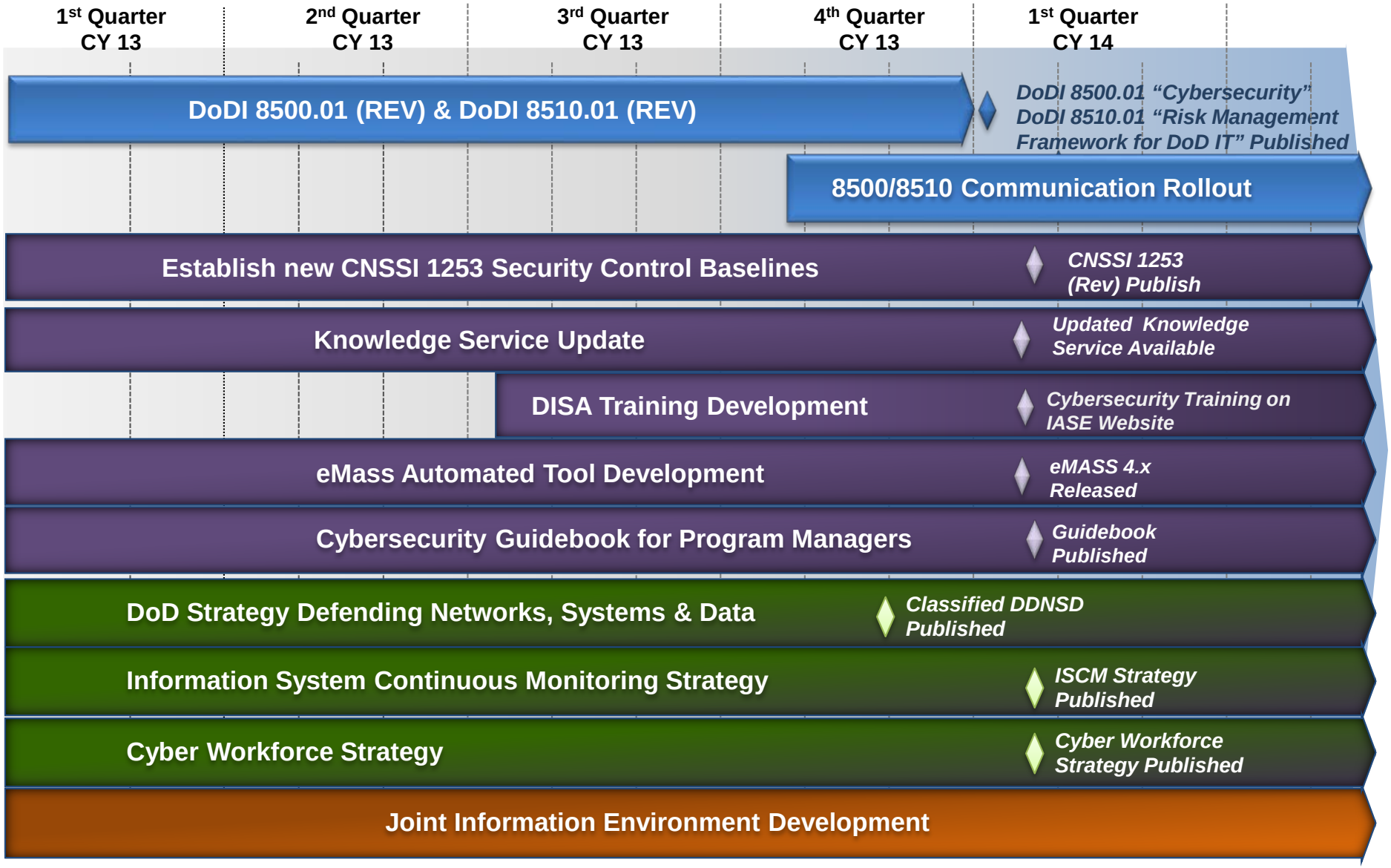
# Cybersecurity Policy Alignment



# DoD Policy Transformation Highlights

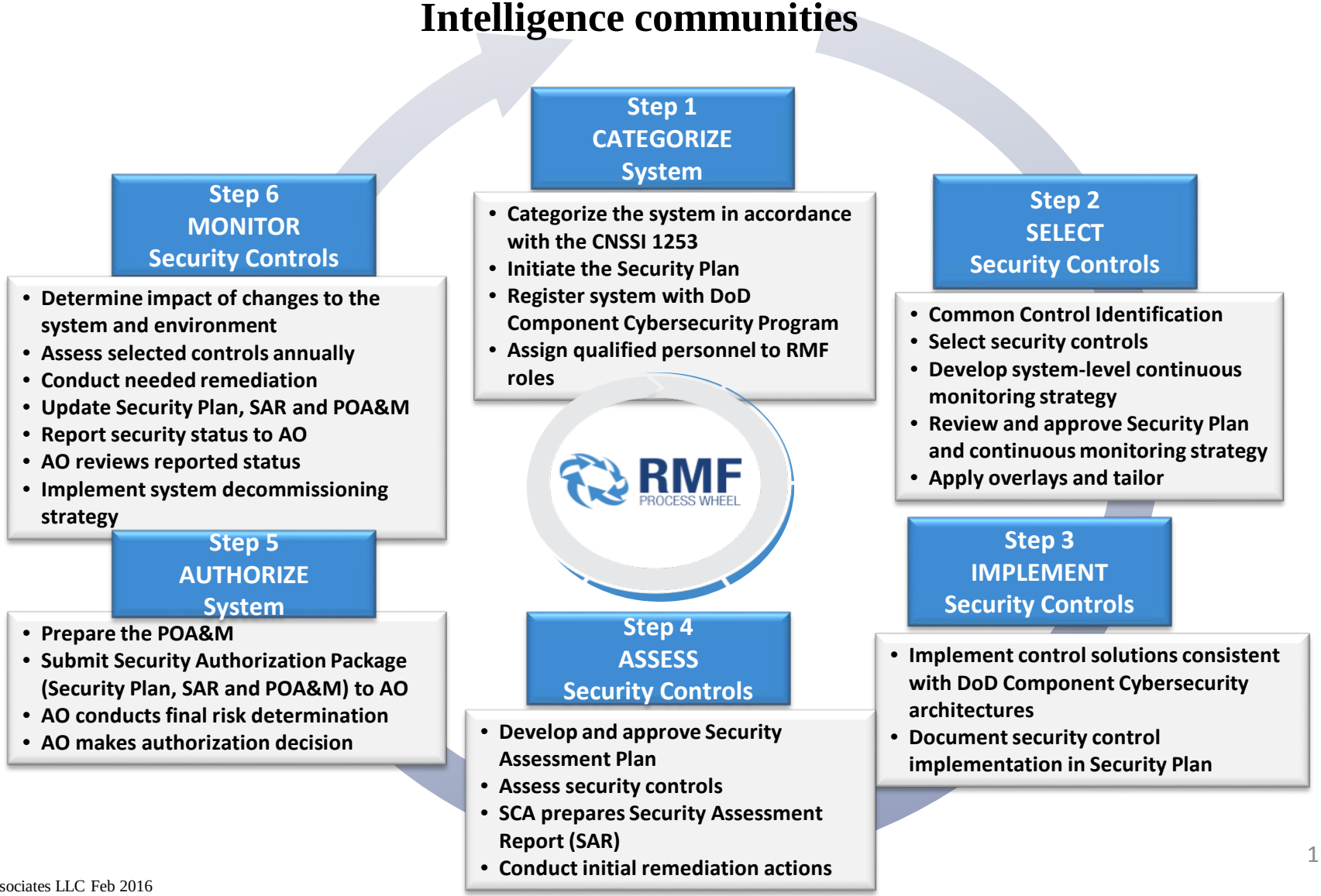


# Cybersecurity Efforts



# DoDI 8510.01 "Risk Management Framework for DoD IT"

## - Adopts NIST's Risk Management Framework, used by Civil and Intelligence communities



# DoDI 8510.01 "Risk Management Framework for DoD IT"

## - Adopts reciprocity as the norm and codifies reciprocity tenets

- Systems have only a **single valid authorization**
- Applied appropriately, reciprocity **reduces redundant testing, assessing and documentation**, and the associated costs in time and resources
- The DoD RMF **presumes acceptance** of existing test and assessment results and authorization documentation
- DoDI 8510 provides **use cases** describing the proper application of DoD policy on reciprocity in the most frequently occurring scenarios

