

Army Regulation 10–82

Organization and Functions

ARMY NATIONAL GUARD INFORMATION TECHNOLOGY

**Headquarters
Department of the Army
Washington, DC
18 June 2018**

UNCLASSIFIED

SUMMARY of CHANGE

AR 10–82

Army National Guard Information Technology

This major revision, dated 18 June 2018—

- o Changes the title from “Army National Guard Computer Center” to “Army National Guard Information Technology” (cover).
- o Articulates the information management and technology mission and responsibilities in delivering information technology to the Army National Guard (paras 4 and 5).
- o Defines mission and functions and prescribes command and staff relationships and communication channels of the Army National Guard Chief Information Officer/G–6 (paras 5, 6, and 7).

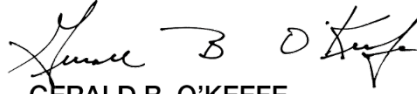
Effective 18 July 2018

Organization and Functions
ARMY NATIONAL GUARD INFORMATION TECHNOLOGY

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:


GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation defines the mission and supporting functions of information technology services within the Army National Guard.

Applicability. This regulation applies to the Army National Guard. It does not apply to the Regular Army or the U.S. Army Reserve.

Proponent and exception authority.

The proponent of this regulation is the Chief, National Guard Bureau. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Army National Guard G–6, Arlington Hall Station, 111 South George Mason Drive, Arlington, VA 22204.

Suggested improvements. Users are invited to send comments or suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Army National Guard G–6, Arlington Hall Station, 111 South George Mason Drive, Arlington, VA 22204.

Distribution. This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Purpose • 1, *page 1*
References • 2, *page 1*
Explanation of abbreviations and terms • 3, *page 1*
Responsibilities • 4, *page 1*
Mission • 5, *page 1*
Functions • 6, *page 1*
Channels of communication • 7, *page 3*

Appendixes

A. References, *page 4*
B. Internal Control Evaluation, *page 6*

Glossary

*This regulation supersedes AR 10–82, dated 21 January 1981.

1. Purpose

This regulation sets forth the mission and functions of the Army National Guard (ARNG) Chief Information Officer/G-6 (CIO/G-6) in managing and delivering information as an ARNG resource and the information technology (IT) that supports the information requirements. It also describes command and staff relationships and channels of communication.

2. References

See appendix A.

3. Explanation of abbreviations and terms

See the glossary.

4. Responsibilities

In accordance with DODD 5105.77, the Chief, National Guard Bureau (CNGB) is responsible for the organization and operations of the National Guard Bureau (NGB). Accordingly, the Director, Army National Guard (DARNG) assists the CNGB in carrying out the functions of the NGB as they relate to the ARNG and the Army National Guard of the United States. The CNGB, as the channel of communications between the Department of the Army (DA) and the 50 States, three Territories (Guam, Puerto Rico, and the U.S. Virgin Islands), and the District of Columbia, appoints the DARNG as the lead agent for GuardNet. As lead agent for GuardNet, the DARNG delegates the management and sustainment of information management (IM) and technology to the ARNG CIO/G-6.

5. Mission

The mission of the ARNG CIO/G-6 is as follows:

- a. Provide Federal and ARNG State-level command, control, communications, computers, and information management (C4IM) to meet the dual State and Federal mission of the ARNG.
- b. Manage information and information technology for the NGB and the 50 States, three Territories (Guam, Puerto Rico, and the U.S. Virgin Islands) and the District of Columbia.

