DCMA Manual 3401-05

Defense Industrial Base Monitoring and Reporting

Office of Primary Responsibility	**Integrating Capability – Defense Industrial Base Mission Assurance**
Effective:	December 6, 2018
Change 1 Effective	December 22, 2020
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 3401, "Defense Industrial Base Mission Assurance," August 29, 2018
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/DIB/SitePages/3401-05r.aspx
Approved by:	David H. Lewis, VADM, USN, Director
Change 1 Approved by:	David G. Bassett, LTG, USA, Director

Purpose: In accordance with the authority in DoD Directive 5105.64, this issuance:

- Implements policy established in DCMA Instruction 3401
- Assigns responsibilities, describes procedures, and provides guidance associated with the Defense Industrial Base Monitoring and Reporting process
- Implements Agency national Defense Industrial Base sector Mission Assurance responsibilities pursuant to DoD Directive 3020.40, DoD Instruction 3020.45, Presidential Policy Directive PPD-21, and related issuances

SUMMARY OF CHANGES

This Manual has substantive changes. The most notable change is in Section 3, “Procedures,” which now includes information related to key process controls (e.g., standard templates, supervisor reviews).

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA Operational Units (OU) as well as DCMA components and capabilities that contribute to Defense Industrial Base (DIB) Monitoring and Reporting as identified in Section 2 of this Manual.

1.2. POLICY. This Manual provides guidance to the DCMA workforce responsible for executing DIB Monitoring and Reporting activities, defines high-level roles, and delineates responsibilities for the various DCMA components and capabilities. It is DCMA policy to:

a. Monitor and report DoD strategic mission execution risk (mission risk) resulting from industrial capability risk. With worldwide presence and access to industrial facilities, DCMA is uniquely positioned to monitor and report on impending threats and hazards that threaten critical DIB asset operational readiness. Therefore, DCMA will maintain situational awareness of strategic mission risk through DIB threat and hazard monitoring, DIB operational reporting, and DIB risk management action tracking.

b. Perform DIB Monitoring and Reporting 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).

c. Deliver value-added DIB insight and share Monitoring and Reporting 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.

d. Safeguard business sensitive and proprietary DIB data, controlled unclassified information (CUI), protected critical infrastructure information (PCII), and classified material routinely gathered or developed in the execution of DIB Monitoring and Reporting.

e. Execute this Manual in a safe, efficient, effective, and ethical manner.

1.3. 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 Division (IAD) is the DIB MA Office of Primary Responsibility (OPR) per 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 IAD 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 goal of the DIB Monitoring and Reporting process is to maintain real-time situational awareness of DIB risk in support of DoD strategic missions. The Monitoring and Reporting process consists of threat/hazard monitoring, operational readiness reporting, and risk management action tracking. Maintaining vigilant insight into the many suppliers that provide critical industrial capabilities ensures the continued function and resilience of DoD mission execution.

SECTION 2: RESPONSIBILITIES

2.1. EXECUTIVE DIRECTOR, PORTFOLIO MANAGEMENT AND BUSINESS INTEGRATION. The Portfolio Management & Business Integration (PM&BI) Executive Director must:

a. Ensure continued execution of DCMA DIB MA MEF.

b. Ensure the DIB Monitoring and Reporting process is sufficiently resourced, integrated within the Agency and can be executed under any operational condition.

c. Empower the IAD Director to take Agency-level action necessary to accomplish DIB Monitoring and Reporting functions.

d. Share DIB Monitoring and Reporting situational awareness and analytical products with the Agency Senior Leadership Team, as needed.

2.2. DIRECTOR, INDUSTRIAL ANALYSIS DIVISION. The IAD Director must:

a. Serve as the Agency OPR for DIB Monitoring and Reporting.

