



# ESF 15 Business / Nonprofit Update

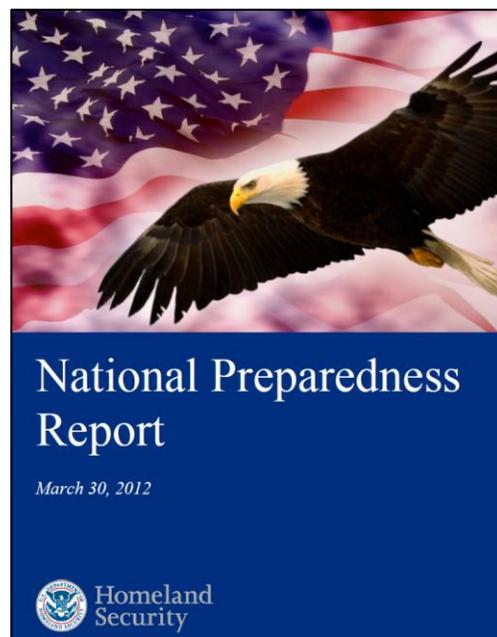
Produced by Emergency Support Function 15 – External Affairs

May 2012

## ITEMS OF INTEREST FOR ESF 15

### National Preparedness Report

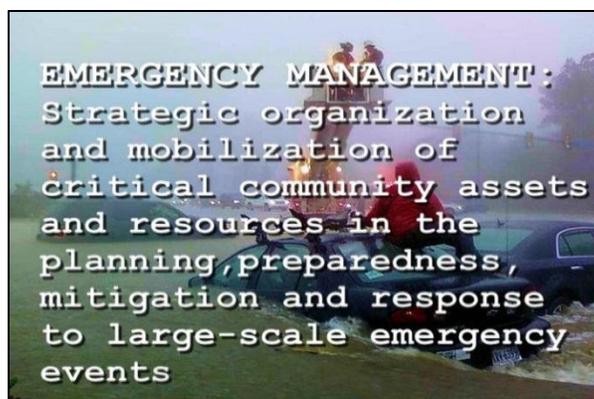
The Federal Emergency Management Agency (FEMA) and its partners recently released the National Preparedness Report (NPR). The report identifies significant progress the nation has made in areas of prevention, protection, mitigation, response and recovery. Overall the report found that the nation has increased its collective preparedness, not only from external threats, but also for natural and technological hazards that face its communities. The report was developed to meet the requirements of “Presidential Policy Directive 8/PPD-8: National Preparedness.” PPD-8 is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics and catastrophic natural disasters. The NPR focuses on five mission areas: Prevention, Protection, Mitigation, Response and Recovery, as outlined in the National Preparedness Goal released in October 2011. Within these mission areas are 31 core capabilities central to preparedness. The NPR assesses each of these 31 core capabilities. Overall, the NPR found the nation has made significant progress in enhancing preparedness and identifies several significant areas of national strength. FEMA developed the NPR in close coordination with leaders of federal departments and agencies, and the report reflects inputs from state, local, tribal and territorial governments, private and nonprofit sector partners, and the general public. Data was also integrated from the 2011 State Preparedness Reports, which are state-wide self-assessments of the core capabilities submitted by all 56 U.S. states and territories through a standard survey. FEMA also conducted research to identify any recent, independent evaluations, surveys and other data related to the core capabilities. The National Preparedness Report is the next step in implementing PPD-8. Since the directive was signed by the President in March 2011, FEMA and its partners have released the first edition of the National Preparedness Goal, the National Preparedness System description and the working drafts of the National Planning Frameworks. For more information on PPD-8 and to download the report, visit [www.fema.gov/ppd8](http://www.fema.gov/ppd8) or contribute your ideas at <http://fema.ideascale.com>.



### Emergency Management Featured on “County Magazine”

The Fairfax County Office of Emergency Management (OEM) is featured on the June edition of Channel 16’s “County Magazine.” The magazine feature provides an overview of emergency management and what the Fairfax County Office of Emergency Management does. The program is available for viewing on cable Channel 16 during the month of June every Sunday at 1:30 p.m., Monday at 6:30 p.m., Tuesday at 6:30 p.m., Thursday at 10:30 p.m., Friday at 3:30 p.m. and Saturday at 3:30 p.m. and via live video streaming at [www.fairfaxcounty.gov/cable/channel16/asx/ive\\_stream.asx](http://www.fairfaxcounty.gov/cable/channel16/asx/ive_stream.asx).

It can also be seen at anytime on the county’s video on demand service at [www.fairfaxcounty.gov/cable/channel16/asx/county\\_mag.asx](http://www.fairfaxcounty.gov/cable/channel16/asx/county_mag.asx) or on the Fairfax County YouTube



Channel at <http://youtu.be/MDBFEOFm79A>. For more information about OEM or emergency preparedness, call 571-350-1000, TTY 711; email [oem@fairfax\\_county.gov](mailto:oem@fairfax_county.gov).

### **Several Huge Wildfires Make Spring Fire Season Memorable**

With more than 43,000 acres burned since Jan. 1, officials with the Virginia Department of Forestry (VDOF), the U.S. Forest Service and the National Park Service were grateful for the late April rains and the official end of spring fire season. Seven large wildfires on National Forest System land began Easter Sunday and Monday and resulted in much of the burned acreage. The Virginia Department of Forestry responded to 355 additional wildfires that burned 6,556 acres since Jan. 1. The National Park Service had a total of 10 fires that burned on 11 acres on the Blue Ridge Parkway and in Shenandoah National Park. The official end of spring fire season in the Commonwealth occurred at 11:59 p.m. on April 30. Each year, from Feb. 15 through April 30, Virginia experiences weather conditions (low humidity, limited precipitation, winds, downed tree limbs, dried leaves, brown grass) that hasten the spread of wildfires. Since the 1940s, Virginia's 4 p.m. burning law has helped reduce the risk of wildfires by preventing open burning before 4 p.m. each day during this 75-day period. (**Note: The state Air Pollution Control Board prohibits open burning in the metropolitan areas of Northern Virginia, Richmond, Hampton Roads, Roanoke and Winchester during the months of May through September. This ban is in effect 24 hours a day.**) "This was definitely an interesting spring," said John Miller, VDOF's director of resource protection. "We had quite a few very large fires and several of them we suspect are arson. There are a lot of people around the state who hope that we never see so many large fires in one week again. And, just because the "official" fire season has ended, we remind Virginians to still be aware of the wildfire threat that exists throughout the year."

[http://www.dof.virginia.gov/press/nr/2012/04-30\\_SpringFireSeasonEnds.htm](http://www.dof.virginia.gov/press/nr/2012/04-30_SpringFireSeasonEnds.htm)

### **More Than 300,000 Complaints of Online Criminal Activity Reported in 2011**

The Internet Crime Complaint Center (IC3) has released the 2011 Internet Crime Report -- an overview of the latest data and trends of online criminal activity. According to the report, 2011 marked the third year in a row that the IC3 received more than 300,000 complaints, a 3.4 percent increase over 2010. The reported dollar loss was \$485.3 million. As more Internet crimes are reported, IC3 can better assist law enforcement in the apprehension and prosecution of those responsible for perpetrating Internet crime. In 2011, IC3 received and processed, on average, more than 26,000 complaints per month. The most common complaints received in 2011 included FBI-related scams – schemes in which a criminal poses as the FBI to defraud victims – identity theft, and advance-fee fraud. The report also lists states with the top complaints, and provides loss and complaint statistics organized by state. It describes complaints by type, demographics, and state.

