

MEMORANDUM FOR THE RECORD

Event: Meeting with Assistant Secretary Robert Liscouski Department of Homeland Security

Type of event: Briefing

Date: Jan. 20, 2004

Special Access Issues: NA

Prepared by: Emily Walker

Team Number: 8

Location: Department of Homeland Security Nebraska Ave. Washington DC

Participants - Non-Commission: Robert Liscouski, Assistant Secretary DHS, Grace something
DHS lawyer

Participants - Commission: Emily Walker and Mark Bittinger

The purpose of this meeting with Asst. Secretary, DHS Infrastructure Protection, was to clarify information Asst. Sec Liscouski provided at the DHS Conference on Jan. 13-14 in Washington, D.C. , share ideas, explain what Emily's work has been on private sector preparedness and the on-going effort to identify recommendations for the Commission on this topic. Unfortunately, Mr. Liscouski was not available to attend or speak at the Nov. conference. It appears there was some communication issues on this topic prior to the hearing including the POC John Mitnick.

Emily began the meeting by describing the work she has done interviewing the private sector companies present on 9-11 in NYC, the issues that arose in those discussions, the movement toward the hearing in Nov. at Drew University, the conclusion of the hearing, the panel being put forward by American National Standards Institute to develop recommendations for the Commission on Emergency Preparedness and COB for the Private Sector. She expressed a willingness to work with DHS in this effort, a desire to be up-to-date with DHS activities in this area and an overall goal to ensure that the Commission's recommendations supported the effort of DHS to work with the private sector in the area of homeland security.

Mr. Liscouski said that his directorate is to prioritize efforts in a way to implement positive change. He said that he believes Security is value-added. The goal of his directorate is to preserve US National Security by protecting critical infrastructure and ensuring that the

COMMISSION SENSITIVE

Government can be restored in case of an event. They start with the worse case scenarios and work toward being protected for them. Protection is also quick recovery. If a target can quickly recover if it is hit, this can shift the focus off the target. They have identified processes that also need to be protected (as well as buildings) such as the check clearing or other financial processes.

He discussed work with ASIS to develop a Threat Advisory System Response Guideline which is applicable to private sector environments which must evaluate and possibly respond to changes in the DHS/HSAS Threat Level Matrix. This matrix provides private business and industry a tool to prompt consideration of possible actions that could be implemented based upon elevated Alert Levels announced by DHS. The guideline is intended to be used as a recommended baseline to drive ultimate threat responses.

In addition to this guideline, Asst. Sec Liscouski would like to see specific guidelines or standards, possibly implemented through insurance or corporate governance methods, which describes best practices and specific tactical responses by industry.

He believes that a risk management approach is the business case that can be supported and through the interchange in this meeting decided to change the wording on his plan from "threats" to "risks". He has looked at all facets of equation and finds that the most simple one is the answer. He believes that the risk management approach toward security should align security with the profit responsibility person who would work with Emergency Action Committees and Incident Management teams. He commented that Reputation, image and trademarks are things that can be lost in a security situation.

He commented that there is a governance component where security issues should report to the Board. He believes that building a culture of security and CEO leadership. He mentioned that this culture can exist in good times, but in hard times, this erodes and over-time there is disaffection. He believes that whatever companies do, it must be effective to be sustainable. It must be culturally driven, systemic and consistent over time. He believes that basic safety services, business continuity and disaster recovery which are not usually under security should be linked and incorporated into the corporate governance.

He spoke about the five fundamental tenants of private-public sector partnership for critical infrastructure protection. Threats – what are they and what information do you require from the government to understand threats. Critical assets – what are they, where are they located and what methodology does the Government use to rank those assets? Vulnerabilities: What are the common and unique vulnerabilities of your critical assets? What are the interdependencies across the industry and supply chain? Programs – what programs are in place to protect your critical assets? How can the Govt help fill in gaps? Metrics- how is the effectiveness of your program measured and fed back? What metrics does the Govt use?

We discussed these tenants. Emily made the point that she believes the best business case in terms of receiving private sector preparedness is in terms of risk management for all hazards, not just terrorism. In fact, many of the plans tenants can be used for any kind of emergency and most events require some usage of the same tenants. She suggested that the term “threats” be changed to “risks” and that the critical assets be more than physical assets but brand etc. Asst. Sec Liscouski agreed, particularly given his background working at Coke.

Asst Sec Liscouski shared a chart on “Tactical and Strategic Executive vs Time Vs Threat Level”. This chart showed that as the threat level varied, there was a current state of capability that showed a gap relative to the desired state which was above the current state. The goal is to over time, move so that the capability gap is lowered as the G8 meet, the Olympics occur, the US Political Conventions happen leading up to reaching the desired state by the elections of '04. He said that the cost of this tactically is reduced over time and the strategic cost is increased as the immediate measures' costs are spread out over time.

Emily shared ideas with Mr. Liscouski on changing the name and/or model of the ICD directorate under J. Caverly to be more in line with a customer service model that Citibank used called relationship management. She recommended that he make the structure more user friendly and suggested that if companies had one liaison in DHS who understood their industry and could relate to the other parts of DHS, it would be easier for companies to respond.

COMMISSION SENSITIVE

She also recommended that increasing public awareness through a DHS seal of approval on preparedness, some kind of award, a kick-off day on Sept. 11 for Emergency Preparedness Week (Similar to fire prevention week) etc would go a long way of building public awareness to this issue and hopefully having an effect on companies. She acknowledged that the National Standards that she is considering are really a "framework", and not the specific standards the Asst. Sec. Liscouski is looking for to prepare each individual sector. He agreed that this framework was useful and understood the desire to build public awareness on this issue.

Mr. Liscouski said that he felt that the meeting was valuable. I hope so because we took a great deal of his time.

Background:

Infrastructure Protection (IP) Overview, Nov. 13, 2003 Powerpoint

2004 Private Sector Conference: ASIP Liscouski Slides no date

Powerpoint Slide Tactical and Strategic Execution vs Time vs. Threat Level from DHS

Draft 4 Threat Advisory System Reponse (TASR) Guideline by ASIS and DHS no date