UC RIVERSIDE

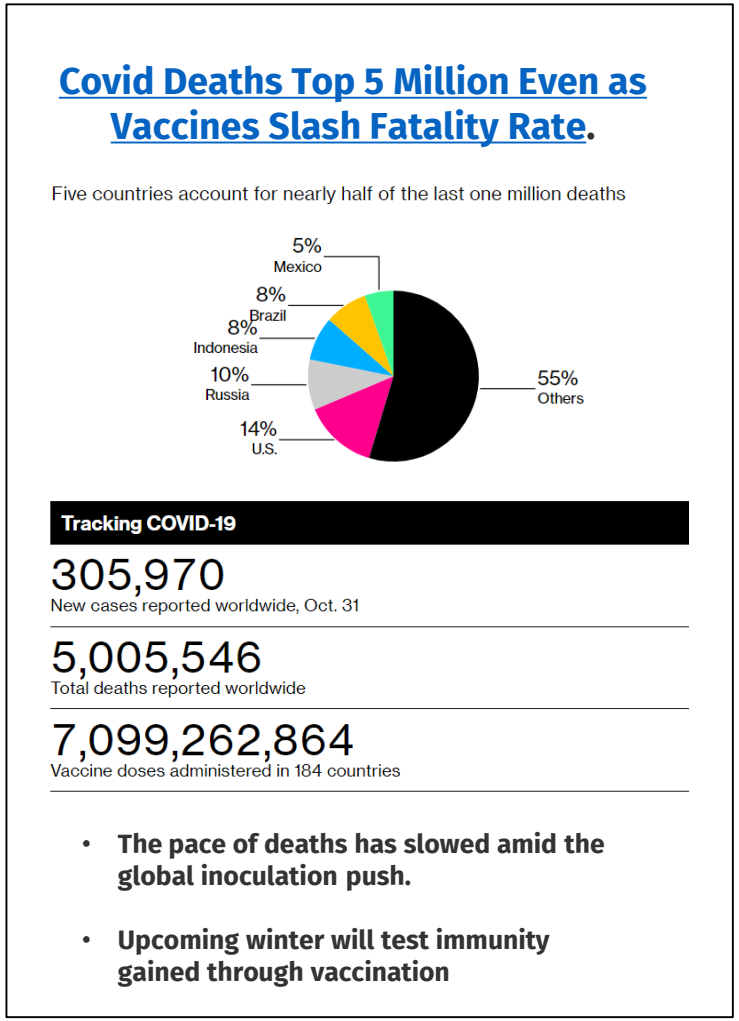
OEM: Weekly SITREP

November 09, 2021

UC RIVERSIDE Office of Emergency Management

USA & WORLD

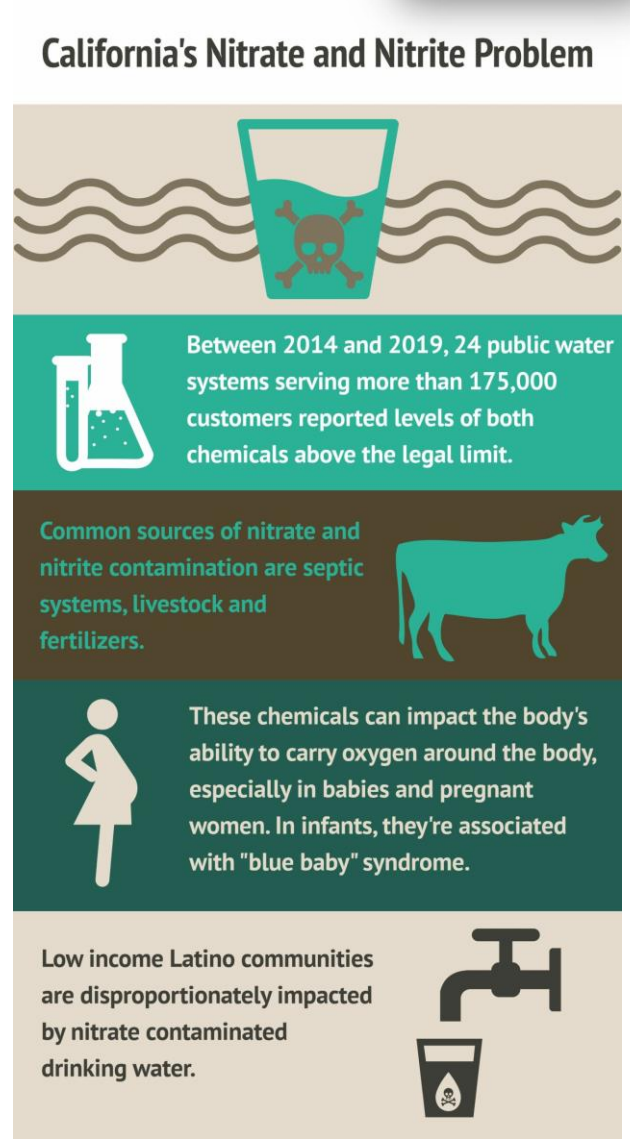
- Global Covid-19 cases surpass 250 million.
- Town declares itself a 'constitutional republic' to buck Covid rules.
- Study: Pfizer antiviral drug could nearly end deaths from COVID-19.
