NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER

Energy, Environment & Natural Resources Committee

2024 Summer Board and Leadership Meeting

Rancho Cordova, CA

Wednesday, June 12, 2024, 1:00-5:00 p.m.
Thursday, June 13, 2024, 8:30-9:30 a.m.

NLC NATIONAL LEAGUE OF CITIES
CITIES STRONG TOGETHER

Summer Board & Leadership Meeting

Energy, Environment and Natural Resources Committee Meeting Agenda

Tuesday, June 11, 2024

5:00 p.m. – 6:30 p.m. **OPENING RECEPTION**
Sacramento Marriott Rancho Cordova – Outdoor Trellis, Lobby level

Wednesday, June 12, 2024

8:00 a.m. – 9:00 a.m. **BREAKFAST**
Sacramento Marriott Rancho Cordova – Outdoor Trellis, Lobby level

9:30 a.m. – 11:30 a.m. **MOBILE WORKSHOP: RANCHO CORDOVA CULTURAL EXPERIENCE**
Buses will load in the Marriott lobby starting at 9:00 a.m. and will depart promptly at 9:30 a.m. Light breakfast will be available prior to bus loading in the Outdoor Trellis.

Explore the rich culture of Rancho Cordova dating back to the 1800s and the Nisenan Indians.

Pre-registration required. To register, please click here.

11:30 a.m. – 11:45 a.m. **PRESS CONFERENCE**
Sacramento Marriott Rancho Cordova – Hotel Lobby

11:30 a.m. – 12:30 p.m. **ATTENDEE NETWORKING LUNCH**
Sacramento Marriott Rancho Cordova – Outdoor Trellis, Lobby level

12:30 p.m. **BUS DEPARTS TO EENR COMMITTEE MEETING LOCATION**
Buses will load in the Marriott lobby starting at 12:00 p.m. and will depart promptly at 12:30 p.m.

1:00 p.m. – 5:00 p.m. **ENERGY, ENVIRONMENT AND NATURAL RESOURCES COMMITTEE MEETING**
California Bureau of Automotive Repair, 10949 North Mather Blvd, Rancho Cordova, CA 95670

1:00 p.m. – 1:30 p.m. **WELCOME, INTRODUCTIONS AND MEETING OVERVIEW**

The Honorable Ruth Grendahl, Chair
Councilmember, City of Apple Valley, Minnesota

Councilmember Grendahl will welcome committee members and provide an overview of the agenda.

Committee member introductions – share one sustainability or climate initiative underway in your community or one grant program that your city has received or is applying for from the Bipartisan Infrastructure Law or Inflation Reduction Act.

1:30 p.m. – 2:20 p.m. **EENR TOPIC: CLEAN ENERGY PROJETS, PERMITTING AND GRID RESILIENCE**

Gregg Fishman
Board Vice President and Director, Sacramento Municipal Utility District

Committee members will learn about energy efficiency programs and renewable energy technologies underway and how the utility is working regionally and across sectors to achieve the utility's clean energy vision by 2030. Committee members will discuss the impact of clean energy sources and projects on grid capacity and resilience.

2:20 p.m. – 3:10 p.m. **EENR TOPIC: ADDRESSING PFAS IN COMMUNTIES**

Evan Jacobs
Vice President, Business Development, Communications and External Affairs, California and Hawaii American Water

Committee members will learn how California water utilities are addressing PFAS drinking water contamination and will discuss viable testing and treatment technologies available to communities.

3:10 p.m. – 3:50 p.m. **REGIONAL CLIMATE POLLUTION REDUCTION PLANNING AND IMPLEMENTATION**

Raef Porter
Transportation and Climate Change Program Manager, Sacramento Metropolitan Air Quality Management District

Committee members will learn how the Sacramento region is working together to determine and implement climate priorities with support from the U.S. Environmental Protection Agency's Climate Pollution Reduction Grant.

3:50 p.m. – 4:00 p.m. **BREAK**
Committee members will walk across the street for a site visit.

4:00 p.m. – 4:45 p.m. **SITE VISIT: BEAR HOLLOW STORMWATER BASIN**
Site visit will consist of an outdoor walk through the basin. Please dress appropriately to be outside for about 45 minutes (comfortable shoes, hat, sunglasses, sunscreen etc.)

Margarita Dronov, PE
Associate Civil Engineer, City of Rancho Cordova, California

The City of Rancho Cordova operates and maintains six stormwater drainage pump stations throughout the city. The Bear Hollow Drainage Pump Station was constructed in 2004. Committee members will learn about the basin's function, new educational signs and the basin's ecosystem, which includes over 500 native species trees.

4:50 p.m. **BUS DEPARTS BACK TO MARRIOTT**

6:30 p.m. – 8:30 p.m. **"AN EVENING ON THE FARM"**
Soil Born Farms, 2140 Chase Drive, Rancho Cordova, CA 95670
Buses will load in the Marriott lobby starting at 6:00 p.m. and will depart promptly at 6:30 p.m.

Be inspired by this beautiful 55-acre urban, regenerative farm situated on the banks of the American River, where you will be treated to a special farm-to-fork dinner by renowned Chef Patrick Mulvaney, libations from Rancho Cordova's Barrel District, music by the Rancho Cordova River City Concert Band, and two unique farm tour experiences.

Thursday, June 13, 2024

7:30 a.m. – 9:30 a.m. **GRAB AND GO BREAKFAST**
Sacramento Marriott Rancho Cordova – Outdoor Trellis, Lobby level

8:00 a.m. – 9:30 a.m. **ENERGY, ENVIRONMENT AND NATURAL RESOURCES COMMITTEE MEETING**
Sacramento Marriott Rancho Cordova – Sacramento Room, Lobby level

The EENR Committee will meet jointly with the Information Technology and Communications (ITC) Committee and the Finance, Administration and Intergovernmental Relations (FAIR) Committee.

