Homeland Security

NIPP NEWS

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 57: JANUARY 2011

Critical Infrastructure Activities and Events

IP Moves to Strengthen Regional Resilience and Implement Risk-Based Programmatic and Budgetary Planning

On November 30, President Obama proclaimed December 2010 "Critical Infrastructure Protection Month." The proclamation reaffirmed America's commitment to critical infrastructure protection and resilience.

During CIP Month, IP reached out to partners, stakeholders, and the public about the importance of:

- Ensuring that critical infrastructure is resilient against all hazards;
- Fostering information sharing among government and private sector partners; and
- Using risk management best practices to strengthen critical infrastructure protection and resilience.

During his keynote address on December 2 at the 2010 CIP Congress in Washington, D.C., Assistant Secretary Todd M. Keil said:

"The threat picture will likely continue to evolve in the next year, and the programs of the Office of Infrastructure Protection and our partners will evolve accordingly. ... [W]e will work with our national-level partners to build and strengthen regional partnerships so that our local communities have the information that they need to make decisions."

Initiatives highlighted during the month include the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), the Private Sector Preparedness Accreditation and Certification Program (PS-Prep), the Regional Resiliency Assessment Program (RRAP), and IP's Critical Infrastructure and Key Resources Information Sharing Environment. PS-Prep is designed as a voluntary program where private sector entities can be certified as compliant with particular preparedness standards. RRAP assessments identify regional critical infrastructure dependencies and evaluate systems' abilities to recover quickly. RRAPs have convened all levels of government and the private sector and have fostered unprecedented information sharing.

Also highlighted was IP's collaboration with State and local fusion centers. A three-day fusion center workshop in mid-December focused on physical and cybersecurity, regional partnerships, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). NSI is a multiagency Federal effort to train State and local law enforcement to recognize behaviors and indicators related to specific threats and terrorism-related crime, standardize how those observations are documented and analyzed, and enhance the sharing of reports with DHS and the FBI. Secretary

Topics in this Issue

Napolitano's national If You See Something, Say Something™ campaign is part of the NSI, and IP and its partners continue to play a key role in that campaign. [See related article below.]

Strengthening Risk-Based Planning and Programming. Last fall, IP established an office-wide task force to better align its risk analysis and planning processes. The task force, which is leading the CIRMEI, is transforming the National Annual Report (NAR) to play a significant role in helping IP and its partners assess how to get closer to achieving shared goals by identifying risk reduction opportunities. The NAR will now include specific outcomes that IP will seek to achieve—as aligned with statutes, the National Risk Profile, the Quadrennial Homeland Security Review, the NIPP, and more—as well as metrics to assess IP's progress in achieving those outcomes. This information and analysis will be included in the 2011 NAR.

Based upon the data in the National Annual Report, NIPP partners will develop a Critical Infrastructure Risk Management Plan to identify specific actions to address gaps and risk reduction opportunities over a three-year period. This plan will directly inform IP's resource planning and provide a clear roadmap for IP and its partners to reduce risks to critical infrastructure. Already, IP's Partnership and Outreach Division, Sector-Specific Agency Executive Management Office, and Infrastructure Analysis and Strategy Division are working with partners to begin transforming these documents into actions so that the NIPP can truly be the foundation for improvements in infrastructure protection and resilience.

This integrated process puts DHS on the path toward implementing a risk-informed resource allocation process for critical infrastructure protection and resilience. By working with the private sector and intergovernmental entities on this integrated effort, IP and its partners will have a common understanding of the greatest risks facing critical infrastructure assets, systems, and networks; the effectiveness of risk reduction efforts; and how the partners will collaboratively achieve an acceptable level of risk over time.

As Mr. Keil stated at a meeting of the Military Operations Research Society in November: "... with a well-coordinated, risk-based approach, we will be more prepared to answer the question of how well we are doing—as a nation—at mitigating risk to critical infrastructure."

Posted Blogs and Tweets. CIP Month themes were highlighted in guest blogs on The Blog @Homeland Security:

- December Is Critical Infrastructure Protection Month
- Enhancing Critical Infrastructure Resilience
- An Agenda for Secure and Resilient Critical Infrastructure

Announcements were also posted on the DHS Twitter account: @DHSJournal for followers of "infrastructure" and "resilience."

