Army Regulation 525–26

Military Operations

Infrastructure Risk Management (Army)

Headquarters
Department of the Army
Washington, DC
22 June 2004

UNCLASSIFIED

SUMMARY of CHANGE

AR 525–26
Infrastructure Risk Management (Army)

Specifically, this regulation--

- o Implements The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (chaps 2, 3, 4, and 5).

- o Assigns responsibility and prescribes policy for Army infrastructure risk management activities (chaps 2 and 4).

- o Provides planning guidance and planning factors associated with the Army core competencies as described by the Army Mission Map and the Strategic Readiness System (chap 3).

- o Describes related national and Department of Defense programs (chap 5).

- o Provides a standardized set of terms in order to form the context for infrastructure-related risk based management (app B, sec II).

Headquarters
Department of the Army
Washington, DC
22 June 2004

Army Regulation 525–26

Effective 22 July 2004

Military Operations

Infrastructure Risk Management (Army)

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

Joel B Hudson

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

History. This publication is a new Department of the Army regulation.

Summary. This regulation implements The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets and Department of Defense Directive 5160.54. It prescribes policy and assigns responsibility for Army infrastructure risk management activities.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States (ARNG/ARGNUS), and the U.S. Army Reserve (USAR). In the event of conflict between this regulation and approved Office of the Secretary of Defense (OSD) or Joint Chiefs of Staff (JCS) publications, the provisions of the latter will apply.

Proponent and exception authority. The proponent agency for this regulation is the Deputy Chief of Staff, G–3. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army management control process. This regulation contains management control provisions but does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA, ATTN: DAMO–ODS 400 Army Pentagon, Washington, DC 20310–0400.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA, ATTN: DAMO–ODS, 400 Army Pentagon, Washington, DC 20310–0400.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States (ARNG/ARNGUS), and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Table List

Chapter 1
Introduction

1–1. Purpose
This regulation prescribes Army policy for managing infrastructure-related risk.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities
Responsibilities are listed in chapter 2.

1–5. Statutory authorities
Statutory authority for this regulation is derived from Sections 117, 3013, and 3062 of Title 10 of the United States Code.

Chapter 2
Responsibilities

2–1. The Deputy Chief of Staff, G–3
The Deputy Chief of Staff, G–3 (DCS, G–3) is the functional proponent for Army infrastructure risk management policy. The DCS, G–3 will—

a. Establish and resource an Infrastructure Risk Management Program Office, with responsibilities as outlined in paragraph 2–19 of this regulation, in support of the Defense Critical Infrastructure Program.

b. Provide oversight of the Infrastructure Risk Management Program.

c. Program and budget for and fund the Infrastructure Risk Management Program.

d. Promote the Infrastructure Risk Management Program.

e. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for space.

f. Designate a liaison point of contact to coordinate Army space matters with the Defense infrastructure sector lead agency for space.

g. Serve as Army lead for coordination with the Defense infrastructure special function lead agency for education and awareness.

h. Designate a liaison point of contact to coordinate infrastructure education and awareness activities with the Defense infrastructure special function lead agency for education and awareness.

i. Through the Commanding General, U.S. Army Training and Doctrine Command, ensure that infrastructure risk management is integrated into doctrine and training at the appropriate levels.

2–2. The Army Secretariat
The Assistant Secretaries of the Army, within the purview of their organizational responsibilities, will—

a. Integrate the infrastructure risk management policy established by this regulation into policy and procedures established under the purview of the Assistant Secretary.

b. Coordinate with the Infrastructure Risk Management Program Office and provide, as required, those infrastructure-related vulnerability assessments for infrastructure (cyber and physical) under the purview of the Assistant Secretary.

2–3. The Assistant Secretary of the Army for Financial Management and Comptroller
The Assistant Secretary of the Army for Financial Management and Comptroller (ASA(FM&C)), in addition to the responsibilities found in paragraph 2–2, above will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for financial services.

b. Designate a liaison point of contact to coordinate Army financial services matters with the Defense infrastructure sector lead agency for financial services.

c. Maintain a system to capture expenditures of infrastructure risk management funds within the Army.

