Department of Defense

MANUAL

NUMBER 3020.45, Volume 2
October 28, 2008

USD(P)

SUBJECT: Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning

References: (a) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
(b) DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management," April 21, 2008

1. PURPOSE

a. In accordance with the authority in Reference (a) and the guidelines and responsibilities as assigned in Reference (b), this Manual provides uniform procedures for the execution of DCIP activities.

b. This Volume describes a process for DoD leaders, once risk has been assessed, to determine, plan, justify, and implement remediation actions to reduce risk to defense critical infrastructure (DCI). The process documented in this Volume ensures informed decisions are made to manage risk to DCI. Informed risk management decisions are important to ensure the availability of DCI while making efficient use of limited resources.

2. APPLICABILITY. This Volume applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

b. Each Defense Infrastructure Sector Lead Agent (DISLA) identified in Reference (a).

3. DEFINITIONS, See Glossary.

4. RESPONSIBILITIES. The Secretaries of the Military Departments; Commander, U.S. Special Operations Command; Chief, National Guard Bureau (in coordination with the National Guard Adjutants General of the States); and Directors of Defense Agencies and DoD Field Activities, having control of DCI assets within their respective areas of responsibility, shall, in accordance with Reference (b):

a. Schedule and conduct vulnerability and risk assessments for DCI owned by the DoD Component in accordance with DCIP standards and benchmarks.

(1) Coordinate with the Chairman of the Joint Chiefs of Staff (CJCS) on vulnerability assessments scheduled by the DoD Component, or referred to the CJCS assessment program for execution.

(2) Provide risk and vulnerability assessment results to the appropriate DoD Components and DISLAs.

b. Develop, coordinate, and record courses of action regarding risk response options for appropriate DoD Components and DISLAs. Provide the status and progress of risk response and/or acceptance of risk to DCI assets controlled by the DoD Component.

c. Prepare and coordinate risk assessment options and recommendations for controlled DCI in accordance with Enclosure 3 of Reference (b) and this Volume.

5. PROCEDURES

a. The DCIP seeks to ensure the availability of DCI through a risk management approach. DCIP risk management is comprised of a risk assessment and appropriate risk response. The DCIP risk assessment process seeks to evaluate an asset's criticality (consequence of loss), the level and likelihood of threats or hazards, and associated vulnerabilities. Asset and mission owners must coordinate to determine the acceptable level of risk to the asset, and then determine the appropriate risk response. Risk response options include remediation of risk, mitigating the effects of loss once it occurs, reconstituting the asset's capabilities after loss, or simply accepting the risk.

b. This Volume identifies and discusses specific actions that are essential to developing and implementing a remediation plan. Remediation planning occurs after a risk assessment has been completed, but before an event occurs that could result in damage or degradation to the critical asset. This Volume is not intended to address requirements for executing other risk response activities, such as mitigation or reconstitution. Remediation planning shall consider a full range of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) options, such as improving doctrine; changing tactics, techniques, and procedures; implementing asset redundancy and/or resiliency; deceiving threat agents; or improving awareness, training, and education. Remediation is not limited to any one solution: it is taking whatever action is necessary, based on a risk management decision, to ensure the DCI is available when needed.

c. An effective remediation process shall include:

(1) Justification for remediation; rationale for why risk is unacceptable.

(2) Remediation options using a DOTMLPF approach; if a materiel solution is warranted, include a preferred cost-benefit action.

(3) Organizations internal and external to the Department of Defense that can assist in remediation planning and implementation.

(4) Management and stakeholders to be involved and informed during evaluating, planning, and implementing remediation options.

(5) Funds available and options for obtaining additional resources.

d. The goal of this Volume is to identify and implement cost-effective remediation. This requires a clear, efficient process that focuses limited DoD resources on the DCI with highest risk. The process described in the enclosure to this Volume is one such solution to apply or adapt, as needed, at all levels in the Department of Defense to ensure the availability of DCI. Other cost-effective remediation processes and solutions exist, and can be utilized as appropriate, provided they address the basic concepts in this Volume.

6. RELEASABILITY. UNLIMITED. This Volume is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Volume is effective immediately.

