DCMA Manual 3401-03
Defense Industrial Base Mission Risk Assessment

Office of Primary Responsibility:	**Acquisition Insight Capability Board**
Effective:	December 20, 2018
Change 1 Effective:	March 18, 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/3401-03.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 Instruction 3401, "Defense Industrial Base Mission Assurance":

- Assigns responsibilities, describes procedures, and provides guidance associated with the Defense Industrial Base Mission Risk Assessment process
- 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

SECTION 1: GENERAL ISSUANCE INFORMATION 3
1.1. Applicability. 3
1.2. Policy. 3
1.3. Records Management. 3
1.4. Overview. 4
1.5. Summary of Changes. 4
APPENDIX 1A. DCMA 3401-03 RECORDS 5
SECTION 2: RESPONSIBILITIES 6
2.1. Executive Director, Enterprise Analytics aND Modernization. 6
2.2. Director, Operational Analytics and Integration Center. 6
2.3. Director, Industrial Analysis Group. 6
2.4. Headquarters Component Heads and Capability Board Managers. 7
2.5. Commanders, Executive Directors, and Directors, Commands. 8
2.6. Commanders and Directors, CMO. 8
2.7. Director, Cost and Pricing Center, Financial Capability Team (FCT). 9
2.8. Director, Technical Directorate, Safety Center. 9
2.9. Director, Security Division. 9
SECTION 3: PROCEDURES 10
3.1. MAA Program Support. 10
3.2. DIB All Hazard Threat Assessment. 10
3.3. DIB MAA. 11
3.4. DIB Sector Assessments. 13
3.5. Reporting Risks to Stakeholders. 14
SECTION 4: GENERAL PRINCIPLES 15
4.1. DoD Mission Assurance. 15
4.2. DCMA DIB Mission Assurance. 15
4.3. DIB Mission Risk Assessment. 16
4.4. DIB Mission Risk Management. 16
GLOSSARY 17
G.1. Abbreviations and Acronyms. 17
G.2. Definitions. 18
REFERENCES 22

FIGURES

Figure 1. Mission Assurance Construct 15

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 the Defense Industrial Base (DIB) Mission Risk Assessment as identified in Section 2 of this manual.

1.2. POLICY.

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

a. Assess risk to prioritized DIB assets and industrial capabilities supporting strategic defense missions (e.g., Defense Critical Missions as defined by Chairman of the Joint Chiefs of Staff (CJCS)).

b. Determine strategic mission risk and report risk to mission owner(s) and other stakeholders, as required and as permitted by law, to facilitate risk management activities.

c. Support CJCS Mission Assurance Assessment Program (MAAP) requirements.

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

e. Deliver value-added DIB insight and share DIB Mission Risk Assessment analytical 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.

f. 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.

g. 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 supporting 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 the DCMA 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 Assessment process is to assess threats and hazards, determine disruption probability, and evaluate ultimate strategic mission risk for prioritized DIB assets and at-risk DIB sectors. Within the DIB MA capability construct, DIB Mission Risk Assessment differs from IBA (DCMA-MAN 3401-01) in its scope, which is operational mission-centric and determines risk to strategic defense missions. DIB Mission Risk Assessment activities largely focus on a single, prioritized, mission-critical asset. IBA is characteristically acquisition program-centric and determines risk to supporting industrial capabilities.

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 3401-03 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	DoD365	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 the DIB Mission Risk Assessment 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 Assessment functions.

c. Share DIB Mission Risk Assessment analytical products with the Agency Senior Leadership Team, as needed.

d. Resource DIB site visits to conduct outreach, assess threats/hazards and vulnerability, and verify and validate facility level industrial capability information for prioritized DIB assets.

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, INDUSTRIAL ANALYSIS GROUP.

The IAG Director must:

a. Serve as the agency OPR for DIB Mission Risk Assessment.

b. Prioritize DIB Mission Risk Assessment workload in accordance with DCMA-MAN 3401-02, “Defense Industrial Base Critical Asset Identification and Prioritization.”

c. Provide necessary DIB subject matter experts (SMEs) to support the Joint Staff MAAP including DoD Component Mission Assurance Assessments (MAA), Joint Mission Assurance Assessments (JMAA), and Balanced Survivability Assessments (BSA), as required.

d. Contribute to DIB-specific MAAP methodology development.

e. Lead DIB All Hazard Threat Assessment (AHTA) for all DIB Task Critical Assets (TCAs). Coordinate a supporting cross-functional team for each assessment.

