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:	March 18, 2022
Change 1 Effective:	August 1, 2024
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
Change 1 Approved by:	Ashish S. Vazirani, Performing the Duties of the Under Secretary of Defense for Personnel and Readiness

Purpose: In accordance with the authority in DoD Directive (DoDD) 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 nonappropriated funds (NAF) information technology (IT).
- Establishes the 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 exchanges; and DoD lodging programs (excluding public-private venture agreements for lodging), as discussed in DoDIs 1015.10, 1015.15, 1015.11, and 1330.21.

c. All NAF IT and information systems (IS), as described by DoDIs 8500.01 and 8510.01 and as specified in Section 3 of this issuance, that receive, process, store, display, or transmit NAF program information. These technologies are broadly grouped as NAF IS, NAF systems and technologies, NAF IT services, and NAF IT products. This includes NAF 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 NAF IT operated by a contractor or other entity on behalf of the NAFI. NAFI systems and technologies are used only for NAF purposes, dedicated to NAF processing, and effectively under NAF configuration control.

1.2. POLICY.

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

b. NAF system(s) and system component investments should link mission needs, information, and technology while efficiently managing resources and implementing cybersecurity requirements in accordance with DoDD 8115.01 and DoDI 8115.02. NAF system(s) and system component investments will be managed in portfolios and enterprise solutions will be reviewed and approved through the governance bodies identified in Paragraph 4.1. NAF IT acquisition processes and procedures will be in accordance with DoDI 5000.82, with exceptions identified in DoDI 4105.67.

c. Procurement of NAF 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.

f. NAF funds for NAF system(s) and system components are invested effectively to support activities and programs defined and described in DoDI 1015.15. NAF funds for NAF systems(s) and system components support activities and programs defined in DoDI 1015.15. NAFI use of NAFs are exempt from the requirements in DoDI 5330.03, at the NAFI's discretion.

g. NAF system(s) and system components governance processes will be established to ensure NAF IT-funded portfolios are reviewed continuously and approved to leverage existing mission support systems deployed by the DoD and NAFIs across the DoD. NAF IT governance will be managed in accordance with DoDI 8115.02 and Section 4 of this issuance.

h. NAF system(s) and system components may be part of the Joint Information Environment (JIE) as the current architecture is written and may be part of similar Component/Service constructs.

(1) Where possible and where it is not a burden to the NAFI, NAF system(s) and system components will work at JIE (or Component/Service equivalent constructs) compatibility or find areas of integration, especially where mission sets may require it.

(2) Where mission sets require JIE (or Service equivalent constructs) compatibility and integration, that requirement is determined and agreed to by the relevant NAFI authority and the supported commander at that echelon.

1.3. SUMMARY OF CHANGE 1.

The changes to this issuance:

a. Add, revise, or remove some terms and phrases to better explain and define what NAF system(s) and system components are and what NAF system(s) and system components are not.

b. Revise and update procedures to reflect the current state of NAF system(s) and system components.

c. Add policy statements to help stakeholders understand NAF system(s) and system components and help NAF IT professionals accomplish their mission.

d. Update references and acronyms for accuracy.

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 NAF system(s) and system components 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.

d. In coordination with the DoD Chief Information Officer (CIO) and the DoD Components, assigns responsibility for NAFI enterprise systems, to be included in the portfolio of the DoD Component responsible for authorizing the NAFI enterprise.

2.2. DOD COMPONENT HEADS.

The DoD Component heads:

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

b. Ensure that each NAF system(s) and system components system is assigned to a trained and qualified authorizing official (AO) designated in writing for all NAF systems and technologies, in accordance with DoDIs 8500.01 and 8510.01. The NAF AO should be nominated by the Component commander or equivalent civilian responsible for the NAFI activities and should be aware of any special requirements for the NAFI systems assigned. AOs should be appointed from leadership positions within each business owner and mission owner organization to promote accountability in authorization decisions that balance mission and business needs and security concerns.

c. Establish NAF system(s) and system components management oversight and internal control systems and encourage reciprocity with other NAFIs, in accordance with DoDI 8510.01.

d. Develop and implement NAFI system(s) and system components Enterprise-level NAFI system(s) and system components acquisition, tracking, integration, oversight, governance, and control policies and procedures that:

(1) Are in accordance with this issuance.

(2) Do not violate NAFI system(s) and system components acquisition policy or acquisitions authorities by removing system(s) and system components acquisitions authorization from the NAFIs or NAF head contracting authority.

(3) Deconflict Component system(s) and system components policy (e.g., those written to meet Department of Defense Information Network and Defense Information System Network (DISN) or JIE requirements, or to meet appropriated fund goals or requirements), without the affected NAFIs' express approval.

(4) Do not place undue financial burden on NAFIs to comply with system(s) and system components policies that NAFIs deem not required.

