Department of Homeland Security
DHS Directives System
Directive Number: 007-03
Revision Number: 00
Issue Date: 03/28/2011

INTEGRATED RISK MANAGEMENT

I. Purpose

This Directive establishes responsibilities for implementing the Department of Homeland Security (DHS) Policy for Integrated Risk Management (IRM).

II. Scope

A. This Directive applies throughout DHS with the exception of the Office of Inspector General.

B. This Directive supersedes Secretarial Memorandum "DHS Policy for Integrated Risk Management," May 27, 2010.

III. Authorities

A. Title 6, United States Code, Section 112, "Secretary; functions"

B. DHS Delegation 17001, Delegation to the Under Secretary for National Protection and Programs

IV. Responsibilities

A. The **Under Secretary for the National Protection and Programs Directorate (NPPD)** is responsible for overseeing all aspects of this Directive and:

1. Leads DHS efforts to establish a common framework to address the overall management and analysis of homeland security risk.

2. Engages the Secretary and Component Heads as needed on risk-related matters and chairs the DHS Risk Steering Committee.

3. The **Director, Office of Risk Management and Analysis (RMA)**:

a. As directed by the Under Secretary for NPPD, advises and represents the Secretary on risk management, risk analysis, and decision support.

b. Administers the Risk Steering Committee (RSC).

c. Develops and coordinates a policy framework, in collaboration with the RSC, to inform risk-based strategies to enhance and integrate the Department's risk management capability.

d. Conducts a periodic assessment of the Department's risk management capability to assess status and progress.

e. Develops and shares innovative concepts, training, and tools to support risk management, analysis, and decision support for DHS and the homeland security enterprise, leveraging existing efforts where possible. This shall include a risk knowledge management system to facilitate the sharing of methodologies, analysis and data across the homeland security enterprise.

f. Supports Component Heads, along with Component lead executives, in promoting IRM within and across the homeland security enterprise.

g. Through a policy framework, informs and executes risk assessments and analysis in support of DHS cross-Component strategic decision-making, including the resource allocation process and other activities related to the Planning, Programming, Budgeting, and Execution process.

h. Participates in and provides risk-related advice and technical assistance to DHS strategic decision-making bodies.

4. The **Assistant Secretary for Infrastructure Protection (IP)**:

a. Leads and executes, in collaboration with Components and Federal departments and agencies, a risk-informed approach for supporting the protection and resilience of critical infrastructure and key resources consistent with the National Infrastructure Protection Plan (NIPP).

b. Provides guidance, methodologies, and assistance to NIPP public and private sector partners in the execution of infrastructure protection risk assessments that contribute to cross-sector risk assessment and IRM.

B. The **DHS Risk Steering Committee** comprised of Component Heads and their representatives:

1. Serves as the governance structure to ensure collaboration and information-sharing for risk management and analysis across DHS.

2. Develops coordinated recommendations to implement Integrated Risk Management for the Secretary.

3. Utilizes a tiered representative membership and governance structure to accomplish its work.

C. **DHS Component Heads**:

1. Manages the risks that impact the Component's effective operations and mission, including risks to the Nation's security assigned to the Component by law, regulation, or policy.

2. Incorporates functionally appropriate risk management methods and practices, including Department-wide risk management doctrine, as required, into relevant Component business practices, including acquisitions, administration, security, human capital, information technology, budget formulation, and finance.

3. Establishes mission-appropriate risk management capabilities, policies, processes, and practices consistent with applicable laws, regulations, policies, and privileges, and ensures implementation.

4. Participates in a periodic assessment of the Department's risk management capability.

5. Designates a member of the Senior Executive Service, or equivalent, as the lead executive with responsibility for integrating risk management into organizational practices and supporting the Department's IRM policy. The Component lead executive for risk management:

a. Advises Component leadership and communicates to Component personnel about risk management, risk analysis, and decision support matters within the organization.

b. Represents the Component and the Component's positions in the effort to build the Department's IRM policies,

processes, and practices, including participating in the RSC and coordinating with the Director of RMA and other Components' lead executives.

c. Establishes, as appropriate, an internal Component coordination process to promote integration for cross-mission risk management requirements.

6. Provides appropriate representation and participation in the RSC and the RSC working groups.

7. Provides subject matter expertise, tailored data, and information, as requested and appropriate, to RMA and other DHS Components executing cross-Component risk analyses.

8. Provides risk data to RMA in support of a risk knowledge management system unless otherwise barred by law, regulation, or policy.

D. The **Administrator of the Federal Emergency Management Agency**:

1. Incorporates IRM policies, processes, and practices into national preparedness efforts, including the development of training and education for homeland security enterprise partners compatible with DHS IRM policies, processes, and practices.

