DCMA Instruction 4401

Information Technology Management

==========

Office of Primary Responsibility	**Information Technology Management Capabililty**
Effective:	January 20, 2020
Releasability:	Cleared for public release
New Issuance	
Internal Control:	Not Applicable
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.intranet.dcma.mil/Sites/Policy/ITM/SitePages/4401r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," establishes policy and assigns responsibility for:

- Alignment of Information Technology Management with the Agency mission, vision and goals
- Implementing Information Technology Management to manage resources, sustain enterprise operations, exploit opportunities, and maximize benefits
- Appropriate management of Information Technology related risk
- Implementing the strategies required to extend Information Technology Management activities into the future

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Establish an Information Technology Management (ITM) framework to ensure international frameworks, standards, and best practices (e.g., International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500, and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems," are applied.

b. Support ITM initiatives to ensure oversight and control of DCMA IT activities to standardize processes and procedures.

c. Define asset management, security and privacy controls, capital planning investment control, and accessibility required to execute the DCMA IT enabling activities.

d. Execute this Instruction in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The DCMA Director will:

a. Provide strategic oversight of ITM functions throughout DCMA Components and Capability Portfolios, IT lifecycle management processes, and investment programs incorporating IT.

b. Ensure adequate funding and resources are allocated to support the IT services and security.

c. Ensure information security management processes are integrated with DCMA strategic, operational, and budgetary planning processes.

d. Ensure compliance with directed cyberspace operations as directed by orders, or other directives such as alerts and bulletins and provide support to cyberspace defense pursuant to DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations."

e. Delegate to the Chief Information Officer (CIO) the authority to ensure compliance with the requirements imposed on DCMA under this Instruction.

f. Ensure all Information Systems under the Director's purview are authorized in accordance with DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)."

g. Ensure military and civilian personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DoD information by not ensuring implementation of DoD security requirements.

2.2. EXECUTIVE DIRECTOR, CHIEF INFORMATION OFFICER (CIO), INFORMATION TECHNOLOGY DIRECTORATE, DCMA. The CIO will:

a. Establish and oversee DCMA's Information Technology Service Management (ITSM) Program.

b. Ensure the effective implementation of DCMA's ITSM and Security programs.

c. Ensure effective implementation and execution of DCMA's cybersecurity controls.

d. Implement IT policies, principles, standards, and guidelines with respect to all areas of information management and security.

e. Develop and maintain ITSM Program policies, procedures, and control techniques to address all applicable requirements.

f. Report annually to the agency Director the effectiveness of DCMA's investment management, service management, and security programs including progress of remedial actions.

SECTION 3: INFORMATION TECHNOLOGY MANAGEMENT

3.1. PROCEDURAL MANUALS (MAN). The manuals listed below will detail the DCMA IT alignment to NIST, Capital Planning Investment Control (CPIC), Asset Management, and 508 Compliance. The MANs listed below will implement this instruction. The processes and procedures will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to facilitate the execution of ITM.

a. ACCESS CONTROL (AC-1). DCMA-MAN 4401-01, "Access Control Manual," details the implementation, assign responsibility, and provide procedural direction to limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

b. CYBERSECURITY AWARENESS AND TRAINING (AT-1). DCMA-MAN 4401-02, "Cybersecurity Awareness and Training," details the implementation, assign responsibility, and provide procedural direction for employees and information system users both initial and periodic refresher cybersecurity training in order to maintain a degree of understanding of cybersecurity policies commensurate with their responsibilities.

c. AUDIT AND ACCOUNTABILITY (AU-1). DCMA-MAN 4401-03, "Audit and Accountability," details the implementation, assign responsibility, and provide procedural direction to create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

d. SECURITY ASSESSMENT AND AUTHORIZATION (CA-1). DCMA-MAN 4401-04, "Security Assessment and Authorization" details the implementation, assign responsibility, and provide procedural direction to ensure that the execution of CA-1 periodically assesses the security controls in DCMA information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in DCMA information systems; authorize the operation of DCMA information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness.

e. CHANGE/CONFIGURATION MANAGEMENT (CM-1). DCMA-MAN 4401-05, "Change/Configuration Management," details the implementation, assign responsibility, and provide procedural direction to ensure that any modification to the DCMA IT environment establishes an orderly and effective procedure for tracking the submission, coordination, review, evaluation, categorization, and approval for release of all changes to a service or service component.

