DCMA Instruction 4402
Cybersecurity Program

Office of Primary Responsibility:	**Organizational Infrastructure Capability Board**
Effective:	September 9, 2025
Releasability:	Cleared for public release
Incorporates and Cancels:	DCMA Instruction 815, "Cybersecurity/Information Assurance (IA)," July 10, 2014
Internal Control Plan:	Not applicable
Labor Codes:	Located on the resource page for this issuance
Resource Page Link:	https://dod365.sharepoint-mil.us/sites/DCMA-BCF-Organizational_Infrastructure/SitePages/4402-Cybersecurity-Program.aspx
Approved by:	Sonya I. Ebright, SES, Acting Director

Purpose: This instruction, in accordance with DoD Directive 5105.64 and DoD Instruction 8500.01:

- Comprises multiple DCMA publications, each containing its own purpose as part of the DCMA Cybersecurity Program.
- Establishes policy, assigns responsibilities, and establishes procedures and acceptable use regarding the DCMA Cybersecurity Program.

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This instruction applies to:

a. DCMA civilian, military, and contractor personnel who manage, maintain, operate, or protect DCMA systems or data.

b. Information technology (IT) systems owned and operated by or on the behalf of DCMA.

c. DCMA or DoD data contained on or processed by IT systems owned and operated by or on the behalf of DCMA.

d. DCMA IT systems classified as Secret or below and electronic data that is Secret or below.

e. This instruction does not apply to IT systems classified as, or including, access privileges to special access programs or compartmentalized data.

1.2. POLICY.

It is DCMA policy to:

a. Ensure that all civilian, military, contractors, and other authorized users strictly adhere to the DCMA Acceptable Use Policy.

b. Ensure that access to DCMA organizational information system (IS), networks, and data is based on the principle of least privilege, ensuring that users have only the minimum necessary access required to perform their assigned duties.

c. Execute and perform cyber incident response activities in strict accordance with applicable DoD and Federal regulations to minimize operational disruption, protect organizational assets, and ensure business continuity.

d. Ensure the execution and performance of vulnerability management to ensure the protection and ongoing security of our digital assets.

e. Implement and enforce all relevant DoD cybersecurity policy, directives, and instructions, including but not limited to, DoD Instruction (DoDI) 8500.01.

f. Execute the processes of this instruction in a safe, efficient, effective, and ethical manner within DCMA workplaces.

1.3. SPECIFIED FORMS AND INFORMATION COLLECTION.

a. DCMA Form (DCMAF) 4402-01-1, "Acceptable Use Policy (AUP)."

(1) The DCMAF 4402-01-1 outlines the conditions and responsibilities for accessing U.S. and DCMA Government IS in accordance with DoDI 8500.01. DCMAF 4402-01-1 emphasizes safeguarding network information from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. DCMAF 4402-01-1 is linked on the resource page for this instruction.

(2) DCMAF 4402-01-1 instructions: All authorized personnel must complete the DCMAF 4402-01-1 to gain initial access to the DCMA network. Authorized personnel are required to review and acknowledge the AUP annually.

b. DCMAF 4402-01-2, "Privileged Access Agreement (PAA)."

(1) The DCMAF 4402-01-2 outlines the terms personnel granted elevated system privileges must agree to concerning accountability and acceptable use, thereby mitigating insider threats and enforcing the principle of least privilege to safeguard critical information and systems in accordance with DoDI 8500.01. This agreement ensures compliance with cybersecurity policies and provides a framework for managing user responsibilities and potential disciplinary actions. DCMAF 4402-01-2 is linked on the resource page for this instruction.

(2) DCMAF 4402-01-2 instructions: All authorized personnel requiring elevated access to a DCMA IS must complete and sign the DCMAF 4402-01-2 to obtain requested access. Personnel with existing elevated rights will need to re-sign when there are any updates or changes to the DCMA PAA.

c. DoD Form (DD Form) 2875, "System Authorization Access Request (SAAR)."

(1) DD Form 2875, also known and referred to in this manual as SAAR, is prescribed to collect data for validating the trustworthiness of individuals requesting access to DoD systems and information.

(2) Pursuant to Volume 1 of DCMA Manual 4501-04, "Records and Information Management Program," and Volume 2 of DCMA Manual 4501-04, "Records Retention Schedule," access control, identification, and authentication records are kept electronically.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA.

The DCMA Director must:

a. Establish the DCMA Cybersecurity Program.

b. Allocate resources and funding for cybersecurity initiatives.

c. Appoint the Authorizing Official (AO).