<http://www.fbi.gov/news/pressrel/press-releases/ic3-2011-internet-crime-report-released>

### **Commonwealth Public Safety Memorial**

The design for a statewide memorial remembering public servants who have died in the line of duty in Virginia was unveiled this month. Governor Bob McDonnell and members of the Virginia Public Safety Foundation, which will oversee building of the memorial, held a press conference at the Darden Memorial Garden, Capitol Square, Richmond to unveil the design for the Commonwealth Public Safety Memorial and officially kick off the campaign to build Virginia's Monument to Heroes. Virginia is one of only six states in the nation lacking a monument to public safety heroes who have given their lives in the line of duty.

<http://www.vpsf.org/Memorial.html>

### **New American Red Cross Online Tools Help Businesses and Schools Prepare for Emergencies**

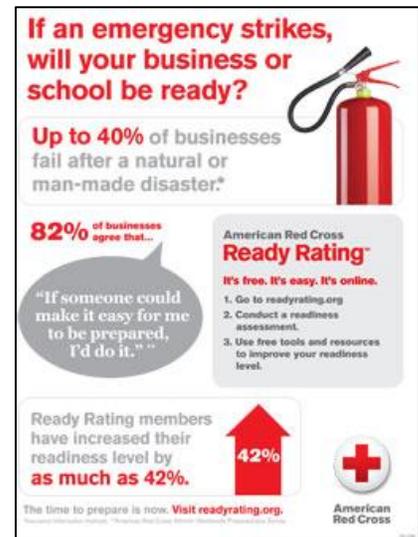
The American Red Cross has launched a new collection of free, online tools to help businesses, schools and other organizations prepare for emergencies. These enhancements to the Red Cross Ready Rating program offer specific steps that organizations can take to be better prepared. The new features include:

- An Emergency Response Plan Tool, which enables program members to build a customized plan to help their employees know their roles in the first 24-72 hours of an emergency.
- A *Next Steps* report that recommends specific actions members should take and the level of effort required.

- A Resource Center that includes preparedness tools including activities and exercises, so businesses, employees and students can better develop and practice preparedness plans.
- A Ready Rating Store with emergency supplies at the click of a button.
- An enhanced user experience that enables easier sign up and access to all tools available.

Emergencies like power outages, water main breaks and medical emergencies can disrupt daily operations. Disasters like tornados, floods, earthquakes and fires have the potential to cause workplaces to fold and schools to close. In an effort to better prepare for such events, Ready Rating members complete a confidential assessment of their current readiness level for emergencies and receive immediate, customized feedback with tips and resources for them to improve their readiness scores. More than 1,300 businesses and organizations and nearly 450 schools are already Ready Rating members. Members have increased their assessment scores – some by as much as 42 percent. The Ready Rating program is consistent with Private Sector or PS-Prep Standards developed by the Department of Homeland Security. More information about the program and the new components can be found at [readyrating.org](http://readyrating.org).

Infographic: <http://162.6.217.113/www-files/Documents/pdf/infographics/ReadyRatingInfographic.pdf>



### Gov. McDonnell Proclaims Hurricane and Flooding Preparedness Week

Virginia families should take action now to get ready for hurricane season, which begins June 1 and often brings significant flooding to both coastal and inland regions. To emphasize the important of emergency preparation, Gov. Bob McDonnell has recognized **May 27-June 2 as Hurricane and Flooding Preparedness Week**. The governor's proclamation coincides with National Hurricane Preparedness Week, sponsored by the National Weather Service. Last year, 10 residents died as a result of Hurricane Irene and Tropical Storm Lee in Virginia. Many communities continue to recover. Before weather disasters and other emergencies hit, families should be prepared with an emergency kit of supplies, a battery-powered and/or hand-crank radio to hear local information when the power is out, and a written family emergency plan. For more information on making a family plan as well as putting together a supply kit, see [www.ReadyVirginia.gov](http://www.ReadyVirginia.gov). Also, consider purchasing flood insurance, which is available to both property owners and renters and is not typically included in homeowners insurance. Consult your insurance agent about flood insurance and learn more at [www.floodsmart.gov](http://www.floodsmart.gov).

### New Virginia Hurricane Evacuation Guide Now Available

The 2012 edition of the Virginia Hurricane Evacuation Guide is now available to the public through multiple agencies and organizations throughout Hampton Roads and Central Virginia. The guide contains essential hurricane season information, including evacuation routes, traffic reversal plans along Interstate 64 and family preparedness. Produced by the Virginia Department of Transportation, the Virginia Department of Emergency Management, and the Hampton Roads Planning District Commission, the guide is part of the Ready Virginia and Ready Hampton Roads public information campaigns.

[http://www.vaemergency.gov/sites/default/files/12034\\_hurricaneEvacBOOK.pdf](http://www.vaemergency.gov/sites/default/files/12034_hurricaneEvacBOOK.pdf)

### The 2012 Virginia Statewide Communication Interoperability Plan

The 2012 Virginia Statewide Communication Interoperability Plan (SCIP) is now available online at: <http://www.vahs.virginia.gov/Initiatives/Interoperability/strategic-plans.cfm>. The SCIP is dedicated to improving communications interoperability at the local, regional, and state level. The annual update of the plan marks the next step towards achieving the 2015 Vision for Interoperability: "by 2015, agencies and their representatives at the local, regional, state, and federal levels will be able to communicate using compatible systems, in real time, across disciplines and jurisdictions, to respond more effectively during day-to-day operations and major emergency situations."

<http://nvers.org/regional-news-blog/2012/may/2012-virginia-statewide-communication-interoperability-plan-scip-now-ava>



[www.CapitalRegionUpdates.gov](http://www.CapitalRegionUpdates.gov)

## PLANNING / PREPAREDNESS

### National Terrorism Advisory System

The Department of Homeland Security's (DHS) National Terrorism Advisory System (NTAS) is a robust terrorism advisory system that provides timely information to the public about credible terrorist threats and replaces the former color-coded alert system. Under NTAS, DHS will coordinate with other federal entities to issue detailed alerts to the public when the federal government receives information about a credible terrorist threat. NTAS alerts provide a concise summary of the potential threat including geographic region, mode of transportation, or critical infrastructure potentially affected by the threat, actions being taken to ensure public safety, as well as recommended steps that individuals, communities, business and governments can take to help prevent, mitigate or respond to a threat. NTAS Alerts will include a clear statement on the nature of the threat, which will be defined in one of two ways:

- “Elevated Threat”: Warns of a credible terrorist threat against the United States.
- “Imminent Threat”: Warns of a credible, specific, and impending terrorist threat against the United States.

Depending on the nature of the threat, alerts may be sent to law enforcement, distributed to affected areas of the private sector, or issued more broadly to the public through both official and social media channels – including a designated DHS webpage ([www.dhs.gov/alerts](http://www.dhs.gov/alerts)), Facebook and via Twitter @NTASAlerts. NTAS alerts and posters will also be displayed in places such as transit hubs, airports and government buildings. NTAS threat alerts will be issued for a specific time period and will automatically expire. Alerts may be extended if new information becomes available or as a specific threat evolves. For more information on the National Terrorism Advisory System or to receive NTAS alerts, visit [www.dhs.gov/alerts](http://www.dhs.gov/alerts).

