Exercises and the Public - Private Partnership

By James Creel

The partnership between the public and private sectors is vital in encouraging participation in cross-sector initiatives. Initiatives such as tabletop exercises and workshops help ensure resiliency across all sectors by measuring preparedness and response capabilities. These exercises and workshops also help sector partners identify key interdependencies and improve communication. This article will touch upon some of the collaborative exercises being conducted throughout the sectors.

Banking and Finance: In September, the Financial Services Sector Coordinating Council (FSSCC) and the Financial Banking Information Infrastructure Committee (FBIIC) conducted an exercise on pandemic flu. Sponsored by the U.S. Department of Treasury and the Securities Industry and Financial Markets Association, participation in this exercise was encouraged to all members of the financial sector. This exercise provided an open forum to discuss different scenarios, test pandemic plans, and assess how a pandemic flu would affect the sector.

Food and Agriculture: Given the extensive scope of the Food and Agriculture (FA) Sector, it is critical that communications between FA sub-sectors flows well. In 2006, the Food and Agriculture Sector Coordinating Council (FASCC) and its government counterparts in the Government Coordinating Council (GCC) decided to replace two of the quarterly joint meetings with two tabletop exercises per year. These tabletop exercises help augment decision-making, improve communication and collaboration, and identify the vulnerabilities sector owners and operators must mitigate.

Information Technology: DHS's National Cyber Security Division (NCSD) sponsors Cyber Storm, the National Cyber Exercise series. Cyber Storm helps enhance preparedness, coordination, and response between the private sector and Federal, State, and local authorities in the event of a cyber attack. Given the fact that up to 85% of sector assets are owned by the private sector, maintaining effective collaboration and cooperation with both public and private security partners is critical. The first Cyber Storm was held in February 2006, and Cyber Storm II has been scheduled for March of 2008.

Water: As discussed in the October edition of *The CIP Report*, the Southern States Energy Board and the Public Technology Institute in collaboration with multiple public and private entities including the U.S. Department of Energy hosted Black Water, the Southeast Energy-Water Interdependence Tabletop Exercise. This tabletop offered participants an opportunity to discuss interdependencies between the Water and Energy Sectors. It also identified ways to enhance communication and collaboration as well as test state approaches under the State Energy Assurance Guidelines.

Tabletop exercises have proven to be quite beneficial to participants and the sectors they represent. They allow private and public entities an open forum to contemplate and prepare for certain scenarios that would otherwise negatively affect business continuity. As SCCs continue to evolve, these exercises and workshops will continue to provide sectors with a valuable resource. ❖

For additional information, please see the following:

FBIIC/FSSCC Pandemic Flu Exercise of 2007:
http://www.fspanfluexercise.com/

FASCC:
http://www.pcis.org/FASCC

Cyber Storm:
http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm

Cyber Storm II:
http://www.us-cert.gov/reading_room/infosheet_CyberStormII.pdf

Black Water:
http://www.seenergywater.govtools.us/

All Sector-Specific Plans available to the public can be viewed at:
http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm#2

DHS-Sponsored Tool Helps Cyber Exercise Participants Explore Complex Problems, Not Just Conduct Rehearsals

By Dennis McGrath, Institute for Security Technology Studies at Dartmouth College
Chris Fogle at Delta Risk, Glen Wada and Jim Marshall at Space Dynamics Laboratory, Utah State University

We usually conduct emergency preparedness exercises as training activities in which we rehearse an established incident response plan. But today's critical infrastructure is increasingly complex, interdependent, and controlled by information technology that is almost always connected to the web. As government agencies and private sector enterprises join forces to develop strategies for critical infrastructure protection, we find that cyber response exercises serve another purpose – discovery of the complex interdependencies, decision processes, constituencies, and considerations that must come into play for an effective response to a threatening incident.

This is particularly true in a cyber exercise, where the "playing field" is a series of complex networks of information systems that control our critical infrastructures. Within those networks, a diverse collection of computers, routers, and control systems enable electronic transactions that are essential to business and government continuity. These networks, largely owned by the private sector, are difficult to characterize even by the people who keep them running on a daily basis. Furthermore, when an attack on those networks is suspected, information passes through a complex human network that involves both public and private sector personnel. As cyber exercises have evolved, they have grown in participation and complexity. The national-level Cyber Storm exercise, conducted in 2006, included over 100 organizations located in 6 different countries. With over 3,000 simulated cyber-events connecting the web of participants, this type of cyber exercise has the potential to overwhelm and confound. The Livewire exercise, conducted in 2003, simulated attacks across multiple critical infrastructure sectors. Consequently, creating a realistic cyber exercise scenario is a daunting task for an exercise design team, but the challenge can be a discovery opportunity if we have the proper tools at our disposal.