2.2. DCMAIT EXECUTIVE DIRECTOR AND CHIEF INFORMATION OFFICER (CIO).

The DCMAIT Executive Director and CIO must:

a. Under the authority of the DCMA Director, serve as AO.

b. Exercise overall responsibility for the Agency's IT and cybersecurity enforcement.

c. Serve as the authority to formally accept the risk of operating a system.

d. Make the final decision on whether to authorize a system to operate and grant an Authority to Operate, if applicable.

e. Appoint the Chief Information Security Officer (CISO) and authorizing official designated representative (AODR).

2.3. CISO AND AODR.

The CISO and AODR must:

a. Develop, implement, and enforce the agency's cybersecurity program and policies.

b. Align cybersecurity decisions with the organization's mission and strategic goals.

c. Oversee risk management and compliance.

d. Serve as a technical advisor to the AO.

e. Accurately evaluate security controls and assess risk.

2.4. INFORMATION SYSTEM SECURITY MANAGER (ISSM) AND INFORMATION SYSTEM SECURITY OFFICER (ISSO).

The ISSM and ISSO must oversee security of one or more IS, including implementing and maintaining security controls.

2.5. INFORMATION SYSTEM OWNER (ISO).

The ISO must oversee procurement, development, integration, modification, operation, maintenance, and disposal of an IS.

2.6. SYSTEM AND NETWORK ADMINISTRATOR.

The system and network administrators must:

a. Maintain system security configurations.

b. Manage network security devices.

c. Apply security patches and updates.

2.7. CYBERSECURITY ANALYSTS.

The cybersecurity analysts must:

a. Analyze security alerts and events.

b. Conduct security assessments.

2.8. AUTHORIZED USERS.

Authorized users must:

a. Review and electronically acknowledge the DCMAF 4402-01-1 prior to gaining initial access to the network.

b. Review and electronically sign a DCMAF 4402-01-2 prior to or upon initial privileged account activation, if applicable.

c. Report security incidents to the DISA Service Center.

SECTION 3: GENERAL PRINCIPLES

3.1. CYBERSECURITY PROGRAM APPROACH.

a. The DCMA Cybersecurity Program is the agency's unified approach to protect unclassified, sensitive, and classified information stored, processed, accessed, and transmitted by DCMA IS and mission applications. The DCMA Cybersecurity Program consolidates and focuses DCMA efforts in securing information, including its associated systems and resources, to increase the level of trust of this information and the originating source.

b. The DCMA Cybersecurity program ensures prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication. The Cybersecurity program ensures the integrity, confidentiality, availability, authentication, and non-repudiation of information contained in these systems and communications.

c. The implementation of cybersecurity program objectives such as integrity, confidentiality, availability, authentication, and non-repudiation enables DCMA to meet its mission and business objectives. To perform its mission, DCMA must implement systems with due consideration of IT-related risks to DCMA and the Department of Defense Information Network.

d. This instruction provides the framework for the DCMA Cybersecurity Program, including overarching policy, responsibilities, and AUP for all other cybersecurity topics.

e. The DCMA Cybersecurity Program will be implemented in a series of DCMA publications following key DoD Cybersecurity policies as shown in Table 1.

Table 1. Relationship of Key Cybersecurity Topics and Supporting Guidance

DoDI – Key Topics	Associated Policy and/or Procedure
Alt Tokens	• DoD Instruction 8520.02 • DoD CIO Memo "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems"
Appointments	• DoD Manual 8140.03
Code Signing Certificates	• DoD Instruction 8500.01
Contracts/Agreements – Cybersecurity Requirements	• DoD Manual 8140.03 • DoD Instruction 4000.19
Incident Management	• DoD Instruction 8530.01 • CJCS Manual 6510.01
Log Management	• National Institute of Standards and Technology Special Publication 800-92
Ports, Protocols, and Services Management	• DoD Instruction 8551.01
Public Key Infrastructure	• DoD Instruction 8520.02
Qualifications	• DoD Manual 8140.03
Risk Management Framework	• DoD Instruction 8510.01
Training	• DoD Manual 8140.03

Table 1. Relationship of Key Cybersecurity Topics and Supporting Guidance, Continued

DoDI – Key Topics	Associated Policy and/or Procedure
Vulnerability Management	• DoD Instruction 8530.01 • DoD Instruction 8531.01 • CJCS Instruction 6510.01

3.2. COMPLIANCE.

Failure to follow any of the DCMAIT security policies, corresponding standards and procedures, or any other DCMA policies of procedures, will result in appropriate action which may include suspension or loss of access to DCMA systems and facilities. DCMA employees may also be subject to discipline under the provisions of DCMA-MAN 4201-02, Maintaining Discipline."