**National Terrorism Advisory System**  
**Alert**  
DATE & TIME ISSUED: XXXX

**SUMMARY**  
The Secretary of Homeland Security informs the public and relevant government and private sector partners about a potential or actual threat with this alert, indicating whether there is an "imminent" or "elevated" threat.

**DURATION**  
An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves.

**DETAILS**  
• This section provides more detail about the threat and what the public and sectors need to know.  
• It may include specific information, if available, about the nature and credibility of the threat, including the critical infrastructure sector(s) or location(s) that may be affected.  
• It includes as much information as can be released publicly about actions being taken or planned by authorities to ensure public safety, such as increased protective actions and what the public may expect to see.

**AFFECTED AREAS**  
• This section includes visual depictions (such as maps or other graphics) showing the affected area(s), sector(s), or other illustrative detail about the threat itself.

**HOW YOU CAN HELP**  
• This section provides information on ways the public can help authorities (e.g. camera phone pictures taken at the site of an explosion), and reinforces the importance of reporting suspicious activity.  
• It may ask the public or certain sectors to be alert for a particular item, situation, person, activity or developing trend.

**STAY PREPARED**  
• This section emphasizes the importance of the public planning and preparing for emergencies before they happen, including specific steps individuals, families and businesses can take to ready themselves and their communities.  
• It provides additional preparedness information that may be relevant based on this threat.

**STAY INFORMED**  
• This section notifies the public about where to get more information.  
• It encourages citizens to stay informed about updates from local public safety and emergency leaders.  
• It includes a link to the DHS NTAS website <http://www.dhs.gov/alerts> and <http://www.dhs.gov/NTASAlerts>.

**If You See Something, Say Something™** Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides information, and does not constitute an endorsement or approval by the Department of Homeland Security, which may be subject to change without notice. For more information, visit [www.dhs.gov/alerts](http://www.dhs.gov/alerts).

### The Importance of Public-Private Partnerships

Hurricane Katrina changed everything in emergency management, especially the private sector's role in disaster response. At the time, Wal-Mart was singled out for its leadership in helping communities respond. That perspective helps shape our public-private collaboration at the state and federal level every day. Wal-Mart's successful response to Hurricane Katrina also contributed to Louisiana launching the country's first fully operational Business Emergency Operations Center (BEOC). Named a "best practice" by the DHS, the state's BEOC provides a platform for private-sector industries and businesses (including retail) to communicate, collaborate and coordinate with government during a disaster.

<http://www.emergencymgmt.com/disaster/Industry-Perspective-Importance-Public-Private-Partnerships.html>

## **U.S. GAO reports on “Cybersecurity: Threats Impacting the Nation”**

The United States Government Accountability Office has issued a new report, “Cybersecurity: Threats Impacting the Nation.” The report outlines the nature of the various cybersecurity threats; highlights the vulnerabilities present in federal information systems and systems supporting critical infrastructure; and discusses reported cyber incidents and their impacts. Highlights include:

- Sources of threats include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare.
- The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations.
- The threat posed by cyber attacks is heightened by vulnerabilities in federal systems and systems supporting critical infrastructure. Specifically, significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems supporting the operations, assets, and personnel of federal government agencies.
- The number of cybersecurity incidents reported by federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past six years, the number of incidents reported by federal agencies to the Federal Information Security Incident Center has increased by nearly 680 percent.
- Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems, disrupting the operations of governments and businesses and the lives of private individuals.

<http://www.continuitycentral.com/news06266.html> | Report: <http://www.gao.gov/assets/600/590367.pdf>

## **Emergency Preparedness Guidelines for Levees**

While accountability for flood risk management is shared between government agencies, private-sector stakeholders, and citizens, the authority to determine land-use in floodplains and to enforce policy falls wholly on state and local governments. Levee systems are considered one of the nation’s critical infrastructures, and all-hazards safety and security of dams and levee systems should be considered in state and local emergency plans. The Department of Homeland Security published the “Emergency Preparedness Guidelines for Levees” (PDF, 380.66 KB) to help public and private entities manage levees and associated flood risk management systems against natural and manmade incidents. The guide gives recommendations and guidance on developing emergency preparedness and security plans. The guide states, “Many of the nation’s levees were built more than 50 years ago with the intent of protecting crops from flooding. Over the past few decades, housing and commercial development on land protected by levees has increased the risk to public health and safety associated with potential levee failure.” The Association of Dam Safety Officials has links to the National Levee Database, a Levees 101 page, a newsletter, and an extensive library on the levee safety section of their website. Additionally, the Federal Emergency Management Agency (FEMA) has information on levee mapping, risk and accreditation on the FEMA Levee Resource Library page.

“Emergency Preparedness Guidelines for Levees” –

[www.damsafety.org/media/Documents/Levees/Emergency%20Preparedness%20Guidelines%20for%20Levees.pdf](http://www.damsafety.org/media/Documents/Levees/Emergency%20Preparedness%20Guidelines%20for%20Levees.pdf)

FEMA Levee Resource Library – [http://www.fema.gov/plan/prevent/fhm/lv\\_reslib.shtm](http://www.fema.gov/plan/prevent/fhm/lv_reslib.shtm)

*Reprinted from the May 2, “Infogram,” from the Emergency Management & Response Information Sharing & Analysis Center. For information regarding the EMR-ISAC visit [www.usfa.dhs.gov/emr-isac](http://www.usfa.dhs.gov/emr-isac) or contact the EMR-ISAC office at 301-447-1325 and/or [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov).*

## **Helmets and Tornadoes**

The Centers for Disease Control and Prevention continues to recommend, as its first recommendation, that people in the path of a tornado find a shelter or a tornado-safe room. The safest place in the home is the interior part of a basement. If possible, get under something sturdy such as a heavy table or workbench. If outdoors, lie down in a gully or ditch.

“We understand that people who have seen the tragedy that tornadoes can impose are looking for any useful and effective ways to protect themselves. We don’t have research on the effectiveness of helmet use to prevent head injuries during a tornado, but we do know that head injuries are common causes of death during tornadoes, and we have long made the recommendation that people try to protect their heads. Individuals

may decide to use helmets to protect their heads. However, because the time to react may be very short, people who choose to use helmets should know where they are and have them readily accessible. Looking for a helmet in the few seconds before a tornado hits may delay you getting safely to shelter. For those who choose to use helmets, these helmets should not be considered an alternative to seeking appropriate shelter. Rather, helmets should be considered just one part of their overall home tornado preparedness kit to avoid any delay.”

CDC continues to promote protective measures for use during natural disasters including tornadoes. For more detailed information, go to <http://emergency.cdc.gov/disasters/tornadoes/during.asp>.

### **May is Building Safety Month**

When you enter a house or building, most likely you assume it is safe and was properly constructed in accordance with building codes. Fortunately, your local safety experts work hard to assure building safety and fire prevention every day. To help raise awareness of building safety, the Federal Emergency Management Agency (FEMA) proudly celebrates Building Safety Month this May. Building Safety Month is a month-long celebration of all aspects of building safety to help families, employers, and leaders understand and appreciate the best practices that keep the places where we live, work and play safe. The campaign is presented by the International Code Council and its 50,000 members worldwide, along with a diverse partnership of professionals from the building construction, design and safety community. In order for residents of a community to qualify for flood insurance from the National Flood Insurance Program (NFIP), the community needs to maintain a minimal level of building code protection and floodplain management. If a community enforces even higher standards, they can participate in the Community Rating System (CRS) program. The CRS provides a reduction in flood insurance premium rates for property owners in communities that implement activities above and beyond the basic requirements of the NFIP. These reduced rates reflect the reduced flood risk.

