DCMA Manual 3401-04
Defense Industrial Base Mission Risk Management

Office of Primary Responsibility:	**Acquisition Insight Capability Board**
Effective:	January 13, 2019
Change 1 Effective:	*April 16, 2021*
Change 2 Effective:	*October 16, 2025*
Releasability:	Not cleared for public release
New Issuance	
Implements:	DCMA Instruction 3401, "Defense Industrial Base Mission Assurance," August 29, 2018
Internal Control Plan:	Linked on the resource page for this issuance
Labor Codes:	Located on the resource page for this issuance
Resource Page Link:	https://dod365.sharepoint-mil.us/sites/DCMA-Projects-PH-PI-IntegrationCB/SitePages/3401-04.aspx
Approved by:	David H. Lewis, VADM, USN, Director
Change 1 Approved by:	*David G. Bassett, LTG, USA, Director*
Change 2 Approved by:	*Sonya I. Ebright, SES, Acting Director*

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64 and DCMA Instruction 3401, "Defense Industrial Base Mission Assurance":

- Assigns responsibilities, describes procedures, and provides guidance associated with the Defense Industrial Base Mission Risk Management processes
- Implements agency national Defense Industrial Base sector Mission Assurance responsibilities pursuant to DoD Directive 3020.40, DoD Instruction 3020.45, National Security Memorandum-22, and related issuances.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to all DCMA commands, as well as DCMA components and capabilities that contribute to Defense Industrial Base (DIB) Mission Risk Management as identified in Section 2 of this manual.

1.2. POLICY.

This manual provides guidance to the DCMA workforce responsible for executing the DIB Mission Risk Management activities, defines high-level roles, and delineates responsibilities for the various DCMA components and capabilities. It is DCMA policy to:

a. Support the Mission Assurance Coordination Board (MACB) and assist the Office of the Under Secretary of Defense for Policy (OUSD(P)) in managing risk to priority DIB assets and the industrial capabilities that support strategic defense missions (e.g., Defense Critical Missions as defined by Chairman of the Joint Chiefs of Staff (CJCS)).

b. Recommend risk management actions for prioritized DIB assets and support DIB critical infrastructure Risk Management Plan (RMP) development.

c. Facilitate DIB risk management activities and advise DIB risk management programs. Coordinate risk management activities between defense acquisition and mission assurance stakeholders.

d. Identify potential alternate sources of supply for perceived DIB single points of failure.

e. Perform DIB Mission Risk Management in a multifunctional, synchronized, and coordinated manner by integrating data throughout DCMA and partnering with other DoD, Federal, state, local, and commercial entities that have a stake in DIB Mission Assurance (MA).

f. Deliver value-added DIB insight and share DIB Mission Risk Management products where appropriate and as permitted by law: (1) externally to DoD, Federal, state, local and commercial industry partners to manage DIB risk efficiently and effectively; and (2) within DCMA to support corporate risk evaluation, major program risk monitoring, contract risk assessment, critical sub-contractor oversight delegation, and surveillance planning.

g. Safeguard business sensitive and proprietary DIB data, Controlled Unclassified Information (CUI), and classified material routinely gathered or developed in the execution of DIB Mission Risk Assessment.

h. Execute this manual in a safe, efficient, effective, and ethical manner.

1.3. RECORDS MANAGEMENT.

a. DCMA employees will maintain all records created as a result of this issuance pursuant to DoDI 5015.02, the National Archives and Record Administration General Records Schedules (GRS), Volume 1 of DCMA Manual (DCMA-MAN) 4501-04, "Records and Information Management Program," and Volume 2 of DCMA-MAN 4501-04, "Records Retention Schedule."

b. Appendix 1A outlines records created as a result of this issuance, identifies the office of primary responsibility (OPR) records custodian, and details correlating storage requirements. Records responsibilities are pursuant to Volume 1 of DCMA-MAN 4501-04. The approved DCMAF 4501-04, "Records File Plan," is linked on the resource page for this manual.