Peter F. Verga
Acting, Principal Deputy Under Secretary
of Defense for Policy

Enclosure
Procedures
Glossary

TABLE OF CONTENTS

ENCLOSURE

PROCEDURES

1. REMEDIATION PROCESS

a. Overview

(1) The risk to specific DCI shall be identified through a risk assessment accomplished by the DoD asset owner, or the asset owner's representative, and distributed to all DCIP community members with interest in the asset. DoD asset owners, in consultation with mission owners, will work with DISLAs to identify risk in the context of "end to end" functionality of the sector. When the risk to the supported mission is determined to be unacceptable, the DoD asset owner or installation commander, in concert with the mission owner, shall seek to reduce this risk through mitigating the impact that the loss of the asset would have on the DoD mission(s) by reducing or eliminating the threat or hazard or by remedying identified vulnerabilities. Non-DoD asset owners or their DoD representatives are encouraged to remediate risks or support the remediation of risk where appropriate in a similar fashion. For non-DoD owned critical infrastructure, the mission owners who rely on the asset in collaboration with the non-DoD asset owners and the asset owner's representative shall prepare mitigation plans in the event of the loss of this asset and coordinate through the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs to seek remediation of these assets through the Department of Homeland Security and the Department of State where appropriate.

(2) The DoD asset owner shall consult with the mission owner to determine the acceptable level of risk for the identified asset. When making risk trade-off decisions, it is essential to take into account cascade effects of such decisions. Non-DoD asset owners or the asset owner's representative should consult with the applicable mission owner and/or DISLA, as necessary, to determine the acceptable level of risk for DCI. If risk is determined to be unacceptable, the asset owner, in collaboration with the mission owner and/or DISLA, may choose to initiate remediation planning to reduce risk to an acceptable level. The mission and DoD asset owners will follow the DOTMLPF approach when developing options for remediation. If a materiel solution is chosen, but the cost exceeds the associated benefits, the mission and asset owners may elect to accept the risk. To ensure the proper level of risk acceptance is achieved, mission owners and appropriate DISLA interests must always be considered in the risk management decision and remediation planning process.

(3) Once a threat and hazard assessment and a vulnerability assessment of DCI are completed, the assessors notify the asset owner of the assessment results. The DoD asset owner initiates a risk assessment process involving the appropriate mission owners, DISLAs, and other interested parties as appropriate, to determine the acceptable level of risk. If risk is determined to be unacceptable and the decision to remediate is made, the remediation planning process begins. Remediation planning seeks to reduce the risk in the most cost-effective means possible.

(4) To achieve the best remediation results, the DCIP remediation planning process recommends asset owners seek support from those responsible for operating and maintaining the asset, the sector the asset falls under, as well as those reliant upon the asset. Obtaining different perspectives will likely result in a wider variety of remediation options to consider than those developed by the asset owner alone. More important, stakeholder involvement ensures an informed risk management decision.

b. Key Personnel Resources

(1) To facilitate and implement the risk response process, asset owners will establish a remediation team (RT) consisting of experienced personnel with the necessary expertise for developing and evaluating remediation options. Examples of RT personnel include (but are not limited to):

(a) Installation or Facility Staff. Representatives of the installation or facility staff have valuable expertise and should be contacted concerning issues such as long-term construction, consolidation, associated funding, and the budgeting process prior to forwarding to higher authorities such as Service or agency staff.

(b) Contracting Officer. The asset owner will contact the contracting officer to resolve and investigate risks arising from reliance on commercial services and infrastructure. Remediation options may include contracting with other commercial enterprises, negotiating contract modifications, or arranging for alternative sources for the commercial service or commodity.

(c) Critical Infrastructure Protection (CIP), Antiterrorism and Force Protection (AT/FP), and Physical Security Officers. These personnel may be either directly or indirectly responsible for installation physical security issues. Remediation options associated with the physical security of the asset include fencing, security lighting, security training, guard forces, physical barriers, entry control points, and other elements regarding the integrity of the installation and facility. Risk remediation issues within these individuals' purview are similar to those of the security officer.

(d) Security Officer. The security officer is responsible for protecting property on the installation; he or she often maintains contact with civilian law enforcement agencies with overlapping or neighboring jurisdiction. Security officers' expertise may assist in establishing memorandums of agreement (MOAs) or accessing local intelligence regarding threats. In many cases, this individual may also be the CIP or AT/FP officer.

