



Security Analysis and Risk Management Association

JOIN SARMA

CONTACT SARMA

[Printer Friendly](#)

## The Risk Communicator: October-November 2008 Edition

Welcome to The Risk Communicator, SARMA's newsletter for information, trends and issues of concern to security analysis and risk management professionals. This complimentary news service is distributed every other month. Please feel free to share this e-mail with your colleagues and encourage them to sign up to get their own copy [here](#).



If your server is blocking HTML e-mails, you can view the current Risk Communicator by pasting the following address into your browser:

<http://sarma.org/news/theriskcommunicato2/>

## Officers' Corner

### Some Thoughts on Risk Management Policy During the Presidential Transition and Beyond

With the nation's economy in the midst of an historic downturn, and Washington preparing to welcome a new administration to power, I believe it is more important than ever to maintain the focus on enhancing our nation's ability to apply consistent, measurable risk management principles to its security investments. Fortunately, others seem to agree.



Kerry Thomas,  
President

As many of you know, the Homeland Security Advisory Council (HSAC) recently released a short report on the "Top Ten Challenges Facing the Next Secretary of Homeland Security" -- and risk management made the cut. In addition to acknowledging the importance of "building a risk-based foundation for security that lasts into the next decade," it also recognized that DHS is in a unique position to lead this effort.

To that end, the HSAC report makes several important recommendations. First, the report calls for "establishing and improving performance metrics for measuring risk and building a framework for risk-informed decision-making." In addition, the HSAC recommends that DHS "make an effort to consolidate the different, existing risk management programs across its many components and agencies, to ensure that the DHS risk methodology is consistent within the Department, and consistent when presented to the Department's many partners." SARMA has long advocated similar goals, and I'm pleased to see them echoed

### Contents

- [Officers' Corner](#)
- [News](#)
- [Key Reports and Reviews](#)
- [Conferences and Training](#)
- [Job Board](#)
- [Miscellaneous](#)

### Subscriptions

[Subscribe](#)  
[Unsubscribe](#)

to the Risk Communicator

### Contact SARMA

#### SARMA

P.O. Box 710172  
Herndon, VA 20171  
Phone: (703) 635-7906  
Fax: (703) 635-7935  
E-mail: [info@sarma.org](mailto:info@sarma.org)

### Get Involved in SARMA

Get involved with SARMA today.

[SARMA website](#)  
[SARMAPedia](#)  
[Volunteer To Serve](#)  
[Feedback / Input Form](#)  
[Join SARMA](#)

in the HSAC report.

I also believe the time is right to go even further. Though the wisdom of applying risk management concepts to guide decision-making on security has been widely endorsed, a coordinated national approach remains elusive. The change in administration offers a unique opportunity to alter this paradigm. To this end, SARMA has offered to members of the Obama transition team several recommendations on the creation of a national risk management program. These recommendations, highlighted later in this issue of The Risk Communicator, were developed by a team of SARMA volunteers with broad experience in government, academia and industry.

Given the confluence of global security challenges and fiscal realities we now face, I am hopeful that the sound recommendations of bodies like the HSAC and SARMA will resonate.

Best wishes for a safe and joyful holiday season!

Kerry Thomas  
President

## SARMA Down Under

As part of SARMA's initiative to incorporate even greater perspectives and experience in security risk management (SRM), I recently traveled to Perth, Australia to attend the 5th annual conference of the Risk Management Institution of Australasia (RMIA). I'm pleased to report that it was a most productive and thought-provoking trip.



Ed Jopeck,  
Immediate  
Past President

While RMIA's focus is on risk management in general, rather than SARMA's more limited focus on security, there were some truly superb presentations on the role of risk management in dealing with economic, social and environmental problems. One notable highlight was a presentation from Nicholas Davis and Gareth Shepherd of the World Economic Forum on "Global Risks 2008 -- Where are the Risks and Opportunities?" The two gave a candid and timely assessment of the implications of the global financial meltdown and the role of risk management in both the crisis and the coming clean-up.

In addition to attending the conference, my secondary objective was to continue discussions begun with the memorandum of agreement between RMIA and SARMA. That agreement, members may recall, established reciprocal member benefits and provided guidelines under which the two associations will collaborate on future projects. To that end, I had several engaging and informative discussions with RMIA members -- sharing and comparing our organizations' projects, interests and perspectives on SRM, risk management standards and other risk practice areas. Across the board, the RMIA leadership and members were very welcoming of me, interested in SARMA and interested in their American counterparts in the risk management profession.

