Global Covid-19 cases surpass 250 million.
Town declares itself a ‘constitutional republic’ to buck Covid rules.
Study: Pfizer antiviral drug could nearly end deaths from COVID-19.
Monoclonal antibodies shown to prevent inflammatory consequences.
Strengthening public safety through the SERVE Act.
Bill addresses wildfire preparedness, response.
Report urges efforts to strengthen pandemic vaccine planning.
FEMA to require on-campus students be fully vaccinated.
Yahoo withdraws from China as Beijing’s grip on tech firms tightens.
Study finds early COVID isolation was positive for many.
Doctors declare national emergency in children’s mental health.
Military: penalties loom for those who refuse to get COVID-19 vaccine.
Poll: researchers of Chinese descent worry about surveillance by the US government and have stepped back from collaborations in China.
With prospects of herd immunity fading, endemic COVID-19 is upon us, and new “whole of society” approaches are needed.
Updated assessment on COVID-19 origins.
Syphilis is resurging in the U.S., a sign of public health's funding crisis.
When a scholar is accused of being a spy.
UK firm sold PIII location data without permission from users.
The pace of deaths has slowed amid the global inoculation push.
Tracking COVID-19
305,970
New cases reported worldwide, Oct. 31
5,005,546
Total deaths reported worldwide
7,099,262,864
Vaccines doses administered in 194 countries
• The pace of deaths has slowed amid the global inoculation push.
• Upcoming winter will test immunity gained through vaccination
• With prospects of herd immunity fading, endemic COVID-19 is upon us, and new “whole of society” approaches are needed.
CALIFORNIA

- Here's why CA may be on the verge of COVID-19 winter surge.
- UCLA and UCSF awarded $41.5M to address toxic stress.
- Long Beach City College allow homeless students to sleep in cars.
- As strike looms, UC lecturers raise the stakes.
- Hastings Law will rebrand after outcry over namesake.
- AKKA extends partnership with UCR.
- UC Health supports CDC on COVID-19 vaccine for children.
- Study: Safe reopening of UC campuses during COVID-19 in Fall 2020.
- PG&E shareholders to pay $125M for igniting massive Kincade Fire.
- Mapping annual wildfire probabilities across California.
- Poll: Should California remain on daylight savings time?
- $10b worth of lost money - check database to see if any of it is yours.
- Drug companies win in California opioid crisis lawsuit.
- “It’s time to sound the alarm and expect more empty shelves.”
- Employers gathering data on work habits - labor advocates protest.
- Truckers tired of taking blame for congestion crisis at California ports.
- 350,000 students: Get vaccinated for Covid-19 or stay home.
- PG&E under federal investigation.
- $182 million in pandemic food aid is going unused in California.
- San Francisco Safeway makes decision to close early due to theft.
The County of Riverside Emergency Operations Center is currently activated to **Management Watch**.

**REGION**

- Environmentalists to [sue](#) the federal government over OC oil spill.
- Pomona school board votes to [bring police back](#) following 'defund' movement.
- Construction of [mega-dorm](#) at UCSB to continue despite resident architect quitting in protest.
- Vet sentenced to **25 years** for attempted bomb plot in Long Beach.
- **Special Alert program** will assist LE responding to calls involving disabilities.
- Irvine man [charged](#) with assault and interference with a flight crew.
- USC president says it took too long to [notify](#) community of sexual assault at fraternity parties.
- Long Beach [school safety officer](#) faces second-degree murder.
- Former [Cal Fire firefighter](#) from Hemet gets 4 years for arson, fraud.

### Majorities across regions say California's leadership in climate change is important

<table>
<thead>
<tr>
<th>Region</th>
<th>Very important</th>
<th>Somewhat important</th>
<th>Not too important</th>
<th>Not at all important</th>
</tr>
</thead>
<tbody>
<tr>
<td>All adults</td>
<td>43</td>
<td>28</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>Central Valley</td>
<td>33</td>
<td>20</td>
<td>28</td>
<td>17</td>
</tr>
<tr>
<td>Inland Empire</td>
<td>41</td>
<td>28</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>54</td>
<td>29</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>Orange/San Diego</td>
<td>36</td>
<td>31</td>
<td>13</td>
<td>19</td>
</tr>
<tr>
<td>SF Bay Area</td>
<td>44</td>
<td>31</td>
<td>13</td>
<td>10</td>
</tr>
</tbody>
</table>

- **Most Californians** expressed that the state's climate change leadership around the world is very (43%) or somewhat (28%) important to them (likely voters: 46% very, 25% somewhat).

- **Majorities of Democrats** (90%), independents (61%), and Republicans (58%) say it is at least somewhat important that California act as a leader in efforts to fight climate change.