(e) Engineering Field Personnel (EFP). EFP are subject matter experts (to include information technology (IT) specialists) that will be engaged when seeking engineering techniques or procedures as potential remediation options. Such techniques could include reengineering an existing asset to create a redundant capability.

(f) Public Works Officer (PWO) or Base Civil Engineer (BCE). The PWO or BCE will be consulted for remediation planning for both DoD and commercially-owned assets. In

most cases, PWO or BCE expertise is necessary for understanding the specific requirements of dependencies on commercial infrastructure. Commercial dependencies include reliance on outside electric power, telecommunications, natural gas, roads, railways, waterways, and any other services provided by a commercial vendor. Normally, the PWO or BCE is the primary interface with commercial providers. Contracting personnel will be included when negotiating remediation actions with commercial providers.

(g) DoD Component and DISLA CIP Staff. The CIP offices for the DoD Components or DISLAs can be good sources for providing "best practices" and solutions to similar or recurring risk situations. These organizations may also be able to provide additional funding or funding advocacy.

(h) Mission Owners. Those who rely upon a given DCI to perform their mission are often in the best position to provide insight on the critical capabilities the asset provides the mission(s), what the mission owner considers an acceptable level of risk, and what remediation options would best serve their interests. These organizations may also be able to provide additional funding or funding advocacy.

(i) Chief Information Officer (CIO). CIOs are responsible for all organization telecommunications and information networks and systems. They are best positioned to advice on broad aspects of security and survivability for these types of assets.

(j) Information Assurance (IA) or Information Security Staff Representative. These personnel are best positioned to provide essential detailed technical advice on measures to secure and assure information and telecommunications networks and systems.

(k) Operations Security (OPSEC) Officer. The Department of Defense regularly compromises significant critical and sensitive data due to OPSEC shortfalls. An OPSEC representative can provide operational advice and reviews of mitigation efforts from OPSEC perspective to ensure mitigation activities are, themselves, not compromising the critical asset.

c. Comprehensive Approach

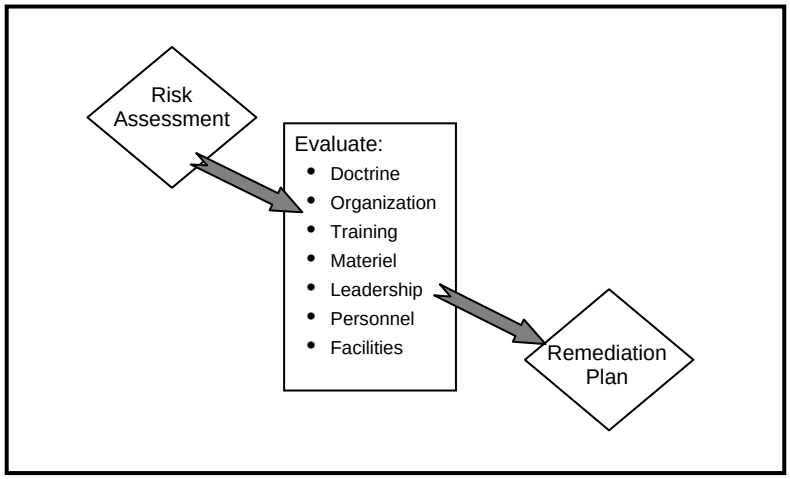
(1) The asset owner RT will focus their remediation efforts on those assets posing the highest risk to DoD missions. The RT should consider all risk remediation strategies during the planning phase. Figure 1 shows a comprehensive approach to developing remediation options.

(2) Remediation planners should analyze the impact remediation options have on the asset's ability to assure the required mission capability as well as the effect of reducing the risk to the asset. Potential subject areas that should be considered to ensure the highest potential for successful remediation include:

(a) Doctrine – Consider:

1. National policies, plans, and Unified Command Plan and OSD policy

Figure 1. Comprehensive Approach to Remediation Planning



2. MILDEP policy

3. Local policies

4. Procedures

5. Agreements with others (MOAs or memorandums of understanding (MOUs))

(b) Organization

1. Structure

2. Location

(c) Training

1. Formal

2. Informal

3. Situational awareness

(d) Materiel

1. Physical

2. Cyber

3. Access control

4. Redundancy with physical diversity

(e) Leadership

1. Leadership

2. Education

(f) Personnel

1. Military (Active or Reserve (drills or call-up))

2. Civilian (Government, full-time equivalent, part-time)

3. Contractors

(g) Facilities

1. Physical

2. Access (physical and electronic)

3. Security

4. Survivability

(3) As an example of the concept illustrated in Figure 1, an asset that relies on electrical power from a single source or via a single node would become unavailable if that single point of failure were interrupted. Obvious remediation options include establishing restoration priority with the commercial provider and implementing an emergency generator capacity. Table 1 provides a further illustration of the remediation planning process and identifies other options using the comprehensive approach.

d. Existing Procedures and Policy Products. While it would be impossible to describe every type of remediation option, there are some basic tools that fit many scenarios. The following examples provide workable options for many situations.

(1) MOUs or MOAs. To provide remediation options beyond the scope of authority of the Government asset owner, use an MOU or MOA where appropriate to describe the understanding or agreement between the asset owner and organizations outside the asset owner's organizational influence. For example, a building that contains DCI might be located at the edge of an installation or facility close to a civilian area. An MOU or MOA could be arranged with local law enforcement authorities to increase patrols in that area during periods of increased threat. At the strategic national level (when applicable), MOUs or agreements with State or host-nation authorities might need to be considered in order to provide greater force projection resiliency, flexibility, and capability for meeting operational planning requirements. Where

Table 1. Commercial Power Reliance Example

ISSUE*:* An asset is totally reliant on commercial power that enters the installation or facility through a single point; the entire installation is on a single feed. By disabling that single point of entry or any break in the circuit, all power to that critical asset could be cut off.

1) Doctrine**:**
   Are there changes in policy or processes that would provide a back-up or secondary source of power?
   Is it feasible to develop a plan that shifts critical functions to another location if the power is lost for an extended period of time?
2) Organization**:**
   Are remediation options involving organizational or location changes available?
   Can the asset's capabilities be temporarily transferred to another organization or location during a power outage?
3) Training**:**
   How might training alleviate the single source aspect?
   Can a manual means be devised and trained to provide the asset's capability in the event of a power loss?
4) Materiel**:**
   What procurement requirements would remediate this risk?
   Can an emergency generator or an uninterruptible power supply provide the necessary electricity while the utility company restores commercial power?
5) Leadership and Education**:**
   Does the risk require a top-level decision-making process?
   Can the responsible authorities provide an option for duplicating critical asset capabilities at another location?
6) Personnel**:**
   What are the additional personnel requirements for remediation options?
   Can the new requirements be accommodated by the existing workforce, or will the workload increase or require a new skill set?
7) Facilities**:**
   What contractual solutions are available? Establishing restoration priority with the commercial provider or establishing a secondary source of power to the asset may be viable options. Other contract options include implementing emergency generator power for critical function(s), including a service agreement to maintain and fuel the generator.

applicable, ensure that MOUs and MOAs incorporate Service level agreements, particularly for response and reconstitution.

(2) Program Objective Memorandum (POM). Where remediation requires significant resources or time beyond the current budget and budget year (such as construction of a redundant facility), the asset owner, through the mission owner or higher headquarters, would initiate a POM submission.

(3) Request for Supplemental or End-of-Year Funds. Implementing remediation options is often unplanned and costly. As a result, funding may not exist in an asset owner's budget to remediate risks. Based on the priority of the remediation need, asset owners should request supplemental or available end-of-year funding if the funding can be obligated within the fiscal year that funds are available.

(4) Integrated Priority List (IPL). During odd numbered years, some Combatant Commanders may have the option of submitting an IPL to address their most serious and pressing DCIP-related risks.

(5) Contract Language. When remediation is required for a contracted service or product, modification of the contract language may be a prudent step to ensure the necessary remediation takes place.

(6) Interservice Supply Support Agreement. This type of agreement provides recurring support to another DoD or non-DoD Federal activity.

(7) Policy Updates. Revise existing or develop new policies, as required.