f. Lead DIB MAA on DIB Tier 1 TCAs and DIB Defense Critical Assets (DCAs). Coordinate a supporting cross-functional team for each assessment.

g. Conduct DIB sector assessments.

h. Partner with DCMA (e.g., those identified in Section 2 of this manual), DoD, Federal, state, local, and commercial entities, as appropriate and as permitted by law, to identify threats and hazards that could result in industrial capability and, ultimately, strategic mission disruption. Leverage and integrate available data from all sources and all MA-related programs and activities to reduce redundancy and provide a more complete risk picture.

i. Report risk to mission owner(s), asset owner(s), CJCS, the DIB SSA, and other stakeholders as required to facilitate risk management activities. Submit DIB AHTA and DIB MAA to the DoD MA system of record upon completion.

j. Notify agency stakeholders with oversight, responsibility, or other significant interest of risk to DIB TCA facilities (e.g., Contract Management Office (CMO) with contract administration responsibility at the prioritized DIB asset).

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

(1) Maintaining IAG personnel security clearances, classified infrastructure, and CUI controls (in accordance with DoD Manual Instruction 5200.48, “Controlled Unclassified Information (CUI)”) necessary to perform DIB Mission Risk Assessment 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 Assessment products.

(3) Maintaining classified (SECRET and TOP SECRET) information processing environments and database(s) to communicate strategic mission risks to stakeholders including DCMA commands.

l. Conduct DIB Mission Risk Assessment outreach and site visits with DCMA, DoD, Federal, state, local, and industry partners to inform communities of DIB MA, assess facility level threats/hazards and determine vulnerability, verify and validate facility level industrial capability information, and expedite risk management activities.

2.4. HEADQUARTERS COMPONENT HEADS AND CAPABILITY BOARD MANAGERS.

Headquarters component heads and capability managers must:

a. Maintain awareness of prioritized DIB assets in accordance with the DIB Critical Asset Identification and Prioritization (CAIP) Manual (DCMA-MAN 3401-02).

b. Accept and manage requests for DIB data in support of DIB Mission Risk Assessment products and assign action officers as needed. A list of Baseline Elements of Information (BEIs) is available on the Resource Page of this manual. DCMA data that would contribute to an integrated facility risk evaluation includes high risk ratings and supporting data as determined during contract administration functions (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations).

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

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

Command executive director, directors, and commanders must:

a. Maintain awareness of prioritized DIB assets and notify responsible CMOs of TCAs in accordance with the DIB CAIP Manual (DCMA-MAN 3401-02).

b. Facilitate DIB data requests to subordinate CMO in support of DIB Mission Risk Assessment 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 or Commander, Special Programs.

2.6. COMMANDERS AND DIRECTORS, CMO.

CMO commanders and directors must:

a. Maintain awareness of prioritized DIB assets in accordance with the DIB CAIP Manual (DCMA-MAN 3401-02).

b. Accept and manage requests for DIB data in support of DIB Mission Risk Assessment products and assign action officers as needed. A list of BEIs is available on the Resource Page of this manual. DCMA data that would contribute to an integrated facility risk evaluation includes higher-than-acceptable risk ratings and supporting data as determined during contract administration functions (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations).

c. Maintain open communication with and surveillance of DIB TCAs in Area of Responsibility (AOR) to provide valuable local insight during an assessment. Open communication includes, but is not limited to site visits, attendance to meetings, town halls, and fostering relationships with private sector companies that fall within the CMOs AOR.

d. Review and act on agency internal health metrics.

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

The FCT Director must:

a. Maintain awareness of prioritized DIB assets in accordance with the DIB CAIP Manual (DCMA-MAN 3401-02).

b. Accept and manage requests to support DIB Mission Risk Assessment products.

c. Survey prioritized DIB asset population to capture facility and parent company historical and forecasted financial data for financial analysis. Coordinate survey with DCMA IAG to ensure efficiency and avoid overburdening industry.

d. Evaluate facility financial risk in accordance with FCT internal operating procedures. Provide facility financial risk ratings and associated financial reports to IAG for assessment integration. Include a general methodology description with the report.

2.8. DIRECTOR, TECHNICAL DIRECTORATE, SAFETY CENTER.

The Director, Safety Center must:

a. Maintain awareness of prioritized DIB assets in accordance with the DIB CAIP Manual (DCMA-MAN 3401-02).

b. Accept and manage requests to support DIB Mission Risk Assessment products.

c. Evaluate DIB facility safety risk and provide threat, hazard, vulnerability, and probability of disruption to IAG for assessment integration.