(5) Encourage shared responsibility and reporting models. Include memorandums of understanding to document NAFI differences in system(s) and system components compliance.

e. Create Component system(s) and system components governance to support and ensure participation in the enterprise governance program and other actions established by the NAF IT Working Group.

f. Ensure NAF system(s) and system components are authorized in accordance with DoDI 8510.01.

g. Conduct business impact analysis that measures financial and operational risk before the implementation of any new or amended requirement provision to ensure such provisions requirement does do not result in a negative impact to the Military Resale NAFI's ability to perform its mission.

h. Ensure NAF system(s) and system components are included in the portfolio of the DoD Component responsible for the NAFI enterprise. The Component commander or equivalent civilian responsible for NAFI activities should nominate a portfolio manager.

SECTION 3: NAF IT

3.1. GENERAL.

a. NAF IT includes all system(s) and system components that are:

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

(2) Acquired to support or manage a NAFI mission.

b. NAF IT does not include any system(s) and system components that are managed or used by public-private venture agreements that:

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

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

3.2. NAF IT FUNCTIONS.

NAF system(s) and system components consist 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. NAF system(s) and system components may have the following attributes:

a. Documented as part of a NAF system(s) and system components with connections to external commercial entities to conduct real-time business transactions.

b. Subject to physical and virtual inspections by outside commercial auditors to ensure compliance with accounting principles and other industry standards where contracted agreements require validation (e.g., the annual industry (PCI) payment card data security standard assessment process).

c. Operation on a non-.mil domain when appropriate registration and waiver are obtained in accordance with DoDI 8410.01.

d. Operation of DoD physical infrastructure or virtual isolated shared infrastructure when connected systems are covered by an authorization to operate (ATO) and have documented approval from the AO responsible for the infrastructure.

e. Business functions and supporting services unique to NAFIs requiring solutions solely for use in commercial operations, which may use different security approaches in achieving compliance. These solutions may require specialized configurations unique to NAF IT.

3.3. NAF IT CATEGORIZATION.

a. Systems used exclusively by DoD NAFIs are not categorized as defense business systems for the purpose of compliance with Section 2222 of Title 10, U.S.C. and as defined in DoDI 5000.75. A defense 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. To efficiently manage the DoD NAF system(s) and system components portfolio, NAF business systems and system components are aligned for tracking, architecture, portfolio management using the categorizations identified in Section 2222(i) of Title 10, U.S.C. and further outlined by the NAF IT Working Group to manage efficiently and effectively NAFI resources to reduce redundancy and system(s) and system components management expenses. This issuance establishes the NAFI systems sub domain.

SECTION 4: NAF IT GOVERNANCE

4.1. GENERAL.

NAF system(s) and system components 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 NAF system(s) and system components will ensure all relevant parties are aware and informed participants in the maintenance and strategic development of NAF system(s) and system components cybersecurity.

4.2. NAF IT BMAO.

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

a. Oversee and coordinate with the Components regarding the annual assessment and inventory listing of systems and applications owned and operated across the NAF IT Portfolio for the purpose of collaboration and process improvement between the NAFI IT Enterprise Owners. The annual NAF IT portfolio assessment and inventory listing will be completed by the NAF IT Working Group by July 1 of each calendar year. NAF IT portfolio data includes but is not limited to: systems comprised of moveable equipment, commercial off-the-shelf software, licenses, and other related hardware and software components.

b. Oversee the cybersecurity risk management of NAF system(s) and system components and distribute RMF information standards and sharing requirements.

c. Chair the NAF IT Working Group.

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

e. Coordinate with the RMF Knowledge Service to host NAF system(s) and system components content as appropriate.

4.3. NAF AO.

Each NAF IT Enterprise-level Owner must have a NAF AO assigned to the NAFI. 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 systems and technologies under their 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., 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. In accordance with the NAFI's mission, identify, evaluate, and determine the correct tools and systems to manage NAF system(s) and system components.

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 systems and technologies.

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

(3) Promote reciprocity with other NAFIs, in accordance with DoDI 8510.01, to the maximum extent possible.

(4) Do not delegate full authorization decisions (e.g., ATOs) below the AO level. Other AO responsibilities and tasks may be delegated to a formally appointed and qualified AO designated representative (AODR) within the AO's NAFI IT Enterprise.

(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 Component CIO or the senior information security office for reporting requirements described in Subchapter II of Chapter 35 of Title 44, U.S.C. (also known and referred to in this issuance as the "Federal Information Security Modernization Act of 2014") and determine if any NAF IT systems are reported to the Component CIO for Federal Information Security Modernization Act of 2014 reporting.

