# DoD Instruction 1015.16

# Nonappropriated Fund Instrumentalities Information Technology Policies and Procedures

---

| | |
|---|---|
| **Originating Component:** | Office of the Under Secretary of Defense for Personnel and Readiness |
| **Effective:** | 0DUF□ |
| **Releasability:** | Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/. |
| **Approved by:** | Gilbert R. Cisneros, Jr., Under Secretary of Defense for Personnel and Readiness |

---

**Purpose:** In accordance with the authority in DoD Directive 5124.02, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for reciprocal acceptance of authorization decisions and artifacts within the nonappropriated funds instrumentality (NAFI) programs governed by DoD Instruction (DoDI) 1015.15, for the authorization and connection of NAFI information technology (IT).
- Establishes the Nonappropriated Funds (NAF) IT Working Group.

# TABLE OF CONTENTS

# SECTION 1: GENERAL ISSUANCE INFORMATION

## 1.1. APPLICABILITY.

This issuance applies to:

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

b. NAFI management of resources, programs, and activities that support military and civilian morale, welfare, and recreation (MWR) programs, Military Services Exchanges, and DoD lodging programs (excluding public-private ventures for lodging), as discussed in DoDIs 1015.10, 1015.15, 1015.11, and 1330.21.

c. All NAFI IT, as specified in Section 3, that receive, process, store, display, or transmit NAF program information. These technologies are broadly grouped as NAFI information systems (IS), NAFI platform IT (PIT), NAFI IT services, and NAFI IT products. This includes NAFI IT supporting market research, product and program development, implementation and evaluation specific to MWR, exchange, DoD official lodging, and other NAFIs, as well as NAF-controlled NAFI IT operated by a contractor or other entity on behalf of the NAFI to include "Software as a Service."

## 1.2. POLICY.

It is DoD policy that:

a. The cybersecurity requirements of NAFI IT will comply with the risk management framework (RMF), as set forth in DoDI 8500.01 and DoDI 8510.01. NAFI IT systems will utilize the RMF in accordance with Section 5.

b. NAFI IT acquisition processes and procedures will be in accordance with DoDI 5000.82, with exceptions identified in DoDI 4105.67.

c. Procurement of NAFI IT will follow policies prescribed in DoDI 4105.67, DoDI 5000.82, DoDI 5000.87, including but not limited to software pathways, and, where appropriate, DoDI 5000.75.

d. All DoD records maintained in IT systems managed by NAFIs must be managed in compliance with DoDI 5015.02.

e. NAFI IT Enterprise Owners should continuously review the portfolio of IT to leverage best practices and modernize systems and software when possible to enable better capability faster delivery, and automation.

# SECTION 2: RESPONSIBILITIES

## 2.1. ASSISTANT SECRETARY OF DEFENSE FOR MANPOWER AND RESERVE AFFAIRS (ASD(M&RA)).

Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness, the ASD(M&RA):

a. Develops uniform DoD NAFI IT policy and guidance to ensure proper administration of NAF procurements and monitors compliance in accordance with Section 5.

b. Oversees the implementation of this issuance.

c. Designates the NAF IT Business Mission Area Owner (BMAO) in accordance with Section 4. The BMAO chairs the NAF IT Working Group, defined in Paragraph 4.5.

## 2.2. DOD COMPONENT HEADS.

The DoD Component heads:

a. Comply with and implement the provisions of this issuance.

b. Ensure that each of their respective MWR and exchange IT enterprise entities has its own trained and qualified authorizing official (AO) designated in writing for all NAF IS and PIT systems, in accordance with DoDI 8500.01.

c. Establish NAFI IT management oversight and internal control systems, in accordance with DoDI 8510.01.

d. Develop and provide NAFI IT Enterprise-level NAFI IT policies and procedures to implement this issuance.

e. Support the establishment of the NAF IT Working Group for all NAFIs to improve NAF IT systems.