8:00 a.m. – 9:30 a.m. **EENR TOPIC: PROTECTING MUNICIPAL INFRASTRUCTURE FROM CYBER ATTACK**

Mario Garcia
Supervisory Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency – Region 9

Donald Hodge
Safe Drinking Water Information System Coordinator, Drinking Water Section, U.S. Environmental Protection Agency – Region 9

Rita Gass
Chief Technology and Information Officer, City of Rancho Cordova, California

Committee members will discuss what steps their communities can take to prevent, prepare for and respond to cyberattacks and how to take advantage of federal resources within their own regional offices.

9:30 a.m. CLOSING AND ADJOURN

The Honorable Kevin Kramer, Chair, ITC Committee
Councilmember, City of Louisville, Kentucky

The Honorable Ruth Grendahl, Chair, EENR Committee
Councilmember, City of Apple Valley, Minnesota

The Honorable Blaine Griffin, Chair, FAIR Committee
Council President, City of Cleveland, Ohio

Enclosures:

- NLC Policy Development and Advocacy Process
- Energy and Environment Legal Update
- Sacramento Water Providers Plan to Meet New Federal Limits for 'Forever Chemicals'
- Cybersecurity & Infrastructure Security Agency Stakeholder Resources & Contacts
- Top Cyber Actions for Securing Water Systems
- Water Sector Cybersecurity Program Case Study
- What You Need to Know about Water Facility Hacks
- Speaker Bios
- 2024 Energy, Environment and Natural Resources Committee Roster

Upcoming EENR Committee Meetings

Monday, July 15, 3:30-4:30 p.m. eastern *– EENR Conference Call for Resolutions Review*

Wednesday, July 31, 3:30-4:30 p.m. eastern *– EENR Conference Call for Resolutions Review*

Wednesday, September 25, 3:30-4:30 p.m. eastern *– EENR Conference Call for Resolutions Review*

City Summit, Tampa, Florida, November 13-16

NLC POLICY DEVELOPMENT AND ADVOCACY PROCESS

As a resource and advocate for more than 19,000 cities, towns and villages, the National League of Cities (NLC) brings municipal officials together to influence federal policy affecting local governments. NLC adopts positions on federal actions, programs and proposals that directly impact municipalities and formalizes those positions in the *National Municipal Policy (NMP)*, which guides NLC's federal advocacy efforts.

NLC divides its advocacy efforts into seven subject areas:

- Community and Economic Development
- Energy, Environment and Natural Resources
- Finance, Administration and Intergovernmental Relations
- Human Development
- Information Technology and Communications
- Public Safety and Crime Prevention
- Transportation and Infrastructure Services

For each of the seven issue areas, a Federal Advocacy Committee advocates in support of NLC's federal policy positions. Members of each committee are appointed by the NLC President and serve for one calendar year.

Federal Advocacy Committees

Federal Advocacy Committee members are responsible for advocating on legislative priorities, providing input on legislative priorities, and reviewing and approving policy proposals and resolutions. Additionally, Committee members engage in networking and sharing of best practices.

Federal Advocacy Committees are comprised of local elected and appointed officials from NLC member cities. NLC members must apply annually for membership to a Federal Advocacy Committee. The NLC President makes appointments for chair, vice chairs, and general membership. In addition to leading the Federal Advocacy Committees, those appointed as committee chairs also serve on NLC's Board of Directors during their leadership year.

At the Congressional City Conference, Federal Advocacy Committee members are called upon to advocate for NLC's legislative priorities on Capitol Hill, as well as develop the committee's agenda and work plan for the year. Committee members meet throughout the year to further the plan, hear from guest presenters, discuss advocacy strategies and develop specific policy amendments and resolutions. At the City Summit, committee members review and approve policy proposals and resolutions. These action items are then forwarded to NLC's Resolutions Committee and are considered at the Annual Business Meeting, also held during the City Summit.

Advocacy

Throughout the year, committee members participate in advocacy efforts to influence the federal decision-making process, focusing on actions concerning local governments and communities. During the Congressional City Conference, committee members have an opportunity, and are encouraged, to meet with their congressional representatives on Capitol Hill. When NLC members are involved in the legislative process and share their expertise and experiences with Congress, municipalities have a stronger national voice, affecting the outcomes of federal policy debates that impact cities and towns.

ENERGY AND ENVIRONMENT LEGAL UPDATE

1. *Union of Concerned Scientists v. National Highway Traffic Safety Administration – DC Circuit – California Waiver*

Update since Congressional City Conference: *None – This case remains in abeyance. In January 2022,* state and local government petitioners *and* respondents *requested that the cases remain in abeyance while EPA continues its reconsideration of the challenged rule.*

Background: In September 2019, EPA and the National Highway Traffic Safety Administration (NHTSA) issued a withdrawal of waiver it had previously provided to California for that State's greenhouse gas and zero-emissions vehicle programs under section 209 of the Clean Air Act.

Before this withdrawal of waiver, California had adopted emissions standards for passenger cars and light trucks for 60 years that were more rigorous than the federal standard. The federal government had repeatedly granted California and other states who have adopted California's standards waivers under the Clean Air Act.

Litigation Status: To date, revocation of this waiver has generated four lawsuits: California and other states; three California air districts; the National Coalition for Advanced Transportation, which represents Tesla and other electric vehicle-aligned companies; and eleven environmental groups. NLC filed an amicus brief in the *Union of Concerned Scientists* case in July 2020 and the DC Circuit had planned to take briefing on both the California waiver and NHSTA preemption issues.

The waiver lawsuit brought by California and other states has been filed in the D.C. Circuit. The Trump administration asked the court to combine the waiver lawsuit and a related preemption lawsuit against the National Highway Traffic Safety Association (California vs. Chao above).

Under the new Biden Administration, the U.S. Environmental Protection Agency asked the U.S. Department of Justice (DOJ) to seek a pause on the litigation while the Administration considers rewriting the rule. The DC Circuit has granted DOJ's request, placing the case on hold.

In Jan. 2021, NLC filed an *amicus* brief in the case of *California v. Wheeler* before the DC Circuit challenging the rollback of fuel economy standards. *California v. Wheeler* has been consolidated into *Union of Concerned Scientists*.