- Monoclonal antibodies shown to prevent inflammatory consequences.
- Strengthening public safety through the SERVE 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.



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.

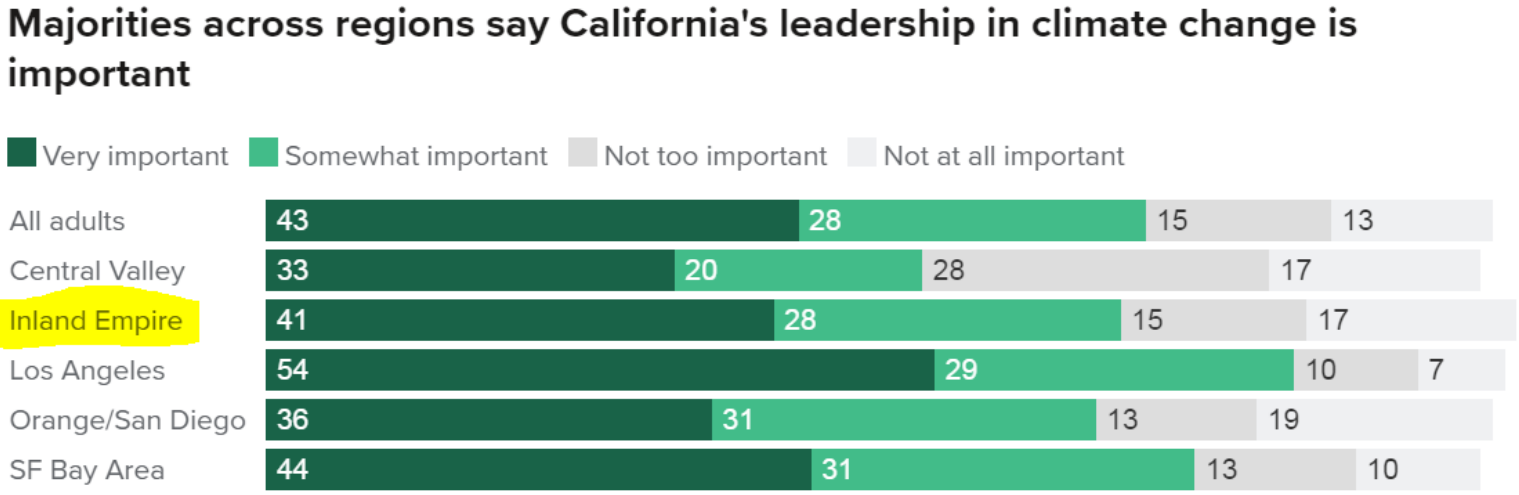
UC RIVERSIDE Office of Emergency Management



Disparities in California’s Tap Water Quality Persist, New Data Shows

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.



