

MISSION ASSURANCE STRATEGY



APRIL 2012



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 07 2012

In today's global risk environment, strategic planning for core defense missions must account for a wide array of manmade and naturally occurring threats and hazards and their resultant vulnerabilities.

To that end, I am releasing a Mission Assurance Strategy, providing the Department with a mission assurance-centric framework focused on ensuring resiliency for the capabilities and assets supporting our core missions.

The framework provides a comprehensive, streamlined approach to mission-essential function (MEF)-focused risk assessment, management, and resource allocation across the Department. It provides transparency, enabling leadership to develop, integrate, and synchronize protection and resilience policies that address systemic risks and trends affecting MEF performance across components, installations, and programs. Additionally, it further enhances relationships with Federal, State, and local governments and with private-sector and international partners to boost all-hazards capabilities in areas involving key dependencies and interdependencies.

I look forward to your full support as we move to implement this Strategy and reap the benefits of a fully operational mission assurance framework.

A handwritten signature in black ink, reading "Carlisle Carter".



Department of Defense Mission Assurance Strategy

Table of Contents

The Challenge.....	1
Mission Assurance: Ends, Ways, and Means.....	6
A Strategic Framework for Mission Assurance across the DoD Enterprise.....	10
Pillar 1: Identify and Prioritize Critical Missions, Functions, and Supporting Assets.....	10
Pillar 2: Develop and Implement a Comprehensive and Integrated Mission Assurance Risk Management Framework.....	11
Pillar 3: Use Risk-Informed Decision Making to Optimize Risk Management Solutions.....	13
Pillar 4: Partnering to Reduce Risk – A Shared Responsibility.....	16
Implementing the Strategy: Next Steps.	18
Conclusion.....	20
References.....	21
Glossary.....	22

The Challenge

The Department of Defense's ability to ensure the performance of its Mission-Essential Functions (MEFs) is at growing risk. Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets -- within the United States and abroad -- on which our forces depend. This challenge is not limited to man-made threats; DoD must also execute its MEFs in the face of disruptions caused by naturally occurring hazards and technological failures.

Many DoD Components are pioneering initiatives to address these threats to MEF performance. Yet this is generally done in an uncoordinated fashion that can result in duplicative programs and leave crucial risks unmitigated. DoD requires a comprehensive and integrative framework to assess and address risks to MEFs. This framework should also help DoD prioritize investments to ensure MEF performance in a constrained fiscal environment.

This document outlines DoD's Strategy for Mission Assurance. The Strategy defines mission assurance as:

A process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD MEFs in any operating environment or condition.¹

Mission assurance focuses on the protection, continued function, and resilience of capabilities and assets critical to supporting MEFs, rather than the operational execution of DoD missions themselves. Within the context of mission assurance, readiness is based on the Joint Mission Essential Task framework and is assessed and tracked in the Defense Readiness Reporting System. Finally, mission assurance is a common integrative framework -- not a single policy or program -- to prioritize protection and resilience efforts and reduce risks from a range of complex threats and hazards.

Mission assurance will leverage existing protection and resilience programs, including but not limited to, antiterrorism, physical security, defense critical infrastructure, and information assurance. It will also provide input to existing DoD planning, budgeting, requirement, and

¹ The Mission Assurance definition in this Strategy supersedes the definition in the DoD 2005 Homeland Defense and Civil Support Strategy and will be incorporated into a revised DoD Directive 3020.40. This definition does not supplant the Mission Assurance concepts and definitions in place within the quality control, acquisition, and systems engineering communities.

acquisition processes. The effectiveness of mission assurance will be measured in relation to DoD's ability to continue to perform its MEFs.²

This Strategy merges the benefits of a consistent strategic DoD-wide risk management framework with the advantages of case-specific implementation at various levels across DoD. For example, the heads of DoD Components need to base their protection and resilience decisions on a common framework. Otherwise, it will remain difficult for senior leaders to make use of data resulting from conflicting Component assessments and prioritize risk reduction efforts across DoD. At the same time, Component heads and installation commanders have the best understanding of local, site-specific circumstances that affect risk management. The Strategy will leverage this local expertise, and keep Component and installation commanders at the leading edge of mission assurance.

This comprehensive mission assurance framework will also provide increased visibility of systemic risks and trends affecting MEFs across individual Components and installations. This will allow DoD to identify and address strategic risk issues more appropriately, particularly those involving external dependencies outside DoD Component control that may jeopardize DoD mission execution, both domestically and internationally. For example, DoD and industry partners are pursuing strategic solutions to DoD's overall dependence on commercial electric power rather than exclusively relying on back-up generators at the installation level.

The framework outlined in this Strategy aligns with the risk management framework and strategic objectives described in the *Quadrennial Defense Review* (QDR) and other DoD strategic guidance and planning documents. This Strategy identifies the principal pillars and initial actions needed to implement the mission assurance framework throughout DoD.

Threats to DoD Mission Performance

The attacks of September 11, 2001, represented a striking example of the challenge that confronts us today. On September 11, Al-Qaeda asymmetrically employed elements of U.S. critical infrastructure systems, in a manner that our military was not ready to counter, to strike the World Trade Center and the Pentagon. This type of asymmetric threat has been growing in many ways ever since. Today, potential adversaries seek both lethal and non-lethal means to attack, or otherwise disrupt, DoD and civilian assets.

