Strategy for Defense Critical Infrastructure

Department of Defense
Washington, D.C.

March 2008

Table of Contents

Foreword

As discussed in the *Strategy for Homeland Defense and Civil Support*, DOD relies on a worldwide infrastructure to execute its missions in a global environment. As such, DOD needs to understand from a global perspective the risks to the infrastructure upon which its missions rely. Defense Critical Infrastructure (DCI) is composed of functional sectors that provide the operational and technical capabilities essential to mobilize, deploy, and sustain military operations in peacetime and war.

Assessing the risk to and mitigating potential effects on DCI are essential to ensuring the mission readiness of our military forces to protect the United States and to project power globally. Because resources are constrained, however, uniform security of all DCI is not possible. Instead, DOD prioritizes DCI assets based on their criticality to executing the National Defense Strategy and seeks to minimize their vulnerability with an integrated risk management approach.

As the DOD Principal Staff Assistant responsible for ensuring DCI resiliency, I established the Defense Critical Infrastructure Program (DCIP), through which the identification, prioritization, assessment, and assurance of DCI are managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect DCI-related sensitive information.

To codify and standardize this effort, I am releasing this *Strategy for Defense Critical Infrastructure*, and I am confident that it will significantly improve DOD's ability to provide for a more resilient and flexible DCI.

Paul McHale
Assistant Secretary of Defense
for Homeland Defense and
Americas' Security Affairs

Executive Summary

The Defense Critical Infrastructure Program (DCIP) *Strategy for Defense Critical Infrastructure* articulates the approach required for ensuring the availability of assets deemed essential to the successful completion of DOD missions in an all-threat and all-hazard environment. This strategy recognizes that although safeguarding the reliability of the nation's critical infrastructure will require a national effort, executing the strategy will provide defense stakeholders with a better understanding of what DOD must do to confirm the availability and resiliency of Defense Critical Infrastructure (DCI).

The United States currently faces a dynamic, flexible, and very pragmatic adversary. Due to the unconventional nature of the terrorist threat and the asymmetrical tactics demonstrated both at home and abroad by our enemies, we can no longer expect the protection formerly provided by the oceans bordering our coasts to serve as an effective deterrent to attack. The attacks of September 11, 2001, and other events demonstrated that an act of terrorism can cause worldwide infrastructure asset disruption. In the past decade, hurricanes or other violent storms have also revealed that our infrastructure assets are at risk from destruction, degradation, or disruption by natural events. Given scarce resources, this Strategy's objectives must be balanced against other priorities outlined in the National Defense Strategy.

DOD will implement this *Strategy for Defense Critical Infrastructure* to ensure we are prepared for threats and hazards that may affect our infrastructure assets. Actions to reduce or mitigate the risks to infrastructure could include, but are not limited to, changing tactics, techniques, or procedures; adding redundancy; selecting alternate ways to perform functions; isolating or hardening; and guarding.

Critical Infrastructure Protection in a Global Environment

The ability of DOD to accomplish its assigned missions depends on a global array of critical infrastructure. This global infrastructure is owned, leased, and/or operated by DOD, other government organizations, the private sector, foreign governments, and foreign industry. Furthermore, these global infrastructure assets have vulnerabilities that, if exploited, may affect the ability of DOD to perform its missions.

Organizing and Integrating Critical Infrastructure Activities

Defense Critical Infrastructure is a complex, interdependent, and decentralized network of public and private-sector systems, services, people, and processes. DCI provides the operational and technical capabilities that are essential to project, support, and sustain military forces and operations worldwide in times of peace and war in support of the National Military Strategy. Additionally, DOD must collaborate with the Critical Infrastructure Protection (CIP) efforts of the Department of Homeland Security and the Department of State to ensure all national and international CIP-related policy issues that

are important to supporting the missions of DOD are properly addressed.

Mission, Vision, and Goals

The mission of the Defense Critical Infrastructure Program (DCIP) is to *enhance the risk management decision making capability at all levels to ensure that Defense Critical Infrastructure is available when required,* and the DCIP vision to accomplish that mission is to *ensure the availability of Defense Critical Infrastructure in an all-threat and all-hazard environment.* Effective risk management in support of the DCIP requires participation at all levels of DOD. Although this Strategy focuses on those assets deemed critical at the department-level, the goals, objectives, and processes described within can be adapted by lower echelons of command/organization to support their own critical infrastructure assurance activities. Accordingly, effective risk management decision-making rests on accomplishing the following five goals:

- Provide DCIP Policy and Program Guidance
- Foster DCIP Strategic Partnerships and Enabling Technologies
- Integrate and Implement DCIP Plans, Programs, and Capabilities at All Levels
- Facilitate DCIP Resourcing at All Levels
- Promote DCIP Education and Outreach

Managing Risks Effectively

There are insufficient resources to remediate all risks to all infrastructures from all threats and hazards at all times. Accordingly, DOD will apply a *risk management* approach to protecting DCI. DOD must know what infrastructure assets are critical to DOD missions, what vulnerabilities the assets have, and what threats and hazards to the assets exist. Armed with this *risk assessment* information, decision makers can make informed risk management decisions and apply appropriate *risk management response* measures.