1.4. OVERVIEW.

a. MA informs mission owners and senior leaders of operational risk to critical capabilities that support Mission Essential Functions (MEFs). DoD applies a standardized MA framework to achieve comprehensive mission risk management across a spectrum of essential capabilities, including those provided by the DIB. DCMA leverages its worldwide presence and access to industrial facilities to execute national DIB sector MA responsibilities on behalf of the national DIB Sector Specific Agency (SSA).

b. DIB MA is an integrating capability within DCMA's Business Capability Framework (BCF) that utilizes available agency data and gathers industry data in order to analyze industrial capability risk. The Industrial Analysis Group (IAG) is the DIB MA Office of Primary Responsibility (OPR) pursuant to DCMA Memorandum 17-072, "Agency Mission Essential Functions;" Under Secretary of Defense Memorandum, "Defense Contract Management Agency Mission Changes;" and as implemented in DCMA Instruction (DCMA-INST) 3401,"Defense Industrial Base Mission Assurance." The IAG serves as the DoD MA center of excellence to identify, analyze, and assess the DIB supply chain network that supports DoD mission execution and assist other DoD Components' efforts with DIB-related analysis. DIB MA is defined by the following processes that act together in concert to achieve comprehensive DIB risk management: Conduct Industrial Base Assessment (IBA); Identify and Prioritize DIB Assets; Assess DIB Mission Risk; Manage DIB Mission Risk; Execute DIB Monitoring and Reporting; and Administer DIB MA Industry Outreach and Awareness.

c. The objective of the DIB Mission Risk Management process is to achieve acceptable risk levels for Defense Critical Missions by addressing identified vulnerabilities and managing issue response at critical DIB assets. Driving down risk to strategic defense missions is paramount to ensuring DoD MEF execution.

1.5. SUMMARY OF CHANGES.

This manual has been substantively changed to include updated organizational terms and records management information and added Operational Analytics and Integration Center responsibilities.

APPENDIX 1A. DCMA 3401-04 RECORDS

Step, Function, Activity, or Section	**Record(s) Created - Key Documentation**	**Record Series**	**Storage Location** Include direction for OPR records custodian	**OPR Records Custodian**
DIB MA	Assessments supporting acquisition decisions	Series 800.01a	DoD365	IAD
DIB MA	Other non-acquisition assessments	Series 800.03a	DoD365	IAD
DIB MA	Important Capabilities List (ICL)	Series 800.03a	DoD 365	IAD
DIB MA	Task Asset List (TAL)	Series 800.03a	SIPR	IAD

SECTION 2: RESPONSIBILITIES

2.1. EXECUTIVE DIRECTOR, ENTERPRISE ANALYTICS AND MODERNIZATION.

In addition to the responsibilities in Paragraph 2.4., the Enterprise Analytics and Modernization Executive Director must:

a. Ensure continued execution of DCMA DIB MA MEF. Specifically, ensure DIB Mission Risk Management process is sufficiently resourced, integrated within the agency, and can be executed under any operational condition.

b. Empower the IAG Director to take agency level action necessary to accomplish DIB Mission Risk Management functions.

c. Share DIB Mission Risk Management situational awareness and informational products with the Agency Senior Leadership Team, as needed.

d. Resource DIB outreach and site visits to inform communities of DIB MA, promote risk management action coordination, validate assumptions and risk management recommendations, and expedite risk management activities.

2.2. DIRECTOR, OPERATIONAL ANALYTICS AND INTEGRATION CENTER.

The Operational Analytics and Integration Center Director must:

a. Build enterprise data analytic capabilities based off the requirements and thresholds established by the Capability Framework using system of record internal and external data sources.

b. Maintain the data analytics if system of record changes occur.

c. Provide health metrics and data analytics using systems of record data internally and externally.