(8) Operational Processes, Procedures, and Plans. Revise existing or develop new operational processes, procedures, and plans, as required (e.g., AT/FP, IT disaster recovery, continuity of operations/government (COOP) and/or COG).

e. Keep Appropriate Authorities Informed

(1) The appropriate authorities, including those of organizations reliant upon DCI, must be informed throughout the remediation planning and implementation process. Informing stakeholders is especially important when remediation falls outside the asset owner's scope of authority and where no remediation action is anticipated.

(2) When remediation appears to be complex, expensive, or requires significant time and manpower, the critical asset users' higher headquarters shall be notified and consulted in development of the plan of action. Higher headquarters' support for the remediation plan is, in most cases, crucial to obtaining funding.

2. BUILDING THE REMEDIATION PLAN

a. Preparation. Once the RT has analyzed remediation options and the asset owner, supported by appropriate mission owner(s) and DISLA(s) inputs, has selected the options to implement, the asset owner's staff will develop a plan of action and milestones (POA&M) outlining the remediation plan. Paragraph 2.b. provides a suggested timeframe and a six-step process to help develop an effective remediation plan.

b. Six Steps to an Effective Plan

(1) Confirm Stakeholders, Prioritize Risk, and Identify Options

(a) Establish a timeframe for completing this step (within 15 days after risk assessment is completed and report received).

(b) Identify parties that own, control, and rely upon the DCI. It is important to know who the "parties of interest" are so that those most relevant can be brought into the process early to identify the acceptable level of risk. Organize an RT of key participants based on the risk to be addressed.

(c) Prioritize risks based on impact to mission and probability of occurrence. Focus remediation efforts first on the greatest risks to critical missions and on those that can be fixed immediately.

(d) Identify options to reduce risk to an acceptable level.

(2) Analyze Options and Determine the Best Approach

(a) Establish a timeframe for completing this step (within 15 days after Step 1 is completed).

(b) Evaluate all options and determine those most executable, logical, cost effective, and likely to reduce risk to an acceptable level.

(c) Identify and implement protective and/or corrective options that collectively achieve either an avoidance of an interruption to the mission or graceful degradation of the critical asset should an incident occur. In addition to identifying realistic goals, an important consideration is the array of resources usually involved to implement a remediation option. Such resources are not just monetary; they also include:

1. Time required to implement remediation.

2. Human resources needed to execute the plan.

3. Impact the remediation effort may have on the relationship between an installation and the surrounding community.

4. Policies and operational plans, processes, and procedures to respond to and recover from critical asset outage or loss.

(d) Perform a cost-benefit analysis to balance risk to the asset and/or mission with the resource requirements necessary to execute a remediation plan. The most cost-effective solution may likely reduce risk to an acceptable level rather than eliminate it altogether.

(e) Determine the likely source(s) of and an OPR for funding for each option. Funding required outside of asset owner chain may impact remediation plan execution and should therefore be identified under cost-benefit analysis.

(3) Develop and Coordinate the Remediation Plan

(a) Establish a timeframe for completing this step (within 60 days after Step 2 is completed).

(b) Establish a remediation plan to include such elements as:

1. Criticality

a. Asset description (general information, e.g., location, points of contact (POCs)).

b. Consequence of loss (mission impact statement, missions supported).

c. Time to impact (time between the asset's loss and when the consequence of the loss is felt by the mission owner(s)).

d. Time to restore (estimated time to restore capability to the Department of Defense through reconstitution or reengineering of a similar asset's capability).

e. Additional consequences (impact on civilian population, economy, potential loss of lives or property, etc.).

2. Threat or hazard assessment

a. Review of threat level associated with asset.

b. Review of hazard level associated with asset and its location.

3. Vulnerability assessment

a. Summary of vulnerabilities (including statements on susceptibility, accessibility, and existing countermeasures).

b. Identification of vulnerabilities to be remediated.

4. Risk assessment

a. Asset owner (risk assessment level and acceptable level of risk).

b. Other(s) (acceptable level of risk to mission owner, DISLAs, etc.).

5. Risk management options

a. Assessment team options.

b. RT identified options.

6. Risk management decision

7. POA&M, with dates, required manpower, budget, etc.

8. Progress updates

9. Asset owner and stakeholder comments

10. Appendices, including (as applicable):

a. Submissions or narrative of actions with the POC.

b. Combating Terrorism Readiness Initiative Fund.

c. Manpower request.

d. Construction project request, as required by military construction submission (DD Form 1391, "Military Construction Project Data").

e. A record of systems to be updated and the data to be entered.