Implications of the Strategy

In developing this Strategy, DOD took into account likely resource and technology implications. Given scarce resources, this Strategy's objectives must be balanced against other priorities outlined in higher-level DOD strategies. As DOD Components and Defense Infrastructure Sector Lead Agents (DISLAs) implement the tenets outlined in this document, a more precise accounting of the required procedural changes, technological advances, and personnel, material, and financial resources will be needed.

This risk management approach will support the prioritization of scarce resources across DOD, focusing priorities on assets at greatest risk based on assessed criticality, vulnerability, and threats and hazards.

To accomplish this end, the DCIP will implement a criticality and sector characterization process to identify DOD's DCI. Through a threat and hazard identification process, the DCIP will further define the potential for loss of DCI assets, and in conjunction with the vulnerability assessment process, will ascertain the assets' inherent weaknesses. The analytic results of these incremental processes will thus allow appropriate DOD decision-makers the capability to properly assess the levels of risk to these critical assets.

Informed risk management decisions can then take place, allowing for appropriate response measures that may include acceptance of the risk, remediation and/or mitigation options, and reconstitution planning.

Ultimately, the DCIP seeks to make DOD more resilient to both natural and man-made events that could disrupt military operations, while seeking to provide the requisite redundancy for those critical assets, the loss of which would prevent DOD from meeting its National Defense Strategy requirements.

For an effective DCIP, DOD must institutionalize the program department-wide by implementing policy and establishing procedures. These actions will provide more focused guidance on the roles and responsibilities of the members of the DCIP community, as well as ensure consistent and coordinated risk management efforts across DOD. Additionally, the DCIP must be nested with all other risk management activities that contribute to force protection, antiterrorism, Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) readiness and consequence management, continuity of operations, and information assurance to contribute effectively to a DOD mission assurance construct.

I. Context

Expanding on the *Strategy for Homeland Defense and Civil Support*, the *Strategy for Defense Critical Infrastructure* focuses on ensuring the availability and protection of Defense Critical Assets (DCAs), a core capability for achieving mission assurance.

Key Definitions

Assessment. In the context of the DCIP, a systematic examination using disciplined processes, methods, and tools that provide an environment for decision makers to continuously measure, evaluate, and prioritize a particular issue.

Asset. In the context of the DCIP, 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.

Asset Owner. The DOD Components with responsibility for DOD assets, or organizations that own or operate non-DOD assets.

Characterization. In the context of the DCIP, the analytic decomposition of functions, systems, assets, and dependencies as they relate to supporting DOD operational capabilities and missions.

Defense Critical Asset (DCA). An asset of such extraordinary importance to DOD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of DOD to fulfill its missions. DCAs are selected from previously identified Task Critical Assets.

Defense Critical Infrastructure (DCI). The composite of DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide. Defense Critical Infrastructure is a combination of Task Critical Assets and Defense Critical Assets.

Defense Critical Infrastructure Program (DCIP). A DOD risk management program that seeks to ensure the availability of assets critical to DOD missions. Activities include the identification, assessment, and effective management of risk to assets essential for executing the National Defense Strategy.

Defense Industrial Base (DIB) Defense Infrastructure Sector. The nation's worldwide industrial complex with capabilities to perform research and development and to design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Defense Infrastructure Sector. A virtual association within the DCIP that traverses normal organizational boundaries, encompasses defense networks, assets, and associated dependencies that perform similar functions within DOD, and are essential to the execution of the National Defense Strategy.

Hazard. In the context of the DCIP, non-hostile incidents (such as accidents, natural forces, and technological failure) that cause loss or damage to infrastructure assets.

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities

that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.

Mission Owner. A DOD organization having responsibility for the execution of missions assigned by statute or by the Secretary of Defense, and supporting organizations with responsibility for execution of all or part of those missions.

Mitigation. Planning actions taken in preparation for an event, or implemented in response to a warning, or after an incident occurs, that are intended to lessen potential adverse effects on military operations or infrastructure.

Reconstitution. In the context of the DCIP, the process of restoring critical assets and their necessary infrastructure support systems or their functionality to pre-incident operational status.

Remediation. Actions taken to reduce risk. These actions are undertaken once a risk has been identified.

Resiliency. In the context of the DCIP, the capability of an asset, system, or network to maintain functionality during, or to recover from, a terrorist attack, natural disaster, or other incident.

Risk Assessment. A systemic 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.

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 Response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation.

Task Critical Asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious and debilitating effect on the ability to execute the task or Mission-Essential Task the asset supports.

Threat. In the context of the DCIP, an adversary having the intent, capability, and opportunity to cause loss or damage..

Vulnerability. In the context of the DCIP, the characteristics of an installation, system, asset, application, and/or the associated dependencies that could permit a degradation or loss as a result of having been subjected to a certain level of threat or hazard.

Authorities and Guidance

In Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003, the President assigned two sets of responsibilities to DOD. First, DOD, like all other Federal Departments, must "identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of all-hazard efforts that would destroy, incapacitate, or exploit them." Second, HSPD-7 designates DOD as the Sector-Specific Agency (SSA) for the DIB. As the SSA for the DIB, DOD is responsible for collaborating with all relevant organizations, conducting or facilitating vulnerability assessments, and for encouraging risk management strategies

to protect against attacks on the DIB. SSAs are responsible for working with the Department of Homeland Security (DHS) to implement the National Infrastructure Protection Plan (NIPP) sector partnership model and risk management framework, to develop protective programs and related requirements, and to provide sector-level Critical Infrastructure and Key Resource (CI/KR) protection guidance. SSAs are also responsible for identifying, prioritizing, and coordinating the protection of sector-level critical infrastructure and for managing the overall process of building security partnerships.