<http://www.fema.gov/news/newsrelease.fema?id=62697>

### **More than Half of Corporate Boards in Survey do not Review Cybersecurity Risks**

More than half of respondents to a cybersecurity survey indicated they do not take important steps to reduce their cybersecurity risks to stop data and security breaches, according to a third annual report from the Carnegie Mellon University (CMU) CyLab. The recent CMU report, “Governance of Enterprise Security: CyLab 2012 Report,” revealed that 57 percent of 108 global companies surveyed were not assessing cyber risk, including an analysis of cyberinsurance coverage. Moreover, close to 80 percent of the boards of companies managing critical infrastructure, like energy utilities and telecommunications companies, did not review cyberinsurance coverage, the survey said. Report: <http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf>

<http://www.hstoday.us/industry-news/general/single-article/more-than-half-of-corporate-boards-in-survey-do-not-review-cybersecurity-risks/c69f63c0b06bb1a3135465345fb99d33.html>

### **Whole Community: Planning for the Unthinkable Tabletop Exercise**

FEMA’s Private Sector Division, Office of External Affairs, began a new series of tabletop exercises in 2010 as a tool to help private sector organizations advance their organization’s continuity, preparedness and resiliency. The series is a part of the division’s vigilant efforts to incorporate the private sector across all stages of FEMA’s emergency management mission, to support FEMA’s capabilities, and to enhance national preparedness, protection, response, recovery and mitigation of all hazards. This new downloadable Tabletop Exercise (TTX) is an interactive exercise, complete with accompanying facilitator’s notes and scripted video injects. It allows organizations to look at the first 72 hours (3 days) of a response to a catastrophic disaster and brainstorm innovative ways to fill critical gaps in both internal and community emergency management plans. In addition to examining immediate response capabilities, the exercise modules focus specifically on the areas of crisis communications and search and rescue. The PowerPoint-based tabletop exercise (TTX) is a free and downloadable, and a complete exercise program for businesses with note pages and Virtual News Network (VNN) inject videos. It incorporates Jeanne Meserve as the VNN anchor, ensuring a more compelling presentation and dialogue. The exercise also drives participants at the end to contribute to an ongoing online dialogue at FEMA’s Collaboration Community.

<http://www.fema.gov/privatesector/exercises.shtm>

## MEDIA ARTICLES OF INTEREST

### **Why You Should Evacuate Before a Hurricane**

Hurricanes are one of the most devastating natural disasters that occur in the world, behind only floods and earthquakes. The Federal Emergency Management Agency lists living in a mobile home, a high-rise building, near or on the coast, on a floodplain or near other bodies of water as reasons to immediately evacuate if a hurricane is coming your way.

<http://www.accuweather.com/en/features/hurricane-forecast/why-you-should-evacuate-before/64504>

### **Why The Cyber Security Act Might Not Be Good For Business**

Will government intervention help reduce the number of security attacks on our nation's infrastructure? The Cyber Security Act of 2012 aims to give the Department of Homeland Security the power to mandate the security level in industries it deems as critical infrastructure, such as power and telecommunications, water treatment facilities and wireless providers. If the legislation successfully makes its way through Congress, the DHS will be in charge of national Internet security standards with the power to federally mandate cyber security performance requirements for Internet infrastructure. The bill also would require private firms to cooperate and let the government know when their systems are compromised. These federally mandated requirements for Internet infrastructure could lead to big costs for U.S. tech, Internet and other firms and fundamentally change the way they operate.

<http://www.forbes.com/sites/ciocentral/2012/04/30/why-the-cyber-security-act-might-not-be-good-for-business/>

### **Survey Looks Into Bring Your Own Device Trends**

Mimecast has released the findings from a survey of 500 IT professionals and administrators from the 2012 DevConnections conference held in Las Vegas. The survey highlights that bring your own device (BYOD) is still a hotly debated enterprise issue and unveiled a divide between employees and the business. While 47 percent of respondents find consumerization of IT important to highly important to the enterprise, when asked about the risk BYOD is perceived to bring to the enterprise, 21 percent said BYOD has been a risk to the business, with a separate 26 percent admitting their business does not allow employees to use their own device for corporate tasks. These results show a significant disconnect: while employees value consumerization of IT, businesses are hesitant due to perceived risks. Half (50.7 percent) of the same set of IT professionals surveyed called out that employee access to personal devices was a productivity necessity, while only 7.9 percent said personal devices were detrimental to productivity. Meanwhile, 74 percent of the respondents emphasized that the enterprise's biggest mobile challenge was managing information security.

<http://www.continuitycentral.com/news06269.html>

### **Symantec Report Charts Big Spike in Cyberattacks, Adding Fuel to Cybersecurity Legislative Debate**

The number of cyberattacks globally spiked significantly last year, and more and more attackers have targeted smaller organizations as well as large ones, reported cybersecurity firm Symantec Corp. recently.

<http://www.hstoday.us/single-article/symantec-report-charts-big-spike-in-cyberattacks-adding-fuel-to-cybersecurity-legislative-debate/e16e47638b63acc7208b0597f584526.html>

### **Planning, Preparation Key to Surviving Severe Storms**

Fort Belvoir, Va. encourages community members to prepare emergency response plans in case of a catastrophic weather event. NOAA and FEMA highlight the importance of planning appropriate response measures to severe weather. The collaborative initiative encourages people to "Be a force of nature" by taking proactive preparedness measures, and inspiring others to do the same. The Directorate of Plans, Training, Mobilization and Security recommends residents and workers at Belvoir prepare plans that include survival kits, emergency shelter locations and listen to the installation emergency communications for updates on weather and road conditions.

<http://www2.belvoireagle.com/news/2012/may/03/planning-preparation-key-surviving-severe-storms-ar-1888158/>

### **PFPA Given Oversight of Emergency Management at Pentagon Reservation**

The Pentagon Force Protection Agency has been recognized as the lead organization concerning emergency management matters on the Pentagon Reservation. Its selection was cited because of its initial incident management and coordination responsibilities in disaster-related preparedness and response functions for both man-made and natural disasters. Michael L. Rhodes, director of Department of Defense Office of Administration and Management, appointed PFPA in December with the authority to oversee coordination of all emergency management activities. Knowing EM is a shared mission, not simply a PFPA activity, he understands that DoD components of the Pentagon reservation will continue to retain responsibility to plan for and conduct their own multiple EM and Continuity of Operations (COOP) activities. The fundamental point and goal for assigning PFPA as a lead is to officially establish a focal point to network, and collaborate planning that can translate requirements into specific patterns of action to achieve unity of effort. The PFPA director will work in close coordination with the Washington Headquarters Services director, the deputy assistant secretary of defense for continuity and crisis management, and all DoD components of the Pentagon reservation to coordinate and synchronize the execution of EM and COOP functions. PFPA shall ensure that this effort is integrated with other Pentagon reservation security, force protection, antiterrorism, law enforcement and fire/safety requirements

<http://www.dcmilitary.com/article/20120504/NEWS10/120509986/pfpa-given-oversight-of-emergency-management-at-pentagon-reservation>

### **State Upgrades Traveler Information Systems**

Ah, summer's almost here: cookouts, beach days, vacations. And, ugh, tourist traffic. Just in time to help manage the notoriously bad summertime traffic jams, the state is rolling out several upgrades to its traveler information systems.