- **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**

The County of Riverside Emergency Operations Center is currently activated to Management Watch.

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

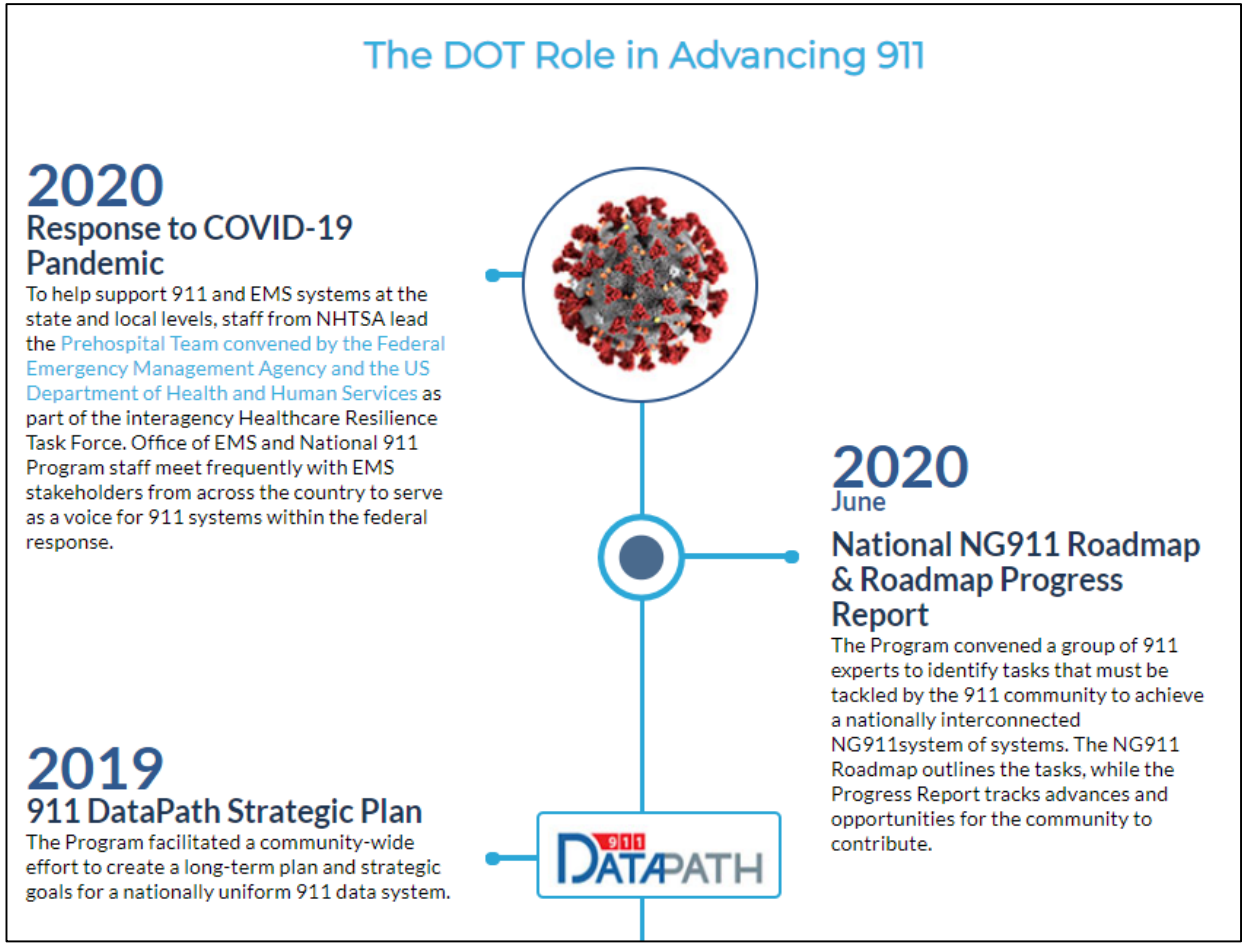
Please Reference Notes Section For More Information

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

National 911 Program

- 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)?