To this end, DHS's Science and Technology Directorate has contracted with leading experts to develop a cyber Scenario Modeling And Reporting Tool (CyberSMART). The development team is led by Utah State University and includes Norwich University Applied Research Institutes, the Institute for Security Technology Studies at Dartmouth College, and Delta Risk, a private consulting firm. This team delivers world-class experience in cyber exercise design, including Livewire and TOPOFF exercises for DHS, Bulwark Defender for the U.S. Air Force, a variety of exercises at the regional and state levels, as well as consulting on cyber exercises for other countries.

Exercise planners can use CyberSMART to develop credible, engaging scenarios for functional cyber exercises up to the national level. Over the next several months, CyberSMART will be beta tested in state-level exercises by teams in Vermont and Massachusetts. A principal benefit of the tool is that it will help DHS's National Cyber Security Division strengthen the response capabilities of state and local agencies in cyber awareness and preparedness. Another benefit is that the tool will help these agencies ensure their cyber exercises are compliant with Homeland Security Exercise and Evaluation Program (HSEEP) guidelines – making them eligible for Homeland Security grants. HSEEP is a capabilities and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning. It is maintained by FEMA, and constitutes a national standard for the planning and execution of exercises. After the beta tests, CyberSMART will be hosted on the FEMA HSEEP website as part of the HSEEP Toolkit, where it can be accessed for DHS-sponsored exercises.

CyberSMART is a collaborative, web-based tool that allows a team of specialists to effectively create a

(Continued on Page 8)

CyberSMART *(Cont. from 7)*

complex cyber scenario. As a web-based tool, the number of specialists is not limited and exercise designers can work from their home offices or remote sites – anywhere they can reach the Internet. Based on a variety of best practices developed by the team's experts, the tool guides users through a disciplined, methodical approach for collecting, connecting, and communicating cyber-event detail. For complex scenarios, CyberSMART is well suited to manage several thousand cyber events, dozens of exercise participants, and provide a convincing, engaging, well-paced scenario of events.

Most exercise development doctrine begins with exercise objectives and ends with a Master Scenario Events List (MSEL). But what happens in between? The process often bogs down as exercise designers try to develop hundreds or thousands of scenario events that contain credible information and do not contradict each other. Because exercise designers often focus on a laundry list of attack methods, but don't incorporate credible detail about the networks in which the attacks will play out, the exercise itself bogs down because the participants don't have enough information about the network to craft a response.

The key to the CyberSMART approach is a "gamespace" model in which exercise designers define transactions, IT assets, and security measures for each participating organization. By focusing on the transactions necessary to maintain business continuity first, then identifying assets that support those transactions, the scenario development team can develop an attack scenario that emphasizes infrastructure protection issues rather than specific cyber attack methods. The scenario events themselves are more credible, since they incorporate accurate information about the context of the attack.

CyberSMART provides a disciplined process for cyber exercise planning, which is the foundation for exercise execution and provides a framework for after action analysis.

While exercises may last only a few hours or days, the exercise development process often takes months. The payoff for this time investment isn't always obvious at first, but the discovery opportunity within the exercise scenario development process almost always turns out to be as valuable as lessons learned during the exercise itself. CyberSMART is designed to maximize the value of exercise planning by emphasizing that understanding of complex systems is just as important as training with realistic scenarios. ❖