One of my personal research interests was to compare the Australian and American approaches to risk management and, in particular, security risk management. I learned that, in spite of having developed separately and in largely different directions, we have much in common with Australian practitioners in trying to implement SRM. I was also surprised by how similar the concerns of

### Sponsor Notices

SARMA thanks the following organizations for their support:



### Links of Interest

[Risk Management Institution of Australasia \(RMIA\)](#)

[SARMA on LinkedIn](#)

### The Risk Communicator

*The Risk Communicator*, newsletter of SARMA, the Security Analysis and Risk Management Association

Send questions and comments to  
Editor-in-Chief  
newsletter@sarma.org

Copyright 2008.  
SARMA All rights reserved.

### [PRIVACY POLICY](#)

The views expressed in the Risk Communicator reflect the views of their authors, and do not necessarily reflect the views of SARMA, the US Government, or the employers or clients of the contributors.

insurance and business risk managers are to those of security risk managers. These experts and practitioners also voiced concerns over the often-overlooked importance of the "soft skills of risk management": communicating with leadership effectively and selecting the right qualitative and quantitative risk methods in practicing successful risk management. Interestingly, I found our Australian counterparts far less interested in developing sophisticated security analysis methodologies to quantify security risks in data-poor situations.

I was also intent on learning about the Australian development of, and reliance upon, risk management standards. The Australian approach differs significantly from our own, and much of our discussion centered on Australia's enthusiasm for the looming completion of the ISO 31000 international standard on risk management. I was keen to explore the utility and possible impact of the publication of ISO 31000 on the US SRM community. Can we use it? Will it fit our needs? Will it add credibility to our efforts and, if so, should we adopt it? (My analysis on the answers to those questions will be the subject of a future article.) I was fortunate enough to be introduced to Kevin Knight, Convenor of the ISO Working Group on Risk Management, RMIA resident expert and all-around wise man on international standards development and risk management, and thanks to his generous support, SARMA is likely to soon become involved in future international standards development activities for risk management.

In spite of nearly 60 hours spent in airplanes and airports to attend this all-too-short conference Down Under, I return energized and full of ideas to explore and write about for the benefit of SARMA's membership. These, I hope, will generate additional information sharing and thoughtful discussions about the future of SRM in the United States. As SARMA continues to evolve from its early focus as an American security risk organization to one that is both internationally involved and more open to interaction with other (foreign and non-security) risk practice areas, I hope that the membership will join me in these intellectually stimulating diplomatic and exploratory missions. Until then, I bid you a hearty, "G'day, Mate".

Ed Jopeck  
Immediate Past President

[Return to the top](#)

## News

### SARMA Members Respond to the NIPP

The comment period for the draft 2009 National Infrastructure Protection Plan (NIPP) closed on 1 December, with a variety of SARMA members and officers offering opinions for consideration by DHS staff in advance of the deadline.

The NIPP is a triennial report required under Homeland Security Presidential Directive 7. Given its importance as a "cornerstone" document within DHS and the broader homeland security community, SARMA urged community members to make full use of this opportunity to help shape the goals and objectives spelled out in the Plan.



The most recent 17-day comment period was the second and final such opportunity before the 2009 NIPP undergoes a senior-level internal DHS review towards the end of the year. A prior comment period earlier this year generated very little external feedback, according to DHS officials.

[\[View the Draft NIPP\]](#)

## SARMA Offers Policy Recommendations to the Incoming Administration

Anticipating that the Obama administration will undertake a major review of homeland security policy, SARMA has offered a series of recommendations to individuals advising the incoming team. The document describes a number of significant challenges well known to SARMA's membership, and argues that presidential leadership is required if the plethora of current risk management policies across the executive branch are to be reconciled.



SARMA has made the following recommendations:

1. Issue a Presidential directive to create a National Security Risk Management Program. The directive would establish a national program for security risk management and provide central coordination over all efforts to implement supporting policies, programs and practices across the interagency community.
2. Require federal departments and agencies to create a Chief Security Risk Officer (CSRO) function, positioned and empowered to synchronize, coordinate and monitor all security risk management efforts within their organizations
3. Direct the DHS CSRO to harmonize homeland security risk management policies and programs to ensure consistency, compatibility and integration, not only within DHS but with state and local governments and private industry.
4. Create a security risk management governance structure to span the interagency community and bring standardization and rigor to the assessment of security risks.