6. Functions

- a. *Information resource management.*
 - (1) Oversees the implementation of IM and IT capital planning and investment-control strategies, as well as, resource planning, programming, budgeting, and execution.
 - (2) Participates in, and provides representation for, the planning, programming, budgeting, and execution process decision group and exercises centralized oversight of IT expenditures for all appropriations.
 - (a) Leverages command, control, communications, computers (C4) metrics to substantiate funding requirements that are essential to meet the dual State and Federal mission.
 - (b) Provides program objective memorandum oversight to the IT Management Decision Package (MDEP).
 - (3) Oversees functional processes within respective functional portfolio areas to maximize end-to-end enterprise processes and reduce redundancy in systems and local processes.
 - (4) Manages the organization's implementation of the ARNG's IT investment strategy, IT infrastructure changes, acquisition strategy, cybersecurity prerequisites, and information assurance (IA).
 - (5) Generates the Congressionally mandated ARNG Office of Management and Budget (OMB) Report.
- b. *Information technology strategy, policy, and governance.*
 - (1) Utilizes legal, fiduciary, and statutory authorities to achieve short- and long-term tactical, operational, and strategic objectives.
 - (2) Recommends and coordinates new standards and ensures IT system compliance to the approved Department of Defense (DOD) IT Standards Registry.
 - (3) Manages IM and IT requirements for the ARNG enterprise and participates in related governance and advisory board activities.
 - (4) Administers enterprise governance through policy, indoctrination, and execution portfolio management.
 - (5) Maintains compliance and provides strategic oversight in C4IM policy.
 - (6) Mission command governance—
 - (a) Provides broad guidance to the ARNG Mission Command Assessment Team while coordinating their activities and reporting results.

(b) Deconflicts all schedules impacting tactical signal echelons at all levels and facilitates risk and impact identification to Signal Soldiers.

(c) Coordinates with, and disseminates information to, multiple echelons within the ARNG tactical signal community, the NGB, Headquarters, Department of the Army (HQDA), and other DOD agencies to facilitate modernization in support of State and Federal missions.

(d) Aligns with the ARNG General Staff and Joint Staff to represent the tactical signal community in process, procedural, training, and equipping forums to ensure sustainable readiness across the tactical signal formations.

c. Information technology architecture.

(1) Oversees system architecture design and IT resources that impact the ARNG enterprise/State network and enabling technologies.

(2) Incorporates doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) standards to ensure information policy and functional requirements are reflected in architectures and plans across the ARNG enterprise, as a means to ensure information sharing, visibility, assurance, and interoperability.

(3) Develops the enterprise C4 and IT architecture in conjunction with C4IM requirements using existing acquisition strategy and procedures.

(4) Enhances ARNG enterprise capabilities that enables support to ARNG Federal and State-level missions.

(5) Manages plans and develops standard operating procedures for the ARNG enterprise architecture.

(6) Identifies, collects, analyzes, maintains, and monitors data elements used in approved information systems, in accordance with DA Data Strategy.

(7) Performs as a central design activity for analysis, design, integration, programing, documentation, testing, installing, maintaining, and modification of assigned information systems in response to ARNG functional requirements.

(8) Develops information systems specifications for acquisition of IT resources.

(9) Provides resource impact assessments and cost estimates for proposed functional changes.

(10) Deploys approved technical and functional software changes.

(11) Maintains and distributes information systems software and related operating procedures and instructions, concurrently, with distribution of functional user manuals to ARNG system users and support personnel.

(12) Provides technical assistance and orientation of new information systems and applications to the 50 States, three Territories, and the District of Columbia.

d. Cybersecurity.

(1) Provides oversight and sustainment of the ARNG Cybersecurity mission.

(2) Directs ARNG-wide cybersecurity policy, mandates procedures for policy compliance/enforcement, performs real time cyber threat detection, and ensures ARNG communications are conducted in a manner that ensures confidentiality, integrity, and availability while mitigating potential risk.

(3) Supports DOD's vision of effective operations in cyberspace where DOD missions and operations continue under any cyber situation or condition and where the DOD has ready access to its information and command and control channels and its adversaries do not, while securely and seamlessly extending to mission partners.

(4) Prescribes the operational aspects of information protection and data security, including processes that enforce ARNG-wide compliance with the Federal Information Security Management Act of 2002 (FISMA of 2002) and the OMB Circular A-130.

(5) Identifies and analyzes threats to the ARNG enterprise network and its enabling technologies.

(6) Measures ARNG compliance with cybersecurity requirements and prescribes an IA program operational execution activities, processes, and practices per AR 25-1.