UC RIVERSIDE Office of Emergency Management

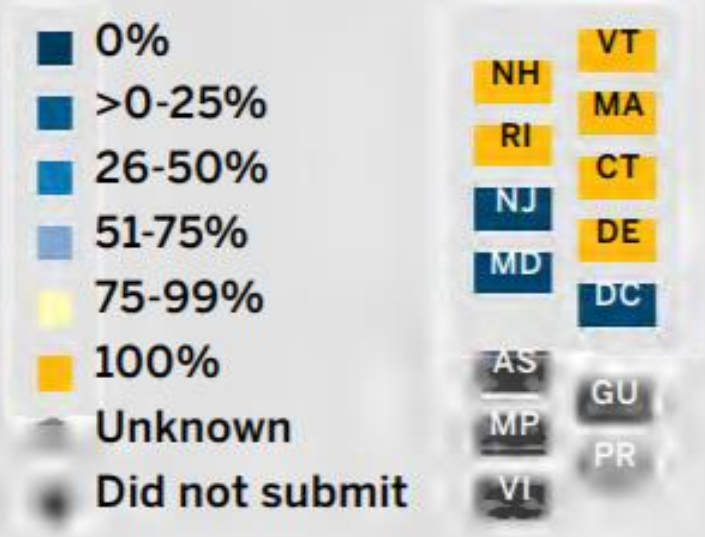
- **What is Next Generation 911 (NG911)?**
  - NG911 is a digital, internet protocol (IP)-based system that will replace the analog 911 infrastructure that's been around for decades.
  - NG911 includes the hardware, software, data and all the procedures and policies that relate to answering every emergency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

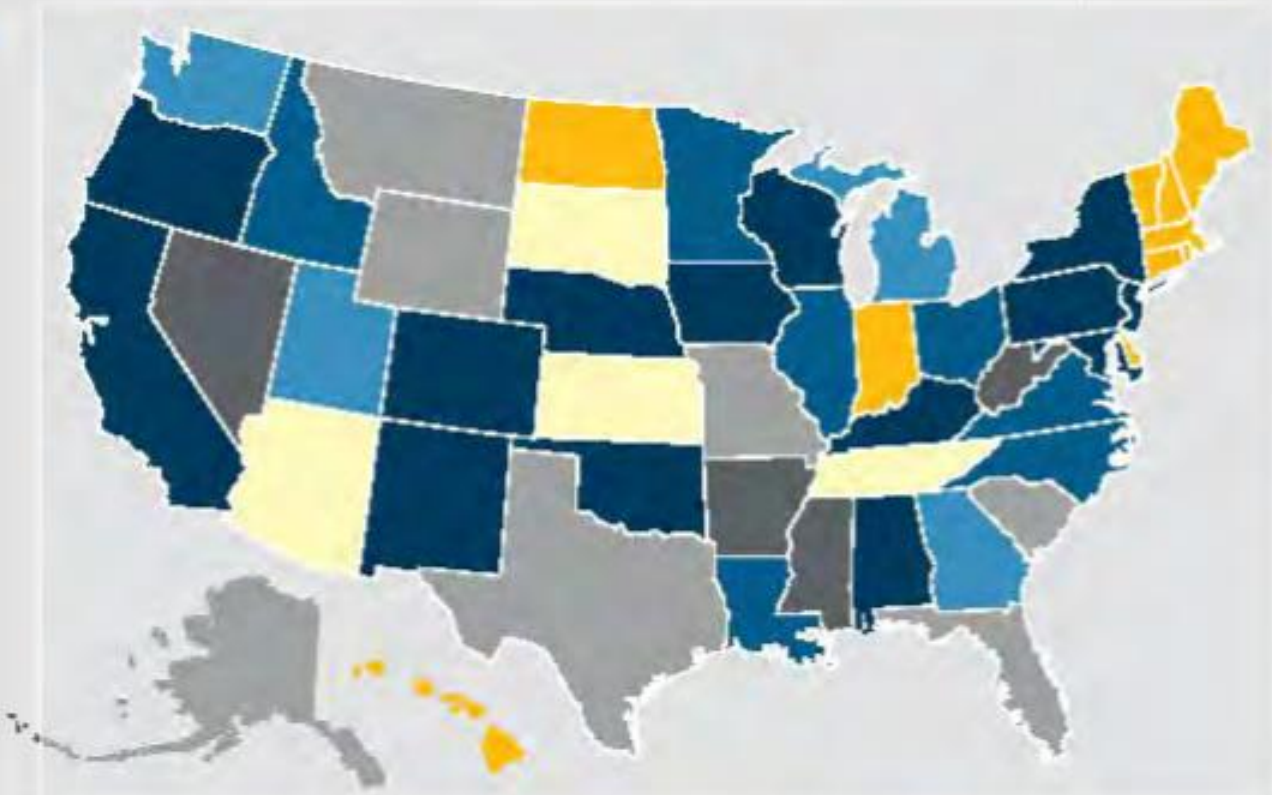
NG911 is much more than just receiving text messages or even video from someone in distress. It will dramatically improve the ways in which all of public safety serves its communities.