2. *Illinois Commerce Commission v. FERC – Seventh Circuit*

Update since Congressional City Conference: *This case is being held in abeyance until a related case in the Third Circuit is decided or April 29, 2024. The court directed the parties to file a statement of position regarding further proceedings or move for voluntary dismissal.*

Illinois Commerce Commission v. FERC was being held in abeyance pending the outcome of another case before the 3rd Circuit (PJM Power Providers v. FERC). The 3rd Circuit issued its decision in that case on December 1, 2023. On December 15, FERC filed a statement of position in the Illinois Commerce Commission case, in which it requested that the court "maintain the abeyance . . . until the Third Circuit rules on any rehearing petition or, if Supreme Court review is sought, until the Supreme Court decides a petition for writ of certiorari."

It is likely that the Illinois Commerce Commission case will be dismissed as moot. As FERC noted in its December statement, the 3rd Circuit decision "concerned a replacement to the Expanded Minimum Offer Price Rule ("MOPR") (i.e., the Revised MOPR) that took effect on September 29, 2021. . . The now-defunct Expanded MOPR is the subject of *Illinois Commerce Commission*. The Third Circuit's determination that the Revised MOPR is lawful means that the Expanded MOPR will not take effect. However, given that the periods for petitioners in [*PJM Power Providers*] to seek rehearing of the Third Circuit's decision and Supreme Court review have not yet expired, the Commission advises that continued abeyance of *Illinois Commerce Commission* is appropriate."

Background: In Dec. 2019, the Federal Energy Regulatory Commission (FERC) directed PJM, a regional wholesale electricity market covering 13 states in much of the mid-Atlantic and Ohio River Valley, to establish a price floor for state subsidized resources in PJM's capacity market, seeking to ensure grid reliability by auctioning power delivery obligations three years before the electricity is needed. That price floor, called the Minimum Offer Price Rule (MOPR), would block many wind, solar and nuclear plants from clearing those auctions.

The MOPR would increase the price of certain wind, solar, and nuclear power generation that receives subsidies from almost every state in PJM's region, thereby removing the impact of the state's subsidy. Specifically, three states in PJM's territory—Ohio, Illinois and New Jersey—have nuclear subsidies, and eleven have renewable energy mandates that would make new clean energy subject to the MOPR. FERC Chairman Neil Chatterjee did note the MOPR will not apply to existing renewable energy plants, energy storage resources, or power generators that are already under ratepayer-funded "self supply" contracts, like those owned by municipal utilities. This is forecast to exempt about 5,000 MW, a small percentage of the total power usage in the region.

Following the rule's publication, many states that participate in PJM, the nuclear industry and renewable energy groups asked FERC to rehear the subsidy case. In April 2020, FERC declined to review its Dec. 2019 decision to limit participation of state-subsidized renewable and nuclear energy in PJM, setting the stage for a raft of legal challenges and potential state exits from the region's long-term electricity auctions.

FERC's decision to toss out appeal requests allows opponents of the decision to file legal challenges at the D.C. Circuit Court. Illinois utility regulators, environmental groups and municipal utilities are filing suit. The case was initially held in abeyance pending FERC's ruling on several petitions for rehearing that were filed with it. FERC has now resolved those petitions and the abeyance will expire on December 14. The court is expected to issue a scheduling order around that time.

The Illinois filing in the U.S. 7th Circuit Court of Appeals was followed by a challenge from the American Public Power Association and American Municipal Power in the D.C. Circuit Court of Appeals. New Jersey and Maryland have also filed in the DC Circuit. The Sierra Club, Natural Resources Defense Council and Environmental Defense Fund also plan to file at the D.C. Circuit. The National Rural Electric Cooperative Association is also planning to formally file suit against the PJM decision.

Local government impact: FERC's decision to deny a rehearing could also push some PJM states with nuclear power subsidies and renewable energy mandates to end their participation in the region's capacity market, while continuing to utilize its shorter-term real-time and day-ahead markets. This could make meeting local or state renewable energy goals or carbon mitigation goals difficult. PJM has proposed a June deadline for states to leave the market as part of its compliance filing, but some states are concerned that coronavirus complications will make that timeline unworkable.

Related: In June, PJM proposed changes to the MOPR that effectively exempt "state-subsidized" renewables from the rule (see here for a brief overview). PJM requested FERC approval to implement the change but the Commission took no action. As a result, in accordance with section 205 of the Federal Power Act, the changes automatically took effect in September. This would seem to moot the case, but it hasn't been formally dismissed, and actions challenging the revised MOPR are expected. Requests for rehearing have already been filed with FERC.

3. Texas v. EPA – Fifth Circuit

Update since Congressional City Conference: *None – NLC filed an amicus brief in this case in March 2023. Oral argument was heard in September 2023. A decision is expected before the end of the term.*

On December 30, 2021, EPA issued a final rule under Section 202(a) of the Clean Air Act, updating the vehicle emissions standards applicable to cars produced in model years 2022-2026. These updated standards reduced the permissible greenhouse gasses ("GHGs") "tailpipe emissions" from these vehicles. For 40 years, these standards have been set, not by per-vehicle measurements, but by "fleetwide averaging" - that is, by averaging the emissions of all vehicles produced by a manufacturer. EPA's new thresholds assume that electric vehicle ("EV") use will continue to increase, and for the purpose of averaging EPA treats EVs as though they have no tailpipe emissions. This rule was immediately challenged by a coalition of several Republican-controlled states (the "State Petitioners"), joined by a number of individual plaintiffs, private sector businesses, and nonprofits (together, the "Private Petitioners"). This coalition has broadly attacked EPA's regulatory authority and cost-benefit methodology and argues that the new rule presents a "major question" that requires express Congressional authorization.

Impact on Local Governments
The local government position in the amicus addresses the familiar climate concerns we have addressed in previous briefs: the impacts climate has on cities nationwide, and the role of cities as climate innovators dependent, to some degree, on federal regulation to provide a predictable and helpful context to reduce GHGs. NLC's *amicus* brief focuses on two narrow legal issues of particular concern to local governments.