(7) Oversees the management of records of respective functional areas to appropriately secure, maintain, and preserve them throughout their life cycle in accordance with AR 25-2, AR 25-400-2, and DA Pam 25-1-2.

e. Enterprise operations.

(1) Provides resources (people, process, technology, projects, and infrastructure) and end-to-end management for service delivery, service operations, infrastructure management, IA, and network defense.

(2) Oversees the development of DOD compliant and secure IT capabilities and services across the ARNG IT enterprise.

(3) Maintains timely responses to changing operational requirements for ARNG, Joint, and State-level missions.

(4) Minimizes the introduction of vulnerabilities and system interoperability performance problems by controlling and approving changes to the ARNG's authorized IT baseline.

(5) Governs the implementation of structured, controlled, repeatable, and measurable processes that drive accountability and compliance for the management of the ARNG's IT enterprise.

(6) Provides ARNG enterprise network services and capabilities, including enterprise architecture, cloud services, network connectivity, and computer network defense.

- (7) Establishes standards for the operation of the ARNG data processing installations.
- (8) Coordinates IT requirements relevant to ARNG continuity of operations plans and systems that support survival, recovery, and reconstitution and ensures essential information services are available and operational, in support of the ARNG continuity of operations (COOP).

7. Channels of communication

The ARNG CIO/G-6—

- a.* Communicates directly with HQDA agencies, the State Adjutants General, U.S. Property and Fiscal Officers, ARNG, and other Government agencies on matters of mutual interest.
- b.* Maintains liaison with other DOD and Government agencies in matters of mutual interest.
- c.* Collaborates with the Joint Force Headquarters-States Directors of Information Management, who are responsible for network enterprise center-like responsibilities for their respective States, as outlined in DODD 8000.01.

Appendix A

References

Section I

Required Publications

This section contains no entries.

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read the publication to understand this regulation.

AR 11–2

Managers' Internal Control Program

AR 25–1

Army Information Technology

AR 25–2

Information Assurance

AR 25–30

Army Publishing Program

AR 25–400–2

The Army Records Information Management System (ARIMS)

Clinger–Cohen Act of 1996

40 USC, Subtitle III

DA Pam 25–1–1

Army Information Technology Implementation Instructions

DA Pam 25–1–2

Information Technology Contingency Planning

DA Pam 25–403

Guide to Recordkeeping in the Army

DODD 5105.77

National Guard Bureau (NGB)

DODD 5144.02

DOD Chief Information Officer

DODD 8000.01

Management of the Department of Defense Information Enterprise (DOD IE)

DODD 8500.01

CyberSecurity

DODI 8510.01

Risk Management Framework (RMF) for DOD Information Technology (IT)

DODI 8530.01

Cybersecurity Activities Support to DOD Information Network Operations

FISMA of 2002

Federal Information Security Management Act of 2002

OMB Circular A–130

Management of Federal Information Resources

10 USC 10541

National Guard and reserve component equipment: annual report to Congress

Section III**Prescribed Forms**

This section contains no entries.

Section IV**Referenced Forms**

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (<https://armypubs.army.mil>).

DA Form 11–2

Internal Control Evaluation Certification

DA Form 2028

Recommended Changes to Publications and Blank Forms

Appendix B

Internal Control Evaluation

B–1. Function

The function covered by this evaluation is the administration of the ARNG IT organization. This includes key controls for Chief Information Officer management, IA, and C4/IT support and services.

B–2. Purpose

The purpose of this evaluation is to assist the ARNG CIO/G–6 in the configuration and control of GuardNet and GuardNet Services. It is intended as a guide and does not cover all controls.

B–3. Instructions

Answers must be based on the actual testing of internal controls (such as document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least once every three years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Evaluation

a. Responsibilities. Have C4/IT plans, programs, and requirements been coordinated with the appropriate IM and IT managers?

b. Army information technology management.

(1) Are the duties and responsibilities of the senior information management official clearly designated in the organization's mission and function?

(2) Has the organization analyzed (and documented the analysis of) its mission and revised mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes?

(3) Does the organization have a strategic plan that is linked to its mission? Is it periodically updated?