The National Strategy for Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, HSPD-7, and the 2006 *National Infrastructure Protection Plan* focus on the national policy, guidance, and planning necessary to secure critical infrastructure. Related documents and strategies issued by DOD have expanded on this baseline to detail DOD Critical Infrastructure Protection (CIP) efforts. The March 2005 *National Defense Strategy (NDS)* outlines an active, layered approach to the defense of the United States and its interests. Included within this active, layered approach is the immediate physical defense of the United States, which includes potential military missions at home to defend, among other things, critical infrastructure from external attack. Furthermore, in an effort to operationalize the *NDS*, DOD senior civilian and military leaders identified "Defending the Homeland in Depth" as one of four priority areas examined during the *2006 Quadrennial Defense Review (QDR)*. Elaborating on this theme, the 2005 *Strategy for Homeland Defense and Civil Support* specifically identifies preparedness and protection of DCI as one of the core capabilities to achieve mission assurance.

Although many systems can easily be identified as "critical" to DOD, analysis that stops at this level is insufficient to meet program needs. Analysts must further seek to identify the specific assets of each system that supports a given mission in order to identify vulnerabilities of these assets and to identify remediation or mitigation options that are specific to the assessed risks.

This Strategy incorporates the national responsibilities assigned by HSPD-7, the *Strategy for Homeland Defense and Civil Support*, and associated risk management policies, and defines through stated goals and objectives how DOD will ensure the availability of DCAs to achieve mission success. Although this Strategy applies specifically to DOD, it is consistent with the risk management framework described in the NIPP.

Defense Critical Infrastructure in a Global Environment

DOD relies on infrastructure consisting of physical, human, and information assets. Such infrastructure includes DOD assets, other Government (non-DOD) assets, and privately owned assets, both domestic and foreign . These assets provide the operational and technical capabilities required to project, support, and sustain military forces and operations worldwide.

The DCIP focuses on domestic and foreign assets that are critical to DOD missions. Some of these assets reside on military installations and/or are owned, leased, or operated by DOD. DCIP can take direct steps to manage risks to these assets.

Other assets that are not owned by DOD, but support its missions, include other Government-owned assets, commercial assets, foreign assets, and DIB assets. Although DOD may be limited in the direct application of resources for their protection, identifying non-DOD owned assets is crucial to the risk management framework. DOD must therefore work collaboratively with these asset owners to encourage and facilitate the management of risks to these assets.

Figure 1 depicts the relational framework among the three categories of infrastructure and assets with which the DOD is concerned.

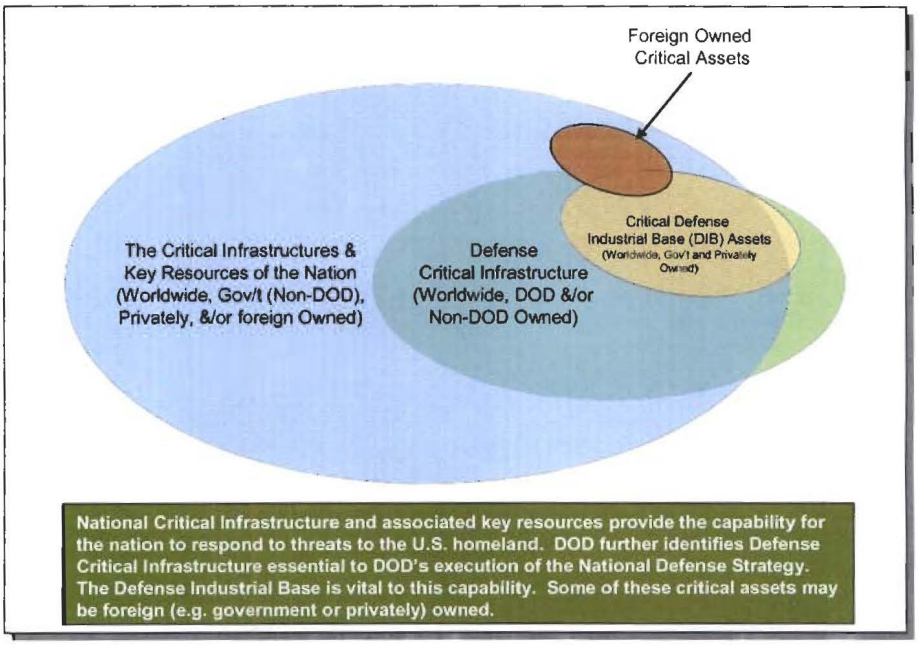

Figure 1

Execution of DOD's responsibility as the DIB SSA fits well within the framework of "Lead, Support, and Enable" as enunciated in the *Strategy for Homeland Defense and Civil Support*. To execute its DIB SSA responsibilities successfully, DOD must engage in ongoing activities to build trust with the DIB critical asset owners and operators to support information sharing.

Finally, as outlined in the *Strategy for Homeland Defense and Civil Support*, the President or the Secretary of Defense might direct U.S. military forces to protect non-DOD assets of national significance that are so vital that their incapacitation could have a debilitating effect on the security of the United States.