- **2 in 3 adults and likely voters**—are in favor of the state government making its own policies, separate from the federal government, to address climate change.
COMMUNICATIONS

• 08 November:
  • Upcoming Standard First Aid w/CPR/AED/Adult/Pediatric training

• 05 November:
  • UCRRA Scholarship applications open

• 04 November:
  • Nationwide aerosol monitoring network launches with a site in Riverside

• 03 November:
  • 12th Annual Inland Empire Economic Forecast Conference: 10 Nov., 3-5 pm

• 02 November:
  • VPIA Search Announcement

Please Reference Notes Section For More Information
NOTABLE

- Narco-Messages and Targeted Assassinations in Mexico Indicate Worsening Turf Wars
- While The Rest Of Us Die: The secret history of the government's Doomsday plans
- Disaster Zone Podcast: The 2017 Las Vegas Mass Shooting
- Cyber Warfare Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)
- Federal cybersecurity leaders are eager for new hiring powers
- LA city councilman faces federal charges for behavior that’s become all too common
- Podcast: Extreme heat, the silent killer
- Facebook: ‘Nanotargeting’ Users Based Solely on Their Perceived Interests
- Tips for improving your approach to business continuity exercises
- First-time gun buyers in pandemic surge more likely to have had suicidal thoughts
- Revisiting ‘The Degradation of the Academic Dogma’
- People are leaving jobs in droves. Here’s what makes them stay
- Webcast: Why Most Schools Are NOT Fully Prepared for a Lockdown
- A Psychologist Shares Common Warning Signs, Motives Among School Shooters
- Could Artificial Intelligence Save the Holiday Shopping Season?
- The Metaverse is Mark Zuckerberg's escape hatch
- Hunted by Taliban, 'abandoned' former Afghan spies turn to ISIS
- Data Breach at University of Colorado
- Microsoft Launches Community College Cybersecurity Program
- Wharton School is accepting cryptocurrency for tuition payments
The National 911 Program is housed within the Department of Transportation’s National Highway Traffic Safety Administration (NHTSA) and is a joint program with the Department of Commerce’s National Telecommunication and Information Administration.

The National 911 Program is responsible for improving coordination and communication among federal, state, and local ECCs, personnel, and telecommunications carriers and vendors.

One of the Program’s primary objectives is to develop and share resources concerning the technology used in providing 911 services.
What is Next Generation 911 (NG911)?

• **What is Next Generation 911 (NG911)?**
  - NG911 is a digital, internet protocol (IP)-based system that will replace the analog 911 infrastructure that’s been around for decades.
  - NG911 includes the hardware, software, data and all the procedures and policies that relate to answering every emergency request for help.

• **How does a NG911 system work?**
  - A next-generation system has four main building blocks: the ESInet (Emergency Services IP Network), Next Generation Core Services (NGCS), NG911 calltaking equipment, and a geographic information system (GIS).

• **Why do we need NG911?**
  - Americans have moved away from landline phones to cell phones and VoIP, in which calls are made via the Web, public safety must adapt to these new communication tools to best serve our communities.

• **How soon will my PSAP/ECC move to NG911?**
  - The transition to NG911 varies widely across the country.
  - States, counties, cities and local authorities are figuring out how to start or complete their own switch away from legacy systems.
  - A few have even made the transition to a next-gen network. According to a 2020 report from the National 911 Program, 33 states reported adopting a statewide NG911 plan.

NG911 is much more than just receiving text messages or even video from someone in distress. It will dramatically improve the ways in which all of public safety serves its communities.
PROGRESS TOWARD NG911

The voluntarily reported data shown here identifies the percentage of PSAPs/ECCs in each state that are capable of processing NG911 emergency calls for all service types (wireline, wireless, VoIP) using next-generation infrastructure and GIS that meets nationally accepted standards.

- 0%
- >0-25%
- 26-50%
- 51-75%
- 75-99%
- 100%
- Unknown
- Did not submit

Source: National 911 Annual Report: 2019 Data, National 911 Program

When fully deployed, NG911 will do things we only dream of today, like seamlessly working with other agencies and neighboring jurisdictions—even with colleagues across the country.
Roadmap: Connecting Systems

Business Governance Goals
Identify strategies and resources to address policy, regulatory, governance, and funding issues or obstacles faced by jurisdictions both independently (along their transition to NG911 capabilities) and collectively as they relate to achieving nationwide interconnectivity.

Technical Goals
Stimulate adoption and enable implementation of NG911 technology by promulgating NG911 open standards and establishing means by which emerging technologies can be validated for compliance and security.

Data Goals
Support the enhancement of 911 services by establishing technical and operational data solutions that support cross-jurisdictional and nationwide situational awareness, information sharing, and predictive data analysis.

Operational Goals
Distinguish, enhance, and promote operating procedures, performance, evaluation, and professional development strategies that support complete and streamlined implementation of NG911 capabilities.