# SECTION 3: NAFI IT

## 3.1. GENERAL.

NAFI IT includes all IT that is:

a. Used or managed exclusively by or within a NAFI defined in DoDI 1015.15.

b. NAFI IT does not include any IT that is managed or used by public-private ventures that:

(1) Fall under the Military Privatization Housing Initiative, pursuant to Sections 2871 through 2885 of Title 10, United States Code.

(2) Are contractor operated (per agreement with DoD) in government-owned, commercially-owned, or commercially-leased facilities, pursuant to DoDI 1015.11.

## 3.2. NAFI IT FUNCTIONS.

NAFI IT consists of Government NAF business, retail, MWR activities, DoD official lodging, and other NAF functions governed by DoDI 1015.15, in accordance with DoDI 5000.75, and is distinct and isolated from DoD and other government appropriated funded warfighting networks and technologies. NAFI IT may have the following attributes:

a. Connections with external commercial entities to conduct real time transactions.

b. Subjection to physical and virtual inspections by outside commercial auditors as part of the annual Payment Card Industry (PCI) audit process.

c. Categorization of .com, .org, .edu, or .gov domains.

d. Shared Layer 1 physical infrastructure used by DoD entities, but is separate and distinct at Layer 2 and higher, as defined in open systems interconnection model.

## 3.3. NAFI IT CATEGORIZATION.

a. As defined in DoDI 5000.75, a business system does not include a national security system or an IS used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the DoD conducted for the MWR of Service members using NAF.

b. Certain NAF IT business systems may be excluded from DoDI 5000.75 governance. NAF IT business systems are not “covered business systems” subject to requirements of Section 2222(g) of Title 10, United States Code, and certification under Appendix 4C.2 of DoDI 5000.75 if the NAFI IT business system is used exclusively by a NAF that is administered through the auspices of a NAFI that is designated for the collective benefit of authorized patrons in accordance with DoDI 1015.15.

# SECTION 4: NAFI IT GOVERNANCE

## 4.1. GENERAL.

NAFI IT governance incorporates and leverages stakeholders across three bodies of governance, the NAF IT BMAO, NAF AOs including DoD NAFI IT Enterprise-level support, and the NAF IT Working Group. These bodies of governance for NAFI IT will ensure all relevant parties are aware and informed participants in the maintenance and strategic development of NAF IT cybersecurity.

## 4.2. NAF IT BMAO.

The NAF IT BMAO, within the Office of the ASD(M&RA), will:

a. Maintain a copy of the inventory data generated by the NAF AOs' annual assessment of the full suite of systems and applications owned and operated across the NAF IT Portfolio. The annual NAF IT portfolio assessment, available at https://dodmwrandresalepolicy.defense.gov/, will be completed by the NAF AOs for each of their respective NAF IT sub-portfolios by July 1 of each calendar year. Each NAF AO will provide the Office of Military Community and Family Policy within ASD(M&RA) with a copy of the assessment. Inventory data includes but is not limited to: systems comprised of moveable equipment, commercial off-the-shelf software, licenses, integrated point-of-sale cash registers, and all other related hardware and software components.

b. Oversee the cybersecurity risk management of NAF IT and distribute RMF information standards and sharing requirements.

c. Chair the NAF IT Working Group.

d. Serve as a member of the RMF Technical Advisory Group and represent the interests of NAFIs in this capacity, in accordance with DoDI 8510.01.

e. Provide detailed analysis and authoring support for the NAF IT portion of the RMF knowledge service.

## 4.3. NAF AO.

Each NAF IT Enterprise-level Owner must have a NAF AO. The NAF AO must be a DoD official who is at least a General Schedule Grade 15 or equivalent, and a U.S. citizen. The NAF AO will serve on a collateral duty basis, unless a NAFI IT Enterprise Owner converts the role to a full-time position. The NAF AO will:

a. Appoint NAFI IT Enterprise-level representatives, including a security control assessor (SCA).

b. Complete the DoD AO computer-based training.

c. Ensure IT, within the AO's NAFI IT Enterprise-level portfolio, operates at an acceptable level of risk to NAFI operations, assets, individuals, or other organizations.