SECTION 4: ACCESS CONTROL AND AUP

4.1. ACCESS CONTROL.

a. User account activity must be continuously monitored for unauthorized access or suspicious behaviors by system/network administrators. Audit logs must be generated and reviewed regularly by cybersecurity analysts and ISO.

b. The use of shared accounts is prohibited at DCMA and is only authorized by the written approval of the AO or designee based on mission requirements.

c. Service accounts must be created only when necessary and will be given only the privileges needed to perform their function.

d. Temporary or emergency accounts must be removed within twenty-four (24) hours post event or incident conclusion driving the creation of the account by the Access Control Team. Where achievable, DCMA must automatically remove or disable temporary and emergency accounts within five (5) business days of non-usage.

e. DCMA users are required to remove system access tokens (e.g., Common Access Card) when the system is not in use. An automatic inactivity logout policy of not greater than five (5) minutes will be enforced on all DCMA IS if tokens are not removed.

f. Upon the discovery of a security and/or privacy incident, user accounts must be disabled within one (1) hour by the Access Control Team and not enabled until approved by the CIO, Deputy CIO, or CISO.

g. System and Network administrator accounts must be identified, documented, and tracked by the Access Control Team and ISO. DCMA must use System Access Authorization Request (SAAR) to support separation of duties.

h. The principles of least privilege, as it relates to personnel performing administration or security functions, must be applied to include the use of non-privileged accounts or roles when performing non-security functions.

i. Accounts (i.e., common access card, local, alternate, multifactor authentication and username and password) will be locked after three (3) consecutive invalid logon attempts. Accounts will be locked for a period of no less than one (1) hour until released by an administrator.

j. To protect classified information, the use of unclassified mobile devices is strictly prohibited in all facilities where such information is processed, stored, or transmitted. This includes, without exception, Sensitive Compartmented Information Facilities unless explicitly authorized by the AO or designee due to critical mission needs.

k. The use of external systems for which DCMA does not have direct control over the implementation of controls or the assessment of control effectiveness for the purpose of processing, storing, or transmitting DCMA or DoD information is prohibited.

4.2. AUP.

All DCMA users will review and acknowledge the AUP prior to or upon account activation. Digital signatures are authorized. The following items are included in the DCMA AUP:

a. DoD policy states that Federal Government communication systems and equipment, including government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems, when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only.

b. All personnel are required to report suspicious activity and/or incidents to the DISA Service Center immediately upon discovery. The Service Center can be contacted via phone (1-844-347-2457).

c. Certain activities are never authorized on DCMA networks. AUPs set out the following activities as prohibited:

(1) Use of ISs for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.

(2) Modification of the IS or software, use of it in any manner other than its intended purpose or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial internet chat, collaborative environments, or peer-to-peer client applications. These applications create exploitable vulnerabilities and circumvent normal means of securing and monitoring network activity. Thus, these commercial applications could provide a vector for the introduction of malicious code, remote access, network intrusions, or the exfiltration of protected data.

(3) Attempts to strain, test, circumvent, or bypass network or IS security mechanisms, or to perform network or keystroke monitoring. Cybersecurity Service Provider, Red Team, or other official activities, operating in their official capacities only, may be exempted from this requirement.

(4) Physical relocation or changes to configuration or network connectivity of IS equipment.

(5) Installation of non-government-owned computing systems or devices without prior authorization of the appointed AO including, but not limited to, USB devices, external media, personal or contractor-owned laptops.

(6) Release, disclosure, transfer, possession, or alteration of information without the consent of the data owner, the original classification authority pursuant to DCMA-MAN 3301-08 "Information Security," the individual's supervisory chain of command, Freedom of Information Act official, Public Affairs Office, or disclosure officer's approval.

(7) Sharing personal accounts and authenticators (e.g., passwords or personal identification numbers) or permitting the use of remote access capabilities through government-provided resources with any unauthorized individual.

(8) Disabling or removing security or protective software and other mechanisms and their associated logs from IS.