2–4. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology

The Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)), in addition to the responsibilities found in paragraph 2–2, above will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for the defense industrial base.

b. Designate a liaison point of contact to coordinate infrastructure research and development activities with the Defense infrastructure special function lead agency for research and development.

c. Integrate the infrastructure risk management policy established by this regulation into acquisition policy guidance, systems in development, systems being acquired, and the supporting industrial base.

d. Integrate the infrastructure risk management policy established by this regulation into Army acquisition policy guidance, including the Army Federal Acquisition Regulations System.

2–5. The Chief, Public Affairs

The Chief, Public Affairs will provide public affairs guidance for the development of command information and public information programs relating to infrastructure risk management.

2–6. The Deputy Chief of Staff, G–1

The Deputy Chief of Staff, G–1 (DCS, G–1) will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for personnel.

b. Designate a liaison point of contact to coordinate Army personnel matters with the Defense infrastructure sector lead agency for personnel.

c. Provide infrastructure-related personnel services or system vulnerability assessments to the Infrastructure Risk Management Program Office.

d. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–7. The Deputy Chief of Staff, G–2

The Deputy Chief of Staff, G–2 (DCS, G–2) will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for intelligence, surveillance, and reconnaissance.

b. Designate a liaison point of contact to coordinate Army intelligence, surveillance, and reconnaissance matters with the Defense infrastructure sector lead agency for intelligence, surveillance, and reconnaissance.

c. Serve as Army lead for coordination with the Defense infrastructure special function lead agency for intelligence support.

d. Designate a liaison point of contact to coordinate infrastructure intelligence support activities with the Defense infrastructure special function lead agency for intelligence support.

e. Provide infrastructure-related threat and capabilities assessments, as required, to the Infrastructure Risk Management Program Office.

f. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–8. The Deputy Chief of Staff, G–4

The Deputy Chief of Staff, G–4 (DCS, G-4) will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for logistics.

b. Designate a liaison point of contact to coordinate Army logistic matters with the Defense infrastructure sector lead agency for logistics.

c. Provide infrastructure-related logistics assessments, as required, to the Infrastructure Risk Management Program Office.

d. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–9. Chief Information Officer, G–6

The Chief Information Officer, G–6 (CIO, G–6) will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for the global information grid.

b. Designate a liaison point of contact to coordinate Army global information grid matters with the Defense infrastructure sector lead agency for the global information grid.

c. Serve as Army lead for coordination with the Defense infrastructure special function lead agency for information assurance.

d. Designate a liaison point of contact to coordinate information assurance activities with the Defense infrastructure special function lead agency for information assurance.

e. Provide infrastructure-related information management vulnerability assessments to the Infrastructure Risk Management Program Office.

f. Coordinate information assurance activities with the Infrastructure Risk Management Program Office.

2–10. The Deputy Chief of Staff, G–8

The Deputy Chief of Staff, G–8 (DCS, G–8) will—

a. Ensure that infrastructure-related risk management is considered in programming decisions where applicable.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–11. The Surgeon General

The Surgeon General will—

a. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for health affairs.

b. Designate a liaison point of contact to coordinate Army Health Affairs matters with the Defense infrastructure sector lead agency for health affairs.

c. Provide infrastructure-related health services or system vulnerability assessments to the Infrastructure Risk Management Program Office.

2–12. The Inspector General

The Inspector General will—

a. Conduct periodic inspections of Army organizations in the area of infrastructure risk management.

b. Report, as the result of the periodic inspections, infrastructure-related risk trends to the Infrastructure Risk Management Program Office.

2–13. The Commanding General, United States Army Corps of Engineers

The Commanding General, United States Army Corps of Engineers will—

a. Serve as the Defense infrastructure sector lead agency for public works.

b. Designate a liaison point of contact to coordinate Army public works matters within the Defense infrastructure sector for public works.

c. Provide infrastructure-related public works vulnerability assessments to the Infrastructure Risk Management Program Office.

d. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–14. The Assistant Chief of Staff for Installation Management

The Assistant Chief of Staff for Installation Management (ACSIM) will—

a. Serve, in accordance with this regulation, as the Headquarters, Department of the Army (HQDA) lead for all infrastructure-related (cyber and physical) policy and procedures relating to the management of Army installations.

b. Coordinate, through the IMA, all infrastructure-related (cyber and physical) installation vulnerability assessments in conjunction with the Army G–3 and major Army commands (MACOMs).

c. Provide infrastructure-related installation vulnerability assessments to the Infrastructure Risk Management Program Office.

d. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–15. The Chief, Army Reserve

The Chief of the Army Reserve will—

a. Work in concert with the ACSIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Program Management Office.