d. Render authorization decisions for DoD NAFI IS and PIT systems under the NAF AO's purview in accordance with DoDI 8510.01.

e. Issue authorization guidance in coordination with the DoD NAFI IT Enterprise Owners and approve or deny the operation (or the testing) of the assigned NAF IT by issuing an authorization decision (e.g., authorization to operate (ATO), ATO with conditions, interim authorization to test, or denial of ATO).

f. Review the security authorization package, accompanied by supporting material and the recommendation of the SCA, as a basis for determining risk to provide an authorization decision.

g. Identify, evaluate, and determine the correct tools and systems to manage NAF IT.

h. In accordance with DoDIs 8500.01 and 8510.01:

(1) Ensure all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned IS and PIT systems.

(2) Monitor and track execution of system-level plans of action and milestones (POA&Ms).

(3) Promote reciprocity, consistent with DoDI 8510.01, to the maximum extent possible.

(4) Refrain from delegating authorization decisions. Other AO responsibilities and tasks may be delegated to a formally appointed and qualified AO designated representative (AODR).

(5) Review the security artifacts in light of mission and information environment indicators and determine a course of action that will be provided to the responsible chief information officer (CIO) or the senior information security office for reporting requirements described in Subchapter II of Chapter 35 of Title 44, United States Code, also known as the "Federal Information Security Modernization Act of 2014."

(6) Downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant.

(7) Determine applicability of PCI Data Security Standard (PCI DSS), RMF security standards, and DoD CIO exceptions to policy for RMF.

(8) Authorize PCI DSS-scoped systems to operate in the NAFI environment and ensure PCI DSS assessments and PCI DSS attestations of compliance are conducted annually or upon major changes to the NAFI environment. The NAFI environment must meet PCI DSS compliance annually as defined and directed by the PCI Security Standards Council. A third-

party PCI DSS qualified security assessor may be used for PCI DSS assessments and PCI DSS attestations of compliance.

i. Conduct an annual NAF IT portfolio assessment and provide Military Community and Family Policy with a copy as required in accordance with Paragraph 4.2.

j. In coordination with the NAF IT Working Group, the NAF AOs will:

(1) Incorporate consideration of the input of NAFI representatives regarding their business interests and potential implications on security requirements into NAF AO guidance.

(2) Advise NAFI IT Enterprise Owner-level support on the applicability of DoD laws, rules, and regulations to NAFI IT operations.

k. Ensure compliance with Section 794d of Title 29, United States Code, also referred to as "Section 508 of the Rehabilitation Act of 1973, as amended." and the electronic and information technology accessibility standards set forth in Part 1194 of Title 36, Code of Federal Regulations.

## 4.4. DOD NAFI IT ENTERPRISE OWNER-LEVEL SUPPORT.

DoD NAFI IT Enterprise Owner-level support will consist of program teams, who are responsible for delivering IT systems, operations teams, and NAFI IT Enterprise-level staff designated by the NAF AO as the office of primary responsibility for AODR functions. DoD NAFI IT Enterprise Owner-level support will assist NAF AOs in the execution of their responsibilities. When authorized by the NAF AO, and in accordance with DoDI 8510.01, NAFI IT Enterprise Owner-level support may:

a. Make decisions with regards to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring of the implementation of POA&Ms and the assessment or determination of risk.

b. Prepare the final authorization package, obtain the NAF AO's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials. The NAF AO may not delegate the authorization decision itself or the authority to sign the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the United States) to the NAFI IT Enterprise Owner-level support office.

## 4.5. NAF IT WORKING GROUP.

The NAF IT Working Group:

a. Is comprised of NAF AOs, AODRs, and other stakeholders as applicable to the topic; it is chaired by the NAF IT BMAO.

b. Meets at least quarterly to discuss activities, identify opportunities for collaboration, discuss strategies to meet overall NAF IT objectives, evaluate compliance with DoD guidance, and review management reports and audit results.

c. Coordinates technology modernization efforts and standards across the DoD NAFI IT Enterprise to leverage best practices and continuously seeks to improve how NAF IT meets the business needs of the NAFIs while appropriately protecting NAFI information and resources.

d. Establishes the NAF IT business mission area (BMA) to represent the NAFIs when collaborating with the DoD CIO and to identify common IT and cybersecurity policy vision, goals, desired capabilities, and outcome measures based on participating NAFIs' input and guidance.

e. Defines roles, and responsibilities within the NAF IT BMA.

f. Advises the NAF AOs regarding the prioritization of ATO decisions based on business or operational inputs and other needs expressed by the NAFIs.