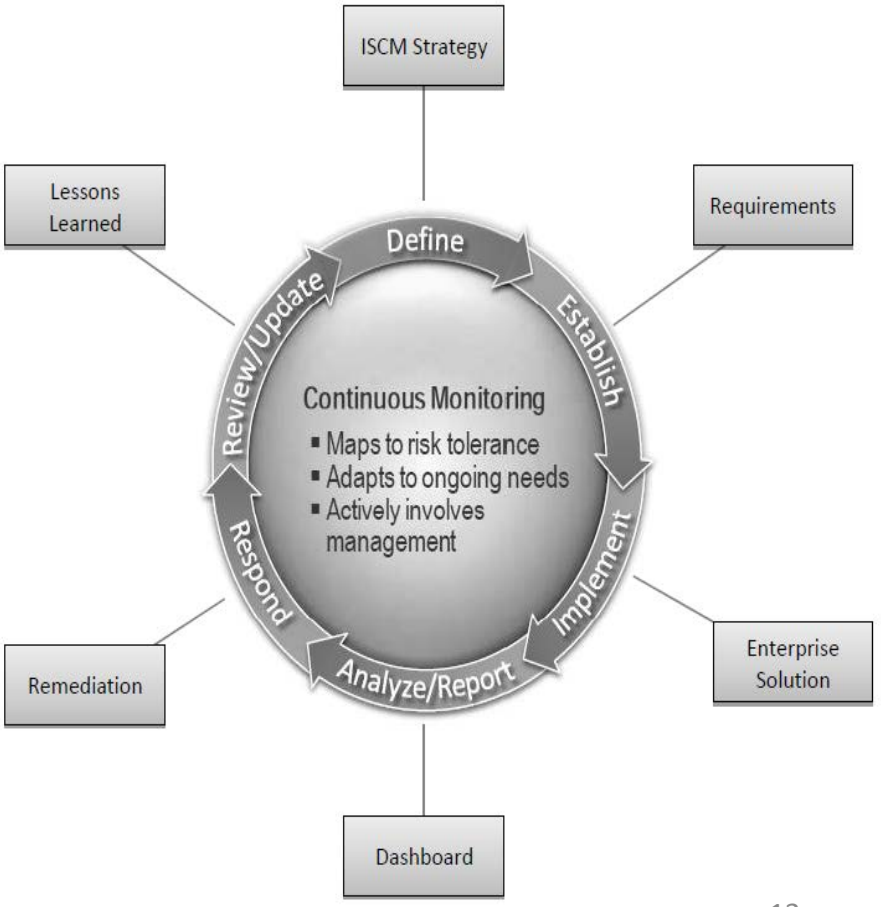
**Process for System Acceptance:**

1. Review the complete security authorization package
2. Determine the security impact of connecting the deploying system within the receiving enclave or site
3. Determine the risk of hosting the deploying system within the enclave or site
4. If the risk is acceptable, execute a documented agreement between deploying and receiving organizations
5. Document the acceptance by the receiving AO
6. Update the receiving enclave or site authorization documentation for inclusion of the deployed system

# DoDI 8510.01 "Risk Management Framework for DoD IT"

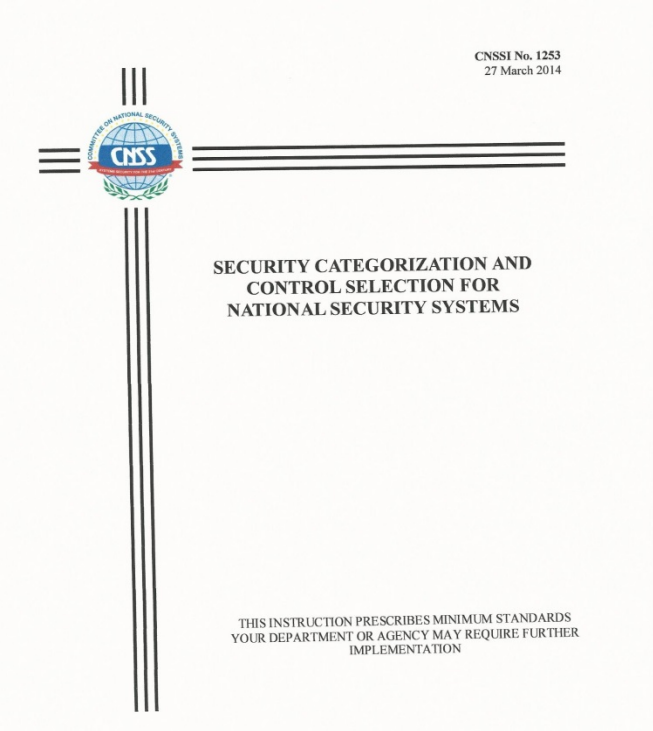
- **Emphasizes continuous monitoring and timely correction of deficiencies**

- RMF is necessary to set the **baseline** for the initial authorization (i.e, meeting CS expectations)
- Developing the programmatics for institutionalizing **ongoing authorization** (vice 3 year reaccreditations) by leveraging a robust **Continuous Monitoring Program,** and **developing joint processes** to adopt reciprocity for cybersecurity across DoD the IC, and Federal Civilian Agencies.



# CNSSI 1253, "Security Control Categorization and Selection for National Security Systems"

- Required by DoD 8510.01 for all information systems and PIT systems
- Builds on and is a companion document to NIST Special Publication SP 800-53
- Should be used as a tool by ISSEs, AOs, SISOs, Data Owners and others to select and agree upon appropriate protections for an NSS
- Adopts FIPS 199, Categorize NSS using three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) for each of the security objectives
- Defines and provides guidance on developing and implementing overlays


CNSSI No. 1253
27 March 2014

SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION

# Committee on National Security Systems

The instructions presented under this topic provide guidance and establishes technical criteria for specific national security systems issues. These instructions include technical or implementation guidelines, restrictions, doctrines, and procedures applicable to information assurance. All instructions are binding upon all U.S. Government departments and agencies. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

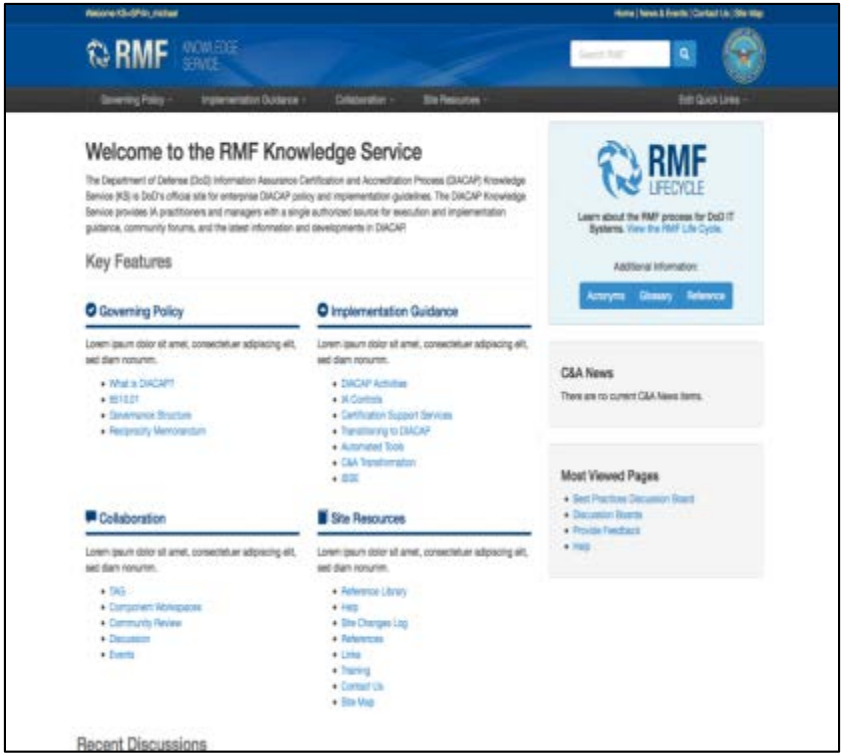
CNSSI No. 1001 - National Instruction On Classified Information Spillage
CNSSI No. 1002 This document is designated FOUO Management of Combined Secure Interoperability Requirements
CNSSI No. 1010 This document is designated FOUO 24x7 Computer Incident Response Capability (CIRC) on National Security Systems
CNSSI No. 1011 This document is designated FOUO Implementing Host-Based Security Capabilities on National Security Systems
CNSSI No. 1012 This document is designated FOUO Instruction for Network Mapping of National Security Systems (NSS)
CNSSI No. 1013 This document is designated FOUO Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS) on NSS
CNSSI No. 1015 Enterprise Audit Management Instruction Provides operational guidance and assigns responsibilities for deploying EAM for National Security Systems.
CNSSI No. 1200 Instruction for Space Systems Used to Support NSS
**CNSSI No. 1253 Security Categorization and Control Selection for National Security Systems**
CNSSI No. 1253F Attachment 1 Security Overlays Template
CNSSI No. 1253F Attachment 2 Space Platform Overlay
CNSSI No. 1253F Attachment 3 Cross Domain Solution Overlay
CNSSI No. 1253F Attachment 4 This document is designated FOUO Intelligence Overlay
CNSSI No.1253F, Attachment 5 Classified Information Overlay
CNSSI No.1253F, Attachment 6 Privacy Overlay
CNSSI 1300 Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25
NSTISSI No. 3003 This document is designated FOUO Operational Security Doctrine for the KG-66/KG-66A/SO-66/KGR-66/KGV-68/KGR-68/KGV-68B
NSTISSI No. 3006 This document is designated FOUO OPSEC Doctrine for the NAVSTAR GPS PPS User Segment Equipment
NTISSI No. 3013 This document is designated FOUO Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal
NTISSI No. 3013 Annex A-D This document is designated FOUO Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal
NTISSI No. 3013 Annex E-G This document is designated FOUO Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal
NTISSI No. 3013 Annex H This document is designated FOUO Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal
NSTISSI No. 3019 This document is designated FOUO Operational Security Doctrine for the FASTLANE (KG-75 and KG-75A)
CNSSI No. 3021 This document is designated FOUO Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device
NSTISSI No. 3022 This document is designated FOUO OPSEC Doctrine for TEDs KG-81, KG-94, KG-95, KG-194, and KIV-19 in Stand Alone Applications
NSTISSI No. 3026 This document is designated FOUO Operational Security Doctrine for the Motorola Network Encryption System (NES)
NSTISSI No. 3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card