PROGRESS TOWARD NG911

UC RIVERSIDE Office of Emergency Management

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.





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

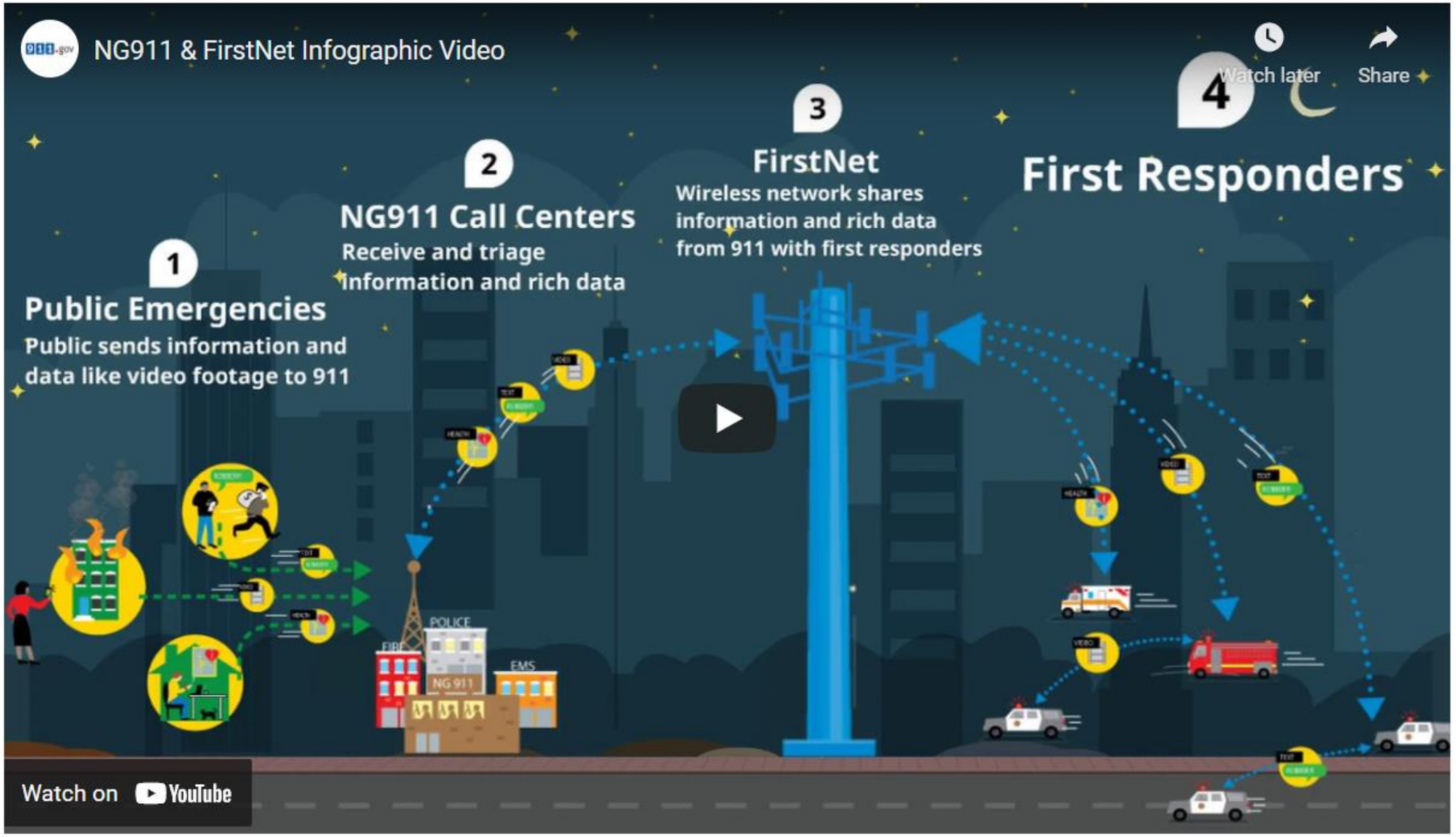
When fully deployed, NG911 will do things we only dream of today, like seamlessly working with other agencies and neighboring jurisdictions—even with colleagues across the country.