# SECTION 5: NAFI IT CYBERSECURITY

## 5.1. GENERAL.

a. The purpose of the NAFI IT cybersecurity program is to ensure that IT is used in a way that gives mission owners and operators confidence in the confidentiality, integrity, non-repudiation, and availability of NAFI IT and NAFI information, is able to deflect an attack by implementation of best practices, and allows them to make choices based on that confidence. The NAFI IT cybersecurity program supports a vision of effective operations in cyberspace where:

(1) NAFI missions and operations are enabled to continue under any cyber situation or condition, after identifying, evaluating, and mitigating any associated cyber risks.

(2) NAFIs participate fully in IT and data optimization initiatives by consolidating inefficient infrastructure, optimizing existing facilities, and transitioning to more efficient infrastructure.

b. DoD NAFI IT should comply with the cybersecurity provisions outlined in DoDIs 8500.01, 8510.01, 8310.01, 8530.01, 8560.01, 8582.01, and 8910.01. DoDI 8530.01 requires DoD NAFI IT Enterprise Owners to report all incidents that appear to be violations of Federal law to DoD NAFI IT Enterprise Owners defense criminal investigative organizations; law enforcement organizations; and the Inspector General of the Department of Defense.

c. The NAF AOs will use the above cybersecurity provisions, including the DoD RMF, defined in DoDI 8510.01, as well as the security standards for NAFI IT systems, in accordance with Paragraph 5.2., to assess and authorize the usage of NAFI IT and ensure effective and continuous cybersecurity activities.

## 5.2. SECURITY STANDARDS FOR NAFI IT SYSTEMS.

### a. RMF Applicability.

(1) Risk management is the responsibility of each NAFI IT Enterprise Owner's NAF AO in collaboration with the NAFI IT Enterprise Owner's CIO or chief information security officer. Risk management consists of a risk analysis, risk assessment, risk mitigation, vulnerability assessment, and controls evaluation.

(2) Before the development, installation, or acquisition of IT, the relevant NAFI IT AODR will consult the IT security and architecture teams within their area of primary responsibility to establish the scope of security-related activities. The NAF AOs are responsible for approving security test plans and test results.

(3) The security test plan and results must demonstrate how the data will be protected from loss, misuse, unauthorized access, modifications, or undetected security-related activities.

(4) The RMF, set forth in DoDI 8510.01, drives the risk-based assessment and authorization process of NAFI IT.

(5) Once a NAFI IT Enterprise Owner designates a NAF AO in a formal capacity, and the AO is at full operational capability as determined by the NAFI BMAO, all NAF IT will be required to complete assessment and authorization successfully pursuant to DoDI 8510.01 to attain an ATO from the relevant NAF AO and will no longer use Component AOs at a level above the NAFI IT Enterprise Owner for IT approvals.

**b. Risk Assessment.**

(1) Risks are derived from the analysis of threats and vulnerabilities. A formal assessment by the NAFI Enterprise-level SCA requires determining relativity among risks and assessing associated damage or loss potentials. This relationship forms the basis for selecting effective safeguards. An SCA will be identified by the NAF IT Enterprise-level Owner and appointed by the NAF AO. The results of the risk assessment will be documented in a security assessment report.

(2) At the onset of the risk analysis process, the NAF AOs will establish the scope of the analysis and the recommended approach.

(3) The NAF AOs will ensure a risk analysis is conducted when a significant change occurs to an established NAF IS or PIT system, at least annually, and at periodic intervals established by the NAFI AO Office.

