



Homeland
Security

NIPP NEWS

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 55: OCTOBER 2010

Critical Infrastructure Activities and Events

Assistant Secretary Keil Delivers Remarks to U.S. Chamber of Commerce National Security Task Force



Todd M. Keil, Assistant Secretary for Infrastructure Protection (IP), delivered remarks and fielded questions before the U.S. Chamber of Commerce National Security Task Force on September 22, 2010. The Task Force seeks to collaborate with lawmakers and officials to develop policies that shape public and private sector efforts to strengthen homeland security. Assistant Secretary Keil discussed the evolution and future direction of IP while highlighting the importance of partnerships and public and private sector participation.

The Assistant Secretary believes his experience in both the public and private sectors has shaped his approach to IP's mission. As a result, Keil told the crowd that he has "a better understanding of the needs and capabilities of our many stakeholders," which helps him to engage with those partners more effectively.

Keil explained how the IP mission was conceived when the idea for a "Homeland Security Agency" was

proposed by the Hart-Rudman Commission prior to September 11, 2001. The Commission emphasized the importance of establishing a "Critical Infrastructure Protection Directorate" as an integral part of an endorsed homeland security agency and supported the idea of Regional Directors.

Keil explained how the thinking on resilience has evolved to be more applicable to interconnected assets and systems. He said that IP has led the way in the promotion of resilience through initiatives such as the Regional Resiliency Assessment Program (RRAP), which evaluates critical infrastructure on a regional level and identifies opportunities to make systems more resilient. Keil believes RRAP is headed in the right direction as a result of its regional focus and benefit to public and private sector stakeholders.

Keil also discussed the Private Sector Preparedness Accreditation and Certification (PS-Prep) Program. Components across DHS support this voluntary program that enables private sector entities to become certified by a third party as conforming to DHS-adopted preparedness standards. These standards focus on organizational resilience, business continuity management, and emergency management.

IP is planning to collaborate with critical infrastructure partners to develop an implementation plan for the National Infrastructure Protection Plan that identifies milestones for IP and its partners to more effectively track progress in executing agreed-upon goals that are developed in partnership. The Assistant Secretary also described how IP has collaborated with Canada and Mexico over the last year and plans to become more engaged with other international partners. These recent interactions have resulted in a better understanding of interdependencies from a global perspective.

Topics in this Issue

- > Assistant Secretary Keil Delivers Remarks to U.S. Chamber of Commerce National Security Task Force
- > New and Improved ACAMS 3.0 Now Available
- > SLTTGCC Fall Plenary Features Assistant Secretary Keil
- > Hampton Roads Initiates a Regional Critical Infrastructure Protection Program
- > Public-Private Partnerships Enhance Critical Infrastructure Protection Efforts in American Cities
- > TSA's I-STEP Moving Full Speed Ahead
- > GridWise Global Forum Highlights IP's Support to the Energy Sector
- > The Education Facilities Subsector: Supporting Infrastructure Protection for K-12 Schools and Higher Education

New and Improved ACAMS 3.0 Now Available

The ACAMS Project Management Office (PMO) within the Office of Infrastructure Protection (IP) recently finalized the release of ACAMS Version 3.0. The migration of ACAMS users from the previous system to 3.0 took place in a staggered approach over the summer, allowing developers to validate asset and user information to strengthen data integrity within the new system. This latest version includes a variety of system upgrades and added features designed to streamline processes and improve the overall user experience. Below is a summary of a few notable changes that have been incorporated within this release.

Redesigned Interface and Workflow

ACAMS users will notice a change in the way they navigate through the system. The redesigned layout, reorganization of data, and the integration of collapsible menus will make it easier for users to access specific views. The introduction of a new Asset Creation wizard also guides users through a step-by-step process to create and submit an asset for approval, or continue with additional data entry for an existing asset.

In addition, ACAMS 3.0 includes a robust workflow process that enables users to effectively determine the current state of any asset. A detailed workflow history allows users to identify who created, submitted, and approved/rejected an asset, as well as when that action took place. Within this new workflow process, assets will be identified in one of three distinct states of data entry: Asset Assessment (AA), Asset Manager Questionnaire (AMQ), or Buffer Zone Plan (BZP). The various data groupings that existed in the previous versions will also be available; however, Inventory (INV), Initial Asset Visit (IAV), and Rapid Action Assessment & Deployment (RAAD) have been pooled into the new draft type “Asset Assessment,” allowing data to be populated in the INV, IAV, or RAAD tabs and submitted for approval in one step.