2–16. The Director, Army National Guard

The Director, Army National Guard will—

a. Work in concert with the ASCIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–17. Commanders, major Army commands

The commanders of major Army commands (MACOMs) will—

a. Work in concert with the ACSIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–18. Direct reporting units

Direct reporting units will—

a. Work in concert with the ACSIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

2–19. The Commander, Army Materiel Command

The commander of the Army Materiel Command (AMC)—

a. Work in concert with the ACSIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

c. Serve as the primary point of contact for infrastructure risk management for AMC installations and depots not covered by the IMA.

2–20. The Military Surface Deployments and Distribution Command

The Military Surface Deployment and Distribution Command will—

a. Work in concert with the ACSIM and the IMA to maintain awareness of infrastructure risk and implement required risk mitigation strategies.

b. Coordinate infrastructure assurance activities with the Infrastructure Risk Management Program Office.

c. Serve as Army lead for coordination with the Defense infrastructure sector lead agency for transportation.

d. Designate a liaison point of contact to coordinate Army public works matters with the Defense infrastructure sector lead agency for transportation.

e. Provide infrastructure-related transportation vulnerability assessments to the Infrastructure Risk Management Program Office.

2–21. The Chief, Infrastructure Risk Management Branch

The Chief, Infrastructure Risk Management Branch will—

a. Provide the center of excellence for Army efforts regarding infrastructure-related risk-based management.

b. Provide the focal point for the management of all aspects of the Infrastructure Risk Management Program.

c. Provide the single point of entry, within HQDA, for all aspects and actions relating to the Department of Defense Critical Infrastructure Program.

d. Provide corporate visibility of the Army infrastructure systems and assets necessary for proficiency in the Army core competencies.

e. Direct the Infrastructure Risk Management Program.

f. Implement the Infrastructure Risk Management Program, as described in chapter 4 of this regulation, and support the Department of Defense Critical Infrastructure Program, described in chapter 5 of this regulation.

g. Ensure that infrastructure-related risk-based management policies, plans, and procedures are consistent with DOD directives and instructions.

h. Program dollars for the development and execution of the Infrastructure Risk Management Program.

i. Develop and execute the budget for the Infrastructure Risk Management Program.

j. Manage and account for Infrastructure Risk Management Program funds.

k. Establish MACOM infrastructure-related risk-based program and budget reporting elements (per ASA–FMC).

l. Develop and promulgate infrastructure-related risk-based policy and procedures.

m. Develop, coordinate, and validate infrastructure-related risk-based requirements.

n. Develop and promulgate infrastructure-related risk-based management strategies supporting the Army core competencies.

o. Ensure coordination among appropriate Department of the Army (DA) functional representatives on infrastructure-related risk-based issues.

p. Facilitate liaison between the DA infrastructure functional representatives and the Defense infrastructure sector and infrastructure special function lead agencies.

q. Promote the Infrastructure Risk Management Program.

Chapter 3
Planning Guidance

3–1. Army core competencies

The Infrastructure Risk Management Program provides corporate visibility of functions and infrastructure systems and assets and develops risk management strategies supporting the Army core competencies. The core competencies establish the necessary requirements of the Army to best support mission accomplishment and reflect the priorities of the Army corporate leadership.

3–2. Methodology

a. The Infrastructure Risk Management Program uses a methodology based on the propagation of risk levels associated with functions and the individual Army assets supporting the core competencies and objectives in order to assess the level of risk to the Army's core competencies and internal process strategic objectives. This methodology relies on objectives identified through the Army's Strategic Readiness System (SRS), assets identified by the Army Staff and MACOMs, and additional data to facilitate the data's applicability to propagation of risk to the Army's core competencies and strategic objectives.

b. The focus of infrastructure-related planning is on risk to the physical and cyber (public and private) infrastructure and the actions taken to mitigate that risk. The planning factors are—

(1) Identification of the Army core competencies and the associated functions, processes, objectives, measures, and targets.

(2) Identification of the infrastructure assets and asset sets associated with the functions.

(3) Identification of infrastructure-related business continuity issues connected to the functions, assets, and assets sets.

(4) Identification of the risk to the functions and the infrastructure assets and asset sets.

(5) Development of measurable thresholds for infrastructure-related risk.

