



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

---

J-5  
DISTRIBUTION: A, B, C

CJCSM 3105.01  
14 October 2016

## JOINT RISK ANALYSIS

References: See Enclosure E

1. Purpose. This manual establishes a Joint Risk Analysis Methodology and provides guidance for identifying, assessing, and managing risk. It introduces and describes a common risk lexicon to promote consistency across Department of Defense (DoD) and Joint Force risk-related processes.

a. The Joint Risk Analysis Methodology enables the Chairman of the Joint Chiefs of Staff (CJCS or the Chairman) to make consistent, timely risk assessments and provide best military advice on risk management in support of title 10 responsibilities, most notably, the National Military Strategy (NMS). Above all, this manual places the Chairman's Risk Assessment (CRA) in context with other Joint Force processes and illustrates how risk connects these efforts.

b. While several Joint Staff documents have addressed risk, this is the first formal and authoritative Joint Staff risk reference. This manual supports the entire range of the Joint Strategic Planning System (JSPS).

2. Superseded/Cancellation. None.

3. Applicability. The Joint Risk Analysis Manual applies to the Joint Staff, Services, Combatant Commands, applicable defense agencies, and joint and combined activities. These organizations can apply the principles outlined in this manual across the entire spectrum of their responsibilities.

4. Procedures. See Enclosures A thru D.


5. Summary of Changes. None.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DOD Components (to include the Combatant Commands), other Federal agencies, and the public, may obtain

copies of this directive through the Internet from the CJCS Directives Electronic Library at: [[http://www.dtic.mil/cjcs\\_directives/](http://www.dtic.mil/cjcs_directives/)]. JS activities may also obtain access via the SIPR Directives Electronic Library Websites.

7. Effective Date. This MANUAL is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



WILLIAM C. MAYVILLE JR.  
LTG, USA  
Director, Joint Staff

Enclosures

- A - Strategic Planning Construct and Risk
- B - Joint Risk Analysis Methodology (JRAM)
- C - Chairman's Risk Assessment
- D - Risk Analysis within the Joint Strategic Planning System (JSPS)
- E - References and Other Risk Documents
- GL - Glossary

## ENCLOSURE A

### STRATEGIC PLANNING CONSTRUCT AND RISK

1. Introduction. This manual presents a common methodology (the Joint Risk Analysis Methodology), consistent with risk best practices, for the Joint Force to address risk comprehensively throughout the Joint Strategic Planning System and related DoD and National systems: the “Strategic Planning Construct (SPC).” In this framework, commanders and staffs enter a risk cycle that appraises, manages and communicates risk. This cycle includes four steps: problem framing, risk assessment, risk judgment (includes characterization and evaluation), and risk management. By applying this method, the Joint Force can use the same terms and processes to communicate strategic and military risk. The risk metrics specified in this manual provide a common method to facilitate risk-based decisions, however, if the situation dictates, other information may be used. The methodology described in this manual, coupled with military judgment, help determine risk levels, mitigation strategies, and acceptable risk levels in relation to problem sets and strategic objectives. Finally, the Joint Risk Analysis Manual formalizes an assessment method to provide consistency across processes to enhance risk communication and decision-making.

a. Risk assessment, management and communication are continuous and cross cutting processes. The President of the United States (POTUS), Secretary of Defense (SecDef), CJCS, Combatant Commanders (CCDRs), Service Chiefs, and their staffs continually consider risks when making military recommendations and decisions. Cyclical risk assessment and analysis serves as the primary feedback mechanism for the Strategic Planning Construct. Figure 1 describes the functions driving the SPC cycle. The Chairman also provides risk assessments to emerging crises and policies as required. In describing risk, leaders should use language that military professionals and civilian policymakers can understand in order to evaluate a situation. Beyond assessing risk, the communication of risk is essential for the Joint Force. The assessment and communication of risk are a continuous cycle.

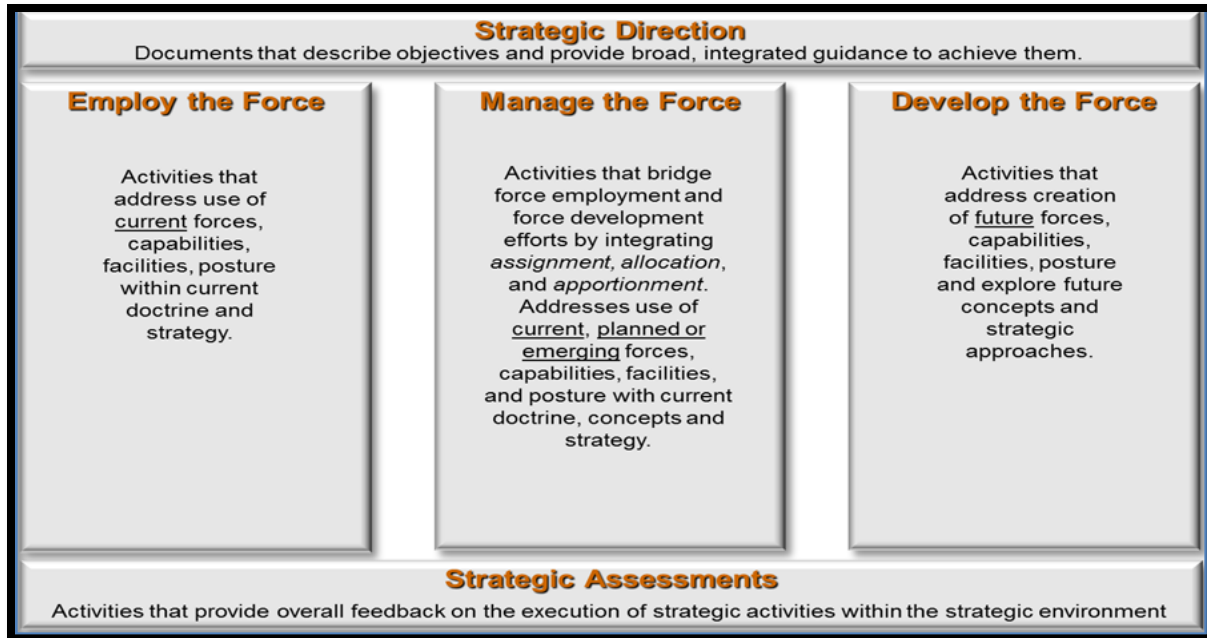


Figure 1: Functions of the Department of Defense

b. In providing the President, the Secretary, and Congress with the best military advice, the Chairman produces a yearly assessment of risk through the CRA. In coordination with the Joint Chiefs, and representing the views of the Combatant Commanders, the Chairman assesses the risks to U.S. interests, the military's risk to carry out missions called for in the NMS, as well as a description of the capabilities needed to address the risk. The CRA stands as the key risk document and process in the JSPS and the larger SPC. This chapter describes how risk assessment nests within this construct and within the JSPS framework.

2. Risk and the Strategic Planning Construct. The Chairman and the Joint Force incorporate risk analysis within a "Strategic Planning Construct" that includes interaction and alignment with National, Congressional and DoD planning processes and products as depicted in Figure 2 below. The construct incorporates five major DoD functions: *Strategic Direction; Force Employment; Force Management; Force Development; and Strategic Assessments*. This construct also accounts for POTUS direction such as the National Security Strategy and the Unified Command Plan. Strategic assessments (risk assessment is a key component) evaluate military *strategic direction* and three key DoD obligations: *Employ the Force, Manage the Force, and Develop the Force*; providing macro, integrated feedback on the execution of strategic activities. Risk assessment serves national, departmental, and military leaders as they set priorities and allocate resources to mitigate risk.

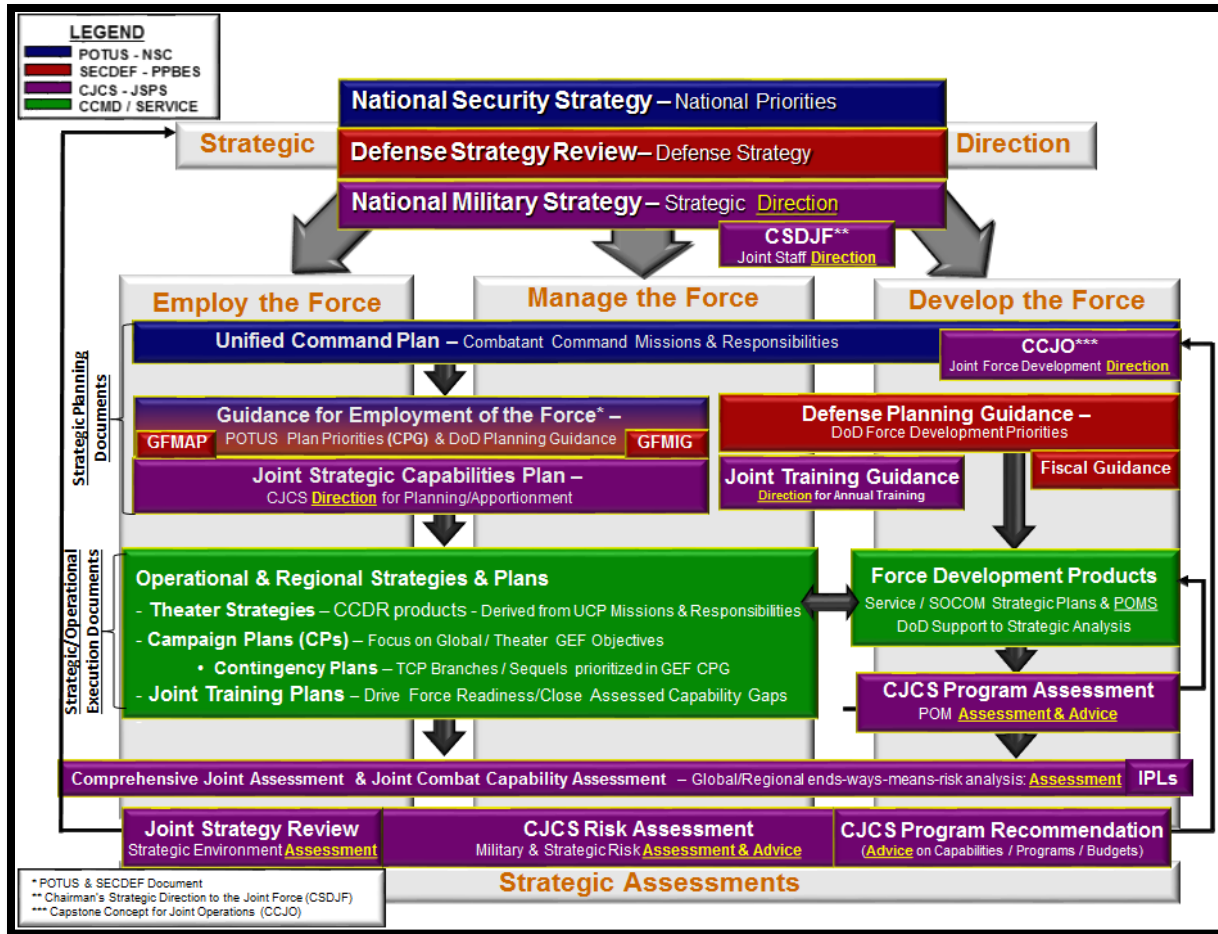


Figure 2. The Strategic Planning Construct

a. CRA. The CRA is informed by the full scope of the Comprehensive Joint Assessment (CJA) survey, Global Force Management, Joint Force Development and Capability Development to provide Congress with the Chairman’s assessment of the nature and magnitude of strategic and military risk in executing objectives called for in the NMS. The CRA is a holistic assessment which allows the Chairman to transmit formal military advice to the Secretary of Defense and Congress. The Secretary develops a Risk Mitigation Plan (RMP) that accompanies the CRA to Congress; the Chairman advises the Secretary during its development as well.

b. Beyond the formal construct of how risk nests within the JSPS, leaders and staffs must provide an explicit and tangible articulation of risk. This assessment better aligns ends, ways, and means to maximize the probability that the nation will meet its targeted policy objectives. Simply stating that a strategy, scenario, or crisis is high or low without context can cause confusion and imprecise guidance. Greater specificity in the description of a risk forces greater discipline upon the Joint Force and its commanders to develop the best assumptions and logic. It also furthers transparency between military and

civilian leadership to guarantee productive dialogue about risk. The Joint Force cannot receive effective guidance from the President or the Secretary of Defense without this dialogue.