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

c. Pursuant to DoD Directive 3020.40, partner with DCMA, DoD, Federal, state, local, and commercial entities, as appropriate and as permitted by law, to monitor and report industrial capability risk that may result in DoD mission risk.

d. Maintain active DIB situational awareness by communicating with government and private industry stakeholders while leveraging Agency, DoD, Federal Government, and publicly available data.

e. Monitor impending threats or hazards (e.g., natural disasters, industrial accident, mergers and acquisitions, bankruptcy, or other reportable event as further defined within this Manual's Resource Page) to prioritized DIB assets as determined by the DIB Critical Asset Identification and Prioritization (CAIP) process (DCMA Manual (DCMA-MAN) 3401-02) and report potential DIB impacts to interagency stakeholders to support risk management activities (DCMA-MAN 3401-04, "Defense Industrial Base Mission Risk Management").

f. Analyze DCMA situational reports (see DCMA-MAN 3301-01, "Agency Mission Assurance Construct," and its associated Resource Page) to identify issues impacting DIB facilities.

g. Deliver stakeholder reports detailing DIB facility impacts. Criteria for reportable issues specific to DIB assets can be found on the DIB Monitoring and Reporting Manual's Resource Page.

h. Track DIB risk management actions and monitor resulting change to risk over time (e.g., risk reduction) at prioritized DIB assets.

i. Prepare and distribute DIB Monitoring and Reporting products to Agency and external stakeholders to facilitate risk management activities while maintaining strict levels of information security. Perform an internal review for accuracy, content, and security before distribution.

j. Report DIB readiness and changes to operational status for prioritized DIB assets via the DoD system of record and participate in Agency Crisis Action Team (CAT) events if DIB assets may be impacted.

k. Identify areas for proactive DIB assessment to support related processes for Industrial Base Assessments (IBA) (DCMA-MAN 3401-01) and DIB Mission Risk Assessments (DCMA-MAN 3401-03).

l. Conduct macro DIB sector assessments to identify sector risk trends.

m. When necessary, coordinate threat or hazard events with the Agency Mission Assurance Group, which will evaluate for Agency impacts.

n. Safeguard DIB Monitoring and Reporting data integrity and security by:

(1) Maintaining IAD personnel security clearances, classified infrastructure, and CUI controls (in accordance with DoD Manual 5200.48, "Controlled Unclassified Information (CUI)") necessary to perform DIB Monitoring and Reporting 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 Monitoring and Reporting products.

(3) Maintaining classified (SECRET and TOP SECRET) information processing environments and database(s) to communicate impending strategic mission threats to prioritized DIB assets.

o. Conduct outreach and site visits with DCMA, DoD, Federal, state, local, and industry partners to inform communities of DIB MA and expedite risk management activities.

2.3. COMPONENT HEADS/CAPABILITY MANAGERS. Includes headquarters components, centers, and DCMA capability leads within the BCF. Component Heads and Capability Managers must:

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

b. Maintain Awareness of prioritized DIB assets in accordance with the DIB CAIP manual (DCMA-MAN 3401-02).

c. Report to the IAD prioritized DIB asset higher-than-acceptable risk ratings identified during contract administration function (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations).

2.4. COMMANDERS/DIRECTORS, OPERATIONAL UNITS. Includes International, Special Programs, and East, Central, and West regions. Operational Unit Commanders/ Directors must:

a. Ensure Contract Management Offices (CMOs) are aware of the risk monitoring and reporting requirements as outlined in this manual and are resourced to respond.

b. Facilitate subordinate CMO support of DIB Monitoring and Reporting products, assigning action officers as needed.

c. Ensure CMOs are aware of Monitoring and Reporting requirements to respond to events or situations in real-time (e.g., situational reports (SITREPs) per DCMA-MAN 3301-01 and the associated Resource Page).

d. Consolidate reporting for large scale All Hazard Events (e.g., category-5 hurricane forecasted to hit the entire east coast, where multiple CMOs may be impacted).

e. 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.