IP Participates in the Nationwide Suspicious Activity Reporting Initiative

Every day, citizens, private security officers, and law enforcement officers at all levels of government observe behaviors that are suspicious. What might seem insignificant (for instance, taking pictures of a national landmark), when combined with other actions and activity, may indicate the possibility of criminal or even terrorist activity. We know that al Qa'ida members involved in the September 11th attacks prepared not only in far-off Afghan training camps, but also in Minnesota and at flight schools in Florida. Often, the actions of terrorists arouse the suspicion of their neighbors and law enforcement officers. We now know that there is a role for all of us to play in preventing terrorism. This is especially true for the Nation's critical infrastructure owners and operators. The DHS Office of Infrastructure Protection (IP) is working closely with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) to expand the connection between critical infrastructure and the SAR process used at State and local fusion centers across the country.

What is NSI?

The October 2007 National Strategy for Information Sharing called for the establishment of a "unified process for reporting, tracking, and accessing [SARs]," in a manner that rigorously protects the privacy and civil liberties of Americans—what is now referred to as the Nationwide SAR Initiative (NSI). NSI is an historic partnership among Federal, State, local, and tribal agencies, led by the Department of Justice's Bureau of Justice Assistance, working in close partnership with DHS; the Federal Bureau of Investigation; Office of the Program Manager, Information Sharing Environment (PM-ISE); and the Department of Defense. NSI establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SARs, referred to as the SAR process. The SAR process is a behavior-based, evaluative approach grounded in known precursor activity. The process focuses on what law enforcement agencies have been doing for years—

gathering information on behaviors and incidents associated with crime to "connect the dots"—but establishes a standardized approach to sharing information. The goal is to detect and prevent criminal activity, including activity that may be associated with domestic and international terrorism.

IP's Contributions to NSI

The NSI process will be strengthened by IP's work to bring critical infrastructure owners and operators into the fold. IP assigned Steve King as Senior Advisor to the NSI, to lead the integration of critical infrastructure into the NSI effort. The National Infrastructure Coordinating Center (NICC) operates 24 hours a day, 7 days a week, 365 days a year to facilitate coordination and information sharing with owners and operators. The NICC produces consolidated critical infrastructure reports for incorporation into the Federal interagency DHS common operating picture, and serves as a resource for critical infrastructure security professionals nationwide.

In 2010, Secretary Napolitano launched a national "If You See Something, Say Something™" campaign to raise public awareness of indicators of terrorism, crime, and other threats and highlight the importance of reporting suspicious activity to the proper authorities. This campaign was launched in conjunction with the roll-out of NSI.

The expansion of NSI to encompass critical infrastructure owners and operators will enhance the initiative and provide law enforcement with another tool to combat crime and terrorism. For more information about the NSI, visit nsi.ncirc.gov or contact nsiinformation@ncirc.gov.

Did you SEE something suspicious on your way to a sporting event?
Then SAY something to local authorities to make it right.
If you are attending a sporting event, help keep America safe.
Report suspicious activity.
Call 1-888-NYC-SAFE
(692-7233)
if you SEE something SAY something™
Homeland Security
US OPEN
Proud to partner with the Department of Homeland Security to keep America safe.

Virtual Meetings Increase Stakeholder Participation in IP Education and Training Opportunities

IP supports the Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE), which is making substantial progress in providing useful critical infrastructure protection and resilience information to an increasing number of sector partners. One tool used to accomplish this goal is the Homeland Security Information Network (HSIN) Connect, which IP has leveraged to deliver training, distribute timely information to partners across the country, and increase partner participation in sector meetings.

Webinars and Web-based conferencing capability help the sectors and IP to provide free training and informational briefings on general and sector-specific topics. Two recent training successes that reached an expanded number of stakeholders include the *Surveillance Detection Awareness Virtual Roundtable* in September and *The Evolving Threat and What You Can Do* Webinar in November. The Evolving Threat event combined a threat briefing for qualified sector members and a pre-recorded presentation by subject matter experts (SMEs) on protective measures and surveillance detection techniques. Approximately 1,000 stakeholders participated in the live event and the recorded SME presentation, IP Protective Measures, has been viewed over 2,600 times. This event was a joint effort between IP and the DHS Office of Intelligence and Analysis.