<http://hamptonroads.com/2012/05/state-upgrades-traveler-information-systems>

### **Verizon Says it is Ready for Hurricane Season**

With less than a month to go until the start of the 2012 hurricane season, Verizon says its wireless network is prepared to serve customers in the event of a major storm or emergency. More than two-thirds of the U.S. most hurricane-prone coastal population, from the Carolinas to the Texas Gulf Coast, is covered by the Verizon Wireless 4G LTE data network. When customers travel outside of 4G LTE coverage areas, wireless devices automatically connect to Verizon Wireless' 3G data network, which is available throughout most of the same coastal area.

<http://www.homelandsecuritynewswire.com/srdisasters20120510-verizon-says-it-is-ready-for-hurricane-season>

### **Survey: Americans Worry More About Cybersecurity than Terrorism**

More Americans want presidential candidates to make cybersecurity a priority than want them to focus on terrorism, according to a bi-annual survey by a computer security firm. Seventy four percent of American respondents told researchers they think it is "very important" that U.S. presidential candidates address cybersecurity issues, according to the Unisys Security Index. That compares to 68 percent for terrorism. Government officials have warned that cybersecurity could overtake physical terrorism as a top threat to the United States. Overall, however, the Unisys study found that the level of concern over all types of national security risks dropped since last year.

<http://www.nextgov.com/cybersecurity/2012/05/survey-americans-worry-more-about-cybersecurity-terrorism/55652>

### **April's Major Disasters Around the World**

The latest edition of the "Global Catastrophe Recap" report, which reviews the natural disaster perils that occurred worldwide during April, has been published by Impact Forecasting. The report reveals that a series of severe weather events across central and southern sections of the United States caused upwards of \$1 billion in insured losses. Economic losses were even higher. During the month's most notable outbreak, multiple central states sustained widespread tornado, hail and wind damage. At least 94 tornado touchdowns were recorded during a 72-hour stretch. In Kansas, an EF-3 tornado just outside the city of Wichita affected at least 777 homes and 165 businesses. Additional tornado damage occurred in southwest Iowa and northwest Oklahoma, killing at least six people. Total insured losses from the outbreak were expected to reach into the hundreds of millions of dollars. Meanwhile, a severe weather outbreak in Texas, which comprised at least 21 tornadoes and widespread hail, damaged more than 1,100 homes alone in the greater Dallas-Fort Worth metro region. Total economic losses were estimated at approximately \$1 billion, while various insurers received at least 105,000 claims with payouts in excess of \$650 million. In South

America, at least 18 people were killed and 20 more were injured as severe weather struck the Argentine capital of Buenos Aires, affecting at least 32,000 homes.

<http://www.continuitycentral.com/news06281.html>

### **Federal Security Funding Plan**

Local homeland security officials in Baltimore, Md., and across the country are fighting a proposal to change how \$2 billion in federal emergency management money is distributed.

[http://articles.baltimoresun.com/2012-05-11/news/bs-md-terrorism-money-20120511\\_1\\_homeland-security-security-funding-regional-planning](http://articles.baltimoresun.com/2012-05-11/news/bs-md-terrorism-money-20120511_1_homeland-security-security-funding-regional-planning)

### **Extreme Weather Alerts**

Wireless carriers and the federal government are launching a system to automatically warn people of dangerous weather and other emergencies via a special type of text messaging to cell phones. The Wireless Emergency Alerts (WEA) service, which begins this month, is free, and consumers won't have to sign up. Warnings will be location-based: If you're traveling, you'll get an alert for whatever emergency is happening where you are.

<http://www.usatoday.com/weather/news/story/2012-05-13/extreme-weather-alerts-texts-cellphones/54943804/1>

### **Guard's WMD Civil Support Teams Can Respond Faster Than Other Federal Assets**

The National Guard's Weapons of Mass Destruction Civil Support Teams are known as some of the most effective first responders when it comes to a potential chemical, biological, radiological, nuclear or enhanced improvised explosive event. Since 2001, CSTs have served as full-time, federally funded National Guard units supporting local civil authorities in responding to events known or suspected to involve weapons of mass destruction, whether it be hostile use of chemicals such as nerve or blister agents, toxic industrial chemical spills, biological events or radiological sources.

<http://www.hstoday.us/single-article/guards-wmd-civil-support-teams-can-respond-faster-than-other-federal-assets/af2160975c8dc3d4ab7f17f0942bdcdc.html>

### **Evacuations and Drills Pared Near Nuke Plants**

Without fanfare, the nation's nuclear power regulators have overhauled community emergency planning for the first time in more than three decades, requiring fewer exercises for major accidents and recommending that fewer people be evacuated right away. The revamp, the first since the program began after Three Mile Island in 1979, also eliminates a requirement that local responders always practice for a release of radiation. At least four years in the works, the changes appear to clash with more recent lessons of last year's reactor crisis in Japan. Under the new rules, the Nuclear Regulatory Commission and the Federal Emergency Management Agency, which run the program together, have added one new exercise: More than a decade after the 9/11 terrorist attacks, state and community police will now take part in exercises that prepare for a possible assault on their local plant. Still, some emergency officials say this new exercise doesn't go far enough. And some view as downright bizarre the idea that communities will now periodically run emergency scenarios without practicing for any significant release of radiation.

<http://bit.ly/LS1G6D>

### **Dominion to Face Extra Oversight at Va. Nuke Plant**

Dominion Virginia Power will face additional federal oversight at its North Anna Nuclear Power Station near Mineral, Virginia, because of a safety violation related to its emergency diesel generators, the U.S. Nuclear Regulatory Commission (NRC) said May 14. Federal regulators said inspectors found that a gasket failure prevented one of the four diesel generators from performing its function following the August 2011 5.8-magnitude earthquake. The failed gasket was not caused by nor related to the earthquake. While it was replaced the same day, inspectors found the plant did not have adequate procedures for installing the gasket. Richmond-based Dominion discussed the issue with federal regulators in April. The NRC deemed it a "white" violation, or one that is of low to moderate safety significance.

<http://www.wtop.com/120/2823543/Extra-oversight-at-Va-nuke-plant>

### **Breaking the Cycle of Reliance on Federal Help After Disasters**

Throughout 2011, media messages exemplified the baseline issues that exist when the federal government acts as primary service provider after a disaster. Articles about FEMA relief funds stalled in Congress ran virtually side by side with articles about FEMA's attempt to recoup funds erroneously given out after Katrina. Still, there is little outcry to repair the broken federal system and few politicians will disagree with the billions of dollars passed through after disaster.

<http://www.emergencymgmt.com/disaster/Breaking-Reliance-Federal-Help-After-Disasters.html>

### **Business EOCs Improve Public-Private Relationships**

When disaster strikes, everyone in the community pitches in to help, including government, neighbors, local stores and charitable organizations. Historically, however, there has been too little coordination between government relief efforts and the private sector. Hurricane Katrina's aftermath in 2005 had emergency managers at all levels trying to improve that coordination by looking at ways to get the business community represented physically or virtually in the EOC. "We approach this from a different perspective, but we all have a common mission and that is the recovery of that community," said Ethan Beckcom, emergency and risk manager for NorthWest Arkansas Community College in Bentonville and project lead for the Arkansas Business Emergency Operations Center. One result is a relatively new kind of partnership, often called a business emergency operations center (BEOC). The operations center takes many forms — some are physical, some are virtual and some aren't even called a BEOC at all. But they all offer a two-way flow of information between government and the business community when planning disaster response and recovery.

