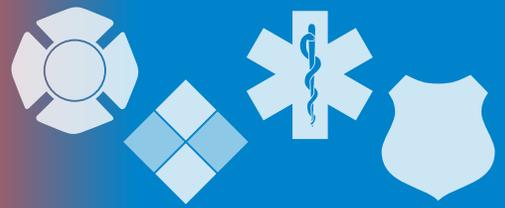# The InfoGram

DHS extends SAFER grant deadline, waives some requirements

In recognition of the economic hardships facing local jurisdictions and fire departments across the country as a result of the COVID-19 pandemic, Acting Secretary of Homeland Security Chad F. Wolf has waived the cost share, position cost limit, supplanting and minimum budget requirements for FY19 SAFER grant applicants. DHS/FEMA will provide more details on the FY 2020 changes soon.

In addition, the application period is being extended to May 27, 2020 at 5 p.m. Eastern. The waiver of the requirements identified above **does not** apply to the FY 2019 Assistance to Firefighters Grant Program (AFG) or to the FY 2020 Assistance to Firefighters Grant – COVID-19 Supplemental Program (AFG-S).

Funds under the FY 2019 SAFER Hiring of Firefighters Activity must be used to hire new, additional firefighters, and the costs to hire those firefighters must be at the usual annual costs of a first-year (i.e., entry-level) firefighter. This requirement has not been waived.

Applicants no longer need to request an economic hardship waiver within the FY 2019 online application. If you have already submitted your FY 2019 application, no further action is needed at this time.

If you have not yet submitted your application, please note the applications will continue to show the cost share/position cost limit. However, as stated above, there is nothing additional that applicants need to do regarding these provisions. The adjustment will be made by the SAFER Program Office.

For details on the changes, see the related documents on the FY2019 SAFER Grants website.

(Source: FEMA)

FEMA creates exercise documents for COVID-19 reopening planning

The Federal Emergency Management Agency (FEMA) developed an Exercise Starter Kit with sample documents your organization can use to conduct your own planning workshop to navigate the complexities of returning to full operations during the COVID-19 pandemic.

The Exercise Starter Kit includes a sample facilitator guide and conduct slides designed to be adapted and customized for your own needs. Suggested discussion questions for the workshop build upon reconstitution planning principles and relevant White House guidance for employers included in the Guidelines for Opening Up America Again.

(Source: FEMA)

Communication cards break barriers for those with hearing disabilities

The nonprofit organization Disability Rights of West Virginia (DRWV) collaborated with fire and EMS departments and other disability-support organizations in the state to develop a Communication Board to help fire and EMS personnel assist people with disabilities who may be having an emergency.

[The card is designed to help gather medical, physical and emotional information from a patient who is deaf, hard of hearing, autistic or who may have an intellectual disability](#). It is designed for patients to touch pictures to express their wants and needs, and gives medical professionals the ability to help through Quick Communication Tips.

DRWV developed a [visor card for both citizens and law enforcement officers](#) to provide better communication options. Availability of the visor card prompted EMS personnel to request a similar product for their specialized work. See this [video describing how the cards work](#).

While West Virginia's cards are available for download at the links above, your state may have something similar. Check with the appropriate state office or nonprofit organizations to find out if these products are available. If not, suggest they create such cards.

(Source: [State of West Virginia](#))

Technology Clearinghouse: Promoting Innovative Solutions

The Department of Homeland Security (DHS) Science & Technology Directorate (S&T), through its online [Technology Clearinghouse](#), provides the homeland security community with curated information to aid in the development, procurement and deployment of innovative technology solutions to address homeland security challenges.

The TCH, mandated by Congress, provides authoritative and actional information on technology requirements and gaps, technology scouting activities, testing and evaluation findings, and funding opportunities.

In a future phase of the TCH, state and local government, first responders, emergency management agencies and other homeland security professionals will have secure access to an expanded and customized library of knowledge content, as well as a community forum area to collaborate with other TCH users.

Until the next phase of the TCH is ready, the team is expanding ways to provide you with resources you need to help you select the best technology to carry out your mission. The TCH team is producing a Pathways to Innovation Learning series available via webinar featuring a variety of topics of interest for first responders. Some future topics may include "Advancements in Emergency Communications Beyond 5G" and "Small Unmanned Aerial Systems (UAS) and Counter UAS."

Additionally, to provide guidance to the first responder community and assist you to conduct activities as safely and efficiently as possible during the COVID-19 pandemic, DHS S&T, led by the Technology Clearinghouse, is providing links to authoritative resources to help inform and guide actions. The resources include valuable information about the rapid development of innovative Personal Protective Equipment (PPE) open-source designs, subsequent production and manufacturing, and other guidelines. Visit the [COVID-19 Information for the First Responder Community](#) page, or [Innovative Public-Private Partnerships Help to Address First Responder Protective Equipment Challenges During COVID-19 Pandemic](#) page to discover these resources and stay informed.

For questions or more information, please reach out to the TCH team at [SandT_TechClearinghouse@hq.dhs.gov](#).

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

Cyber Threats

Cyber Diligence and Health Crises

The Department of Health and Human Services (HHS) CSA 405(d) Task Group released the one-page safety sheet Cyber Diligence & Health Crises to help the medical community keep patients safe.

The graphic is short and simple, listing the top five cybersecurity threats and the five cyber safety tips medical personnel can use to avoid falling for them.

This sheet would be a good handout for staff or poster to hand around the workplace. See the HHS CSA 405(d) Task Group website for more cybersecurity information geared toward the healthcare sector.

(Source: HHS 405d)

Phishing attacks lure through threat of termination, stimulus money

Two new phishing attacks are trying to exploit employee fears by delivering fake "Zoom meeting about termination" emails and fake notifications about COVID-19 stimulation/payroll processing.

One campaign comes in the form of emails seemingly coming from the organization's human resources department, urging the recipient to attend a Zoom meeting scheduled to start in a few minutes to discuss the employee's termination.

The second phishing campaign is made to look like an email from an outsourced contractor informing employees of additional stimulus being provided to them and asking recipients to view the latest payroll report.

(Source: HelpNetSecurity)

CISA releases Cybersecurity Framework for Emergency Service Sector

The Cybersecurity and Infrastructure Security Agency (CISA) released the final approved Cybersecurity Framework Implementation Guidance for the Emergency Services Sector.

Based on the National Institute for Standards and Technology's 2018 Framework for Improving Critical Infrastructure Cybersecurity, this document provides guidance for private sector organizations to improve their ability to prevent, detect and respond to cyberattacks.

Local jurisdictions are top targets of malware and phishing campaigns. All departments and agencies should be working to strengthen their cybersecurity posture, this framework can be a good guide to work from.

(Source: CISA)

6 Steps to Securing IoT Devices and Taking Back Your Privacy

In today's world we are more connected than ever — not only to each other, but to our devices. For example, people now have the ability to open and close their garage doors and even start their cars directly from their phones. But what information do we put at risk when we do all of these amazing things? Securing Internet of Things (IoT) devices and keeping personally identifiable information (PII) safe and secure these days is of the utmost importance.

(Source: CISecurity.org)

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

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