(6) Development of course of action to mitigate risk to the functions and the infrastructure assets and assets sets.

(7) Analysis of cost/benefits against the course of action.

Chapter 4
Infrastructure Risk Management Policy

4–1. General

a. Infrastructure risk management is the fundamental building block, if not the foundation, of DOD efforts in homeland defense and of the Department of Defense Critical Infrastructure Program. Specifically tied to the Army's core competencies, it provides the Army corporate leadership with a method for analyzing infrastructure risk and developing both short- and long-term infrastructure risk mitigation and management strategies.

b. The U.S. Army implements the Department of Defense Critical Infrastructure Program through its Infrastructure Risk Management Program. This U.S. Army program transcends traditional protection programs by focusing on the continuation of essential business functions regardless of threats from or vulnerabilities to unplanned natural, technological, or manmade (deliberate attack or accidents with unintended consequences) events. Policy and procedures consider cyber and physical infrastructure as supporting elements of essential business functions.

c. Infrastructure risk management is a process of analyzing trends, threat and capabilities, vulnerabilities, and dependencies of systems and assets supporting the U.S. Army core competencies. The results of this analysis are twofold. The first result is a better understanding of the environment within which the U.S. Army operates; the second provides the basis for the development of risk management strategies.

d. Infrastructure risk management brings to bear all the skills and abilities residing within the U.S. Army, both organizationally and individually, in order to ensure its continued functioning as an institution. This means that the effort is not specifically focused on protection but that it considers protection as one of many methods for mitigating risk resulting from vulnerabilities.

4–2. Policies

In establishing infrastructure risk management polices the Army will—

a. Provide a corporate tool focusing on the Army, tied to the Army's core competencies, and designed to provide corporate visibility to measurable results within the overall theme of risk.

b. Ensure that internal Army infrastructure risk management strategies address the reliance upon physical and cyber public and private infrastructure.

4–3. Implementation

The Army implements the Infrastructure Risk Management Program by—

a. Determining relationships between and among core competencies, strategic objectives, and assets.

b. Analyzing infrastructure-related assessments and reports provided by multiple sources.

c. Determining risk.

d. Discovering trends.

e. Providing strategically focused risk management strategies.

Chapter 5
Critical Infrastructure Protection Programs

5–1. The National Critical Infrastructure Protection Program

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies the infrastructures deemed most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence. They include but are not limited to: agriculture and food, water, public health, emergency services, defense industrial base, telecommunications; energy; banking and finance; transportation; chemical industry and hazardous materials, and postal and shipping. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. However, as a result of advances in information technology and the necessity to improve efficiency, these infrastructures have become increasing automated and interlinked. These same advances have created new vulnerabilities from equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Military operations today are heavily dependent on globally (U.S. and foreign, government and civilian) shared infrastructures (physical and cyber). Technological advances have interconnected these infrastructures, better enabling mission accomplishment anywhere in the world. Although this connectivity enhances mission accomplishment, it also increases the vulnerability to various physical and cyber occurrences. For this reason, it is necessary to identify, protect, and assure these infrastructures.

5–2. Department of Defense Critical Infrastructure Protection Program

DOD Directive 5160.54 provides policy and implementation guidance for the Department of Defense Critical Infrastructure Program. Defense infrastructure sectors have been identified to align with the critical infrastructures identified in the national strategy. These sectors are: logistics; transportation; personnel; health affairs; financial services; global information grid; space; intelligence, surveillance, and reconnaissance; public works; and the defense industrial base. Each of the sectors is assigned a lead agency or lead organization from within the department. The lead agency or lead organization is responsible for integrating critical infrastructure protection activities; characterizing the sector and developing a sector database; coordinating infrastructure assessments; and assisting in the execution of the total program. Table 5–1 shows the Defense infrastructure sectors, the Defense lead agency or organization, and the Army alignment. Additionally, there are five special functions: intelligence support; industrial policy & security; information assurance; education and awareness; and research and development. Each of the infrastructure special functions is assigned a lead agency or lead organization from within the department. The special functions are niche areas having broad applicability to the overall program. Table 5–2 shows defense special functions, the Defense lead agency or organization, and the Army alignment.