Enhanced Viewing and Reporting Capabilities

In an effort to distinguish PCII from non-PCII information, ACAMS 3.0 now has specific asset screens that display only information designated strictly as non-PCII. These data include general asset information such as an asset’s address and the associated responding police, hospital, and fire departments, which have been deemed publicly available data by the DHS PCII Office.

The new system also will improve reporting capabilities by giving users the ability to view relevant data in an organized and exportable format. When required, PCII designations have been added to these reports to allow users to print with minimal effort. In addition to the legacy reports, new reports such as Inventory, AMQ, Options for Consideration, and MSHARRPP+V Analysis are available as well.

Asset Types

The identification of asset-specific types in release 3.0 will allow users to enter additional information for schools, hospitals, police stations, and fire departments. This will help ACAMS users collect and display relevant asset data and establish better situational awareness.

In addition to the many system enhancements that help streamline the data entry, search, and reporting capabilities, a flexible security model has also been implemented to aid in the management of users, roles, teams of users, and groups of assets. New baseline data requirements will also ensure the continuity of data collection efforts across the country.

The ACAMS PMO will continue to collaborate with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to identify, validate, and prioritize requirements for future upgrades. We encourage users to provide suggestions and feedback on current or recommended capabilities to support our stakeholders in the infrastructure protection community. If you have any questions or would like additional information on ACAMS 3.0, please contact acamshelp@hq.dhs.gov.

Home | Asset Search | Reports | Resources | Administration

My ACAMS

Announcements

June 21, 2010 - Welcome to ACAMS v3.0 - The ACAMS PMO is happy to welcome you to the release of ACAMS v3.0. This version includes major revisions designed to streamline processes and improve the overall user experience. Notable changes can be found in the What's New section of this site.

February 05, 2010 - TRIPwire - The Technical Resource for Incident Prevention (TRIPwire) is DHS 24/7 online information-sharing network that combines expert analyses and reports with relevant documents and videos. This information is gathered directly from terrorist sources to help emergency services personnel anticipate, identify, and prevent improvised explosive device (IED) incidents.

ACAMS Help Desk E-mail: acamshelp@hq.dhs.gov Helpline: 1.866.634.1958	ACAMS Project Office E-mail: acams-info@hq.dhs.gov	ICAV Project Office E-mail: icav.info@dhs.gov	PCII Program Office E-mail: pcli-info@dhs.gov Phone: 202.360.3023
--	---	--	---

Recall that by utilizing the ACAMS tool, you have expressly acknowledged and declared that you understand and will protect the confidential nature of this information.

SLTTGCC Fall Plenary Features Assistant Secretary Keil

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) held its 2010 Fall Plenary meeting September 14-16 in Washington, DC. The SLTTGCC is the cross-sector coordinating council for State, local, tribal, and territorial governments and includes representatives from jurisdictions across the country.

Addressing the Plenary, IP Assistant Secretary Keil stated, “We all agree that State, local, tribal, and territorial governments represent the front lines of critical infrastructure protection and are essential to enhancing the resilience of their communities.”

The SLTTGCC drafted a white paper entitled “Aligning Federal CIKR Capabilities to Meet Needs in the Field,” which identifies areas where IP can provide the greatest support to State, local, tribal, and territorial governments. One of the paper’s chief recommendations is to incorporate the State and local perspective into the entire cycle of CIKR program identification and development. Assistant Secretary Keil recognized that this recommendation “is at the core of the reason behind the creation of the SLTTGCC,” and provides “a better understanding and appreciation for where IP needs to go.”

In order to ensure that stakeholder concerns are being heard and considered, Keil announced that IP is conducting a “Stakeholder Input Project” to provide an opportunity for a wide range of stakeholders to give feedback to IP in order to build on best practices and make improvements.

In closing, the Assistant Secretary acknowledged the value of the SLTTGCC and the importance of maintaining an ongoing exchange of information. “Continued engagement and frank, open discussions of this type are essential to maintaining an effective and sustainable partnership.”