First, it addresses Private Petitioners' argument that EPA acted arbitrarily by regulating "tailpipe" emissions rather than considering the full "lifecycle emissions" of EVs (which would include emissions from power plants that charge EVs). This is particularly important to local governments because tailpipe emissions are a major source of air pollution in municipalities across the country. The Clean Air Act prevents state and local governments from regulating tailpipe emissions on their own, and so municipalities have no tools to restrain these emissions except federal regulation. While EPA's rule focuses on GHG emissions, it will also save American communities more than $12 billion in public health benefits by reducing non-GHG tailpipe emissions that cause asthma, heart attacks, respiratory illnesses and premature death. Private Petitioners ignore these benefits in their brief.

Second, the amicus brief addresses petitioners' proposed expansion of the "Major Questions Doctrine." Petitioners argue that EPA's rule will cause more EVs to be produced, and that more EVs may strain electrical grids, which are largely regulated by states. Petitioners argue that this causal chain means that any EPA action that might encourage EV use must be specifically approved by Congress. However, if the Major Questions Doctrine is expanded in the way that Petitioners ask, it could cause chaos in local governments. Many federal regulations overlap with and affect important areas of state and local policy; barring any federal regulation that would affect an area of state interest ignores the reality of American federalism and would cripple municipalities’ ability to rely on and respond to federal regulation.

Sacramento water providers plan to meet new federal limits for ‘forever chemicals’

By: Kristin Lam, April 17, 2024
Capradio

Sacramento water providers are planning how they will meet and cover the costs of complying with new federal limits on “forever chemicals.”

One local water agency estimates it will cost $45 million to remove the chemicals, also known as perfluoroalkyl and polyfluoroalkyl substances or PFAS, from contaminated groundwater wells.

The U.S. Environmental Protection Agency announced new drinking water standards last week in an effort to reduce exposure to the chemicals, which are used in a variety of products, take a long time to break down and may cause health issues. Public water systems must test for the chemicals and have five years to reduce them if they exceed the new limits.

About six of the Sacramento County Water Agency’s 70 wells wouldn’t meet the new standards, county spokesperson Matt Robinson said Tuesday. But those wells are among the 15 the agency stopped operating over a couple years after detecting forever chemicals in them, Robinson said.

“Fortunately for the Sacramento County Water Agency, we have enough water,” Robinson said. “So, by taking these 15 wells offline, we're not being impacted.”

The agency doesn’t know why the sites have higher PFAS levels compared to the rest of its system, but he said a consultant estimated each well will cost $3 million to fix.

Although settlement money from a class-action lawsuit, grants and loans could help cover the costs, Robinson said the county is considering the potential of raising water rates.

If the agency increases rates for its about 58,000 customers, he said it will also be because of other water system improvements – not just forever chemicals.

California American Water, or Cal-Am, is one of more than 20 other water systems in Sacramento County. Spokesperson Evan Jacobs said the company, which serves about 65,000 homes and businesses in the region, aims to comply with the new standards in a cost-effective way.

“Our focus is really on technology, efficiencies of scale and cost management to ensure that we're installing the treatment we need to continue providing safe, clean water while not driving up rates too much,” Jacobs said. “We need to also focus on the affordability of this.”

The company operates 112 wells in the Sacramento region and is looking to install about five new ones a year for the next few years, Jacobs said. To increase efficiency, the company is considering strategies such as building a cluster of wells that could be connected to a single treatment plant. Installing new wells in areas that aren’t affected by forever chemicals is another strategy, Jacobs added.

Cal-Am has been treating one well in Rancho Cordova for PFAS contamination since 2017, Jacobs said. The company sued the federal government in 2020, alleging it spent $1.29 million to install a granular activated carbon treatment system because the military contaminated the groundwater at Mather Air Force Base with PFAS. Fire-fighting foam the Air Force used for training at the base allegedly leached into the aquifer the Rancho Cordova well draws from.

The complaint became part of the class action lawsuit — the same one the Sacramento County Water Agency referenced — against the company DuPont, which produces PFAS. Cal-Am is in the process of working on claims under the settlement, Jacobs said.

But higher levels of forever chemicals in some Sacramento-area groundwater wells could be linked to structural matters, too. Carlos Eliason, spokesperson for the City of Sacramento Department of Utilities, said building wells deeper decreases possible PFAS contamination.

Sacramento's older wells are more shallow in comparison to the ones at a new facility near Cosumnes River College, which treats water from as far as 1,200 feet underground, Eliason said. Some well sites also aren't big enough to add a lot of additional equipment to treat the water for PFAS, Eliason said.

The city, which gets 20% of its water from groundwater and the rest from the Sacramento and American rivers, has 30 permitted wells. Nine are in service, while the rest aren't currently being used for various reasons, including the city's strategy of letting groundwater wells recharge during wet years while drawing from them more frequently during dry years.

The city has no history of detecting PFAS in its water from the rivers, but Eliason said meeting the new forever chemical standards could cost at least tens of millions of dollars. City staff are coming up with a financial plan for compliance and are trying to balance quality and affordability, he added.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY STAKEHOLDER RESOURCES & CONTACTS

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY STAKEHOLDER RESOURCES & CONTACTS

Sign up for Alerts:
https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED
REPORT A CYBERSECURITY INCIDENT: REPORT ANOMALOUS CYBER ACTIVITY AND/OR CYBER INCIDENTS 24/7 TO REPORT@CISA.GOV OR (888) 282-0870.