# Committee on National Security Systems

CNSSI No. 3029 This document is designated FOUO Operational Systems Security Doctrine for TACLANE (KG-175)
CNSSI No. 3029 2004 Amendment This document is designated FOUO Operational Systems Security Doctrine for TACLANE (KG-175)
CNSSI No. 3029 2006 Amendment This document is designated FOUO Operational Systems Security Doctrine for TACLANE (KG-175)
NSTISSI No. 3030 This document is designated FOUO OPSEC Security Doctrine for the FORTEZZA PLUS (KOV-14) and Cryptographic Card and Associated STE
NSTISSI No. 3030 2006 Amendment This document is designated FOUO Amendment to NSTISSI-3030
CNSSI No. 3031 This document is designated FOUO Operation Systems Security Doctrine for the Sectera In-Line Network Encryptor (KG-235)
CNSSI No. 3032 This document is designated FOUO Operational Security Doctrine for the VIASAT Internet Protocol (VIP) Crypto Version 1 (KIV-21)
CNSSI No. 3034 This document is designated FOUO Operational Security Doctrine for the SECNET 11 Wireless Local Area Network Interface Card
CNSSI No. 3035 This document is designated FOUO OPERATIONAL SECURITY DOCTRINE FOR THE REDEAGLE KG-245 IN-LINE NETWORK ENCRYPTOR
CNSSI No. 4000 This document is designated FOUO Maintenance of Communications Security (COMSEC) Equipment
CNSSI No. 4001 This document is designated FOUO Controlled Cryptographic Items
NTISSI No. 4002 2009 Amendment This document is designated FOUO Pen and Ink Changes for NTISSI 4002
NTISSI No. 4002 2004 Amendment This document is designated FOUO Pen and Ink Changes for NTISSI 4002 9 Jul 2004
**CNSSI No. 4003 This document is designated FOUO Reporting and Evaluating COMSEC Incidents**
CNSSI No. 4004.1 This document is designated FOUO Destruction and Emergency Protection Procedures for COMSEC and Classified Material
CNSSI No. 4005 This document is designated FOUO Safeguarding COMSEC Facilities and Materials
CNSSI No. 4005 Amendment This document is designated FOUO CNSS-008-14 Amendment to CNSSI 4005
CNSSI No. 4006 This document is designated FOUO Controlling Authorities for Traditional COMSEC Keying Material
CNSSI No. 4007 Communications Security (COMSEC) Utility Program
CNSSI No. 4008 Program for the Management and Use of National Reserve Information Assurance Security Equipment
CNSSI No. 4009 Committee on National Security Systems (CNSS) Glossary
**NSTISSI No. 4010 This document is designated FOUO Keying Material Management**
**NSTISSI No. 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals**
**CNSSI No. 4012 National Information Assurance Training Standard for Senior Systems Managers**
**CNSSI No. 4013 National Information Assurance Training Standard For System Administrators (SA)**
**CNSSI No. 4014 Information Assurance Training Standard for Information Systems Security Officers**
**NSTISSI No. 4015 National Training Standard for Systems Certifiers**
**CNSSI No. 4016 National Information Assurance Training Standard For Risk Analysts**
CNSSI No. 4031 Cryptographic High Value Products (CHVP)
CNSSI No. 4032 This document is designated FOUO Title not available
CNSSI No. 4033 Nomenclature for Communications Security Material
CNSSI No. 5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony
CNSSI No. 5001 Type-Acceptance Program for Voice Over Internet Protocol (VoIP) Telephones
CNSSI No. 5002 National Information Assurance (IA) Instruction for Computerized Telephone Systems
CNSSI No. 5006 National Instruction for Approved Telephone Equipment
CNSSI No. 5007 Telephone and Security Equipment Submission and Evaluation Procedures
NACSI No. 6002 National COMSEC Instruction
CNSSI No. 7003 Protected Distribution Systems

# DIACAP/RMF Knowledge Service

The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework


https://diacap.iaportal.navy.mil/login.htm

# RMF Technical Advisory Group (RMF TAG)

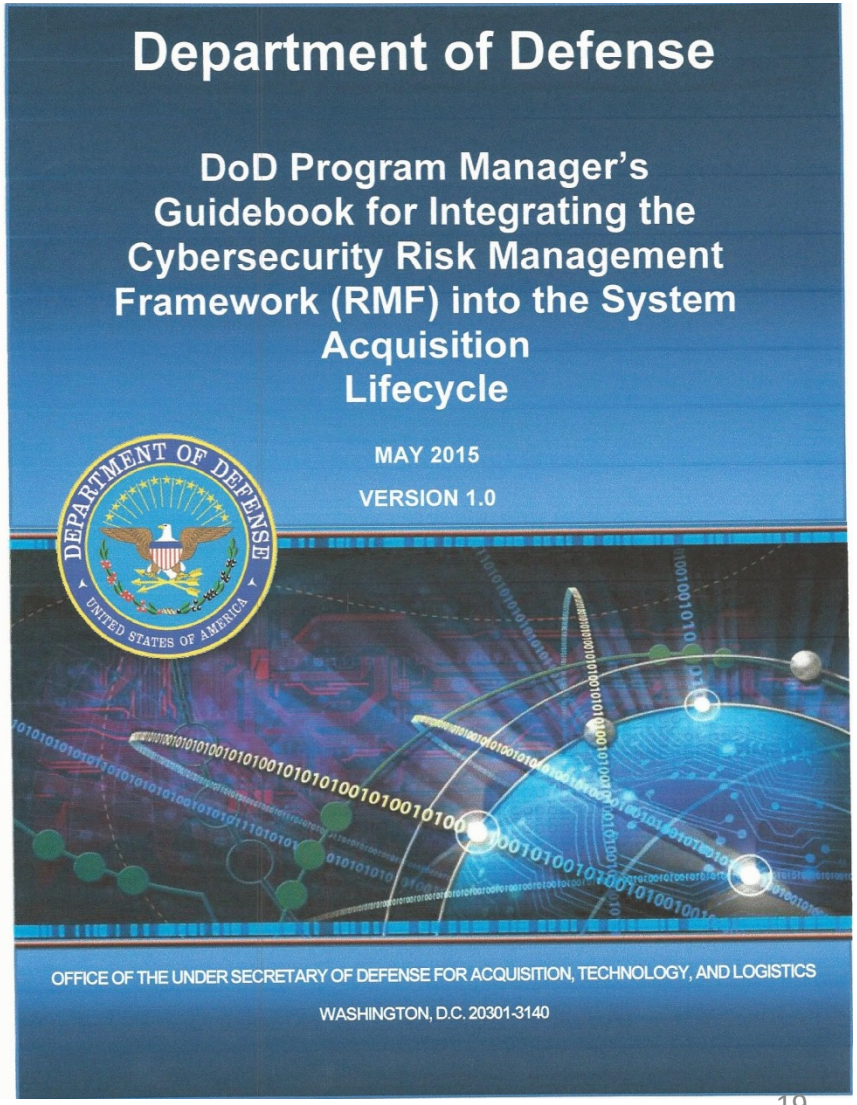
- Mission: Strengthen **and evolve** the ability for DoD to rapidly deploy secure IT systems that enable information sharing between the Department, the IC, and other entities.
- Duties:
  - Provide implementation guidance for the RMF
  - Provide detailed analysis and authoring support for the enterprise portion of the Knowledge Service (KS)
  - **Recommend changes to security controls, baselines, and RMF policy**
  - Advise DoD forums established to resolve RMF priorities and cross-cutting issues
  - **Develop and manage RMF automation requirements**
- Chair: DoD SISO appointed
- Members: All DoD Components are authorized to be represented by one primary and one alternate cybersecurity SME.