² Performance measurement requires recognition that a positive mission impact may not be demonstrated by a quantifiable event or action, but may in fact be shown by the absence of an unwanted event.

Both this Mission Assurance Strategy and the Defense Strategy for Operating in Cyberspace (DSOC) address information assurance.³ They differ, however, in depth and scope. The DSOC establishes new policy to guide DoD cyberspace operations and outlines strategic initiatives to achieve cyberspace operational objectives. The Mission Assurance Strategy has a broader focus and leverages, rather than replicates, the in-depth guidance provided by DoD's cyber strategy. The Mission Assurance Strategy provides a framework for risk management across all protection and resilience programs. The Mission Assurance Strategy also accounts for the full range of threats and hazards to the capabilities and supporting assets on which our fighting forces depend, not just cyber threats.

Mission assurance must address an all-threat and all-hazards environment, DoD and non-DoD risks, and cascading downstream effects on MEFs:

1. Threats and hazards to mission execution range from naturally occurring events to unintentional or deliberate manmade disruptions. This includes incidents such as earthquakes, naturally occurring pandemics, space weather events, technological failures, and industrial accidents, as well as physical or virtual attacks by state or non-state actors. Threats can also emanate from insiders with ties to foreign counterintelligence organizations, homegrown terrorists, or from individuals who have a malicious agenda, as evidenced by the 2010 Wikileaks incident or Fort Hood shootings. This Strategy rests upon an all-threats, all-hazards framework for risk assessment and remediation and assumes that simultaneous or coordinated attacks or mission disruptions are very possible (e.g., a hybrid cyber and physical attack or disruption).
2. Threats to non-DoD government and commercially owned infrastructure, facilities, and capabilities - including the Defense Industrial Base (DIB) - can jeopardize DoD mission execution. A Mission Assurance Strategy focused only on DoD-specific vulnerabilities is likely to fail. DoD must adopt a comprehensive framework for mission assurance in order to manage risk in a way that accounts for DoD dependence on civilian capabilities and assets, the second and third order cascading consequences of their disruption, and the physical risk posed by the proximity of certain civilian critical infrastructure facilities to defense installations.⁴ This framework must also recognize the lead role of other Federal

³DoD released its "Defense Strategy for Operating in Cyberspace" in July 2011. The Strategy describes five Strategic Initiatives: treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential; employ new defense operating concepts to protect DoD networks and systems; partner with other Federal departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy; build robust relationships with U.S. Allies and international partners to strengthen collective cybersecurity; and leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

⁴ These supporting capabilities, assets and infrastructures include, but are not limited to, transportation networks; global supply chains; electric power, telecommunications, and information technology systems; nuclear power plants; chemical manufacturing facilities; dams; and water treatment plants.

departments and agencies (especially the Departments of Homeland Security, Energy, and Transportation), commercial infrastructure owners and operators, and other private sector and international partners in coordinating risk mitigation strategies for threats to private sector and Federal non-DoD infrastructure.

3. Many attacks or disruptions could not only degrade or disrupt DoD's net-dependent operations, but may also have downstream physical effects that would further affect the performance of MEFs. Ninety-eight percent of the electric power used by DoD comes from commercial providers.⁵ A severe natural disaster, or targeted cyber or kinetic attack on commercial electric power infrastructure would not only degrade DoD MEFs, but it also could cascade to other critical infrastructures necessary for sustained DoD operations, such as water treatment systems, fuel distribution, communications, and transportation nodes.

Assessing and Mitigating Risks to Mission Performance: Value Proposition

Many DoD Components -- particularly the Military Departments -- have been aggressively developing mission assurance frameworks; analyzing missions, functions, and supporting assets; developing risk assessment methodologies; growing an inventory of assessment data to identify significant vulnerabilities; and pursuing a range of mitigation options to reduce known risks. Some individual protection and resilience programs also use risk-based approaches to guide investment and policy decisions. However, there is wide variation in the use of MEFs as a common baseline across DoD. The net result: from a DoD-wide perspective, overall progress is uneven and insufficient to meet emerging threats. The following problems are pervasive:

- Conflicting or duplicative risk assessment efforts, even within individual Military Departments/Services. For example, today there are at least fifteen different, uncoordinated protection-focused vulnerability assessments performed or directed by the Joint Staff, Military Services, Combatant Commands, individual programs, and other Components.
- Little ability to identify strategic protection and resilience risks or critical interdependencies and, therefore, to make sound policy and investment decisions DoD-wide. Individual commanders, Component heads and program managers may inadvertently sub-optimize protection and resiliency decisions when national or joint critical mission interdependencies exist. As an important exception to this general rule, based on its new protection program framework, one Service identified changes in Emergency Management equipment allocation, Explosive Ordnance Disposal unit stationing, and construction planning at ammunition plants and arsenals that would not have been identified without analyzing protection risks at all DoD installations.

⁵ Defense Science Board Report, "More Fight, Less Fuel," 2008.