Table 5–1
Defense Infrastructure Sector

Defense Infrastructure Sector	Defense Lead Agency	Army Lead Agency
Logistics	Defense Logistics Agency	Office of the Deputy Chief of Staff, G–4
Transportation	United States Transportation Command	Office of the Deputy Chief of Staff, G–4
Personnel	Defense Human Resources Agency	Office of the Deputy Chief of Staff, G–1
Health Affairs	Office of the Assistant Secretary of Defense (Health Affairs)	Office of the Surgeon General
Financial Services	Defense Financing and Accounting Service	Office of the Assistant Secretary of the Army for Financial Management and Comptroller

Table 5–1
Defense Infrastructure Sector—Continued

Defense Infrastructure Sector	Defense Lead Agency	Army Lead Agency
Global Information Grid	Defense Information Systems Agency	Chief Information Officer, G–6
Space	United States Strategic Command	Office of the Deputy Chief of Staff, G–3
Public Works	United States Army Corps of Engineers	United States Army Corps of Engineers
Intelligence, Surveillance, and Reconnaissance	Defense Intelligence Agency	Office of the Deputy Chief of Staff, G–2
Defense Industrial Base	Defense Contract Management Agency	Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology

Table 5–2
Defense Special Function

Defense Special Function	Defense Lead Agency	Army Lead Agency
Intelligence support	Defense Intelligence Agency	Office of the Deputy Chief of Staff, G–2
Industrial policy & security	Under Secretary of Defense (Acquisitions, Technology, and Logistics)	Office of the Deputy Chief of Staff, G–3
Information assurance	Assistant Secretary of Defense (National Information Assurance)	Office of the Deputy Chief of Staff, G–6
Education and awareness	National Defense University	Office of the Deputy Chief of Staff, G–3
Research and development	Director of Defense Research and Engineering	Office of the Assistant Secretary of the Army (Acquisitions, Technology, and Logistics)

Appendix A
References

Section I
Required Publications

This section contains no entries.

Section II
Related Publications

A related publication is a source of additional information. The user does not have to read it to understand the publication.

AR 1–1
Planning, Programming, Budgeting and Execution System

AR 5–9
Area Support Responsibilities

AR 11–2
Management Control

AR 25–1
Army Information Management

AR 70–1
Army Acquisition Policy

AR 210–20
Master Planning for Army Installations

DA Pam 190–51
Risk Analysis for Army Property

DODD 5160.54
Critical Asset Assurance Program (CAAP) (http://www.dtic.mil/whs/directives)

FM 8–55
Planning for Health Service Support

FM 100–14
Risk Management

FM 100–22
Installation Management

Presidential Decision Directive 63
Critical Infrastructure Protection. (This publication may be obtained at http://www.dtra.mil/ or from the Superintendent of Documents, P.O. Box 37954, Pittsburgh, PA 15250–7954.)

Presidential Decision Directive 67
Enduring Constitutional Government & Continuity of Government Operations. (This publication may be obtained at http://www.dtra.mil/ or from the Superintendent of Documents, P.O. Box 37954, Pittsburgh, PA 15250–7954.)

Risk Management Guide for DoD Acquisition, February 2001, Chapter 2, Risk and Risk Management
(This publication may be obtained at http//www.whitehouse.gov/ or from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954.)

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
(This publication may be obtained at http://www.whitehouse.gov/ or from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954.)

The National Strategy for Homeland Security
(This publication may be obtained at http://www.whitehouse.gov/ or from the Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954.)

Title 10, Section 117, United States Code
Readiness Reporting System: Establishment; Reporting to Congressional Committees (http://uscode.house.gov/usc.htm)

Title 10, Section 3013, United States Code
Secretary of the Army (http://uscode.house.gov/usc.htm)

Title 10, Section 3062, United States Code
Policy; Composition; Organized Peace Establishment (http://uscode.house.gov/usc.htm)

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

This section contains no entries.

