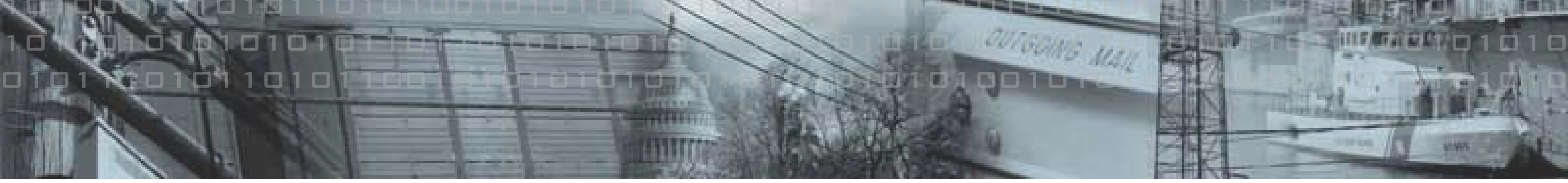


THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

JULY 2014

STATE AND TRIBAL

VOLUME 13 NUMBER 1

EDITORIAL STAFF

EDITORS
Kendal Smith
Emily Drake
Daniel Miktus

PUBLISHER
Melanie Gutmann

JMU COORDINATORS
Ben Delp
Ken Newbold

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

GEORGE MASON UNIVERSITY

School of Law

CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

This month, *The CIP Report* examines several **State and Tribal** critical infrastructure programs and initiatives.

First, Al Harley explains how state and local governments are incorporated into national critical infrastructure security and resilience efforts by providing an overview of the State, Local, Tribal, and Territorial Government Coordinating Council. Next, Steven Gutkin describes New Jersey's Critical Infrastructure Protection Bureau, illustrating the unique challenges of critical infrastructure security in a populated, industrialized area. Kevin M. Clement describes how states may model their critical infrastructure apparatus on the federal blueprint by detailing the Texas Private-Public Partnership Model and the development of his state's *Critical Infrastructure Security and Resiliency Plan*. John W. Madden explains how Alaska has been successful at maintaining critical services despite enormous distances and a treacherous environment. James J. Battese outlines tribal efforts and challenges, particularly within the Miami Tribe of Oklahoma. Finally, Sylvia Ifft highlights how Florida has taken a regional approach to their critical infrastructure protection organization.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The State, Local, Tribal, and Territorial Government Coordinating Council

by Al Harley

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) was formed in April 2007 following the release of the first edition of the National Infrastructure Protection Plan (NIPP), which advocated for the creation of a body that could offer perspectives of state, local, tribal, and territorial representatives on the nationwide effort to secure and protect critical infrastructure assets.

The SLTTGCC strengthens the national infrastructure protection effort by bringing together experts from all levels of government and from a wide range of professional disciplines that relate to critical infrastructure protection. It supports geographically diverse partnerships to ensure that state, local, tribal, and territorial officials play an integral role in national critical infrastructure security and resilience (CISR) efforts.

The Council includes a minimum of 24 state, local, tribal, and territorial leaders who have CISR expertise and experience. Led by the Executive Committee, consisting of the Chair, Vice Chair, and the Chairs of the various Council working groups, the current leadership includes:

- Chair – Curtis Parsons, Homeland Security and Emergency Management Coordinator, Lenawee County, Michigan
- Vice Chair – Brian Wright, Director, Critical Infrastructure Program, state of New York

Working Group Chairs and Co-Chairs:

- Bill Minear, Access Credentialing Working Group
- Brian Wright, Automated Critical Asset Management System Working Group
- Mark Hogan, Cybersecurity Working Group
- Shelly Schechter, Information Sharing Working Group
- Brian Wright, IP Gateway Working Group
- Irene Navis, Regional Resiliency Assessment Program Working Group
- James Battese (Past Vice Chair), Tribal and Territorial Working Group
- Irene Navis and Kevin Clement, Regional Initiative Working Group

The Council is pursuing key initiatives regarding the implementation of NIPP 2013, including a renewed examination of the CISR programs in governments nationwide, and developing a more geographically diverse membership.

During its 2014 Spring Plenary, held May 6 and 7 in Arlington, Virginia, the SLTTGCC discussed the status of several ongoing initiatives, and also set a path for the efforts and studies to be conducted beginning in the 2014-2015 Council session.

The release and implementation of NIPP 2013 was a key topic of conversation during the Plenary, with the Council discussing its options for supporting its rollout. Council members played an important role in the NIPP's development by participating in federal working groups tasked with revising and updating the previous edition. Since the release of the updated version in December 2013, the SLTTGCC has made successful adoption and use of the framework provided in NIPP 2013 a priority goal. During the Plenary, members agreed on several initiatives that would support the NIPP 2013 rollout, including conducting outreach to raise stakeholder awareness, developing best practices for implementation, discussing how SLTT governments can create analogous plans, and educating SLTT officials and private sector stakeholders on how the NIPP can aid their efforts to secure and protect critical infrastructure.

Another key issue that received considerable attention at the Plenary was the decommissioning of the Automated Critical Asset Management System (ACAMS) and the transition to the Infrastructure Protection (IP) Gateway. The Council confirmed that it understands the internal pressure the Department of Homeland Security (DHS) has been under to advance the next generation of tools and

(Continued on Page 3)

(Continued from Page 2)

services, but maintains that the IP Gateway should not be implemented until the agreed-upon security architecture is in place. Prohibiting authorized users who are currently performing homeland security duties and have a need to know from gaining access to this material would not support our common goal of improved information sharing and infrastructure protection. Therefore, once the appropriate security architecture is in place, legacy data designated as Protected Critical Infrastructure Information without a limited distribution exemption should be included in the release.

The Council also reaffirmed its plans to conduct a second phase of its landmark Regional Landscape Reports series. Beginning in 2011, the Council began work on a series of reports that studied the status and progress of CISR program implementation in jurisdictions across the nation, as well as the challenges faced by SLTT governments. The second phase of this study will review the findings of the first phase and update the data as necessary; determine how jurisdictions are addressing challenges uncovered in the prior study; examine how SLTT governments are approaching cybersecurity; and review best practices and initiatives that can assist governments in hardening their programs in the face of diminishing funding. The initial phase of the Regional Landscape Reports series included 9 reports on the 10 Federal Regions and provided an overview of how state and local governments organize and manage their CISR operations; which federal programs have the greatest value to those governments; and what issues present the greatest difficulties in implementing and maintaining CISR efforts. Nearly 300 officials were interviewed over the course of the series, offering a comprehensive picture of the status of the CISR mission across the nation. Study findings included: the DHS Protective Security Advisor (PSA) program is vital to sustain SLTT-level CISR programs; economic drivers and lifeline sectors are the priority sectors for most states and localities; no two states' programs are organized, staffed, or resourced in the same ways; and grants are central to the SLTT-level CISR mission, as they support most or all of a government's efforts.

The Council has also launched an effort to further enhance its own diversity by expanding its membership to incorporate representatives from more jurisdictions and disciplines. Under the plan, the Council is seeking to add new members from states that are not currently represented on the SLTTGCC, with an ultimate goal of having at least one member from each of the 50 states. Key qualities for prospective candidates for membership include having homeland security-related oversight responsibilities at a director or equivalent level; decision-making authority for their jurisdictions' CISR mission; and a willingness to represent and consider the perspectives of state and local governments in collaboration with federal and private sector stakeholders. Interested parties are encouraged to contact the Council for more information about the nomination process, particularly states that are currently unrepresented at any jurisdictional level, at SLTTGCC@hq.dhs.gov.

The Council has conducted numerous studies on important critical infrastructure issues through its working groups. Council working groups have provided both ad hoc and ongoing input on key federal programs and initiatives, such as: the IP Gateway system and its rollout; a Centers for Disease Control review of prioritization of anthrax vaccine dispersal as post-event prophylaxis; and a survey determining the effects that Windows XP technical support cessation would have on SLTT networks.

One key area of study, conducted by the Council's Access Credentialing Working Group (ACWG), examined the importance of, and need for, rapid access by critical personnel to disaster sites. This has led to further collaborative efforts between the Council and other organizations. The report, titled *Credentialing: Issues, Initiatives, and Options*, was finalized in October 2012, and examined options and best practices available for the enhancement of SLTT credentialing across the nation. Recommendations to the federal government include: that DHS clarifies whether the National Incident Management System (NIMS) Guideline for the Credentialing of Personnel requires compliance with the NIMS to utilize federal funding for credentialing initiatives; recognizing that a range of state and local credentialing systems are viable options for managing access during a variety

(Continued on Page 4)

(Continued from Page 3)

of situations; and coordinating the efforts of federal (and federally supported) credentialing initiatives and working groups. Since the release of this report, the ACWG has worked with the Fleet Mobility Working Group to further address the issues and challenges that accompany the establishment of an effective, universal credentialing system.