The virtual roundtable interactive event included a live discussion between participants from the Commercial Facilities Sector and experts on surveillance detection awareness. Several videos demonstrating types of surveillance were shown, responses were polled, and questions from the attendees were discussed by the experts in a roundtable forum. The session trained participants to identify activities related to surveillance, recognize behaviors that may indicate potential terrorist activities, and report suspicious behavior. The training also provided solutions to assist owners and operators with identifying suspicious activities at their facilities and promoting best practices that can contribute to safer, better-prepared work environments. Approximately 1,000 stakeholders participated in the live event and the recorded On the Job training video has been viewed on HSIN over 4,000 times. Several IP divisions collaborated in this effort.

Sectors have stressed the need to reach partners and stakeholders who are unable to attend meetings in person. Some sectors, such as Chemical, Commercial Facilities, and Nuclear, have already used HSIN Connect to enable virtual participation in sector quarterly council and workgroup meetings. In addition, some sectors have taken advantage of the technology's "polling" capability, which can engage audience input and allow sector leadership to learn more about stakeholder needs and priorities. For more information on the CIKR Information Sharing Environment, contact CIKR.ISE@dhs.gov.

SLTTGCC Expands Outreach through Alliance Networks

State, local, tribal, and territorial (SLTT) governments have a unique role in protecting critical infrastructure and public safety and ensuring that communities and businesses within their jurisdiction receive essential services. The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC, Council)—formed in 2007—fully integrates SLTT governments as active participants into the national critical infrastructure planning process. Its unique perspective informs and improves national efforts to increase protection and resilience at all levels of government and with critical infrastructure owners and operators.

Working solutions that are solidly grounded in actual operations, training, and exercise experience are integral to helping jurisdictions institutionalize learning, implement lessons learned, and use resources more effectively during tough budgetary times. The Council, with support from DHS, shares these best practices by producing studies that cover a variety of critical infrastructure topics, such as State partnership characteristics, State critical infrastructure capabilities, State sunshine laws, and fusion center capabilities. These studies are distributed through the Alliance Networks established by the Council. Current Alliance Network partners include State Homeland Security Advisors, State Critical Infrastructure Protection Coordinators, State Emergency Management Directors, IP's Protective Security Advisors, Urban Areas Security Initiative officials, National Guard officers, State railroad associations, Government and Sector Coordinating Council Chairs, and SLTT subject matter experts.

The Council leverages the full spectrum of Alliance Networks by sponsoring opportunities to discuss effective practices, develop partnerships, and share timely information. For example, the Council used Alliance Networks to inform key SLTT partners about a Webinar on IP's Buffer Zone Protection Program, thereby tripling the number of participants.

The Council's use of Alliance Networks supports IP's regional capability for disseminating sector partnership products and information on protection and resilience programs. By building trusted communication pathways and strengthening relationships, the Alliance Networks assist with regional deployment of critical infrastructure resources and tools.

Inquiries about the SLTTGCC, its activities, or participation in the Alliance Networks may be sent to SLTTGCC@dhs.gov. For general information about the SLTTGCC, visit http://www.dhs.gov/files/committees/gc_1177096698216.shtm.

IP and Regional Personnel Celebrate "GIS Day" with State and Local Officials

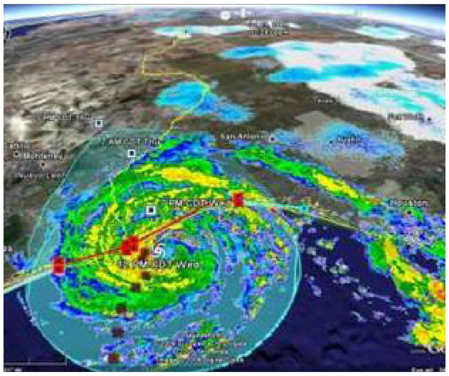
On November 17, 2010, IP officials and regional Information Exchange Brokers (IEBs) from the Homeland Infrastructure Foundation Level Data (HIFLD) program celebrated "Geographic Information Systems (GIS) Day" at several events across the country. The IEBs are part of the HIFLD to the Regions program, which is a collaborative effort between DHS and the National Geospatial-Intelligence Agency (NGA) as the regional support to the HIFLD working group. Working alongside Federal, State, and local partners, the IEBs coordinate with key mission partners to identify and share critical infrastructure data, inform about available geospatial resources, and assist with DHS and NGA-related efforts to further the mission of homeland security prevention, protection, response, and recovery.