2.3. DIRECTOR, IAG.

The IAG Director must:

a. Serve as the Agency OPR for DIB Mission Risk Management.

b. Ensure required MEF output tasks can be executed under any operational condition.

c. Provide necessary DIB subject matter experts (SMEs) to support the MACB, Industrial Base Council, Joint Industrial Base Working Group (JIBWG), and other DIB risk management forums as required.

d. Perform JIBWG Executive Agent duties as assigned in the JIBWG charter and in accordance with DCMA-INST 3401. Promote DIB risk management action coordination across JIBWG stakeholder components.

e. Prioritize DIB Mission Risk Management workload in accordance with DIB asset criticality pursuant to DCMA-MAN 3401-02, "Defense Industrial Base Critical Asset Identification and Prioritization," (CAIP) and risk rating as determined by DCMA-MAN 3401-03, "Defense Industrial Base Mission Risk Assessment."

f. Conduct market research and identify potential alternate sources of supply for perceived DIB single points of failure. Determining potential alternate sources of supply is a required MEF output task for DIB MA

g. Support DIB RMP development and recommend risk management actions for prioritized DIB facilities assessed via the DIB Mission Risk Assessment process (DCMA-MAN 3401-03). Lead coordination and integration of DCMA component and capability input to DIB RMP development. Pursuant to DoD Instruction 3020.45, "Mission Assurance (MA) Construct," RMPs are required within 180 days of a DIB mission assurance assessment (MAA) report to facilitate the prioritization of risk management activities.

h. Advise DoD risk management programs on DIB investments. Coordinate risk management activities between defense acquisition and MA stakeholders. Promote DIB MA awareness with DIB risk management program OPRs and synchronize risk management activities among stakeholders to the maximum extent possible.

i. Document DoD DIB risk management actions in the agency repository of defense industry data. A link to the agency system of record is located on the Resource Page of this manual.

j. Partner with DCMA (e.g., those components and capabilities identified in Section 2 of this manual), DoD, Federal, state, local, and commercial entities, as appropriate and as permitted by law, to manage defense mission risk stemming from DIB asset vulnerabilities identified during MAA (DCMA-MAN 3401-03) and industrial capability risk identified pursuant to DCMA-MAN 3401-01, "Industrial Base Assessment."

k. Safeguard DIB Mission Risk Management data integrity and security by:

(1) Maintaining IAG personnel security clearances, classified infrastructure, and CUI controls (in accordance with DoD Manual 5200.48 necessary to perform DIB Mission Risk Management functions.

(2) Ensuring position descriptions and position requirements documents define appropriate security clearance levels in order for assigned personnel to perform required job duties associated with DIB Mission Risk Management products.

(3) Maintaining classified (SECRET and TOP SECRET) information processing environments and database(s) to coordinate strategic mission risk management actions among stakeholders.

l. Conduct DIB Mission Risk Management outreach and site visits with DCMA, DoD, Federal, state, local, and industry partners to inform communities of DIB MA, promote risk management action coordination, validate assumptions and risk management recommendations, and expedite risk management activities.

2.4. HEADQUARTERS COMPONENT HEADS AND CAPABILITY BOARD MANAGERS.

Headquarters component heads and capability board managers must:

a. Ensure component or capability is aware of the risk management requirements as outlined in this manual and are resourced to respond.

b. Support IAG Director's efforts to identify alternate sources of supply by leveraging corporate knowledge of industrial capabilities in Area of Responsibility (AOR).

c. Where higher-than-acceptable risk ratings at prioritized, DIB facilities are reported for contract administration functions (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations) pursuant to DCMA-MAN 3401-03, recommend risk management actions to IAG for RMP integration.

d. Define and develop enterprise data analytic requirements for agency internal health metrics to include compliance thresholds.