The Tribal and Territorial Working Group's (TTWG) report, *Tribal Critical Infrastructure Priorities and Needs*, fostered enhanced communication between DHS and tribal governments, and provided a template for the federal government to share valuable information about CISR programs and initiatives with tribes. The report examined the status of the CISR mission as implemented by tribal governments, and included several recommendations that laid out how the federal government could better work with tribal governments.

The Council is also continually seeking ways to provide a more complete picture of the SLTT perspective and to share those views with a wider range of agencies and organizations in the CISR mission space. In 2011, the Council launched the Critical Infrastructure Protection Coordinators Alliance Network (CIP Alliance). This network was created in order to gather the input of those SLTT governments not represented on the Council and to share news and information about federal CISR programs among a wider audience. The CIP Alliance incorporates a greater diversity of disciplines and regions and currently includes more than 130 members nationwide. Additionally, the Council maintains a Sector Liaison program, in which Council members serve as SLTT liaisons at the meetings of sector-specific Government Coordinating Councils (GCCs). In addition to providing the GCCs with information about recent and ongoing council initiatives, liaisons also provide the Council as a whole with reports on GCC activities, which enhances situational awareness of other CISR efforts and offers further opportunities for collaboration.

In the years since its launch, the SLTTGCC's work and initiatives have cemented it as a flagship council in the national effort to enhance the security and resilience of critical infrastructure assets. For additional information, please visit http://www.dhs.gov/state-local-tribal-and-territorial-government-coordinating-council.❖

New Jersey Office of Homeland Security & Preparedness Critical Infrastructure Protection Bureau

by Steven Gutkin, Bureau Chief, Critical Infrastructure Protection Bureau
New Jersey Office of Homeland Security & Preparedness

The state of New Jersey is rich in Critical Infrastructure Key Resources (CIKR). Additionally, as the most densely populated state in the nation, the majority of our critical facilities and systems are located in the most urban areas of New Jersey, increasing the implications of critical dependency failure. Consequently, the New Jersey Office of Homeland Security & Preparedness' (OHSP) Critical Infrastructure Protection (CIP) program has ongoing and robust responsibilities divided into two branches: Field Operations and Risk Mitigation. The CIP Bureau is supported by these separate branches and aligned with established sector working groups comprised of private and public sector partners that meet regularly.

The mission of the CIP Bureau is to ensure the protection, preparedness, and resiliency of New Jersey's CIKR through implementation of the National Infrastructure Protection Plan (NIPP).[1] The Bureau's staff is assigned to act as liaisons to the 16 U.S. Department of Homeland Security (DHS) defined sectors.

The CIP Bureau also manages New Jersey's Infrastructure Advisory Committee (IAC), a subset of the New Jersey Domestic Security Preparedness Task Force. The Task Force is the state's Cabinet-level body responsible for setting homeland security and domestic preparedness policy and was formed by law (New Jersey Domestic Security Preparedness Act) in 2001. The IAC acts as a liaison between the public and private sectors and is co-chaired by the OHSP Director (State Homeland Security Advisor) and two senior executives from the private sector. Its private sector membership includes representatives of utility companies, chemical and pharmaceutical firms, the telecommunications and healthcare industries, and others.

Field Operations Branch

The Field Operations Branch works closely with its public and private sector constituents to identify and catalogue New Jersey's most critical assets based upon criteria set forth by DHS, the state of New Jersey, and subject-matter experts from each critical infrastructure sector. A team comprised of federal, state, county, and municipal officials works with facility owners and operators to conduct on-site visits

(Continued on Page 6)

[1] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, http://www.dhs.gov/national-infrastructure-protection-plan.

(Continued from Page 5)

(Site Assistance Visits (SAVs)) to identify gaps and recommend potential mitigation measures in an attempt to protect critical infrastructure from natural or human-induced hazards. Information from these SAVs is incorporated into a risk analysis process which serves, in part, as the basis for grant allocation as well as training and project identification. OHSP Field Operations staff coordinates with New Jersey's DHS Protective Security Advisors (PSAs) to provide the highest level of assistance to CIKR owners and operators.

To support risk mitigation efforts throughout the state, OHSP funds several county-level Risk Mitigation Planners (RMP) and coordinates with other county-based Critical Infrastructure Coordinators (CIC). The RMPs and CICs are viewed as an extension of OHSP's CIP Bureau and provide critical linkages to CIKR owners and operators at the local and county level for any assets that might not already be noted within the state's portfolio.

Risk Mitigation Branch

The Risk Mitigation Branch also works closely with its public and private sector partners and is responsible for developing and implementing the DHS Homeland Security Exercise and Evaluation Program—a private sector exercise program designed to examine public and private sector plans, policies, and procedures. Sector partners participate in the exercise planning process so that the exercise objectives meet the needs of the sector. Each exercise produces an After Action Report and an Improvement Plan that seeks to identify gaps and recommend mitigation actions. The Branch also works with its public and private sector partners to address specific sector concerns and is responsible for several projects involving sector resiliency and interdependency.

Recent Program Highlights

Port Area Resiliency Studies

The CIP Bureau focuses on resiliency both for the state and for CIKR owners and operators. To that end, the Bureau has worked on several studies that have examined key lifeline sectors with significant attention in the areas surrounding the Ports of Newark, Elizabeth, and New York. These areas include seven of New Jersey's 21 counties and are home to approximately 50 percent of the state's 8.9 million residents.

The CIP Bureau was the lead for the first DHS Regional Resiliency Assessment Program (RRAP) in 2009 ("Exit 14") focusing on facilities in and around the New Jersey Turnpike (I-95) Exit 14 and their dependent lifeline sectors. The 10-mile area surrounding "Exit 14" has one of the highest concentrations of CIKR in the United States. Following this RRAP, CIP staff engaged with our local, state, and federal partners to examine the water sector assets in this region as well as specific port facilities, and then developed a Port Resiliency and Resumption of Trade Plan.

As a result of the resilience studies in this region, OHSP is finalizing the development of a Decision Support Tool (DST). The DST incorporates all of the assets considered during the Exit 14 project. These assets are mapped and dependencies and interdependencies are linked. In order to assist in making recovery prioritization recommendations, the system then allows the user to model a number of "What If?" scenarios to gauge the impact on these key assets and to examine potential recovery times following an event.

Private Sector Coordination Desk

Just prior to Hurricane Irene's 2011 landfall in New Jersey, OHSP realized that coordination between the public and private sector could be improved, especially during a disaster. OHSP developed

(Continued on Page 7)

(Continued from Page 6)

the Private Sector Coordination Desk (PSD) that is housed in the State Emergency Operations Center (SEOC). The PSD is activated during certain events and is triggered by SEOC operational levels. The PSD is designed and intended to be a conduit between state decision makers, emergency managers, and the owners and operators of critical infrastructure assets and systems in New Jersey. The PSD is coordinated and staffed by OHSP personnel. It operated on a 24/7 basis for more than two weeks during Superstorm Sandy in 2012 and has been lauded by the private sector as a highly effective mechanism for them to gain real-time situational awareness during an event and as a direct linkage to obtain assistance in solving sector-specific problems.

Following Superstorm Sandy, the PSD has been activated to support the SEOC and private sector during significant snow storms and Super Bowl XLVIII that took place in New Jersey in February 2014.

Computer Assisted Data Enhancement Tool

As part of OHSP's capability to conduct on-site vulnerability assessments for CIKR, an add-on is now available. The Computer Assisted Data Enhancement Tool (CADET) integrates with the comprehensive SAV report to integrate the vulnerability assessment data with panoramic video and geospatial data. CADET has proven to be an effective mechanism for providing facility-specific virtual tours of assets and is useful as both a planning and response tool.