**from draft RMF TAG charter revised for updated DoDI 8510*

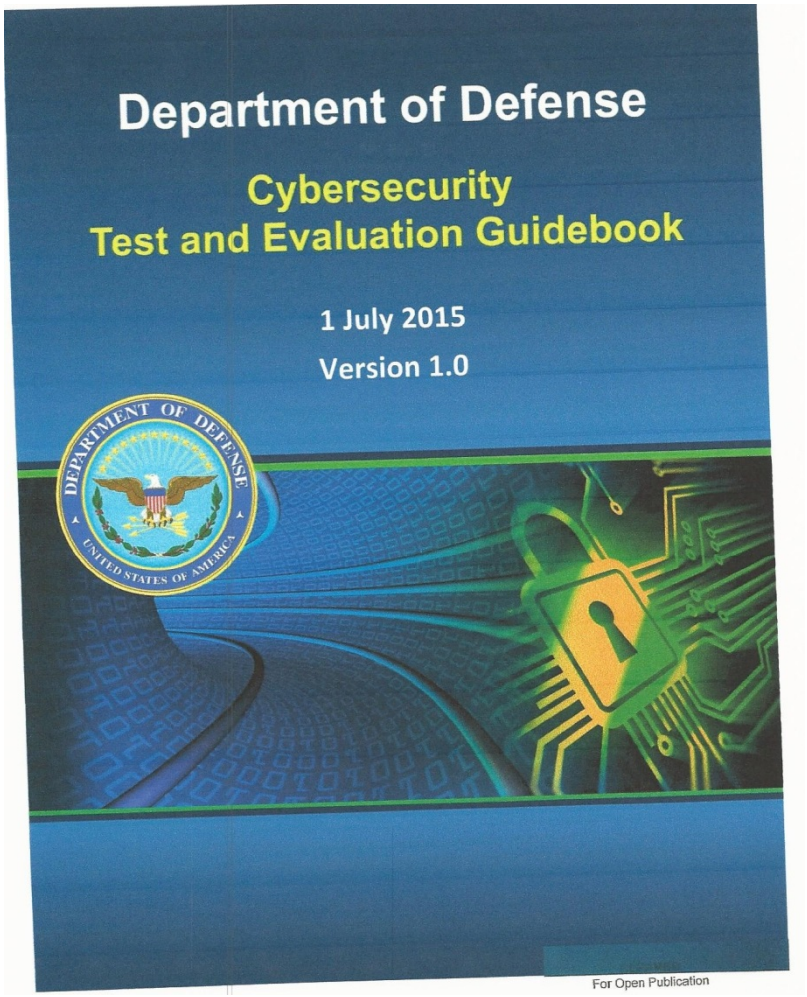
# Cybersecurity Guidebook for PMs

"DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle," Version 1.0, MAY-26-2015

- A practical reference for PMs to integrate cybersecurity throughout the acquisition lifecycle
- Authoring team chaired by USD(AT&L) and DoD CIO
  - Participants: DOT&E, Joint Staff, Army, Navy, Marine Corps, Air Force, USCYBERCOM, DISA, NSA and DIA



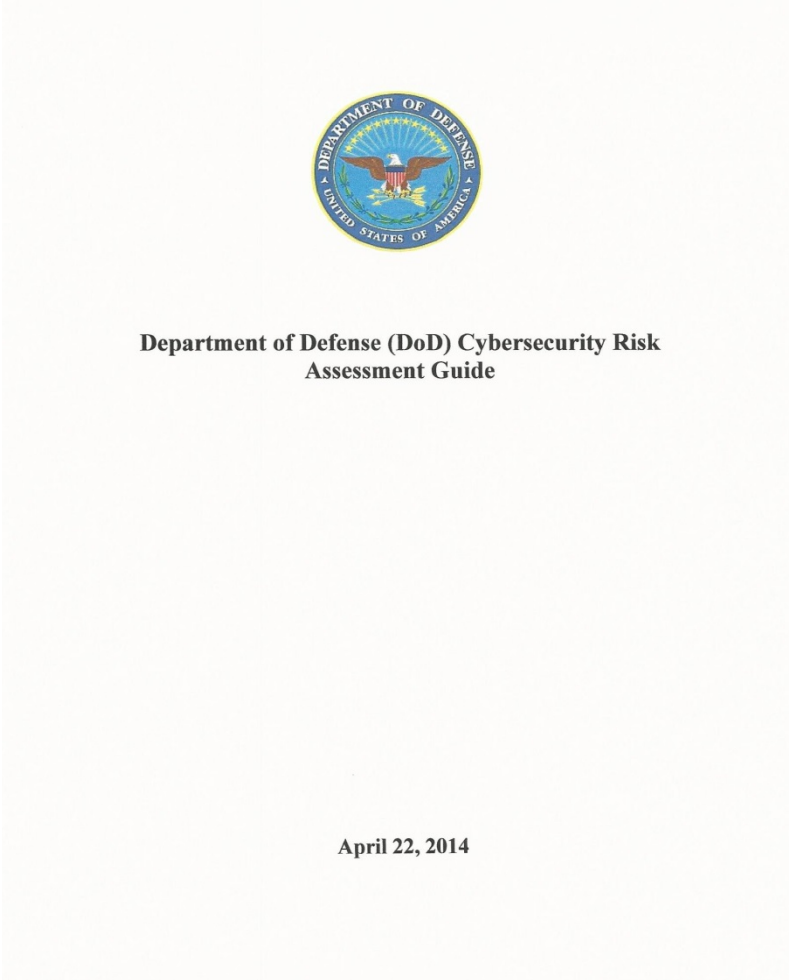
# DOD Cybersecurity Test and Evaluation Guidebook



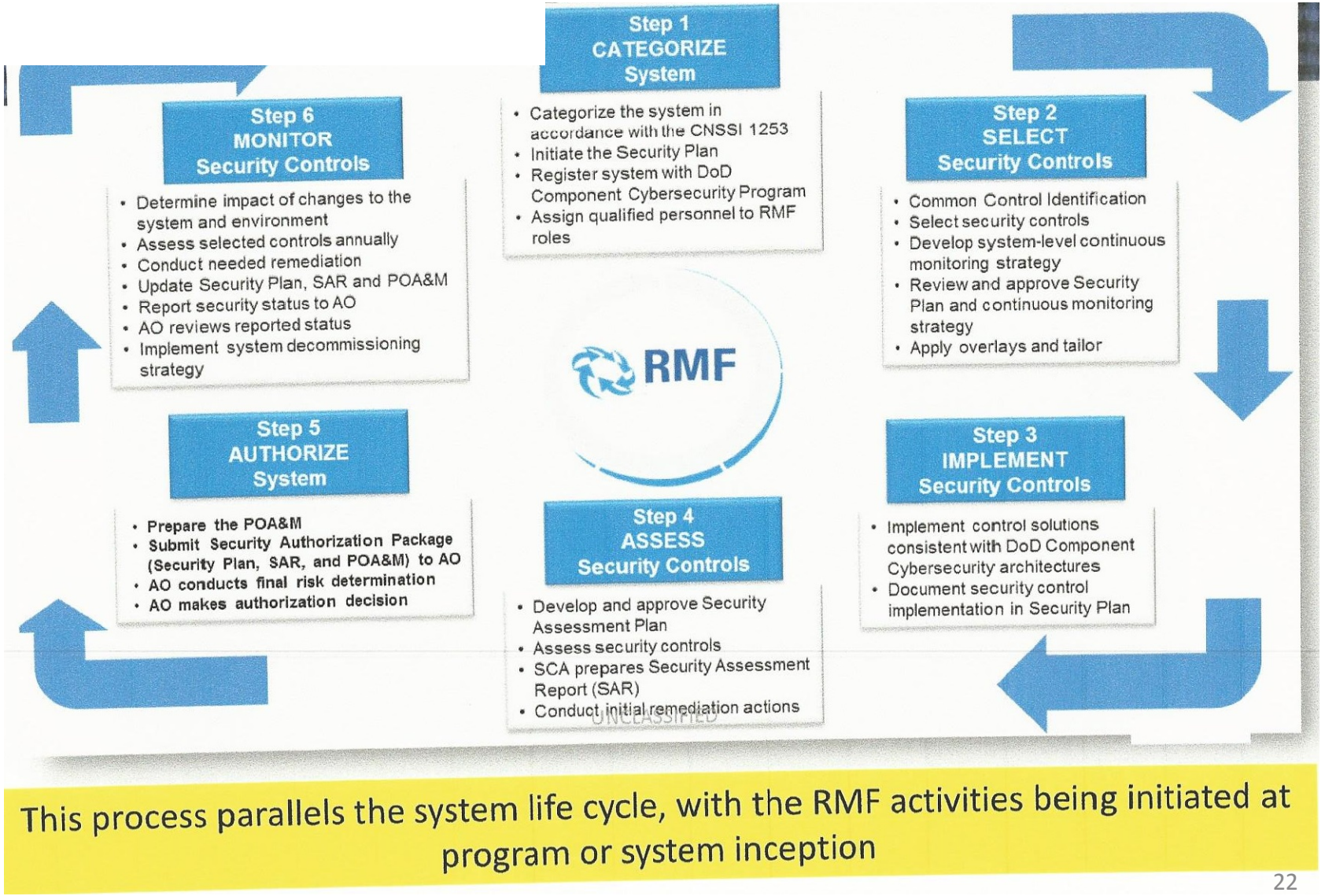

The purpose of this guidebook is to provide guidance to Chief Developmental Testers, Lead Developmental Test and Evaluation (DT&E) Organizations, Operational Test Agencies (OTAs) and the larger test community on planning, analysis, and implementation of cybersecurity T&E. Cybersecurity T&E consists of iterative processes, starting at the initiation of an acquisition and continuing throughout the entire life cycle.

# Cybersecurity Risk Assessment Guide

PURPOSE: Provide a framework, methodology, and process for conducting risk assessments within the Department of Defense (DoD), aligned with NIST SP 800-30, Guide for Conducting Risk Assessments.
NOTE: This guide summarizes and often cites specific content in NIST SP 800-30. In particular, the risk factors and definitions used herein are taken directly from NIST SP 800-30. As practitioners require more information or desire to build more expertise, they should reference NIST SP 800-30.