2.5. COMMANDERS/DIRECTORS, CONTRACT MANAGEMENT OFFICES. CMO Commanders/Directors must:

a. Manage DIB Monitoring and Reporting responsibilities and delegate authority as needed.

b. Prioritize DIB Monitoring and Reporting efforts in accordance with the output of the DIB CAIP process (DCMA-MAN 3401-02).

c. Maintain open communication with and surveillance of prioritized DIB facilities (DCMA-MAN 3401-02) in Area of Responsibility (AOR) to identify potential disruptive events and to maintain situational awareness when an event occurs. Open communication includes, but is not limited to, site visits, meeting attendance, participating in town halls, and fostering relationships with private sector companies.

d. Notify the IAD via SITREPs or informal communication of all threat or hazard issues and risks impacting the DIB, as well as any resulting operational status changes at DIB Important Capabilities List (ICL) facilities. A list of DIB-specific events or risk indicators that require reporting can be found on this Manual's Resource Page. A situation or event relevant to the DIB that does not require SITREP reporting, should be informally and timely communicated to the IAD. If a reportable event takes place at a DIB facility that is not on the DIB ICL and the CMO has reason to believe a product at the facility meets the ICL criteria, then a CMO will nominate that facility for inclusion on the ICL in accordance with DCMA-MAN 3401-02.

e. Support the IAD by collecting necessary data in response to a reported event or situation. Data should include impact to facilities, equipment, or materiel that results in a risk to DIB readiness. For the duration of an event or situation, maintain communication with the IAD and other DCMA.

f. Ensure correct security methods are followed for DIB-related SITREPS and notifications. Information regarding business operations and associated data can often be sensitive and proprietary.

g. Report to the IAD prioritized DIB asset higher-than-acceptable risk ratings identified during contract administration function (e.g., pre-award assessment, quality assurance, cybersecurity and business systems verification, safety inspections, contract surveillance, and other evaluations).

h. Partner with IAD during CMO-hosted industry days or town hall events to facilitate industry outreach and promote DCMA's DIB MA mission.

2.6. AGENCY MISSION ASSURANCE LEAD, CORPORATE OPERATIONS DIRECTORATE. The Agency MA Lead must coordinate Agency threat or hazard events with the IAD, who will evaluate for DIB impacts.

2.7. TEAM LEAD, COST AND PRICING REGIONAL COMMAND, FINANCIAL CAPABILITY TEAM (FCT). The FCT Team Lead must:

a. Maintain awareness of prioritized DIB asset lists. See DIB CAIP Manual (DCMA-MAN 3401-02) for additional details.

b. Conduct requested financial assessments to monitor priority DIB assets for financial viability and to support DIB MA assessments (DCMA-MAN 3401-03).

SECTION 3: PROCEDURES

3.1. MONITORING THE DEFENSE INDUSTRIAL BASE FOR THREATS/HAZARDS. The IAD will monitor, analyze, and report to stakeholders impending threats or hazards that might impact the DIB. Prioritization of monitoring efforts will be in accordance with the DIB CAIP process. Supporting data will come from a variety of sources including government, industry, and publically available information.

a. The DCMA CMO network, components, and capabilities will inform the IAD of potential or realized risks at DIB facilities within their AOR. CMOs must provide information for any situation that could negatively impact the ability of a DIB facility to meet DoD requirements. This information can be submitted formally through the SITREP process or informally to the IAD (see this Manual's Resource Page for additional information).

b. Reporting can be formal (e.g., All Hazard Report (AHR) or DIB Alert) and/or can serve as an input to the other Mission Assurance processes (e.g., IBA or DIB Mission Risk Assessment). The DCMA IAD will participate, as needed, when an agency CAT is initiated during significantly critical events that could impact multiple DIB facilities and DoD programs. IAD maintains a backup ICL to ensure availability of data and relies on subject matter experts' knowledge to analyze the event in a timely manner.

c. DIB AHRs are initiated in response to an emergency situation and will address known and potential impacts to prioritized assets. AHRs should be submitted to the greater DIB community within two business days of the confirmed reportable event. AHR updates will be distributed as needed. CMOs with respond to questions and follow-up with contractors for the duration of the AHR event.

d. DIB Alerts are initiated in response to a situation that poses a concern to the DoD but does not present an immediate risk to a prioritized DIB facility. DIB Alerts will address the risks associated with the situation and are submitted to relevant stakeholders within 30 days of the IAD becoming aware of the situation. CMOs will provide input and support as needed. DIB Alert updates will be distributed as needed.