Conclusion

As outlined within Presidential Policy Directive 21[2] and Presidential Executive Order 13636,[3] New Jersey OHSP is continually seeking to enhance its relationship with CIKR owners and operators throughout the state. The longstanding relationships already in place have provided the optimal platform for improving these public/private sector partnerships and for a continued focus on resilience.❖

[2] The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[3] The White House, Executive Order No. 13636: Improving Critical Infrastructure Cybersecurity, February 12, 2013, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.gpo.gov%2Ffdsys%2Fpkg%2FFR-2013-02-19%2Fpdf%2F2013-03915.pdf&ei=fkq8U7HrDJSjyATrmYGICw&usg=AFQjCNEUdtkUzDaoVVv-vG-U9Jb8FEEnrQ&sig2=Lu2zqhKNOwi0CKpUVv3F7A&bvm=bv.70138588,d.aWw.

The Texas Critical Infrastructure Private-Public Partnership Model

by Kevin M. Clement, CEM, TEM

The proposed *Texas Critical Infrastructure Security and Resiliency Plan* (TISR), currently in its final stages of coordination, introduces a new Private-Public Partnership Model specific to Texas. Much like private-public partnership models developed for other states, the Texas model parallels and complements that of the federal government, while designed to foster a private-public sector interface tailored to the structure of government and private entities unique to Texas.

Tailoring any model to the characteristics and idiosyncrasies of Texas is a significant task. Texas is ranked as the world's 14th largest economy. The state covers an area of 268,820 square miles, encompassing 254 counties that are further organized into 24 Councils of Government. Texas shares a 1,254-mile border with Mexico and a coastline of more than 367 miles along the Gulf of Mexico. Texas recognizes three Native American tribes and hosts five Urban Area Security Initiatives in the metropolitan areas of Austin, Dallas-Fort Worth-Arlington, El Paso, Houston, and San Antonio.

Private-Public Sector Interface

The Texas Private-Public Partnership Model is designed to support the following "Calls to Action," listed in the National Infrastructure Protection Plan (NIPP) 2013:

- #2: Determine Collective Actions through Joint Planning Effort
- #3: Empower Local and Regional Partnerships to Build Capacity Nationally
- #4: Leverage Incentives to Advance Security and Resilience
- #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions.

The Private Sector

Texas recognizes its private sector as that part of the economy consisting of an amalgam of private individuals, businesses and corporations, industry trade groups, business organizations, and professional societies. Also included with these "for profit" entities is the oft-termed "Voluntary Sector," consisting of private and non-profit organizations, think tanks, and policy institutes.

With the support of the Texas Higher Education Coordinating Board, the Texas Office of Homeland Security engaged representatives of colleges, universities, and other institutes of higher education that participate in relevant sector

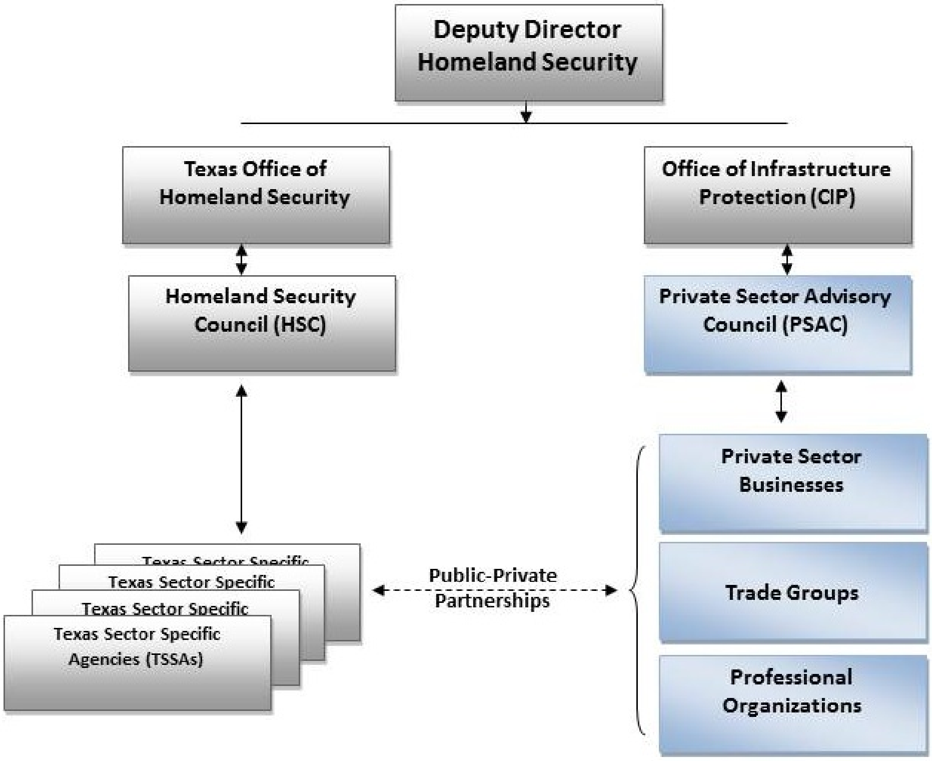

Deputy Director Homeland Security
Texas Office of Homeland Security
Office of Infrastructure Protection (CIP)
Homeland Security Council (HSC)
Private Sector Advisory Council (PSAC)
Texas Sector Specific
Texas Sector Specific
Texas Sector Specific
Texas Sector Specific Agencies (TSSAs)
Public-Private Partnerships
Private Sector Businesses
Trade Groups
Professional Organizations

Figure 1 – Proposed Texas Private-Public Partnership Model

(Continued on Page 9)

(Continued from Page 8)

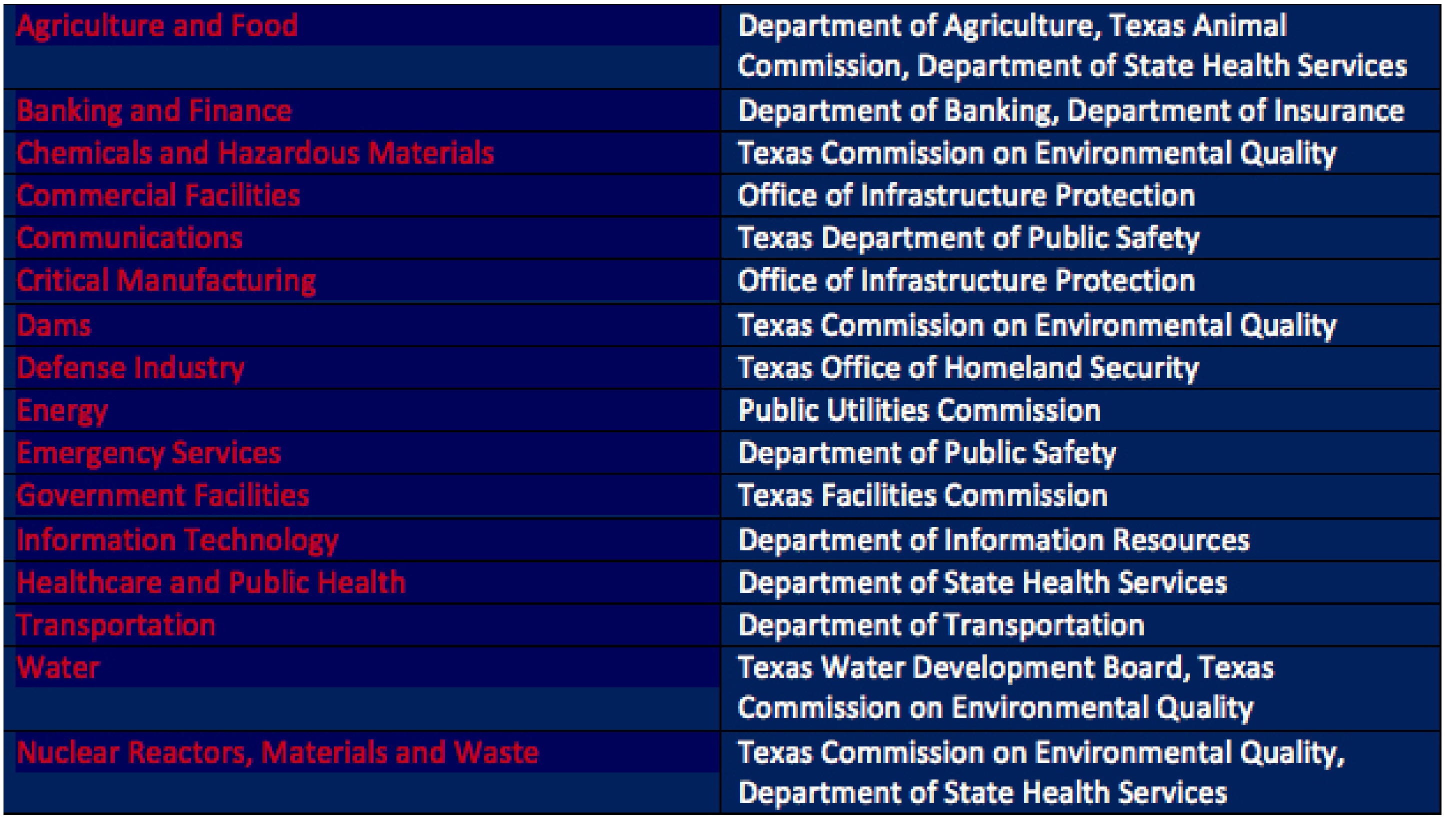
specific research. The intent was to foster research and development projects for each sector. The response was prolific.