Hampton Roads Initiates a Regional Critical Infrastructure Protection Program

The Hampton Roads Planning District Commission (HRPDC) held a workshop in July to explore the benefits, costs, and risks of creating a regional critical infrastructure protection plan. Hampton Roads is home to one of the largest ports in the world, multiple bridges and tunnels that carry millions of people annually, and a thriving regional economy heavily dependent on the defense industrial base.

Recognizing this unique risk landscape, the Hampton Roads region has initiated the Hampton Roads Critical Infrastructure Protection Program (HR CIPP). The workshop was held in conjunction with the Governor’s Office of Commonwealth Preparedness and in collaboration with the University of Virginia Center for Risk Management of Engineering Systems and the James Madison University Institute for Infrastructure and Information Assurance.

The workshop brought together more than 60 partners from local, State, and Federal government, higher education, nonprofits, and owners and operators with a stake in the resilience of the region’s critical infrastructure. The Office of Infrastructure Protection’s (IP) Protective Security Advisor (PSA) for Hampton Roads was instrumental in bringing representatives from U.S. Joint Forces Command and Langley Air Force Base to the workshop.



The HR CIPP workshop offered three sessions designed to familiarize participants with the benefits of working together to develop a sustainable approach to critical infrastructure protection in the Hampton Roads region. The sessions focused on making a value proposition for critical infrastructure protection; identifying key assets, leveraging existing regional organizations, and measuring progress; and setting initial steps, goals, and milestones. In addition, representatives from the Governor’s Office for Commonwealth Preparedness presented the Virginia Critical Infrastructure Protection and Resiliency Strategic Plan. IP representatives from the NIPP Program Management Office and the PSA Program also attended the workshop.

The workshop culminated in participants agreeing to formalize the HR CIPP under the leadership of HRPDC. The University of Virginia Center for Risk Management of Engineering Systems has offered to draft an initial strategy for HR CIPP members to review this fall. In the interim, HRPDC will continue to facilitate regular HR CIPP meetings aimed at producing a regional infrastructure protection strategy that provides value to the region, its businesses, and its citizens.

For more information on the HR CIPP, please contact Richard Flannery, Emergency Management Administrator for HRPDC at (757) 420-8300, or Megan Samford, Critical Infrastructure Coordinator for the Governor’s Office of Commonwealth Preparedness at (804) 371-2602.

Public-Private Partnerships Enhance Critical Infrastructure Protection Efforts in American Cities

Cities from across the Nation are establishing partnerships to enhance business continuity and information sharing between their public, private, and nonprofit sectors. Representatives from Denver, Dallas, and New York City were chosen to share their partnership experiences in a forum co-sponsored by the Partnership Programs and Information Sharing Branch within the Office of Infrastructure Protection (IP) at the 2010 National Urban Areas Security Initiative (UASI) Conference in June. Denver, Dallas, and New York City were chosen because of the ongoing success of their business partnerships, including open and transparent lines of communication and continual identification and engagement of new partners. The common element of success in all three partnerships was ensuring that they continue to provide meaningful benefits to the private sector.

In 2008, Denver formed the Colorado Emergency Preparedness Partnership (CEPP) in preparation for hosting the Democratic National Convention. CEPP coordinates training and exercise programs for the private sector, manages an all-hazards public alert tool, and leads a virtual Business Emergency Operations Center that businesses use to respond to and communicate during critical events. CEPP also has initiated a private sector resource registry to catalog private sector assets for use by emergency managers during a declared disaster.

Dallas established the Dallas Emergency Response Team (DERT) after a tornado killed five people and caused more than \$500 million worth of damage in Fort Worth in 2000. DERT partners with city business leaders to pre-issue emergency perimeter passes to property managers and operates the city's public alert notification system. DERT remains an important mechanism for the public and private sector to collaborate on security and emergency response plans for next year's Super Bowl in nearby Arlington, Texas.

New York City facilitates public-private partnerships through its Office of Emergency Management (OEM). OEM works closely with private sector organizations to ensure that they have the resources and information they need to make decisions before, during, and after an emergency. NYC OEM maintains seats in the City's Emergency Operations Center for private sector umbrella organizations that help coordinate the private sector's planning role as well as response and recovery efforts of specific industries. OEM provides free email alerts to the private sector on non-sensitive emergency situations through a dedicated business portal known as CorpNet.

IP will continue to highlight innovative approaches to public-private partnerships that enhance critical infrastructure protection and resilience. The experiences shared by Denver, Dallas, and New York City at the UASI Conference will be used by IP to assess the effectiveness of its programs in promoting public-private partnerships in the field.