3. Summary. The SPC describes nested strategic products and processes. This conceptual construct facilitates an iterative dialogue to produce the best strategy and force for the Nation. This dialogue must employ a risk assessment framework paired with articulation of actual costs, options, impacts, and end-states. Identifying, assessing, and mitigating strategic and military risk lays the foundation and priorities to employ, manage, and develop the Joint Force to meet national military objectives. This manual next explains the Joint Risk Analysis Methodology followed by its application to the CRA and the remainder of the JSPS.

## ENCLOSURE B

### JOINT RISK ANALYSIS METHODOLOGY (JRAM)

1. Introduction. Risk, the probability and consequence of an event causing harm to something valued, is a key element of decision-making across the Joint Force. Accurately appraising risk allows leaders and staffs to manage and communicate risk effectively to inform decisions across disparate processes. The JRAM provides a consistent, standardized way to analyze and manage risk. This methodology applies to the entire Strategic Planning Construct and specifically the JSPS.

2. JRAM. The JRAM uses a framework with three major components and four steps or activities (see Figure 3) to address risk comprehensively. The three components are *Risk Appraisal* – generation of knowledge and understanding; *Risk Management* – decisions and actions to manage or mitigate risk; and *Risk Communication* – the exchange of risk perspectives across processes and among leadership. Four steps are essential in a viable risk process: 1) Problem Framing - establishing the risk conventions and “risk to what?”; 2) Risk Assessment - identifying and scaling threats, “risk from what?”; 3) Risk Judgment – developing a risk profile, “how much risk?” and evaluating the risk – “how much risk is ok?”, and 4) Risk Management – decisions and actions to accept or mitigate – “what should be done about the risk.”

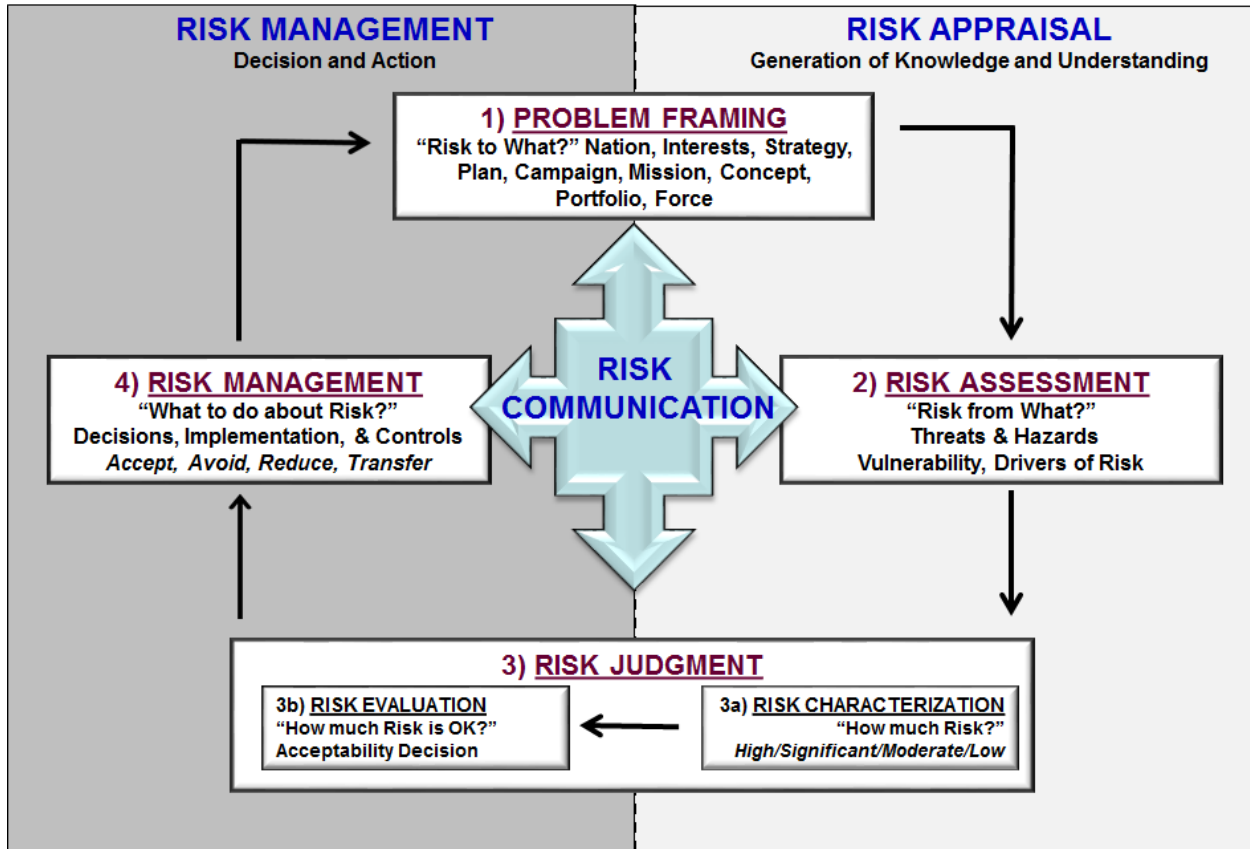


Figure 3. The Joint Risk Framework

a. Problem Framing (Step 1). The first step of the JRAM is to frame the problem by identifying the item or idea which is “valued” and has the potential to be “harmed.” Protecting national interests, successfully executing a strategy or plan, or maintaining a viable, ready force are examples of relevant risk topics with which the military is concerned. In order to frame a problem properly, one must answer the question “risk to what?” and define the standards (criteria, scale, terms, etc.) to be used during the assessment. This includes defining the levels of probability and consequence.

(1) Probability – A simple four-level table helps the assessor designate level of probability of an event occurring or an objective being met (see Figure 4). The categories “Highly Unlikely” and “Very Likely” are assigned smaller intervals to ensure these two categories are reserved for more certain events (i.e. more certain to happen or not to happen). The Probable and Improbable categories capture the less certain outcomes. The definitional structure deliberately omits a category for very low, zero, or negligible risk. While pursuing a strategy and an associated force structure that operate without risk may be desirable, the cost of moving from highly unlikely to no risk may require an exponential increase

Probability of Event (P)
Highly Unlikely (~0-20%)
Improbable (~21-50%)
Probable (~51-80%)
Very Likely (~81-100%)

Figure 4. Probability Levels



in resources. Resources are finite; commanders and staff must spend time and energy better through risk management.

(2) Consequences – Similarly, a chart with four levels of consequence helps assessors categorize the expected severity of the harm to the object of value (see Fig.5). These levels from “Minor” to “Extreme” can be tailored to describe specific risk scenarios. Harm is generally estimated considering vulnerability, the scale of damage, and the speed of recovery/resiliency (permanence).

Levels of Consequence (C)
Minor harm to something of value
Moderate harm to something of value
Major harm to something of value
Extreme harm to something of value

Figure 5. Consequence Levels

b. Risk Assessment (Step 2). This step links a potentially harmful event with likely consequences and expected probability. First, one must identify the sources and drivers of risk that will cause the harmful event. Sources of risk can be categorized as either a *threat* or a *hazard*.

(1) Sources of Risk – Threats or hazards which alone or in combination have potential to harm the item or idea that is valued.

(a) Threat – A state or non-state entity with the capability and intent to cause harm.

(b) Hazard – Security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

(2) Drivers of Risk – Factors that act either to increase or decrease the probability, frequency, or consequence of risks arising from various sources. For example, if insufficient resources are available to respond to a threat or hazard, it may “drive” an increase in assessed risk. Other risk driver considerations include:

(a) Vulnerability to the threat or hazard (how much harm can be caused over what timeframe?).

(b) Resilience (how quickly can we recover?), including redundancy (alternatives) and robustness (level of protection/preparedness).

(c) Criticality (How important is the object?).

(d) Accessibility (How easily can a hostile force or capability reach the object?)

(e) Recognition (how easily can the object be identified by a hostile force or capability?).

(f) Impact of damage (how severe are the secondary and tertiary effects of damage to the object?).

(3) Once the assessor has identified a threat or hazard, s/he must determine the expected consequence and probability of occurrence using the criteria established during problem framing. This information (the source of risk, an estimation of the severity of related consequences, and probability of occurrence) will be used to assign a risk level in the risk judgment step.

c. Risk Judgment (Step 3). Although every effort should be made to quantify the consequence and probability assessments associated with sources of risk, most quantification serves to bound, not measure risk. Risk judgment is ultimately a qualitative effort aimed at determining a decision-maker's degree of acceptable risk. It involves two actions—risk characterization and evaluation.

(1) Risk Characterization (Step 3a). Risk characterization establishes a risk level for each potential threat. The risk level is a function of the previously assessed probability (P) and consequence (C) ( $\text{Risk} = f(P,C)$ ).

Plotting the source of risk's assessed probability and consequence on a risk contour graph (Figure 6) can help determine the risk level. This part of the process is subjective, and a visual depiction of the assessed probability and consequence will allow subject matter experts or decision-makers to determine an appropriate risk level. The combination of probability and consequence determines the initial risk characterization.

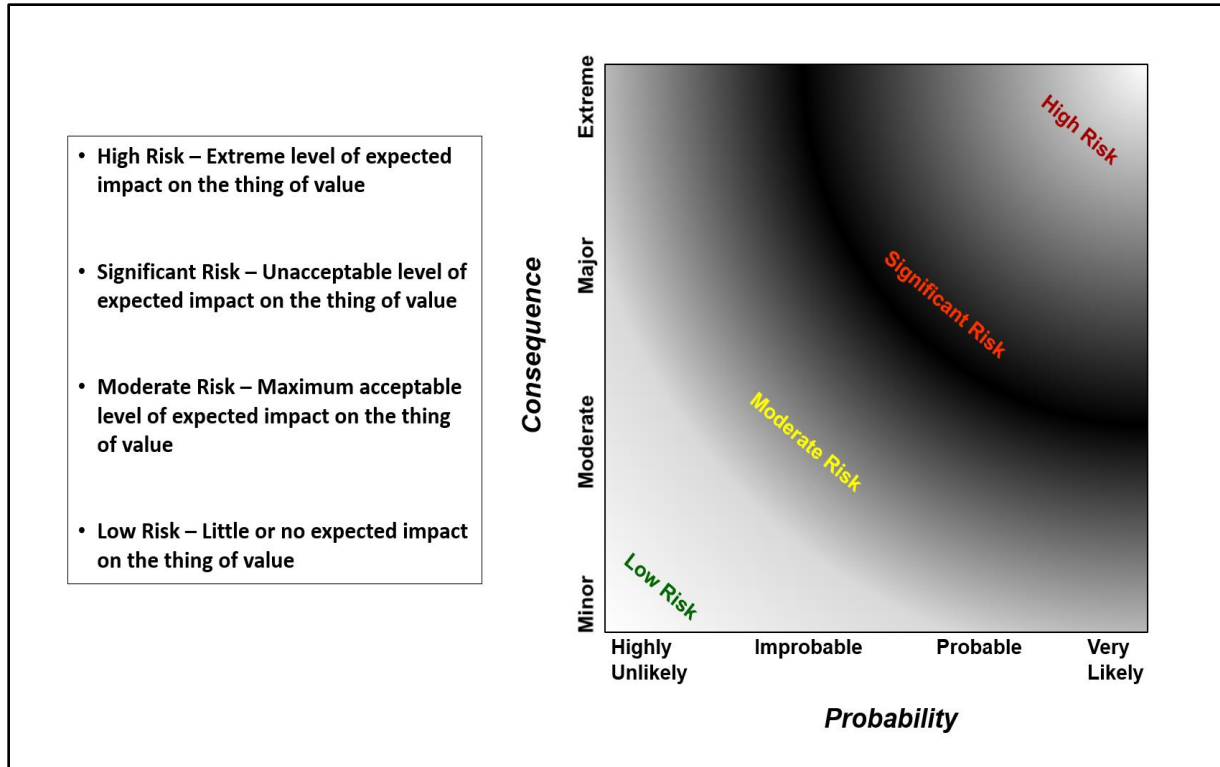


Figure 6. Generic Risk Contour Graph

(2) Risk Evaluation (Step 3b). During risk evaluation, a decision-maker makes a judgment about the acceptability of a risk, which will inform decisions on how to manage the risk. During evaluation s/he may weigh probability or consequence more heavily; e.g., address more probable moderate impact threats over less likely extreme threats.

(a) Acceptable – An activity where certain risks remain low enough that additional risk reduction efforts are not required.