2.5. EXECUTIVE DIRECTORS, DIRECTORS, AND COMMANDERS, COMMANDS.

Command executive directors, directors, and commanders must:

a. Ensure contract management offices (CMOs) are aware of the risk management requirements as outlined in this manual and are resourced to respond.

b. Facilitate subordinate CMO support of DIB Mission Risk Management products, assigning action officers as needed.

c. Implement the procedures in this manual to the maximum extent possible for Special Access Programs and Sensitive Compartmented Information contracts managed by the Director, Special Programs.

d. Accept and manage DIB MA Mission Risk Management responsibilities, delegating authority as needed.

2.6. COMMANDERS AND DIRECTORS, CMO.

CMO commanders and directors must:

a. Support IAG Director's efforts to identify alternate sources of supply by leveraging corporate knowledge of industrial capabilities in AOR. During Important Capabilities List review, pursuant to DCMA-MAN 3401-02, identify potential alternate sources to IAG.

b. Maintain open communication with prioritized DIB facilities in AOR under assessment (see DCMA-MAN 3401-03) and monitoring (see DCMA-MAN 3401-05). Report existing facility risk management plans and ongoing risk management actions to IAG for integration into RMP development.

c. Where higher-than-acceptable risk ratings at prioritized, DIB facilities are reported for contract administration functions (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations) pursuant to DCMA-MAN 3401-03, identify contractual requirements that may address facility vulnerabilities and recommend risk management actions to IAG for RMP integration.

d. Accept and manage DIB MA Risk Management responsibilities, delegating authority as needed.

e. Review and act on agency internal health metrics.

2.7. DIRECTOR, COST AND PRICING CENTER, FINANCIAL CAPABILITY TEAM (FCT).

The FCT Director must recommend risk management actions to IAG for RMP integration where higher-than-acceptable financial risk ratings are reported for prioritized DIB assets pursuant to DCMA-MAN 3401-03.

2.8. DIRECTOR, TECHNICAL DIRECTORATE, SAFETY CENTER.

The Safety Center Director must recommend risk management actions to IAG for RMP integration where higher-than-acceptable facility safety risk ratings are reported for prioritized DIB assets pursuant to DCMA-MAN 3401-03.

2.9. DIRECTOR, CHIEF OF STAFF, SECURITY DIVISION.

The Security Division Director must recommend risk management actions to IAG for RMP integration where higher-than-acceptable facility security risk ratings are reported for prioritized DIB assets co-located with a resident CMO pursuant to DCMA-MAN 3401-03.

SECTION 3: PROCEDURES

3.1. IDENTIFYING POTENTIAL ALTERNATE SOURCES OF SUPPLY.

Proactively identify options to remediate perceived DIB single points of failure. Determining potential alternate sources of supply is a required DIB MA MEF output task.

a. Leverage IBA (DCMA-MAN 3401-01), DIB CAIP (DCMA-MAN 3401-02), and/or customer input to ascertain single, sole, or strategic multi-source DIB suppliers.

b. Conduct market research and integrate agency and stakeholder partner input to identify potential alternate sources with requisite industrial capabilities and record findings in the agency repository of defense industry data. IAG developed tools will be used to track data collection requirements.

c. Determine time, cost, and note any barriers to qualify alternative supplier(s).

d. Report to stakeholders and record in the agency repository of defense industry data linked on the Resource Page for this manual.

e. The IAG uses standard templates with clearly marked classification and distribution statements and performs a peer/supervisor review to ensure there is no unauthorized disclosure of classified or CUI.

3.2. FACILITATING DIB RISK MANAGEMENT PLANS.

In accordance with DoD Instruction 3020.45, RMPs must be prepared for all prioritized critical infrastructure assets within 180 days of MAA report completion. IAG must support DIB SSA in the development of RMPs for prioritized DIB assets with higher-than-acceptable risk as determined by MAA (DCMA-MAN 3401-03).

a. Collect and consolidate recommended risk management actions from assessment stakeholders, including those DCMA components and capabilities identified in Section 2 of this manual, that identified higher-than-acceptable risk during DIB Mission Risk Assessment (DCMA-MAN 3401-03). IAG developed tools will be used to track data collection requirements.