For more information on the three cities' business partnerships, please visit: Denver: <http://www.thecepp.org>; Dallas: <http://dallasalert.org>; New York City: <http://www.nyc.gov/html/oem/html/businesses/businesses.shtml>.

CEPP
Colorado
Emergency
Preparedness



News from the Sectors

TSA's I-STEP Moving Full Speed Ahead

I-STEP | Intermodal Security
Training and
Exercise Program

It has been a busy fiscal year for the Transportation Security Administration's (TSA) Intermodal Security Training and Exercise Program (I-STEP), which provides exercise, training, and security planning tools and services to the transportation community.

I-STEP made impressive progress toward its goal of planning and facilitating 20 exercises in Fiscal Year 2010. To date, the I-STEP team has supported the following exercises:

- **Freight Rail:** Two workshops in St. Louis and one in Memphis to introduce TSA's new Freight Rail Infrastructure Assessment Tool.
- **Highway and Motor Carrier:** Five exercises, including a tabletop exercise on infrastructure in Rutgers; tabletop exercises on school bus security in Albany and Los Angeles; a motor coach tabletop in Northern Virginia; and an advanced tabletop involving critical manufacturing companies that was conducted simultaneously in four locations.
- **Mass Transit:** Three exercises, including a tabletop and seminar in Cleveland focusing on improvised explosive devices (IEDs); and a working group session with transportation representatives from throughout the National Capital Region.

- **Pipeline:** Three tabletop exercises in Boston, Baltimore, and New York City, and an upcoming planned tabletop with the Alyeska Pipeline in Anchorage, AK.
- **Port and Intermodal:** Three joint exercises with the U.S. Coast Guard, including a recovery tabletop in Baltimore, an isolation-and-quarantine tabletop in Boston, and a hazardous materials train derailment tabletop in Long Island.

I-STEP also provided program manager support at the 9th Annual Security Seals Symposium in Houston, TX. The joint TSA and Department of Defense symposium brought together participants from across the country to exchange strategies for enhancing intermodal security. The I-STEP team has worked on several mode-specific initiatives, such as the Ferry Watch Program for Port and Intermodal, strategic planning for Highway and Motor Carrier, and a bridge risk tool for Freight Rail.

Additionally, I-STEP is currently developing multi-modal resources for all transportation security stakeholders, including a comprehensive matrix outlining transportation security training resources. TSA recently convened a working group to update and enhance I-STEP's exercise planning and tracking tool, the Exercise Information System (EXIS). Once released, EXIS will provide a suite of scalable resources designed to serve transportation partners in all modes. To learn more about I-STEP products and services, email a TSA modal representative at ISTEP@dhs.gov.

GridWise Global Forum Highlights IP's Support to the Energy Sector

On September 22, 2010, Assistant Secretary Keil gave a speech at the GridWise Global Forum in Washington, D.C. Mr. Keil discussed the Office of Infrastructure Protection's (IP) ongoing initiatives to protect and enhance the resilience of the electric grid. Specifically, Mr. Keil spoke about the Buffer Zone Protection Program (BZPP), which provides funding to State and local law enforcement to increase the preparedness of jurisdictions responsible for the safety of communities surrounding high-priority critical infrastructure assets. IP has conducted assessments of 623 Energy Sector assets and has allocated approximately \$45 million in BZPP grant funds to first responders in jurisdictions surrounding critical Energy Sector assets. To help mitigate the all-hazard risks facing the Energy Sector, IP also sponsors security clearances for private sector representatives so they can participate in classified threat briefings and working group meetings.

Through its collaboration with the Energy Sector, IP has helped to provide an effective arena to identify and discuss vulnerabilities as well as to assess, compare, and manage risks.

The Education Facilities Subsector: Supporting Infrastructure Protection for K-12 Schools and Higher Education

Many protective efforts for the Education Facilities (EF) Subsector involve two key programs that support infrastructure protection, the Readiness and Emergency Management for Schools (REMS) and the Emergency Management for Higher Education (EMHE) discretionary grant programs. These protective programs are aligned with EF's goal that all schools have comprehensive, all-hazards emergency management plans based on the four phases of emergency management to enhance school safety, minimize disruption, and ensure continuity of the learning environment. These grant programs also build on over a decade of school emergency management efforts by the Department of Education's Office of Safe and Drug-Free Schools (OSDFS), where the EF Subsector-Specific Agency is housed. Following are updates on these key protective programs for FY 2010.