(c) Forward a copy of the plan in accordance with the organization's appropriate requirements for coordinating and tracking remediation efforts. Ensure all parties who rely upon the DCI are provided this information.

(4) Implement the Remediation Plan

(a) Establish a timeframe for completing this step (within 2-4 weeks of remediation plan approval, subject to funding and manpower approval as required).

(b) In most cases, start the remediation plan once all approvals have been received and issues such as manpower and scheduling are in line. It is important to realize that this process can take several years if it requires competing and securing funding through the POM process and conducting a contract competition. Additionally, to maintain support and adequate and proper visibility throughout the Military Department, organization, or agency, appropriate officials at all levels should be engaged in the process for those actions that cannot be implemented at the local level.

(c) Track the milestones, budget, time, and manpower in order to measure the plan's success.

(5) Keep Appropriate Officials Informed

(a) Implement at commencement, significant milestones, and completion of remediation plan.

(b) At plan execution, notify all interested parties from paragraph 2.b.(1) of this enclosure that remediation has begun. Completion of significant milestones may allow stakeholders to release or discontinue temporary solutions, equipment, plans, or procedures implemented to achieve acceptable levels of risk to mission assurance, so keep all parties informed of the progress. Once the plan is completed, notify these same parties. For multi-year remediation efforts, a yearly status report update should be submitted to these same parties detailing the remediation efforts to date along with an estimation of when the plan and its execution will be completed.

(6) Execute Follow-Up Actions

(a) Suggested timeframe for follow-up actions is no more than 3 years after risk assessment completion.

(b) In the case of defense critical assets (DCAs), schedule another risk assessment to be accomplished no more than 3 years after the completion of the last, or in the case of other DCI as may be directed. Where applicable, an annual review may be considered. Risk assessment coordination shall comply with DCIP policy.

c. Summary View of the Remediation Process. Table 2 lists the actions an asset owner should follow to develop an effective remediation plan.

3. SAMPLE CASES OF RISK REMEDIATION

a. Overview. This section provides examples of risks discovered during actual assessments and the actions available to remediate them. It is assumed that a risk assessment on these assets determined that the level of risk was unacceptable and the chosen risk response option was to conduct remediation. These examples include the defense industrial base (DIB), commercial, and DoD-owned critical infrastructure. In many cases, remediation actions can be applied to assets regardless of ownership.

b. Physical Security

(1) AT/FP Assessment. The assessment of physical or personnel security areas is often called an AT/FP assessment. In a broad sense, it is a look at the physical and personnel security and associated training that a facility uses to maintain both protection of critical infrastructure and a safe environment for asset or installation personnel and their families.

Table 2. Remediation Planning Process

Action	Description	Timeframe	Inform
Step 1: Confirm Stakeholders, Prioritize Risk, and Identify Options	Concerned parties involved determine acceptable level of risk; determine if remediation is warranted.	Within 15 days after risk assessment is complete.	Critical asset owner, DISLA, and mission owner leadership, operators, and maintainers.
Step 2: Analyze Options and Determine the Best Approach	RT recommends best approach to reduce risk to acceptable level.	15 days after Step 1 is complete.	Critical asset owner, DISLA, and mission owner leadership, operators, and maintainers.
Step 3: Develop and Coordinate the Remediation Plan	Asset owner staff develops POA&M to remediate critical asset risks.	Within 60 days after Step 2 is complete.	Critical asset owner, DISLA, and mission owner leadership, operators, and maintainers.
Step 4: Implement the Remediation Plan	Asset owner staff executes plan to remediate risk.	Within 2-4 weeks after approval of remediation plan by chain of command (subject to funding and manpower approval as required).	Critical asset owner, DISLA, and mission owner leadership, operators, and maintainers.
Step 5: Keep Appropriate Officials Informed	Asset owner staff prepares written report detailing remediation efforts.	At commencement; at achievement of significant milestones; yearly for multi-year efforts; and within 2-4 weeks after remediation plan completion.	Critical asset owner, DISLA, and mission owner leadership, operators, and maintainers.
Step 6: Execute Follow-Up Actions	Asset owner staff schedules follow-up vulnerability assessment.	In the case of DCAs, no later than 3 years after last vulnerability assessment; for other DCI, as directed.	Consistency with Reference (b).