(4) The NAF AOs are responsible for determining the criteria for defining significant changes and will define these criteria commensurate to the sensitivity of the data being processed.

(5) Risk analysis will focus on the automated technical and administrative security control techniques associated specifically with the process under review. This includes the interface between the operating IT and the applications, or the communications environment and applications, and threats inherent to processing in a specific environment.

(6) A POA&M will be developed for the NAF AOs by relevant program managers or system managers and be maintained to address known vulnerabilities in the NAFI IS or PIT system(s).

**c. Security Controls.**

(1) Security controls are designed to create a set of defined security requirements (i.e., safeguards or countermeasures) that are identified and prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information, and are maintained by the NAF AOs to ensure sufficient protections are implemented in the most efficient and effective way for NAF IT.

(2) Standard configurations ensure that IT components are configured using industry best practices for security and establish a security configuration baseline to be applied to all similar

IT components in the NAFI enterprise. Additionally, Office of Management and Budget (OMB) Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47 provide guidelines for interconnecting IS.

(3) The applicable IS owner and cyber security team will identify the system specific controls for each IT during the initial discovery meeting. NAFI IT Enterprise Owners must specify which framework takes precedence, the Federal Information Security Management Act or PCI DSS for their internal operational procedures.

(4) All NAFI IT must incorporate standard configurations or have a documented exception approved by the relevant NAF AO.

(5) NAFI implementation of updates to security controls and assessment procedures for NAFI IT system categorization will be coordinated through the RMF Technical Advisory Group in accordance with DoDI 8510.01.

### d. Privacy Impact Assessment (PIA).

(1) The PIA process establishes a formal procedure for the determination of the protection requirements for IS and electronic collections of information of personally identifiable information (PII), or protected health information (PHI), and applies to all IS and electronic collections of information that collect, maintain, use, transmit, display, store, or process PII or PHI.

(2) NAFI IT may collect PII about Service members and their families, NAF employees, and business partners in accordance with NIST SP 800-53, Revision 5 and NIST SP 800-122. NAFI IT that collects, maintains, or disseminates PII must comply with privacy and information security related laws, regulations, and policies in accordance with DoDI 5400.11 and DoDI 5400.16. The NAF AOs must ensure the completion of PIAs on NAFI IT systems and may be required to submit the PIA to the NAFI IT Enterprise-level CIO in accordance with DoDI 5400.16 and DoD guidelines.

### e. Security Risk Assessment.

(1) All IT is required to successfully complete the security assessment and authorization process, as defined in DoDI 8510.01. Successful completion of the assessment and authorization process results in a risk decision from the NAFI AO and documented in an authorization decision (e.g., ATO, denial of ATO, interim authorization to test, ATO with conditions). When IT receives an ATO, the IT is placed into the continuous monitoring phase.

(2) Failure to receive an ATO requires the system operator to remediate security assessment findings until an ATO is received.

(3) IT in design or development may receive an interim authorization to test while under test but must receive an ATO or ATO with conditions before being placed into production.

### f. Information Security Continuous Monitoring.

All IT that has completed the security assessment and authorization process and has received an ATO begin the information security continuous monitoring process, pursuant to DoDI 8510.01.

### g. PCI DSS Compliance.

PCI security standards are technical and operational requirements set by the PCI Security Standards Council to protect cardholder data. The standards apply to all entities that store, process, or transmit cardholder data with guidance for software developers and manufacturers of applications and devices used in those transactions. NAFIs handling payment card data must maintain compliance with the PCI DSS and report compliance to their merchant banks and relevant NAFI IT Enterprise Owner-level offices as required.

## 5.3. FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP) COMPLIANCE.

a. In accordance with the DoD Cloud Computing Security Requirements Guide, DoD NAF IT mission partners (i.e., exchanges; MWR organizations; other NAFIs) that typically operate networks outside of the Defense Information Systems Network or .mil domain will need to implement boundary cloud access points (BCAPs) or internal cloud access points (ICAPs) when connecting cloud service provider (CSP) infrastructure to their networks.

b. Mission partner environment (MPE) network connectivity and access to off-premises commercial DoD Level 4/5 cloud service offerings (CSOs) will not traverse a Non-classified Internet Protocol Router Network (NIPRNet) BCAP or a NIPRNet Federated Gateway when connecting to or accessing modern process equipment applications instantiated in such a CSO.

c. NAFI IT can utilize commercial cloud access points (CAPs) and is not restricted to using a DoD CAP.