Texas Sector Specific Agencies

Texas recognized the need to establish and maintain close relationships between government and private sector entities based upon a comprehensive knowledge and understanding of those characteristics and idiosyncrasies unique to each sector of the state's critical infrastructure. To this end, the state of Texas designated a Sector Specific Agency for each of the state's 16 sectors of critical infrastructure.

Texas Sector Specific Agencies (TSSAs) act as the primary point of engagement to state government for private businesses, professional organizations, and trade groups in their assigned sector. In this capacity, the TSSAs will work with their private sector partners to: provide sector-level critical infrastructure guidance; enact the *TISR* for their assigned sector; implement the risk management framework; develop protection and resilience strategies; and collaborate with the private sector to encourage, develop, and implement information sharing and intelligence analysis mechanisms within their sectors.

Those government agencies designated as TSSAs and the critical infrastructure sectors for which they have oversight are identified in *Figure 2*.



Agriculture and Food	Department of Agriculture, Texas Animal Commission, Department of State Health Services
Banking and Finance	Department of Banking, Department of Insurance
Chemicals and Hazardous Materials	Texas Commission on Environmental Quality
Commercial Facilities	Office of Infrastructure Protection
Communications	Texas Department of Public Safety
Critical Manufacturing	Office of Infrastructure Protection
Dams	Texas Commission on Environmental Quality
Defense Industry	Texas Office of Homeland Security
Energy	Public Utilities Commission
Emergency Services	Department of Public Safety
Government Facilities	Texas Facilities Commission
Information Technology	Department of Information Resources
Healthcare and Public Health	Department of State Health Services
Transportation	Department of Transportation
Water	Texas Water Development Board, Texas Commission on Environmental Quality
Nuclear Reactors, Materials and Waste	Texas Commission on Environmental Quality, Department of State Health Services

Figure 2 – Texas Sector Specific Agencies

Roles and Responsibilities. Representatives from each of the TSSAs met in four successive planning sessions to reach consensus regarding roles and responsibilities. The representatives reviewed recommendations from the 2009 NIPP and the roles and responsibilities of analogous Sector Specific Agencies in other states. Ultimately they agreed that TSSAs will:

- Serve as the point of engagement for the state of Texas to sector private partners
- Encourage and enhance private-public partnerships
- Promote sustainable economic development within the sector
- Support sector research and

(Continued on Page 10)

(Continued from Page 9)

critical infrastructure security and resiliency initiatives with state, regional, and local governments

- Promote and facilitate implementation of sector critical infrastructure security and resiliency policies, strategies, priorities, and activities
- Assist in establishing sector parameters for information gathering and sharing
- Facilitate information sharing between government and private sector partners for information on physical and cyber threats, vulnerabilities, incidents, and recommended protective measures
- Assist in coordination between private sector partners and government entities
- Identify and disseminate sector/sub-sector "best practices" and "lessons learned"
- Develop sector specific criteria for critical infrastructure
- Identify sector specific critical infrastructure
- Assist in conducting the annual data call
- Facilitate and assist in the implementation of sector specific risk assessment tools
- In collaboration with private partners, establish sector specific goals, objectives, and performance metrics
- Build consensus and encourage commitment by private entities to sector goals and objectives
- Consider incentives for private sector organizations that attain sector objectives
- Represent the state of Texas and its corresponding critical infrastructure sector on Government Coordinating Councils as well as sector and cross-sector workgroups
- Provide sector perspectives in collaboration with other state sector specific agencies
- Encourage business continuity planning by private business
- Assist in disseminating information on sector specific cyber threats and encourage appropriate protective measures, information-sharing mechanisms, and recovery plans for sector information assets, systems, and networks
- Assist in conducting sector facility assessments
- Promote and facilitate sector participation in critical infrastructure security and resiliency training and exercises where applicable
- Provide an annual report to the state of Texas addressing sector goals, accomplishments, issues, and concerns.

Sector Plans. In calendar year 2015, each TSSA, working in conjunction with private sector representatives and supporting state agencies, will develop a Sector Plan outlining sector goals, objectives, key tasks, and performance metrics for the next five years. These Sector Plans will seek to align with corresponding national-level Sector-Specific Plans and will include actions to support implementation of the *TISR* business continuity, cyber security, border security, and ports and maritime initiatives.

Annual Report. Beginning in September 2015, each TSSA is responsible for the creation of an annual critical infrastructure sector report, developed in coordination with its private partners and supporting government agencies. This report is an assessment of the sector's current status; its progress

(Continued on Page 11)

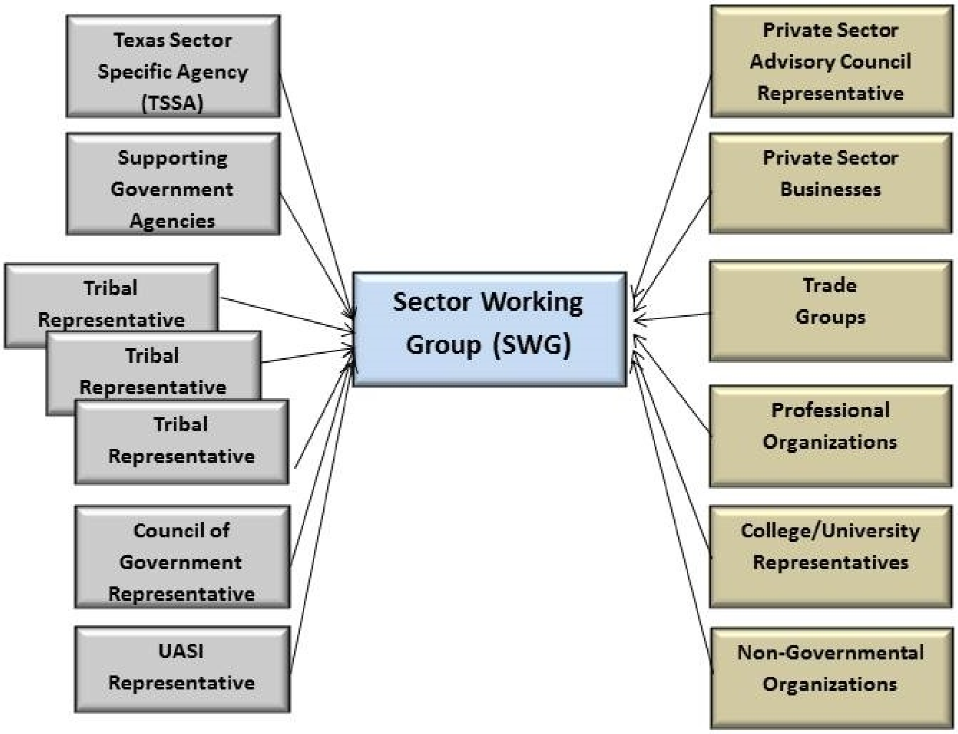

Texas Sector Specific Agency (TSSA)
Supporting Government Agencies
Tribal Representative
Tribal Representative
Tribal Representative
Council of Government Representative
UASI Representative
Sector Working Group (SWG)
Private Sector Advisory Council Representative
Private Sector Businesses
Trade Groups
Professional Organizations
College/University Representatives
Non-Governmental Organizations

Figure 3 – Recommended Participants - Texas Sector Working Group Proposed Texas Private-Public Partnership Model

(Continued from Page 10)

in implementating the *TSIR*; and attainment of goals and objectives specific to its sector. This report also includes recent accomplishments, any revised goals and objectives for the year to come, major issues of concern, and research and development initiatives pertinent to its sector. The report will be submitted to the Texas Office of Homeland Security not later than September 1st of each year for incorporation into the State Preparedness Report.