e. Macro DIB sector assessments are initiated to monitor broad threat or hazard trends which may impact multiple DIB assets or whole industrial sectors (e.g., DoD budget changes). The outcome of macro DIB sector assessments will be reported to relevant stakeholders. If a macro DIB sector assessment concludes that DIB task critical assets or defense critical missions common to a sector could be impacted by broader threat or hazard trends, then a micro DIB sector assessment will be initiated (DCMA-MAN 3401-03).

f. As part of the monitor process, the IAD may initiate proactive assessments of DIB facilities and sectors to identify gaps in available industrial capability or other industrial base risks. This can include IBAs or MA Assessments in accordance with the IBA (DCMA-MAN 3401-01) and DIB Mission Risk Assessment (DCMA-MAN 3401-03) processes.

g. The IAD will use standard templates with clearly marked classification and distribution statements and performs a peer or supervisor review to ensure there is no unauthorized disclosure of classified or controlled unclassified information (CUI).

3.2. TRACKING DEFENSE INDUSTRIAL BASE RISK MANAGEMENT ACTIONS. Situational awareness of existing DIB risk management actions and continual evaluation of risk reduction efforts must be maintained.

a. For prioritized DIB assets, the IAD will maintain situational awareness of DIB risk management actions and report change to DIB capability risk rating over time. From documented risk management actions per DCMA-MAN 3401-04, execution of DIB risk management actions should be tracked and communicated with cognizant CMO assistance and inform stakeholders (e.g. DoD Components, Joint Staff, Combatant Commands, Program Offices, interagency partners, industry asset owners) of changes or delays to risk reduction activities.

b. The IAD will assess the efficacy of risk management plans to determine whether risk management actions lowered risk. 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. This information will be reported to stakeholders (e.g. DoD Risk Management Programs) annually and as needed.

c. The IAD will use standard templates with clearly marked classification and distribution statements and performs a peer or supervisor review to ensure there is no unauthorized disclosure of classified or controlled unclassified information (CUI).

3.3. REPORTING DEFENSE INDUSTRIAL BASE READINESS. DoD readiness reporting provides a means to manage and report the ability of DoD and its subordinate components to execute the national military strategy. DIB readiness reports will be issued to stakeholders, principally the Joint Staff and Combatant Commands. The following supports MEF output task execution for DIB Readiness Reporting:

a. The IAD will identify and prioritize DIB critical infrastructure in accordance with DCMA-MAN 3401-02 and provide alerts to stakeholders if readiness at prioritized DIB assets may be degraded.

b. The IAD and CMOs will maintain open lines of communication with one another as well as with prioritized DIB facilities to ensure that the DIB is ready and able to meet DoD mission requirements.