# Risk Management Framework Six Step Process




This process parallels the system life cycle, with the RMF activities being initiated at program or system inception

# Steps 1 and 2 – Risk Management Framework


- **Step 1 - Categorize System**
  - Categorize the system in accordance with CNSSI 1253 and document the results in the security plan.
  - Describe the system (including system boundary) and document the description in the security plan.
  - Register the system with the DoD Component Cybersecurity Program
  - Assign qualified personnel to RMF roles.
- **Step 2 - Select Security Controls**
  - Common Control Identification - Common controls are selected as "common" and provided via the Knowledge Service based on risk assessments conducted by these entities at the Tier 1 and Tier 2 levels
  - Security Control Baseline and Overlay Selection - Identify the security control baseline for the system
  - Monitoring Strategy - Develop and document a system-level strategy for the continuous monitoring of the effectiveness of security controls

# Steps 3 And 4 – Risk Management Framework


- **Step 3 - Implement Security Controls**
  - Implement the security controls specified in the security plan
  - Document the security control implementation
  - Security controls that are available for inheritance (e.g. common controls) by IS and PIT systems will be identified and have associated compliance status provided by hosting or connected systems
- **Step 4 - Assess Security Controls**
  - Develop, review, and approve a plan to assess the security controls.
  - Assess the security controls in accordance with the security assessment plan and DoD assessment procedures
  - Prepare the Security Assessment Report, documenting the issues, findings, and recommendations from the security control assessment
  - Conduct remediation actions on non-compliant security controls based on the findings and recommendations of the SAR and reassess remediated control(s)

# Steps 5 And 6 – Risk Management Framework


- **Step 5 - Authorize System**
  - Prepare the Plan of Actions and Milestones (POA&M) based on the vulnerabilities identified during the security control assessment
  - Assemble the security authorization package and submit the package to the AO for adjudication.
  - Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation
  - Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable
- **Step 6 - Monitor Security Controls**
  - Determine the security impact of proposed or actual changes to the IS or PIT system and its environment of operation
  - Assess a subset of the security controls employed within and inherited by the IS or PIT system
  - Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M
  - Implement a system decommissioning strategy, when needed, which executes required actions when an IS or PIT system is removed from service

# Key Risk Management Framework Documents

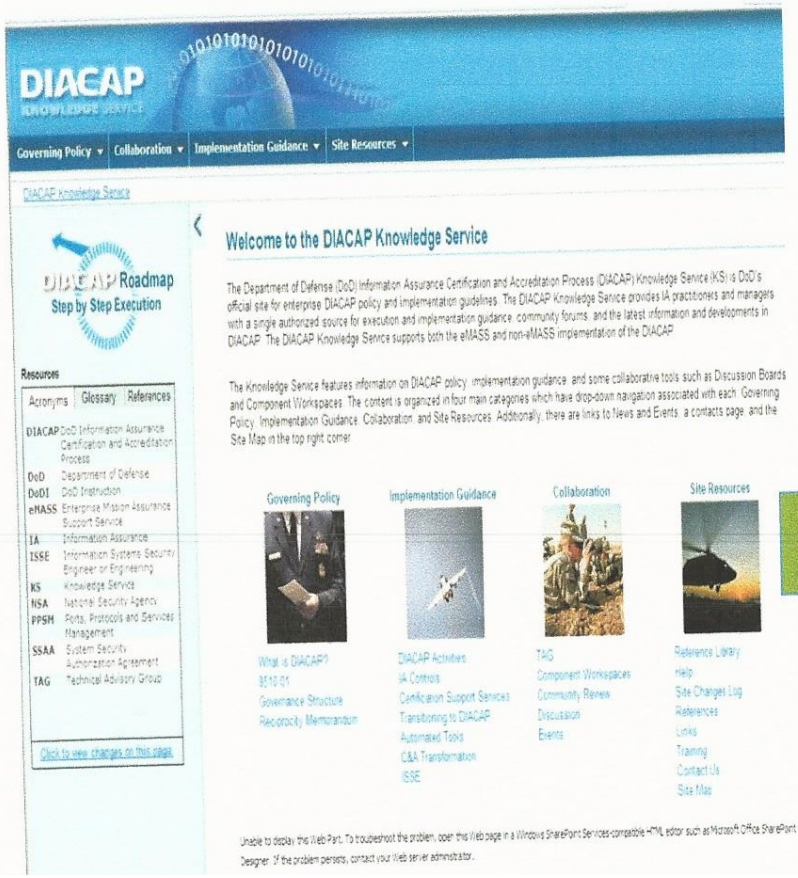
- **NIST Special Publications (SP)**
  - 800-37 – Guide for Applying the RMF
  - 800-39 – Managing Information Security Risks
  - 800-53 – Security and Privacy Controls
  - 800-53A - Guide for Assessing the Security Controls
  - 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories
  - 800-137 – Information Security Continuous Monitoring
- **Committee on National Security Systems (CNSS)**
  - Instruction 1253 - Security Categorization and Control Selection for National Security Systems
  - Instruction 4009 – Information Assurance Glossary
  - Policy 11 - National Policy Governing the Acquisition of IA and IA-Enabled IT Products

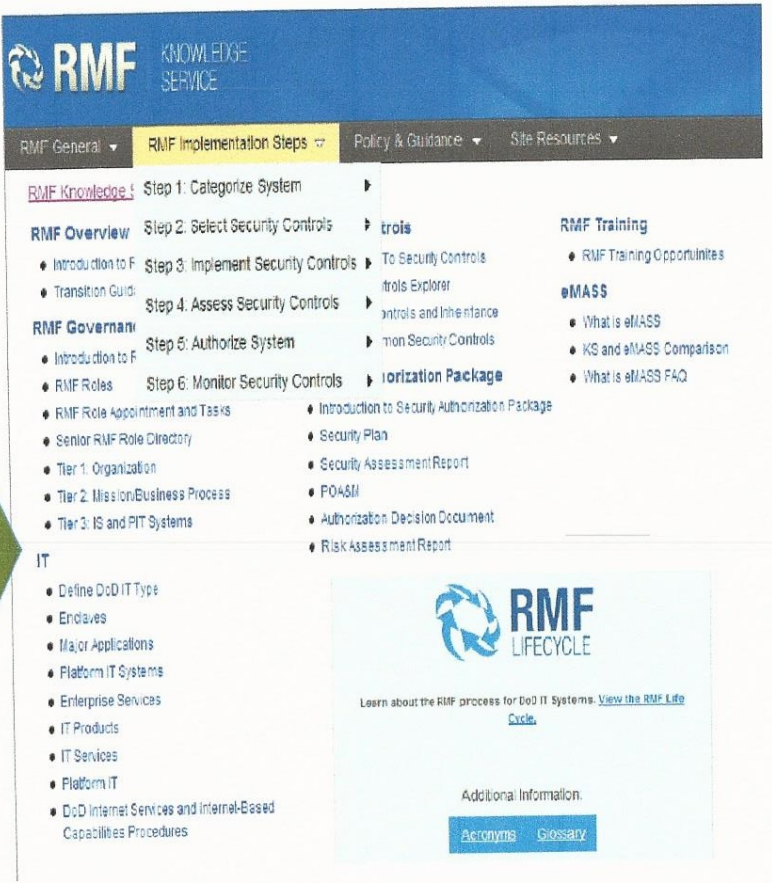
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

**DoDI 8500.01 - Cancels or supersedes 11 DoD Directives, Instructions, or Memorandums, and references a total of 132 policy documents, including 12 NIST Special Publications and 9 CNSS Instructions or Policies.**