What Is GIS Day?

GIS Day is part of Geography Awareness Week, which was started in 1987. The goal of GIS Day is to "provide an international forum for users of GIS technology to demonstrate real-world applications that are making a difference in our society. More than 80 countries participated by holding events such as user conferences, corporate open houses, hands-on workshops, community expos, school assemblies, and more." (http://www.gisday.com). To celebrate GIS Day, IP personnel and IEBs participated in the 2010 Hampton Roads GIS Day in Norfolk, VA; the 10th Annual Mid-South GIS Conference in Germantown, TN; the Army North Situational Awareness Conference in San Antonio, TX; the Rocket City GIS Conference in Huntsville, AL; and the Seven Hills Regional User Group Workshop in Tallahassee, FL.

Attendees at these events included mission partners from FEMA, the U.S. Geological Survey, the U.S. Army, the U.S. National Guard, State emergency management organizations, State emergency operations centers, public utility organizations, GIS user groups, GIS councils, academia, and the private sector.

Why Is GIS Day Important to the Infrastructure Protection Mission?



GIS Day events supported IP's recent initiatives to engage and support partners in mitigating risk to critical infrastructure, enhancing resilience, and strengthening regional partnerships. IP reached out to key stakeholders to promote the use of GIS in critical infrastructure protection and emergency response, as well as provide overviews of the Homeland Security Information Network (HSIN) GIS Community of Interest, geospatial tools such as the Integrated Common Analytical Viewer (iCAV) and DHS Earth, and the Homeland Security Infrastructure Protection (HSIP) geospatial datasets. At the IP information booth, IP personnel and IEBs engaged with attendees on data collection, data protection, private sector partnerships, and fusion center roles in GIS.

For more information on the HIFLD Group, visit: http://www.hifldwg.org/. For information on iCAV and DHS Earth, visit: https://icav.dhs.gov/

Version 4 of the Infrastructure Data Taxonomy Coming Soon

IP has recently completed the biennial revision of the Infrastructure Data Taxonomy (IDT), with an upcoming release of the IDT version 4 in early 2011. Federal, State, and local governments and the private sector are encouraged to use the taxonomy to facilitate consistent communication, categorization, and dissemination of infrastructure information.

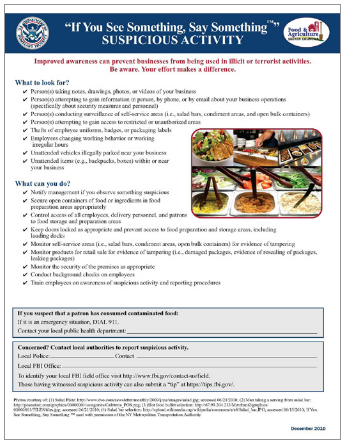
The taxonomy establishes a standard vocabulary so that those who own, operate, protect, and defend the Nation's infrastructure can communicate about it in a consistent way. The IDT also facilitates more efficient data integration and transfer of information between systems; thus, it is the foundation for the many DHS IT tools and systems that identify, collect, and catalog national critical infrastructure.

IP has produced three previous versions of the IDT, with input provided by Sector-Specific Agencies, private sector partners, State and local governments, and other Federal agencies.

For additional information on the taxonomy and to register to receive e-mail updates, visit http://www.dhs.gov/files/publications/gc_1226595934574.shtm. If you have any questions or would like additional information on the IDT, please e-mail IDT@hq.dhs.gov.

News from the Sectors

Food and Agriculture Sector—Suspicious Activity Awareness for Food Service and Retail Food Establishments



"If You See Something, Say Something™"
SUSPICIOUS ACTIVITY

Improved awareness can prevent businesses from being used in illicit or terrorist activities. Be aware. Your effort makes a difference.

What to look for?

- ✔ Person(s) taking notes, drawings, photos, or videos of your business
- ✔ Person(s) attempting to gain information in person, by phone, or by email about your business operations (specifically about security measures and personnel)
- ✔ Person(s) conducting surveillance of self-service areas (i.e., salad bars, condiment areas, and open bulk containers)
- ✔ Person(s) attempting to gain access to restricted or unauthorized areas
- ✔ Thefts of employee uniforms, badges, or packaging labels
- ✔ Employees changing working behavior or working irregular hours
- ✔ Unattended vehicles illegally parked near your business
- ✔ Unattended items (e.g., backpacks, boxes) within or near your business

What can you do?