b. Synchronize recommended actions with DoD risk management programs and interagency stakeholders to determine overlap with existing actions and identify gaps.

c. Coordinate with cognizant CMO to identify existing contractual requirements that may address facility vulnerabilities and record any ongoing facility-level risk management actions.

d. Identify potential alternate suppliers with comparable industrial capabilities via the agency repository of defense industry data and other available data sources. Validate alternate supplier industrial capability information via cognizant CMO(s) and DoD partners.

e. Prioritize risk management actions taking into account resource limitations and residual mission impacts and identify OPR.

f. Where risk acceptance is recommended, confirm with mission owners and asset owners and elevate to appropriate authority via the MACB.

g. Support MACB decision briefings on RMPs for prioritized DIB assets, as required.

h. Communicate RMP to stakeholders (e.g., DoD Components, Joint Staff, Combatant Commands, Program Offices, interagency partners, industry asset owners) via JIBWG, other MA forums, office calls, etc.

i. The IAG uses standard templates with clearly marked classification and distribution statements and performs a peer/supervisor review to ensure there is no unauthorized disclosure of classified or CUI.

3.3. SUPPORTING DoD DIB RISK MANAGEMENT PROGRAMS.

DoD Components and interagency partners execute existing programs to manage DIB risk. A selection of programs, their OPRs, and purpose are provided on this manual's Resource Page.

a. Validate industrial capability risk to support proposed risk management actions. As part of the validation, synchronize input from the other DIB MA processes highlighted in Table 1. IAG developed tools will be used to track data collection requirements.

Table 1. Other DIB MA Process Inputs to DIB Risk Management

Process	Input to Validation
Industrial Base Assessment (DCMA-MAN 3401-01)	Industrial Capability Risk and Potential Alternate Sources of Supply
DIB CAIP (DCMA-MAN 3401-02)	Facility and Industrial Base Criticality
DIB Mission Risk Assessment (DCMA-MAN 3401-03)	Mission Risk and Facility Vulnerabilities
DIB Monitoring and Reporting (DCMA-MAN 3401-05)	Existing Risk Management Actions and Risk Trends

b. Recommend risk management actions to mitigate or remediate validated industrial capability risk. Identify alternate courses of action to address the highest priority risks. Record findings in the agency repository of defense industry data and report findings to DoD risk management program customer.

c. Document risk management action implementation (see Paragraph 3.4.).

d. The IAG uses standard templates with clearly marked classification and distribution statements and performs a peer/supervisor review to ensure there is no unauthorized disclosure of classified or CUI.

3.4. DOCUMENTING DIB RISK MANAGEMENT ACTION IMPLEMENTATION.

a. Collect and integrate facility-level DIB risk management input from CMOs for prioritized DIB facilities and DIB risk management program actions from stakeholder OPRs. IAG developed tools will be used to track data collection requirements.

b. Document DIB risk management actions, OPR, and timeline in the agency repository of defense industry data.

c. Track execution of DIB risk management actions with cognizant CMO assistance and in accordance with DCMA-MAN 3401-05. IAG developed tools will be used to track data collection requirements.