Glossary

Section I
Abbreviations

ACSIM
Assistant Chief of Staff for Installation Management

AMC
Army Materiel Command

ARNG/ARNGUS
Army National Guard/Army National Guard of the United States

ASA(AL&T)
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ASA(FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

ASD(AT&L)
Assistant Secretary of Defense (Acquisition, Technology, and Logistics)

C3
command, control, and communications

CG
commanding general

CIO, G–6
Chief Information Officer, G–6

CIP
critical infrastructure protection

CPA
Chief, Public Affairs

DCS, G–1
Deputy Chief of Staff, G–1

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3
Deputy Chief of Staff, G–3

DCS, G–4
Deputy Chief of Staff, G–4

DCS, G–8
Deputy Chief of Staff, G–8

DFAS
Defense Finance and Accounting Service

DHRA
Defense Human Resource Agency

DIA
Defense Intelligence Agency

DIB
defense industrial base

DISA
Defense Information Systems Agency

DLA
Defense Logistics Agency

FOIA
Freedom of Information Act

GIG
global information grid

HQDA
Headquarters, Department of the Army

IMA
Installation Management Agency

ISR
intelligence, surveillance, and reconnaissance

JCS
Joint Chiefs of Staff

J–3
Joint Staff Operations Directorate

MACOM
major Army command

NDU
National Defense University

OPLAN
operations plan

OSD
Office of the Secretary of Defense

SCG
Security Classification Guide

SRS
Strategic Readiness System

TIG
The Inspector General

TRADOC
United States Training and Doctrine Command

TSG
The Surgeon General

UD
Un-determined

USACE
United States Army Corps of Engineers

USAR
United States Army Reserve

USSTRATCOM
United States Strategic Command

USTRANSCOM
United States Transportation Command

Section II
Terms

This section standardizes infrastructure risk-related terminology. Definitions and terms included in this section describe the environment of infrastructure-related risk. They form the context for infrastructure-related risk and risk-based management.

Accepted risk
An approach that does nothing with a risk, but rather prepares for and deals with the consequences of a risk should it occur. No risk management resources are expended in dealing with accepted risks.

Acceptance rationale
A type of action plan that documents the reasons for accepting a risk (doing nothing with it).

Analysis
An appraisal of the information and conclusions drawn from one or more assessments.

Assessment
The process of compiling and examining information and data from various sources and drawing conclusions about the object of the assessment.

Asset
For the purpose of infrastructure risk management, there are four types of assets: infrastructure, non-infrastructure, mission-essential, and symbolic. Infrastructure assets are public, private, and governmental (Federal and military) interdependent cyber and physical networks and systems available to support national security. Non-infrastructure assets are units, individuals, and materiel required to support Army missions. Mission-essential assets are infrastructure and non-infrastructure systems and assets fundamental to the accomplishment of the Army core competencies. Symbolic assets are those national objects having cultural significance and the capacity to excite or objectify a response.

Assurance
Proactive risk management actions intended to mitigate or prevent the destruction or incapacitation of the infrastructure.

Attribute
An inherent characteristic or quality of risk, that is, reliability, maintainability, portability, and complexity. Sometimes referred to as quality attributes.

Avoidance
A mitigation strategy that eliminates the threat of a specific risk, usually by eliminating its potential cause.

Baseline assessment
The initial set of probability and impact assessments usually made when risks are first identified. Initial assessments describe risks under the initial baseline plan and may indicate areas for needed risk management. Subsequent events, risk management actions, and new information will always change the assessment, which will ultimately be adopted as the baseline.

Business continuity
The process of identifying the impact of potential losses on an organization's functional capabilities; formulating and

implementing viable recovery strategies; and developing recovery plans, to ensure the continuity of organizational services in the event of an event, incident, or crisis.

Capability analysis
The process of identifying and drawing conclusions about the functional capabilities of an adversary's ability to disrupt the infrastructure and the Army's capabilities to ensure continuity of business operations under all conditions.

Condition
The key circumstances and situations that are causing concern, doubt, anxiety, or uncertainty.

Consequence
The plausible negative outcomes of the current conditions that are creating uncertainty.

Consistency
The degree of uniformity, standardization, and freedom from contradiction among documents or parts of a system or component.

Context
The additional detail regarding events, circumstances, and interrelationships that may affect risk.

Continuous risk management
A practice with processes, methods, and tools for managing risk. It provides a disciplined environment for proactive decisionmaking in order to continuously assess risks to determine which risks are important and to implement strategies.

Control
A process, based on reporting data, that takes risk-tracking status reports for the watched and mitigated risks and decides what to do with them. The general process includes analyzing status reports, deciding on how to proceed, and executing the decision.

Cost-benefit analysis
The part of the management decisionmaking process in which the costs and benefits of different alternatives are compared and the most appropriate alternative is selected. Costs include not only the cost of tangible material, but also the on-going operational costs associated with the countermeasure implementation. Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasures with respect to the assessed vulnerabilities.