- ✔ Notify management if you observe something suspicious
- ✔ Secure open containers of food or ingredients in food preparation areas appropriately
- ✔ Control access of all employees, delivery personnel, and patrons to food storage and preparation areas
- ✔ Keep doors locked as appropriate and prevent access to food preparation and storage areas, including loading docks
- ✔ Monitor self-service areas (i.e., salad bars, condiment areas, open bulk containers) for evidence of tampering
- ✔ Monitor products for retail sale for evidence of tampering (i.e., damaged packages, evidence of resealing of packages, leaking packages)
- ✔ Monitor the security of the premises as appropriate
- ✔ Conduct background checks on employees
- ✔ Train employees on awareness of suspicious activity and reporting procedures

If you suspect that a patron has consumed contaminated food:
If it is an emergency situation, DIAL 911.
Contact your local public health department: ____________________

Concerned? Contact local authorities to report suspicious activity.
Local Police: ____________ Contact ____________
Local FBI Office: ____________________
To identify your local FBI field office visit http://www.fbi.gov/contact-us/field.
Those having witnessed suspicious activity can also submit a "tip" at https://tips.fbi.gov/.

Photos courtesy of: (1) Salad Plate: http://www.dvo.com/newsletter/monthly/2009/june/images/salad.jpg; accessed 06/21/2010; (2) Man taking a serving from salad bar: http://posnation.com/graphics/00000001/categories/Cafeteria_POS.png; (3)Hot food buffet selection: http://67.99.204.233/Merchant2/graphics/00000001/TILES/tiles.jpg; accessed 06/21/2010; (4) Salad bar selection: http://upload.wikimedia.org/wikipedia/commons/e/e8/Salad_bar.JPG; accessed 06/15/2010; If You See Something, Say Something ™ used with permission of the NY Metropolitan Transportation Authority

December 2010

To improve suspicious activity awareness and reporting within the Food and Agriculture (FA) Sector, the sector leadership worked with partners in DHS and other Federal agencies to develop a one-pager highlighting indicators of suspicious activity and recommended protective measures. These efforts are part of the "If You See Something, Say Something™" Campaign. This document is the first in a series of outreach materials targeted for food service and retail food establishments.

The FA Sector suspicious activity one-pager is intended to be posted in work areas within food service and retail food establishments to make employees aware of what they should be looking for each day and what actions they should take if they observe something suspicious. The sector also wants to encourage managers to raise awareness during staff meetings and other training opportunities. The FA Sector greatly appreciates any assistance partners can provide in the further distribution of this document to food service and retail food establishments.

Currently, the document is available only in a PDF electronic format. The FA Sector is working to translate it into Spanish. Printed copies with English on one side and Spanish on the other will be available later this year.

In addition, two "For Official Use Only" (FOUO) conference calls were held on December 17, 2010, to discuss recent efforts to increase public/private sector awareness of potential food supply threats and indicators of suspicious activity. One call included select private sector representatives from the FA and Commercial Facilities Sectors, with 102 participants. The second call included the FA Sector Government Coordinating Council and select representatives from the Healthcare and Public Health (HPH) Sector, with 59 participants. Agenda topics included an FOUO Evolving Threat briefing; an FOUO presentation on Potential Indicators and Protective Measures; an overview of DHS' "If You See Something, Say Something™" campaign; and updates from sector leadership on outreach efforts in the FA and HPH Sectors.

For additional information on the FA Sector's efforts regarding suspicious activity awareness, contact LeeAnne Jackson (LeeAnne.Jackson@fda.hhs.gov) or Jessica Pulz (Jessica.Pulz@osec.usda.gov).

Healthcare and Public Health Sector Expands Information Sharing

Information sharing has been the primary focus for many infrastructure protection partners and stakeholders over the past year. Many sectors have taken great steps in enhancing the capabilities and the information presented on their Homeland Security Information Network (HSIN) portals to provide relevant and timely information to sector and cross-sector constituents. In an effort to expand awareness, membership, and the knowledge base on the Healthcare and Public Health (HPH) Sector portal, sector leadership, members, and support staff have developed and distributed a HSIN-HPH Media Pack. The dissemination of this information has assisted the sector in obtaining more than 1,200 members and provides tangible documentation for companies, organizations, and associations to distribute in routine communications.