Roadmap: Connecting Systems

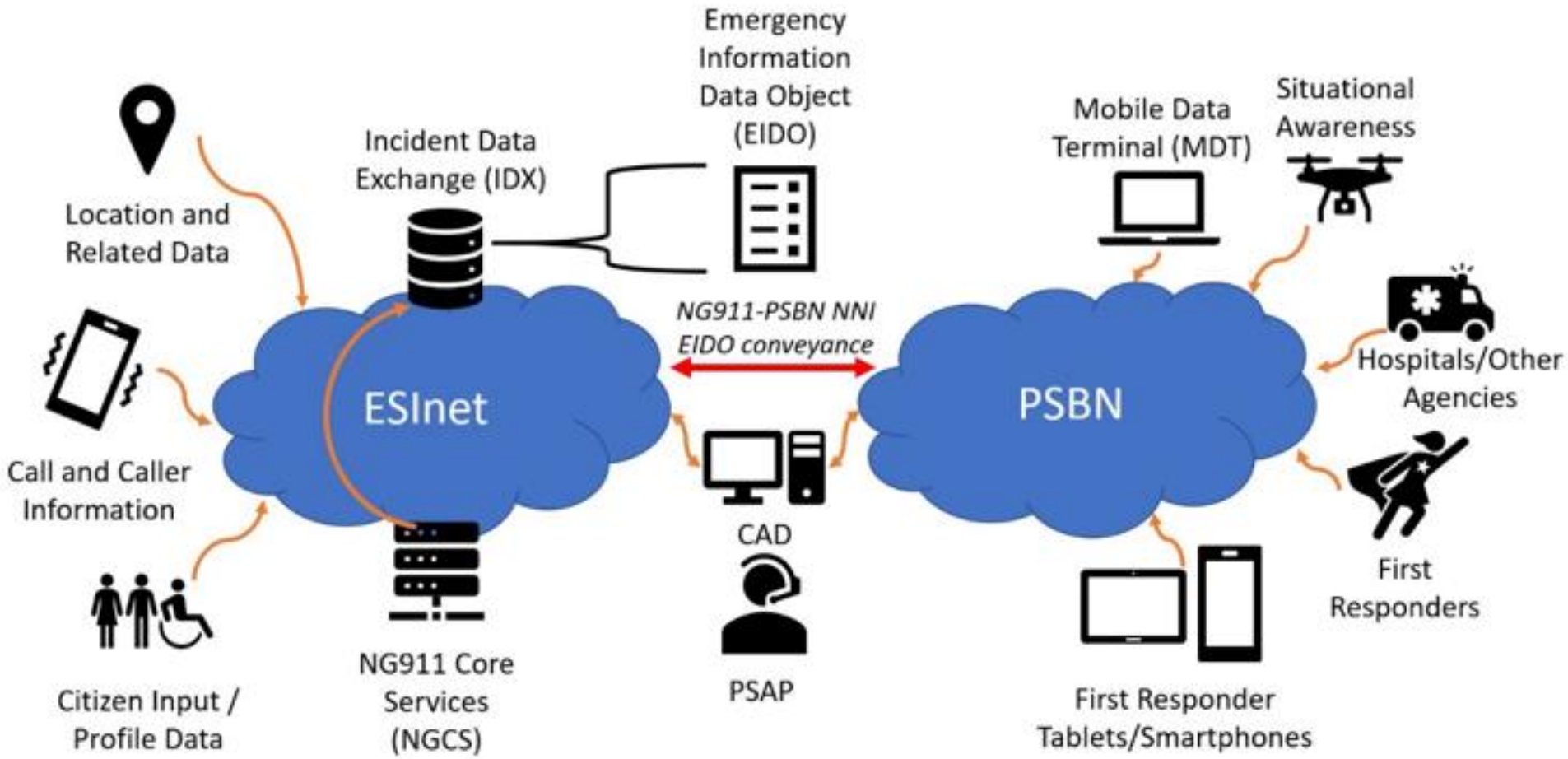
UC RIVERSIDE Office of Emergency Management