2. Risk-informs the National Preparedness Goals, National Planning Scenarios, and National Preparedness System, or successors.

3. Coordinates with RMA, the RSC, IP, the NIPP Sector Specific Agencies, and other appropriate stakeholders to develop a common approach to assist State, local, tribal, and territorial government organizations in assessing and managing risks, compatible with DHS integrated risk management and the NIPP.

4. Provides strategic and operational natural hazard analysis and assessments to support the Department's overall risk-informed decision-making requirements.

E. The **Under Secretary of Intelligence and Analysis**:

1. Provides strategic and operational threat analysis and assessments, to include analytic judgments, to support DHS risk assessments and risk-informed decision-making requirements.

2. Serves as the interface to the larger Intelligence Community for all formal support requests related to integrated risk management.

F. The **Under Secretary for Management**:

1. Incorporates functionally appropriate risk management methods and practices, including Department-wide risk management doctrine, as required, into relevant DHS business practices, including acquisitions, administration, security, human capital, information technology, budget formulation, and finance.

2. Works with the Office of the Secretary, the Under Secretary for NPPD, and all Components, to support the efforts to acquire and implement appropriate hardware and software on both unclassified and classified networks for risk management and analysis, recruit and hire a multidisciplinary risk management and learning and development program.

3. The **Chief Financial Officer**:

a. Ensures that DHS programming and budgeting activities use risk analysis to inform resource decisions and justify allocation of resources.

b. Utilizes methodologies developed by RMA and the RSC, where appropriate, to evaluate the extent to which DHS programs and activities manage risk.

G. The **Under Secretary of Science and Technology**:

1. In cooperation with the other heads of DHS Components, and with appropriate representatives from other affected entities, ensures that the identification, prioritization, and funding of homeland security research and development programs and projects is risk-informed.

2. With input from the RSC, conducts research and development efforts to improve the state of knowledge in the risk sciences and application of this knowledge to support homeland security risk management.

H. The **Assistant Secretary for Intergovernmental Affairs**, in conjunction with RMA and the RSC, facilitates consultation with homeland

security enterprise partners in the development and implementation of IRM policies, processes, and practices.

I. The **Assistant Secretary for Policy**:

1. Ensures that DHS policy, strategy, and regulations are risk-informed.

2. Ensures that the strategic development process and strategic requirements planning process are risk-informed and, in coordination with RMA and the RSC, develops clear guidance on how to do so.

J. The **Assistant Secretary for Public Affairs**, in conjunction with RMA and the RSC, develops the Department's strategy for risk communications with external stakeholders and the public.

V. Policy and Requirements

A. DHS uses IRM to inform strategies, processes, and decisions to enhance security and to work in a unified manner to mange risks to the Nation's homeland security.

B. Homeland Security is about effectively managing risks to the Nation's security, including from acts of terrorism, natural and manmade disasters, cyber attacks, and transnational crime. The Department's IRM is based on the premise that security partners working together can most effectively manage risk, which is important since DHS plays a leadership role in the Nation's unified effort to manage risks across the homeland security enterprise, including Federal, state, local, tribal, territorial, nongovernmental, and private sector partners.

C. It is the policy of DHS to:

1. Incorporate the risk management process into the overall mission and management of the Department. The Department uses a risk management process that includes:

a. Determining the context, goals, objectives, stakeholders, and the policy, legal, and practical constraints under which the organization and decision maker are operating;

b. Identifying potential risks within the context;

c. Assessing and analyzing the identified risks;

d. Developing and analyzing alternative strategies to manage risks, considering the projected costs, benefits, and ramifications of each alternative to manage or mitigate the risk;

e. Deciding and implementing the risk management strategies giving consideration to all relevant factors; and

f. Monitoring and evaluating performance of the risk management strategies.

Communication is critical to this process and occurs within and throughout the steps of the cycle.

2. Use risk information and analysis to inform decision-making, striving to better understand risks and capabilities to manage those risks and capabilities, while remaining flexible to changing risks. Homeland security risks are inherently uncertain, and risk analysis will not always yield precise answers. The Department uses risk information and analysis to make its assumptions more transparent, encourage creative thinking, and provide defensible decisions, made with the best available tools and information, for the best achievable outcomes.

3. Develop methodologies, where appropriate to determine the extent to which its programs and activities manage and reduce risk to the Nation. DHS uses this information, among other inputs, to measure the Department's progress toward achieving strategic goals, inform decision-making, build its budget, help guide the allocation of limited resources, and promote understanding and collaboration among homeland security enterprise partners.

4. Use a unified approach to manage risks working with all of our homeland security enterprise partners.

VI. Questions

Address questions or concerns regarding this Directive to the Director of RMA at risk_management@hq.dhs.gov.

Rafael Borras
Under Secretary for Management

3-28-2011
Date