Organizing and Integrating Critical Infrastructure Activities

The DCIP is a DOD-wide effort involving stakeholders from the Office of the Secretary of Defense (OSD), the Joint Staff, the Combatant Commands, the Military Departments, the Defense Agencies and

Field Activities, the Defense Infrastructure Sector Lead Agents (DISLAs), and the National Guard Bureau (NGB). These DOD stakeholders and officials must work together, form partnerships, and integrate their activities in order to accomplish the goals outlined in this Strategy. Additionally, DOD must collaborate with the national infrastructure efforts of the Department of Homeland Security and the international infrastructure protection efforts of the Department of State to ensure all infrastructures important to supporting the missions of DOD are addressed. The DCIP roles and responsibilities of each DOD stakeholder, to be elaborated in follow-on issuances, are summarized below.

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA))

Under the direction and control of the Under Secretary of Defense for Policy, the ASD(HD&ASA) is responsible for DCIP policy and program direction, and oversight. The ASD(HD&ASA) represents DOD on all DCIP-related matters with the Executive Office of the President, DHS, other Federal agencies, and state and local entities as appropriate.

Commensurate with responsibilities assigned to DOD in HSPD-7, the ASD(HD&ASA) assists the Secretary of Defense (SecDef) as the lead SSA official for the DIB. Furthermore, the ASD(HD&ASA) is the approval authority for determining which assets are identified as Defense Critical Assets (DCAs).

Joint Staff

The Joint Staff will prepare an integrated, prioritized list of Combatant Command, Military Department, and DISLA-nominated Task Critical Assets (TCAs) to support assessment and risk management activities and will nominate a list of potential DCAs from all submitted TCAs to ASD(HD&ASA) for final validation and approval.

The Joint Staff will assess the capability of the Combatant Commands and Military Departments to monitor and report all relevant DCIP-related data on threats, hazards, vulnerabilities, and related trends, as well as assist the Under Secretary of Defense for Intelligence (USD(I)) and the ASD(HD&ASA) in implementing processes for monitoring, reporting, and sharing DCIP-related information.

The Joint Staff will establish and execute a DOD DCIP vulnerability assessment program in concert with the ASD(HD&ASA), serving as the focal point for consolidation of the assessment data. This program will include an annual assessment schedule that is coordinated through the DOD Components and DISLAs and will outline the Joint Staff's plan for the assessment of DCAs.

The Joint Staff will advise ASD(HD&ASA), the DOD Components, and DISLAs about military operational requirements to prevent or mitigate the loss or degradation of DOD-owned DCAs and of non-DOD owned DCAs within the respective areas of responsibility of the regional or functional Combatant Commanders.

The Joint Staff will further review DCIP-directed readiness and risk management plans developed and submitted by the

Military Departments and will integrate DCIP functions and activities into joint planning, doctrine, training, and exercises.

Combatant Commands

As Mission Owners, the Combatant Commands will lead efforts to identify mission capability requirements and coordinate with the Military Departments, Defense Agencies, DOD Field Activities, and Defense Infrastructure Sector Lead Agencies to identify those Task Critical Assets (TCAs) necessary for accomplishment of each assigned mission. Combatant Commands will then submit a list of identified TCAs to the Joint Staff for consideration as DCAs.

The Combatant Commands will also nominate assets to the Military Departments and Joint Staff for assessment and remediation; monitor and respond to threats and hazards to assets within their area of responsibility; and mitigate, through planning and post-incident efforts, the effect of the loss or disruption of TCAs for their missions.

Military Departments, Defense Agencies, and DOD Field Activities

As Mission Owners, the Secretaries of the Military Departments and Directors of Defense Agencies and DOD Field Activities will lead efforts to identify mission capability requirements. They will coordinate with other Military Departments, Defense Agencies, DOD Field Activities, and DISLAs to identify those TCAs necessary to accomplish each assigned mission. Each will then submit a list of TCAs to the Joint Staff for consideration as DCAs.

As asset owners and capability providers, they will coordinate with the Combatant Commands and DISLAs to identify and prioritize the assets required to support Combatant Command Mission-Essential Tasks.

Asset owners will monitor and report threats and hazards to TCAs, assess identified TCAs to identify vulnerabilities, and develop and implement appropriate remediation strategies. Furthermore, they will assist mission owners to mitigate, through planning and post-incident efforts, the effect of the loss or disruption of DCI assets on their missions. Asset owners are also responsible for reconstitution of critical asset-provided capabilities.

Defense Infrastructure Sector Lead Agents

DISLAs are designated defense sector organizations that perform Defense Infrastructure Sector responsibilities. In coordination with their respective Principal Staff Assistants (PSAs), DISLAs will characterize their respective defense infrastructure sector, identifying functions, systems, and ultimately sector TCAs that support Combatant Command, Military Department, and Defense Agency missions and sector functions. They will collaborate with other DISLAs and DOD Components to identify interdependencies. Each DISLA will submit a list of TCAs related to sector functions to the Joint Staff for consideration as DCAs.

DISLAs will monitor threats to sector TCAs, recommend assets for assessment and remediation, and assist Mission Owner efforts to mitigate, through planning and post-incident efforts, the effect of the loss or

disruption of identified DCAs to assigned missions.

DISLAs are also responsible for analyzing how potential or real-world events affect the overall health of their respective sectors.

National Guard Bureau (NGB)

The NGB is unique in that it provides support to both the Federal government and State governors. This role provides the NGB an ability to serve as a liaison between DCIP and local commercial infrastructure providers and members of the DIB regarding National Guard (NG) matters.

In this regard, the NGB may facilitate vulnerability assessments of DIB sites by NG vulnerability assessment teams, therefore ensuring these limited resources deploy to high-priority locations in a timely manner and in response to emerging threats. Accordingly, the NGB should develop a capability to review and assess risk to DIB facilities and respond to related requirements as part of pre-deployment preparation, planning, and coordination of NG forces to protect critical infrastructure sites. Risk assessments significantly contribute to the overall DOD effort to assess and, when tasked, protect critical DIB infrastructure.

Mission, Vision, and Goals

The DCIP is primarily concerned with global, strategic missions and their direct support. By identifying DCAs, assessing related threats and vulnerabilities, and analyzing relevant infrastructure data, DOD will be positioned to make risk management decisions to ensure the appropriate infrastructure assets are available, when needed, to support DOD missions.

- **DCIP Mission:** Enhance risk management decision-making capability at all levels to ensure that Defense Critical Infrastructure is available when required.
- **DCIP Vision:** Ensure the availability of Defense Critical Infrastructure in an all-threat and all-hazard environment.
- **DCIP Goals:** To achieve the DCIP mission and vision, DOD has identified five goals.
    1. Provide DCIP Policy and Program Guidance
    2. Foster DCIP Strategic Partnerships and Enabling Technologies
    3. Integrate and Implement DCIP Plans, Programs, and Capabilities at All Levels
    4. Facilitate DCIP Resourcing at All Levels
    5. Promote DCIP Education and Outreach

Managing Risks Effectively

DOD will protect DCI through a risk management approach that supports the prioritization of scarce resources, while focusing priorities on assets at greatest risk based on assessed criticality, vulnerability, and threats and hazards.

The immense scope of infrastructure assets and the interdependent nature of their environments necessitate a comprehensive risk management effort. Providing complete assurance of every critical asset from all conceivable threats or hazards is

not feasible. Therefore, DOD will apply the principles of risk management to DCI.

Risk management principles will be applied by first performing a *Risk Assessment* to understand (1) what assets are *critical* to DOD missions and why (i.e., what is the consequence of disruption or loss?), (2) identifying *threats and hazards* to those assets, and (3) identifying *vulnerabilities* of those assets. DCIP risk assessment practices will result in sufficient information to support DCIP risk decisions.

Decision makers will use the results of the assessment to determine appropriate *Risk Response* measures. Such measures may include choosing to accept the identified risk, minimizing the effect of a potential threat or hazard (i.e., *mitigation*), applying resources to reduce the identified risk (i.e., *remediation*), , and restoring lost capability in the aftermath of an event (i.e., *reconstitution*).

Risk Mitigation Options

Risk mitigation options that address risk to DCI may include, but are not limited to, changing tactics, techniques, or procedures; adding redundancy; selecting alternate ways to perform functions; isolating or hardening identified critical assets; and physically guarding previously unprotected assets. These mitigation options should be adapted as the situation demands and risk changes.

Risk Management Decision Process

When addressing DCAs, senior DOD leadership will review a summary of the alternatives subordinates considered to address the risk. This summary will include a statement of the common factors used to evaluate risk response alternatives, and the findings from the evaluation of each alternative. Additionally, the Asset and Mission or Function owner must provide a cost-benefit judgment about how effectively each alternative addresses the risk to the DCA. This risk management decision will also apply to the evaluation of TCAs.

Effective risk management decision-making activities must include:

- Determining which *risk response options* are most appropriate in a given situation and the most cost effective means for reducing risk to an acceptable level.
- Determining the *priority* for a given risk response relative to other projects that impact a *specific* mission.
- Determining the *priority* for a given risk response relative to *all other DCIP projects* that impact the DOD's ability to execute the National Military Strategy.

A need exists for the development of a risk management decision-making process and the identification of information required to execute the process. The latter must be defined in terms of expected outputs from the threat, vulnerability and criticality elements of the risk assessment as implemented by the appropriate DOD Components. Defining the information needed to make risk management decisions will establish a unifying framework that is logical, repeatable, consistent, and effective, which will allow the Department to focus limited resources on assets at highest risk.

Figure 2 shows the key elements of DCIP risk management.

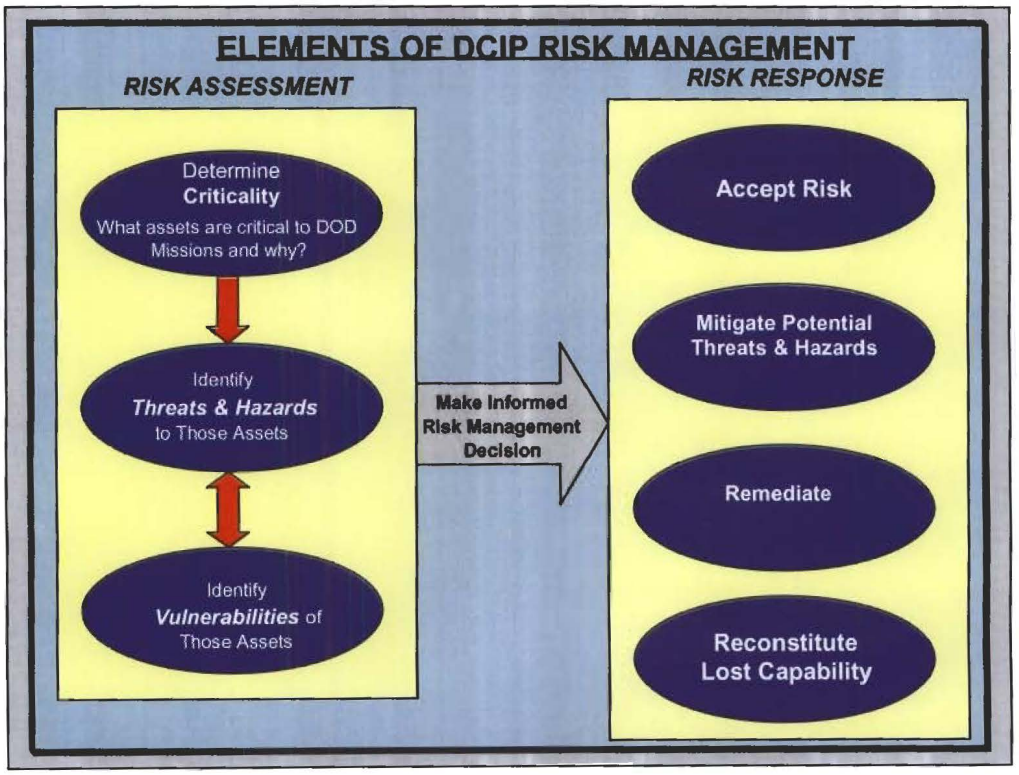
ELEMENTS OF DCIP RISK MANAGEMENT
RISK ASSESSMENT
RISK RESPONSE
Determine
Criticality
What assets are critical to DOD Missions and why?
Identify
Threats & Hazards
to Those Assets
Identify
Vulnerabilities of
Those Assets
Make Informed
Risk Management
Decision
Accept Risk
Mitigate Potential
Threats & Hazards
Remediate
Reconstitute
Lost Capability

Figure 2.

II. Program Goals and Objectives

The DCIP seeks to reduce the risks to DCAs, thus enabling the execution of DOD-level missions, regardless of threat or hazard. The program will achieve this by enhancing the ability of DOD leadership, at all levels, to make risk management decisions about those assets critical to the National Defense Strategy. Effective risk management decision-making rests on accomplishing the following five goals and their respective objectives.

Goal 1: Provide DCIP Policy and Program Guidance

To accomplish the implementation processes outlined in this document, DCIP community members will coordinate and publish the necessary guidance to implement these steps.

Objective 1: Develop appropriate DCIP policy and guidance

The *Strategy for Homeland Defense and Civil Support* lists preparedness and protection of DCI as a core capability in achieving a key Department objective of mission assurance. Building on this foundational document, additional DOD issuances are being developed to define specific roles and responsibilities and outline program implementation guidelines. DOD Components and DISLAs should issue their own guidance and implementing documents with respect to internal DCIP activities.

To provide comprehensive program guidance, the DCIP is developing a series of overarching documents. These documents include this strategy, a program directive, implementation guidance, standards and benchmarks, handbooks, a security classification guide, and various memoranda of agreement.

Objective 2: Coordinate DCIP interests with other DOD policy and guidance

DOD will review all other applicable DOD issuances to ensure that DCIP roles and responsibilities are defined and implemented appropriately.

As guidance documents are prepared, the DCIP community will have opportunities to coordinate and comment, ensuring their interests are represented appropriately.

Objective 3: Enhance Ability to Achieve Mission Assurance

DOD will develop and implement policy and guidance that seamlessly integrates with complementary activities that contribute to DOD's ability to achieve mission assurance, including force protection, antiterrorism, continuity of operations, critical infrastructure protection, CBRNE readiness and consequence management, and information assurance.

Objective 4: Coordinate DCIP interests with non-DOD guidance, including national and international policy development

DOD will actively participate in the Federal interagency coordination process to ensure DCIP interests are addressed in strategies, policies, plans, publications, guides, and memoranda of agreement.

DOD will examine all applicable Presidential Directives and Executive Orders (EO) to ensure the DCI mission is not affected adversely by the proposals or activities of other Federal Departments or Agencies and to ensure total collaboration with interagency partners as DOD executes its responsibilities as the DIB SSA. This action ensures that DOD is able to identify and protect all DCIP equities and participate, when necessary, in the interagency process. This action further ensures that DOD perspectives on protecting DCI assets, including the DIB, are accurately and appropriately represented.

In coordination with the Department of State and other Federal entities, DOD will ensure that DCI is addressed in relevant policy documents. These documents may include: host-nation agreements; the Security and Prosperity Partnership between the United States, Canada, and Mexico; the DIB Sector Specific Plan; and North Atlantic Treaty Organization strategies. Regional Combatant Commanders should coordinate on CIP issues within their areas of responsibility, at a minimum, through the Theater Security Cooperation Plan and bilateral initiatives.

Goal 2: Foster DCIP Strategic Partnerships and Enabling Technologies

The DCIP will identify interagency and international information sharing partners, while fostering an effective data sharing environment through the establishment of integrated enterprise architecture.

Objective 5: Establish interagency and international information sharing agreements

DOD will identify interagency and international information sharing partners for DCIP. DOD will coordinate and collaborate with these partners, via appropriate national and international channels, to establish memoranda of agreement or appropriate bilateral or multilateral agreements for sharing critical infrastructure information.

