

The InfoGram



Volume 18 — Issue 12 | March 22, 2018

Unannounced hospital mystery patient drills and toolkit

Between December 2015 and May 2016, New York City hospitals took part in mystery patient drills. A person entered an emergency department reporting fever and symptoms of either Middle East Respiratory Syndrome (MERS) or measles (along with a moulage measles red rash).

The drills determined if staff would identify the patient as being high risk, move them to an isolation room and provide them a mask. A total of 95 drills took place in 49 hospitals.

If a patient was not triaged within 30 minutes, the drill was considered a failure and terminated. Overall, 74 drills passed but 19 hospitals failed at least one drill. The median time from entry to triage was one minute, and the median time from entry to isolation was 8 minutes for the measles scenario and 11 minutes for the MERS scenario.

In the above case, results from these drills were used to develop the “[Infectious Disease Readiness](#)” toolkit to help other hospitals perform similar drills. Unannounced or unexpected drills and exercises are an excellent way to determine if your level of employee training is up to expected standards. Facilities can also use them as tools to identify and address gaps in response or to test protocols.

(Source: [CDC](#))

DHS Science & Technology Directorate puts out call for new technology

The [Next Generation First Responder](#) (NGFR) Apex Program increases availability of life-saving technology to improve protection, communications and situational awareness for firefighters, law enforcement and EMS personnel, while still keeping it budget-friendly.

The Department of Homeland Security’s Science and Technology Directorate (S&T) seeks innovative first responder technology for testing and evaluation at December’s Operational Experimentation (OpEx) in Texas. Specifically, it is looking for on-body, incident area, agency-wide or cross-jurisdictional capabilities such as sensors, data analytics tools and interfaces. [The official notice provides details on the specific gaps S&T is looking to fill and more information.](#)

In addition to the NGFR, [current Apex programs](#) support flood resiliency, border security, airport screening and cybersecurity. S&T’s overarching goal is to integrate new technology, tools and knowledge products into everyday use by first responders.

(Source: [DHS S&T](#))

Upcoming FLETC training schedule for SLTT law enforcement

The [Federal Law Enforcement Training Centers](#) (FLETC) released its third-quarter training course schedule. The schedule currently listed on the FLETC site runs through the end of September 2018.

FLETC offers both free and at-cost training for sworn state, local and tribal law

Highlights

Unannounced hospital mystery patient drills and toolkit

DHS Science & Technology Directorate puts out call for new technology

Upcoming FLETC training schedule for SLTT law enforcement

Webinar: learn how to strengthen your organization’s cybersecurity



U.S. Fire Administration

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

enforcement officers. Most courses are at the four FLETC locations in [Georgia](#), [New Mexico](#), [South Carolina](#) and [Maryland](#), but many courses are held at other locations all around the country. Examples of available no-cost training:

- Tactical Medical for First Responders.
- Active Shooter Threat Instructor Training Program.
- Leadership Through Understanding Human Behavior.
- Back Country Tactical Training Program.
- Basic Incident Response to Digital Evidence.

Interested officers can review the schedule and associated requirements for applying on the [FLETC Application for Student Training](#) site.

(Source: [FLETC](#))

Webinar: Learn How to Strengthen Your Organization's Cybersecurity

The economic cost of cybercrime is somewhere around \$1.5 trillion annually and rising. The Emergency Services Sector (ESS) is a target for cybercriminals. As the Sector increasingly relies on technology, protecting against cyber risks becomes vital to successful operations.

DHS's [Emergency Services Sector Cybersecurity Initiative](#) offers departments and agencies resources tailored to the Sector's unique needs. Leaders should review the ESS Cybersecurity Framework Implementation Guide, the ESS – Cyber Risk Assessment, and Roadmap to Secure Voice and Data Systems. Other resources are also available through the ESS Cybersecurity Initiative.

On Wednesday, March 28, 2018, from 12-1 p.m. Eastern, the [C3 Voluntary Program](#) will participate in a webinar highlighting cybersecurity resources and best practices.

Hosted by Federal Emergency Management Agency (FEMA) Region II and the FEMA Individual and Community Preparedness Directorate, the webinar provides an overview of two programs:

- The Department of Homeland Security (DHS) will discuss incident response, hands-on technical assistance and information sharing resources available from the Critical Infrastructure Cyber Community (C3) Voluntary Program.
- The Financial Services Information Sharing and Analysis Center (FS-ISAC) is presenting on how its trusted network can assist with crisis planning, exercises, and response and recovery activities.

Join the webinar to learn about resources for agencies of all types and sizes. [Interested parties must register.](#)

(Source: [C3 Voluntary Program](#))

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local [FBI office](#) and also the [State or Major Urban Area Fusion Center](#).

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.

The U.S. Fire Administration maintains the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC). For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Disclaimer of Endorsement: The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.