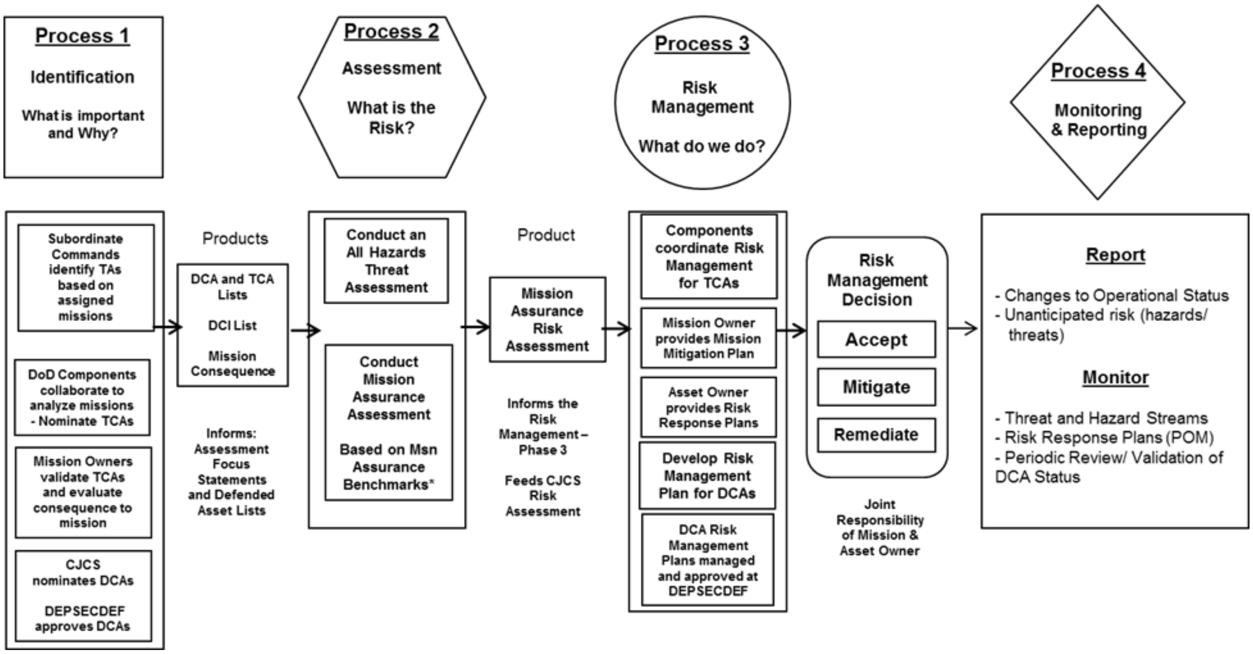
c. The IAD will report DIB readiness conditions via the DoD readiness system of record.

d. The IAD will use standard templates with clearly marked classification and distribution statements and performs a peer or supervisor review to ensure there is no unauthorized disclosure of classified or controlled unclassified information (CUI).

SECTION 4: GENERAL PRINCIPLES

4.1. DoD MISSION ASSURANCE CONSTRUCT. 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

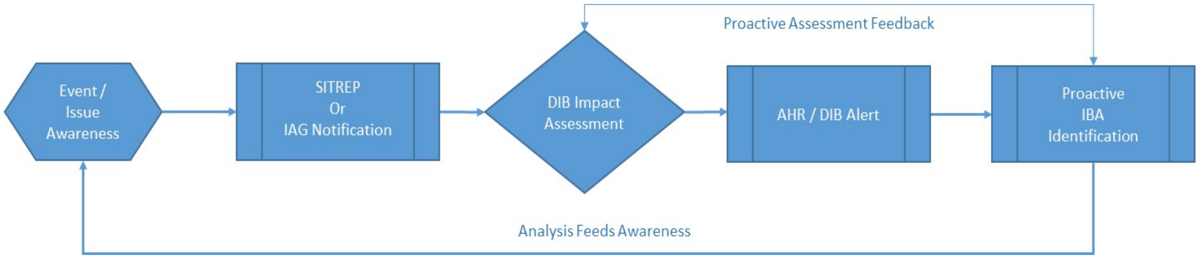

Process 1
Identification
What is important and Why?
Process 2
Assessment
What is the Risk?
Process 3
Risk Management
What do we do?
Process 4
Monitoring & Reporting
Subordinate Commands identify TAs based on assigned missions
DoD Components collaborate to analyze missions - Nominate TCAs
Mission Owners validate TCAs and evaluate consequence to mission
CJCS nominates DCAs
DEPSECDEF approves DCAs
Products
DCA and TCA Lists
DCI List
Mission Consequence
Informs: Assessment Focus Statements and Defended Asset Lists
Conduct an All Hazards Threat Assessment
Conduct Mission Assurance Assessment
Based on Msn Assurance Benchmarks*
Product
Mission Assurance Risk Assessment
Informs the Risk Management – Phase 3
Feeds CJCS Risk Assessment
Components coordinate Risk Management for TCAs
Mission Owner provides Mission Mitigation Plan
Asset Owner provides Risk Response Plans
Develop Risk Management Plan for DCAs
DCA Risk Management Plans managed and approved at DEPSECDEF
Risk Management Decision
Accept
Mitigate
Remediate
Joint Responsibility of Mission & Asset Owner
Report
- Changes to Operational Status
- Unanticipated risk (hazards/ threats)
Monitor
- Threat and Hazard Streams
- Risk Response Plans (POM)
- Periodic Review/ Validation of DCA Status