# Risk Management Framework Knowledge Service

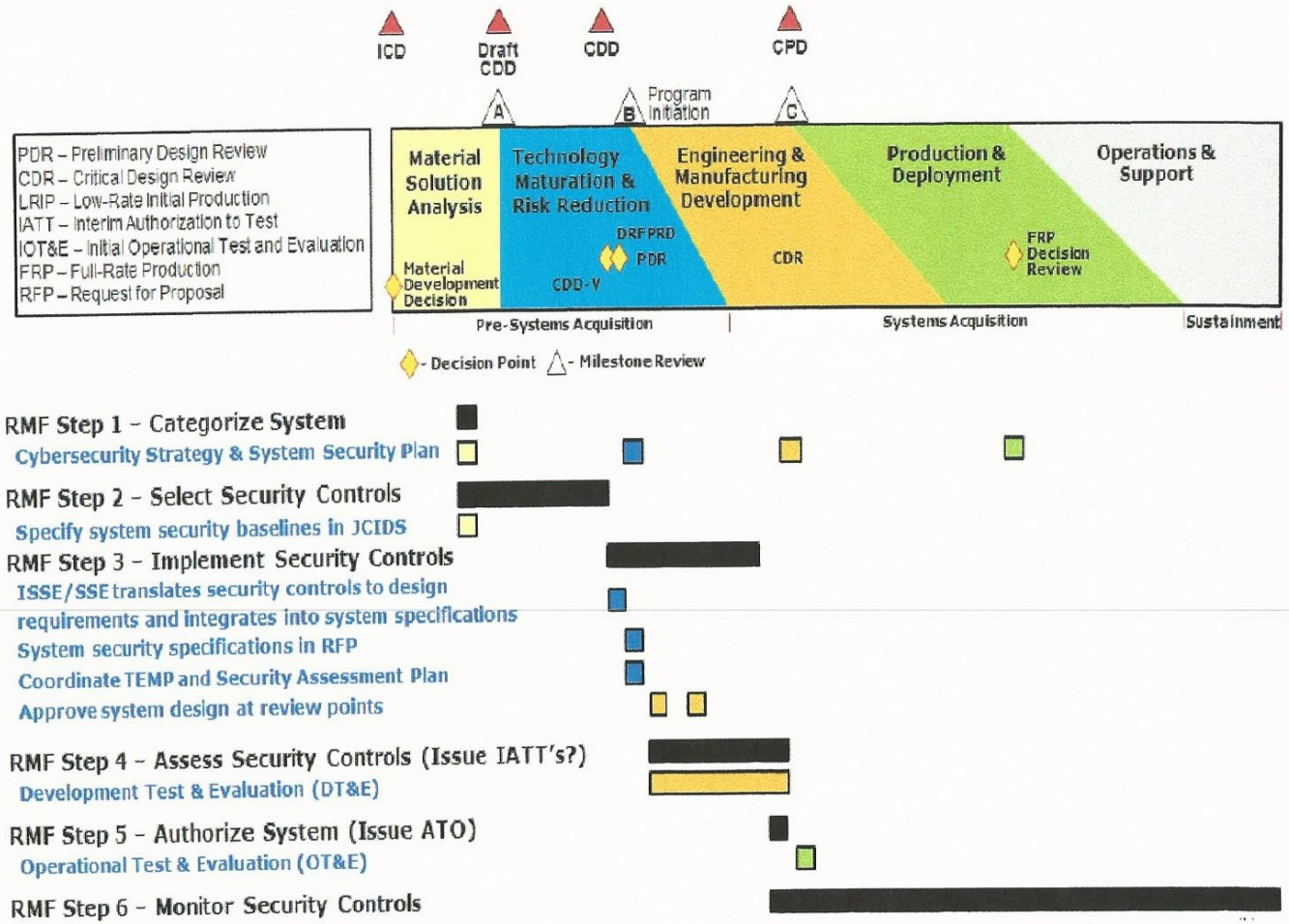
The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework



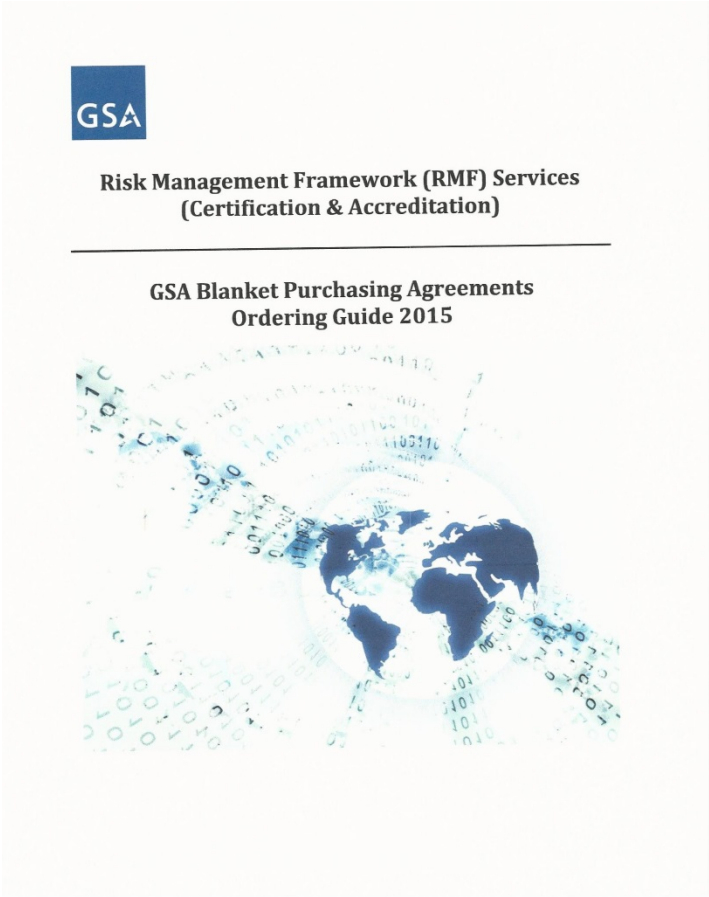
# Risk Management Framework and The Current Acquisition Cycle

**Cybersecurity requirements must be identified and included throughout the lifecycle of systems to include acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions.**



# Risk Management Framework (RMF) Services (Certification & Accreditation) GSA Blanket Purchasing Agreements Ordering Guide 2015

The GSA established multiple BPAs for RMF CA offerings on behalf of the ISSLOB.
The RMF CA BPAs were awarded competitively against GSA Multiple Award Schedule (MAS) 70 contracts. It is the responsibility of the ordering activity contracting officer to ensure compliance with all applicable fiscal laws prior to issuing an order under a BPA, and to ensure that the selected BPA holder provides the best value for the requirement being ordered.
Authorized BPA Users: Orders may be placed under this BPA by sources identified under GSA Order, ADM 4800.2G, United States Federal agencies, Department of Defense (DoD) components, State, Local, and Tribal Governments, and cost-reimbursement Contractors authorized to order in accordance with FAR Part 51.
For the purposes of this agreement, a DoD component is defined as: the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (DoD IG), the Defense Agencies, the DoD Field Activities, the U.S. Coast Guard, and the Intelligence Community. GSA or other applicable ordering organizations/agencies are authorized to place orders under this BPA on behalf of DoD end users and must comply with Defense Federal Acquisition Regulation Supplement (DFARS) 208.7400.



# Risk Management Framework Authorizations

| Authorization Type | Decision Criteria | Authorization Period |
|---|---|---|
| **Authorization to Operate (ATO)** | Overall risk is determined to be acceptable, and there are no NC controls with a level of risk of "Very High" or "High". | Must specify an Authorization Termination Date (ATD) that is within 3 years of the authorization date unless the IS or PIT system has a system-level, DoD policy compliant ,continuous monitoring program. |
| **ATO with conditions** (Only with permission of the DoD Component Chief Information Officer (CIO)) | NC controls with "Very High" or "High" risk that can't be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality | Should specify an AO review period that is within 6 months of the authorization date. If the system still requires operation with a level of risk of "Very High" or "High" after 1 year, the DoD Component CIO must again grant permission for continued operation of the system. |
| **Interim Authority To Test (IATT)** | Risk determination is being made to permit testing of the system in an operational information environment or with live data, and the risk is acceptable, | Should expire at the completion of testing (normally for a period of less than 90 days ) |
| **Denial of Authorization to Operate (DATO)** | Risk is determined to be unacceptable | Immediate or in concert with a system decommissioning strategy |

# Risk Management Framework Transition Timeline

| | System Authorization Status | Transition Timeline And Instructions |
|---|---|---|
| 1 | New start or unaccredited | Transition to the RMF within six months |
| 2 | System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan | Transition to the RMF within six months |
| 3 | System has begun executing the DIACAP Implementation Plan | Either:<br>a. Continue under DIACAP. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline<br>or<br>b. Transition to the RMF within six months |
| 4 | System has a current valid DIACAP accreditation decision | Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline |
| 5 | System has a DIACAP accreditation that is more than 3 years old | Transition to the RMF within six months |

# Risk Management Framework Transition Timeline

| Completed DIACAP Package Submitted to AO for Signature | ATO Date | Maximum Duration of ATO under DIACAP |
|---|---|---|
| Present through May 31, 2015 | Determined by AO Signature Date | 2.5 years from AO signature date |
| June 1, 2015 through February 1, 2016 | | 2 years from AO signature date |
| February 2, 2016 through October 1, 2016 | | 1.5 years from AO signature date |

**What this means:**

The longer you stay with DIACAP, the shorter the ATO. DIACAP certified systems should be almost extinct by mid-year 2018.

# ETSI Cyber Security Technical Committee (TC CYBER)

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).

ISO/IEC 27000-series
ISO/IEC 27001:2005
ISO/IEC 27001:2013
ISO/IEC 27002 (formerly ISO/IEC 17799)

BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use.

Information Security Forum (ISF) published a comprehensive list of best practices for information security, published as the Standard of Good Practice (SoGP). The ISF continues to update the SoGP every two years; the latest version was published in 2013.

The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200. The newest version of NERC 1300 is called CIP-002-3 through CIP-009-3 (CIP=Critical Infrastructure Protection). These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best-practice industry processes.

# Federal Information Security Modernization Act (FISMA)

The Federal Information Security Modernization Act (FISMA) of 2014 updates the Federal Government's cybersecurity practices by:
• Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security Federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems;
• Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by
• Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting."

**FISMA 2014 codifies the Department of Homeland's Security's role in administering the implementation of information security policies for Federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing the policies.**

The legislation provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. It also:
• Authorizes DHS to provide operational and technical assistance to other Federal Executive Branch civilian agencies at the agency's request;
• Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
• Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
• Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
• **Requires agencies to report major information security incidents as well as data breaches** to Congress, as they occur and annually and
• Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting, while adding new reporting requirements for major information security incidents.