(b) Unacceptable – Risk is too high to pursue a desired activity without additional risk mitigation efforts.

d. Risk Management (Step 4). This step focuses on designing, implementing, and monitoring risk decisions. Decision-makers may choose to accept, avoid, reduce, or transfer risk.

(1) Accept – Make an informed decision to act without mitigating the risk.

(2) Avoid – Forgo the activity that would produce intolerable risk.

(3) Reduce – Implement measures (risk mitigation activities) that decrease the probability or consequence of harm.

(4) Transfer – Take action to change where and when the risk is incurred and potentially who or what incurs it.

Reducing and transferring risk are components of risk mitigation. Acceptance and avoidance are risk decisions made as a matter of strategy, policy, operations, or tactics.

e. Risk Communication (throughout each step). Risk communication is at the core of any successful effort to appraise and manage risk. Effective communication between risk stakeholders reduces misunderstandings and potential surprises and is critical to enhancing dialogue and creating confidence in the outcomes. Senior leaders must illustrate ratings such as “significant” or “existential” with detailed analysis. Risk communication must occur in every step of the joint risk methodology.

### 3. Other Significant Considerations.

a. Three major challenges to successful risk analysis exist:

(1) Complexity - difficulty in establishing cause and effect relationships and intervening variables

(2) Uncertainty - human knowledge is inherently incomplete and assessments require assumptions

(3) Ambiguity - multiple legitimate interpretations exist and the exact problem or source of risk is not agreed upon by stakeholders.

Thus, the degree of confidence in any risk analysis is based on the availability of relevant data, the number of variables, and assessors’ depth of knowledge.

b. The time horizon is another important consideration. It takes into account how to balance risk over time. Decisions to accept, avoid, or mitigate risk today may affect risk exposure in the future. Conversely, making decisions that focus on mitigating potential future risk may cause increased risk in the present or near-term.

c. The challenges explained above (assets, impacts, threats, solutions, planning cycle, complexity, uncertainty, ambiguity, time horizon) are why decision-makers’ judgment and experience are critically important within the risk analysis methodology. In a military context, it is the senior leader or commander who can often provide a distinct and broader perspective or apply

*coup d'oeil* (strategic intuition) that helps determine the appropriate risk decision.

d. Risk assessment and management for any process complies with these universal insights:

- (1) Clarifying “Risk to what?” is critical to risk management and appraisal.
- (2) Risk related terminology is not standardized across all disciplines, but is necessary for risk assessment and management.
- (3) Risk assessment and management are inherently empirical processes—an approach that employs a practical method not guaranteed to be perfect—even when underpinned by numerical data and calculations.
- (4) There are common characteristics of risk management processes, but variation exists and terms have little practical impact on design or execution.
- (5) Exact breakout of process steps (elements) is unimportant, provided basic elements are included.
- (6) Definitions and business rules for prioritization and consolidation are important to understanding and executing risk management.
- (7) Data suggest the number of consequence and likelihood degrees should probably be five—but with important limitations and caveats.
- (8) Descriptors are important, even when numbers are depicted on a scale.

e. Leaders and staffs must identify and define “risk to what, to whom” in military terms. They will articulate “risk to what, to whom” after considering risk inputs from many organizations. Figure 7 below displays the nested direction and missions and their sources (left) along with the nested associated risks (right). This framing better enables assessment activities to scope, detail importance, show linkages and properly focus mitigation for strategic and military risk.

## **CJCS Assesses Risk for Syria Options in 2013 Vignette: Assessing and Communicating Risk**

*In a letter to Senator Levin and the Senate Armed Services Committee on 19 July 2013, General Dempsey offered an assessment of options for military force in Syria. The Chairman assessed the risk of five options for action in Syria: 1. Train, Advise, and Assist the Opposition; 2. Conduct Limited Stand-off Strikes; 3. Establish a No-Fly Zone; 4. Establish Buffer Zones; and 5. Control Chemical Weapons. In describing the costs and risk for each option, he addressed tangible aspects of risk to include forces, time, and end states. The mostly costly option-control chemical weapons-offers the best example of linking concrete risks to informed strategy development.*

*“Control Chemical Weapons: This option uses lethal force to prevent the use or proliferation of chemical weapons. We do this by destroying portions of Syria’s massive stockpile, interdicting its movement and delivery, or by seizing and securing program components. At a minimum, this option would call for a no-fly zone as well as air and missile strikes involving hundreds of aircraft, ships, submarines, and other enablers. Thousands of special operations forces and other ground forces would be needed to assault and secure critical sites. Costs could also average well over one billion dollars per month. The impact would be the control of some, but not all chemical weapons. Our inability to fully control Syria’s storage and delivery systems could allow extremists to gain better access. Risks are similar to the no-fly zone with the added risk of U.S. boots on the ground.”*

*In communicating a range of options, the scenarios in the Chairman’s letter sketch tangible, plausible future states and potential costs to achieve them, providing the ability for policymakers to weigh the costs and benefits of the various Syrian options, including the option to continue the status quo. The best military advice informed by both a military and strategic risk assessment apprised a political-military dialogue, and, ultimately, a political assessment and decision.<sup>1</sup>*

General Dempsey’s assessment was not part of the CRA, but the unclassified example demonstrates how leaders present a usable assessment for political leadership. Whether the CRA or an impromptu risk assessment, clear communication of risks is a key component of best military advice. Risk characterization and knowledge must be effectively communicated to the Secretary, Office of the Secretary of Defense (OSD) staff, Congress, and other stakeholders via the CRA report, memorandums such as that above, testimony, and office calls. The national leadership can then make risk management decisions that are consistent, well-informed, and complete.



Figure 7: Risk to What, To Whom?

4. Summary. Accurately appraising and effectively managing risk is important for decision-makers across the DoD and the Joint Force. The JRAM provides a framework and establishes a common lexicon for identifying, communicating, analyzing, and making decisions about risk. It is used across the JSPS and within the Combatant Commands and Services.

ENCLOSURE C

CHAIRMAN'S RISK ASSESSMENT

1. Introduction. The Fiscal Year 2000 National Defense Authorization Act amended title 10, United States Code to establish the requirement for an annual Chairman's Risk Assessment. General Henry Shelton published the first Chairman's Risk Assessment on 6 March 2000. Formally, the Chairman must provide an annual risk assessment to the Secretary of Defense and to Congress about the strategic risks to national interests and military risks in executing the National Military Strategy. The Chairman continually considers risk when fulfilling his primary roles (assess, advise, direct, execute) within the JSPS (see CJCSI 3100.01C). Specifically, the CRA provides a risk baseline that informs his assessment and advisory actions throughout the year. The CRA cuts across processes and acts as a key feedback mechanism throughout the JSPS and by extension the SPC.

The Chairman's specific statutory responsibilities related to risk are:

**Paragraph 2 (Chairman's CRA Responsibilities)**

10 USC 153(b)(2)(A- B)	Risk Assessment.-(A) The Chairman shall prepare an annual assessment of the risks associated with the most current National Military Strategy (or update)...The risk assessment shall be known as the "Risk Assessment of the Chairman of the Joint Chiefs of Staff." The Chairman shall complete preparation of the Risk Assessment in time for transmittal to Congress pursuant to paragraph (3), including in time for inclusion of the report of the Secretary of Defense, if any, under paragraph (4). (B) The Risk Assessment shall do the following: (i) As the Chairman considers appropriate, update any changes to the strategic environment, threats, objectives, force planning, and sizing constructs, assessment, and assumptions that informed the National Military Strategy required by this section. (ii) Identify and define the strategic risks to United States interests and the military risks in executing the missions of the National Military Strategy. (iii) Identify and define levels of risk distinguishing between the concepts of probability and consequences, including an identification of what constitutes "significant" risk in the judgement of the Chairman. (iv (I-II)) Identify and assess risk in the National Military Strategy by category and level and the ways in which risk might manifest itself, including how risk is projected to increase, decrease, or
------------------------------	---



	<p>remain stable over time; and for each category of risk, assess the extent to which current or future risk increases, decreases, or is stable as a result of budgetary priorities, tradeoffs, or fiscal constraints or limitations as currently estimated and applied in the most current future.</p> <p>(v) Identify and assess risk associated with the assumptions or plans of the National Military Strategy about the contributions of support of (I-III) other departments and agencies of the U.S. Government, alliances, allies, friendly nations, and contractors.</p> <p>(vi) Identify and assess the critical deficiencies and strengths in force capabilities (including manpower, logistics, intelligence, and mobility support) identified during the preparation and review of the contingency plans of each unified combatant command, and identify and assess the effect of such deficiencies and strengths for the National Military Strategy.</p> <p><i>Note: While the code refers to the document as the “Risk Assessment of the Chairman of the Joint Chiefs of Staff,” it is simply referred to as the “Chairman’s Risk Assessment.”</i></p> <p>.....</p> <p><b>Paragraph 3 (Congressional role in the CRA)</b></p>
<p>10 USC 153(b)(3)(B)</p>	<p>Not later than February 15 each year, the Chairman shall, through the Secretary of Defense, submit to the Committees on Armed Services of the Senate and the House of Representatives the Risk Assessment ...</p> <p>.....</p> <p><b>Paragraph 4 (Secretary of Defense’s role in the CRA)</b></p>
<p>10 USC 153(b)(4)(B) (i-ii)</p>	<p>If the Risk Assessment ... includes an assessment that a risk or risks associated with the National Military Strategy are <i>significant</i>, or that <i>critical deficiencies in force capabilities exist for a contingency plan</i> described in paragraph (2)(B)(vi), the Secretary shall include in the transmittal of the Risk Assessment the plan of the Secretary for mitigating such risk or deficiency. A plan for mitigating risk of deficiency under this subparagraph shall: (i) address the risk assumed in the National Military Strategy (or update) concerned, and the additional actions taken or planned to be taken to address such risk using only current technology and force structure capabilities; and (ii) specify, for each risk addressed, the extent of, and a schedule for expected mitigation of, such risk, and an assessment of the potential for residual risk, if any after mitigation. <i>Note: The name of the Secretary of Defense’s plan is the RMP.</i></p>

2. CRA. The Joint Staff develops the CRA final report using the Joint Risk Analysis Methodology described in Enclosure B. The JRAM serves as the framework to assess risk across the entire JSPS. The risk appraisal portion of the framework is accomplished by the Joint Staff J5 with input from the Combatant Commands, Services, other Joint Staff elements, the intelligence community, and academia. In accordance with 10 USC 153(b)(4)(B), if the Chairman assesses risks as “significant” or higher, the Secretary of Defense is required to submit to Congress a plan for mitigating those risks. This risk management portion of the framework is addressed through the Secretary’s Risk Mitigation Plan, which identifies needed adjustments to authorities, policies, and/or priorities for each significant strategic or military risk. Figure 8 below shows how the Joint Risk Analysis Methodology is applied to the CRA. The CRA articulates the risk details in regards to the Nation’s strategy and Joint Force using this methodology as the foundation.