4.2. DCMA DEFENSE INDUSTRIAL BASE MISSION ASSURANCE. In accordance with DCMA-INST 3401, DCMA IAD 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. DEFENSE INDUSTRIAL BASE MONITORING AND REPORTING. During the DIB Monitoring and Reporting process, DCMA maintains situational awareness of strategic mission risk through threat or hazard monitoring, operational reporting, and risk management action tracking. The IAD integrates insights from Agency components and capabilities and leverages interagency partnerships to monitor and report potential DoD mission execution risk resulting from industrial capability risk. The IAD keeps stakeholders informed to enable timely DIB risk management and assure critical defense missions.

a. With worldwide presence and access to industrial facilities, DCMA is uniquely positioned to monitor and report on impending threats or hazards that threaten critical DIB asset operational readiness. During the course of contract administration, the distributed CMO network provides a means to identify impending threats or hazards across the DIB. DCMA IAD also receives monitoring input from external sources, including other Federal partners. After a monitoring input signal is received, it is evaluated for potential DIB impact, and a stakeholder report is generated. Figure 2 is a graphical overview of several key tasks within the Monitoring and Reporting process and how they are related.

Figure 2. Defense Industrial Base Monitoring and Reporting Process Overview


Proactive Assessment Feedback
Event / Issue Awareness
SITREP Or IAG Notification
DIB Impact Assessment
AHR / DIB Alert
Proactive IBA Identification
Analysis Feeds Awareness

b. Once a threat/hazard is analyzed, readiness and industrial capability impacts are reported to defense acquisition community (e.g., office of the Under Secretary of Defense for Acquisition and Sustainment and the buying commands) as well as operational community stakeholders (e.g., office of the Under Secretary of Defense for Policy and office of the Chairman of the Joint Chiefs of Staff) via All Hazard Reports, DIB Alerts, and/or input to the DoD readiness system of record. The reports describe the threat/hazard, analyze potential DIB impact, and provide recommendations to support potential risk management actions as collected and consolidated per DCMA-MAN 3401-04.

c. By partnering with DIB risk management program owners in accordance with DCMA-MAN 3401-04, DCMA maintains situational awareness of DIB risk management actions, especially those that affect prioritized DIB assets. Risk management actions are part of the mission risk assessment calculus (DCMA-MAN 3401-03) and can also influence DIB asset criticality (e.g., establishment of an alternative source; see DCMA-MAN 3401-02). The ultimate objective of mission assurance is to reduce operational mission risk.

d. During the course of continuous monitoring and analysis, the Monitoring and Reporting process will identify DIB facilities, products, or sectors for which additional industrial capabilities data is needed. Subjects for proactive assessment are provided in a feedback loop to the Industrial Base Assessment process (DCMA-MAN 3401-01) or DIB Mission Risk Assessment process (DCMA-MAN 3401-03). DIB Monitoring and Reporting is an ongoing effort in DIB MA, completing the cyclic nature of the interconnected processes and providing feedback for continued DIB assessment.

GLOSSARY

G.1. DEFINITIONS.

All Hazard Report (AHR). "All-Hazard" is an inclusive emergency management term, addressing natural, technological, and man-made emergencies such as an earthquake, epidemic, flood, hurricane, radiological release, industrial accident, terrorist event, or other reportable situation.

Area of Responsibility. A pre-defined geographical area within which the CMOs have authority and duty to oversee the status of DoD contractors.

Asset. A distinguishable entity 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.

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.

Business Capability Framework. DCMA conceptual model describing how the Agency: meets customer needs and contributes to DoD; organizes, trains and equips its workforce to meet those needs; employs a system engineering approach to organizational design; and defines "Return on Investment" in terms of capability value stream outputs. It is a set of high level contract management functions that underpin the Agency's strategic plan and capture the results of the daily, multi-functional activities in order to provide actionable insight to the Defense Acquisition Enterprise.