2.9. DIRECTOR, SECURITY DIVISION.

The Director, Security Division must:

a. Maintain awareness of prioritized DIB assets in accordance with the DIB CAIP Manual (DCMA-MAN 3401-02).

b. Accept and manage requests to support DIB Mission Risk Assessment products.

c. Provide threat, hazard, vulnerability, and probability of disruption to IAG for assessment integration where priority DIB asset under evaluation is co-located with a resident CMO, evaluate DIB facility security risk (e.g., Antiterrorism and Physical Security).

SECTION 3: PROCEDURES

3.1. MAA PROGRAM SUPPORT.

Pursuant to DoD policy, DoD components will lead MA assessments during MA construct execution. DCMA will provide necessary DIB SMEs to support the Joint Staff MAAP. DCMA will:

a. Evaluate Joint Staff MAAP schedule and nominate assessments with potential DIB equity annually.

b. Coordinate with Joint Staff and DoD Components for participation on assessments with potential DIB equity.

c. Provide DIB SMEs to support assessments, as requested.

d. Participate in assessment planning and pre-assessment site visit, as required.

e. Provide dependency analysis and identify DIB-specific threats, hazards, and vulnerabilities (e.g., single points of failure). Leverage available IBA data (DCMA-MAN 3401-01) and criticality determination from the DIB CAIP process (DCMA-MAN 3401-02). IAG developed tools will be used to track data collection requirements.

f. Accompany assessment team on site visit to verify and validate threat, hazard, vulnerability, DIB dependency and industrial capability information.

g. Update DIB-specific assessment with data gathered from site visit.

h. Write DIB-specific report annex and deliver to assessment lead.

i. Participate in risk management plan development, as required. See DCMA-MAN 3401-04, "Defense Industrial Base Mission Risk Management."

j. 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 controlled unclassified information (CUI).

3.2. DIB ALL HAZARD THREAT ASSESSMENT.

The AHTA provides a baseline of known hazards and threats at an asset (e.g., DIB facility) based on the likelihood that the hazard or threat may occur. Probability of occurrence is based on historical data, prevailing environmental conditions, and detailed intelligence analysis. The AHTA will consider the historical frequency and a range of likely intensity for the particular threat or hazard, when applicable. DCMA will:

a. Leverage DIB CAIP outputs (DCMA-MAN 3401-02) to prioritize assets.

b. Assemble and coordinate a cross-functional team from MA-related programs to provide a complete risk picture.

c. Identify and describe facility level threats and hazards and evaluate the likelihood of occurrence for each. Leverage all available data sources by contacting DCMA, DoD, Federal, state, local, and industry partners. For most threats, and some hazards, precise probability data are not available. In this case, assessors will assign relative probability (e.g., low, moderate, significant, and high) pursuant to Joint Staff MAA Concept of Operations. IAG developed tools will be used to track data collection requirements.

d. Contact local representatives and/or perform a site visit to gather local-level threat/hazard information.

e. Write DIB AHTA report.

f. Post completed DIB AHTA to the CJCS MA database of record while abiding by all appropriate information security requirements.

g. 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. DIB MAA.

The DIB MAA considers asset criticality, assesses threats and hazards, determines disruption probability, and evaluates ultimate strategic mission risks for prioritized DIB assets. DCMA will:

a. Leverage DIB CAIP outputs (DCMA-MAN 3401-02) to prioritize assets.

b. Assemble and coordinate a cross-functional team from MA-related programs to provide a complete risk picture.

c. Assess vulnerability to AHTA-identified threats and hazards taking into consideration resilience, accessibility, recognition, ongoing risk management actions, and cascading effects. IAG developed tools will be used to track data collection requirements.

d. Consider the compilation of threats, hazards and associated vulnerabilities to determine disruption probability for all threats/hazards and rank order them to prioritize risk drivers. Additionally, estimate time to mission impact.

e. Evaluate disruption probability against loss-consequence from the DIB CAIP process (DCMA-MAN 3401-02) to derive industrial capability risk (i.e. facility disruption risk) and risk

to the supported strategic mission(s). Assign a strategic mission risk rating of Low, Moderate, Significant, or High according to Joint Staff MAA Concept of Operations.