<http://www.emergencymgmt.com/safety/Business-EOCs-Improve-Public-Private-Relationships.html>

### **DHS Forced to Release List Terms it Monitors on Social Media**

Following a Freedom of Information Act (FOIA) request by the Electronic Privacy Information center (EPIC), DHS was forced to release its 2011 Analyst's Desktop Binder. The binder, among other things, contains a list of words DHS uses as triggers of suspicious communication when the department's analysts monitor social media. The department insists it only looks for evidence of genuine threats to the United States and not for signs of general dissent. Forbes quotes DHS to say that it uses these terms as "signs of terrorist or other threats against the U.S." The Daily Mail reports that EPIC wrote a letter to the House Homeland Security Subcommittee on Counter-terrorism and Intelligence, describing the department's choice of words as "broad, vague and ambiguous."

<http://www.homelandsecuritynewswire.com/dr20120529-dhs-forced-to-release-list-terms-it-monitors-on-social-media>

## FLU

### **H5N1 Flu Virus Could Put Millions at Risk**

"Seasonal flu affects 10 to 20 percent of the world every year- - as much as a billion people or more," Thomas Inglesby, CEO and director of the Center for Biosecurity of the University of Pittsburgh Medical Center, says. "The case fatality rate of wild H5N1 in the WHO database is nearly 60 percent. So if a strain of H5N1 with that fatality rate were engineered to spread like seasonal flu, hundreds of millions of people's lives would be at risk. Even a strain a hundred times less fatal would place at risk millions of people's lives." Concern has grown recently over advances in the field of biotechnology, in which scientists have created synthetic viruses in laboratories. Inglesby says that mistakes can be made in laboratories, like the one in 1977 when "H1N1 caused a mini-pandemic, probably from a lab escape.

<http://www.catholic.org/health/story.php?id=45969>

### **Nearly Censored Bird Flu Paper Published**

One of two now-notorious bird flu studies was published on Wednesday, May 2, four months after a panel of US federal advisers asked researchers and scientific journals to hold on, just in case the information in the paper was

dangerous. In the paper, flu expert Yoshihiro Kawaoka of the University of Wisconsin (Madison) describes how he genetically engineered H5N1 bird flu – the virus that’s been decimating poultry in Asia, Egypt, and elsewhere – using pieces of the virus that caused the 2009 pandemic of H1N1 swine flu in people. The paper itself is interesting to scientists and flu junkies. Published in “Nature,” it shows that four genetic changes can make the usually hard-to-catch H5N1 virus spread more easily among ferrets – animals that acquire flu in much the same way that people do. <http://www.govexec.com/defense/2012/05/one-two-nearly-censored-bird-flu-papers-published/55552/>

### **Report Details Changes that May Boost H5N1 Spread in Mammals**

The first of two controversial H5N1 avian influenza studies to see print suggests that just four mutations in one of the virus's surface proteins may be enough to equip it to spread among mammals, but the findings are freighted with qualifiers. After months of debate and discussion, “Nature” published the report by Yoshihiro Kawaoka, DVM, PhD, and colleagues describing a lab-derived hybrid virus, with elements of H5N1 and pandemic H1N1, that spread among ferrets via respiratory droplets. Kawaoka works at the University of Wisconsin. The authors say their findings answer the “fundamental question” of whether flu viruses wearing the H5 hemagglutinin (HA) surface protein found in H5N1 can spread in mammals. However, the virus did not kill any of the ferrets or even make them severely ill. Moreover, the authors caution that they don't know if the four mutations that supported transmission in the hybrid would accomplish the same thing in an H5N1 virus containing no foreign genes. Their reassortant virus contained seven genes from 2009 H1N1 and just one – the HA – from H5N1. At the same time, the researchers say one of the four key mutations they identified has already been seen in circulating H5N1 viruses on three continents, so it would take only three more to create an HA that supports mammalian transmission. They assert that their findings, by alerting scientists to potentially dangerous H5N1 mutations, will help surveillance.

<http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/news/may0312kawaoka.html>

### **H1N1: Hospitals in India in State of High Alert**

With more than a dozen cases confirmed, the health department has put all doctors in government and private hospitals [in India] on high alert for symptoms of the infection especially if accompanied by other health complications. H1N1 screening centres have been opened in all taluk hospitals and other government hospitals in Ernakulam, from where two positive cases have been reported. Officials from the state Virology Institute, Alappuzha, collected throat swab samples of patients with positive symptoms from three hospitals in the district, the general hospital, Ernakulam, the district hospital Aluva and the general hospital, Muvattupuzha. In Kozhikode district, from where 11 cases have been reported, district medical authorities have taken necessary preventive measures. According to Dr. Mohanan, district medical officer, the situation is under control.

<http://www.deccanchronicle.com/channels/cities/kochi/h1n1-hospitals-state-high-alert-281>

### **Fairfax County Flu Preparedness**

Be sure to visit the county’s flu Web page for information on upcoming events and other preparedness news.

<http://www.fairfaxcounty.gov/flu>

## TRAININGS / EXERCISES / CONFERENCES

The logo for FEMA (Federal Emergency Management Agency) is displayed in a large, bold, blue serif font.

*Emergency  
Management  
Institute*

The Federal Emergency Management Agency's  
Emergency Management Institute offers an extensive  
catalog of training and education at numerous locations.  
[View website](#)

<http://training.fema.gov/EMI/>

The ESF 15 Business / Nonprofit Update is designed to provide information about Emergency Support Function 15 (External Affairs) along with news articles and informational updates relating to Homeland Security and emergency management to ESF 15 partners. Inclusion of any resource, information or Web link is not an endorsement of the product, service or organization. The ESF 15 Business / Nonprofit Update is produced by Fairfax County’s Office of Public Affairs – the lead agency for ESF 15.

### **2012 Management of Change: “Coming Clouds of Change”**

June 3-5; Hyatt Regency Chesapeake Bay, Cambridge, Md.

Attend the American Council for Technology – Industry Advisory Council’s Management of Change (MOC). This education and training event brings together over 500 government and industry information technology professionals to focus on cloud, security and mobility challenges in government. The theme, “Coming Clouds of Change,” points to how future cloud and mobility technologies will usher in new efficiencies...as well as fresh security issues. Together, we will examine what the next generation of government and industry leaders might need to consider for the future by providing tangible take-aways and best practices. The inaugural Tech Expo will showcase and demonstrate early entry technology solutions to foster additional discussion, debate and learning.

<http://www.actgov.org/events/managementofchange/Pages/default.aspx>

### **EMI 15th Annual Higher Ed Conference**

June 4-7; Emmitsburg, Md.

FEMA’s Emergency Management Institute Higher Education Conference is designed for representatives of colleges and universities THAT have an existing hazard, disaster, emergency management program in place or are attempting to develop and implement a hazard, disaster, or emergency management program on their campus (e.g., a degree, certificate, minor, or concentration). The conference will be held on the grounds of the Federal Emergency Management Agency’s National Emergency Training Center (NETC) in Emmitsburg, Md. – about 75 miles northwest of Washington, D.C.