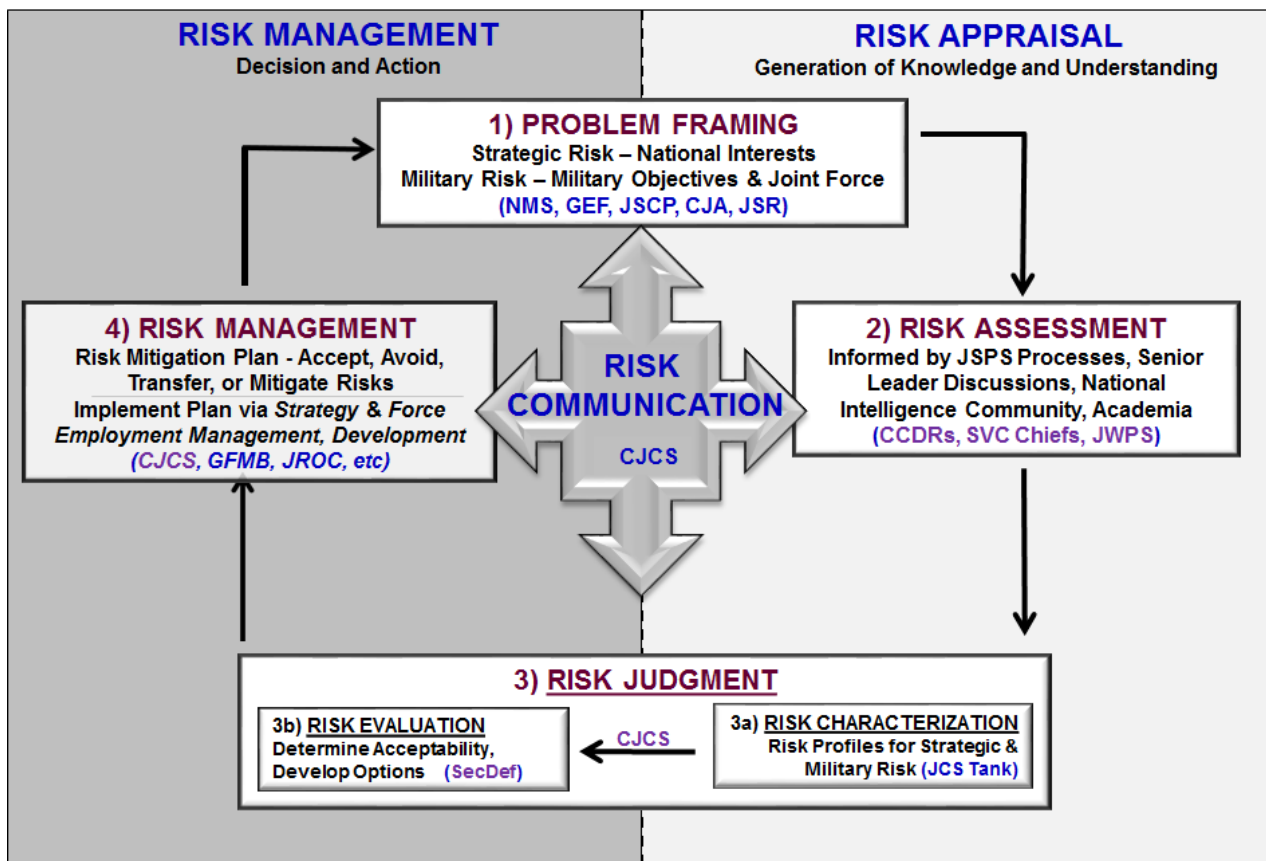
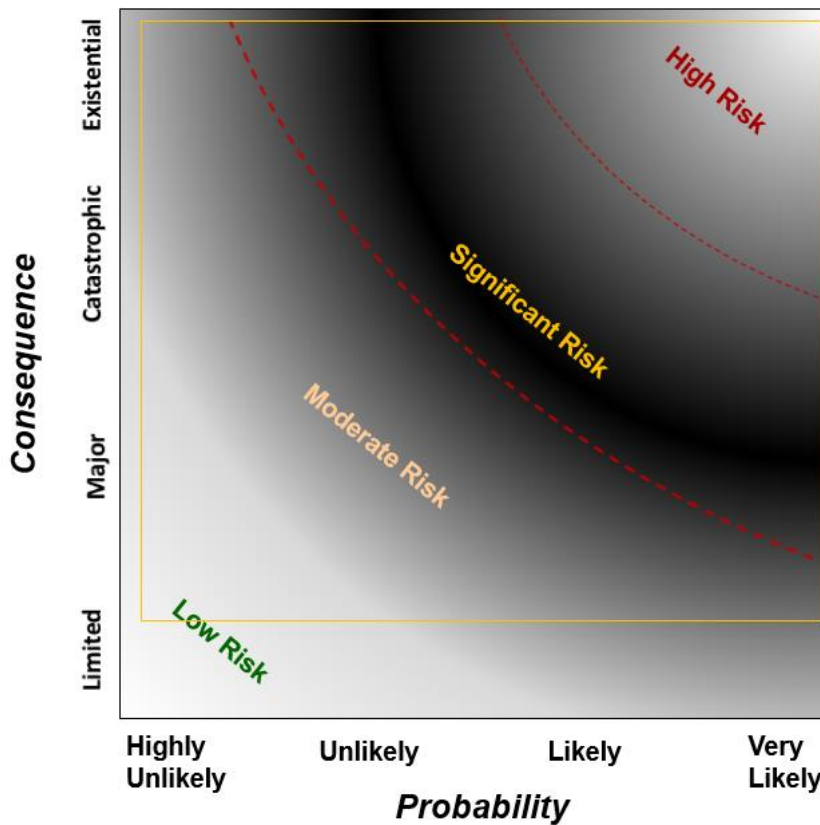


Figure 8. JRAM Applied to the Chairman’s Risk Assessment

a. CRA Problem Framing (Step 1). The CRA must evaluate two types of risk—*Strategic Risk* (risk to national interests) and *Military Risk* (risk to military objectives and to the Joint Force). During this step, the Joint Staff J5, with concurrence from the Chairman, establish standardized definitions and probability and consequence levels for each type of risk. Throughout the

development of the CRA, the Joint Staff J5 applies the Joint Risk Analysis Methodology as outlined in Enclosure B.

(1) Strategic Risk is the potential impact upon the United States- including the U.S. population, territory, civil society, critical infrastructure, and interests - of current and contingency events given their estimated consequences and probabilities (e.g. the security of the United States and its citizens). Strategic risk has four probability and consequence levels, depicted in Figures 9 and 10 below. As noted in the definition of strategic risk, the consequences are all tied to national interests, which are articulated in strategic guidance provided by the President. The degree of strength of an interest should be determined before a detailed analysis of threats to those interests. The Chairman uses these interests as a starting point for assessment of strategic risk.



Strategic Risk on an ISO curve reflects a risk level based upon both the range of consequences and the probabilities of risk events. Disparate events could have “equal” risk levels, with one weighted more on probability and one on consequence.

HIGH: A likely existential hazard to strategic interest.

SIGNIFICANT: A somewhat likely catastrophic hazard to strategic interest.

MODERATE: A somewhat unlikely medium hazard to strategic interest.

LOW: A strategic risk event with a combination of low likelihood and limited consequence.

Figure 9. Strategic Risk Contour

Probability of Event (P)	Consequence of Event (C)	Strength of National Interest (SOI)
Highly Unlikely (~0-20%)	Limited: Confined, Short-term damage to Interests	4: Premier: Impacts U.S. Homeland, Vital Interests
Unlikely (~21-50%)	Major: Considerable, mid-term damage to Interests	3: Strong: Impacts Key Global Systems, Allies
Likely (~51-80%)	Catastrophic: High order, long-term damage to Interests	2: Moderate: Impacts Key Partners, Regional Interests
Very Likely (~81-100%)	Existential: Permanent destruction relative to Interests	1: Low: Impacts “Others”, Local Interests

Figure 10. Strategic Risk Tables

The strategic value of the interest being targeted should be considered when determining the consequence level. It is critical that interests do not become a function of a particular threat. If the United States begins with a threat assessment before a conceptualization of interests and intensities, it risks reacting to a threat with major commitments and resources devoid of any rational linkage to the relative critical value of interests. For example, the effect on U.S. national interests from a ballistic missile hazard varies depending on whether it is directed at the homeland, a treaty ally, or a partner. Thus, strategic value becomes part of determining whether a consequence is categorized as limited, major, catastrophic, or existential. To assist with this, the JRAM incorporates a Strategic Risk Matrix (see Figure 11) to frame the interest threatened and the degree of harm to that interest.

EVENT TITLE:		Hazard Estimate (Consequence based on damage to interest, time, resiliency) (w/ Illustrative Exemplars)				Probability	RISK to Interest
Enduring National Interest	Strength of Interest HLD/Vital: 4 Global System/Ally: 3 Partner/Regional: 2 Other/Local: 1	Limited (1) Minor damage to interests, and/or short-term impacts	Major (2) Moderate damage to interests and/or mid-term impacts	Catastrophic (3) Major damage to interests and/or long-term impacts	Existential (4) Extreme damage to interests, and/or permanent destruction of defining system	HIGH 81-100% SIG 51-80% MOD 21-50% LOW 0-20%	HIGH SIG MOD LOW
The Security of the U.S., its population, civil society, Allies and Partners	HLD/Vital: 4 Global System/Ally: 3 Partner/Regional: 2 Other/Local: 1	<ul style="list-style-type: none"> <li>- Small Scale Contingency Ops (NEO, HA/DR)</li> <li>- Tactical Terror Attack (Lone Wolf)</li> <li>- Minor domestic civil disturbance</li> <li>- American hostage(s)</li> <li>- Loss of access</li> <li>- Coop Security activity or arrangement cancelled</li> </ul>	<ul style="list-style-type: none"> <li>- Minor Armed Conflict</li> <li>- Operational Terror Attack</li> <li>- Isolated or Minor Attack on Global Domain or critical infrastructure</li> <li>- Major domestic civil disturbance</li> <li>- Isolated Attack on U.S. Embassy or Business</li> <li>- Loss of Ally or Partner</li> <li>- Rise of Regional Hegemon</li> <li>- Unsecured global domains</li> <li>- Isolated epidemic or natural disaster</li> </ul>	<ul style="list-style-type: none"> <li>- Theater War on Major Armed Conflict</li> <li>- Strategic Terror Attack (9/11)</li> <li>- Strategic Attack on Global Domain or critical infrastructure</li> <li>- Concurrent widespread major domestic civil disturbances</li> <li>- Integrated regional attacks on U.S. Embassies or Businesses</li> <li>- Invasion or Loss of Major Ally or Partner</li> <li>- Regional Security Organization (NATO) breakup</li> <li>- Major epidemic or natural disaster (Spanish Flu of 1918, Katrina)</li> </ul>	<ul style="list-style-type: none"> <li>- Nuclear War (U.S. or Allies)</li> <li>- WMD Terror Attack</li> <li>- Domestic rebellion</li> <li>- Pandemic or natural disaster that threatens U.S. existence</li> </ul>		
Security of the U.S. Economy & the global economic system	HLD/Vital: 4 Global System/Ally: 3 Partner/Regional: 2 Other/Local: 1	<ul style="list-style-type: none"> <li>- Limited trade, resource, or financial interruption</li> <li>- Limited Interference in critical infrastructure</li> <li>- Change in currency standard</li> <li>- Minor cyber compromise</li> </ul>	<ul style="list-style-type: none"> <li>- Extended trade, resource, or financial interruption</li> <li>- U.S. Recession</li> <li>- Extended interference in critical infrastructure</li> <li>- Failure of IMF</li> <li>- Lack of intl norms</li> <li>- U.S. Depression</li> </ul>	<ul style="list-style-type: none"> <li>- Financial failure of major institution or market</li> <li>- Major Degradation of critical infrastructure</li> <li>- Access to Global Domain(s) disrupted by adversary</li> </ul>	<ul style="list-style-type: none"> <li>- Global or U.S. economic collapse</li> <li>- Closed economic system</li> <li>- Destruction of critical infrastructure</li> <li>- Seizure of U.S. business/industry</li> <li>- Access to Global Domain(s) denied by adversary</li> </ul>		
Preservation, and extension of universal values	HLD/Vital: 4 Global System/Ally: 3 Partner/Regional: 2 Other/Local: 1	<ul style="list-style-type: none"> <li>- Local Atrocities</li> <li>- Imposition of martial law by Ally or Partner</li> <li>- Democratic regression in Ally or Partner</li> </ul>	<ul style="list-style-type: none"> <li>- Mass atrocities</li> <li>- Democratic regression in Key Ally or Partner</li> <li>- Local imposition of alternate value system</li> </ul>	<ul style="list-style-type: none"> <li>- Genocide (Holocaust)</li> <li>- Regional imposition of alternate value system</li> <li>- Emergence of powerful totalitarian nation</li> </ul>	<ul style="list-style-type: none"> <li>- Global Imposition of alternate value system</li> </ul>		
Advancing & maintaining U.S.- led International Order	HLD/Vital: 4 Global System/Ally: 3 Partner/Regional: 2 Other/Local: 1	<ul style="list-style-type: none"> <li>- Local or State order undermined replaced by alternative system, neutral or antagonistic to U.S. system; sets negative precedent</li> </ul>	<ul style="list-style-type: none"> <li>- Regional Order undermined or replaced by alternative system, neutral or antagonistic to U.S. system</li> </ul>	<ul style="list-style-type: none"> <li>- Elements of International order undermined or replaced by alternative system, neutral or antagonistic to U.S. system</li> </ul>	<ul style="list-style-type: none"> <li>- US Order Replaced in total by alternate system, hostile to current U.S. system</li> </ul>		
<b>Strategic Risk:</b> Summary discussion of strategic risk criteria and factors to each US Interest to develop an overall strategic risk assessment.							