National 911 Program Interoperability

UC RIVERSIDE Office of Emergency Management



National 911 Program Interoperability



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.

How NG911 Can Benefit Emergency Mgt.

UC RIVERSIDE Office of Emergency Management

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.

UC RIVERSIDE Office of Emergency Management

Protecting 911 from Ransomware

UC RIVERSIDE Office of Emergency Management

PROTECT YOUR CENTER FROM RANSOMWARE

CSEC DIR

TEXAS DEPARTMENT OF INFORMATION RESOURCES (DIR)

RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When 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

   For laptops: hold down the power button until the light is completely off and remove the battery if possible

WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.

Note To Users:

Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.

⚠ *The Federal Government advises organizations NOT to pay any ransom. Organizations should maintain off-site, tested backups of critical data.*

IMPORTANT CONTACTS

If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance

STATE OF TEXAS*

- Network Security Operations Center (NSOC) (888) 839-6762 24x7 security-alerts@dir.texas.gov
  - Option 1: Network
  - Option 2: Security
- DIR Cybersecurity Incident Response Team and Assistance Hotline 1-877-347-2476 24x7
- Commission on State Emergency Communications (CSEC) 911alerts@csec.texas.gov

FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- FBI Dallas Field Office (972) 559-5000
- FBI El Paso Field Office (915) 832-5000
- FBI Houston Field Office (713) 693-5000
- FBI San Antonio Field Office (210) 225-6741
- FBI Field Office Cyber Task Forces www.fbi.gov/contact-us/field

*If you have any questions, please contact the Office of the Texas Statewide Interoperability Coordinator (SWIC) at txswic@dps.texas.gov

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.

PHISHING

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 co-worker, give them a call to verify
- ☑ Report suspicious emails to your IT staff
- ☑ Never check personal email from computers with access to Computer Aided Dispatch (CAD), Records Management System (RMS), or other mission critical systems
- ☑ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different— this is a red flag
- ☑ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

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 trusted relationships.

- ☑ Remove any work-related information from your social media accounts
- ☑ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ☑ Be suspicious of emails from coworkers and friends 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 site will enable malware or ransomware infection.

- ☑ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ☑ 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
- ☑ Web browsing should be limited to websites related to your mission and job responsibilities

USERNAME & PASSWORD COMPROMISE

Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain access to your agency's network. If your password is too simple, it can also be easily guessed.

- ☑ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ☑ Don't reuse passwords across different accounts and online services
- ☑ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, Etc)

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

- ☑ Never connect USB devices to CAD, RMS, or other mission critical systems
- ☑ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet