

The Integration of the ISACs into Government and Department of Defense Homeland Security and Homeland Defense Exercises

ISAC Council
White Paper
January 31, 2004

1. INTRODUCTION AND BACKGROUND.

The federal Government has conducted two major Homeland Security Exercises – “Topoff I” and “Topoff II.” Topoff I was conducted under the auspices of the Department of Justice. These exercises were conducted in Seattle and Chicago. Topoff II and subsequent exercises was/will be conducted under the auspices of the Department of Homeland Security (DHS). The Department of Defense will presently conduct a Homeland Defense exercise titled “Determined Promise ’03 and Amalgam Chief 03-13”. This robust command post and field exercise is the precursor/requirement for Northern Command’s (NORTHCOM) approval for “Full Operational Capability (FOC)” status.

There has been little to no integration of active private industry/infrastructure into these exercises. In Topoff II, private industry participation in the scenario was “simulated.” There has been no ISAC involvement in these national level exercises.

The Secret Service Electronics Crime Unit (ECU) is reaching out to the private sector and supporting table-top exercises to address the security of private infrastructures. The upcoming “Live Wire” exercise, sponsored by Dartmouth College, is taking steps to integrate the private sector into this cyber exercise effort.

TSA in coordination with the U.S. Navy War College is also beginning the planning for a series of exercises.

2. DISCUSSION.

The ISACs and private infrastructure must become fully integrated into these exercises. Based on the axiom that “you train as you fight,” private industry must become a critical element of training to protect the nation. Exercising is a major element of both homeland security and homeland defense training.

ISACs can exercise, mature, and demonstrate their capabilities through exercise participation.

The following provides specific recommendations for private industry/ISAC exercise participation.

A. Private industry/exercise participation must begin with the initial scenario development. Some of the recent scenarios developed by the government have not been valid and this can be directly attributed to the lack of private industry participation.

B. Private industry must establish and integrate their individual industry security objectives/goals into the exercise. Both national and private sector goals can be established during the creation of the exercise and then addressed during the exercise play. For example exercising the ISAC capabilities is an extremely worthwhile objective. The national and private sector requirement for information sharing, outreach, and partnership is addressed by integrating the ISACs. The involvement of sector organizations, such as the ISACs, will support the inclusion of the sectors that may want to participate in the exercise.

C. Once the scenario and objectives/goals are established the master events sequence list (MESL) must reflect the focused private industry participation.

D. Specific participation in the exercise must be conducted. This participation is both at the working level and at the leadership level of industry.

E. Full integration and participation with the Government and Military leadership during the conduct of the exercise must be accomplished by industry/ISAC leaders/ reps.

F. During the “hotwash” and final review, private industry must provide comments and critique both their processes and the federal government processes. Recommendations must be provided to the “go forward plan” that addresses the maturing of homeland security/defense and the ongoing exercise effort.

G. Private industry/ISAC efforts must continue and become more fully integrated as the cycle/series of exercises develop and continue. Many private sector organizations are developing crisis management plans and these processes will mature through exercise participation.

3. **RECOMMENDATIONS.** That the ISAC Council:

A. adopt this issue as one of the common issues for the individual ISACs and work with the individual ISACs as they pursue direct involvement.

B. present this issue to DHS, DOD, and other federal agencies at the soonest opportunity and offer to serve as a liaison with interested ISACs.

C. request that DHS vet the numerous exercises being planned/proposed for ISAC participation and provide a central clearing house for ISAC exercise participation.

D. work with member ISACs and the government to establish funding requirements for private sector exercise participation.

E. request a calendar of projected exercises and specific points of contact within the Government to begin these processes.

Information Sharing and Analysis Centers, or ISACS, are private sector operational organizations which today are collecting, distributing, analyzing and sharing sensitive information regarding threats, vulnerabilities, alerts and best practices in order to protect our national critical infrastructures.

Eleven ISACs -- Chemical, Electricity, Energy, Financial Services, Healthcare, Information Technology, Public Transit, Surface Transportation, Telecommunications, Truck, and Water -- have joined together as an ISAC Council, partnering with their sectors, with one another, and with government to advance the physical and cyber security of the critical infrastructures of North America.

Please note that this paper was written by the ISAC Council as a consensus document, with input and review by member ISACs. However, its views and findings do not necessarily represent the official position of each ISAC. For more information on the ISAC Council and the ISACs which form its membership, please visit www.isaccouncil.org.