(1) NAFIs may use acceptable CAP-equivalents for protecting their networks from risks associated with the use of commercial clouds.

(2) The use of a cloud access security broker having minimally a FedRAMP moderate provisional authority may be one-such alternative.

(3) MPEs, such as NAFI IT, that utilize network(s) other than NIPRNet or Secret Internet Protocol Router Network (e.g., Defense Red Switch Network), will need to implement BCAPs or ICAPs for those network(s) that provide equivalent protections to those defined in the Secure Cloud Computing Architecture Functional Requirements Document.

d. The NAF AO has the authority to determine applicable cloud security compliance requirements for NAFI IT cloud-based solutions, such as FedRAMP, in alignment with the Cloud Computing Security Requirements Guide.

## 5.4. NAF PERSONNEL COMPLIANCE.

Every NAF personnel with privileged access to a DoD IS performing cybersecurity, regardless of job or occupation series, is required to carry an approved certification for their particular job classification, in accordance with DoD Directive 8140.01 and DoDI 5200.02.

## 5.5. DOD/CIO EXCEPTIONS TO POLICY.

DoDI 8010.01 requires all DoD IT to use the Department of Defense information network (DoDIN) for primary network transport and control and provides parameters for the use of commercial connections as alternatives to Defense Information Systems Network-provided transport. Exceptions to use a commercial internet service provider are made on a case-by-case basis through the DoD/CIO exceptions to policy process. Paragraph 4.4.i. of DoDI 8010.01 and Appendix A of the Defense Information Systems Agency Connection Process Guide consider DoD NAFIs that operate in accordance with DoDIs 1015.15 and 1015.10 and Volume 13 of DoD 7000.14-R to be non-DISN requirements that process, store, and transmit publically releasable DoD data. Therefore, the NAF AO will tailor appropriate security controls to ensure conformance with DoD cybersecurity requirements.

# GLOSSARY

## G.1. ACRONYMS.

| ACRONYM | MEANING |
|---|---|
| AO | authorizing official |
| AODR | authorizing official designated representative |
| ASD(M&RA) | Assistant Secretary of Defense for Manpower and Reserve Affairs |
| ATO | authorization to operate |
| BCAP | boundary cloud access point |
| BMA | business mission area |
| BMAO | business mission area owner |
| CAP | cloud access point |
| CIO | chief information officer |
| CSO | cloud service offering |
| CSP | cloud service provider |
| DoDI | DoD instruction |
| DoDIN | Department of Defense information network |
| FedRAMP | Federal Risk and Authorization Management Program |
| IS | information system(s) |
| IT | information technology |
| MPE | mission partner environment |
| MWR | morale, welfare, and recreation |
| NAF | nonappropriated funds |
| NAFI | nonappropriated funds instrumentalities |
| NIPRNet | Non-classified Internet Protocol Router Network |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PCI | Payment Card Industry |
| PCI DSS | Payment Card Industry Data Security Standard |
| PHI | protected health information |
| PIA | privacy impact assessment |
| PII | personally identifiable information |
| PIT | platform information technology |

| ACRONYM | MEANING |
|---|---|
| POA&M | plan of action and milestones |
| RMF | risk management framework |
| SCA | security control assessor |
| SP | special publication |