<http://training.fema.gov/EMIWeb/edu/educonference12.asp>

### **Fifth Annual Health Information Security Conference**

June 6-7; Washington, D.C.

The National Institute of Standards and Technology is co-hosting the fifth annual Safeguarding Health Information: Building Assurance through HIPAA Security conference on June 6 and 7, at the Ronald Reagan Building and International Trade Center. The conference is hosted in conjunction with the Department of Health and Human Services Office for Civil Rights. The conference is an opportunity for HIPAA security rule implementers; security, privacy and compliance officers; assessment teams and audit staff in health care providers to explore current issues in health information security and to discuss practical strategies, tips and techniques for implementing the HIPAA Security Rule. Specific sessions will cover a variety of current topics, including updates on HHS health information privacy and security initiatives, OCR's enforcement of health information privacy and security activities, integrating security safeguards into health IT, safeguards to secure mobile devices, and removing sensitive data from the Internet

<http://www.nist.gov/itl/hipaa-041712.cfm>

### **Chemical Industry Outreach Workshop**

June 6; Richmond, Va.

The Richmond Division of the Federal Bureau of Investigation is offering a free workshop providing explosive demonstrations of conventional and improvised explosives made from easily obtainable chemicals with an emphasis on illustrating the teaching points covered in the morning briefings. The workshop is Wednesday, June 6, at the J. Sargeant Reynolds Community College (Parham Campus) located at 1651 E. Parham Road, Richmond, Georgiadis Hall, The Gallery, Room B101. Contact FBI Special Agent Tom Adams with any questions on the workshop at 804-314-5454, or email at [thomas.adams@ic.fbi.gov](mailto:thomas.adams@ic.fbi.gov).

<https://chemicalindustryoutreach.org/EBForms.aspx?EBID=28&EBType=WLR&RefID&AspxAutoDetectCookieSupport=1>

### **Re-inventing Cybersecurity: Moving from Crime Scene Investigators to Pre-Crime Oracles**

June 12; Herndon, Va.

Be part of an open dialogue with Dr. Anup Ghosh and discuss these important topics that address this particular question: Is prevention a failed security strategy? Given the lack of innovation in prevention techniques over the past decade and the exponential evolution of our adversaries, many in the security industry would say yes. The event will be held 10:30 a.m. to noon on June 12 at the Cypherpath, Center for Innovative Technology, Herndon. There is a cost to attend; to register call 703-435-1300.

## **Virginia Healthcare Emergency Management State Forum**

June 13-15; Norfolk, Va.

“Partnerships in Preparedness” is the theme for the 11th statewide healthcare emergency management program being held in Norfolk, June 13-15. Preparedness is crucial to survival and management of emergency situations, which can happen on short notice. This forum will provide attendees with the tools and knowledge so Virginia is compliant, informed and ready to act when the need arises.

<http://www.vhha.com/documents.html?id=738>

## **Workshop on Privacy Compliance**

June 20; Washington, D.C.

The all-day “Privacy Compliance Workshop” will review the privacy compliance process at DHS, privacy and data security, and the privacy compliance life-cycle. The program will be held in the conference center at the headquarters of the Federal Trade Commission at 601 New Jersey Avenue, NW, Washington, DC, from 8:30 a.m. to 4:30 p.m., on May 25. Advanced sessions in the afternoon will cover the Paperwork Reduction Act, the Freedom of Information Act and privacy compliance reviews. To register, email [privacyworkshop@hq.dhs.gov](mailto:privacyworkshop@hq.dhs.gov) by June 15, and include your full name, email address and organizational affiliation. Further information is available at 703-235-0780.

## **Infrastructure Risk/Vulnerability Assessment Taking CARVER to the Next Level**

June 25-27, Arlington, Va.

This course, using criticality, accessibility, recuperability, vulnerability, effect and recognizability (CARVER) – an all-hazards assessment tool – emphasizes kinetic threats from small arms (active shooter) and improvised explosive devices; students will learn to identify threats and vulnerabilities of all sorts and apply risk management processes for incident planning. The course is designed for facility security, law enforcement and emergency management professionals charged with planning for and implementing protective measures for personnel, facilities, and infrastructure. Students will conduct an actual on-scene preliminary security vulnerability assessment and develop and deliver a briefing of their findings.

<http://www.governmenttraininginc.com/CARVER-Vulnerability-Assessment-120609.asp>

## **IED Counterterrorism Workshop**

July 10; Richmond, Va.

A free IED Counterterrorism Workshop is being sponsored by the Department of Homeland Security, Office for Bombing Prevention and the Virginia Office of Veterans Affairs and Homeland Security. The workshop will be held July 10 at the Richmond City Police Department’s Law Enforcement Training Academy Auditorium. To register for the workshop, email Jeremiah Hockman, Virginia Office of Veterans Affairs and Homeland Security at [dhstraining@governor.virginia.gov](mailto:dhstraining@governor.virginia.gov) (by July 2) with the name, agency, position, email and phone number of the officials attending.

## **VASART Conference**

July 13; Blue Ridge Community College, Weyers Cave, Va.

The Virginia State Animal Response Team will be sponsoring a training day on July 13, at Blue Ridge Community College, from 8 a.m. to 4:30 p.m. There is limited seating available.

Questions: 804-346-2611.

[www.virginiasart.org](http://www.virginiasart.org)



## **Symposium on Homeland Security: Enhancing Public-Private Partnerships and Coordination**

July 19-20, 2012; Christopher Newport University, Newport News, Va.

Increasingly complex threats to the U.S. require innovative, cross-disciplinary responses from local, state and federal government entities. Private sector firms continue to work hand in hand with government to produce new technology, develop groundbreaking practices and shape products and services to robustly address today’s evolving threat environment. Natural disasters, man-made incidents, and acts of cyberterrorism and cyberespionage underscore that

strong partnerships and coordination are more needed now than ever before in American history. Held at Christopher Newport University's Center for American Studies, the Greater Hampton Roads Chapter of the National Defense Industrial Association, Continuity First and Verizon Wireless will present the 2nd annual "Symposium on Homeland Security: Enhancing Public-Private Partnerships and Coordination."

<http://symposiumonhomelandsecurity.com/>

### **Building Resilience through Public-Private Partnerships Conference**

July 20-27; Colorado Springs, CO

U.S. Northern Command (USNORTHCOM), in collaboration with the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security Headquarters, will host the 2nd annual Building Resilience through Public-Private Partnerships Conference July 23-24, in Colorado Springs, Colorado. The conference will cover a wide range of issues related to effective, whole- community collaboration toward resilience.

[https://resweb.passkey.com/Resweb.do?mode=welcome\\_ei\\_new&eventID=9559689](https://resweb.passkey.com/Resweb.do?mode=welcome_ei_new&eventID=9559689)

### **2012 Chemical Sector Security Summit**

July 31-Aug. 2; Baltimore, Md.

The National Protection & Programs Directorate's Office of Infrastructure Protection and the Chemical Sector Coordinating Council are co-sponsoring the 2012 Chemical Sector Security Summit in Baltimore, Md. The sixth annual Summit will provide a forum for representatives from the chemical community to exchange information and network with other security professionals, share best practices, learn more about chemical security regulations, and gain insight into the roles of state, local and federal agencies and departments involved in chemical security.

[http://www.dhs.gov/files/programs/gc\\_1176736485793.shtm](http://www.dhs.gov/files/programs/gc_1176736485793.shtm)

### **Public/Private Situational Awareness Workshop**

Aug. 16; McLean, Va.