Countermeasure
An action taken or a physical entity used principally to reduce or eliminate one or more vulnerabilities. Countermeasures may also affect the threat (intent and/or capability) as well as an assets value. The cost of a possible countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

Critical
A notional concept. A term that is first among equals (vital and essential) but not interchangeable when ascribing military necessity. In infrastructure assurance, the notion that a mission will fail if the particular infrastructure asset is not available, regardless of reason, at a point in time.

Critical infrastructure protection
A process. A holistic approach for assuring that infrastructure assets are available to support national security. Key components of the process are the identification of public, private, and governmental (Federal and military) infrastructure assets both cyber and physical; the conduct of vulnerability assessments; the determination of risk; and the management of risk.

Defense infrastructure sector
An artificial construct designed to facilitate the characterization of Department of Defense infrastructure. The Defense infrastructure sectors are as follows: personnel; health affairs; financial services; space; logistics; intelligence, surveillance, and reconnaissance (ISR); Defense information infrastructure and command, control, and communications (DII / C3); and public works (includes DOD-owned or -operated utilities, roads, rails and railheads, and their interface to commercial and other government systems).

Dependency assessment
The process of drawing conclusions about identified dependencies between and within the characterized defense and commercial infrastructure sectors for the purpose of determining a connection or a lack thereof with mission-essential systems and assets.

Education and awareness
The process of developing tools (briefings, papers, etc.) in order to increase the understanding of the Army Infrastructure Risk Management Program and its relationship to the Army mission.

Effectiveness
A measure of the favorable effect of implementing one or more risk management actions.

Enterprise resilience
Enterprise resilience is the ability and capacity to withstand infrastructure discontinuities and adapt to new risk environments. A resilient organization effectively aligns its strategy, operations, management systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks and better endure disruptions.

Expected value
The equivalent risk-free average outcome (mean value) of a future state.

Exposure
The frequency and length of time the infrastructure is subjected to a hazard or hazardous conditions. The impact of a risk multiplied by its probability of occurring.

Findings
Risk-based conclusions drawn, by applying expert judgment, that identify the most important issues, problems, or opportunities based on statements or facts from an assessment, evaluation, audit, or review.

Function
A set of related activities, undertaken by individuals or organizations to accomplish a set purpose or end.

Functional assessment
The process of characterizing and drawing conclusions about the Army’s business processes and related supporting infrastructure.

Fusion
A supporting process. A merging and analysis of diverse, distinct, and separate infrastructure-related reports and information in order to determine systemic and functional infrastructure vulnerabilities and risk, determine and report trends, develop departmental infrastructure risk management strategies, and develop policy or assist in the development of supporting policy.

Fusion activity
A supporting process. The act of collecting, collating, cataloging, and preparing for analysis diverse, distinct, and separate infrastructure-related unclassified and classified reports, studies, and information from the public and private sector, the executive branch of the federal government, and from within the Department of Defense.

Hazard
A condition with the potential of injuring personnel, damaging equipment or structures, losing material, or reducing the ability to perform a prescribed function.

Identity
A process of transforming uncertainties and issues about the infrastructure into distinct (tangible) risks that can be described and measured. It involves capturing a statement of risk and its context.

Impact
The loss or affect if the risk occurs. The impact is traditionally described in two dimensions, its likelihood of occurring and the impact on an objective should it occur. It is both qualitative (low, medium, high) and quantitative (money, time, performance).

Infrastructure
The framework of public, private, and governmental (Federal and military) interdependent cyber and physical networks and systems available to support national security.

Installation
An aggregation of contiguous or near contiguous, common mission-supporting real property holdings under the jurisdiction of the Department of Defense controlled by and at which an Army unit or activity is permanently assigned.

Institutional mission-based assessment
The process of mapping and drawing conclusions about institutional infrastructure functions, systems, and assets required to support the Army's core competencies.

Mitigation
Short- or long-term activities designed to alleviate the adverse affects of infrastructure vulnerabilities by reducing the effect of the risk should it occur.

Odds
The ratio of probabilities of occurrence or non-occurrence.

Opportunity cost
The value associated with not selecting the best alternative use of the resource.

Probability
The likelihood that a risk will occur as expressed in qualitative or quantitative terms.

Procedure
A written description of a course of action taken to perform a given task.