Figure 11. Strategic Risk Matrix

### **Postponing the Cross-channel Invasion Vignette: Strategic Risk**

*Considered one of the most important Allied strategic decisions of World War II, President Franklin Roosevelt's decision to execute Operation TORCH—the invasion of North Africa in November 1942—postponed the amphibious landings in France until June 1944, but allowed the United States to complete mobilization of its immense industrial and manpower resources. Basically, the Army needed time to build training facilities and housing for expansion. Manpower mobilization had to proceed cautiously to avoid calling up the skilled hands necessary to build training facilities before they built those bases. The second major limitation was industrial, since defense industries to support the requirements of Lend Lease, not more than 15 percent of the industrial capacity of the United States, were devoted to defense. America needed time to convert industries to defense production. Additionally, limited shipping presented problems for the Navy. The ships available could only move 50,000 men with their equipment and 90 days' supplies to a trans-oceanic theater. Shipping required to transport the Army and Air Corps alone overseas amounted to around seven million tons, or one thousand vessels. Maintaining that force in overseas theaters required about ten million tons of shipping, or 1,500 ships. The two years needed to build those vessels coincided with the time the general staff estimated the Army needed to raise and train combat divisions. Prior to an invasion, air power was the principal weapon with which the United States could accomplish successful military operations against the Axis and the Air Corps needed more time to build aircraft and train crews. By strategic aerial bombardment, the Air Corps could attack the German industrial and economic structure. Moreover, all of this preparation coincided with the period of maximum risk: 1942 was the earliest Germany could invade Great Britain, should the Soviet Union collapse.*

*General Marshall and Admiral King advised against undertaking Operation TORCH. They mentioned the reasons why the operation itself was risky—that it would gain momentum slowly and would for some time hang on uncertain political decisions. They also drew attention to the danger of “thinning out” naval escorts to meet new commitments. If the United States waged any war outside the western hemisphere it would be at a considerable disadvantage. The United States and its Allies had to weaken the enemy by overextending and dispersing its armies. But these objections, however serious in themselves, were incidental to the main objection - that a North African invasion would be an untimely, ineffectual departure from BOLERO (buildup of forces in Great Britain in preparation for a cross-channel invasion). As professional officers, the Chiefs of Staff were uncomfortably aware of how quickly military situations could change and of how important it was to have uncommitted reserves in the field and at home. In this respect, they were more cautious than President Roosevelt*

*and Prime Minister Churchill. The Chiefs of Staff did not want to accept any strategic risk that would jeopardize the 1943 invasion of Europe.*

*In the end, President Roosevelt intervened and overruled his military advisers to support the British proposal for landings in North Africa. He based his decision on the political necessity to keep Germany the main focus of the American war effort. The President accepted the risk that the Soviet Union could not survive, and that fighting the Germans in the Mediterranean sooner rather than later would be more beneficial than a 1943 cross-channel invasion. Even with the loss of the Soviet Union and/or Great Britain, President Roosevelt grasped that losing American support and engagement for the war stood as an existential risk to the Nation. The President had to keep the country engaged in the war. The decision to pursue TORCH delayed invasion of Europe until 1944 but greatly improved its chance of success, forced the Allies to establish an effective combined, joint high command, bought more time for the United States to mobilize, and allowed the Allies to control the Mediterranean Sea.<sup>1</sup>*

In this vignette, the Combined Chiefs of Staff explained the strategic risk to the President. Despite these impacts, President Roosevelt grasped the military leaders' concerns and overruled their advice. This frank dialogue about the strategic risk to the nation took place because the military leadership articulated risks in terms the civilian leadership could fully understand. The strategic risk matrix (Figure 11) above serves as a template to explain strategic risk. On the left hand side, strength of interest drives the initial importance of an interest (especially in relation to the Nation, an ally, a partner, etc.). Across the top of the matrix, leaders next determine the consequence of a threat on that interest. In the TORCH vignette, the President and military leaders considered national interests and made determinations of strategic consequence. President Roosevelt evaluated loss of American support to attack the Axis as an existential threat to the security of the United States. He rated the loss of the Soviet Union as a catastrophic threat. Where General Marshall would not accept risk in postponing an invasion, especially if the Soviet Union surrendered to Germany, the President did not want to risk losing popular support for the war against Germany. He reasoned that keeping Britain as an effective ally and keeping the United States in the war outweighed supporting a potential Soviet collapse.

---

<sup>1</sup> Charles Kirkpatrick, *An Unknown Future and A Doubtful Present: Writing the Victory Plan of 1941*, Center of Military History: Washington, D.C., 2011 and Maurice Matloff and Edwin M. Snell, *United States Army in World War II: Strategic Planning for Coalition Warfare, 1941-1942*, Center of Military History: Washington, D.C., 1999 for more discussion on the strategic ramifications and discussions of Operations GYMNAST, TORCH, and BOLERO.

(2) Military Risk is the estimated probability and consequence of the Joint Force's projected inability to achieve current or future military objectives (risk-to-mission), while providing and sustaining sufficient military resources (risk-to-force). In the context of the CRA, military objectives are identified in the NMS, and the sufficiency of military resources is identified in the CJA. Military risk has two complementary dimensions: risk-to-mission and risk-to-force (Figure 12). Both must be considered when calculating military risk, as it involves balancing a Combatant Command's ability to attain steady-state, current operations, and contingency plan objectives against the Services' and Joint Force Provider's abilities to support Combatant Command missions.

The concepts of risk-to-mission and risk-to-force can be differentiated into four risk subsets based on source of risk and time horizon. Two of the subsets measure risk-to-mission (operational risk and future challenges risk) and two subsets measure risk-to-force (force management risk and institutional risk). Time horizon will remain subjective based on strategic trends, threats, the Chairman, and policy. This manual presents time horizon best practices based on the CJA<sup>2</sup>, traditional budget cycles, force readiness, strategic trends since 1991, and the Chairman's typical service term of four years. Generally, the Joint Force considers risk in relation to three time categories: Near-term (0-2 years), Mid-term (3-7 years), and Far-term (8-20 years).

(a) Operational Risk (Risk-to-Mission) reflects the current force's ability to attain current military objectives called for by the current NMS, within acceptable human, material, and financial costs. Operational risk is a function of the probability and consequence of failure to achieve mission objectives while protecting the force from unacceptable losses. This risk subset considers the ability to execute current, planned, and contingency operations in the near-term (0-2 years). The normal military planning process allocates enough time and dialogue to develop operational plans that can work in a war or crisis. These plans illuminate risks against known threats or crises. The collective assessment of these plans factors into risk assessment for the CRA, emerging crises, global force management, and other assessments, such as integrated priority lists (IPL). The SecDef's interim progress review planning process is one of the methods used to identify risks for future plans. The time-phased force deployment data (TPFDD) for each of these plans serves to identify and limit risk to the force. Plans without a verified TPFDD have more risk. Commanders consider the feasibility of these plans in conjunction with operational concerns to assess risk to a threat adequately.

---

<sup>2</sup> The CJA survey collects inputs for the CJCS's unified, synchronized strategic assessment effort, informing multiple assessments across the JSPS. The CJA produces a common understanding of the strategic environment and spotlights risks to strategy and the Joint Force.



(b) Future Challenges Risk (Risk-to-Mission) reflects the future force’s ability to achieve future mission objectives over the near and mid-term (0-7 years) and considers the future force’s capabilities and capacity to deter or defeat emerging or anticipated threats. Future challenges risk is a function of the probability and consequence of failure to meet future mission requirements.

(c) Force Management Risk (Risk-to-Force) reflects a Service and/or Joint Force Provider’s ability to generate trained and ready forces within established rotation ratios and surge capacities to meet current campaign and contingency mission requirements; force management risk is a function of the probability and consequence of not maintaining the appropriate force generation balance (“breaking the force”). This risk subset considers the ability to execute plans today (e.g., “fight tonight” on the Korean peninsula) to contingency missions (e.g., potential conflict arising over an economic exclusion zone or a disputed territory) in the near-to mid-term (0-7 years).

(d) Institutional Risk (Risk-to-Force) reflects the ability of organization, command, management, and force development processes and infrastructure to plan for, enable, and improve national defense. Institutional risk is a function of the probability and consequence of the DoD or Services failing to perform established functions. The timeframe associated with this risk subset is much broader. All three time categories—near-, mid-, and far-term—will impact institutional risk (0-20 years). It considers organization and process effectiveness, including the acquisition process, as well as Program Health, Health of the Force, and the Defense Industrial Base.

<b>Military Risk Type</b>	<b>Subset</b>	<b>Timeframe</b>	<b>Assessed against</b>	<b>Sources for Assessment</b>
Risk-to-Mission	Operational Risk	0-2 years	Current military objectives as described in current, planned, & contingency operations.	Campaign Plans, Crisis Response Execution (EXORDs), GEF Objectives, GFM
Risk-to-Mission	Future Challenges Risk	0-7 years	Future mission objectives; capability and capacity to address emerging or anticipated threats	Joint Strategy Review, NIC Global Trends, Defense Planning Guidance, Global Posture, GFM
Risk-to-Force	Force Management Risk	0-7 years	Sufficient trained & ready forces to meet CCMD requirements; force stress versus mission importance	GFM, Readiness, Joint Training, BOG/Dwell Ratios, Service Strategic Plans
Risk-to-Force	Institutional Risk	0-20 years	Organization & process effectiveness in improving national defense	Unified Command Plan, Defense Planning Guidance, Force Quality, Acquisition & Support Processes, GFM

Figure 12. Military Risk Subsets



Military risk is assessed using the four probability and consequence levels depicted in Figures 13 and 14. As with strategic risk, judgment is required to integrate different levels of probability and consequence during the Risk Characterization step. Commanders and their staffs must place risk in context through the application of costs, impacts, time, and end-states in order to inform policy-makers.

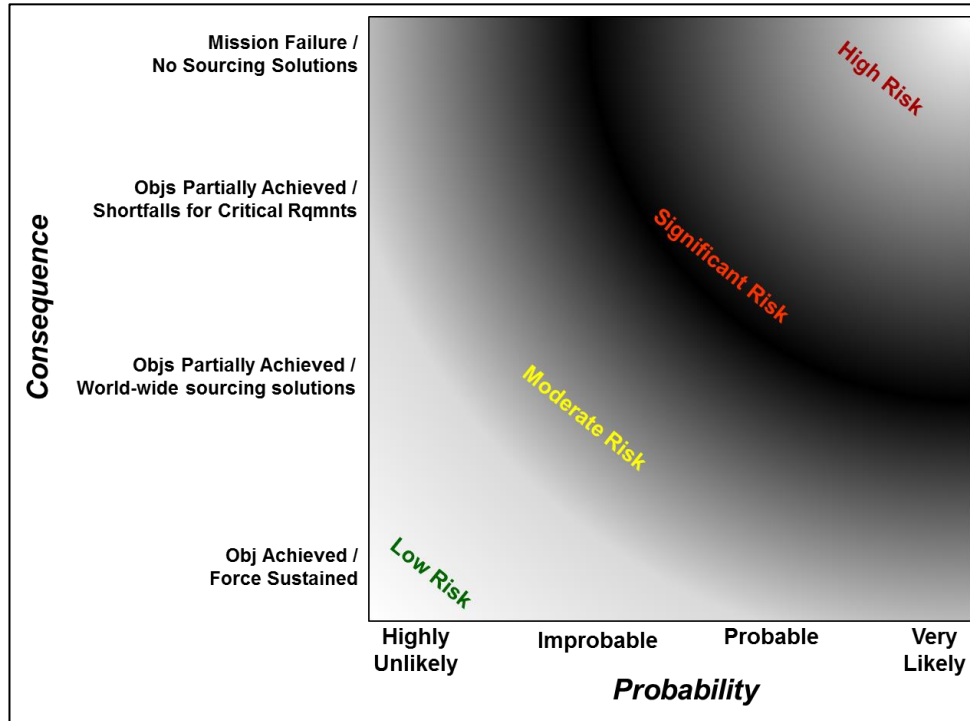


Figure 13. Military Risk Contour

Probability of Event (P)	Consequence of Event (C)
Highly Unlikely (~0-20%)	<ul style="list-style-type: none"> <li>• Mission Success, Objectives Achievable</li> </ul>
Improbable (~21-50%)	<ul style="list-style-type: none"> <li>• Joint Force Fully Sustained and Requirements Sourced</li> </ul>
Probable (~51-80%)	<ul style="list-style-type: none"> <li>• Objectives Partially Achieved (consider time, priority)</li> <li>• Worldwide Sourcing Solutions Exist for Most Requirements</li> </ul>
Very Likely (~81-100%)	<ul style="list-style-type: none"> <li>• Objectives Partially Achieved (consider time, priority)</li> <li>• Shortfalls Exist for Critical Requirements</li> <li>• Mission failure, Objectives Unachievable</li> <li>• No Sourcing Solutions Exist for Critical Requirements</li> </ul>

Figure 14. Military Risk Tables

The following military risk matrix (Figure 15) establishes standard criteria across several variables to help frame the discussion on consequences. The military risk matrix serves as a common risk framework across the Joint Force since it resides in the Global Force Management Implementation Guidance (GFMIG). The military risk matrix and the one in the GFMIG reflect the same information with minor exceptions. Each row presents a factor for consideration with graduated consequences toward success or failure. After considering each applicable factor and assigning an expected result within the matrix, the assessor must use judgment to determine the overall expected consequence level for a situation. This tool facilitates a comprehensive picture of military risk using common metrics for the Joint Force. However, the risk analysis should not be limited to the metrics shown in the figure; if other metrics and categories present relevant information, they should be included in the analysis to facilitate leadership making the most informed decision possible. Coupled with the strategic consequences assessment, commanders and staffs can reach an integrated risk assessment for strategy and military considerations.