The All-Hazards Consortium, the Department of Homeland Security Science and the Technology Directorate's Office of First Responder Programs, and MITRE will co-host a multi-state and regional workshop focused on situational awareness and information sharing between public and private sectors during natural and man-made disasters. The workshop will develop recommendations from participants on a "suite of standards and approaches" that support a framework and path forward for the integration of the various situational awareness platforms in order to better support collaborative decision making in both the public and private sectors during disasters

[www.ahcusa.org](http://www.ahcusa.org)

### **APCO International 78th Annual Conference and Expo**

Aug. 19-22; Minneapolis Convention Center, Minneapolis, MN

It's the public safety communications industry's biggest event of the year.

<http://www.apco2012.org/>

### **IAEM Annual Conference**

Oct. 26-Nov. 1; Orlando, Fla.

The International Association of Emergency Managers (IAEM) will host the annual IAEM Conference, Oct. 26-Nov. 1, in Orlando, Fla. The theme of this year's conference is "Resilience."

<http://www.iaem.com/>

### **2013 Mid-Atlantic Expo and Symposium**

Feb. 21-24, 2013; Virginia Beach, Va.

The Virginia Fire Chiefs Association is calling for presenters for its 2013 Mid-Atlantic Expo and Symposium Feb. 21-24, 2013, at the Virginia Beach Convention Center. Presentation subject matter can include, but is not limited to strategy and tactics; EMS, ICS, leadership; management; safety and health; new initiatives/concepts/trends; case studies; etc.

[http://www.vfca.us/index.php?option=com\\_content&view=article&id=92&Itemid=108](http://www.vfca.us/index.php?option=com_content&view=article&id=92&Itemid=108)

### **National Capital Region Homeland Security Events**

[http://www.mwcog.org/committee/committee/events\\_homeland.asp?COMMITTEE\\_ID=134](http://www.mwcog.org/committee/committee/events_homeland.asp?COMMITTEE_ID=134)

### **Virginia Emergency Management Courses**

<http://www.vaemergency.com>

### **FEMA Independent Study Courses**

<http://www.training.fema.gov/EMIWeb/IS/>

### **American Red Cross Disaster Services Training**

[http://www.redcrossna.org/Online/disaster\\_registration.php](http://www.redcrossna.org/Online/disaster_registration.php)

## **LINKS**

### **Fairfax County Blogs and Web Resources**

- Fairfax County Emergency Information Blog – [www.fairfaxcounty.gov/emergency/blog](http://www.fairfaxcounty.gov/emergency/blog)
- Fairfax County CERT - <http://fairfaxcountycert.blogspot.com/>
- Fairfax County Citizen Corps Web Page - [www.fairfaxcounty.gov/oem/citizencorps/](http://www.fairfaxcounty.gov/oem/citizencorps/)
- Fairfax County Citizen Corps Blog - <http://citizencorps.blogspot.com/>
- Virginia Citizen Corps - [www.vaemergency.com/citcorps/index.cfm](http://www.vaemergency.com/citcorps/index.cfm)

### **DHS Science & Technology Directorate Newsletter**

The U.S. Department of Homeland Security's Science & Technology Directorate has a free newsletter, "S&T Snapshots," featuring stories about current research projects and opportunities with laboratories, universities, government agencies, and the private sector. The newsletter is produced monthly.

<http://www.homelandsecurity.org/snapshots/>

### **DHS Daily Open Source Infrastructure Report (OSIR)**

The Department of Homeland Security provides a Web-based "Daily OSIR," which is posted on the DHS public Web site. Accessing the report via the Web enables readers to retrieve the current Daily Report as well as 10 days of archived DHS Daily Reports. Once you arrive at the Web page you will find the most recent Daily OSIR at the top of the page, under the title "Current Report." This report is posted each morning, except for weekends and holidays. Simply click on the title "DHS Daily Open Source Infrastructure Report." This will launch the current days report in PDF format. You can submit content comments or make suggestions by contacting the DHS Daily Report Team by telephone at 202-312-3421 or by e-mail at [NICCCReports@dhs.gov](mailto:NICCCReports@dhs.gov). You can access the Daily OSIR at: [http://www.dhs.gov/files/programs/editorial\\_0542.shtm](http://www.dhs.gov/files/programs/editorial_0542.shtm).

### **Fairfax County Government Emergency Information Web Page**

This page features easy navigation and a clean look so that residents can easily find emergency information.

[www.fairfaxcounty.gov/emergency/](http://www.fairfaxcounty.gov/emergency/)

### **Fairfax County Government Emergency Information Line**

[www.fairfaxcounty.gov/opa/infoline.htm](http://www.fairfaxcounty.gov/opa/infoline.htm)

### **Fairfax County Emergency Blog**

<http://www.fairfaxcounty.gov/emergency/blog>

### **FEMA Private Sector**

<http://www.fema.gov/privatesector/>

**FAIRFAX COUNTY 703-817-7771**  
**EMERGENCY**  
**INFORMATION LINE**

### **ESF 15 Contact Information**

Merni Fitzgerald, Director  
Fairfax County Office of Public Affairs  
12000 Government Center Parkway, Suite 551 ♦ Fairfax, Va. 22035-0065  
Tel: 703-324-3187 ♦ Direct: 703-324-3189  
E-mail: [Merni.Fitzgerald@fairfaxcounty.gov](mailto:Merni.Fitzgerald@fairfaxcounty.gov)  
Web site: [www.fairfaxcounty.gov](http://www.fairfaxcounty.gov)  
Emergency Information: [www.fairfaxcounty.gov/emergency](http://www.fairfaxcounty.gov/emergency)

### **To Unsubscribe:**

E-mail [publicaffairs@fairfaxcounty.gov](mailto:publicaffairs@fairfaxcounty.gov) with “Remove from ESF 15 Business/Nonprofit Update” in the subject line and you will be immediately removed from the distribution list.

In accordance with NIMS – the National Incident Management System – the Fairfax County Emergency Operations Plan states that Emergency Support Function 15 (External Affairs) is led by the Office of Public Affairs. This ESF 15 Business/Nonprofit Update is part of the county's outreach efforts for our business and nonprofit partners as a way to provide information about the county's ESF 15, Homeland Security and emergency management.

Please feel free to forward this ESF 15 Business/Nonprofit Update to other contacts you have inside or outside your organization. Should someone you know like to be added to our distribution list, have them send an e-mail to [jim.person@fairfaxcounty.gov](mailto:jim.person@fairfaxcounty.gov) and ask to be subscribed to the ESF 15 Business/Nonprofit Update.

If you have any suggestions on how to improve this update or other communications between Fairfax County and the business/nonprofit community, please contact Merni Fitzgerald, Director of the Fairfax County Office of Public Affairs, at 703-324-3187, TTY 711, or by e-mail at [merni.fitzgerald@fairfaxcounty.gov](mailto:merni.fitzgerald@fairfaxcounty.gov).

The ESF 15 Business / Nonprofit Update is designed to provide information about Emergency Support Function 15 (External Affairs) along with news articles and informational updates relating to Homeland Security and emergency management to ESF 15 partners. Inclusion of any resource, information or Web link is not an endorsement of the product, service or organization. The ESF 15 Business / Nonprofit Update is produced by Fairfax County's Office of Public Affairs – the lead agency for ESF 15.