The HPH Sector Media Pack includes the following:

- 150-word news article;
- 400-word news article;
- Letter from an association to its members;
- Letter to an association POC;
- HSIN-HPH Flyer; and
- HSIN-HPH business cards (optional).

If you are interested in receiving any of this information to pass along to Healthcare and Public Health community members or have any questions, please contact Steve Curren (Stephen.Curren@hhs.gov) or Briana Stephan (Briana.Stephan@hhs.gov). For your information, the 400-word article is provided below.

Valuable Resources and Tools Available Through Information-Sharing Portal

The newly revamped HSIN-HPH portal offers a wealth of information-sharing and preparedness resources for HPH Sector stakeholders.

What is HSIN-HPH?

HSIN-HPH is the nation's primary Web portal for public/private collaboration to protect HPH Sector critical infrastructure. It is the primary means by which the Departments of Homeland Security (DHS) and Health and Human Services (HHS) share sensitive but unclassified (SBU) information with their trusted partners. Through HSIN-HPH, users have access to:

- Timely, relevant and actionable information about threats, vulnerabilities, security, policy, cybersecurity, and incident response and recovery activities affecting the healthcare and public health community;
- Alerts and notifications of credible threats;
- Best practices for protection and preparedness measures for HPH stakeholders;
- Critical infrastructure preparedness and resiliency analysis and research products; and
- Tools for communication and collaboration with other subject matter experts.

How Can HSIN-HPH Help You?

HSIN-HPH was designed specifically to meet the needs of those responsible for collecting, analyzing, sharing, and using information for the protection of our nation's HPH infrastructure. In addition to providing access to its vast document library, HSIN-HPH can help HPH stakeholders communicate through resources such as a Webinar tool for live, virtual presentations, a discussion board for collaboration, and a members-only area for private sector users to share sensitive information.

HSIN-HPH in Action: H1N1 Pandemic

During an emergency, an incident-specific site is established on HSIN-HPH to share timely and relevant information with sector partners. Such an incident site was established during the 2009-2010 H1N1 flu pandemic. Unique content, provided by both government (DHS and HHS) and private sector (corporate and association) partners, included important contact information, Federal situation reports, information on H1N1 impacts on HPH infrastructure and supply chain, sector teleconference announcements, and guidance for private sector organizations. The H1N1 incident Web site received heavy traffic during the flu season, and significantly enhanced the HPH Sector's ability to share information with sector partners and to better prepare and respond to the H1N1 pandemic.

How to Access HSIN-HPH

HSIN-HPH is available to qualified members of the HPH community. To request access to HSIN-HPH, visit https://connect.hsin.gov/hph/event/registration.html and complete the online application form. For questions regarding HSIN-HPH, contact the HHS Critical Infrastructure Protection Program Office at cip@hhs.gov.

Education Facilities Subsector Hosts a Meeting of School Security Officials and Safe School Center Directors

School Security Officials/School
Safety Center Directors Meeting
STOP
SCHOOL
November 15-17, 2010
Orlando, FL

The U.S. Department of Education (ED) held a School Security Officials and Safe School Center Directors Meeting on November 15-17, 2010, in Orlando, Florida. The meeting covered a wide variety of issues ranging from trafficking and radicalization of youth, to bullying and the pros and cons of using cell phones in schools. Attendees learned about issues faced by other districts and shared best practices on how they could be addressed. Approximately 45 school security officials and safe school center directors from across the Nation attended the meeting.

The most common issues cited by districts included budget/resource cuts and staff lay-offs; the need for cultural competency to combat youth radicalization; bullying; derogatory social media postings; sexting; suicide (by parents, teachers, and students); gangs; and violence on school buses and at bus stops.

Participants were most interested in learning more about additional training for district staff on violent extremism, ways to address bullying, and policies related to the use of technology.

Subject matter experts offered useful training on issues facing schools, including Human Trafficking (Federal Law Enforcement Training Center); Office of Civil Rights Guidelines on Bullying and Harassment (Office for Civil Rights); The Use of Technology in Bullying and Harassment (Orange County Public Schools Security Services); and Youth Radicalization and Violent Extremism (National Counterterrorism Center). To learn more, contact Sara Strizzi at Sara.Strizzi@ed.gov.

> 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.