- Limited cross-Component and cross-program information sharing, insufficient protected information sharing with industry or international partners, and limited DoD-wide visibility on emerging protection and resilience best practices and performance metrics. At least three programmatic assessments examine Information Assurance vulnerabilities, but fail to share both the results of the assessments and remediation efforts already put in place by asset owners.
- Inadequate attention to “beyond-the-perimeter” challenges and external partner relationships, especially dependence on private sector-provided critical infrastructure and functions, as well as those owned and operated by foreign entities. For example, DoD has a limited understanding of supply chain risks in the DIB. These risks could include single-point-of-failure vendors or counterfeit parts that end up in warfighting platforms or mission enablers.

Pursuing a common mission assurance framework will create qualitative and quantitative benefits for DoD. Mission assurance will enable a more holistic look at protection and resilience requirements, provide closer coordination between “mission owners” and “asset owners,” identify systemic vulnerabilities, and eliminate redundancies in the myriad risk assessment approaches currently employed. It will also encourage increased sharing of best practices and help individual decision-makers more fully understand the risks they are managing.

A common and comprehensive risk management framework will also help reduce programmatic stovepipes and create a more complete, accurate, all-threats/all-hazards understanding of risks to the performance of MEFs. Currently, DoD doctrine for Force Protection only accounts for intentional hostile acts as opposed to an all-threats, all-hazards approach. Additionally, at many levels across DoD, “mission owners” and “asset owners” do not sufficiently coordinate or inform one another’s individual processes for assessing and mitigating mutual risk.

Such narrowly focused approaches provide an incomplete risk picture for decision-makers. This Strategy addresses the full-spectrum of risk and will result in better risk decisions across DoD, based on MEF and supporting asset prioritization. It will also allow more effective and efficient allocation of finite resources within and across protection and resilience related programs.

Mission Assurance: Ends, Ways, and Means

Ends

This Strategy will enhance the protection and resilience of critical assets and capabilities that allow DoD to ensure the continued performance of its MEFs in today's complex threat environment. Although DoD can never eliminate risk entirely, a mission assurance focus will enable DoD leaders at all levels to develop, integrate, and synchronize vulnerability and risk assessment methodologies, and protection and resilience related policies, plans, and programs. It will also enable the allocation of resources in a way that more proactively links strategic risk analysis and mitigation to operational requirements and critical functionality in normal, as well as stressed, operating environments. These principal benefits can be summarized as follows:

- **Reduce risk to MEFs, including those risks involving external dependencies.**
- **Apply resources efficiently to provide the best risk reduction for financial, personnel, and other costs incurred.**
- **Achieve increased readiness and resilience across DoD's MEFs.**

Ways

This strategy comprises four pillars. They are summarized below and subsequent sections of this Strategy describe them in further detail.

1. **Identify and Prioritize Critical Missions, Functions, and Supporting Assets and Capabilities**: DoD will evaluate, refine, and leverage existing DoD and DoD Component mission analysis and mission decomposition processes. This effort will build upon the solid foundations provided by the Continuity of Operations and Defense Critical Infrastructure Programs and identify, characterize, and prioritize the assets and capabilities that are critical to performing MEFs. This will include a wide array of mission-critical human, physical, information, supply chain, and supporting assets and capabilities.
2. **Develop and Implement a Comprehensive and Integrated Mission Assurance Risk Management Framework**: DoD will review existing risk assessment and management processes and develop a holistic approach to identify and assess all-threat/all-hazard risks to MEFs. This approach will examine the inter-connectedness of DoD's critical assets and external dependencies and the cascading consequences from asset failure or capability disruption. This will enable decision-makers at the installation, Component, and Departmental levels to prioritize actions to manage risk more effectively and efficiently. DoD will utilize red-teaming, war-gaming, and alternative analysis to

facilitate and inform this process and share assessment results, so that DoD-wide decision-makers can identify and address resultant trends and strategic issues. This risk assessment process will leverage the DoD-wide risk methodology currently under development.⁶

3. **Use Risk-Informed Decision Making to Optimize Mitigation Solutions:** DoD Components will leverage existing or establish new integrative processes and advocacy forums at the installation, Component, and DoD-wide levels to implement the mission assurance framework and provide coordinated input into DoD's *existing* planning, budgeting, requirements, and acquisition processes. DoD will only establish new advocacy entities in the absence of an existing process or structure. These processes and advocacy forums will recommend ways to integrate mitigation measures and measures of effectiveness more effectively across protection and resilience-related programs, and advocate new or modified policies, plans, capabilities, and/or resource investments.
4. **Partner to Reduce Risk:** DoD MEF execution depends on public and private assets that the DoD does not own. DoD must nurture relationships and enhance information sharing with key external stakeholders at each level of responsibility (installation, Component, and DoD-Wide) -- including key Federal interagency, other governmental, private sector, and international partners. This will enable DoD to build a more comprehensive, accurate, and integrated picture of critical mission risk and develop more effective and efficient approaches to risk mitigation that fully account for the interconnectedness of DoD, private, and foreign-owned assets and capabilities.

Means

DoD will implement this Strategy in a severely resource-constrained environment. DoD must achieve efficiencies and eliminate duplication of effort within and across existing programs, while leveraging appropriate DoD Component efforts wherever possible. Similarly, DoD must carefully target new investments to optimize value and measurably reduce risk to MEFs.