[\[View SARMA's Recommendations\]](#)

## DHS Releases Risk Lexicon

In what SARMA officials described as "an important step forward for DHS," the agency's Risk Steering Committee has released an official DHS Risk Lexicon, dated September 2008. Containing definitions of 73 terms and concepts critical to the practice of homeland security risk management, the Lexicon is intended "to build a common vocabulary and language within the Department and enhance the ability of the DHS risk community to utilize risk information and assessments to set priorities for reducing the risks facing the Nation."



Part of the department's ongoing effort to build an Integrated Risk Management Framework, the Lexicon mirrors prospective efforts by the White House to issue a Presidential Directive requiring such a common vocabulary -- and complements

SARMA's ongoing initiatives in this area through its Common Knowledge Base program and other consensus-building activities. The authors of the DHS Lexicon also acknowledge that this will be a "dynamic document" with room left for changes and additions, and provide information on how such modifications might be made:

New terms may be submitted through a Component's RSC Tier-III/RLWG representative or through the DHS Lexicon Section. Proposed additional terms submitted to DHS ESEC will be forwarded to the RLWG. The RLWG coordinates the addition of terms into the DHS Risk Lexicon on the submitter's behalf, although the submitter is welcome to participate as appropriate in the process. Submitters can send single terms or lists of terms to [Lexicon@dhs.gov](mailto:Lexicon@dhs.gov) with a copy (cc) to [RMAexecsec@hq.dhs.gov](mailto:RMAexecsec@hq.dhs.gov), or submit terms through their Component's RSC Tier-III representative.

The document also lays out how the Lexicon will be institutionalized throughout DHS by incorporating it into all documents, and expresses DHS's desire to "socializ[e] the existence of the DHS Risk Lexicon with the current community of risk practitioners and [support] them as they adopt its definitions for use within their Components."

SARMA officials said they looked forward to working with DHS on the important process of standardizing security risk analysis and risk management practices for the profession. "It's an important piece of the lexicon solution that will be incorporated immediately into the SARMA Common Knowledge Base, thereby helping to advance a vocabulary that will ultimately be representative of the entire profession," said SARMA President Kerry Thomas.

[\[View the Lexicon\]](#)

## Join SARMA on LinkedIn

Have you ever wished you could network more effectively with other SRM professionals? Ever wanted to ask a question, discuss an issue of interest or share a good article with other security analysis and risk management professionals?



Now you can. And thanks to the marvel of social networking, doing all this from the comfort of your own computer screen is easier than ever.

SARMA has created a group accessible to anyone with a LinkedIn account and approval from the group manager. Why not check it out today and sign up? Join a group that is informative, professionally beneficial and fun!

To create an account, go [here](#). If you already have an account, you can go directly to the SARMA group [here](#).

See you online!

[Return to the top](#)

## ***Key Reports and Reviews***

The Financial Impact of Cyber Risk: 50 Questions Every CFO

## Should Ask

This report from the American National Standards Institute and the Internet Security Alliance points out that there has "not been any agreed upon methodology for understanding and mitigating the potential financial losses associated with network security and cyber risk." Appendices provide models on the probability of financial loss based on mitigating action; the frequency of financial loss for certain risk events; and the severity of financial loss for certain risk events.



[\[Get the Report\]](#)

## Top Ten Challenges Facing the Next Secretary of Homeland Security

"In an effort to assist with the first Presidential administration transition of the Department of Homeland Security, the Homeland Security Advisory Council has identified ten key challenges that will face the next Secretary of Homeland Security."



[\[Get the Report\]](#)

## Intelligence Community Directive Number 503: Information Technology Systems Security Risk Management, Certification and Accreditation

This Directive, which rescinds and replaces the Director of Central Intelligence Directive 6/3 Policy, Protecting Sensitive Compartmented Information within Information Systems, instructs the intelligence community to "consider risk management an essential management function, and ... ensure that it is tightly woven into the system development life cycle."