f. CONTINGENCY PLANNING (CP-1). DCMA-MAN 4401-06, "Contingency Planning," details the implementation, assign responsibility, and provide procedural direction to

establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for DCMA information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

g. IDENTIFICATION AND AUTHENTICATION (IA-1). DCMA-MAN 4401-07, "Identification and Authentication," details the implementation, assign responsibility, and provide procedural direction to identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to DCMA information systems.

h. INCIDENT RESPONSE (IR-1). DCMA-MAN 4401-08, "Incident Response," details the implementation, assign responsibility, and provide procedural direction to establish an operational incident handling capability for DCMA information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate DCMA officials and/or authorities.

i. MAINTENANCE (MA-1). DCMA-MAN 4401-09, "Maintenance," details the implementation, assign responsibility, and provide procedural direction to identify periodic and timely maintenance on DCMA information systems; and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. DCMA will manage information systems maintenance and repairs through an effective security best practices maintenance program.

j. SECURITY PLANNING (PL-1). DCMA-MAN 4401-10, "Security Planning," details the implementation, assign responsibility, and provide procedural direction to develop, document, periodically update, and implement security plans for DCMA information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

k. RISK ASSESSMENT (RA-1). DCMA-MAN 4401-11, "Risk Assessment," details the implementation, assign responsibility, and provide procedural direction for the Cyber security risk assessment, an essential tool, to DCMA stakeholders with the information needed to understand information system vulnerabilities which may negatively impact our mission.

l. SYSTEM AND SERVICES ACQUISITION (SA-1). DCMA-MAN 4401-12, "System and Services Acquisition," details the implementation, assign responsibility, and provide procedural direction to allocate sufficient resources to adequately protect DCMA information systems; employ system development life cycle processes that incorporate information security considerations; employ software usage and installation restrictions; and ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from DCMA.

m. SYSTEM AND COMMUNICATIONS PROTECTION (SC-1). DCMA-MAN 4401-13, "System and Communications Protection," details the implementation, assign responsibility, and provide procedural direction to monitor, control, and protect DCMA communications (i.e., information transmitted or received by DCMA information systems) at the external boundaries

and key internal boundaries of the information systems; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within DCMA information systems in order to deny unauthorized access to sensitive or valuable information.

n. SYSTEM AND INFORMATION INTEGRITY (SI-1). DCMA-MAN 4401-14, "System and Information Integrity," details the implementation, assign responsibility, and provide procedural direction to identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within DCMA information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

o. SECURITY PROGRAM MANAGEMENT (PM-1). DCMA-MAN 4401-15, "Security Program Management (PM-1)," details the implementation, assign responsibility, and provide procedural direction to develop and disseminate a DCMA-wide, supporting information security program. The manner in which DCMA implements the program management controls depends on specific DCMA characteristics including, for example, the size, complexity, and mission/business requirements of the respective organizations.

p. CAPITAL PLANNING INVESTMENT CONTROL (CPIC). DCMA-MAN 4401-16, "Capital Planning Investment Control," details the implementation, assign responsibility, and provide procedural direction to ensure the IT Directorate executes specific policy, procedural, and analytic guidelines for planning, budgeting, acquisition, and management of major IT capital investments.

q. ASSET LIFECYCLE MANAGEMENT (AM). DCMA-MAN 4401-17, "Asset Lifecycle Management," details the implementation, assign responsibility, and provide procedural direction to establish policy, assign responsibility, and prescribe general principles associated with Accountable Property and General Equipment. It provides guidance and direction for operational management of IT hardware and software.

r. INFORMATION AND COMMUNICATION ACCESSBILITY (508 Compliance). DCMA-MAN 4401-18, "Information and Communication Accessibility," details:

(1) Responsibility and provides procedural direction for the agency's 508 compliance implementation in accordance with Section 794d of Title 29, United States Code.

(2) Accessibility for DoD employees or members of the public with disabilities seeking information or services from the DoD. Ensures they have access to information and data comparable to the access and use by individuals without disabilities, unless such access and use would impose an undue burden on the DoD.