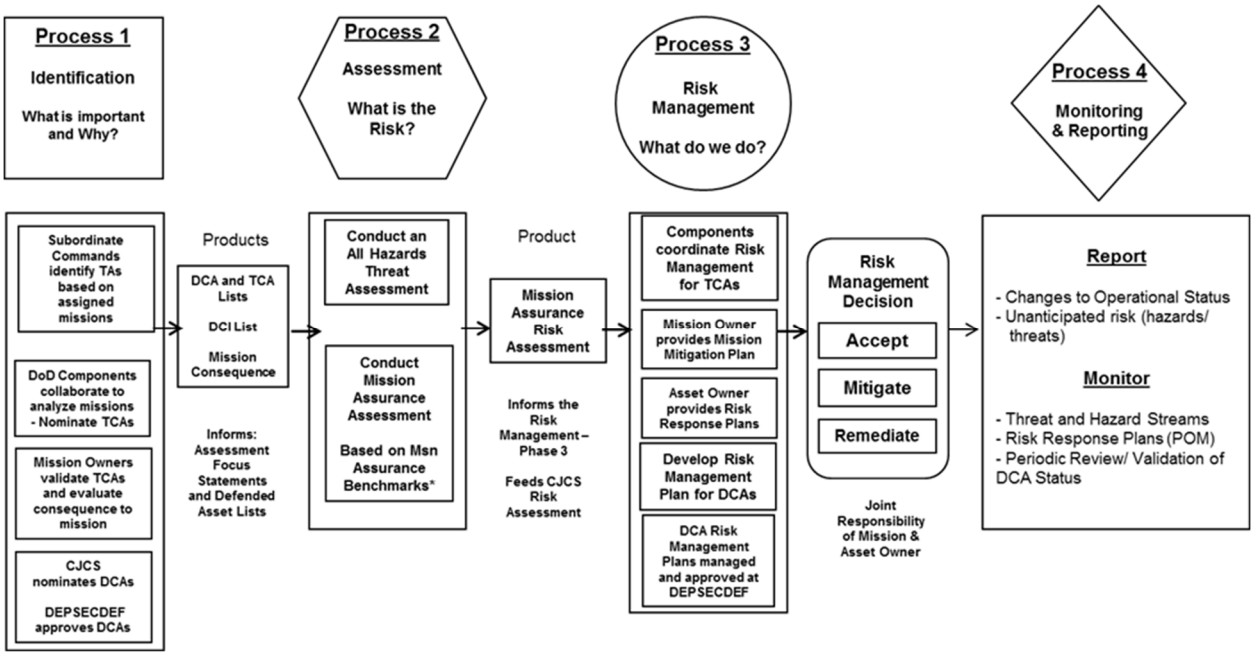
d. Reflect risk management actions in follow-on DIB MA CAIP (DCMA-MAN 3401-02) and Mission Risk Assessment (DCMA-MAN 3401-03) activities. If the risk management actions are effective, the result should be decreased Defense Critical Mission risk either by reduced asset criticality or decreased probability of disruption.

SECTION 4: GENERAL PRINCIPLES

4.1. DoD MISSION ASSURANCE.

MA seeks to prioritize DoD's efforts and resources to address the most critical mission execution risks. To achieve comprehensive risk management, the MA construct synchronizes and integrates various existing DoD risk management programs and activities. The general processes within the DoD MA construct are identification, assessment, risk management, and monitoring and reporting. The relationship of these processes to one another is illustrated in Figure 1. In accordance with DCMA-INST 3401, DCMA applies the MA construct to evaluate the DIB sector.

Figure 1. DoD Mission Assurance Construct



4.2. DCMA DIB MISSION ASSURANCE.

In accordance with DCMA-INST 3401, DCMA IAG is assigned responsibility to identify, analyze, and assess the DIB supply chain network supporting DoD mission execution and assist other DoD Component efforts with DIB-related analysis. According to DCMA-INST 3401, DCMA executes DIB MA through six processes that integrate and expand upon the DoD MA construct: conduct IBAs; identify and prioritize DIB assets; assess DIB mission risk; manage DIB mission risk; execute DIB monitoring and reporting; and administer DIB MA industry outreach and awareness. DIB MA focuses on commercial and organic DIB asset risks that could impact the supply of mission essential goods or services required by the warfighter.