(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. 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.

j. Ensure compliance with Section 794d of Title 29, U.S.C., 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 NAFI IT Enterprise Owner's information officers, senior information security officers, and other stakeholders as applicable to the topics discussed.

b. Is chaired by the NAF IT BMAO.

c. 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.

d. 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.

e. 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.

f. Defines roles~~,~~ and responsibilities within the NAF IT BMA.

g. Advises the NAF AOs periodically regarding relevant topics (e.g., the prioritization of ATO decisions based on business or operational inputs and other needs expressed by the NAFIs).

SECTION 5: NAF IT CYBERSECURITY

5.1. GENERAL.

a. The purpose of the NAF system(s) and system components cybersecurity program is to ensure that system(s) and system components are 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 NAF~~I~~ 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 system(s) and system components and data optimization initiatives by consolidating inefficient infrastructure, optimizing existing facilities, and transitioning to more efficient infrastructure.

b. DoD NAF system(s) and system components should comply with the cybersecurity provisions outlined in DoDIs 8500.01, 8510.01, 8310.01, 8530.01, 8560.01, 8582.01, and 8910.01 and DoDD 5205.16. 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, the insider threat program, and the Inspector General of the Department of Defense.

c. The NAF AOs will use the cybersecurity provisions in this paragraph, including the DoD RMF, defined in DoDI 8510.01, as well as the security standards for NAF IT systems, in accordance with Paragraph 5.2., to assess and authorize the usage of NAF 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 information officers or senior information security officer. Risk management consists of a risk analysis, risk assessment, risk mitigation, vulnerability assessment, and controls evaluation. If the NAF IT Enterprise utilizes the Department of Defense Information Network, the DoD vulnerability management process will be used, in accordance with DoDI 8531.01.

(2) Before the development, installation, or acquisition of system(s) and system components, the relevant NAFI IT AODR will consult the system(s) and system components 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 NAF IT.

(5) Once a NAFI IT Enterprise Owner designates a NAF AO in a formal capacity, and the AO is at full operational capability NAFI, all NAF system(s) and system components 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 system(s) and system components 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 system or technology, at least annually, and at periodic intervals established by the NAF 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 system(s) and system components and the applications, or the communications environment and applications, and the 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 NAF system(s) and technologies.

c. Security Controls.

(1) Security controls are designed to create a set of defined security requirements (e.g., 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 system(s) and system components.

(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 Circular A-130 and National Institute of Standards and Technology Special Publication (NIST SP) 800-47 provide guidelines for interconnecting IS.

(3) The applicable IS owner and cybersecurity team will identify the system specific controls for each IT during the initial discovery meeting.

(4) All NAF system(s) and system components 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) In accordance with OMB Circular No. A-130 and OMB Memorandum M-03-22, a PIA is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis. NAF activities implement the formal procedures established in DoDI 5400.16 for the completion and approval of PIAs to ensure personally identifiable information (PII) in electronic form is managed in a manner that protects privacy.

(2) NAFIs may collect PII about Service members and their families, NAF employees, and business partners and maintain such PII on NAF IT in accordance with applicable law, regulation, and policy. NAFIs that collect, maintain, use, or disseminate PII must comply with privacy, information security, and information-collection related laws, regulations, and policies as applicable, including but not limited to Section 552a of Title 5, U.S.C. (also known as the "Privacy Act of 1974", as amended); Section 208 of Public Law 107–347 (also known as the "E-Government Act of 2002"); Subchapter I of Chapter 35 of Title 44, U.S.C. (also known as the "Paperwork Reduction Act"); the Federal Information Security Modernization Act of 2014; DoDIs 5400.11, 5400.16, and 8910.01; Volume 2 of DoD Manual 8910.01; and applicable Committee on National Security Systems policies (e.g., Committee on National Security Systems Instruction 1253 and DoD CIO's privacy overlay). The NAF AOs must ensure the completion of PIAs on NAF system(s) and system components and may be required to submit the PIA to the NAFI IT Enterprise-level information officer in accordance with DoDI 5400.16 and DoD guidelines.

e. Security Risk Assessment.

(1) NAF IT must 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 documented in an authorization decision (e.g., ATO, denial of ATO, interim authorization to test, ATO with conditions). When system(s) and system components receive an ATO, the system(s) and system components are 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) System(s) and system components 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.

NAF IT that has completed the security assessment and authorization process and has received an ATO begins 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.

h. Key Security Principles.

NAF system(s) and system components and NAF information should use key security principles to allow NAF mission owners and operators to have confidence in the confidentiality, integrity, and availability of NAF IT and NAF information to make decisions. All NAFIs must implement cyber operations to protect NAF system(s) and system components. NAFIs must employ activities to support operations in response to vulnerabilities and threats, including vulnerability assessment and analysis, vulnerability management, malware protection, incident response, continuous monitoring, warning intelligence, and attack sensing and warning. Cyber operation compliance may be met:

(1) With internal resources certified as a cyber security service provider; or

(2) Through contracted service from a DoD-certified cyber security service provider.