- Report an Incident
- Report Phishing
- Report a Vulnerability

CONTACT US: HTTPS://WWW.CISA.GOV/ABOUT/CONTACT-US

CISA LEADERSHIP

CISA	Director	Deputy Director	Executive Director
	Jen Easterly	Nitin Natarajan	Brandon Wales
	Executive Assistant Director	**Deputy Executive Assistant Director**	
CSD	Eric Goldstein	Mathew Hartman	
ECD	Bill Bob Brown Jr	Vincent Delaurentis	
ISD	Dr. David Mussington	Steve Harris	
	Assistant Director	**Deputy Assistant Director**	
IOD	Bridgette Bean	Boyden Rohner	
NRMC	Mona Harrington	Jennifer Pedersen (A)	
SED	Alaina Clark	Trent Frazier	

STAKEHOLDER ENGAGEMENT DIVISION - STRATEGIC RELATIONS

HQ	Associate Director	Deputy Associate Director	Partnership's Branch Chief
STRATEGIC RELATIONS	Kevin Dillon kevin.dillon@cisa.dhs.gov	Sara Pease sara.pease@cisa.dhs.gov	Bob Nadeau robert.nadeau@cisa.dhs.gov

REGIONAL CONTACTS

Region	Regional Director	Deputy Regional Director	Executive Officer
Region 1	Matthew McCann	Tom Filippone	Tracy Shawyer
Contacts Regional office: CISARegion1@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 2	John Durkin	Mohammad Telab	Kelly Quinones
Contacts Regional office: CISARegion2@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 3	William Ryan	James Cratty	Deadra Sotero- Long
Contacts Regional office: CISARegion3@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 4	Julius Gamble	Kate Nichols	
Contacts Regional office: CISARegion4@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 5	Alex Joves	Kathryn Young	Beth Windisch
Contacts Regional office: CISARegion5@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			

Region 6	Harvey Perriott	Robert Russell	Ricardo Gonzalez
Contacts Regional office: CISARegion6@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 7	Phil Kirk	Ethan Cole	Steven Marin
Contacts Regional office: CISARegion7@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 8	Shawn Graff	Joseph O'Keeffe	Andre Mouton
Contacts Regional office: CISARegion8@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 9	David Rosado	Ernest Calvillo	Christopher Fiorenza
Contacts Regional office: CISARegion9@cisa.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			
Region 10	Patrick Massey	Barret Adams-Simmons	Jason Osleson
Contacts Regional office: CISARegion10@hq.dhs.gov Media inquiries: CISAMedia@cisa.dhs.gov After hours: Central@cisa.gov To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.			

RESOURCES

Secure Our World – CISA's New National Cybersecurity Awareness Program: https://www.cisa.gov/secure-our-world
Staying Safe Online is Easier Than You Think! We're increasingly connected through digital tools and more of our sensitive information is online. This convenience comes with risks. Each of us has a part to play in keeping ourselves and others safe. It's easy to do and takes less time than you think! See all the new resources CISA has developed so that we can all take steps everyday to reduce on-line risk.

Active Shooter Pocket Card | CISA: https://www.cisa.gov/resources-tools/resources/active-shooter-pocket-card
The Active Shooter Pocket Card offers suggestions about how a bystander should react in an active shooter situation.

Best Practices: https://www.cisa.gov/topics/cybersecurity-best-practices
CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks.

Cloud Environment Factsheet of Free Tools:
https://www.cisa.gov/news-events/alerts/2023/07/17/cisa-develops-factsheet-free-tools-cloud-environments
CISA has developed and published a factsheet, Free Tools for Cloud Environments, to help businesses transitioning into a cloud environment identify proper tools and techniques necessary for the protection of critical assets and data security. Free Tools for Cloud Environments provides network defenders and incident response/analysts open-source tools, methods, and guidance for identifying, mitigating, and detecting cyber threats, known vulnerabilities, and anomalies while operating a cloud or hybrid environment.

CISA Gateway: https://www.cisa.gov/resources-tools/services/cisa-gateway
The CISA Gateway serves as the single interface through which DHS partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis.

CISA Services: https://www.cisa.gov/resources-tools/services
A searchable database of services offered by CISA.

CISA Strategic Plan: https://www.cisa.gov/cybersecurity-strategic-plan
The *FY2024-2026 Cybersecurity Strategic Plan* guides CISA's efforts in pursuit of a new vision for cybersecurity: a vision grounded in collaboration, in innovation, and in accountability. Aligned with the National Cybersecurity Strategy and nested under CISA's 2023–2025 Strategic Plan, the Cybersecurity Strategic Plan provides a blueprint for how the agency will pursue a future in which damaging cyber intrusions are a shocking anomaly, organizations are secure and resilient, and technology products are secure by design and default. To this end, the Strategic Plan outlines three enduring goals:

- Address Immediate Threats by making it increasingly difficult for our adversaries to achieve their goals by targeting American and allied networks;
- Harden the Terrain by adopting strong practices for security and resilience that measurably reduce the likelihood of damaging intrusions; and
- Drive Security at Scale by prioritizing cybersecurity as a fundamental safety issue and ask more of technology providers to build security into products throughout their lifecycle, ship products with secure defaults, and foster radical transparency into their security practices so that customers clearly understand the risks they are accepting by using each product.

CISA Training: https://www.cisa.gov/cybersecurity-training-exercises
CISA looks to enable the cyber-ready workforce of tomorrow by leading training and education of the cybersecurity workforce by providing training for federal employees, private-sector cybersecurity professionals, critical infrastructure operators, educational partners, and the general public. CISA is committed to supporting the national cyber workforce and protecting the nation's cyber infrastructure.

CISA TTX Packages: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Cyber Hygiene Services: https://www.cisa.gov/cyber-hygiene-services Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. The Cybersecurity and Infrastructure Security Agency (CISA) offers scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.

Cyber Guidance for Small Businesses : https://www.cisa.gov/cyber-guidance-small-businesses
We offer an action plan for small businesses that is informed by the way cyber-attacks actually happen, that lays the groundwork for building an effective security program.

Cross Sector Cybersecurity Performance Goals
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
Developed in coordination between CISA, the National Institute of Standards and Technology (NIST), and the interagency community, these voluntary cross-sector Cybersecurity Performance Goals (CPGs) are intended to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts.

Cybersecurity Education & Career Development: (https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development)
Cybersecurity professionals are critical - in both private industry and the government - to the security of individuals and the nation. The Cybersecurity and Infrastructure Security Agency (CISA) is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders.

