Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 20 — Issue 23 | June 4, 2020

DHS updates Chemical Properties Database for Law Enforcement Ops

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate released the latest version of its Chemical Agents Reactions Database (CARD), designed to help law enforcement authorities identify harmful chemicals.

The latest CARD is part of the S&T Chemical Security Analysis Center's (CSAC) efforts to collate data such as molecular structure, toxicity and boiling point levels to provide insight into how "chemicals of interest" are produced and used. To date, the database has information on over 1,000 chemicals and 2,000 chemical synthetic methods.

If, for example, officers found labeled chemicals in a clandestine laboratory, they could put these names into CARD as a list to find out if the suspects were making, illicit drugs, poisons, or warfare agents.

The CARD platform is hosted on a Department of Defense (DoD) server and contains both classified and unclassified data. It is accessible to state and local agencies as well as authorized personnel at DHS and the Department of Justice (DOJ).

For more information on the CARD or if you want a demonstration, please contact Dr. David Morton at David.Morton@ST.DHS.GOV. To get other CSAC knowledge management products including current news and daily opensource report, please also email Dr. Morton.

(Source: S&T)

CISA releases first of six Cyber Essential Toolkits

The Cybersecurity and Infrastructure Security Agency (CISA) released the first in a series of six Cyber Essentials Toolkits as a follow-up to the November 2019 release of Cyber Essentials. This is a starting point for government agencies and small businesses to understand and address cybersecurity risk as they do other risks.

CISA's toolkits provide greater detail, insight and resources on each of the Cyber Essentials' six "Essential Elements" of a Culture of Cyber Readiness. Today's launch highlights the first "Essential Element: Yourself, The Leader" focusing on the role of leadership in forging a culture of cyber readiness in their organization with an emphasis on strategy and investment.

Developed in collaboration with state and local governments and small businesses, Cyber Essentials aims to equip smaller organizations that historically have not been a part of the national dialogue on cybersecurity with basic steps and resources to improve their cybersecurity. Cyber Essentials includes two parts - guiding principles for leaders to develop a culture of security, and specific actions for leaders and their information technology professionals to put that culture into action.

Each of the six Cyber Essentials includes a list of actionable items anyone can take to reduce cyber risks. These are:

- Drive cybersecurity strategy, investment, and culture.
- Develop heightened level of security awareness and vigilance.

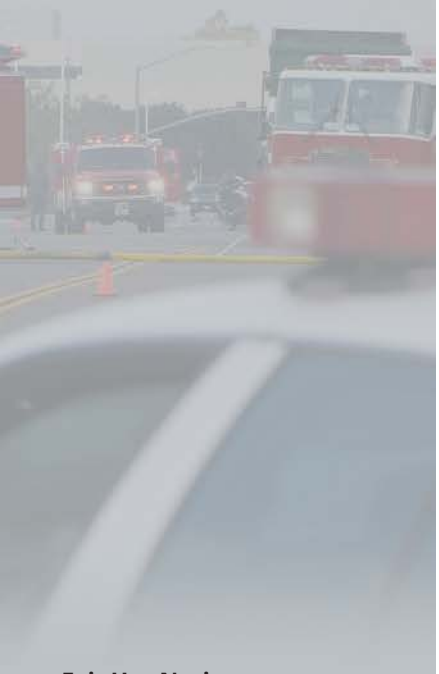
Highlights

U.S. Fire Administration

The U.S. Fire Administration operates 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.

Subscribe here



- Protect critical assets and applications.
- Ensure only those who belong on your digital workplace have access.
- Make backups and avoid loss of info critical to operations.
- Limit damage and restore normal operations quickly.

(Source: CISA)

Medical Operations Coordination Cells toolkit

The Healthcare Resilience Task Force released the first edition of the Medical Operations Coordination Cells (MOCC) Toolkit to help regional government ensure load-balancing across healthcare systems during pandemic response.

MOCCs work within emergency operations centers at the regional, state and federal levels. They help enable patient movement, staffing and resource allocation. Those involved in MOCC operations may include EMS, healthcare facility staff, and state and local government partners.

The toolkit offers sample Standard Operating Procedures for the three levels of MOCCs:

- Sub-State, Regional MOCC (RMOCCs).
- State MOCC (SMOCCs).
- Federal Regional MOCC (FMOCCs).