(2) Example - Waterborne Attack

(a) Risk. A risk assessment at an installation discovered that DCI was at risk to waterborne attack because of poor lighting, lack of fencing, and related security measures near the piers. When ships were not present, there was virtually no security provided to the area adjacent to the water.

(b) Remediation. Fencing around the perimeter of the harbor could inhibit unauthorized personnel from entering the installation. Security patrols could monitor the area adjacent to the water, and lighting and motion detectors could alert security personnel to intrusions. Canine patrols could also be employed to further secure the area. The level of remediation implemented would depend on the level of risk that the asset and mission owners are willing to assume.

(3) Example - Telecommunications

(a) Risk. An assessment of an installation determined that all supporting telecommunications nodes were collocated in the same building just outside the confines of the installation. According to the assessment, the building's destruction would disrupt all installation local and long distance telephone service and have a significant impact on mission command and control.

(b) Remediation. The installation commander or asset owner could contact the local telecommunications provider to determine what capabilities might exist to provide continued service should the building be destroyed. Given proper planning with local service providers, the telecommunications provider could reroute traffic through another telecommunications node or provide portable and temporary service equipment to use during commercial service disruptions. Another means of remediation for some communications requirements might be achieved by ensuring that all key installation personnel had cellular telephones to use for mission execution.

c. Public Dependency

(1) The DoD mission depends upon public infrastructure networks and services in many cases, such as transportation, electric power, and communication networks. The DoD facility should establish good communications with public service providers about service requirements; that relationship does not have to wait for the identification of a vulnerability. The remediation of risks posed by commercial dependency may be more complicated than that of DoD-owned infrastructure. Public service remediation efforts should be coordinated through the facility's public works officer or base civil engineer, contracting officer, public affairs officer, legal officer, or other relevant personnel on the installation. Installation commanders or asset owners should also inform the applicable DISLA CIP staff (via the appropriate chain of command) and affected mission owners of remediation activity for these services.

(2) To remediate risks that involve a public utility, an asset owner would need the local facilities engineering support staff to take advantage of their contractual relationship with that provider. In some cases, the commercial enterprise (from power, telecommunications, water, rail, etc.) may willingly support changes that can remediate the risk based on customer relationships or a demonstrated business policy. Review service level agreements, acquisition programs, contracts, and operational processes for opportunities to address and include stronger resiliency language and requirements for future remediation efforts.

(3) In some cases, the commercial dependency is not directly connected to or may be located away from the DoD facility (such as a commercial port used to deploy forces). As such, the first challenge often comes with identifying appropriate POCs at the commercial facility. Commanders may consider requesting additional security measures or increased police patrolling at the commercial facility. For assets located outside the United States, coordination between the applicable geographic Combatant Commander and/or the State Department with the host nation may be required.

(4) Military operations are heavily dependent not just on computers and information technology, but also on shared critical information infrastructures and the IT foundation provided by the Global Information Grid. As a result, ensuring their availability, integrity, and resiliency is important to mission assurance. DoD computer systems and communications equipment must be protected and controlled to ensure those authorized to use them have access and those who would disrupt or corrupt them do not.

(5) For example, consider this case involving security awareness:

(a) Risk. An assessment of a DCI computer system disclosed that system users did not have an information security (IS) or IA awareness program. Furthermore, users demonstrated a lack of basic knowledge and skills for the safe, appropriate use of the system. The lack of user awareness and training presented a risk of serious compromise to the DCI.

(b) Remediation. Through remediation planning, the asset owner decides to implement IS and IA awareness training for all system users that requires at least an annual certification to demonstrate knowledge and understanding of policies and procedures. Alternatively, the asset owner could substitute manual processes for the automated system to eliminate the dependency on the DCI.

d. Emergency Management (EM), COOP, Consequence Management (CM) Planning

(1) The EM/COOP/CM planning for a critical asset should cover the four phases of a disruptive event for an asset: pre-event, response, recovery, and reconstitution. Such planning ensures continued operational capability during less than optimal conditions. The remediation activities in this Volume focus on the EM/COOP/CM planning done prior to any disaster event. These plans use a variety of terms to describe similar, continuity-type functions. An installation may employ a single, comprehensive plan or a series of integrated plans to coordinate its actions.