**FY16 FISMA Documents**
FY16 CIO Annual FISMA Metrics

http://www.dhs.gov/fisma

**FY15 FISMA Documents**
FY15 CIO Annual FISMA Metrics
FY15 IG FISMA Metrics
FY15 SAOP FISMA Metrics
FY15 CIO Q3 FISMA Metrics
FY15 CIO Q2 FISMA Metrics
FY15 CIO Q1 FISMA Metrics

**FY14 FISMA Documents**
FY14 CIO Annual FISMA Metrics
FY14 Micros Annual FISMA Metrics
FY14 IG Annual FISMA Metrics
FY14 SAOP Annual FISMA Metrics
FY14 CIO Q2 FISMA Metrics
FY14 SAOP Q2 FISMA Metrics

# Industrial Automation and Control Systems

ISA/IEC-62443 (formerly ISA-99)

ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

Group 1: General ISA-62443-1-1 (IEC/TS 62443-1-1) (formerly referred to as "ISA-99 Part 1") was originally published as ISA standard ANSI/ISA-99.00.01-2007, as well as an IEC technical specification IEC/TS 62443-1-1. The ISA99 committee is currently revising it to make it align with other documents in the series, and to clarify normative content.
ISA-TR62443-1-2 (IEC 62443-1-2) is a master glossary of terms used by the ISA99 committee. This document is a working draft, but the content is available on the ISA99 committee Wiki.
ISA-62443-1-3 (IEC 62443-1-3) identifies a set of compliance metrics for IACS security. This document is currently under development and the committee will be releasing a draft for comment in 2013.
ISA-62443-1-4 (IEC/TS 62443-1-4) defines the IACS security life cycle and use case. This work product has been proposed as part of the series, but as of January 2013 development had not yet started.

https://www.isa.org/isa99/

# Industrial Automation and Control Systems

Group 2: Policy and Procedure ISA-62443-2-1 (IEC 62443-2-1) (formerly referred to as "ANSI/ISA 99.02.01-2009 or ISA-99 Part 2") addresses how to establish an IACS security program. This standard is approved and published the IEC as IEC 62443-2-1. It now being revised to permit closer alignment with the ISO 27000 series of standards.
ISA-62443-2-2 (IEC 62443-2-2) addresses how to operate an IACS security program. This standard is currently under development.
ISA-TR62443-2-3 (IEC/TR 62443-2-3) is a technical report on the subject of patch management in IACS environments. This report is currently under development.
ISA-62443-2-4 (IEC 62443-2-4) focuses on the certification of IACS supplier security policies and practices. This document was adopted from the WIB organization and is now a working product of the IEC TC65/WG10 committee. The proposed ISA version will be a U.S. national publication of the IEC standard.

Group 3: System Integrator ISA-TR62443-3-1 (IEC/TR 62443-3-1) is a technical report on the subject of suitable technologies for IACS security. This report is approved and published as ANSI/ISA-TR99.00.01-2007 and is now being revised.
ISA-62443-3-2 (IEC 62443-3-2) addresses how to define security assurance levels using the zones and conduits concept. This standard is currently under development.
ISA-62443-3-3 (IEC 62443-3-3) defines detailed technical requirements for IACS security. This standard has been published as ANSI/ISA-62443-3-3 (99.03.03)-2013. It was previously numbered as ISA-99.03.03.

Group 4: Component Provider ISA-62443-4-1 (IEC 62443-4-1) addresses the requirements for the development of secure IACS products and solutions. This standard is currently under development.
ISA-62443-4-2 (IEC 62443-4-2) series address detailed technical requirements for IACS components level. This standard is currently under development.

# IASME Standard

The IASME standard was developed over several years during a Technology Strategy Board funded project to create an achievable cyber security standard for small companies. The international standard, ISO27001, is comprehensive but extremely challenging for a small company to achieve and maintain. The IASME standard is written along the same lines as the ISO27001 but specifically for small companies. The gold standard of IASME demonstrates baseline compliance with the international standard

It provides criteria and certification for small-to-medium business cybersecurity readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cybersecurity posture of the enterprise and its protection of personal/business data.

IASME was established to enable businesses with capitalization of 1.2 billion pounds or less (1.5 billion Euros; 2 billion US dollars) to achieve an accreditation similar to ISO 27001 but with reduced complexity, cost, and administrative overhead (specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO 27001).

The cost of the certification is progressively graduated based upon the employee population of the SME (e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees); the certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor. Some insurance companies reduce premiums for cybersecurity related coverage based upon the IASME certification.

https://www.iasme.co.uk/index.php/about

# IEC 62443 Conformity Assessment Program

http://www.isasecure.org/en-US/Certification

ISASecure® Certifications
The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure™ conformance certification program. ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities.

ISCI also offers an ISASecure organization process certification for product development organizations. The Security Development Lifecycle Assurance (SDLA) certification promotes security development lifecycle practices intended to improve the quality of security in IAC systems.

The ISA Security Compliance Institute (ISCI) www.isasecure.org operates the first conformity assessment scheme for **IEC 62443 IACS cybersecurity standards.** This program certifies Commercial Off-the-shelf (COTS) IACS products and systems, addressing securing the IACS supply chain.

Certification Offerings Two COTS product certifications are available under the ISASecure® brand: ISASecure-EDSA (Embedded Device Security Assurance) certifying IACS products to the **IEC 62443-4-2 IACS cybersecurity standard** and ISASecure-SSA (System Security Assurance), certifying IACS systems to the **IEC 62443-3-3 IACS cybersecurity standard**.

A third certification, SDLA (Secure Development Lifecycle Assurance) is available which certifies IACS development organizations to the **IEC 62443-4-1 cybersecurity standard**, providing assurances that a supplier organization has institutionalized cybersecurity into their product development practices.

**ISO 17065 and Global Accreditation** The ISASecure 62443 conformity assessment scheme is an ISO 17065 program whose labs (certification bodies or CB) are independently accredited by ANSI/ANAB, JAB and other global ISO 17011 accreditation bodies (AB).
Through Mutual Recognition Arrangements (MRA) with IAF, ILAC and others, the accreditation of the ISASecure labs by the ISA 17011 accreditation bodies ensures that certificates issued by any of the ISASecure labs are globally recognized.

Test Tool Recognition The ISASecure scheme includes a process for recognizing test tools to ensure the tools meet functional requirements necessary and sufficient to execute all required product tests and that test results will be consistent among the recognized tools.

Chemicals, Oil and Gas Industries ISCI development processes include maintenance policies to ensure that the ISASecure certifications remain in alignment with the IEC 62443 standards as they evolve. While the IEC 62443 standards are designed to horizontally address technical cybersecurity requirements of a cross-section of process industries, the ISASecure scheme's certification requirements have been vetted by representatives from the chemical and oil and gas industries and are reflective of their cybersecurity needs.

# US CERT

Standards and References

**https://ics-cert.us-cert.gov/Standards-and-References**

This page provides an extensive bibliography of references and standards associated with control system cyber topics. The list is categorized as follows with web links provided where applicable:

- Cyber Security Policy Planning and Preparation
- Establishing Network Segmentation, Firewalls, and DMZs
- Patch, Password, and Configuration Management
- Control System Cyber Security Training for Engineers, Technicians, Administrators, and Operators
- Establishing and Conducting Asset, Vulnerability, and Risk Assessments
- Control System Security Procurement Requirements Specification
- Placement and Use of IDSs and IPDSs
- Authentication, Authorization, and Access Control For Direct and Remote Connectivity
- Securing Wireless Connections
- Use of VPNs and Encryption in Securing Communications
- Establishing a Secure Topology and Architecture
- Applying and Complying with Security Standards
- Ensuring Security when Modernizing and Upgrading

# Recently Enacted Legislation

P.L. 114-113, Cybersecurity Act of 2015, signed into law December 18, 2015. Promotes and encourages **the private sector and the US government** to rapidly and responsibly exchange cyber threat information.

P.L. 113-274, Cybersecurity Enhancement Act of 2014, signed into law December 18, 2014. Provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

P.L. 113-282, National Cybersecurity Protection Act of 2014, signed into law December 18, 2014. **Codifies an existing operations center for cybersecurity**.

P.L. 113-246, Cybersecurity Workforce Assessment Act, signed into law December 18, 2014. Directs the Secretary of Homeland Security, within 180 days and annually thereafter for three years, to conduct an assessment of the cybersecurity workforce of the Department of Homeland Security (DHS).