SECTION 5: PRIVILEGED ACCESS POLICY

All DCMA users requiring privileged access to DoD ISs will review and electronically sign a DCMAF 4402-01-2 prior to or upon initial account activation. Digital signatures in accordance with DoD policy are authorized for PAA execution. At a minimum, the following items are included in the DCMA PAA:

a. A clear statement outlining the specific elevated rights being granted and the authorized purposes for their use.

b. A detailed description of the user's obligations in safeguarding the system and data, including adherence to security policies and procedures.

c. Acceptable use guidelines with explicit rules governing the appropriate use of privileged access.

d. A non-exhaustive list of prohibited activities that are strictly forbidden when utilizing privileged access, including:

- Unauthorized installation or execution of software
- Disabling or bypassing security controls without explicit authorization
- Accessing or modifying data that is not required for official duties
- Sharing privileged account credentials with others
- Using privileged accounts for personal activities or unauthorized purposes
- Connecting unauthorized devices to DCMA ISs
- Attempting to gain unauthorized access to systems or data beyond the scope of granted privileges
- Intentional introduction of malicious code (e.g., viruses, worms)
- Neglecting to report security incidents or vulnerabilities
- Violating data spillage or cross-domain transfer policies

e. A statement emphasizing user accountability, or all actions taken with their privileged accounts and the understanding that these actions may be audited.

f. A clear outline of the potential disciplinary and legal repercussions for unauthorized or inappropriate use of privileged access.

g. Instructions on how to report security incidents or suspected vulnerabilities related to privileged access.

h. Confirmation that the user has received and understands relevant security awareness and privileged access training.

i. Specification of the agreement’s validity period and the requirement for periodic review and re-signature, especially upon significant system changes or policy updates.

GLOSSARY

G.1. ABBREVIATIONS AND ACROYNMS.

ACRONYM	MEANING
AO	authorizing official
AODR	authorizing official designated representative
ALT	alternate logon tokens
AUP	acceptable use policy
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DCMAF	DCMA Form
DCMAF 4402-01-1	Acceptable Use Policy Form
DCMAF 4402-01-2	Privileged Access Agreement Form
DCMAIT	Information Technology Directorate
DCMA-MAN	DCMA manual
DD Form 2875	System Authorization Access Request
DoDI	DoD instruction
IS	information system
ISSM	information system security manager
ISO	information system owner
ISSO	information system security officer
IT	information technology
PAA	Privileged Access Agreement
USB	universal serial bus

GLOSSARY

G.2. DEFINITIONS.

TERM	MEANING
authorized users	Any appropriately cleared individual with a requirement to access an IS for performing or assisting in a lawful and authorized Federal Government function.
AO	Senior (Federal) official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations, including mission, functions, image, or reputation, organizational assets, individuals, other organizations, and the United States.
computer network defense	Actions taken to defend against unauthorized activity within computer networks. Computer network defense includes monitoring, detection, analysis (e.g., trend and pattern analysis), and response and restoration activities.
controlled unclassified information	Defined in DoDI 5200.48.
cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
IS	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. ISs also include specialized systems such as industrial and process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
ISSM	Individual responsible for the information assurance of a program, organization, system, or enclave.
ISSO	Individual assigned responsibility for maintaining the appropriate operational security posture for an IS or program.
IT	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display,

	switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services, including support services, and related resources.
public key infrastructure	The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
privileged access	Authorized logical or physical access to DoD information, ISs, or controlled areas that exceed the access granted to non-privileged users. This access enables the performance of security-relevant functions, including system configuration, administration, maintenance, and the ability to impact system security posture and data confidentiality, integrity, and availability.
privileged user	Authorized individual who has been granted privileged access to perform security-relevant functions that ordinary users are not authorized to perform. These functions typically involve the control, monitoring, or administration of the system, its security mechanisms, and the data it contains.
Red Team	A group of security professionals authorized to simulate real-world cyberattacks in order to test an organization's defenses.
remote access	Access to an organization's nonpublic IS by an authorized user or an IS communicating through an external, non-organization-controlled network (e.g., the Internet).

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 6510.01, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
Chairman of the Joint Chiefs of Staff Manual 6510.01, "Cyber Incident Handling Program," July 10, 2012, as amended
DCMA Manual 3301-08, "Information Security," January 21, 2019
DCMA Manual 4201-02, "Maintaining Discipline," January 25, 2020
DCMA Manual 4501-04 Volume 1, "Records and Information Management Program," April 16, 2021
DCMA Manual 4501-04 Volume 2, "Records Retention Schedule," April 14, 2021
DoD Chief Information Security Officer (CIO) Memo "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems," August 20, 2018
DoD Instruction 4000.19, "Support Agreements," December 16, 2020
DoD Instruction 5200.48. "Controlled Unclassified Information (CUI)" March 6, 2020
DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Systems," July 19, 2022
DoD Instruction 8520.02, "Public Key Infrastructure and Public Key Enabling," May 18, 2023
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 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 31, 2023
DoD Manual 8140.03, "Cybersecurity Workforce Qualification and Management Program," February 15, 2023.
National Institute of Standards and Technology Special Publication 800-92, "Guide to Computer Security Log Management," October 23, 2023