Sample documents consist of forms, checklists, situation report templates and transportation flow. This toolkit also covers funding solutions from several federal sources and data management systems for patient tracking and resource allocation.

(Source: Technical Resources, Assistance Center, Information Exchange (TRACIE))

State-by-State Reopening Guidance

The United States Chamber of Commerce is tracking the status of each state as they move toward reopening and offers a helpful webpage listing reopening guidance. Though it is primarily geared toward businesses, this information is helpful for first responders to know.

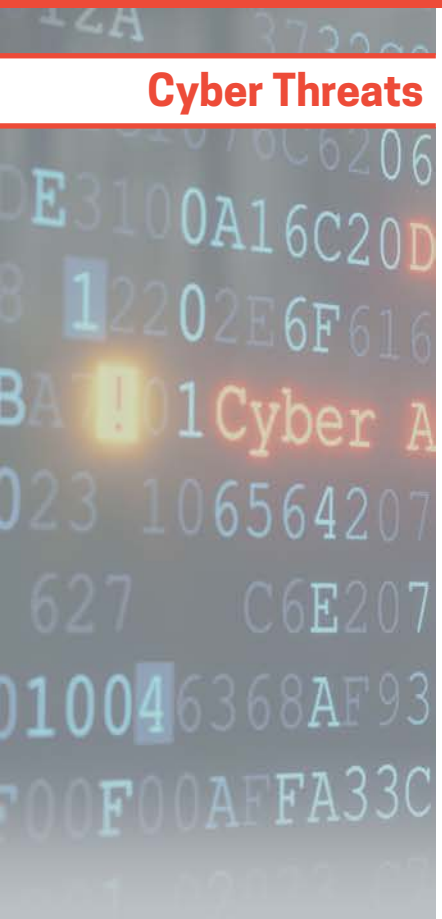
By clicking a state on the color-coded map, you get a page dedicated to the details of that state's reopening plan to include:

- Effective dates.
- Links to the governor's full reopening plan.
- Top-line guidance on public PPE use.
- Social distancing guidelines.
- Sector-specific recommendations.

This is a helpful, succinct resource to have available, especially for those people who may need to cross state borders regularly for work or personal reasons. You may consider sharing this with people living in your jurisdiction so they have a better idea what is expected of them as we move forward.

(Source: U.S. Chamber of Commerce)

Cyber Threats



Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

Hackers and hucksters reinvigorate 'Anonymous' brand amid protests

The internet activist movement known as Anonymous staged an online resurgence in the past week on the back of real-world protests against police brutality.

Born from internet chat boards more than a dozen years ago, the collective was once known for organizing low-skill but effective denial-of-service attacks that temporarily shut down access to payment processors that had stopped handling donations to the anti-secrecy site WikiLeaks.

But accounts using variations of the Anonymous name recently claimed credit for temporarily knocking a Minneapolis police website offline and, inaccurately, for hacking police passwords.

(Source: Reuters)

Health Industry Cybersecurity Tactical Crisis Response Guide

The Health and Public Health Sector Coordinating Council released the Health Industry Cybersecurity Tactical Crisis Response Guide last month to give the sector more tools to combat cyberattacks.

Many hospital systems around the world have been victims of ransomware and other attacks over the past few months, proving hackers and cybercriminals are still willing and able to carry out attacks against healthcare organizations during a serious crisis.

Healthcare organizations need a tactical response for managing cybersecurity threats. This guide will help those in the Health and Public Health Sector as well as government experts plan for and manage cyberattacks. It will also help refine any plans you may already have written.

(Source: HPH Sector Coordinating Council)

NSA warns of ongoing Russian hacking campaign against US systems

The National Security Agency (NSA) warned government partners and private companies about a Russian hacking operation using a special intrusion technique to target operating systems often used by industrial firms to manage computer infrastructure.

The notice is part of a series of public reports by the spy agency, which is responsible for both collecting foreign intelligence and protecting Defense Department systems at home, to share actionable cyber defense information.

(Source: New York Times)

Ransoms grew by a factor of 14 in one year

Ransomware has become one of the most insidious threats in the past couple of years, with actors scaling up their operations to the point that the average ransom demand increased more than 10 times in one year.

Since the GandCrab group called it quits in 2019, the ransomware landscape changed drastically. The ransomware-as-a-service model they introduced is now the norm, paving the way for professional attackers with a clear strategy to make money.

(Source: Bleeping Computer)

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