Readiness and Emergency Management for Schools (REMS) Discretionary Grant Program

The REMS discretionary grant program is the primary program administered by OSDFS that supports infrastructure protection for K-12 schools. On August 19, 2010, OSDFS announced the REMS grant recipients for FY 2010, comprising 98 grants totaling \$28.8 million. On September 30, 2010, OSDFS announced an additional five grant awards under this program, bringing the total amount awarded in FY 2010 to \$30,117,179.

The REMS grant program provides funding to local educational agencies (LEAs) to create, strengthen, or improve emergency management plans at the district and school building levels through training for school personnel and coordination with local community partners. Grantees must agree to develop plans that consider the communication, transportation, and medical needs of students and staff with disabilities and support implementation of the National Incident Management System (NIMS). In addition, grantees must develop plans for communicating emergency policies to parents and guardians; improving LEA capacity to sustain the emergency management process; and preparing the LEA for a possible infectious disease outbreak, such as pandemic influenza.

Additional grant requirements include coordinating with the State or local homeland security plan and developing a written food defense plan that is designed to safeguard the school district's food supply. Since the establishment of this discretionary grant program in FY 2003, the Department of Education has awarded over \$230 million in grants to 820 school districts, many of which support a large number of schools in their emergency management efforts.

For more information on the REMS discretionary grant program, please visit: <http://www.ed.gov/news/press-releases/us-department-education-awards-288-million-school-districts-improve-readiness-an>

Emergency Management for Higher Education (EMHE) Discretionary Grant Program

In 2008, OSDFS, in collaboration with the Department of Health and Human Services' (HHS) Substance Abuse and Mental Health Services Administration (SAMHSA), developed a new discretionary grant program to assist institutions of higher education in developing their emergency management plans. On September 27, 2010, OSDFS announced the EMHE grant recipients for FY 2010 (<http://www.ed.gov/news/press-releases/us-department-education-awards-more-92-million-institutions-higher-education-eme>). OSDFS awarded 17 grants, totaling \$9.2 million. On September 30, 2010, OSDFS announced one additional award of \$424,624, bringing the total FY 2010 awards to \$9,667,817.

Specifically, the EMHE grant program provides funding to institutions of higher education to develop (or review and improve) and fully integrate all-hazards, campus-based emergency management planning efforts. EMHE grantees must agree to do the following:

- Train campus, staff, faculty, and students in emergency management procedures;
- Coordinate emergency plans with all campus offices and departments, as well as with local and State emergency management efforts;
- Develop a written plan that incorporates medical, mental health, communication, and transportation needs to include those with disabilities, special needs, and other circumstances into emergency protocols;
- Develop or update a written plan that prepares the campus for a possible infectious disease outbreak;
- Develop or enhance a written plan for preventing violence by assessing and addressing the mental health needs of students, staff, and faculty who may be at risk of causing harm to self or others; and
- Develop or update a written continuity of operations plan that would enable the campus to maintain and/or restore key educational, business, and other essential functions following an emergency.

Since the establishment of this discretionary grant program in FY 2008, the EMHE program has awarded over \$28 million in grants to 61 higher education institutions.

> Resources Available for DHS Critical Infrastructure Partners

Infrastructure Protection (IP) sponsors a free online NIPP training course at <http://training.fema.gov/EMIWeb/IS/crslist.asp>. IP also has a trade show booth available for sector use. Please contact NIPP@dhs.gov for information on IP participation and/or exhibition at an upcoming sector event or to schedule a trained speaker for your event.

> Implementation Success Stories

IP continues to seek NIPP and/or SSP implementation success stories from the sectors to be shared with other critical infrastructure partners. Please submit suggestions or brief write-ups to NIPP@dhs.gov.

> NIPP News

The NIPP News is produced by the Office of Infrastructure Protection. NIPP partners are welcome to submit input. To submit information for inclusion in upcoming issues, please contact NIPP@dhs.gov. Recipients of this newsletter are encouraged to disseminate it further to their critical infrastructure partners.

- > Learn more about the DHS critical infrastructure protection program at www.dhs.gov/criticalinfrastructure.