RISK	REF	CRITERIA	LOW	MODERATE	SIGNIFICANT	HIGH
Risk to Mission	GEF TCP EXORD	Achieve Objectives (CCMD Daily Ops)	Very Likely (81-100%) Can fully achieve all OBUJ	Likely (51-80%) Can achieve all critical OBUJ	Unlikely (21-50%) Can achieve only most critical OBUJ	Highly Unlikely (0-20%) Potential failure; can't achieve critical OBUJ
	CPG JSCP	Achieve Plan Objectives (Contingencies)	As Planned (Minimal Costs)	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable Costs)
	CCMD	Authorities	Full authority provided to achieve all objectives	Sufficient authority provided to achieve most objectives, no critical shortfalls	Insufficient authority provided to achieve some critical objectives	Insufficient authority for key objectives, potential mission failure
	JCCA	Resources meet required timelines	As Planned (Minimal Costs)	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable costs)
Risk to Mission & Force	CCMD & Service	Partnerships	Partnerships Effective	Critical Partnerships Effective	Critical Partnerships Partially effective	Critical Partnerships Ineffective, Potential Mission Failure
		Messaging	Messaging Effective	Key Messages Effective	Key Messages Partially Effective	Key Messages Ineffective, Potential Mission Failure
		DOTMLPF-P Capability vs. Threat Capability	Dominance	Superiority	Parity	Inferiority
Risk to Force	GFM	Meet CCDR Requirements (CCMD Daily Ops)	GFM Sourced $\geq$ 90% (Some shortfalls)	GFM Sourced $\geq$ 80% (No critical shortfalls)	GFM Sourced $\leq$ 70% (Critical shortfalls)	GFM Sourced $\leq$ 70% (Shortfalls cause mission failure)
	JCCA / GFM	Meet CCDR Requirements (Contingencies)	Full capacity to source all CCDR requirements	Shortfalls cause minor plan deviations (No critical shortfalls)	Shortfalls cause major plan deviations	Shortfalls cause plan failure
	JFRR & DRRS	Readiness (DRRS)	Full Spectrum C1 Full Capacity	Ready for MCO C1/C2 Some capacity shortfalls	Ready for Minor Armed Conflict Critical Capabilities C1/C2 Limited Capacity	Critical Capabilities $\leq$ C2 Capacity shortfalls cause mission failure
	GFM	Stress on AC Force	Minor Stress (DT > 1:2)	Moderate Stress (1:2 > DT > 1:1.5)	Major Stress (1:1.5 > DT > 1:1)	Extreme Stress (DT < 1:1)
		Stress on the RC Force	Minor Stress (DT > 1:5)	Moderate Stress (1:5 > DT > 1:4)	Major Stress (1:1.4 > DT > 1:3)	Extreme Stress (DT < 1:3)
	JCIDS / CPR	Programmatic	Meets or exceeds schedule, IOC or FOC; incurred savings	Minor delays, milestone $\geq$ B Minor budget difficulty	Major Delays, milestone $\leq$ A Over Budget (Nunn-Murphy)	Program failure, Zeroed Out (De-funded)
JCIDS / CJA	Force Development & Industrial Base	Meet all mission requirements	Meet priority mission requirements (no critical shortfalls)	Critical shortfalls cause major plan deviations	Failure to meet essential requirements causes mission failure	

Figure 15. Military Risk Matrix

### **Army Force Generation (ARFORGEN) Vignette: Risk-to-mission and Risk-to-force**

*In response to requirements generated by the global war against terrorism (defined as an era of “persistent conflict”), the U.S. Army implemented the ARFORGEN process to manage military risk. This existed as a rotational readiness model designed to maximize strategic flexibility. In essence, the Army defined this process as the structured progression of unit readiness (both active and reserve components) over time to produce trained, ready, and cohesive units prepared for operational deployment in support of the combatant commander and other Army requirements. The ARFORGEN process served as the Army’s core process for force generation that cycled units through three force pools: Reset, Train/Ready, and Available. Each of the three force pools contained a balanced force capability to provide a sustained flow of forces (approximately one-third of brigade combat teams) for current commitments and to hedge against unexpected contingencies. For example, using 45 Brigade Combat Teams (largest force structure during the global war against terrorism), 15 would be deployed to combat (10 to Iraq and 4 to Afghanistan), 15 brigades would be in Reset, and 15 brigades would be in training cycles preparing for deployment. While a third of the brigades existed in each of the three categories, the units sustained different progression timelines to maximize the limited assets of training centers (combat training centers and Kuwait) and movement resources (strategic lift and movement node throughput). The ARFORGEN process could supply three levels of force demand: steady-state, surge, or full surge. Furthermore, this model supported the Army’s planning, programming, budgeting, and execution (PPBE) process and synchronized the Army’s efforts to provide land forces to the Nation.*

*The ARFORGEN process balanced risk-to-mission and risk-to-force for the U.S. Army during a demanding period fighting global terrorism. Before ARFORGEN (pre-9/11), the Army employed a tiered readiness strategy for force generation. The Army had relied mainly on major theater war scenarios to plan and modernize its force. Counterinsurgencies in Afghanistan and Iraq exposed the flaws of tiered readiness aimed at fielding the majority of the Army to fight one or two major theater wars either simultaneously or near simultaneously. ARFORGEN allowed the Army to meet mission requirements in Iraq and Afghanistan while not “breaking” the Army as a functional service. This process produced an agile force structure that could support multi-year insurgencies or full mobilization to combat major theater wars. While the ARFORGEN process certainly had shortcomings—most notably about meeting equipment demands at the same time for both active and reserve components, limited strategic air and sea lift, and sustainable equipment maintenance—it effectively managed military risk at a time of war. Without this process, the Army could have erred against the mission by failing to provide adequate forces or tilted the other direction by*

*overusing the force, rendering it moot for a future conflict. This model built a resilient system that maintained a credible Army.*<sup>3</sup>

The ARFORGEN vignette highlights balance achieved for military risk. ARFORGEN implementation caused the Army to remain functional to support both current strategic aims and remain ready to address future conflicts such as a general theater war. In addressing military risk, the Joint Force must consider risk-to-mission and risk-to-force over time. During the height of the wars in Iraq and Afghanistan, the Nation would not mortgage the Army's future abilities completely against the strategic priorities of the global war against terrorism. The adoption of ARFORGEN put the best possible Army in the field without incurring strategic risk if the Nation had called the Army to fight a general war.

---

<sup>3</sup> Consult *Army Regulation 525-29, Military Operations: Army Force Generation* (14 March 2011) and RAND study, *Efficiencies from Applying a Rotational Equipping Strategy* (2011) for more information on the ARFORGEN process.

(3) Integrated Risk. The integrated risk matrix (Figure 16) combines the assessments from the strategic and military risk matrixes. The integrated risk matrix serves as a tool to visually capture the combined aspects of CJCS strategic risk, CJCS military risk, CCMD operational risk, and force management risk. Commanders and staffs derive integrated risk information from their own assessments and the military risk and strategic consequence matrices. The decision to execute an Afghanistan surge along the model of 2007 in Iraq demonstrates the way in which both military leaders and policy-makers integrate strategic and military risk. This integrated matrix allows an organization to present a comprehensive risk assessment. A leader will use this matrix as a basis to articulate risk and place it into context for policy makers.

RISK	CRITERIA	LOW	MODERATE	SIGNIFICANT	HIGH	
CJCS Strategic Risk	Probability of Event	Very Likely (81-100%)	Likely (51-80%)	Unlikely (21-50%)	Highly Unlikely (0-20%)	
	Consequence of Event	Limited Interests	Major Damage to US Interests	Catastrophic Damage to US Interests	Existential Damage to US Existence	
CJCS Military Risk	Resource & Execute NMS Missions	Very Likely full range of missions	Likely ability to execute missions	Unlikely to execute missions	Highly Unlikely to execute missions	
	Mission Importance	Other Missions (Non-GEF Missions)	Important Missions (GEF Cat. 3-5)	Critical Missions (GEF Cat. 1-2)	Essential Missions (U.S. Existence)	
CCMD Operational Risk <i>Ability to execute assigned missions at acceptable human, material, financial and strategic cost</i>	Achieve Military OBJS (Current Ops)	Very Likely (ex: 81-100%)	Likely (ex: 51-80%)	Questionable (ex: 21-50%)	Highly Unlikely (ex: 0-20%)	
	Achieve Objectives (Contingencies)	Very Likely (ex: 81-100%)	Likely (ex: 51-80%)	Questionable (ex: 21-50%)	Highly Unlikely (ex: 0-20%)	
	Authorities	Full Authority Provided for all OBJs	Sufficient Authority to achieve critical OBJs	Insufficient Authority to achieve key OBJs	Lack of Authority jeopardizes mission	
	Planning	Level III or IV Plans	Level I or II Plans	CCDR CONOPs (Anticipated Event)	Initiate Planning (Complex Crisis)	
	Resources Meet Required Timelines	As Planned (Minimal Costs)	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable Costs)	
Service / JFP Force Management Risk <i>Ability to recruit, man, train, equip and sustain the force to meet strategic objectives</i>	Meet CCDR Req's (Current Ops)	GFM Sourced > 90% (Some shortfalls)	GFM Sourced > 80% (No critical shortfalls)	GFM Sourced > 70% (Critical shortfalls)	GFM Sourced < 70% (Mission failure)	
	Meet CCDR Req's (Contingencies)	Full capacity to source all CCDR req's	Shortfalls cause minor plan deviations	Shortfalls cause major plan deviations	Shortfalls cause plan failure	
	DOTMLPF-P Capability vs Threat	Dominance	Superiority	Parity	Inferiority	
	Readiness	Strategic Depth for All NMS Missions	Strategic Depth for Current Operations	Next-to-Deploy Forces Ready "Just in Time"	Deployed Forces Not Ready for Mission	
	Health of Force	Stress on AC Force	Minor Stress (DT > 1:2)	Moderate Stress (1:2 > DT > 1:1.5)	Major Stress (1:1.5 > DT > 1:1)	Extreme Stress (DT < 1:1)
		Stress on RC Force	Minor Stress (DT > 1:5)	Moderate Stress (1:5 > DT > 1:4)	Major Stress (1:1.4 > DT > 1:3)	Extreme Stress (DT < 1:3)

Figure 16. Integrated Risk Matrix

**2009 Surge in Afghanistan Vignette: Integrating Strategic and Military Risk**

*In 2009, the CJCS assessed the relative strategic risks to U.S. interests and the relative military risks to the missions in Iraq and Afghanistan. He asked the Joint Staff to assess risks in other areas of responsibilities. Military and Strategic risk in Iraq had decreased and the strategic situation was stable, while Military and Strategic Risk in Afghanistan were elevated and rising. Based upon this collective assessment and balancing the risks, the Chairman recommended the "Afghan Surge." The President considered the risks and shifted priority to Afghanistan. The surge required 40,000 more Soldiers and Marines – which increased military risk-to-force but was necessary to decrease military risk-to-mission in theater and associated strategic risk. This is another example of highly correlated strategic and military risk.*

**2007 Integrated Risk Vignette. "Balancing Strategic and Military Risk on the Risk Contour"**

*The risk contour graphs help leaders and staff visualize an event or situation when considering military and strategic risk. During the annual CJA submission, in support of CRA development, Commander USPACOM assessed risk. He assessed military risk to the defense of a Treaty Ally as "High"; that is, in event that OPLAN X was executed it was unlikely that the Plan would achieve its objectives. However, he assessed the strategic risk of the actual attack as "Low"; very unlikely to occur. He concluded that his overall risk was "Moderate"; giving equal weight to the strategic risk probability and military consequence. This assessment provided a very measured, clear-eyed view of risk which better informed Global Force Management (GFM) decisions and other risk tradeoff discussions. This is an example where strategic and military risk were not highly correlated since strategic risk was driven down by economic and political factors and the deterrent impact of forward forces indeterminate. In this example, the PACOM Commander's risk assessment resides in the moderate risk band effectively representing the threat.*

b. Risk Assessment for the CRA (Step 2). The CRA leverages multiple perspectives to delineate the sources and drivers of risk over time and the Nation's vulnerability to those threats. These inputs provide a basis for initial estimates of probability and expected consequences and set the stage for risk characterization using the tables established in problem framing. The majority of feedback comes from JSPS processes and products, to include:

(1) CJA: Captures Combatant Command and Service perspectives regarding strategic risks to national interests in their Areas of Responsibility and risks to achieving their military objectives in the near- and mid-terms.