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 (e.g., exchanges, MWR organizations, other NAFIs) that typically operate networks outside of the Defense Information Systems Network or .mil domain will need to implement NAF system(s) and system components AO-approved boundary cloud access points (BCAPs) or internal cloud access points (ICAPs) when connecting cloud service provider infrastructure to their networks.

b. Mission partner environment (MPE) network connectivity and access to off-premises commercial DoD Level 4 or 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. NAF system(s) and system components 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 NAF system(s) and system components, 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 DoD Secure Cloud Computing Architecture Functional Requirements Document.

d. The NAF AO has the authority to determine applicable cloud security compliance requirements for NAF system(s) and system components cloud-based solutions, such as FedRAMP, in alignment with the Cloud Computing Security Requirements Guide.

e. NAF system(s) and system components may utilize non-standard cloud security service providers (CSSPs) where:

(1) The cloud service is not part of the DISN.

(2) Relevant NAF system(s) and system components services cannot meet some or all CSSP requirements.

(3) Neither DISA nor the Component CSSP can meet all the CSSP requirements.

(4) The CSSP activities can be assessed by the AO as an MPE.

5.4. NAF CYBER SECURITY WORKFORCE.

All NAF personnel with privileged access to a DoD IS performing cybersecurity, regardless of job or occupation series, must carry an approved certification for their particular job classification, in accordance with DoDD 8140.01 and DoDIs 8500.01 and 5200.02.

5.5. DOD CIO EXCEPTIONS TO POLICY.

Exceptions to use a commercial internet service provider are made on a case-by-case basis through the DoD CIO exceptions to policy process. In addition, in accordance with Paragraph 4.4.i. of DoDI 8010.01 the NAF AO will tailor appropriate security controls to ensure conformance with DoD cybersecurity requirements for non-DISN requirements operated by DoD NAFIs that process, store, and transmit publicly releasable DoD data through systems intended for personal, private, non-mission use (e.g., free WiFi). 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
CSSP	cloud security service provider
DISN	Defense Information System Network
DoDD	DoD directive
DoDI	DoD instruction
FedRAMP	Federal Risk and Authorization Management Program
ICAP	internal cloud access point
IS	information system(s)
IT	information technology
JIE	Joint Information Environment
MPE	mission partner environment
MWR	morale, welfare, and recreation
NAF	nonappropriated funds
NAFI	nonappropriated funds instrumentality
NIPRNet	Non-classified Internet Protocol Router Network
NIST SP	National Institute of Standards and Technology special publication
OMB	Office of Management and Budget
PCI	payment card industry
PCI DSS	Payment Card Industry Data Security Standard
PIA	privacy impact assessment
PII	personally identifiable information

ACRONYM	MEANING
POA&M	plan of action and milestones
RMF	risk management framework
SCA	security control assessor
U.S.C.	United States Code

G.2. DEFINITIONS.

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

TERM	DEFINITION
AODR	An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization.
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.
cloud service provider	Defined in DoDI 8010.01.
continuous monitoring	Defined in NIST SP 800-137.
CSO	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 NIST SP 800-37.

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 at https://rmfks.osd.mil/.
mission partners	Defined in DoDD 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.
NAF IT	Information technology, system(s) and system component associated with nonappropriated instrumentalities.
NAFI IT Enterprise Owner	Each NAFI organization with each Military Department that owns and controls NAF IT systems (e.g., Army IMCOM G9, CNIC, NEXCOM, AAFES).
PIA	Defined in OMB Memorandum M-03-22 and OMB Circular No. A-130.
POA&M	Defined in Committee on National Security Systems Instruction Number 4009.
public-private venture agreements	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.

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. 1253, "Security Categorization and Control Selections for National Security Systems," March 27, 2014

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," March 7, 2022

Defense Information Systems Network Connection Process Guide Version, current version

DoD Cloud Computing Security Requirements Guide Version 1, Release 4, January 14, 2022

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

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

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

DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005

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," January 23, 2023

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, "Requirements for the Acquisition of Digital Capabilities," June 1, 2023

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 5330.03, "Single Manager of DoD Document Services," May 7, 2021

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 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," April 7, 2023

DoD Instruction 8410.01, "Internet Domain Name and Internet Protocol Address Space Use and Approval," December 4, 2015, as amended

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

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

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

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020

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, "DoD Implementation of the Paperwork Reduction Act," December 5, 2022

DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections," June 30, 2014, as amended

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

National Institute of Standards and Technology Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 20, 2018

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 800-137, "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

Public Law 107–347, Section 208, "E-Government Act of 2002," December 17, 2002

United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974")

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