Supporting Government Agencies

In addition to the designated TSSAs, the state of Texas recognizes the capabilities and expertise provided by other state, regional, and local government agencies throughout the state. While not designated as TSSAs, these entities share responsibilities, functions, and concerns particular to their sectors. State agencies, offices, and commissions support the designated TSSA and their private partners in the development and implementation of Sector Plans and initiatives.

Tribal Governments

Texas recognizes three major Native American tribes within its borders: the Alabama-Coushatta Tribe; the Kickapoo Traditional Tribe of Texas, and the Ysleta del Sur Pueblo. During the course of developing the *TSIR*, a state representative travelled to each tribe to brief them on the details of the plan, answer their questions, and solicit the tribes' engagement. Each tribe was invited to participate in Texas' critical infrastructure security and resiliency initiatives and each was allocated standing representation on all Sector Working Groups.

Sector Working Group

The state of Texas will combine the expertise, capabilities, and resources of private sector businesses, professional associations, trade groups, non-governmental organizations, and colleges and universities with that of the TSSAs and other government entities through the establishment of Sector Working Groups (SWGs).

The SWGs serve to share information between the public and private sectors and refine sector specific and cross-sector security and resiliency goals, policies, practices, and procedures. Each SWG will establish goals and objectives in support of its sector's implementation of the *TISR*. Additionally, it will develop performance measures to track its sector's progress in attaining its stated goals over time. The SWG will assist in providing input to the development of the Sector's Annual Report. Texas representatives to the respective national-level Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) will be selected from the membership of the SWGs.

SWG composition will vary based on sector characteristics. Private sector membership will include individual owners and operators of private businesses, high-level corporate executives, leaders of trade organizations, and professional associations. Great care is used to ensure that private sector membership approximates that of the public sector from the outset. Public sector members will include representatives of the TSSA, supporting government agencies, tribal representatives, selected municipalities, and regional Councils of Government (COG). COG representation will be provided on a 3-year rotating basis, coordinated by the Texas Association of Regional Councils (TARC). Additionally, an SWG may also invite representation by DHS Protective Security Advisors and other federal agencies that possess a significant presence and subject-matter expertise in its sector. SWGs will solicit the engagement of colleges, universities, and policy and/or research institutes (think tanks) to facilitate research and development. The involvement of institutions of higher education and policy/research institutes in SWG operations directly supports Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions, as identified in NIPP 2013.

An SWG is normally co-chaired by the lead representative of the TSSA and an individual selected by participants from the private sector. Typically, this private sector leader is that sector's representative to the Governor's Private Sector Advisory Council.

Lifeline Sector Working Groups

The state of Texas designated the critical infrastructure sectors of Energy, Communications, Water/Wastewater, Financial Services, and Transportation as lifeline sectors, recognizing the importance and priority of these sectors in homeland security and emergency

(Continued on Page 12)

(Continued from Page 11)

management operations. While the state's goal is to create SWGs for each critical infrastructure sector over the course of this five-year plan, its focus in this first year is to establish SWGs for each of the lifeline sectors.

To date, SWGs have been established for the Financial Services and Water/Wastewater Sectors. Based on lessons learned in their creation, the Texas Office of Homeland Security has created the *Guide to Texas Sector Working Groups* to assist in the establishment of additional SWGs in 2014-2015.

Cross-Sector Working Groups

Through coordination with the Texas Homeland Security Council and the Governor's Private Sector Advisory Council (PSAC), Texas will establish four standing cross-sector working groups to address issues and concerns in the areas of Business Continuity, Cyber Security, the Border Region, and Ports and Maritime.

Texas Representation on Sector and Government Coordinating Councils

In recent years, Texas has not enjoyed significant representation on Sector Coordinating Councils or Government Coordinating Councils at the national level. However, following the creation of TSSAs, the state's representation has begun to improve. Private sector representatives to the Sector Coordinating Councils are normally solicited from the PSAC or an individual it nominates. Texas representatives to Government Coordinating Councils typically are members of TSSAs or individuals nominated by those agencies. Prior to their nomination, all candidates are vetted to ensure that they are both willing and possess the time needed to work on Sector or Government Coordinating Councils.❖

The TISR *is currently in coordination among government agencies and private entities prior to its final approval. While elements of the Private-Public Partnership Model have already been enacted, the plan and the Texas Private-Public Partnership Model remain subject to change.*

Critical Infrastructure in Alaska: A System of Competitive Collaboration

by John W. Madden*

There is a saying that every Alaskan is a tour guide who well serves our friends and families as well as our guests from around the world. But besides this lighthearted saying, there is an even better truism that every Alaskan is a logistician. Our quality of life depends on resilient supply lines. Our economy is based on the steady and reliable movement of goods and commodities to our state and to our national and international trading partners.

Our reliance on our transportation system and the supporting critical infrastructure is as great as anywhere in the nation. We share many of these same conditions with Hawaii and the territories of the Caribbean Sea and the Pacific Ocean.

One of the underpinnings of effective critical infrastructure security is to protect those elements upon which other systems rely. The importance of identifying any single point of failure is well described in the proverb of the connection between the loss of a horseshoe nail and the loss of the kingdom. The homeland security leadership in Alaska early recognized the vitality of these connections. Part of that recognition was in deciding that we must achieve, maintain, and enhance our resilience through partnerships with owners and operators of critical infrastructure from both the private and public sectors.

Alaska has very long and tenuous supply lines within our state and with our trading partners. We cannot overcome the tyranny of distance and time; but we have built the appropriate systems most effective for our conditions. Over the years we evolved a hybrid of two logistical approaches. We use “just in case” for many of the Alaskan communities off the road systems for the commodities that are difficult, if not impossible, to move in winter conditions. Seasonal storage of fuel, water, and durable goods are common and essential. For the remainder of our essential commodities, we use “just in time” systems for consumables such as foodstuffs and medical supplies.

Following the emergence of the new threats revealed by September 11, 2001, the military leadership in Alaska initiated a new collaboration to protect the continuity of the supplies and services crossing their fence line and thus preserving their ability to perform their strategic mission for the nation. We brought together state and federal agencies, large and small private sector corporations, and non-governmental organizations for the express mission of protecting the movement of goods and people and the provision of essential services. The Alaska Partnership for Infrastructure Protection (APIP) has steadily developed what has come to be described as a system of competitive collaboration. From the beginning, APIP has been market based for its members and its priorities. The value of participation must exceed the investment in time. Our continued growth for more than a decade shows that we do provide value.

Unlike some other public/private partnerships, APIP has an important role in planning and preparedness in peacetime and an operational role in the events we have faced. The spring and summer of 2009 brought a series of overlapping hazards that threatened our collective ability to keep our supply lines open—volcanic eruptions, threat of H1N1 pandemic outbreak, historic floods on the Yukon River, and an exceptionally early wildfire season. I call 2009 our year of flow, flu, floods, and flames.

Our APIP partners worked together at each stage of these threats to keep our goods moving and our essential services uninterrupted. With the first eruption of Mount Redoubt in late March, APIP members foresaw the consequences of ash fall and the closure of our airspace and maritime lanes. Our private sector partners collaborated to meet the anticipated needs for face masks, automotive engine filters, car window cleaners, and

(Continued on Page 14)

(Continued from Page 13)

many other commodities. The public never experienced any shortages of critical goods.

We also anticipated the likelihood of absenteeism related to heavy ash fall on government missions and private sector essential services. Planning in this area proved of even greater import with the first reports of the H1N1 flu virus in April 2009. As the nation began analyzing the potential effects on critical infrastructure of social distancing to limit the spread, Alaska adapted its volcanic eruption plans to this emerging threat.

The May 2009 floods on the northern Yukon River were the most damaging of the past century, yet did not damage our statewide logistics system. All APIP partners worked collaboratively to rebuild the community of Eagle—which suffered rocord flooding and was virtually destroyed—before the onset of winter. Our early collaboration enabled the state, supported by several federal partners, to rebuild dozens of residences, the electrical grid, and health facilities. We also had to adapt to several closures of airspace resulting from thick smoke caused by the third-worst fire season in history, with almost three million acres burned.

With its continuing growth across Alaska and with more members, APIP focuses intensively on the cyber threat. We found that the world's oldest threat of volcanic eruption had similarities to the world's most recent threat of cyber-attacks. Our plans to sustain our communications systems through one threat proved of great benefit in preparing to face another threat. Our analysis of the effects of terrorist attacks also aided our understanding of the potential kinetic consequences of cyber-attacks.