[\[Get the Report\]](#)

## Homeland Security 2015: Workshop Proceedings

In October 2006, representatives of DHS, the Canadian Office of Public Safety and academics from both the United States and Canada, met to brainstorm about the likely state of homeland security in 2015. Earlier this year, the group released a



belated report on the proceedings. SARMA members may be particularly interested in the section titled "Risks -- Key Findings."



[\[Get the Report\]](#)

## Defense Imperatives for the New Administration

Prepared by the Defense Science Board, this report describes a host of critical defense and homeland security challenges to be faced by the next Secretary of Defense (who, as this issue goes to press, appears to be the current SecDef: Robert Gates). Among the report's recommendations is the need for an "intelligence collection architecture... that harmonizes foreign and domestic intelligence, and all the means we have available for learning the capabilities, intentions, identities, and locations of terrorists and their supporters."



[\[Get the Report\]](#)

## Department of Defense OPSEC Manual

On 3 November 2008, the US Department of Defense issued the DoD Operations Security (OPSEC) Program Manual, Number 5205.02-M. The 38-page document emphasizes the importance of threat analysis, vulnerability analysis and risk assessment in developing proper countermeasures in maintaining operational security: "Determining the level of risk is a key element of the OPSEC process and provides justification for the use of countermeasures."



[\[Get the Report\]](#)

## Remarks by Homeland Security Secretary Michael Chertoff on Risk Management

In recent remarks to the Wharton School at the University of Pennsylvania, Secretary of Homeland Security Michael Chertoff reflects on "the larger context of managing risk which I think is the first objective I saw when I got sworn in almost four years ago and remains, I think, the fundamental social problem that we face in the 21st century."



Wharton's  
Huntsman Hall

[\[Get the Transcript\]](#)

[Return to the top](#)

## Conferences and Training

### Call for Speakers and Sponsors: 3rd National Conference

SARMA is seeking speaker proposals and expressions of interest from organizations wishing to sponsor our next National Conference. The 2009 National Conference on Security Analysis and Risk Management is the only national conference organized by security risk analysts and managers for their peers in government, industry and academia.



SARMA's 2008 National Conference

The conference will be held in June 2009 in the Washington DC metro area (final dates and location to be announced shortly).

Please email the SARMA Conference Committee at [conference@sarma.org](mailto:conference@sarma.org) for additional information and submission requirements.

[\[View the 2008 Conference Program, Speaker Presentations and Photos\]](#)

[Return to the top](#)

## Job Board

### Management and Program Analyst (Risk Analyst)

National Protection and Programs Directorate

Vacancy Ann.#: DHSHQRA08-5147

Who May Apply: Public

Pay Plan: GS-0343-13/15

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 7/18/2008

Closing Date: 12/31/2008

Salary: From 82,961.00 to 149,000.00 USD per year [\[View the Announcement\]](#)

### Management and Program Analyst (Strategic Risk Specialist)

National Protection and Programs Directorate

Vacancy Ann.#: DHSHQRA08-5146

Who May Apply: Public

Pay Plan: GS-0343-11/13

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 7/18/2008

Closing Date: 12/31/2008

Salary: From 58,206.00 to 107,854.00 USD per year [\[View the Announcement\]](#)

### Management and Program Analyst (Risk Analyst)

National Protection and Programs Directorate

Vacancy Ann.#: DHSHQRA08-5175

Who May Apply: Public

Pay Plan: GS-0343-9/11

Appointment Term: Permanent  
Job Status: Full-Time  
Opening Date: 7/28/2008  
Closing Date: 12/31/2008  
Salary: From 48,108.00 to 75,669.00 USD per year [[View the Announcement](#)]

### Management and Program Analyst (Risk Analyst)

National Protection and Programs Directorate  
Vacancy Ann.#: DSHQRA09-6009  
Who May Apply: Public  
Pay Plan: GS-0343-11/13  
Appointment Term: Permanent  
Job Status: Full-Time  
Opening Date: 10/16/2008  
Closing Date: 12/31/2008  
Salary: From 58,206.00 to 107,854.00 USD per year [[View the Announcement](#)]

[Return to the top](#)

## Miscellaneous

### Want to Contribute to The Risk Communicator?

Do you know of an item you would like to see included in The Risk Communicator? Do you have ideas for new and interesting features for future editions? If so, please contact the newsletter staff at [newsletter@sarma.org](mailto:newsletter@sarma.org).



[Return to the top](#)