GLOSSARY

G.1. DEFINITIONS.

AM. Asset Lifecycle Management establishes policy, assigns responsibility, and prescribes general principles associated with Accountable Property and General Equipment. It provides guidance and direction for operational management of IT hardware and software.

AC-1. Access Control limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AT-1. Cyber Awareness and Training provides employees and information system users both initial and periodic refresher cybersecurity training in order to maintain a degree of understanding of cybersecurity policies commensurate with their responsibilities.

AU-1. Audit and Accountability creates, protects, and retains information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

CA-1. Security Assessment and Authorization periodically assesses the security controls in DCMA information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in DCMA information systems; authorize the operation of DCMA information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness.

CIO. Accountable for the overall operations of the DCMA ITSM. Ensures execution of DCMA IT Governance. Provides leadership and direction to other relevant groups and bodies based on best-practices and standards for ITSM. Escalates conflicts for issue resolution up the chain of command.

CM-1. The Change/Configuration Management process ensures all changes are assessed, approved, implemented and reviewed in a controlled manner. To this end, Change Management ensures that any modification to the IT environment, whether it involves an addition, maintenance, or deletion of a service or service component, is in line with the overall mission strategy. This process provides standardized methods and procedures for efficient and prompt handling of technical changes, to minimize the impact of change-related incidents to service quality, and improves day-to-day operations of the organization.

CP-1. Contingency Planning establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for DCMA information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CPIC. Capital Planning Investment Control will ensure the Information Technology Directorate executes specific policy, procedural, and analytic guidelines for planning, budgeting, acquisition, and management of major IT capital investments.

IA-1. Identification and Authentication identifies information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to DCMA information systems.

IR-1. Incident Response establishes an operational incident handling capability for DCMA information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate DCMA officials and/or authorities.

MA-1. Maintenance identifies periodic and timely maintenance on DCMA information systems; and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. DCMA will manage information systems maintenance and repairs through an effective security best practices maintenance program.

PL-1. Security Planning develops, documents, periodically updates, and implements security plans for DCMA information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

PM-1. Security Program Management develops and disseminates a DCMA-wide, supporting information security program. The manner in which DCMA implements the program management controls depends on specific DCMA characteristics including, for example, the size, complexity, and mission/business requirements of the respective organizations.

RA-1. Risk Assessment is an essential tool for providing DCMA stakeholders with the information needed to understand information system vulnerabilities which may negatively impact our mission. DCMA will ensure RA-1 implements a strong risk assessment program.

SA-1. System and Services Acquisition allocates sufficient resources to adequately protect DCMA information systems; employ system development life cycle processes that incorporate information security considerations; employ software usage and installation restrictions; and ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from DCMA.

SC-1. System and Communications Protection monitors, controls, and protects DCMA communications (i.e., information transmitted or received by DCMA information systems) at the external boundaries and key internal boundaries of the information systems; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within DCMA information systems in order to deny unauthorized access to sensitive or valuable information.

SI-1. System and Information Integrity identifies, reports, and corrects information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within DCMA information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

GLOSSARY

G.2. ACRONYMS.

AC-1	Access Control
AM	Asset Lifecycle Management
AT-1	Cybersecurity Awareness and Training
AU-1	Audit and Accountability
CA-1	Security Assessment and Authorization
CIO	Chief Information Officer
CM-1	Change/Configuration Management
CP-1	Contingency Planning
CPIC	Capital Planning Investment Control
DCMA-MAN	DCMA Manual
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
IA-1	Identification and Authentication
IR-1	Incident Response
IT	Information Technology
ITM	Information Technology Management
ITSM	Information Technology Service Management
ITSMO	IT Service Management Office
MA-1	Maintenance
MAN	Manual
NIST	National Institute of Standards and Technology
PL-1	Security Planning
PM-1	Security Program Management
RA-1	Risk Assessment
SA-1	System and Services Acquisition
SC-1	System and Communications Protection
SI-1	System and Information Integrity
SP	Special Publication

REFERENCES

DoDD 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," July 28, 2017, (as amended)
DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 07, 2017, (as amended)
NIST SP 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015 (as amended)
United States Code, Title 29, Section 794d