

**Better Integrating Risk Analysis Into
Critical Infrastructure Security Policies and Programs**
Military Operations Research Society (MORS) Special Meeting
Homeland Security Studies and Analysis Institute (HSSAI)
November 16, 2010
(As prepared for delivery)

Good morning—and thank you for that kind introduction. I am grateful to be here with you this morning, and I know that we will learn a lot from one another today.

When the conference planners informed me that the purpose of today’s meeting is to examine the status of methods for assessing risk and allocating risk-reduction resources and to identify new or improved processes for optimizing investments in infrastructure protection, I was eager to participate, as this is an ideal forum to discuss some exciting and relevant developments at the Department of Homeland Security’s Office of Infrastructure Protection (IP). Today’s discussion and resulting recommendations will enhance our progress.

Today, I will discuss the necessity of developing metrics for assessing the efficacy of risk-mitigation efforts to critical infrastructure, and the importance of using those metrics to inform resource allocation and planning. In my view, there is no other defensible planning paradigm for critical infrastructure security. Many of the challenges that we currently face are grounded in a lack of a common understanding of what critical infrastructure is, and the need to implement more programs that mitigate risks to a specific universe of assets and systems. My remarks this morning will highlight the importance of a few things:

- Defining the universe of critical infrastructure;
- Assessing risk to that infrastructure;
- Measuring risk reduction;
- Identifying gaps and adjusting resourcing priorities accordingly, through robust partnerships among relevant partners.

Following that discussion, I will describe how DHS and the Office of Infrastructure Protection are incorporating a risk-based approach into their critical infrastructure security activities.

The Definition of Critical Infrastructure

As I mentioned, many of the current challenges that we face in critical infrastructure protection are grounded in a lack of common understanding of what critical infrastructure is. The generally accepted definition of “critical infrastructure” was established in 2001 by the PATRIOT Act. It describes “critical infrastructure” as “systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” This definition provides a necessary amount of flexibility;

however, when it comes to clearly and tangibly defining the universe of critical infrastructure so that we can allocate resources effectively, additional guidance is required.

Importantly, in the Implementing Recommendations of the 9/11 Commission Act of 2007, Congress required the Department of Homeland Security to develop and maintain a “prioritized critical infrastructure list” that would have specific, Department-developed criteria to determine what was on the list, and what was not. This list is significant because it provides the Executive Branch with necessary direction on defining a specific scope of critical infrastructure on which to focus planning efforts.

To reiterate, planning efforts for critical infrastructure security cannot take shape without having a clearly defined universe of assets and systems. Such a universe ensures that stakeholders across the critical infrastructure security community understand what is to be included and what is *not* to be included. This, of course, is easier said than done, but I think that a common, shared understanding of what we mean when we say “critical infrastructure”—especially from a national perspective—is a prerequisite for effective risk-based planning. The “Prioritized Critical Infrastructure List” that I just described helps to give us this shared understanding.

With this list and a defined universe of critical infrastructure at our fingertips, it is important that we utilize (1) sound risk assessment methodologies; (2) assess risk mitigation outcomes; (3) conduct gap analyses; and (4) incorporate long-term planning processes into our critical infrastructure protection efforts.

(1) *Risk Assessment*

First, I will discuss the importance of risk assessment. We cannot effectively know whether we are *securing* critical infrastructure unless we have an agreed-upon understanding of the *risks* to that infrastructure. It is essential that the Department, its Federal partners, state and local governments, and the private sector have a common understanding of the security risks so that there is a clear direction for what needs to be addressed. Once that understanding is achieved, we can assess how well we have done at mitigating those risks. We often talk about the *need for* risk-based planning, but we do not always define what those risks are. We cannot defensibly allocate risk-reduction resources until we know what risks we are attempting to mitigate. As such, the Office of Infrastructure Protection is working to develop a shared understanding of risk among its critical infrastructure partners.

(2) *Measuring Risk Mitigation*

The second component of effective infrastructure protection that I mentioned is measurement. Once there is a clear understanding of what “critical infrastructure” is, and a set of defined risks to that critical infrastructure, policymakers need to determine how effective programs are at reducing risks to critical infrastructure. They can make this determination based on outcome-based metrics that (1) measure whether risks to critical infrastructure are being mitigated by specific programs; (2) align with national strategies; and

(3) assess whether programs are leading to the desired outcomes. Such metrics will enable policymakers to understand the efficacy of programs and the security risks facing critical infrastructure, identify gaps and redirect resources; encourage the implementation of protective measures; and provide a transparent assessment to taxpayers. Without these metrics, policymakers will be in a vicious cycle of never accurately understanding whether risks have been acceptably managed.

(3) Identifying Gaps

An effective planning, programming, budgeting, and reporting cycle requires a continuous reexamination of risk and tolerable thresholds of risk as well as the commensurate allocation of resources. Thus, once the reduction of risk to critical infrastructure is measured, it is essential that these results inform resource allocation decisions. Intolerable gaps in risk reduction must be identified and mitigated through the infusion of resources and the modification of programs.

(4) Long-Term Planning

A cyclical approach such as this will lead to two positive developments. First, it will spur discussion among relevant stakeholders about how to narrow or eliminate the gaps identified through the assessment. Second, this important cycle that brings together risk assessment, a predetermined class of critical infrastructure, and outcome-based metrics will keep the essential public-private partnership aligned and leaning forward. As you know, the Nation's approach to critical infrastructure security is based upon partnerships among all levels of government and between the government and the private sector. A cyclical approach to planning, programming, reporting, and budgeting will keep all of these players on the pulse of developments, and will encourage them to remain committed to the partnership. It is only when this cycle is absent that there is room for confusion. In short, the approach I have outlined is part of a multi-purpose, long-term planning effort that upholds the importance of the partnership approach to critical infrastructure security.

Efforts at the Office of Infrastructure Protection

It is imperative that we develop metrics to assess the efficacy of our risk mitigation efforts, and that we link those metrics to resource allocation and planning activities. In order to do this, we, at the DHS Office of Infrastructure Protection, must clearly define what we mean when we say "critical infrastructure;" effectively assess risk to that infrastructure; and mitigate those risks through proper planning. There are several efforts taking place at the Office of Infrastructure Protection that will get us to where we need to be, and I would like to highlight just a few.

Last month, IP established an office-wide Task Force to improve the alignment of our risk profile with our planning processes. The Task Force is developing an exhaustive list of critical infrastructure that will be used for planning purposes. It will be based upon the Prioritized Critical Infrastructure List as well as other lists developed by IP and its partners. It is important

to note that the critical infrastructure assets on these lists are *not* the only ones about which we care, but they will serve as a baseline for what we know we must plan to secure.

Concurrently, the Task Force is helping to guide the development of a comprehensive risk assessment for this set of infrastructure. This assessment will identify (1) the highest relative risks to critical infrastructure among a number of natural and manmade hazards, and (2) those critical infrastructure sectors that are at a higher risk from the greatest number of hazards.

Through the intersection of the definable universe of critical infrastructure and the risk profile that I just described, IP and its partners will develop a three-year plan to mitigate security risks to these assets and systems. This plan will serve as an implementation plan for the strategic framework provided by the National Infrastructure Protection Plan, and will focus on mitigating or eliminating security gaps that are identified through the annual audit of DHS' ability to mitigate risk to critical infrastructure. It will outline a clear path for where the critical infrastructure security community intends to be over a period of three years. This will keep the partnership moving forward, together.

Importantly, the Office of Infrastructure Protection will also assess, on an annual basis, how well we are following our plan. We will keep close track of whether or not we have met the agreed-upon benchmarks, and if it is determined that we have not, we will adjust accordingly. The annual assessment will directly feed into our resource-allocation process, and will be used to determine (1) the effectiveness of programs; (2) whether more resources may be necessary; and (3) from where they can be diverted. If the annual report highlights that IP and sector programs do not mitigate risks to critical infrastructure, our resource planning for the following year will be adjusted accordingly.

This process puts DHS and IP on the path to implementing a truly risk-based resource allocation process for critical infrastructure security. By working in partnership with the private sector and our intergovernmental partners, the Office of Infrastructure Protection will be able to acquire a common understanding of the assets and systems that we are responsible for protecting. We will also be on the same page with our partners about what the greatest risks to those assets are; how we plan to mitigate those risks; and how effective we are at reducing risk. Importantly, this partnership-wide effort will directly inform our annual resource allocation process.

Conclusion

I am certainly aware that this will likely not be done as neatly as I have described it. We will undoubtedly face challenges along the way. However, with a well-coordinated, risk-based approach, we will be more prepared to answer the question of how well we are doing—as Nation—at mitigating risk to critical infrastructure. As you discuss methods for reducing risk and optimizing resource allocation in your working group sessions, I hope that you will think about challenges that the Office may face and approaches we should take to confronting them. In addition, I would like to hear your thoughts on how to best measure the reduction of risk to our

most critical assets and systems. I hope that what I have discussed today will stimulate a thoughtful discussion about how best to integrate risk analysis into critical infrastructure security policies and programs. A continued dialogue among us is imperative.

The framework that I have described today demonstrates a renewed focus for the Office of Infrastructure Protection on ensuring that policy, programming, and resourcing decisions are risk-based and transparent to American taxpayers. At the Department and at IP, we are committed to working with our partners to understand where it is that we need to go together, and determining how best to get there. With that said, I look forward to hearing your feedback and responding to your questions so that we might be better able to fulfill our important mission of securing the Nation's most critical infrastructure.

Thank you, and I look forward to your questions, comments, and ideas.