4.3. DIB RISK MANAGEMENT.

DIB Mission Risk Management relies on partnership strategies and mechanisms for addressing risk to non-DoD-owned infrastructure and critical industrial capabilities that support Defense Critical Missions.

a. The objective of the DIB Mission Risk Management process is to achieve acceptable risk levels for Defense Critical Missions by addressing identified vulnerabilities and managing issue response at critical DIB assets. The process requires a thorough understanding of DoD resource limits and available interagency means (e.g., programmatic, legislative, regulatory). MA risk management consists of elements of risk acceptance, mitigation, or remediation. Mitigation includes planning to quickly return critical assets to operational status, such as a prepositioned stockpile of unique industrial equipment spares, and contingency planning by mission owners devising alternative methods to continue mission execution, such as utilizing other weapon systems or platforms to execute the mission. Remediation focuses planning upon corrective actions to known TCA vulnerabilities by enhancing the security, protection, operations, resiliency, and/or redundancy to improve essential capability resilience.

b. The IAG executes DIB MA as a holistic risk management construct that is continuously analyzing the industrial base to identify, assess, manage, monitor and report potential mission risks. RMP implementation is at the discretion of the mission, asset, and/or risk management program owners and is constrained by available resources. Many of the assets DoD relies upon to execute its strategic missions are either owned or supported by entities outside of DoD, which presents unique risk management challenges. Accordingly, DoD may not be able to direct commercial industry asset owners to adopt all recommended risk management actions, as would be possible for DoD-owned infrastructure. To overcome some of these challenges, DCMA will partner with DoD, Federal, state, local, and industry stakeholders through the DIB SSA. Where unresolved critical industrial capability vulnerabilities result in unacceptable Defense Critical Mission risk, decisions will be elevated through the MACB to Deputy Secretary of Defense (DEPSECDEF) for ultimate resolution.

GLOSSARY

G.1. ABBREVIATIONS AND ACRONYMS.

ACRONYM	MEANING
AOR	Area of Responsibility
BCF	Business Capability Framework
CAIP	Critical Asset Identification and Prioritization
CCMD	Combatant Command
CMO	Contract Management Office
CONPLAN	Concept of Operation Plan
CUI	Controlled Unclassified Information
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DIB	Defense Industrial Base
DIB MA	Defense Industrial Base Mission Assurance
IAG	Industrial Analysis Group
IBA	Industrial Base Assessment
JIBWG	Joint Industrial Base Working Group
JMET	Joint Mission-Essential Task
MA	Mission Assurance
MAA	Mission Assurance Assessment
MACB	Mission Assurance Coordination Board
MEF	Mission Essential Function
OPLAN	Operational Plan
OPR	Office of Primary Responsibility
RMP	Risk Management Plan
SSA	Sector Specific Agency
TA	Task Asset
TCA	Task Critical Asset

GLOSSARY

G.2. DEFINITIONS.

TERM	MEANING
Asset	See "DIB Asset."
Assessment (risk)	A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.
Capability	Ability to achieve a desired effect under specified standards and conditions; involves a combination of ways and means across doctrine, organization, training, materiel, leadership and education, personnel, and facilities to perform a set of tasks to execute a specified course of action.
Capability (DCMA)	Organizational construct under the Business Capability Framework. Capabilities can be characterized as Primary, Integrating, or Enabling and have associated command and control structures to manage their respective area of responsibility.
Component (DCMA)	As defined in DCMA-MAN 4501-03, "Organization Structure, Mission and Functions."
Component Head (DCMA)	As defined in DCMA-MAN 4501-03.
Contract	Mutually binding legal relationship that obligates the seller to furnish supplies or services (including construction) and the buyer to pay for them. Includes all types of commitments that obligate the Government to an expenditure of appropriated funds that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements.
Contract Administration Service (CAS)	Pre-award and post-award actions accomplished for the benefit of the Government that are necessary for performance of a