(4) Has a forum been established to develop and implement C4/IT procedures, requirements, and priorities?

(5) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration?

(6) Does the IT investment screening process include addressing the questions in this checklist, resolving all issues prior to making an IT investment, and initiating any process analysis or improvement?

(7) Does the process support core or priority mission functions?

(8) Can the process be eliminated?

(9) Can the process be accomplished more effectively, efficiently, and at less cost by another Government source (for example, DOD or other Federal agency) or the private sector?

(10) Does the IT investment process clearly establish who in the organization has the responsibility and authority for making final IT-related investment decisions?

(11) Are exceptions to the IT investment screening process clearly documented?

(12) Does the organization require that management evaluations for the IT investment screening process, as well as scoring, ranking, and prioritization results, be documented (either manually or through the use of automated applications such as a decision support tool)?

(13) Are IT investment decisions a part of the organization's integrated capital planning process or are IT projects separated out?

(14) Does the organization have a process in place to conduct periodic reviews (in-house or via outside consultant or expert) of its current IT investment portfolio to assess alignment with mission needs, priorities, strategic direction, or major process reengineering?

(15) Does the organization have a process for documenting and disseminating results of this review?

(16) Have functional managers developed a set of goals and objectives (with performance measures) to gauge overall functional mission improvement? Have accomplishments been reported to enterprise-level managers?

(17) Have performance measures been developed for each IT investment that supports the organizational mission before execution of that investment?

(18) Have IT investments been synchronized to overall DOD and ARNG mission priorities?

(19) Are performance measures linked to management-level goals, objectives, and measures?

(20) Are financial, logistics, facilities, human resources, contractors, and other senior ARNG leaders held accountable for ensuring business processes comply with financial audit standards?

(21) Does the policy minimize the number of IT devices per employee and provide the least amount required for the assigned mission?

c. Information assurance (see AR 25–2).

d. Information Technology architecture (see para 5c).

(1) Has the organization developed the appropriate architecture for the ARNG to support the DOTMLPF–P components as mapped to net-centric data and services?

(2) Has the organization developed the appropriate architecture for the Army Business Enterprise Architecture (BEA) to support current systems infrastructure, enterprise application integration, and business-process modernization; and align with the following DOD BEA Core Business Missions: materiel supply and service management, real property and installations life cycle, human resources management, and financial management?

e. Installation information technology services and support.

(1) Is a process in place for acquiring IT and ensuring all required licensing and registration are accomplished?

(2) Are periodic reviews of current IT being conducted to ensure they are still required and meeting user needs?

(3) Are evaluations being conducted of existing systems for obsolescence?

(4) Is an accurate inventory being maintained and validated annually for IT equipment?

(5) Are COOP plans and procedures documented, distributed, and tested at least annually?

(6) Has guidance been provided to ensure all software is checked for viruses before being loaded?

(7) Are existing capabilities and assets considered prior to upgrading, improving, or implementing local area networks?

(8) Are uneconomical IT service contracts identified and terminated?

(9) Have the acquisition of licenses been coordinated with the Computer Hardware, Enterprise Software Solutions office prior to entering into an agreement with a commercial off-the-shelf vendor?

(10) Are spare capacity and functional expansion of IT being considered or used when new requirements are identified?

(11) Are measures being taken to ensure that hard drives are disposed of properly?

(12) Are criteria established for justifying and approving the acquisition of cellular phones?

(13) Has guidance been provided to review and revalidate cellular telephones every 2 years?

(14) Do procedures require the establishment of a reutilization program to identify and turn in cellular phones that are no longer required or seldom used?

(15) Is there a requirement for cellular phones to be recorded in the property book?

(16) Have accountable billing procedures been implemented?

(17) Have maintenance and support strategies been devised to minimize overall systems life cycle cost at an acceptable level of risk?

(18) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws?

(19) Are private sector service providers made aware that written assurance of compliance with software copyright laws may be required?

(20) Are users of the ARNG publicly accessible Web site provided with privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service?

(21) If applicable, does the Web site contain a disclaimer notice for links to any site outside of the official DOD Web information service (usually the .mil domain)?

