Building a Culture of Cyber Preparedness

October is National Cybersecurity Awareness Month; a month to ensure all Americans are safer and more secure online. At FEMA, we are always focused on preparing ourselves, our partners, and the American people for the many threats and hazards we face as a nation. As the need for cybersecurity has grown, so too has our cyber preparedness efforts.

In partnership with our colleagues at the Cybersecurity & Infrastructure Security Agency (CISA), we support numerous programs aimed at making the nation more resilient to cyber-attacks. In the past ten years, we have invested over $165 million in grant funding to bolster state and local jurisdictions' cyber preparedness. While more can always be done, this funding addresses what we are seeing in national reports and assessments where cybersecurity is identified as a national area for improvement. Our state and local partners are using the funding to develop cybersecurity plans and programs, provide training, conduct outreach and exercises, and acquire hardware and software, firewall enhancements, and closed emergency network infrastructure.

Just like a more traditional response to a natural disaster, we must also be ready to respond to a "cyber disaster" as a cyber-attack can trigger physical consequences. These physical consequences could result in significant impacts to governments, businesses, and individuals. Thus, we work with CISA and other federal agencies to ensure our response plans are coordinated and rehearsed regularly with our government and private sector partners.

Next year we are facilitating a national level exercise based on a major cyber-attack. The exercise, known as NLE 2020, will integrate several existing exercises, including CISA's series of exercise modules called Cyber Storm. This will enable us to examine different phases of a connected incident through a unified and collaborative effort. The exercise participants will include all levels of government and the private sector. We will examine each participants' respective roles and responsibilities to respond to such an event. Our joint goal is to ensure this is the largest and most impactful cyber exercise for all our stakeholders. Exercises, such as this large-scale event or the more frequent offerings led by CISA, are instrumental in increasing our level of preparedness for cybersecurity incidents.

We also provide our state and local partners with the technical skills they require to make their communities more secure and resilient to cyber-attacks. We offer over 20 online and in-person courses, focused on everything from network assurance and digital forensics, to information security and cyber incident response. Since 2004, FEMA has trained more than 87,000 federal, state, local, tribal, and territorial officials on cybersecurity.

But cybersecurity does not fall squarely on the shoulders of government. Every American has a role to play, which is why this month is focused on raising awareness about what you can do to protect yourself at home, work, or school. Using complex and different passwords for your accounts, keeping your antivirus software and operating systems up to date, and scrutinizing emails before clicking on links are simple things that make a big difference. The theme of this year's awareness month is "Own IT. Secure IT. Protect IT." because these individual steps are

often more important than technological solutions. Learn more about what you can do at www.Ready.gov/cybersecurity.

Preparedness is a team sport. Whether it be for natural disasters or cyber-attacks, it takes all of us to reduce our vulnerability to these risks. Given increasing cyber threats, we should strive to build a culture of cyber preparedness.

Daniel Kaniewski is deputy administrator for resilience at the Federal Emergency Management Agency and the Agency's Acting Deputy Administrator.