	contract or in support of buying offices, system/project managers, and other organizations. Includes quality assurance, engineering support, production surveillance, pre-award surveys, mobilization planning, contract administration, property administration, industrial security and safety.
CMO	OU within DCMA assigned post-award functions related to contract administration. Office is responsible for managing and administering assigned contracts from contract receipt to contract closeout.
CUI	As defined in Title 32, Code of Federal Regulations.
Critical	Designation assigned to an essential capability, system, or asset without which a supported strategic mission would be significantly degraded or could not be executed.
Critical Infrastructure Information (CII)	Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems.
DCA	An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DoD to fulfill its missions.
DCI	The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of TCAs and DCAs.
DIB Asset	A distinguishable DIB entity (typically a contractor facility) that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.
Essential Capability	A mission owner-defined ability necessary to execute a mission essential task from a strategic mission. Mission owners, with support from appropriate resource providers, define essential capabilities during mission decomposition as tactical-level, Service or Defense Agency Universal Joint Task List tasks linked to those strategic national, strategic theater, or operational Universal Joint Task List mission essential tasks necessary to execute their strategic mission.
Force Management Risk	This area defines risks of sufficiently trained, equipped, and ready forces to meet operational requirements. Military

	Departments will assess and report force management risk related to their Title 10, United States Code, responsibilities.
Future Challenges Risk	This area defines risks to future objectives, capabilities, or capacities to address anticipated threats. These risks are addressed through the weapon system acquisition, reliability, and force management processes where the MA community works with other governance structures established to address these issues.
Hazards	Condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.
Infrastructure	The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.
Issue	Event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (probability = 1).
Institutional Risk	This area defines risks to organizational, operational, and process effectiveness in improving national defense. OSD and DoD Components will assess and report institutional risk related to their MEFs.
MA	A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition.
MEF	The specified or implied tasks required to be performed by, or derived from, statute, Executive Order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DoD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control.

Mission Essential Task (MET)	Tasks based on mission analysis and approved by the commander that are necessary, indispensable, or critical to the success of a mission.
Mitigation	Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure.
Operational Risk	This area defines risk to current military objectives as described in current, planned, or contingency operations. Combatant Commands (CCMDs) will assess and report operational risk related to campaign plans, operational plans (OPLANs), and concept of operation plans (CONPLANs).
Remediation	Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified.
Risk	Probability and severity of loss linked to threats or hazards and vulnerabilities. Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur.
Risk Management	A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. Risk management is composed of risk assessment and risk response. Risk management includes elements of risk acceptance, mitigation, and remediation.
Stakeholder	Any group or organization with a responsibility or influence directly related to the outcome of an action or result; can affect the outcome or are the recipient of the results.
TA	An asset that provides a service or capability for mission execution but for which the loss of the asset will not severely degrade or fail mission execution of a DoD or OSD Component-level MEF or CCMD OPLAN, CONPLAN, or core JMET.
TCA	An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or mission-essential task it supports. TCAs are used to identify DCAs.

TCA Tier 1	An asset whose loss, incapacitation, or disruption would result in mission failure at the DoD Component level of a MET or essential capability aligned with strategic missions.
Threat	An adversary having the intent, capability, and opportunity to cause loss or damage.

REFERENCES

Code of Federal Regulations, Title 32
DCMA Instruction 3401, "Defense Industrial Base Mission Assurance," August 29, 2018, as amended
DCMA Manual 3401-01, "Industrial Base Assessment," December 17, 2018, as amended
DCMA Manual 3401-02, "Defense Industrial Base Critical Asset Identification and Prioritization," September 14, 2018, as amended
DCMA Manual 3401-03, "Defense Industrial Base Mission Risk Assessment," December 20, 2018, as amended
DCMA Manual 3401-05, "Defense Industrial Base Monitoring and Reporting," November 30, 2018, as amended
DCMA Manual 4501-03, "Organization Structure, Mission and Functions," April 3, 2019
DCMA Memorandum 17-072, "Agency Mission Essential Functions," April 27, 2017
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013, as amended
DoD Directive 3020.40, "Mission Assurance," November 29, 2016, as amended
DoD Instruction 3020.45, "Mission Assurance (MA) Construct," August 14, 2018, as amended
DoD Manual 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020
National Security Memorandum-22, "Critical Infrastructure Security and Resilience," April 30, 2024
Under Secretary of Defense Memorandum "Defense Contract Management Agency Mission Changes," May 20, 2019
United States Code, Title 10