(22) Is the Web site free of commercial sponsorship and advertising?

(23) Is the Web site free of persistent cookies or other devices designed to collect personal identifiable information about Web visitors?

(24) Is the operational information identified below purged from the ARNG publicly accessible Web site?

(a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

(c) Personal information about U.S. citizens, DOD employees, and military personnel, to include the following: Social Security numbers; dates of birth; home addresses; directories containing name, duty assignment, and home telephone numbers; names; locations; or any other identifying information about Family members of DOD employees or military personnel.

(d) Technological data such as weapon schematics, weapon system vulnerabilities, electronic wire diagrams, and frequency spectrum data.

(25) Are operational security tip-off indicators in the following categories purged from the ARNG publicly accessible Web site?

(a) *Administrative.* Personnel travel (personal and official business), attendance at planning conferences, commercial, support contracts, and for official use only information.

(b) *Operations, plans, and training.* Operational orders and plans; mission-specific training; exercise and simulations activity; exercise, deployment, or training schedules; unit relocation or deployment information; inspection results, findings, and deficiencies; unit vulnerabilities or weaknesses.

(c) *Communications.* Spectrum emissions and associated documentation; changes in activity or communications patterns. Use of Internet and email by unit personnel (personal or official business); availability of secure communications; hypertext links with other agencies or units; and Family support plans, bulletin board postings, or messages between Soldiers and their Family members.

(d) *Logistics and maintenance.* Supply and equipment orders and deliveries; transportation plans; mapping; imagery and special documentation support; maintenance and logistics requirements; and receipt or installation of special equipment.

(26) Are existing infrastructure capabilities and assets considered prior to upgrading, improving, or modernizing?

(27) Are the Web servers IA vulnerability alerts-compliant and placed behind a reverse proxy server?

B-5. Supersession

This is the initial internal control evaluation for AR 10-82.

B-6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to ARNG G-6, Arlington Hall Station, 111 S. George Mason Drive, Arlington, VA 22204.

Glossary

Section I

Abbreviations

AR

Army regulation

ARNG

Army National Guard

BEA

Business Enterprise Architecture

C4

command, control, communications, computers

C4IM

command, control, communications, computers and information management

CIO/G-6

Chief Information Officer/G-6

CNGB

Chief, National Guard Bureau

COOP

continuity of operations

DA

Department of the Army

DARNG

Director, Army National Guard

DOD

Department of Defense

DOTMLPF-P

doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy

HQDA

Headquarters, Department of the Army

IA

information assurance

IM

information management

IT

information technology

MDEP

Management Decision Package

NGB

National Guard Bureau

OMB

Office of Management and Budget

USC

United States Code

Section II

Terms

Cloud services

Cloud services are services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.

Cybersecurity

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

DOTMLPF-P

An analysis framework used by DOD in a problem solving construct for assessing current and future force capabilities while managing change.

Information assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information management

Planning, budgeting, manipulating, and controlling information throughout its life cycle.

Information system

An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.

Information technology

- a. Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- b. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources (see 40 USC Subtitle III (Clinger-Cohen Act of 1996)).

Information technology architecture

Is the process of development of methodical information technology specifications, models, and guidelines, using a variety of Information Technology notations within a coherent Information Technology architecture framework, following formal and informal Information Technology solution, enterprise, and infrastructure architecture processes.

Infrastructure

The shared computers, ancillary equipment, software, firmware, and similar procedures; and services, people, business processes, facilities (such as building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format (including audio, video, imagery, or data) whether supporting IT or national security systems as defined in the Clinger-Cohen Act of 1996.

MDEP

An integration of requirements to ensure that the Army is properly resourced. To accomplish this task, the Army aggregates all requirements into a set of Management Decision Packages (MDEP).

OMB 300 Report

A DOD report for Congress that ensures IT systems conform to the requirements of OMB Circular No. A-130.

Service operations

Service operations consists of: incident management, event management, problem management, spectrum management, and database and Internet Web management.

Section III

Special Abbreviations and Terms

This section contains no entries.

UNCLASSIFIED

PIN 048040-000