# Legislation Worth Watching

**H.R. 104, Cyber Privacy Fortification Act of 2015.** Would protect cyberprivacy. Introduced January 6, 2015, by J. Conyers (D-MI)

**H.R. 234, Cyber Intelligence Sharing and Protection Act**. Would provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities. Introduced January 8, 2015, by D. Ruppersberger (D-MI)

**H.R.555, Federal Exchange Data Breach Notification Act of 2015**. Would require an Exchange established under the Patient Protection and Affordable Care Act to notify individuals in the case that personal information of such individuals is known to have been acquired or accessed as a result of a breach of the security of any system maintained by the Exchange. Introduced January 27, 2015, by D. Black (R-TN)

**H.R. 580, Data Accountability and Trust Act.** Would protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and provide for nationwide notice in the event of a security breach. Introduced January 28, 2015, by B. Rush (D-IL)

**H.R. 1053, Commercial Privacy Bill of Rights Act of 2015**. Would establish a regulatory framework for the protection of personal data for individuals under the Federal Trade Commission, and improve provisions relating to collection, use, and disclosure of personal information of children. Introduced February 27, 2015, by A. Sires (D-NJ)

**H.R. 1560, Protecting Cyber Networks Act**. Would improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats.

Introduced March 24, 2015, by D. Nunes (R-CA) Reported (Amended) April 13, 2015, by the Committee on Intelligence. H. Rept. 114-63. Passed House April 22, 2015, by a vote of 307 to 116.

**H.R. 1704, Personal Data Notification and Protection Act of 2015**. Would establish a national data breach notification standard. Introduced March 26, 2015, by J. Langevin (D-RI)

**H.R. 1731, National Cybersecurity Protection Advancement Act of 2015** Would enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections. Introduced April 13, 2015, by M. McCaul (R-TX)

Reported (Amended) April 17, 2015, by the Committee on Homeland Security. H. Rept. 114-83. Passed House April 23, 2015, by a vote of 355 to 63.

# Legislation Worth Watching

**H.R. 1770, Data Security and Breach Notification Act of 2015**. Would require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information. Introduced April 14, 2015, by M. Blackburn (R-TN)
**H.R. 2029, Cybersecurity Act of 2015**. Would improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. Passed House December 18, 2015, by a vote of 316 to 113 Passed Senate December 18, 2015, by a vote of 65 to 33 Signed into law (P.L. 114-113) by President Obama December 18, 2015
**H.R. 2205, Data Security Act of 2015**. Would protect financial information relating to consumers and require notice of security breaches. Introduced May 1, 2015, by R. Neugebauer (R-TX)
**H.R. 2977, Consumer Privacy Protection Act of 2015**. Would ensure the privacy and security of sensitive personal information, prevent and mitigate identity theft, provide notice of security breaches involving sensitive personal information, and enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information. Introduced July 8, 2015, by D. Cicilline (D-RI)
**H.R. 4350, Cybersecurity Act of 2015 Repeal**. Would repeal the Cybersecurity Act of 2015. Introduced January 8, 2016, by J. Amash (R-MI)
**S. 135, Secure Data Act of 201**5. Would provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities. Introduced January 8, 2015, by R. Wyden (D-OR)
**S. 177, Data Security and Breach Notification Act of 2015**. Would protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and provide for nationwide notice in the event of a breach of security. Introduced January 13, 2015, by B. Nelson (D-FL)
**S. 456, Cyberthreat Sharing Act of 2015**. Would codify mechanisms for enabling cybersecurity threat indicator sharing between private and government entities, as well as among private entities, to better protect information systems. Introduced February 11, 2015, by T. Carper (D-DE)

# Legislation Worth Watching

**S. 547, Commercial Privacy Bill of Rights Act of 2015**. Would establish a regulatory framework for the protection of personal data for individuals under the Federal Trade Commission, and improve provisions relating to collection, use, and disclosure of personal information of children. Introduced February 24, 2015, by R. Menendez (D-NJ)

**S. 754, Cybersecurity Information Sharing Act of 2015**. Would improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. Introduced March 17, 2015, by R. Burr (R-NC) Senator Burr from Select Committee on Intelligence filed written report, April 15, 2015. Report No. 114-32.
Passed Senate October 27, 2015 by a vote of 74 to 21

**S. 961, Data Security Act of 2015**. Would protect information relating to consumers and require notice of security breaches. Introduced April 15, 2015, by T. Carper (D-DE)

**S. 1027, Data Breach Notification and Punishing Cyber Criminals Act of 20**15. Would require notification of information security breaches and enhance penalties for cyber criminals. Introduced April 21, 2015, by M. Kirk (R-IL)

**S. 1158, Consumer Privacy Protection Act of 2015**. Would ensure the privacy and security of sensitive personal information, mitigate identity theft, and provide notice of security breaches. Introduced April 30, 2015, by P. Leahy (D-VT)

**S. 2410, Cybersecurity Disclosure Act of 20**15. Would promote transparency in the oversight of cybersecurity risks at publicly traded companies. Introduced December 17, 2015, by J. Reed (D-RI)

# The Cybersecurity Act of 2015 (P. L. 114-113)

Government entities and private-sector organizations in the United States now have a common framework that encourages the sharing of cybersecurity threat information among each other, thanks to new federal legislation. These guidelines also protect the privacy of personally identifiable information and provide liability protections to organizations that follow the framework and act in good faith.

Just before adjourning for the year, the US Congress passed the Cybersecurity Act of 2015 (P. L. 114-113) on 18 December 2015, and President Barack Obama signed the measure into law later the same day. The legislation was tacked on to a massive omnibus appropriations bill at the last minute to facilitate consideration of the bill in the full House of Representatives and the Senate. The Cybersecurity Act of 2015 aims to defend against cyberattacks by creating a framework for the voluntary sharing of cyber threat information between private entities and the federal government as well as within agencies of the federal government. Simultaneously, the legislation also aims to protect individuals' privacy rights by ensuring that personal information is not unnecessarily divulged.

The goal of the legislation is to promote and encourage the private sector and the US government to exchange cyber threat information rapidly and responsibly. Under the Act, information about a threat found on one system can be quickly shared in order to prevent a similar attack or mitigate a similar threat to other companies, agencies and consumers. Privacy advocates counter that the new law authorizes and enables broader surveillance by the federal government and provides weak privacy protections.

# Risk Management Framework Training

**http://www.dhs.gov/risk-management-framework-certification-and-accreditation-service-offerings**
**DHS Risk Management Framework Certification and Accreditation Service Offerings** The Risk Management Framework (RMF) Shared Service Centers (SCC) were established to facilitate the implementation of common RMF solutions for areas that many agencies are missing when striving to achieve greater efficiencies in executing the RMF Certification & Accreditation (C&A) process.

SSCs are intended to improve quality of service and reduce the costs of completing certification and accreditation on systems across the Federal Government. RMF C&A SSCs are complemented by the RMF C&A Private Industry Service Blanket Purchase Agreements (BPAs) processed under the ISSLoB Industry Service Acquisition Program. Fourteen BPAs have been awarded and are available. Please visit the U.S. General Services Administration Risk Management Services page for further information.

**http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training/**
http://csrc.nist.gov/groups/SMA/fisma/rmf-training.html
Applying the Risk Management Framework to Federal Information Systems Welcome to the course “Applying the Risk Management Framework to Federal Information Systems”.

# Example Training Course

**Course Topics**

**Introduction to RMF for DOD IT**
• Understanding the Military Security Authorization Process & History
• Risk Management Framework
• Categorization of Information System
• Establishing the Security Control Baseline
• Applying Security Controls
• Assessing the Controls
• Authorization of the Information System
• Monitoring Security Controls
• DOD adaptation of RMF
• DODI 8510.01
• DODI 8500.01
• CNSSI-1253, rev.2
• Understand the Risk Management Approach to Security Authorization
• Understand and Distinguish among the Risk Management Framework (RMF) Steps
• Terms and Definitions
• Define and Understand Roles and Responsibilities
• Relationship between the RMF and SDLC
• Legal, Regulatory, Guidance & Required Documents
• Inter-related Security Authorization Processes
• Ongoing Monitoring Strategies

**RMF Step 1 - Categorization**
• Information System
• System Security Plan
• Categorize a System
• National Security System
• System Boundaries
• Register System

**RMF Step 2 – Establish the Security Control Baseline**
• Common Controls and Security Control Inheritance
• Risk Assessment as part of the Risk Management Framework (RMF)

**RMF Step 3 – Apply Security Controls**
• Implement Selected Security Controls
• Tailoring of Security Controls
• Document Security Control Implementation

**RMF Step 4 – Assess Security Controls**
• Prepare for Security Control Assessment
• Establish Security Control Assessment Plan (SAP)
• Determine Security Control Effectiveness – Perform the Testing
• Develop Initial Security Assessment Report (SAR)
• Perform Initial Remediation Actions
• Develop Final Security Assessment Report and Addendum

**RMF Step 5 - Authorize Information System**
• Develop Plan of Action and Milestones (POAM)
• Assemble Security Authorization Package
• Determine Risk
• Determine the Acceptability of Risk
• Obtain Security Authorization Decision

**RMF Step 6 – Monitor Security Controls**
• Determine Security Impact of Changes to System and Environment
• Perform Ongoing Security Control Assessments
• Conduct Ongoing Remediation Actions
• Update Key Documentation
• Perform Periodic Security Status Reporting
• Perform Ongoing Risk Determination and Acceptance
• Decommission and Remove System

# Contact Information

## For any questions or comments, contact

**David C. Hall**
**ESEP/CISSP**
**Hall Associates LLC**
**301 641-1530**
**Dave.hall@hallassociateshsval.com**