(2) Joint Staff Independent Risk Assessment: Independent assessment to gather perspectives from across the Joint Staff in order to identify potential sources and drivers of strategic and military risk.

(3) The Chairman's Readiness System (CRS): The CRS strategic readiness component is carried out via the Joint Combat Capability Assessment process and has two major assessments—the Joint Force Readiness Review (JFRR) and Joint Combat Capability Assessment-Plan Assessment (JCCA-PA). The results capture the Joint Force ability to resource and execute missions reflected in the NMS. Readiness outputs help determine military risk, risk-to-force, risk-to-mission, and potential impacts on strategic risk events.

(4) GFM: GFM aligns force assignment, apportionment, and allocation methodologies in support of the Department's strategic guidance. It gives senior DoD leadership comprehensive insight into the global availability of forces, and the risk and impact of proposed force changes.

(5) Capability Gap Assessment (CGA): Identifies critical capability shortfalls and assesses how the future year's defense plan will address those gaps. The CRA is informed by the previous year's gaps and the state of previously identified gaps.

(6) Joint Strategic Intelligence Estimate (JSIE): Provides a global intelligence picture, analyzed across regions to expose gaps and seams.

(7) Joint Logistics Estimate (JLE): An evaluation of how well the Joint Force can project, support, and sustain itself in the near-, mid-, and far-terms in support of the missions called for in the Unified Command Plan (UCP), NMS, and the Joint Strategic Capabilities Plan (JSCP).

(8) Senior military and defense officials' views are gathered during the 4-star Strategic Seminar Series, the Senior Leader Conferences, JCS and Operations Deputies tank meetings, and interviews with the National Intelligence Council (NIC). Contributions from academia and think tanks are also considered when assessing risk.

c. Risk Characterization (Step 3a). After evaluating the probability and consequence of strategic and military sources and drivers of risk, events are assigned a risk level of high, significant, moderate, or low. While numerous senior officers, stakeholders, and experts contribute ideas and thoughts on how to characterize each risk, the Chairman makes the final decision on risk levels conveyed in the CRA.

(1) Military Risk. Both risk-to-mission and risk-to-force must be considered when characterizing military risk. The military risk contour graph

is used to plot probability and consequence to determine the appropriate level of risk.

(2) Once all of the strategic and military risks have been characterized and approved by the Chairman, the Joint Staff J5 finalizes the CRA report and forwards it to the Chairman for signature. It is then passed to the Secretary of Defense to evaluate and manage the risk.

d. Risk Evaluation (Step 3b). During this step, the Secretary determines the acceptability of risk presented in the CRA report and develops options for managing the risk. Depending on the situation, the Secretary may decide to accept, avoid, or transfer the risk as described in Enclosure B, Joint Risk Analysis Methodology (JRAM). For example, the Secretary may accept risk in the near-term, while directing mid-term mitigation actions or transferring risk to the future by focusing resources on current issues. In this case, transfer would be asking the next higher authority—POTUS—to decide to accept this risk.

Another major consideration during the risk evaluation step is to trade space between strategic and military risk. This is particularly true if an adversary acts in an opportunistic fashion. The key is to contemplate second and third order effects of risk decisions. Decisions made to accept or mitigate military risk have the potential to increase strategic risk. The 2007-08 Iraq Surge is a good example of this aspect of risk evaluation. The decision to surge forces to win the current fight in Iraq mortgaged readiness for future conflict. Decision-makers determined that the strategic risk to future conflict remained acceptable to assume more military risk in the near-term.

e. Risk Management (Step 4). The RMP is the formal means for the Secretary to explain how the Department will mitigate “significant” or “high” risk identified by the Chairman. It is designed to address risk enterprise-wide and is normally developed in concert with the Joint Staff, Combatant Commands, and Services. The DoD mitigates risk in many ways. Strategic risk is mitigated by adjusting authorities, policies, budget, and priorities. The previously-defined military risk subsets (based on source and time horizon) help determine the most effective ways to address that type of risk.

(1) Changing priorities in the JSCP or Guidance for the Employment of the Force (GEF) impact Operational Risk and the future.

(2) Changes to the GFMIG can mitigate Future Challenges Risk.

(3) Updates to the Defense Planning Guidance (DPG), Chairman’s Program Recommendation (CPR) and Joint Requirements Oversight Council (JROC) guidance generally address Force Management Risk, both in the near-term and beyond.



(4) Updates to the UCP, doctrine, concepts, or professional military education can mitigate Institutional Risk.

f. Risk Communication. Clear communication between all leaders and staff is critical to achieving a cohesive and balanced CRA report. For example, Combatant Commanders and Service chiefs must have a common understanding of terms, definitions, and how to characterize risk in order to properly convey risk in their CJA responses—one of the significant inputs to the CRA. The Joint Staff and other contributors must have the same baseline understanding to ensure their feedback is relevant and appropriately aligned.

3. Summary. The Chairman's Risk Assessment serves as the keystone for risk calculation to the Nation's strategy and Joint Force. Together with the National Military Strategy, the Joint Force will use the CRA as a starting point to assess risk for other processes and operations. The next chapter outlines how to assess risk for other JSPS requirements.

ENCLOSURE D

RISK ANALYSIS WITHIN THE JOINT STRATEGIC PLANNING SYSTEM (JSPS)

1. Introduction. While the Chairman's Risk Assessment of the National Military Strategy serves as the basic strategic and military risk bench marker for the nation and the Joint Force, commanders and staffs daily consider risks that affect operations in relation to current and future threats and their own forces. The cyclical nature of the JSPS requires the Joint Staff, Combatant Commands, and Services to utilize the Joint Risk Analysis Methodology (explained in Enclosure B) to assess risk for each of these system components. Calculating risk throughout the JSPS will lead to the best decisions and recommendations as the Joint Force executes its title 10 statutory requirements, functions, and products.

a. Risk Analysis in Support of Other JSPS Processes. Many processes within the JSPS and the Planning, Programming, Budgeting, Execution System require risk analysis to inform decision-making. Some of these major efforts are force readiness (J3), force allocation (J3 and J8), Integrated Priority Lists (J8), and Interim Progress Review for Plans (J5). Using the standardized methodology of this manual allows leaders to manage risk effectively. This may mean transferring risk from one area (e.g. risk to mission – force employment) to another (e.g. risk to force – force management) or from one timeframe (e.g. near) to another (e.g. far) or finding other ways to reduce risk identified through the risk analysis.

b. Risk in Military Readiness. Readiness is a major component of the Joint Force's ability to resource, execute, and sustain military operations adequately. Identifying and mitigating readiness shortfalls are essential to quantify, assess, and mitigate military risk. The outputs of the Chairman's Readiness System, the Joint Forces Readiness Review and Joint Combat Capability Assessment and Plan Assessment, are used to inform the CRA. Mitigation decisions based on CRA data can, in turn, drive priorities for military readiness.

c. Risk in Force Employment – Global Force Management (GFM). The CRA provides the strategic and military risk baseline to inform senior leaders' prioritization and decisions to source CCDR requirements via the GFM allocation process (e.g., rotational forces, emergent requirements). The CRA and RMP help senior leaders understand where the Joint Force is accepting or accruing risk, for how long, and with what mitigation. Specifically, the Chairman considers the GEF's Readiness and Availability Priorities (RAP) to assist the Secretary in evaluating the cumulative impacts caused by GFM decisions and the force readiness, to meet prioritized mission sets.

(1) GFM Problem Framing. This step involves a guidance review, to include examining steady state GEF objectives, the Force Allocation Decision Model, the RAP, and other readiness reporting information.

(2) GFM Risk Assessment. During this step, the status and progress towards achieving the Combatant Commands' steady state objectives, current operations, and abilities to meet contingency plan timelines and objectives is assessed. This helps identify the extent to which current investments and activities are mitigating risk to priority missions.

(3) GFM Risk Judgment (Characterization and Evaluation). The GFM Board (GFMB) characterizes risk, preparing recommendations for the Secretary based upon a holistic dialogue on assigned forces, risk, competing demands, and mission priorities. To transfer or align DoD's near-term operational risk profile, the GFMB assesses the recommended GFM Allocation Plan (GFMAP) base order. The Secretary ultimately evaluates risk and is the approval authority for the GFMAP via the Secretary of Defense Orders Book (SDOB).

(4) GFM Risk Management. The GFMAP Base Order establishes the near-term operational risk for the fiscal year. Adjustments to the allocation of forces are included in modifications to the GFMAP throughout the annual GFMAP life cycle. Any modifications are included in the SDOB, normally updated bi-weekly, though changes can be entered as or when required. The Secretary considers the Chairman's, Combatant Commander's, Force Provider, Joint Force Coordinator, and Joint Force Provider risk assessments which include impact on the ability to meet surge requirements, Service readiness recovery goals, availability of the future force or capability in question, and deployment or mobilization timelines.

d. Risk in Force Management. The GFMIG addresses risk across time by integrating assignment, apportionment, and allocation information. The force assignment tables in the GFMIG and Forces for Unified Command Memorandum ("Forces For"), which documents the Secretary's direction to the Service Secretaries for the assignment of forces to CCDRs in accordance with title 10, address long term missions and risk. The force apportionment tables and the GFMIG's apportionment guidance addresses risk by describing the forces available for contingency planning.

(1) GFMIG Problem Framing. This includes a strategic guidance review of the DSR, NMS, UCP, GEF, force assignment tables, force apportionment tables, previous CRA, CJA information, and the JSCP.

(2) GFMIG Risk Assessment. Long-term risk to achieving UCP-directed missions, the Chairman's Program Guidance-and JSCP-directed planning requirements, and Theater Campaign Plan are assessed.

(3) GFMIG Risk Judgment and Management. The GFMIG documents the Secretary's direction for the GFM assignment, allocation, and apportionment processes. The Secretary mitigates risks by assigning forces to CCDRs and redistributing those forces among the CCDRs via the allocation process. The apportionment process provides the Services' assessment of the number of specific types of forces that can reasonably be expected to be available (globally) over a rough timeline to inform planning.

e. Risk in Force Development (FD). Strategic and military risk analysis is used to inform programming and budgeting decisions as they relate to force development. This relationship is why the 15 February due date for the CRA and RMP is critical. Most importantly, the CRA informs the Secretary of Defense's input to the annual Presidential Budget.

(1) FD Problem Framing. As in previous examples, this step includes a review of strategic guidance, specifically the DPG.

(2) FD Risk Assessment. IPLs are submitted each year as Service and CCMD input to the CJA. J8 leads the Joint Staff-wide CGA based on the IPLs. The staff compares gaps identified by Combatant Commands with previous gaps and ongoing efforts. The CRA provides strategic and military risk context for the CGA and aids in capability portfolio prioritization and action recommendations to the JROC.

(3) FD Risk Judgment. The CRA provides context in which the Functional Capability Boards and the Joint Capability Board can make risk judgments during the CGA. It also provides the JROC with perspective on whether ongoing capability development efforts are sufficient or if additional emphasis is needed on programs yielding the future force.