Prioritizing risk and risk mitigation efforts will allow DoD to increase programming and budgeting efficiencies, eliminate unnecessary redundancies, achieve closer integration of key activities, and inform the resourcing of existing programs and future investments related to mission assurance more effectively. Potential resources and programs affected include, but are not limited to:

- Antiterrorism
- Physical Security

⁶ The Secretary of Defense directed a Department-wide study of risk in 2010. The study is a joint effort of the Office of the Under Secretary of Defense (OUSD) for (Policy), the Joint Staff, OUSD (Personnel and Readiness), and the Office of the Deputy Chief Management Officer.

- Law Enforcement
- Defense Critical Infrastructure Program (DCIP)
- Installation Emergency Management (including Fire and Emergency Services and Explosive Ordnance Disposal)
- Continuity of Operations (COOP)
- Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Protection
- Force Health Protection
- Information Assurance

DoD will apply the mission assurance framework at three distinct levels, with senior leaders and commanders at each level working in a more integrated way to assess and manage risk appropriately:

- Installation. At the most basic level, at facilities and installations worldwide, installation commanders and tenant unit commanders and asset managers are responsible for protecting and ensuring the continued availability of personnel, equipment, facilities, networks, information, infrastructure, and supply chains. Decision-makers at this level need a complete understanding of the MEFs, critical assets, and capabilities under their protection and the associated risks, even if those assets and capabilities are not under their operational command or direction. This visibility must extend to external dependencies, as partnerships with civilian infrastructure owners and service providers are often most critical at the installation level. Decision-makers at this level are, in many cases, also well positioned to apply and implement significant aspects of the DoD-wide risk management framework provided in this Strategy.
- Component. Individual Combatant Commands, Sub-unified Commands, Component Commands, and Defense Agencies and Field Activities analyze the assets, systems, and capabilities needed to perform their MEFs and make recommendations regarding acceptable levels of risk. Pictures of risk developed and corresponding risk management decisions taken by one of these entities may affect others in significant ways. For example, U.S. Strategic Command is responsible for analyzing the capabilities essential to missile defense. It needs better visibility into the Service risk and vulnerability assessment results associated with each installation and asset involved in this mission. This is a complex problem made even more challenging by interwoven administrative and command relationships. Solving such problems is vital to providing a better understanding of crosscutting risks and interdependencies, and associated risk management solutions.
- DoD-wide. The Secretary of Defense and his OSD Principal Staff Assistants, the Chairman and the Joint Chiefs of Staff, the Secretaries of the Military Departments, and the Military Service Chiefs of Staff must analyze risks to MEFs and supporting assets and capabilities

across multiple missions. Decision-making at this level requires visibility of the strategic implications of installation or Component-level risk and risk decisions, and of strategic protection and resiliency trends and vulnerabilities. Engagement at this level is often necessary to establish risk management priorities that affect other government agencies or commercial infrastructure sectors.

A gradual approach to implementation will simplify the challenge of applying the mission assurance framework across DoD, and will allow the sharing of best practices and concept refinement as DoD moves mission assurance implementation forward. To create immediate benefits, initial implementation at the DoD-level will focus on the two extremes of the risk spectrum. First, implementation will identify areas where DoD has great risk and little remediation, such as DoD's dependence on commercial power. In this case, with measured investments, reprioritization of certain installation-level investments, and closer coordination with private sector utility and infrastructure providers, a more strategic approach could significantly and more efficiently reduce risks associated with the loss of commercial power.

Second, initial implementation will also seek to identify areas where DoD has significant remediation efforts underway, but low risk regarding DoD's ability to perform its MEFs. An example of this effort is the current "one size fits all" antiterrorism program. Applying the mission assurance framework to the \$13 billion allocated to antiterrorism and physical security investments in FY 2011 should lead to changes in assessment requirements and required levels of physical protection that reflect a more integrated approach to risk management at the installation level.

The assessment and decision-making framework (described in more detail in subsequent sections) will create synergies and efficiencies across these programs and others. Additionally, this framework will interface with and support DoD's existing resource allocation processes and Title 10, U.S. Code, authorities.

A Strategic Framework for Mission Assurance across DoD

Pillar 1: Identify and Prioritize Critical Missions, Functions, and Supporting Assets

The first pillar of mission assurance is the identification and prioritization of MEFs and supporting assets and capabilities. DoD has made progress in developing and implementing mission analysis processes, and analyzing the physical and cyber assets and systems that support MEFs. This includes some assets outside of DoD operational control - particularly in regard to critical infrastructure. The process for identifying these assets and capabilities is commonly referred to as “mission decomposition.”

Mission assurance requires a common mission analysis process as the foundation for analyzing risk and providing appropriate protection and resilience of critical assets and capabilities. This Strategy will leverage and expand upon the existing mission decomposition architecture defined by the COOP and DCIP communities. This mission decomposition architecture is well established, supports a national-level framework, and applies a “mission-essential” filter to all DoD functions. Further, operational commands and installations review this architecture on a routine basis as part of operational planning. Additional efforts to link Combatant Command strategic planning to the capabilities provided by Military Departments/Services and the current DoD readiness construct should also be undertaken as part of this effort.