Cross-Cutting Goals
Facilitate education and knowledge transfer on an ongoing basis.
National 911 Program Interoperability

1. Public Emergencies
   - Public sends information and data like video footage to 911

2. NG911 Call Centers
   - Receive and triage information and rich data from 911

3. FirstNet
   - Wireless network shares information and rich data from 911 with first responders

4. First Responders
A variety of public and private entities are also conducting a series of activities to contribute to the ultimate goal of understanding, establishing, and widely deploying a uniform interconnection.
Better Location Accuracy
NG911 tools allow you to get not just a caller’s latitude and longitude, but an extremely accurate dispatchable location. PSAPs will be able to view, too, a three-dimensional map showing which floor in a building someone is calling from. Even better, all the data that comes in with a next-gen call can be immediately transferred to field responders, medical providers or others who may need the information.

Improved Crash Data
Telematics, already integrated into many vehicles, are capable of notifying 911 with precise location information and crucial details like speed at impact, airbag deployment, number of occupants, and how many seat belts were in use. This data, available at dispatch, helps fire services and EMS prepare appropriate equipment and provides medics with key information to plan for transport to the appropriate hospital or trauma center.
How NG911 Can Benefit Emergency Mgt.

Public Safety Communications Center
- Information to 911
- Information from 911

More Ways to Help All Types of Callers
NG911 will enable new services like language assistance/translation for non-native English speakers and help for the deaf and hard-of-hearing. These technologies will be embedded in Next-Gen platforms, making them seamless for telecommunicators to use.

Improved Field Responder Safety & Awareness
New and emerging technologies in the NG911 environment provide information in the form of photos, streaming video, texts and other data that helps your colleagues in law enforcement, fire services and EMS better understand what’s happening even before they’re on-scene. Telecommunicators can access building sensors and video feeds, too, helping to identify hazardous materials, environmental conditions or the location of potential victims.
Protecting 911 from Ransomware

PROTECT YOUR CENTER FROM RANSOMWARE

TEXAS DEPARTMENT OF INFORMATION RESOURCES (DIR)

RANSOMWARE: WHAT IS IT?
Ransomware is a type of malicious software (a.k.a. a malware) that cyber criminals use to extort money from organizations. Once activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive. There are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

1. Contact your IT department and supervisor immediately.
2. If you can locate the Ethernet cable, unplug the computer from the network.
3. If you can't disconnect the computer from the network, unplug it from power.
4. For laptop: shut down the power button until the light is completely off and remove the battery if possible.

IMPORTANT CONTACTS

STATE OF TEXAS
- Network Security Operations Center (NSOC)
  (832) 639-6702 24x7
  security-alerts@dir.state.tx.us
- Operation 1: Network
- Operation 2: Security
- DIR Cybersecurity Incident Response Team
  and Assistance Hotline 1-877-408-0747 24x7
- Commission on State Emergency Communications
  (CSEC) 1-877-767-2722

FEDERAL PARTNERS
- Cybersecurity and Infrastructure Security Agency (CISA)
  (866) 282-0870
  cisa.gov
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  (902) 737-4722
- FBI Internet Crime Complaint Center (IC3)
  ic3.gov
- FBI Dallas Field Office (972) 559-5000
- FBI El Paso Field Office (915) 832-5000
- FBI Houston Field Office (713) 593-5000
- FBI San Antonio Field Office (210) 223-5741
- FBI Field Office Cyber Task Forces
  www.fbi.gov/contact-us/fi

If you have any questions, please contact the Office of the Texas Statewide Interoperability Coordinator (SWIC) at swic@texaspublicsafety.org

PROTECTING YOUR CENTER

Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.

- Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.
  - Be suspicious of any email asking you to follow a link or open an attachment.
  - If you are not expecting an email attachment from a coworker, give them a call to verify.
  - Report suspicious emails to your IT staff.
- Never click on or download attachments from unknown or unsolicited sources.

SOCIAL ENGINEERING

Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trust relationships.

- Remove any work-related information from your social media accounts.
- Be suspicious of emails from unknown sources asking you to click a link or open an attachment.
- Drive-by Download
  - Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious website can enable attackers to infect your systems.
  - Never browse the Internet from a computer with access to CAD, RMS, or other mission critical systems.
  - If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled.
- Website browsing should be limited to websites related to your mission and job responsibilities.

TACTICAL STRATEGIES FOR ESSENTIAL PERSONNEL

Attacks can be prevented by increasing security measures. If you work in an area where your computer can be accessed by unauthorized personnel:

- Use strong passwords that include upper and lower case letters, special characters, and numbers, or use a 4-word pass phrase if the option is available.
- Do not share passwords with other users, protect them, and change them periodically.
- Never leave your computer unattended.
- Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave themselves in public places hoping you will insert them into your computer.
- Never connect USB devices to CAD, RMS, or other mission critical systems.
- Never leave any device unattended when it is connected to a computer.
- Never charge any device on a wall outlet.

Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave themselves in public places hoping you will insert them into your computer.