The Alaska Division of Homeland Security and Emergency Management is central to our efforts to improve our resilience and also to our investments in safety and security for the people and economy of Alaska. Starting with the inclusion of homeland security in 2002, the Division conducted security vulnerability assessments on critical infrastructure. Similar to many states, our initial focus was on security within the fence line. We found that many facilities were exceedingly secure from physical threats across the fence, but nonetheless had dramatic vulnerabilities due to interdependencies in the surrounding community. Water and power services, transportation and communications systems, and effective response by local law enforcement are all necessary for continuity of services and continued movement.

After expanding our scope to the community-based assessment, we found that the vulnerabilities were often outside of the infrastructure owner or operator's ability to change. We aligned our homeland security strategy to the capabilities needed to protect all the essential systems throughout the state.

In all of our efforts, we must be ever vigilant that we are truly addressing the risks from threats and hazards and reducing those risks through investments in equipment and skilled people. If we simply shift the risk to another link of the supply line or another element of the network, we have not reduced risk but merely relocated it. This migration of risk is expensive, unproductive, and misleading. Every investment must consider the entire system. Alaska, as all states, must think and plan across our entire enterprise, even as we invest in local capabilities. Alaska does not have the redundant and overlapping systems common throughout the rest of the nation. We must protect our critical infrastructure through more assertive means and with the competitive collaboration of all our partners.❖

**John W. Madden is the Director of the Alaska Division of Homeland Security and Emergency Management and is the Past President of the National Emergency Management Association.*

Challenges of Tribal Homeland Security

by James J. Battese
Director, Department of Homeland Security and Counter Terrorism
Miami Tribe of Oklahoma*

Tribal nations strive to protect their citizens and infrastructure, much like the United States government. Also like the federal government, most tribal governments view their mission as multi-faceted with their success largely dependent on interagency cooperation.

According to the Department of Homeland Security (DHS), critical infrastructure is defined as, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters."[1]

In 2006, DHS released the first National Infrastructure Protection Plan (NIPP). A key component of the NIPP is coordination and cooperation among all levels of government. The body tasked with facilitating that effort is the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC). According to DHS, the SLTTGCC "serves as a forum to ensure that SLTT homeland security officials or their equivalents are fully integrated as active participants in national critical infrastructure protection and resilience efforts and to provide an organizational structure to coordinate across their jurisdictions on guidance, strategies and programs."[2] The Miami Tribe of Oklahoma has had a representative on the SLTTGCC since its inception, and has made great progress in raising awareness in the tribes about their role in the critical mission of protecting our nation's critical infrastructure.

There are 566 federally recognized tribes located on approximately 55 million acres of land throughout the United States. Many tribes also own land that is not considered "trust land." The Miami Tribe of Oklahoma's jurisdiction includes part of Ottawa County in far Northeastern Oklahoma. The tribe owns approximately 1,500 acres in or near our jurisdictional boundaries, some of which was originally allotted by the federal government, but we also own land in other parts of the country that hold historic significance to our tribe.

In addition to the land comprising this acreage, our infrastructure protection efforts must take into account more than a dozen buildings that house our government operations and services, several tribal businesses, historical homes, and sacred grounds. The tribe owns interests in businesses located in several states and even foreign countries. Our facilities are susceptible to the same threats as those faced by any other government facility, including cyber terrorism, bomb threats, race-based hate crimes, and natural disasters. We plan to meet and defeat these risks by staying current on risk assessments, preparedness, training, security, and redundancy.

Since our tribe is located in "tornado alley," we have committed extensive resources to preparedness and response plans for this particular threat. In the past few years, we have had three deadly tornados touch down within a few miles of our jurisdictional boundaries, including one in 2007 that destroyed one of our

(Continued on Page 16)

[1] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, http://www.dhs.gov/national-infrastructure-protection-plan.

[2] U.S. Department of Homeland Security, State, Local, Tribal, and Territorial Government Coordinating Council, January 2013, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.ahcusa.org%2Fdocuments%2FSLTTGCC-Slides-2013FleetWorkshop.pdf&ei=8Om6U7PvBMGTyASezIA4&usg=AFQjCNHX2b4kgYHhpPHhYSA4U065kUvzbA&sig2=tvaiv-erohtyWh0RdQ498g&bvm=bv.70138588,d.aWw.

(Continued from Page 15)

tribal homes. The tornado caused hundreds of thousands of dollars in damage, as it also destroyed part of our farm and several pieces of agriculture equipment.

In the past year, the tribe's Business Committee, the tribal governing board, has undertaken several measures to increase our homeland security. The tribe has created a Tribal Homeland Security Department and an Emergency Management Office. The staffs of these two departments have implemented many initiatives and plan to do more in the coming year.

Among our efforts, we have begun the process of increasing employee awareness and participation in our efforts to protect our nation. On the preparedness front, we have developed a committee comprised of "team leaders" from each of our buildings. These leaders are charged with communicating critical information to fellow employees, tribal members, or customers. We are in the process of compiling employee rosters for use in the event of a disaster, and these rosters include helpful information such as photographs and emergency contacts.

We also have held informational luncheons for our elders about tornado awareness. Our city and county emergency managers have led the discussions and provided safety tips and guidance for elders to make sheltering plans in their homes. We also have provided weather radios to elders and helped them program and learn to operate them. On the response front, we are hosting first aid/CPR certification training for all employees, as well as more in-depth, tactical training on triage and wound care for our law enforcement officers and other key players.

The tribe has also made an effort to interact with outside government officials including city and county emergency managers and law enforcement officials from other city and tribal jurisdictions. An example of this teamwork was evident when a deadly tornado destroyed much of Quapaw, Oklahoma, a small town about 5 miles from our tribal jurisdiction. Our officers responded immediately, and our tribe provided other crucial resources in the aftermath of the storm. We are certain they would do the same for us.

In February 2013, the Tribal and Territorial Working Group of the SLTTGCC published a study entitled, "Tribal Critical Infrastructure Priorities and Needs." It emphasized the need to increase coordination and collaboration regarding critical infrastructure among all levels of government. I am proud that we strive to achieve that here at the Miami Tribe of Oklahoma.

Our elders teach us that our wealth is shown by how much we give to others. I am proud of our tribe's Business Committee's efforts to share knowledge and resources with other governments. This cooperation will ensure a more secure infrastructure for future generations, not just for the Miami Nation, but for the entire nation.❖

**James Battese served as the Director of the Department of Public Safety for the Miami Nation from 2001 to 2012 before moving to his current position as Director of Homeland Security and Counter Terrorism. He also administrates the Miami Nation's road program and serves on the Oklahoma State Department of Transportation's Tribal Advisory Board. He has significant law enforcement experience and is the Chair of the SLTTGCC Tribal & Territorial Working Group.*

Florida's Critical Infrastructure Protection Program

by Sylvia Ifft*

Each region, each state, and each county is unique in geography, population density, and industry characteristics. This makes standardizing critical infrastructure protection efforts challenging. How can decision makers develop plans and policies applicable to such a vast array of landscapes, hazards, and events? Along with many other states across the nation, Florida faced this challenge head-on in late 2001. Florida's unique geography and hazard environment required leadership to take a thoughtful approach in terms of domestic security post 9-11.

Background

Florida, surrounded by 1,350 miles of coastline, presents a distinct environmental challenge. Bounded by the warm waters of the Atlantic Ocean and Gulf of Mexico, Florida experiences the effects of forty percent of all U.S. hurricanes. Eighty-three percent of category 4-and-above hurricane strikes have hit either Florida or Texas; sixty percent of all hurricanes affecting Georgia actually come from the south or southwest across northwestern Florida.[1] Connectivity to the electric grid and land transportation limited to the northern border compounds the potential consequences of this threat.

In addition to volatile environmental hazards, Florida has to manage an extremely diverse and dense population. In terms of population density, Florida ranked eighth in the nation in 2012. That same year, Florida ranked number four by number of immigrants behind California, New York, and Texas—all of which share a border with a neighboring country.

Most Americans may consider border security a problem exclusive to the Southwest. However, while Florida's border physically touches no other country, smugglers consistently land on South Florida shores, bringing with them undocumented immigrants literally by the boatload. The problem goes beyond smuggling of Cuban and Haitian migrants; these covert operations include bringing in people from all over the world to include Chinese, Dominicans, Mexicans, and Ecuadorans. Yet interdictions other than for Cubans and Haitians typically fall under the public radar and receive little media attention.[2] Further complicating matters, Florida ranks among the highest in the nation in the number of identified hate groups.[3] These statistics are a serious concern to intelligence officials. Both foreign and domestic threats are a reality.