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 Manager. Individual identified by the DCMA Director as the proponent with advocacy for all Agency efforts under a given capability. The Capability Manager is responsible for the doctrine (instructions and manuals), tools, and training associated with the process and activities that fall under the purview of the capability.

Component Head (DCMA). The leader of an organization reporting to the Director, DCMA.

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.

Criticality Factors. Criticality factors are those that make a product or service difficult to replace. The six criticality factors are skilled labor, design, and facility/equipment requirements needed to produce a military product or service, its "defense uniqueness," the availability of alternative sources, and the time and cost required to replace it.

Defense Critical Asset (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.

Defense Critical Infrastructure (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 (DIB) Alert(s). An inclusive emergency management term, addressing business related situations that pose a concern to the DoD because of the uncertainty and risks of a particular business or industry, which could include a merger, acquisition, bankruptcy, plant closure or relocation, or other reportable event.

Event. See "Issue."

External Customer. Non-DCMA organization that receives products or service requests that result from DCMA action (e.g., military service program offices).

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.

Hazard. Condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.

Institutional Risk. This area defines risks to organizational, operational, and process effectiveness in improving national defense. Office of the Secretary of Defense (OSD) and DoD Components will assess and report institutional risk related to their MEFs.

Integrate. The arrangement of efforts to reduce redundancy and operate as a whole.

Internal Customer. DCMA organization or capability that receives products or service requirements from another DCMA organization or capability.

Issue. Event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (probability = 1).

Mission Assurance. 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 MEFs in any operating environment or condition.

Mission Essential Function. 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 DoDs ability to provide vital services or exercise authority, direction, and control.

Mission Owner. The OSD or DoD Component having responsibility for the execution of all or part of a mission assigned by statute or the Secretary of Defense.

Operational Unit. The headquarters offices of the 5 DCMA regions including International, Special Programs, and East, Central, and West regions.

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).

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.

Situation Report (SITREP). An unscheduled, rapid report of a significant event or situation that is projected to negatively impact DCMA’s mission execution capability or impact the DIB readiness state to support the war fighter.

Situation. See “Issue.”

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.

Task Critical Asset (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.

Threat. An adversary having the intent, capability, and opportunity to cause loss or damage.

GLOSSARY

G.2. ACRONYMS.

AHR	All Hazard Reports
AOR	Area of Responsibility
BCF	Business Capability Framework
CMO	Contract Management Office
CAIP	Critical Asset Identification and Prioritization
CAT	Crisis Action Team
CUI	Controlled Unclassified Information
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DCMA-INST	DCMA Instruction
DCMA-MAN	DCMA Manual
DIB	Defense Industrial Base
IAD	Industrial Analysis Division
ICL	Important Capabilities List
IBA	Industrial Base Assessment
MA	Mission Assurance
MEF	Mission Essential Function
OPR	Office of Primary Responsibility
OU	Operational Unit
PCII	Protected Critical Infrastructure Information
PM&BI	Portfolio Management & Business Integration

REFERENCES

DCMA Instruction 3301, "Agency Mission Assurance," May 14, 2018

DCMA Manual 3301-01, "Agency Mission Assurance Construct," December 16, 2018

DCMA Manual 3301-02, "Continuity of Operations and Emergency Management," September 7, 2018

DCMA Manual 3401-01, "Industrial Base Assessment," December 17, 2018

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

DCMA Manual 3401-04, "Defense Industrial Base Mission Risk Management," January 13, 2019

DCMA Memorandum 17-072, "Agency Mission Essential Functions," April 27, 2017

DoD Directive 5105.64, "Defense Contract Management Agency," January 10, 2013

DoD Directive 3020.40, "Mission Assurance," September 11, 2018, as amended

DoD Instruction 3020.45, "Mission Assurance (MA) Construct," August 14, 2018

DoD Manual 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

Presidential Policy Directive PPD-21, "Critical Infrastructure Security and Resilience," February 12, 2013

Under Secretary of Defense Memorandum "Defense Contract Management Agency Mission Changes," May 20, 2019