Cybersecurity Awareness Month (October): https://www.cisa.gov/cybersecurity-awareness-month (email: AwarenessCampaigns@cisa.dhs.gov)
2023 is the 20th Cybersecurity Awareness Month! Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace. CISA and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

Decider Fact Sheet: https://www.cisa.gov/resources-tools/resources/decider-fact-sheet
On March 1, 2023, CISA released Decider, a free tool to help the cybersecurity community map threat actor behavior to the MITRE ATT&CK framework. Created in partnership with the Homeland Security Systems Engineering and Development Institute™ (HSSEDI) and MITRE, Decider helps make mapping quick and accurate through guided questions, a powerful search and filter function, and a cart functionality that lets users export results to commonly used formats. CISA encourages the community to use the tool in conjunction with the recently updated Best Practices for MITRE ATT&CK® Mapping guide.

Election CyberSecurity Toolkit: https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
CISA has compiled a toolkit of free services and tools intended to help state and local government officials, election officials, and vendors enhance the cybersecurity and cyber resilience of U.S. election infrastructure. This toolkit includes free tools, services, and resources provided by CISA, JCDC members, and the cybersecurity community.

Emergency Communications: https://www.cisa.gov/topics/emergency-communications
CISA provides plans, resources, and training to support emergency communications for first responders.

Emergency Communications Awareness Month (April): https://www.cisa.gov/emergency-communications-month
Through its emergency communications mission, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and government officials to be able to communicate in the event of a natural disaster, terrorist act, or other hazard. CISA also provides guidance on how facilities can establish protocols for identifying and reporting significant cyber incidents to appropriate facility personnel, local law enforcement, and the agency.

Free Cybersecurity Services and Tools: https://www.cisa.gov/free-cybersecurity-services-and-tools
As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. The list is not comprehensive and is subject to change pending future additions.

Homeland Security Information Network- Critical infrastructure: https://www.dhs.gov/hsin-critical-infrastructure
The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive but Unclassified (SBU) information. The Critical Infrastructure community on HSIN (HSIN-CI) is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure.

Infrastructure Security Awareness Month (November): https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/infrastructure-security-month-2022
CISA invites all Americans to remember that Infrastructure Security is National Security. Keeping the nation's critical infrastructure secure is important to our national security, economy and overall way of life. Critical infrastructure spans everything from telecommunications and chemical facilities to healthcare and financial systems and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services that keep our country and our economy running.

JCDC News and Resources: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-news-and-resources
Links to external news sources that highlight relevant cybersecurity information. The Cybersecurity and Infrastructure Security Agency established JCDC—the Joint Cyber Defense Collaborative—to unify cyber defenders from organizations worldwide. This diverse team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response.

K-12 Report: https://www.cisa.gov/K12Cybersecurity
Malicious cyber actors are targeting K–12 education organizations across the country, with potentially catastrophic impacts on students, their families, teachers, and administrators. A new report from the Cybersecurity and Infrastructure Security Agency (CISA) helps schools reduce the risks of a cyber catastrophe.
And Toolkit: https://www.cisa.gov/resources-tools/resources/partnering-safeguard-k-12-organizations-cybersecurity-threats-online
To help schools address cybersecurity risks, CISA developed a report with recommended actions and cybersecurity guidelines for leaders in the K-12 community. The report and this corresponding toolkit are designed to help K-12 schools and school districts most effectively reduce their cybersecurity risks.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: (https://www.cisa.gov/national-initiative-cybersecurity-education-nice-cybersecurity-workforce-framework)
The NICE Cybersecurity Workforce Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks.

National Initiative for Cybersecurity Careers and Studies: (https://niccs.cisa.gov/cybersecurity-career-resources/additional-resources)
NICCS provides cybersecurity-related resources and links provided here for your information and convenience.

Partnerships: (https://www.cisa.gov/topics/partnerships-and-collaboration)
At CISA, partnership and collaboration are our foundation and the lifeblood of what we do. Information sharing and cooperative action – across both public and private sectors – is essential to our goal of raising the nation's collective defense.

Protecting Houses of Worship: Perimeter Security Considerations Infographic:
https://www.cisa.gov/resources-tools/resources/protecting-houses-worship-perimeter-security-considerations-infographic
This resource is a companion piece to CISA's and the Federal Bureau of Investigation's (FBI) co-branded Protecting Places of Worship: Six Steps to Enhance Security Against Targeted Violence Fact Sheet, which highlighted the following steps: understand risk; understand your space; develop and practice a plan; inform and educate greeters; pursue grants; and report hate crimes and other incidents. This infographic outlines low- to no-cost solutions to help implement these suggested practices and highlights ways to identify funding for security improvements. To learn more about layered security and other recommended mitigations, visit CISA's Mitigating Attacks on Houses of Worship Security Guide.

Ransomware Resources: https://www.cisa.gov/stopransomware
Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Resource Hub: https://www.cisa.gov/cyber-resource-hub
CISA offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help organizations manage risk and strengthen the cybersecurity of our Nation's critical infrastructure.

School Safety: https://www.cisa.gov/topics/physical-security/school-safety CISA, along with other organizations throughout government, law enforcement, and communities nationwide, supports K-12 schools and districts in their efforts to enhance school safety and security. CISA's School Safety Task Force is the agency's dedicated program established to strengthen schools' safety and security across the country.

Shields Ready: https://www.cisa.gov/shields-ready
CISA's Shields Ready campaign is about making resilience during incidents a reality by taking action before incidents occur. As a companion to CISA's Shields Up initiative, Shields Ready drives action at the intersection of critical infrastructure resilience and national preparedness. This campaign is designed to help all critical infrastructure stakeholders to take action to enhance security and resilience—from industry and businesses to government entities at all levels, and even individuals by providing recommendations, products, and resources to increase individual and collective resilience for different risk contexts and conditions.

State and Local Cybersecurity Grant Program: https://www.cisa.gov/state-and-local-cybersecurity-grant-program
On September 16, 2022, DHS announced a first-of-its-kind cybersecurity grant program specifically for state, local, tribal and territorial (SLTT) governments. Funding from the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state, local and territorial (SLLT) governments. Through two distinct Notice of Funding Opportunities (NOFO), SLCGP and TCGP combined will distribute $1 billion over four years to support projects throughout the performance period of up to four years.

Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks:
https://www.cisa.gov/resources-tools/resources/securing-smb-supply-chains-resource-handbook
Developed by the ICT Supply Chain Risk Management (SCRM) Task Force, this handbook provides an overview of the highest supply chain risk categories commonly faced by ICT small and medium-sized businesses (SMBs), including cyber risks, and contains several use cases that can assist ICT SMBs in identifying the necessary resources to implement ICT supply chain security practices.

Secure by Design: https://www.cisa.gov/securebydesign
It's time to build cybersecurity into the design and manufacture of technology products. The cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.

COMMUNITY SUPPORT RESOURCES

Election Security Advisors (ESA): ESAs will build stronger connective tissue between election officials and our team at CISA. These election security advisors will be experts in the space, with firsthand knowledge of and experience with the infrastructure and officials across their regions in order to provide more tailored guidance and support to reduce risk from the full range of cyber and physical threats to election infrastructure.

Emergency Communications Coordinators (ECC): Emergency Communications Coordinators support emergency communications interoperability by offering training, tools, and workshops, and provide coordination and support in times of threat, disruption, or attack. These services assist CISA stakeholders in ensuring they have communications during steady and emergency operations. Through these programs, CISA helps ensure public safety and national security and emergency preparedness communities can seamlessly and securely communicate.

Chemical Security Inspectors (CSI): Chemical Security Inspectors (CSIs) advise and assist facilities with hazardous chemicals on security measures to reduce the risk of those chemicals being weaponized. For facilities covered under the Chemical Facility Anti-Terrorism Standards (CFATS) program, this includes working with the highest-risk chemical facilities to develop security plans and inspecting to ensure that security is in place. For facilities that do not fall under the CFATS program, CSIs facilitate and provide voluntary security resources, including guidance, best practices, and training.

Cybersecurity Advisors (CSA): approximately 120 cybersecurity subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.

Protective Security Advisors (PSA): over 170 security subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.

Physical Security Resources: builds security capacity of the public and private sector to mitigate a wide range of threats including active shooters, vehicle ramming, insider threats, and small unmanned aircraft systems.

- Securing Public Gatherings: https://www.cisa.gov/topics/physical-security/securing-public-gatherings
- Mass Gathering Security Planning Tool: https://www.cisa.gov/resources-tools/resources/mass-gathering-security-planning-tool
- Protecting Infrastructure During Public Demonstrations: https://www.cisa.gov/sites/default/files/publications/Protecting%20Infrastructure%20During%20Public%20Demonstrations_102220_FINAL_508.pdf

Targeted Violence Prevention

- Pathway to Violence: Warning Signs and What You Can Do: https://www.cisa.gov/resources-tools/resources/pathway-violence
- Power of Hello: https://www.cisa.gov/sites/default/files/publications/CISA_Power_of_Hello_SlickSheet.pdf
- Personal Security Considerations: https://www.cisa.gov/sites/default/files/publications/CISA

Fact Sheet_Personal Security Considerations_FINAL_508_0.pdf

- Mitigating the Impacts of Doxing: https://www.cisa.gov/sites/default/files/publications/CISA Insight_Mitigating the Impacts of Doxing_508.pdf

Active Shooter Preparedness: https://www.cisa.gov/topics/physical-security/active-shooter-preparedness

- Active Shooter Preparedness Webinar: https://www.cisa.gov/resources-tools/training/active-shooter-preparedness-webinar
- Planning and Response to an Active Shooter Guidance: https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- Active Shooter Preparedness: Access & Functional Needs – What You Should Know Video: https://www.youtube.com/watch?v=m3-_z1Q1bFg
- Translated Active Shooter Preparedness Resources: https://www.cisa.gov/translated-active-shooter-preparedness-products-and-resources

Vehicle Ramming Mitigation: https://www.cisa.gov/topics/physical-security/vehicle-ramming-mitigation

- Vehicle Ramming Self-Assessment Tool: https://www.cisa.gov/vehicle-ramming-self-assessment-tool
- Vehicle Ramming Action Guide: https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide
- Active Vehicle Barrier Selection Tool: https://www.cisa.gov/resources-tools/resources/active-vehicle-barrier-selection-tool
- Guide to Active Vehicle Barrier Specification and Selection Resources: https://www.cisa.gov/resources-tools/resources/guide-active-vehicle-barrier

Insider Threat Mitigation: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

- Insider Threats 101 Fact Sheet: https://www.cisa.gov/resources-tools/resources/insider-threat-101-fact-sheet
- Insider Risk Mitigation Program Evaluation Self-Assessment Tool: https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe

Bombing Prevention Resources: https://www.cisa.gov/topics/physical-security/bombing-prevention

- Counter-IED Awareness Products: https://www.cisa.gov/counter-ied-awareness-products/
- What to Do: Bomb Threat Resources: http://www.cisa.gov/what-to-do-bomb-threat
- What to Do: Bomb Threat Video: https://www.youtube.com/watch?v=pg7yVTBciWg
- Bomb Threat Guidance Brochure: https://www.cisa.gov/sites/default/files/publications/Bomb-Threat-Guidance-Quad-Fold.pdf

- Suspicious or Unattended Item Card: https://www.cisa.gov/sites/default/files/publications/Unattended_vs._Suspicious_Item_Postcard_508Compliant.pdf
- What to Do: Suspicious or Unattended Item Video: https://www.youtube.com/watch?v=rl3iJlFTFC0
- Technical Resource for Incident Prevention (TRIPwire): https://www.tripwire.dhs.gov/

TRAINING

Bombing Prevention Training and Resources: https://www.cisa.gov/topics/physical-security/bombing-prevention/office-bombing-prevention-obp-training
Response to Suspicious Behavior and Items Course: https://cdp.dhs.gov/training/course/AWR-335
Surveillance Detection for Bombing Prevention Course Fact Sheet: https://www.cisa.gov/sites/default/files/publications/PER-346-Fact-Sheet-508-V2.1.pdf
Active Shooter Instructor-led and Online Training Modules: https://www.cisa.gov/resources-tools/training/active-shooter-what-you-can-do
Active Shooter Options for Consideration Training Video: https://www.youtube.com/watch?v=tq21iSXDBWg
Defusing Potentially Violent Situations: https://www.cisa.gov/sites/default/files/publications/De-Escalation_Final 508 %2809.21.21%29.pdf

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1,2,3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the internet.