Nationwide, critical infrastructure protection programs have begun to put more emphasis on consequence analysis and cascading effects of loss. Most recognize Florida as a tourism powerhouse, attracting nearly 95 million visitors spending some $76 billion in the state each year.[4] However, seventeen Fortune 500 Companies call the Sunshine State home.[5] Florida is a global leader in international trade ($158 billion in 2013). Its economy is the fourth largest in the United States and ranks among the top 20 in the world, attracting infrastructure, talent, and the headquarters of many nationally ranked companies. Collapse of this economic machine would have a devastating impact.

What does all this mean from the perspective of domestic security and

(Continued on Page 18)

[1] "The Deadliest, Costliest, and Most Intense Untied States Tropical Cyclones from 1851 to 2006 (and Other Frequently Requested Hurricane Facts)," *NOAA Technical Memorandum NWS TPC-5*, updated April 15, 2007. http://www.nhc.noaa.gov/pdf/NWS-TPC-5.pdf

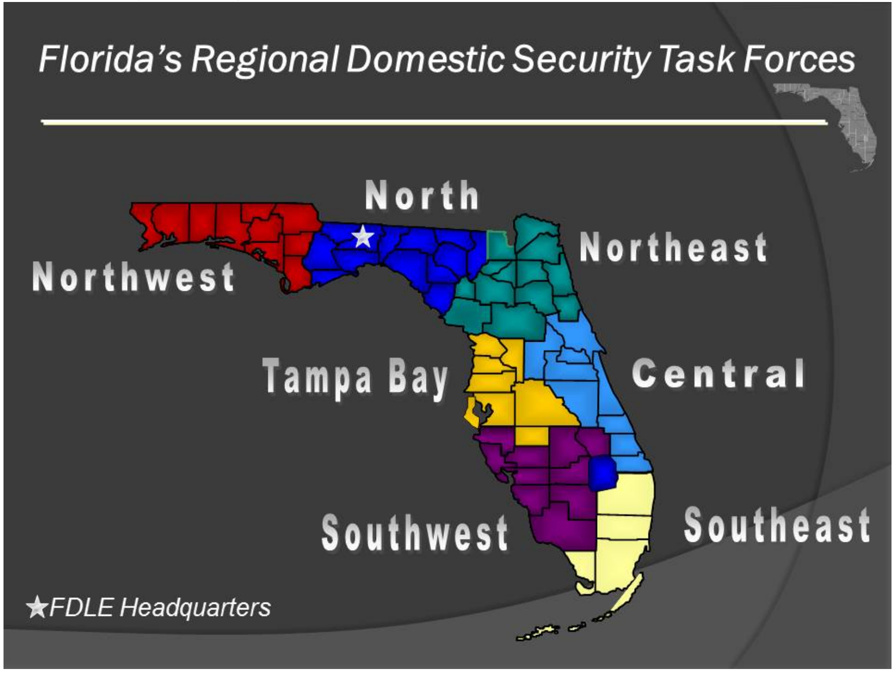
[2] Al Chardy, "Smuggling of Brazilians, other migrants growing in South Florida," *Miami Herald*, October 30, 2012 http://www.miamiherald.com/2012/10/29/3073277/smuggling-of-brazilians-other.html

[3] "Hate Map," Southern Poverty Law Center, 2013, accessed July 17, 2014. http://www.splcenter.org/get-informed/hate-map

[4] "Research and Data," Enterprise Florida, accessed July 7, 2014. http://www.enterpriseflorida.com/research-data/

[5] Robert Trigaux, "On latest Fortune 500, most of the few Florida companies to make list rise in ranks," *Tampa Bay Times*, June 2, 2014. http://www.tampabay.com/news/business/corporate/on-latest-fortune-500-most-of-the-few-florida-companies-to-make-list-rise/2182572

(Continued from Page 17)



critical infrastructure protection?

Program Development

In October of 2001, Florida's leadership developed a comprehensive counter-terrorism strategy. That leadership, in partnership with state and local governments and key members of the private sector, created a *Domestic Security Strategic Plan*[6] designed to integrate multi-agency needs, yet remain focused on one state and one mission. To this day, this plan is refined regularly as state and local capabilities evolve. This strategy is directly supported by a comprehensive structure comprised of multi-jurisdictional and multi-disciplinary participation at all levels of government.

This multi-jurisdictional and multi-disciplinary representation comprises the membership of Florida's seven Regional Domestic Security Task Forces (RDSTF). The RDSTF structure was codified by state statute in November 2001 with the Florida Department of Law Enforcement (FDLE) appointed as lead agency. The design of the seven RDSTFs mirrored the Florida Division of Emergency Management's (FDEM) multi-county regional structure. This was done intentionally to ensure the emergency management and law enforcement communities worked seamlessly in preparedness and response efforts. In order to maintain domestic security mission focus statewide, a State Working Group on Domestic Preparedness—comprised of voting delegates from the seven RDSTFs, designated urban areas, and key state agencies—meets quarterly to identify domestic security issues and to set and revise policies and guidelines at the state level. However, the core strength of Florida's Domestic Security program is the RDSTFs.

RDSTF leadership recognized that a comprehensive understanding of critical infrastructure vulnerabilities is a necessary component of an overall domestic security policy. The first step is identifying critical infrastructure; but how do you define critical infrastructure? How do you develop a "list" of critical infrastructure assets? A foundation must exist that defines the threshold consequences—what facilities ensure continuity of government and continuity of services to the mass populace?

To lay the foundation, Florida's Critical Infrastructure Protection program began by compiling information collected under specific reporting requirements for certain facilities per Florida statute. For example, all state owned or leased facilities are required under statute to complete a security assessment—water management districts and private sector entities were strongly encouraged, though not required, to participate as well. General-aviation airports meeting designated parameters are required to provide information to FDLE for use in critical infrastructure protection. Before the duties were returned to the U.S. Coast Guard in May 2011, FDLE conducted annual inspections of Florida seaports to evaluate security measures and identify areas of improvement.

At the same time, the FDEM, concerned with the consequences associated with the loss of assets directly affecting communities, designed a robust program to identify those facilities critical to local populations. FDEM's Geographic Information System Lab continues

(Continued on Page 19)

[6] "Florida Domestic Security Strategic Plan 2012-2014," Florida Department of Law Enforcement, accessed June 7, 2014. http://www.fdle.state.fl.us/Content/getdoc/13b174e9-e137-41b0-98fc-09b846bc8cdb/StrategicPlanandFundingStrategyOctober2001.aspx

(Continued from Page 18)

to work with local, state, and federal agencies to maintain datasets of shelters, emergency operations centers, critical facilities, and hazardous material facilities.[7]

Members of the RDSTF under the leadership of FDLE set forth a multi-year project to identify and assess public and private assets between 2002 and 2005. During those years, Florida successfully conducted hundreds of site assessments utilizing a common methodology. This was a first step in developing a state standard for Florida's Critical Infrastructure Protection (CIP) program. One of the primary obstacles was transferring the field assessments into a secure electronic database. Keying in hundreds of field assessments proved a daunting task, therefore much of the assessment data remained filed in paper form until 2007.

As Florida moved forward with the statewide assessments, DHS assigned five Protective Security Advisors (PSAs)[8] to Florida in March 2005. Working with the state Deputy Homeland Security Advisor, the PSA districts were later revised to match the state's RDSTF structure. To this day, the PSAs are an essential partner in Florida's CIP program.

In an effort to improve electronic-data collection capabilities, Florida in 2007 moved toward utilizing the Automated Critical Asset Management System (ACAMS) as the next evolution of the statewide assessment process. To support the new program, FDLE hired eight Critical Infrastructure Planners between 2007 and 2008; one was assigned to each of the Regional Domestic Security Task Forces and one to FDLE Headquarters to coordinate statewide efforts and serve as a liaison between the seven RDSTFs and between the state and federal government.

Based upon information compiled through the assessments and reported during the prior years, as well as guidance from DHS, the State Working Group's Critical Infrastructure Committee developed a statewide critical infrastructure strategy. This strategy outlined guiding principles, strategic objectives, implementation of assessments, and the criteria for identifying infrastructure significant to the state of Florida.