Under the continuity of operations architecture, mission decomposition begins with the Presidentially established National Essential Functions (NEFs) and DoD’s five Primary MEFs (PMEFs) that support the NEFs.⁷ These PMEFs are supported by a series of DoD MEFs, mission-essential tasks (METs), Concept Plans, and Operation Plans, which are further broken down into the specific assets and capabilities critical to mission execution in any environment or condition.

No architecture is perfect, however. The mission decomposition process described above will need to expand over time to capture supporting human, information, infrastructure, and supply chain assets and capabilities, both internal and external to DoD, more effectively. Input from key public and private sector partners external to DoD will be essential to this effort. Finally, this process must analyze mission-critical assets and capabilities to differentiate their level of

⁷ PMEFS, MEFs, and Component-level MEFs also derive from DoD Directive 5100.01, “Functions of the Department of Defense and its Major Components.” DoD Directive 5100.01 describes the functions of the Department of Defense and its major Components, supporting the core mission areas of the Armed Forces, which are broad DoD military operations and activities required to achieve the strategic objectives of the National Security Strategy, National Defense Strategy, and National Military Strategy.

importance in fulfilling the mission they support and aid in prioritizing investment decisions. Some assets are inherently more critical than others, but the current mission decomposition process does not support such prioritization.

An expanded and enhanced mission decomposition process will enable DoD to assess risk associated with the most important assets and capabilities, as well as contribute to more effective, efficient, and integrated protection and resiliency decisions across DoD.

Pillar 2: Develop and Implement a Comprehensive and Integrated Mission Assurance Risk Management Methodology Process

A comprehensive, integrated, and well-understood risk assessment methodology and process is at the heart of the mission assurance concept. Complementary to the QDR risk framework, mission assurance risk assessments will consider both the consequence of disruption, and the likelihood of an event occurring -- which will be measured by an analysis of both threats and vulnerabilities. Risk assessments must consider a wide array of threats and hazards, current mitigation status, and the urgency and volatility of the total risk picture, as these factors all influence mitigation decision-making. Components should develop metrics that will allow comparison of risks and allow leadership at each decision-making level to prioritize risk mitigation options.

Currently, DoD lacks a consistent, standardized, and commonly accepted methodology to synthesize, analyze, and integrate DoD-wide mission assurance-focused threat, vulnerability, and consequence information. Individual Components and security disciplines each have separate risk assessment methodologies that are not linked horizontally or vertically.⁸ This results in duplicative assessment efforts, an incomplete risk picture, and undue burden on asset owners. Further, current risk assessment efforts do not consistently or systematically account for risks that stem from dependence on external assets. Without an overarching risk management framework that uses methodologies that examine connections to externally owned assets, such as commercial water distribution systems, transportation systems, and the electric grid, leaders may overlook components that are critical for the execution of their MEFs and fail to manage risk appropriately.

On an annual basis, it is common for a given asset to have an antiterrorism vulnerability assessment, physical security inspections, information assurance compliance verifications, and so on. For example, one Service installation is currently undergoing five similar assessments within

⁸ The vertical track begins at the installation level, runs up through the mission-owner level of DoD Components, and should end with an examination of risk from a DoD-wide perspective. The horizontal track should encompass the integration of multiple programmatic assessment efforts across DoD (e.g., assessments focused on areas such as CBRNE, physical security, information assurance, and antiterrorism) and interdependent threat, vulnerability, and consequence assessments.

an eighteen-month period. This is a waste of time and resources. It is also typical for assessment results to receive limited dissemination and to be warehoused in a compartmented fashion due to the extensive damage that can be done to critical U.S. capabilities or missions if unauthorized access to and subsequent exploitation of assessment results occurs. Thus, although the distribution of individual assessment results must remain controlled, DoD must improve its processes for ensuring senior leaders have access to the requisite information to make informed risk management decisions. Additionally, most Military Departments/Services and Components utilize different tools to analyze and store their assessment results, leading to duplicative development efforts and additional access layers for assessment results.

Through better integration of assessment methodologies, tools, and approaches and increased visibility of assessment schedules and results, DoD could eliminate significant redundancy, relieve the burden on asset owners, reduce potential seams, and identify more efficient and effective mitigation and response plans. These improvements would also support an increased ability to examine risk from a DoD-wide perspective, and identify those trends and strategic issues that individual installation commanders or heads of DoD Components may not recognize at their level. For example, due to sensitive security issues and individual clearance levels, in certain situations installation commanders are not even aware of critical assets located on the installation they are responsible for protecting. Increased visibility will also spur sharing of best practices and integrated approaches to risk mitigation.

Many installations conduct multi-program vulnerability assessments, but this practice is inconsistent and is less prevalent from the Component or DoD-wide perspective. The Marine Corps recently piloted a new comprehensive risk assessment framework that integrates across protection programmatic lines at the installation level and provides visibility of assessment results throughout the Service. DoD should build on this pilot program and examine how to expand this integrated assessment approach and increase strategic visibility across multiple Components and disciplines. Similarly, the Air Force has recently instituted a comprehensive review of various functional area inspections and assessments with an eye toward combining them in a more efficient way. DoD should look to the best practices that will derive from this effort to support DoD mission assurance implementation.