(1) Low.

Current situation should not impact assigned missions.

(2) Moderate.

Current situation may degrade mission capability, but considerable ability for mission execution remains.

(3) Significant.

Current situation may significantly degrade mission capability leaving diminished ability to execute assigned missions.

(4) High.

Current situation will likely cause mission failure or result in a marginal capability to execute assigned missions.

f. Group risks, if applicable, according to the below categories described in DoDI 3020.45, in order to align with CJCS Joint Risk Analysis (CJCS Manual 3105.01).

(1) Operational Risk.

This area defines risks to current military objectives as described in current, planned, or contingency operations. Combatant Commands (CCMDs) will assess and report operational risks related to campaign plans, operational plans (OPLANs), and concept of operation plans (CONPLANs).

(2) 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.

(3) 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.

(4) 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.

g. Write DIB MAA report. The MAA report is comprised of three distinct supporting elements: the criticality assessment, the AHTA, and vulnerability assessment. Together, these three elements combine to estimate mission risks and provide context to localized issues that may have broader implications to mission accomplishment.

h. Post completed DIB MAA to the CJCS MA database of record while abiding by all appropriate information security requirements.

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.

3.4. DIB SECTOR ASSESSMENTS.

DIB sector assessments will identify macro-sector or sub-sector risk trends that may impact TCAs or DCMs. DCMA will:

a. Based on input from the IBA process (DCMA-MAN 3401-01) and/or DIB Monitoring and Reporting process (DCMA-MAN 3401-05), determine if TCAs common to a sector could be impacted by broader threat/hazard trends.

b. If TCAs within a DIB sector or sub-sector will be impacted, initiate a DIB sector assessment.

c. Integrate data from other components within DCMA (e.g., those identified in Section 2 of this manual), DoD, Federal, state, local, and industry partners. IAG developed tools will be used to track data collection requirements.

d. Conduct a trend analysis to determine likelihood of disruption.

e. Evaluate disruption probability against loss-consequence from the DIB CAIP process (DCMA-MAN 3401-02) to identify ultimate risk to strategic missions.

f. Write DIB sector assessment report.

g. Post completed DIB sector assessment to the CJCS MA database of record while abiding by all appropriate information security requirements.

h. 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.

3.5. REPORTING RISKS TO STAKEHOLDERS.

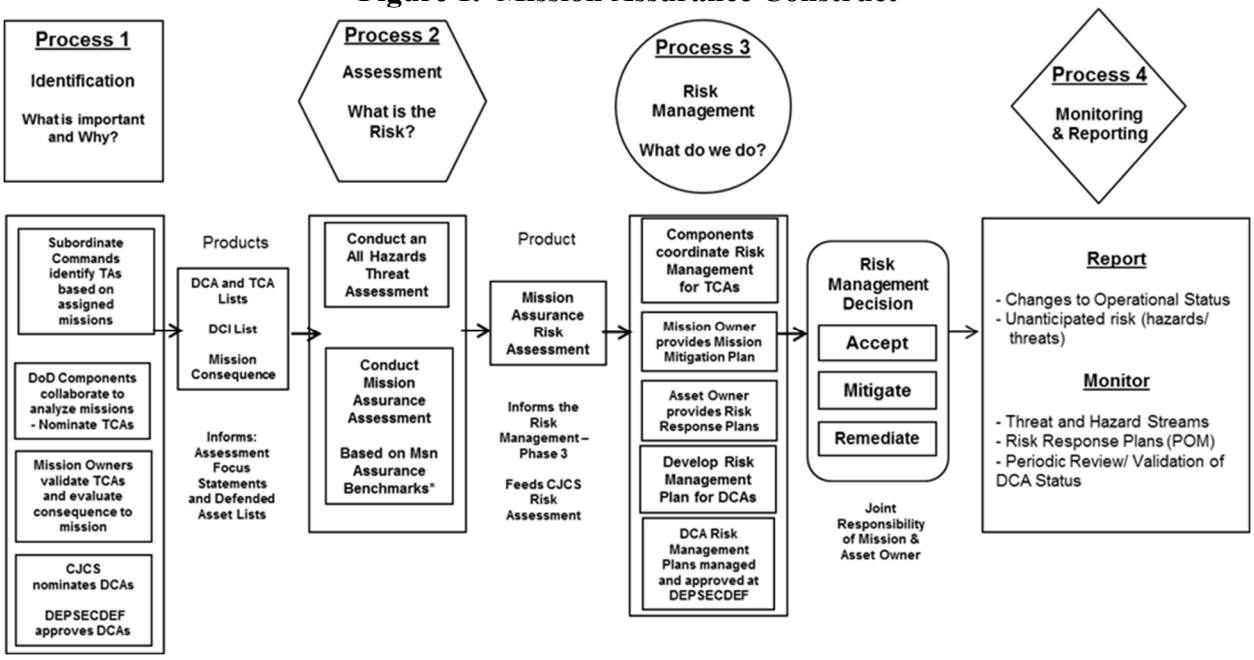
DCMA will report most-probable threats/hazards, industrial capability and mission risk, as well as recommended risk management actions to mission owner(s), asset owner(s), CJCS, the DIB SSA, risk management program offices, cognizant DCMA CMO, and other stakeholders as required to facilitate risk management activities (see DCMA-MAN 3401-04 for details on DIB risk management).