The statewide strategy became the field guide for the CI Planners assigned to the RDSTFs. Initially, the primary responsibility of the CI Planners was to serve as regional administrators and training coordinators for the ACAMS program. As the state CIP program evolved, the duties of the Planners grew to include other critical infrastructure outreach initiatives such as special event and fusion-center support.

In essence, Florida created its own "mini" PSA program. Rather than duplicate efforts, the Florida CI Planners and PSAs actually complement each other. The PSAs coordinate with owners and operators of nationally significant infrastructure, while the CI Planners focus on infrastructure significant at a state and local level. Often times, the PSAs, CI planners, and representatives of local response agencies visit owners and operators of critical infrastructure assets as a multi-discipline, yet unified, component of the RDSTF.

Florida CI Planners, working in concert with the PSAs, are tasked with coordinating resources within the RDSTFs to implement critical infrastructure protection awareness training, conduct and update vulnerability assessments, compile information for national data calls, provide support and recommendations regarding policies related to critical infrastructure protection, and identify and develop infrastructure protection initiatives.

Just as the PSAs provide support to National Special Security Events (NSSE), Florida's CI Planners provide event-planning support for significant state and local events such as the governor's inauguration, college football games, airshows, and major festivals. Prior to events, the CI Planners work with local agencies to conduct vulnerability assessments and identify supporting infrastructure and security concerns. The CI Planners provide an additional layer of support to the PSAs for NSSEs by collaborating on assessments and coordinating with local response agencies.

(Continued on Page 20)

[7] "Critical Facilities," Florida Division of Emergency Management, accessed June 7, 2014. http://www.floridadisaster.org/GIS/criticalfacilities/index.htm

[8] For more information on the DHS PSA program, visit http://www.dhs.gov/protective-security-advisors.

(Continued from Page 19)

During the planning for the Republican National Convention (RNC) held in Tampa in August 2012, all of the state's domestic security disciplines were brought to the table. Infrastructure assessments were conducted for all the major venues, including stadiums, convention centers, arenas, and event and delegate hotels. Interdependent relationships with these venues and supporting facilities, such as electric, gas, water, sewer, and communication connections were identified, mapped, and assessed for vulnerabilities. This included electric power stations located far from the convention forum, major fiber lines for communication, and locations of water and sewer pipes and access points at ground level. This effort ensured that should there be a natural or man-made incident that could be a threat to the convention or its attendees, the cascading effects would be readily known and potential mitigation measures initiated immediately.

Additionally, supporting infrastructure not physically linked to the major venues but providing important services to the RNC, such as the city's major trauma hospital, was also evaluated, as were assets in proximity to the convention site which had the potential to be used for terrorist activities. These included downtown office buildings, the rail systems that run through the central business district, and facilities at the nearby Port of Tampa.

Terry Cullen, a Critical Infrastructure Planner with the Tampa Bay Regional Domestic Security Task Force noted, "CI planning played a key role for a safe convention. The CI planning that went into the RNC created many new relationships between the public and private sectors. Many private sector companies that wouldn't normally discuss security information with law enforcement came to the table and were willing to collaborate."[9]

The RNC opened up new possibilities for critical infrastructure planning in the Tampa Bay area. FDLE created a focus group of security leaders from regional businesses to discuss the concept of establishing a permanent private-sector-driven-domestic security collaborative. The response was a unanimous yes, and P3 was born. P3, Private/Public Partnership, is comprised of up to 32 directors, two from each of the 16 critical infrastructure sectors. Each sector will eventually develop a Peer Industry Group of regional businesses that comprise the range of their industry group.

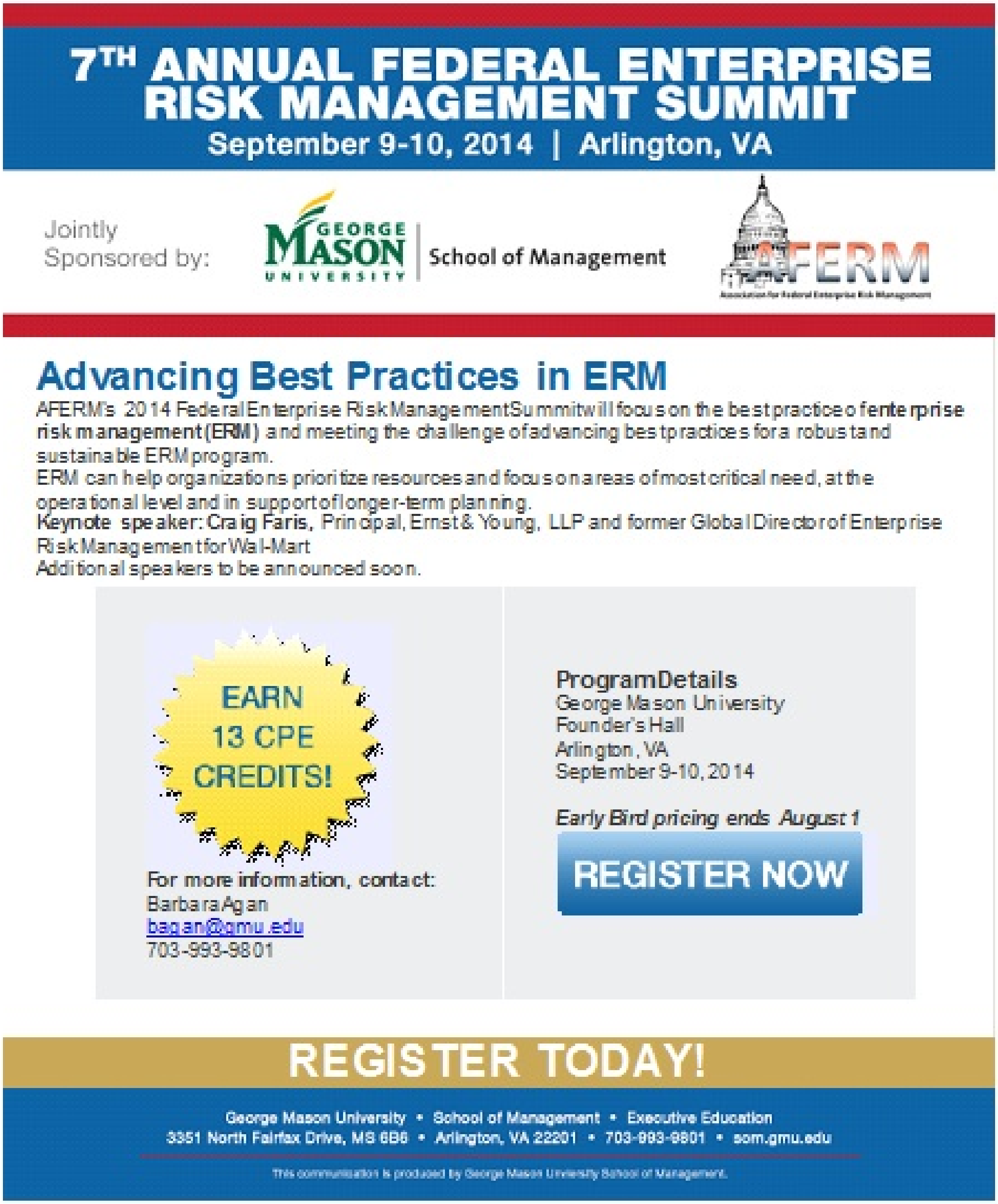
Conclusion

The state of Florida has taken a unique approach to critical infrastructure planning. The regionalized approach allowed the RDSTFs to adjust to the unique context of their areas of responsibility. The Tampa Bay urban area is very different from the rural areas of the Panhandle. This approach fosters CIP program innovation, such as the P3 initiative, and this in turn could provide spin-off innovations in other areas such as training. Mission and guidance are coordinated at the State Working Group level; however, implementation can vary according to the needs of the region.

Since the mindset has shifted over the years from examining critical infrastructure at a capacity level to a consequence scenario, planners can focus on the drivers of their state's economy and the needs of the population to identify and categorize critical infrastructure assets. Determine what's at the top of the list then peel away the layers of dependencies and interdependencies and the critical of the critical will be revealed.❖

**Sylvia Ifft is a statewide Critical Infrastructure Protection Planner for the Florida Fusion Center at the Florida Department of Law Enforcement. Sylvia has been involved with Critical Infrastructure Protection efforts though Florida's Regional Domestic Security Task Forces and State Working Group on Domestic Preparedness since 2007.*

[9] Interview with Terry Cullen, July 10, 2014.



The Center for Infrastructure Protection and Homeland Security (CIP/HS) 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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