To achieve a common framework for mission assurance risk assessment, DoD needs to review existing methodologies and assessment capabilities and identify a range of options for integrating assessments. Options should include setting common benchmarks and standards, coordinating assessment schedules, increasing visibility of assessment results, promoting the sharing of tools and best practices, and streamlining assessment capabilities. The core DoD mission assurance risk management framework must contain sufficient flexibility to enable its decentralized application across disparate geographies, functional domains, programs, and asset types, and allow for continuous innovation as threats and vulnerabilities change.

Achieving this approach and integrating threat, vulnerability, consequence, and program-based assessments appropriately at the installation, Component, and DoD-wide levels requires a renewed commitment to information sharing within DoD. It will also require appropriate and secure information sharing approaches with international, private sector, and other external partners. Simply stated, for this concept to work, decision-makers must have access to all of the pertinent information required to support time-sensitive and risk-based decisions.

DoD will also need to examine the analytical capabilities available to identify risk trends and strategic issues. Each Military Department/Service and several Defense Agencies have existing analytic capabilities that could enable such analysis. Data sharing and coordination regarding these analytic capabilities will be essential for more comprehensive DoD-wide mission assurance risk analysis. Red-teaming, war-gaming, and alternative analysis should augment individual assessment efforts to provide additional perspectives.

U.S. Marine Corps Mission Assurance Assessment Teams (MAAT)

MAATs combine Antiterrorism, Critical Infrastructure Protection, CBRNE, Installation Emergency Management, and Physical Security program Assessments under one umbrella.

Completed MAAT Pilot Assessments of Marine Corps Air Station Iwakuni, Marine Base Quantico, and Camp Lejeune in 2010 revealed substantial time and fiscal efficiencies from both the assessment team and operator perspectives and identified several crosscutting protection issues that individual assessment programs might have overlooked.

Pillar 3: Use Risk-Informed Decision Making to Optimize Risk Management Solutions

Pillars 1 and 2 will provide senior leaders at the three levels across DoD with powerful, integrative processes and tools to help them make informed, risk-based decisions regarding mission assurance-related policies, plans, programs, and resource investments within their existing authorities. In a severely constrained resource environment, this approach will allow senior leaders at all three levels to apply limited resources to the highest-priority risks.

Mission assurance is based upon an integrated, multi-level framework for comprehensively assessing risk, informing policy and resource allocation, and measuring risk mitigation management effectiveness across DoD. This framework also provides strategic level awareness of risk issues that cut across multiple DoD installations, Components, or functional program areas. However, within this framework, many risk management decisions will also remain decentralized at the installation or Component level. In some instances, the Military

Departments/Services, with Combatant Command input, will be in a much better position to determine appropriate mitigation strategies based upon the specific risk assessed.

At the strategic level, mission assurance will focus on mitigating risks that affect overall DoD MEFs, identifying economy of scale solutions and setting DoD-wide priorities. An example of this approach is the collaboration currently underway among DoD, the Departments of Energy and Homeland Security, and the North American Electricity Reliability Corporation to provide strategic solutions to commercial power grid dependency issues that are DoD-wide. To capitalize on the benefits of this approach, DoD must establish appropriate means to channel mission assurance-focused inputs into the existing Planning, Programming, Budgeting, and Execution System (PPBES), Joint Capabilities Integration Development System, and Defense Acquisition System processes DoD-wide.

Currently, these requirements enter the resource investment decision cycle through individual program and Service stove pipes and are funded as such, not necessarily informed by a comprehensive and integrated risk picture. For example, until recently, individual installations were pursuing micro-grid investments to strengthen energy security without higher-level mission-focused input into where the need for these investments is most critical from a MEF perspective.

Risk management decisions at all levels must explicitly consider remediation and mitigation choices. Decisions should weigh the potential benefit of investing in additional protective measures versus focusing on additional capacity for resilience. To achieve the mission assurance vision, capabilities development, resource prioritization, and future protection investments must be integrated and risk-informed across DoD from the installation to the Military Department headquarters and DoD levels.

To move beyond these current limitations, DoD must make use of existing advocacy forums wherever possible to establish a crosscutting advocacy framework that focuses on mission assurance equities at the three decision-making levels. DoD must also develop and promulgate guidelines for efficiently operating these forums, as well as processes to facilitate information and best-practice sharing. The Army and the Marine Corps have made considerable progress along these lines through protection advocate frameworks and operating structures recently instituted at the Service level.

These advocacy forums will be responsible for integrating the outputs of mission criticality determinations and strategic risk analysis at their respective levels, and for advising decision-makers at various levels within DoD's existing planning, budgeting, requirements development, and acquisition processes on protection and resilience-focused mitigation priorities. These forums must bring together representatives of appropriate key stakeholder organizations to support risk-based decision-making and inform investments across DoD. In many cases, mission

assurance advocacy forums already exist, but they often fail to include a full spectrum of mission assurance-related program representation or specific processes to integrate their inputs into the higher-level risk decision picture.

At the installation level, this framework will help bring together operational, support, and tenant units in a more unified way to understand and collaboratively mitigate shared risk more effectively. Installation commanders will utilize a complementary approach -- leveraging existing, installation-level protection or emergency management councils wherever possible -- to ensure that information gathered from their mission and asset decomposition and risk assessment processes guide their risk mitigation decisions and resource investments.

Component-level organizations, similar in purpose to the existing Marine Corps Mission Assurance Operational Advisory Group (MA OAG)⁹, will have the ability to inform resource investments across programs to address the threats and vulnerabilities most critical to MEFs. At the Component level, these advocacy bodies will also provide oversight for the mission assurance framework and for risks and risk decisions affecting subordinate commands and installations.

Component-level mission assurance advocacy forums will:

- Serve as advocates for the integrated mission assurance framework ;
- Facilitate senior leader discussion of risk issues affecting the Component;
- Promote the sharing of critical information among relevant parties;
- Commission cross-cutting trends analysis; and
- Inform the determination and execution of mission assurance requirements across DoD decision processes.

DoD will identify or establish a DoD-wide Senior Steering Group (SSG) to review trend analysis, discuss strategic protection and resiliency issues, and provide input to the overall DoD risk management framework. This group will focus on coordinating Department-level policy issuances, setting overall protection and resilience priorities, and assessing the effectiveness of risk reduction efforts, as well as identifying specific issues at the two extremes of the risk spectrum. Finally, the SSG will recommend and oversee effective mechanisms for partnering with external stakeholders to communicate priorities and identify joint solutions to mission assurance-related challenges.

⁹ The MA OAG is chartered as the central forum to make recommendations on how the Marine Corps should organize, staff, train, and equip Operational Forces and the Supporting Establishment. The MA OAG recommends mission assurance program priorities to protect and sustain mission essential functions, personnel, and resources, and provides direct interaction among the deputy commandants, Operating Forces, Supporting Establishment, HQMC directorates, and other working-level representatives concerned with mission assurance programs. The MA OAG also serves as a vehicle to develop and recommend for approval to the Protection Advocate and the Marine Requirements Oversight Council (MROC) capabilities, gaps, and solution strategies to ensure there are relevant, timely inputs into the Program Objective memorandum and Expeditionary Force Deployment System processes to protect people and resources optimally.

The SSG, working within the PPBES framework, will assist in advising the Secretary of Defense on budgetary decisions that involve DoD-wide risks. Generally speaking, the majority of mission assurance-related remediation investments remain the responsibility of asset owners -- in coordination with mission owners -- at the Component and installation levels, with the SSG providing advice and input that informs decisions with strategic or cross-cutting implications for DoD through existing resource planning processes.

Pillar 4: Partnering to Reduce Risk – A Shared Responsibility

Mission assurance is not something DoD can do alone. In fact, ensuring DoD's ability to perform its MEFs in today's complex, interdependent risk environment encompasses a broad scope of collaborative engagement and important contributions across government, industry, and the international community. As a case in point, protecting the nation's critical information infrastructure -- including DoD's unique and shared systems and data -- is a responsibility shared by a host of others, including Defense Industrial Base companies, computer hardware and software manufacturers, and the Federal homeland security, law enforcement, and intelligence communities.

The principal challenge herein is focusing on common interests and responsibilities across these diffuse stakeholder groups. It is also about packaging the appropriate mix of authorities, technical capabilities, relationships, and resources to get the job done -- while respecting the various statutory, policy, and regulatory imperatives that govern these diverse, complex public-private sector relationships.

Thus, a major focus of this Strategy is to drive trusted interaction with key strategic partners external to DoD, including: 1) other Federal, State, and local agencies; 2) international Allies and friends; and 3) private sector critical infrastructure owners, operators, and service providers. This very diverse set of external actors represents key stakeholders with often-divergent perspectives on risk, whose roles and responsibilities in mission assurance are distributed and shared. The main challenge in leveraging this framework is finding the best way, wherever possible, to forge a common understanding of risk, establish a mutual value proposition for partnering on risk mitigation, and communicate DoD priorities clearly to partners who also have limited resources.

The collaborative structures required to facilitate and drive this type of engagement will be issue-based, leveraging to the greatest extent possible existing forums. A good example of this approach is the collaboration with the Department of Homeland Security and the Federal Sector-Specific Agencies designated in Homeland Security Presidential Directive-7 to address our mutual protection challenges across the national critical infrastructure landscape. This framework also supports the national preparedness guidance provided in the recently released Presidential Policy Directive-8.

Moving beyond government to engage the private sector, DoD must transform the way government and industry interact from a mission assurance perspective and create a value proposition that supports investments and innovation to assess and address threats and other risk factors collaboratively. DoD must encourage those industries and service providers that DoD depends on to design and use systems and processes that can withstand disruption and mitigate associated consequences.

Further discussion must also take place to help reinforce the notion of redundancy of critical personnel and components, address single points of failure and supply chain deficiencies, encourage investment in capital modernization, and develop and test business continuity plans in concert with other partners. In essence, DoD must encourage critical mission owners, installation commanders, and private industry leaders to invest in lowering risk while exploring compliance-based alternatives where necessary to ensure certain standards of mission performance under denied circumstances.

DoD must also promote greater collaboration among DoD, other government agencies, and the private sector in the context of joint risk and interdependency analysis, information sharing, scenario-based and continuity of operations planning, technological innovation, and outcome measurement and evaluation. Current partnerships with the diverse array of DIB companies reflect the many positive benefits of this approach. As an example, through the DIB Cyber Security/Information Assurance Program, DoD is collaborating with commercial companies to improve the security of DoD unclassified program information residing on or transiting unclassified DIB networks.

Differences in national interests, public-private sector structural relationships, legal concerns, and language barriers will challenge international partnerships with Allies and friendly governments, international organizations, multinational corporations, and the scientific community. Addressing threats and vulnerabilities associated with the “global commons” (areas outside national jurisdiction), transnational infrastructures and information systems, and global supply chains -- particularly in the areas of energy, transportation, and critical manufacturing -- can only be accomplished through far-reaching international partnerships.

These partnerships may take the form of bilateral relationships with Allies and friends, generally through the auspices of the Department of State. They may also center on Geographic Combatant Command relationships with key regional security partners. Finally, they may also play out through engagement with important multinational governmental or industry forums with regional or global reach, including the North Atlantic Treaty Organization, Asia-Pacific Economic Cooperation, and others.

Because the number of potential partners is large and the partners appropriate to any particular issue vary widely, DoD will need to prioritize and develop a long-term, systematic framework for focusing such partnerships. Accordingly, DoD will:

- (1) Leverage existing external partner forums and processes such as those supporting its interaction with the Defense Industrial Base.
- (2) Escalate time-sensitive, critical issues through ad hoc partnering arrangements in the absence of existing forums.
- (3) Work progressively over the long term to establish new forums in critical areas along a functional, regional, or international basis.

Implementing the Strategy: Next Steps

Protecting DoD's people and ensuring the continued function of DoD's mission-critical capabilities, equipment, facilities, information and information systems, and supporting infrastructure are enduring responsibilities. In order to fulfill these overarching responsibilities and implement the framework outlined in this Strategy, DoD must continue to build upon and strengthen successful initiatives and structures already in place, and resolve to establish new mechanisms and activities where necessary. As such, DoD will undertake an initial set of actions to guide mission assurance implementation over the next year, including:

- Enhancing existing DoD mission analysis and decomposition processes and related training to enable a more complete identification of critical capabilities and human, physical, infrastructure, information, and information systems assets and capabilities subject to and outside of DoD control.
- Achieving better integration of, and coordination among, the following relatively mature programs:
 - Antiterrorism
 - Physical Security
 - Defense Critical Infrastructure Program
 - Information Assurance
 - Installation Emergency Management
 - Continuity of Operations
- Leveraging and enhancing existing or establishing new advocacy bodies at the installation, Component, and DoD-wide levels to advocate for and integrate the mission assurance perspective into policy, planning, and resource decisions.
- Developing a DoD-wide policy to standardize mission assurance goals, objectives, roles, and responsibilities; supporting structures and processes; and, developing outcome metrics applicable across DoD.

- Reviewing existing assessment processes and developing a range of options for streamlining and integrating current approaches.
- Identifying or establishing the means to share assessment results.
- Identifying existing capabilities across DoD that can produce DoD-wide analysis of mission assurance risk trends and strategic issues.
- Integrating and expanding internally and externally focused partnerships at all three decision-making levels regarding the following issues:
 - Energy grid security
 - Transportation
 - Financial services
 - Cyber
 - Telecommunications
 - International collaboration
 - Supply chain concerns

The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs will issue a coordinated Implementation Plan that will expand on these deliverables and provide amplifying information. This plan will include additional information regarding resources required for implementation.

Conclusion

Effective implementation of the tasks discussed above will enable the development of an integrated, collaborative, and risk-based framework for mission assurance across DoD. The processes and structures associated with this framework must be sustainable over time and remain responsive, adaptive, and capable of addressing new challenges and opportunities as they emerge in the years to come. Achieving the principal ends of this Strategy will provide DoD with a comprehensive appreciation of all-threats/all-hazards risk to its MEFs. Although it will not lead to a “zero-risk” environment, this focus will enable leaders at all levels across DoD to develop, integrate, and synchronize mission assurance policies, plans, programs, and resource investments in ways that more proactively link strategic mitigation decisions to operational requirements and critical functionality. Finally, the mission assurance framework will provide symbiotic benefit to DoD and its government, private sector, and international partners in areas of critical mutual concern.

REFERENCES

- (a) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," January 14, 2010
- (b) Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003
- (c) DoD Directive 5220.22, "National Industrial Security Program," September 27, 2004
- (d) Department of Homeland Security, "National Infrastructure Protection Plan (NIPP)," 2009

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CBRNE	Chemical, Biological, Radiological, Nuclear, and High Explosive
DCIP	Defense Critical Infrastructure Program
DIB	Defense Industrial Base
DoD	Department of Defense
DSOC	Defense Strategy for Operating in Cyberspace
MAAT	Mission Assurance Assessment Team
MA OAG	Mission Assurance Operational Advisory Group
MEFs	Mission-Essential Functions
NEFs	National Essential Functions
OUSD	Office of the Under Secretary of Defense
PMEFs	Primary MEFs
PPBES	Planning, Programming, Budgeting, and Execution System
QDR	Quadrennial Defense Review
SSG	Senior Steering Group