Process
A set of activities performed for a given purpose.

Process capability baseline
A documented characterization of the range of expected results that would normally be achieved by following a specific process under typical circumstances.

Process descriptions
Documentation that specifies, in a complete, precise, and verifiable manner, the requirements, design, behavior, or other characteristics of a process.

Readiness
The ability of U.S. military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels—a. *Unit readiness.* The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. b. *Joint readiness.* The combatant commander's ability to integrate and synchronize ready combat and support forces to execute his or her assigned missions.

Reconstitution
Actions taken to re-establish an organization or the capabilities of an organization that have been destroyed or severely damaged.

Remediation
Actions taken to facilitate immediate response, to minimize the negative impact of a hazardous situation on or a vulnerability to people, facilities, operations, or services, and to quickly restore services.

Response
Activities to address the immediate and short-term effects of an emergency.

Risk
A concept used to give meaning to things, forces, or circumstances that pose a danger to people or the things that they

value. Normally stated as—a. The probability/likelihood of failing to achieve a particular outcome. b. The consequences/impacts of failing to achieve that outcome.

Risk analysis
The process of examining each identified infrastructure-related risk area to refine the description of the risk, isolate the cause, and determine the effects in order to increase the understanding of the substantive qualities, seriousness, likelihood, and conditions of a hazard or risk and the options for managing it. It includes risk rating and prioritization in which risk events are defined in terms of their probability of occurrence, severity of consequence/impact, and relationship to other risk areas or processes.

Risk assessment
The process of identifying and analyzing (quantifying) the probability/likelihood and consequences of an infrastructure-related event in order to provide the basis for informed decisions.

Risk assumption
The acknowledgement of the existence of a particular risk situation and a conscience decision to accept the associated level of risk with engaging in any special efforts to control it.

Risk documentation
The recording, maintaining, and reporting of assessments, handling analysis and plans, and monitoring results.

Risk handling
The process that identifies, evaluates, selects, and implements options in order to set risk at acceptable levels, given constraints and objectives.

Risk identification
The process of compiling infrastructure-related data from various sources in order to identify and document each associated risk.

Risk management
The act or practice of controlling risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk-handling options, monitoring risk to determine changes, and documenting the overall risk management program.

Risk management strategy
A blueprint providing recommendations to the corporate leadership for the management of risk. It documents the actions, goals, schedule dates, tracking requirements, and all other required supporting information.

Risk monitoring
The process of systematically tracking and evaluating the performance of risk-handling actions against established metrics.

Risk planning
A component of the risk management strategy. The process of developing and documenting an organized, comprehensive, and interactive blueprint and the methods for identifying and tracking risk areas, developing risk-handling plans, performing continuous risk assessments to determine changes in risk, and assigning adequate resources.

Sound business practices
A concept that coordinated and seamless enterprise-wide operations will improve operational effectiveness across an organization. Components of sound business practices supporting operations are leveraging technologies into key processes, optimizing the delivery of non-core competencies, and promoting acquisition reform with industries.

Statement of work
A narrative description of products or services to be supplied under contract that states the specifications or other minimum requirements; quantities; performance dates, times, and locations; and quality requirements.

Threat
Any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Threat analysis
The process of identifying and drawing conclusions about the possibility, probability, and degree of severity posed by an adversary's ability to disrupt the infrastructure under all conditions.

Trend analysis
The process of identifying and classifying threats, capabilities, risks, and vulnerabilities to physical and cyber systems and assets and drawing conclusions in order to determine both positive and negative tendencies.

Uncertainty
A situation in which only part of the information needed for decisionmaking is available.

Variance
The difference between the baseline and the current expected value.

Vulnerability
A flaw affecting the integrity of an infrastructure that when compromised or attacked causes the degradation or failure of the infrastructure.

Vulnerability analysis
The process of identifying and drawing conclusions about the characteristics of a physical or cyber system or asset causing it to suffer a definite degradation—incapability to perform the designated mission—as a result of having been subjected to a certain level of effects under all conditions.

Section III
Special Abbreviations and Terms

This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 216

PIN:	080134–000
DATE:	06-24-04
TIME:	11:29:16
PAGES SET:	21

DATA FILE:	C:\wincomp\r525-26.fil
DOCUMENT:	AR 525–26

SECURITY:	UNCLASSIFIED
DOC STATUS:	NEW PUBLICATION