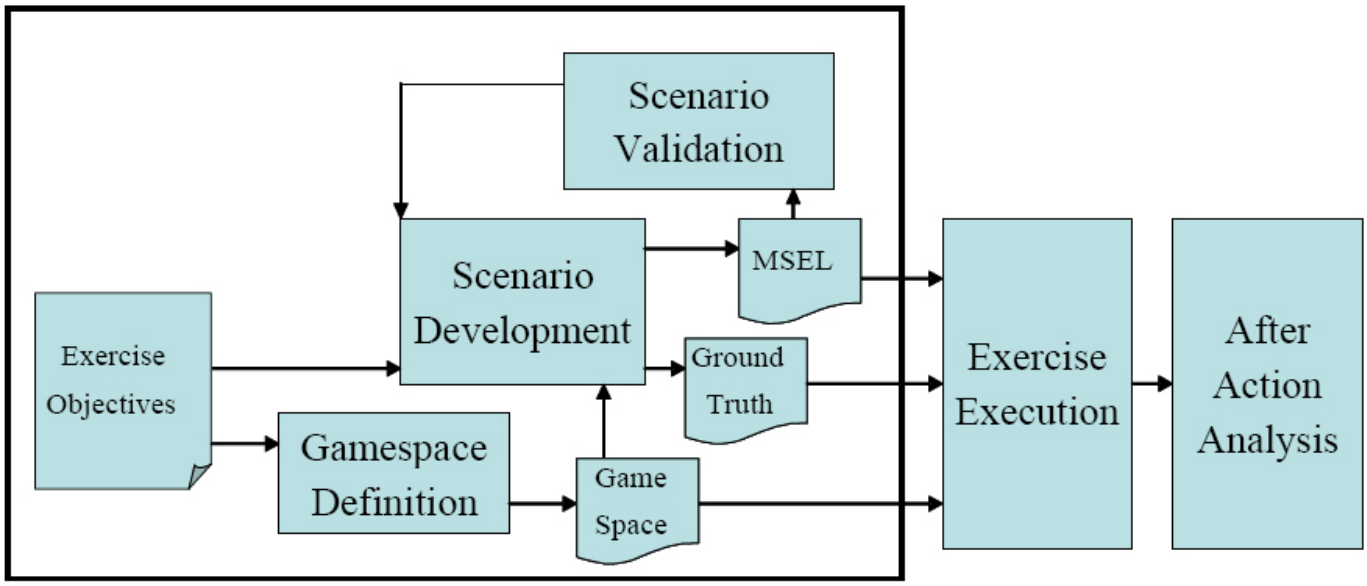

Figure 1 – The CyberSMART tool, sponsored by DHS, provides a disciplined process for cyber exercise planning.

HSEEP *(Cont. from 2)*

and procedure designed to depict an actual or assumed real-life situation.

Operations-based Exercises:

- Drill - a coordinated, supervised activity usually employed to test a single, specific operation or function within a single entity.

- Functional Exercise - examines and/or validates the coordination, command, and control between various multi-agency coordination centers. It does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time).

- Full-Scale Exercise - a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional and "boots on the ground" response (e.g., firefighters decontaminating mock victims).

For more information, please visit HSEEP's website at: https://hseep.dhs.gov/. ❖

CUBIC CORPORATION

Preparation *(Cont. from 5)*

the population – both affected and unaffected – of the current situation and prevent the spread of fear and confusion in the population. By incorporating a public affairs component, numerous officials have been tested through mock press conferences that can be broadcast live on a secure network run by the exercise developers.

Exercises are designed to test the implementation of plans, policies and procedures. As such, there must be an evaluation portion of the exercise. Having studied our clients' plans, policies, and procedures and learned best practices from evaluating other exercises, Cubic is able to observe exercise participants and provide constructive feedback based on the objectives that were identified at the beginning of the planning cycle. At the end of the exercise, Cubic conducts a Facilitated After Action Report (FAAR) with the primary training audience to discuss what went well and what needs improvement while the exercise is still fresh in the participants' minds. Within 30 days of the end of the exercise, Cubic provides a written analysis of the exercise providing specific observations and recommendations for each objective the training audience identified. This written report becomes a historical document officials can use to improve operations and understand why certain decisions may or may not have worked when a real event occurs.

Cubic is proud to continue to support our nation's first responders at all levels as it has over the past 25 years. Our cadre of expertise spans not only all facets of exercise design and implementation but also subject matter experts in homeland security, military affairs, and chemical, biological, radiological, and nuclear (CBRN) agents. ❖

TOPOFF *(Cont. from 3)*

practices and lessons learned have been gathered for each TOPOFF exercise and shared with stakeholders, as appropriate. Although DHS's TOPOFF 3 and TOPOFF 4 after-action reports have yet to be publicly released, the official summary reports from TOPOFF 1 and TOPOFF 2, as well as non-DHS TOPOFF after-action reports, are available on the Internet.

For additional information, also see DHS's Training, Technical Assistance, and Exercises website at: http://www.dhs.gov/xprepresp/training. ❖

Legal Conference on State Open Government Law and Practice in a Post-9/11 World

On November 15-16, the CIP Program participated in a legal and policy conference at the National Press Club in Washington, D.C. The conference featured approximately 30 subject matter experts, who commented on the non-release provisions to open government laws enacted by various states since the September 11, 2001 terrorist attacks. The event also included the release of a new book detailing changes in state public information laws.

Conference panelists commented on various categories of concern, including Critical Infrastructure, Public Health, Cyber Security, Political Structure, and Terrorism Investigations. The CIP Program's Legal Research Associate, Maeve Dion, spoke on the critical infrastructure panel. Her papers will be excerpted in next month's issue of *The CIP Report*.

The conference opened with remarks from Senator John Cornyn, Congressman Michael McCaul and Congressman Henry Cuellar, as well as special remarks by law professor John Norton Moore and Lucy Dalglish, Executive Director of the Reporter's Committee for the Freedom of the Press.

The conference was made possible by the Center for Terrorism Law, at St. Mary's University School of Law in San Antonio. The conference was supported by a 2006 Congressionally-directed Homeland Defense and Civil Support Threat Information Collection grant, administered by the Air Force Research Laboratory. The Center for Terrorism Law is a non-profit, non-partisan academic research center dedicated to examining legal issues associated with terrorism. A vital partner in the conference and state law compilation was the Reporters Committee for the Freedom of the Press.

The various subject matter experts prepared conference whitepapers, which will be released in the near future as conference proceedings by the Center for Terrorism Law. The book of state freedom of information laws will also be released in digital form, soon to be available from the Center for Terrorism Law's website, at http://www.stmarytx.edu/ctl/.

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1