Objective 6: Establish a DCIP common operating picture

DOD will establish specifications and standards to unify the disparate DCI datasets supporting DOD missions into a DCIP common operating picture. Thus established, the DOD Community of Interest (COI) will share information requirements and essential elements of information, along with protocols and standards for a common operating environment.

The resultant common operating picture will be incorporated into command and operations centers throughout DOD, such as the National Military Command Center, Service Operations Centers, and Combatant Command and Joint Emergency Operations Centers, as needed.

Goal 3: Integrate and Implement DCIP Plans, Programs, and Capabilities at All Levels

The DCIP requires active participation from the highest to the lowest levels of DOD. Only through close coordination of efforts among the DCIP COI can the program's processes be successfully implemented.

Objective 7: Identify and maintain a list of Defense Critical Infrastructure

DOD will conduct an in-depth characterization of Defense Infrastructure Sectors, as well as mission decomposition of Combatant Commands, Defense Agencies, Defense Field Activities, and Military Departments to identify TCAs. These assets will then be vetted through the Joint Staff and selectively recommended to the ASD(HD&ASA) for final approval as DCAs. The Joint Staff should ensure the list is reviewed and updated regularly as asset owners report on the readiness of their assets.

Objective 8: Report threats and hazards potentially affecting Defense Critical Infrastructure

DOD will develop and maintain appropriate and adequate threat and hazard operational analysis capabilities, including reporting and supporting procedures and protocols linked to identified DCI Assets. Results of any threat and hazard operational analysis will be maintained in a secure web portal or database. This comprehensive approach will establish ready access to an accurate, visible, and understandable, authoritative data source as part of the overall DCIP Enterprise Architecture.

Objective 9: Assess Defense Critical Infrastructure and maintain a directory of associated vulnerabilities

DOD will establish DCIP Assessment standards and benchmarks used to determine the vulnerabilities of specified DCI assets. Assessment results will reside in a secure web portal or database that easily links associated threat and hazard data, thus increasing the overall situational awareness of the DCIP community.

Objective 10: Identify remediation actions and their status

In collaboration with the asset and mission owners, DOD will recommend remediation strategies and advocate for funding or other actions, to reduce risks to DCAs based upon information derived from risk assessments. Asset owners will determine an appropriate response, including resource identification and prioritization.

Objective 11: Develop mitigation plans for identified DCI

Asset owners and asset users will work with supported Combatant Commands to develop plans to support and execute missions in the face of un-remediated risks to DCI. Unresolved issues will be adjudicated through the Joint Staff and the ASD(HD&ASA).

Objective 12: Provide DCIP-related information and recommendations as required

DOD Components and DISLAs should provide decision makers within DOD, Federal Agencies, State, Local, or host-nation governments with timely and accurate information on risks to and effects on critical infrastructure in times of emergency or crisis, or as otherwise may be required.

Goal 4: Facilitate DCIP Resourcing at All Levels

Organizations with DCIP responsibilities will develop the necessary resources to meet these requirements. Funding requirements should be considered in the

regular budgeting process to ensure stability of the program.

Objective 13: Determine, prioritize, and validate DOD resource allocations

All DOD Components and DISLAs are responsible for identification and prioritization of mission/organizational requirements and goals, including programming for necessary resources to enable the accomplishment of the goals set forth in this Strategy. The ASD(HD&ASA) will maintain oversight of all DCIP-related spending activities, providing guidance as necessary to ensure the goals of this Strategy are being met.

Objective 14: Acquire funds

DOD Components and DISLAs must ensure resources are requested and made available to support their assigned DCIP responsibilities. Components need to identify, validate, and prioritize requirements and to provide adequate DCIP resources in their baseline budget estimates generated through the Planning, Programming, Budgeting and Execution System (PPBES) process. Previously, program funds were provided by the ASD(HD&ASA), but commencing in Fiscal Year 2008 (FY08), the Components are responsible for providing adequate resources throughout the Future Years Defense Plan (FYDP). Reliance on supplemental funds will not allow for comprehensive management and is not an option. Accordingly, it is imperative that Components, including the individual Military Departments, include support of their DCIP responsibilities in their budget estimate submission.

Objective 15: Receive and consolidate performance metrics

The ASD(HD&ASA) will track program performance by DOD Component and Defense Infrastructure Sector through appropriate channels to ensure the efficient and effective accomplishment of the five DCIP goals. Individual DOD Components and DISLAs are responsible for measuring progress and reporting their status toward achieving these goals to the ASD(HD&ASA). Combatant Commands will report through the Joint Staff, the Military Departments directly to the ASD(HD&ASA), and DISLAs through their designated PSA.

Goal 5: Promote DCIP Education and Outreach

Ensuring the success of the DCIP means that proper training for stakeholders is accomplished, while those customers who would benefit most from program's results are made aware of its capabilities.

Objective 16: Establish focused education and outreach goals, objectives, and standards

The ASD(HD&ASA) will establish a baseline of DCI education and outreach requirements.