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. 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 mission assurance 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 MISSION RISK ASSESSMENT.

The goal of the MA assessment process is to quantify the probability of risk to assets, systems, and essential capabilities supporting strategic missions by integrating the various MA-related programs and activities through a holistic approach. The assessment process is composed of:

a. Identifying threat and hazard damage mechanisms capable of causing harm to (i.e., disrupting) the asset or system supporting the mission-essential capability, along with assessing the likelihood of these events occurring. This assessment is conducted at the local level through AHTA. AHTA results will be stored in the MA system of record.

b. Identifying vulnerabilities related to assessed threats and hazards, but with adjustments based on asset, system, or capability resilience, accessibility, recognition, and cascading effects. This is accomplished through either the CJCS or DoD Component-led MA assessment, and by local-level self-assessments. All MAAP assessments will be conducted in accordance with supplemental CJCS guidance, and results will be stored in the MA system of record.

c. Evaluating the compilation of threats, hazards and associated vulnerabilities to assign a probabilistic risk rating to the asset, system, or capability and the strategic mission(s) it supports. The calculated mission risk rating and estimated time to mission impact provides a basis for risk management prioritization.

4.4. DIB MISSION RISK MANAGEMENT.

The DIB Mission Risk Assessment process is completed when the DIB asset's potential risk has been analyzed and a mission risk rating has been determined. The follow-on step in the DIB MA construct is to perform the DIB Mission Risk Management process which is addressed in DCMA-MAN 3401-04.

GLOSSARY

G.1. ABBREVIATIONS AND ACRONYMS.

ACRONYM	MEANING
AHTA	All Hazard Threat Assessment
AOR	Area of Responsibility
BCF	Business Capability Framework
BEI	Baseline Element of Information
CAIP	Critical Asset Identification and Prioritization
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CMO	Contract Management Office
CONPLAN	Concept of Operation Plan
CUI	Controlled Unclassified Information
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DCM	Defense Critical Mission
DCMA-INST	DCMA Instruction
DCMA-MAN	DCMA Manual
DIB	Defense Industrial Base
FCT	Financial Capability Team
IAG	Industrial Analysis Group
IBA	Industrial Base Assessment
MA	Mission Assurance
MAAP	Mission Assurance Assessment Program
MEF	Mission Essential Function
OPLAN	Operational Plan
OPR	Office of Primary Responsibility
SSA	Sector Specific Agency
SME	Subject Matter Expert
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
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.
Criticality	A metric used to describe the consequence of loss of an asset, based on the effect the incapacitation, destruction, or loss of the asset would have on a DoD acquisition program or DoD operations.

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 task critical assets and DCAs.
Defense Industrial Base 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.
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 DoD'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.
Mission Owner	The OSD or DoD Component with responsibility for the execution of all or part of a mission assigned by statute or the Secretary of Defense.
Operational Risk	This area defines risk to current military objectives as described in current, planned, or contingency operations. CCMDs will assess and report operational risk related to campaign plans, OPLANs, and 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

Chairman of the Joint Chiefs of Staff Manual 3105.01, "Joint Risk Analysis," October 14, 2016
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 Assessments," December 17, 2018, as amended
DCMA Manual 3401-02, "Defense Industrial Base Critical Asset Identification and Prioritization," September 14, 2018, as amended
DCMA Manual 3401-04, "Defense Industrial Base Mission Risk Management," January 13, 2019, as amended
DCMA Manual 3401-05, "Defense Industrial Base Mission 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 26, 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