(4) FD Risk Management. Risk in Force Development is managed through decisions made on future capability development and associated budget choices. It is also managed via non-material solutions derived from Joint Concept Development (JCD) processes. JCD provides an azimuth for future force development by anticipating operational challenges and proposing solutions with associated capabilities to overcome those challenges. Strategic and military risk assessments inform joint concept selection. The Capstone Concept for Joint Operations, Joint Operating Environment, and Joint Operating Concepts provide a framework to consider the joint operations and capabilities needed for risk mitigation and future success. Risk management is included in the Joint Capabilities Integration and Development System process and is addressed during milestones.

(5) FD Risk Communication. The CGA results are recorded and distributed by publishing a JROC Memorandum. The CPR is developed during the CGA process and provides the Chairman's risk-informed priorities for force

development. The CPR serves as a bridging document between the CRA and OSD's DPG and Fiscal Guidance.

f. Risk-Informed Strategy Development. The Chairman is required, by statute, to assess the risk to the NMS and the DSR. The insights and outputs of these assessments, in addition to the Chairman's advice to the President, Secretary of Defense, and the National Security Council (NSC), inform broad interagency, and national-level document development. For example, the Chairman's advice during National Security Strategy development is largely based upon the CJCS's risk assessment, in particular strategic risk.

(1) Numerous other national level strategies and strategic documents, such as directives from the White House or the NSC are also informed by risks to interests, missions, and forces as characterized by the Joint Staff and OSD. Risk is also used when developing DoD strategic documents and approaches, such as the strategy on specific issues (e.g. cyberspace), and overarching defense guidance (e.g. DSR).

(2) The Chairman is required by statute to provide an independent risk assessment of the DSR, which is included in the final report. The DSR risk assessment follows the Joint Risk Analysis Methodology.

(a) During years when the DSR is published, the Chairman is still required to complete an annual risk assessment to the NMS. The DSR and NMS assessments have different time horizons, so the Chairman must ensure these assessments remain different, but are complementary.

2. Special Risk Assessments. During day-to-day operations and strategy-related endeavors, questions arise about risk related to conditions, choices, or activities. The Joint Staff is able to accomplish short-notice risk analysis using the Joint Risk Analysis Methodology to frame options. Some examples of this type of rapid risk analysis are:

- (1) Strategic and military risk analysis on the Ottawa Treaty banning landmine use;
- (2) Strategic risk assessment on future adversary assertiveness;
- (3) Strategic risks associated with the Treaty on Conventional Forces in Europe;
- (4) Strategic and military risk associated with the campaign against ISIL.

3. Summary. The Joint Force must consider risk to apportion resources, set priorities, and achieve national military objectives. This is done primarily through the processes and products within the JSPS. As each process tackles problem sets, commanders and staffs will utilize risk analysis to come to the best military advice possible in pursuit of an effective strategy.

## ENCLOSURE E

### REFERENCES AND OTHER RISK DOCUMENTS

1. Introduction. Practitioners study risk for various reasons. The study of risk crosses disciplines, from business and economics to science and technology, and is applicable to the military. The methodology and concepts presented in this manual are based on and aligned with the research accomplished across the broader risk community.

2. Joint Publications and CJCS Directives.

a. Joint Publication (JP) 5-0, *Joint Operation Planning*, discusses risk as part of planning and operations. JP 5-0 emphasizes the importance of risk identification and mitigation throughout the planning process. Risk in this context is focused on mission accomplishment and impact to mission.

b. JP 3-0, *Joint Operations*, delves into risk management as a function of command and a key planning consideration. It depicts a very basic risk management process.

c. JP 1-02 *Department of Defense Dictionary of Military and Associated Terms*, includes standard definitions for risk terms utilized in this manual.

d. CJCS Instruction 3100.01 Series, *Joint Strategic Planning System*, explains how the Chairman meets statutory responsibilities as directed by U.S. Code. The Chairman's Risk Assessment is a key JSPS documents directed by U.S. Code.

e. CJCS Manual 3122.01 Series, *Joint Operation Planning and Execution Systems (JOPES) Volume 1, Planning and Policies and Procedures*.

f. CJCS Manual 3130.06 Series, *Global Force Management Allocation Policies and Procedures*, governs risk analysis for the GFM.

g. CJCS Instruction 3141.01 Series, *Management and Review of JSCP-Tasked Plans*.

h. CJCS Instruction 3401.02 Series, *Force Readiness Reporting*.

i. CJCS Instruction 3401.01 Series, *Joint Combat Capability Assessment*.

3. Non-Governmental Sources of Risk Knowledge.

a. Documents from the International Risk Governance Council (IRGC) were particularly informative in developing this manual. The IRGC, a science-based think tank, is an independent, non-profit organization whose mission includes “developing concepts of risk governance, anticipating major risk issues, and providing risk governance policy advice for key decision-makers.” The IRGC white paper, “*Risk Governance: Towards an Integrative Approach*,” by Ortwin Renn and Peter Graham, provided key background and substantiated fundamental concepts used when producing this Manual.

b. The International Organization for Standardization (ISO) is another non-governmental international organization and independent resource. ISO 31000:2009, “*Risk Management – Principles and Guidelines*,” provides principles, a framework and process for managing risk.

4. Risk in Other U.S. Government Agencies. This list of resources is not exhaustive, but it gives a sense of how risk is applied in other agencies.

a. U.S. Department of Commerce: *Enterprise Risk Management*, DAO 216-20.

b. National Institute of Standards and Technology: *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems*. NIST Special Publication 800-37, Rev 1.

c. Office of Management and Budget (OMB): OMB Circular A-123, *Internal Control Systems*, establishes enterprise risk management approaches.

d. Department of Homeland Security (DHS): *DHS Risk Lexicon*, September 2010. The DHS Risk Lexicon is part of that Department’s efforts to establish a common framework for overall management and analysis of homeland security risk.

e. Central Intelligence Agency: *Measuring Risk to US Interests: A Framework for Risk Exposure and National Strategic Importance* (9 March 2015).

5. Risk in the Department of Defense. The most common or well-known type of risk management within the DoD centers on Operational Risk Management (ORM) or, in the US Army, simply Risk Management as described in Army Pamphlet 385-30. However, more recently the Department has recognized the need for risk principles to be applied across diverse issues, including acquisition and information technology.



a. DoD Instruction 6055.01, *DoD Safety and Occupational Health (SOH) Program, October 14, 2014*. This document provides overarching DoD guidance regarding risk principles and risk management with respect to health and safety. The instruction provides a five-step risk management process which is used across all Services to help ensure synergy across Joint Force operations. The risk management strategies are applied to eliminate occupational injury or illness and loss of mission capability. They are intended for use in all military operations and activities, including acquisition, procurement, logistics, and facility management.

b. Another DoD document, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (June 2015)*, focuses on the relationship between effective risk management and programmatic success. It provides guidance on establishing a risk management program for defense acquisition programs.

c. DoD Instruction 8510.01, *Risk Management Framework for DoD Information Technology (IT)*, describes policy and procedures applicable to the integrated enterprise-wide structure for cybersecurity risk management.

d. *Global Force Management Implementation Guidance, FY 2016-2017* provides a key explanation of how the CRA places GFMB force allocation in context.

6. Summary. While risk in operations, acquisitions, and information technology has been addressed by the DoD, this manual offers a Joint Risk Analysis Methodology that can be applied at the strategic level to inform senior decision-makers on significant programmatic, strategy, and policy-level concerns.

## GLOSSARY

### PART I-ABBREVIATIONS AND ACRONYMS

AC	Active Component
AOR	Area of Responsibility
ARFORGEN	Army Force Generation
BOG	Boots on the Ground
CAT	Category
CCDR	Combatant Commander
CCJO	Capstone Concept for Joint Operations
CCMD	Combatant Command
CGA	Capability Gap Assessment
CJA	Comprehensive Joint Assessment
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COOP	Cooperation
CP	Campaign Plan
CPG	Chairman's Programming Guidance
CPR	Chairman's Program Recommendation
CRA	Chairman's Risk Assessment
CRS	Chairman's Readiness System
CSDJF	Chairman's Strategic Direction to the Joint Force
DHS	Department of Homeland Security
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOTMLPF-P	Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Policy
DPG	Defense Planning Guidance
DRRS	Defense Readiness Reporting System
DSR	Defense Strategy Review
EXORDS	Executive Orders
FCB	Functional Capability Board
FD	Force Development
FOC	Full Operational Capability
FYDP	Future Years Development Plan
GEF	Guidance for Employment of the Force
GFM	Global Force Management
GFMAP	Global Force Management Allocation Plan
GFMB	Global Force Management Board
GFMIG	Global Force Management Implementation Guidance
HA/DR	Humanitarian Assistance/Disaster Relief

HLD	Homeland Defense
IMF	International Monetary Fund
INTL	International
IOC	Initial Operational Capacity
IPL	Integrated Priority List
IRGC	International Risk Governance Council
ISIL	Islamic State of Iraq and the Levant
ISO	International Organization for Standardization
IT	Information Technology
JCB	Joint Capabilities Board
JCCA	Joint Combat Capability Assessment
JCCA-PA	Joint Combat Capability Assessment and Plan Assessment
JCD	Joint Concept Development
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
JFP	Joint Force Provider
JFRR	Joint Forces Readiness Review
JLE	Joint Logistics Estimate
JOPEs	Joint Operation Planning and Execution Systems
JP	Joint Publication
JRAM	Joint Risk Analysis Methodology
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JSCP	Joint Strategic Capabilities Plan
JSIE	Joint Strategic Intelligence Estimate
JSIRA	Joint Staff Independent Risk Assessment
JSPS	Joint Strategic Planning System
JSR	Joint Strategy Review
JWPS	Joint Worldwide Planners Seminar
MCO	Major Combat Operations
MOD	Moderate
NATO	North American Treaty Organization
NEO	Noncombatant Evacuation Operation
NIC	National Intelligence Council
NIST	National Intelligence Support Team
NMOs	National Military Objectives
NMS	National Military Strategy
NSC	National Security Council
NSS	National Security Strategy
OBJs	Objectives
OMB	Office of Management and Budget
OPS	Operations
OPSDEPS	Service Operations Deputies Source
ORM	Operational Risk Management

OSD	Office of the Secretary of Defense
POM	Program Objective Memorandum
POTUS	President of the United States
PPBES	Planning, Programming, Budgeting, Execution System
RAP	Readiness and Availability Priorities
RC	Reserve Component
RMF	Risk Management Framework
RMP	Risk Mitigation Plan
SASC	Senate Armed Services Committee
SDOB	Secretary of Defense Orders Book
SecDef	Secretary of Defense
SIG	Significant
SLC	Senior Leader Conference
SOCOM	Special Operations Command
SOH	Safety and Occupational Health
SOI	Strength of an Interest
SPC	Strategic Planning Construct
SSS	Strategic Seminar Series
SVC	Service
SYS	System
TCP	Theater Campaign Plan
TPFDD	Time-Phased Force Deployment Data
UCP	Unified Command Plan
WMD	Weapons of Mass Destruction

## PART II-DEFINITIONS

Drivers of Risk – Factors that act either to increase or decrease the probability, frequency, or scale of risks arising from various sources.

Hazard – Security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

Joint Risk Analysis Methodology (JRAM) – A risk framework providing a consistent, standardized way to assess risk and recommend risk mitigation measures.

Joint Strategic Planning System –The primary means by which the Chairman of the Joint Chiefs of Staff performs statutory assistance to the President and Secretary of Defense to provide strategic direction to the Armed Forces.

Military Risk – The estimated probability and consequence of the Joint Force's inability to achieve objectives while providing and sustaining military resources.

Problem Framing – First step in the JRAM, generating a common understanding of the risk issue(s), major assumptions, and procedural rules.

Risk – The probability and consequence of an event causing harm to something valued.

Risk Assessment – Second step in the JRAM, during which sources of harm are linked with likely consequences and expected probability.

Risk Characterization – Sub-step of Risk Judgment during which events are assigned a level of risk.

Risk Evaluation – Sub-step of Risk Judgment, during which a decision-maker determines the acceptability of a risk.

Risk Judgment – Third step in the JRAM, composed of Risk Characterization and Risk Evaluation, aimed at determining acceptability of a risk.

Risk Management – Fourth step in the JRAM, during which risk decisions to accept, avoid, reduce, or transfer risk are designed, implemented, and monitored.

Sources of Risk – Threats or hazards which alone or combined have potential to cause harm to the valued item or idea.

Strategic Risk – The estimated probability and consequence of an event(s) causing harm to U.S. national interests.

Threat – A state or non-state entity with capability and intent to cause harm.