## G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

| TERM | DEFINITION |
|---|---|
| **AODR** | Defined in DoDI 8510.01. |
| **BCAP** | Defined in the DoD Secure Cloud Computing Architecture Functional Requirements Document. |
| **BMA** | Defined in DoDI 8115.02. |
| **BMAO** | The owner of a BMA, defined in DoDI 8115.02, responsible for ensuring compliance with consistent cybersecurity requirements and standards across their designated BMA. |
| **CAP** | Defined in DoDI 8010.01. |
| **continuous monitoring** | Defined in NIST SP 800-137. |
| **CSO** | Defined in DoDI 8010.01. |
| **CSP** | Defined in DoDI 8010.01. |
| **ICAP** | Defined in the DoD Secure Cloud Computing Architecture Functional Requirements Document. |
| **IS** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **IS owner** | Defined in DoDI 8510.01. |

| TERM | DEFINITION |
|---|---|
| **IT** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **IT product** | Defined in DoDI 8500.01. |
| **IT service** | Defined in DoDI 8500.01. |
| **knowledge service** | Defined in DoDI 8510.01. |
| **mission partners** | Defined in DoDI 8000.01. |
| **MPE** | Defined in DoDI 8110.01. |
| **NAFI AO** | Senior management official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to the organization. |
| **NAFI IT Enterprise** | Each Military Department organization that owns and controls NAF IT systems. |
| **PHI** | Defined in DoDI 6025.18. |
| **PIA** | Defined in OMB Memorandum M-03-22, OMB Circular No. A-130, and Committee on National Security Systems Instruction Number 4009. |
| **PIT** | Defined in DoDI 8500.01. |
| **POA&M** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **public-private ventures** | Defined in DoDI 1015.13. |
| **risk analysis** | Examination of information to identify the risk to an IS. |
| **risk assessment** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **risk mitigation** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **SCA** | Defined in NIST SP 800-137. |

| TERM | DEFINITION |
| --- | --- |
| **security controls** | Defined in Committee on National Security Systems Instruction Number 4009. |
| **test and evaluation** | Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system. |
| **vulnerability assessment** | Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. |

# REFERENCES

Code of Federal Regulations, Title 36, Part 1194

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

Defense Information Systems Network Connection Process Guide Version 5.1, May 2016

DoD 7000.14-R, Volume 13, "Department of Defense Financial Management Regulation (DoD FMR): Nonappropriated Funds Policy," current edition

DoD Cloud Computing Security Requirements Guide Version 1, Release 3, March 6, 2017

DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprises (DoD IE)," March 17, 2016, as amended.

DoD Directive 8140.01, "Cyberspace Workforce Management", October 5, 2020

DoD Instruction 1015.10, "Military Morale, Welfare, and Recreation (MWR) Programs," July 6, 2009, as amended

DoD Instruction 1015.11, "Lodging Policy," October 6, 2006, as amended

DoD Instruction 1015.13, "DoD Procedures for Implementing Public-Private Ventures (PPVs) for Morale, Welfare and Recreation (MWR), and Armed Services Exchange Category C Revenue-Generating Activities," March 11, 2004

DoD Instruction 1015.15, "Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources," October 31, 2007, as amended

DoD Instruction 1330.21, "Armed Services Exchange Regulations," July 14, 2005

DoD Instruction 4105.67, "Nonappropriated Fund (NAF) Procurement Policy and Procedure," February 26, 2014, as amended

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017, as amended

DoD Instruction 5000.82, "Acquisition of Information Technology," April 21, 2020

DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020

DoD Instruction 5015.02, "DoD Records Management Program", February 24, 2015, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)", March 21, 2014, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs", January 1, 2019, as amended

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019

DoD Instruction 8010.01, "Department of Defense Information Network (DoDIN) Transport," September 10, 2018

DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021

DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006

DoD Instruction 8310.01, "Information Technology Standards in the DoD," February 2, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring," August 22, 2018

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014, as amended

DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements Document (FRD), January 31, 2017

National Institute of Standards and Technology Special Publication 800-47, Revision 1, "Managing the Security of Information Exchanges," July 2021

National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020, as amended

National Institute of Standards and Technology Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010

National Institute of Standards and Technology Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," September 2011

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016

Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003

United States Code, Title 10

United States Code, Title 29, Section 794d (also known as "Section 508 of the Rehabilitation Act")

United States Code, Title 44, Chapter 35, Subchapter II (also known as the "Federal Information Security Modernization Act of 2014")