(2) For example, consider this case involving access for first responders.

(a) Risk. Assessors determined an installation's response plan called for tightly controlled access to a building housing DCI after a disruptive event. The access was controlled so tightly that emergency first responders would not be able to obtain access to fight fires, care for casualties, or prevent damage or destruction of the DCI.

(b) Remediation. The remediation option selected for the EM/COOP/CM plan should consider procedures allowing first responders access to areas of the installation requiring emergency support. Access to DCI should be tightly controlled, but it should not interfere with the emergency response. Installation commanders and asset owners should involve emergency responders in their pre-event planning.

e. DIB Products and Services. The Department of Defense relies on the DIB to provide goods and services necessary for mission execution. These cases provide examples of specific remediation actions for a DIB asset:

(1) Example - Manufacturing Capability

(a) Risk. DoD industry analysts evaluated a sole-source supplier and discovered it developed subcomponents that are integrated into more than 30 DoD programs supporting combat operations. A DoD team performed a site risk assessment that determined the loss of the facility and the associated capability would severely affect DoD ability to execute numerous combat roles and missions.

(b) Remediation. The Department of Defense collaborated with the company to analyze remediation options. The Department performed a long-range market forecast that supported a business case for duplicating the capability at another facility in a different geographic location.

(2) Example - Law Enforcement Presence

(a) Risk. There is a cluster of DIB critical asset sites located in close proximity. During a DCIP awareness visit, DoD personnel learned of plans to reduce the local police force due to budgetary constraints, posing an increased security risk to the DIB sites.

(b) Remediation. DoD personnel informed the Department of Homeland Security. The local police force became a candidate for a Federal grant.

4. REMEDIATION PROCESS TIMELINE AND CHECKLIST

a. Within 15 days after the risk assessment is completed:

(1) Identify the stakeholders for RT.

(a) Contracting officer

(b) CIP or antiterrorism officer

(c) Security officer

(d) EFP

(e) Information systems security officer

(f) PWO or BCE

(g) Support staff to the asset or installation

(h) Others, as required

(i) CIP working group members

(2) Prioritize the risks for remediation.

(3) Identify the acceptable level of risk for the DCI.

(4) Identify potential remediation options using the DCIP remediation planning process comprehensive approach.

b. Within 15 days after Step 1 is completed, evaluate and rank options: weigh risk to asset or mission versus cost.

c. Within 60 days after Step 2 is completed:

(1) RT produces remediation plans with timelines for accomplishing selected approach and distributes to stakeholders.

(2) Asset owner or installation commander seeks support for resources required to implement selected remediation options through chain of command to include, as appropriate, affected Combatant Commanders.

d. Within 2-4 weeks of remediation plan approval (subject to funding and manpower approval as required):

(1) Asset owner or installation commander implements remediation plan.

(2) Appropriate authorities and interested parties (Mission Owners and DISLAs) are notified of remediation plan.

e. One year after receipt of risk assessment report, as applicable, if effort is long term, a follow-up report regarding status and estimate of completion is provided to relevant authorities and interested parties.

f. Three years after risk assessment, the next risk assessment is due (in the case of a DCA or as directed for other DCI).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AT/FP	antiterrorism and force protection
BCE	base civil engineer
CIO	Chief Information Officer
CIP	critical infrastructure protection
CJCS	Chairman of the Joint Chiefs of Staff
CM	consequence management
COOP	continuity of operations
DCA	defense critical asset
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DIB	defense industrial base
DISLA	Defense Infrastructure Sector Lead Agent
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EFP	engineering field personnel
EM	emergency management
IA	information assurance
IPL	integrated priority list
IS	information security
IT	information technology
MOA	memorandum of agreement
MOU	memorandum of understanding
OPSEC	operations security
POA&M	plan of action and milestones
POC	point of contact
POM	program objective memorandum
PWO	public works officer
RT	remediation team

PART II. TERMS AND DEFINITIONS

asset. Defined in Reference (a).

asset owner. Defined in Reference (b).

defense critical infrastructure. Defined in Reference (a).

DISLA. Defined in Reference (a).

mission owner. Defined in Reference (b).

remediation. Defined in Reference (a).

risk. Defined in Reference (a).