Objective 17: Develop plans, procedures, and tools to implement education and outreach goals, objectives, and standards

DOD Components, DISLAs, and DOD educational organizations should integrate DCI subject matter into their educational plans and curricula. To assist in this effort, the Director, Critical Infrastructure Protection, who is assigned to OASD(HD&ASA), will establish an educational Web presence on the NIPRNET and SIPRNET, as well as a Share Point

repository for sensitive, but unclassified information. Furthermore, DOD Components should integrate DCI issues into ongoing exercise programs.

All DOD Components should develop DCI training and education plans. Plans will stress the importance of DCI in support of their specific missions and address their respective efforts to manage risks for their identified DCI assets.

III. Implications of the Strategy

As discussed in the *Strategy for Homeland Defense and Civil Support*, securing the U.S. Homeland is the first among many competing priorities outlined in the National Defense Strategy. In a resource-constrained environment, this priority must be balanced against DOD's other requirements. Accordingly, a risk management approach that acknowledges the importance of an active, layered defense is deemed the most economical and credible means of meeting these complex responsibilities in which Homeland Defense and operations in the forward regions of the world are integrated conceptually and functionally.

As a risk management program, the DCIP involves taking actions to prevent, correct, or minimize the risks to the most important assets (i.e., DCAs) that support DOD missions. The DCIP enables risk management by processing criticality, vulnerability, and threat/hazard information in a quantifiable risk assessment framework. Decision makers then can use the results of the assessment process to determine appropriate *risk response* measures to accept risk, reduce or eliminate risk (i.e., remediation), minimize the effect of a potential threat or hazard or actual event (mitigation), and/or restore lost capability in the aftermath of an event (i.e., reconstitution). The desired end-state of the DCIP, therefore, is to improve overall critical infrastructure protection and resiliency, thus contributing to mission success. Finally, through this risk management methodology, DCIP complements and strengthens other risk management programs that contribute to the DOD mission assurance paradigm.

To achieve its overarching goal, the Strategy for Defense Critical Infrastructure requires:

- Information sharing throughout DOD, across the Federal government, and among our international partners;
- The implementation of risk management activities focused on critical infrastructure;
- Technologies to integrate and protect disparate infrastructure data sources; and
- Adequate and sustained resources supporting the Defense Critical Infrastructure risk management framework.

Information Sharing

The importance of DCAs requires an environment of effective information sharing. Since information sharing can be viewed as a means to manage risk more effectively and, in turn, help deter, prevent, mitigate, and respond to threats, DOD needs to promote and support timely and accurate sharing of information regarding critical infrastructure across the DOD components and with appropriate international partners, as well as with other Federal, State, and local entities.

The more information about asset criticality, potential threats, hazards, and vulnerabilities to defense critical infrastructure that is available to appropriate organizations, the better able

they will be to understand the risk and to ensure the continuity of essential missions and services. Information regarding DCI that should be shared includes information about threats, hazards, vulnerabilities, incidents, protection and mitigation measures, and best practices. This process will require the determination of the nature of the information required and the most appropriate mechanism to exchange the information.

Information identifying specific infrastructure assets as critical also creates its own set of challenges, in that such knowledge becomes an attractive target to malicious actors. Information related to critical infrastructure assets must therefore be protected for reasons of national security and public safety, as well as for competitive and economic interests. The publication of a DCIP Security Classification Guide, and complementary information sharing policy, is paramount to meet this requirement.

Risk Management Activities

The DCIP is a *risk management* program that seeks to ensure the availability of assets critical to DOD missions. The risk management *process* is accomplished through the *assessment* of risk to the accomplishment of DOD missions/functions and the identification of DOD, non-DOD, and DIB DCAs. Once these risks are understood, DOD can take appropriate *risk response* measures to ensure mission accomplishment unimpeded by damage or disruption to defense critical infrastructure. Specific guidance regarding the execution of the sub-elements of the risk management process (i.e., risk assessment and response) will be provided in follow-on documents as appropriate. Additionally, risk management decisions will be made at each appropriate level of authority as stated in this strategy, and expanded upon in subordinate documents.

Technology

The use of existing technology and the ability to leverage existing efforts is important to the effective implementation of a DCIP decision support system. Currently DCI data is maintained in disparate databases across DOD. DOD must ensure that data collected through the risk assessment process be standardized, secure, and accessible through a distributed database available across DOD and accessible to decision makers in an all-threats or all-hazards environment. To ensure the most current and accurate infrastructure data is available to decision makers when needed, data will be maintained by the asset owners, based on data standards defined by the ASD(HD&ASA).

Resourcing

Adequate and stable funding to achieve the goals supporting DCI activities is required. Currently DCI efforts organized within DCIP have been centrally funded through OASD(HD&ASA), but as the program matures, DOD Components and DISLAs with responsibilities to support DCIP will be required to fund their own activities. The ASD (HD&ASA) will retain policy oversight responsibilities throughout DOD and will serve as an advocate for helping organizations obtain programmatic resources.

IV. Conclusion

DCI is vulnerable to natural events and non-hostile incidents (hazards) as well as deliberately destructive/disruptive human action (threats). DOD will use a standardized and synchronized approach in managing the risks to DCAs to ensure that this infrastructure is always available to support DOD missions worldwide. The accomplishment of the five goals outlined in this Strategy will ensure that risks to DCAs are properly identified, assessed, offset, and managed.

Through the implementation of this Strategy, DOD will ensure that those responsible for supporting the warfighter have the tools and mechanisms in place to make informed decisions about the risks to supporting infrastructure, thus ensuring mission success is not jeopardized.