- **Free resource:** CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
- **Free service:** Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.

- **Free service:** EPA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resources:**
    - CISA's Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. A free CPG assessment can be administered by a CISA cybersecurity advisor CISA Regions) or through a self-assessment.
    - The American Water Works Association's (AWWA's) Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool can help a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented.
    - AWWA's Water Sector Cybersecurity Risk Management Guidance for Small Systems is a *getting started guide* that helps small, rural utilities (who serve <10,000 people) assess and implement cyber best practices.
    - The WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities provides an overview of cybersecurity measures with resources to accompany each measure for deeper exploration.
    - The MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Critical Security Controls (CIS Controls) cybersecurity best practices. The CIS RAM Family of Documents provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.

[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities

[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure. Weak default or insecure passwords are easy to discover and exploit, and they may allow cyber threat actors to make changes to a water systems' operational processes. This can negatively impact public health and safety. Change default or insecure passwords and implement multifactor authentication (MFA) where possible. Focus on deploying MFA to IT infrastructure, such as email, to make it difficult for threat actors to access OT systems. Consider asking manufacturers to eliminate default passwords.

- **Free resources:** CISA's Secure our World Campaign: Use Strong Passwords and More than a Password Campaign. For additional cyber guidance, see CISA's Cyber Guidance for Small Businesses.

4. Conduct an Inventory of OT/IT Assets

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.

- **Free service:** EPA's Cybersecurity Technical Assistance Program supports you in conducting an inventory.
- **Free tool:** A first step in conducting an inventory is identifying the devices on the network. CISA's Malcolm tool enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

- **Free resources**: EPA's Cybersecurity Action Checklist and CISA's Incident Response Plan (IRP) Basics help to develop cyber incident response plans. The Joint CISA-FBI-EPA Water Incident Response Guide provides valuable information on how to work with federal response partners before, during, and after a cyber incident. **Note:** See this guide for contact information for CISA, FBI, and the EPA Water Infrastructure and Cyber Resilience Division.

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.

- **Free tools:** CISA Tabletop Exercise Package (CTEP) and EPA tabletop exercise (TTX) scenario tools assists critical infrastructure owners and operators in developing their own tabletop exercises to meet their specific needs.

6. Backup OT/IT Systems

Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule: 3) Keep three copies: one primary and two backups; 2) Keep the backups on two different media types; 1) Store one copy offsite.

- **Free resources:** CISA's Cyber Essentials Toolkit Chapter 5: Your Data and NIST's Protecting Data From Ransomware and Other Data Loss Events provide guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog during scheduled downtime of OT equipment; prioritize patches in IT, as applicable. CISA's Secure our World Campaign provides guidance on updating software.

8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

- **Free resources:** See EPA Cybersecurity Training and CISA's free Industrial Control Systems cybersecurity virtual training to learn how to protect against cyberattacks to critical infrastructure. Also see CISA's Secure our World Campaign: Employee Phishing Training for practical steps to help your employees avoid phishing scams.

Support

If you require additional support for implementing any of these actions, contact EPA and/or your regional CISA cybersecurity advisor for assistance.

Disclaimer

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked or referenced within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: *Medium Drinking Water System #2*

Cybersecurity: Take Charge and Take Advantage

OVERVIEW

This medium-sized drinking water utility provides safe drinking water to 85,000 customers. With cybersecurity threats growing every day, and news that other local entities had experienced ransomware disruptions, this utility decided to reduce its cyber risks while increasing staff cybersecurity awareness and culture.

CYBERSECURITY APPROACH

With no one person in charge of cybersecurity, past efforts at the utility lacked momentum and cohesion. To energize and focus these efforts, the utility hired a full-time IT Manager to oversee both its information technology (IT) and operational technology (OT) systems. The new manager leveraged several free cybersecurity resources and technical assistance programs:

- EPA's cybersecurity assessment and technical assistance program
- Tabletop exercises conducted by regional DHS Cybersecurity and Infrastructure Security Agency (CISA) representatives
- Nationwide Cybersecurity Review (NCSR) self-assessment based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Guidance, tools, and free services (e.g., alerts) from the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- American Water Works Association (AWWA) water sector cybersecurity resources
- Local water sector associations/organizations
- A cyber audit performed by the state auditor's office

These resources enabled the IT manager to better understand the water sector's cyber risks and what could be done to mitigate them. Several cyber improvents were instituted at the utility:

DEVICE SECURITY

- Completed a thorough asset inventory to identify and replace legacy equipment
- Implemented server upgrades

DATA SECURITY

- Deployed a Managed Detection and Response (MDR) service

VULNERABILITY MANAGEMENT

- Employed active vulnerability detection to apply software updates and patches

RESPONSE AND RECOVERY

- Established offsite back-ups of critical data

OTHER

- Instituted virtual local area networks (VLANs) to segment the OT and IT networks

The IT Manager is also working on creating the utility's IT and OT standards to cover topics such as hardware retirement/replacement, acceptable use of utility devices, incident response procedures, data disposal criteria, password control, malware detection, and media protection.

LESSONS LEARNED

- Research and take advantage of all the free resources available to help implement cybersecurity practices.
- A stepwise, methodical approach with the understanding that you will not be able to do everything you want to do at once can help limit frustration.
- Invest time and resources on staff cybersecurity awareness training. Bottom line: you want to build both cybersecurity awareness and a cybersecurity culture at your utility.

READY TO BUILD YOUR CYBERSECURITY PROGRAM?

Ready to make your utility more cyber secure? EPA can help. Visit the *Cybersecurity for the Water Sector* website and learn more about resources that can bring your utility one step closer to cybersecurity resilience.

PROANALYSIS

WHAT YOU NEED TO KNOW ABOUT

Water Facility Hacks

BY MAGGIE MILLER AND JESSIE BLAESER | 05/22/2024 05:00:00 AM EDT

PRO POINTS

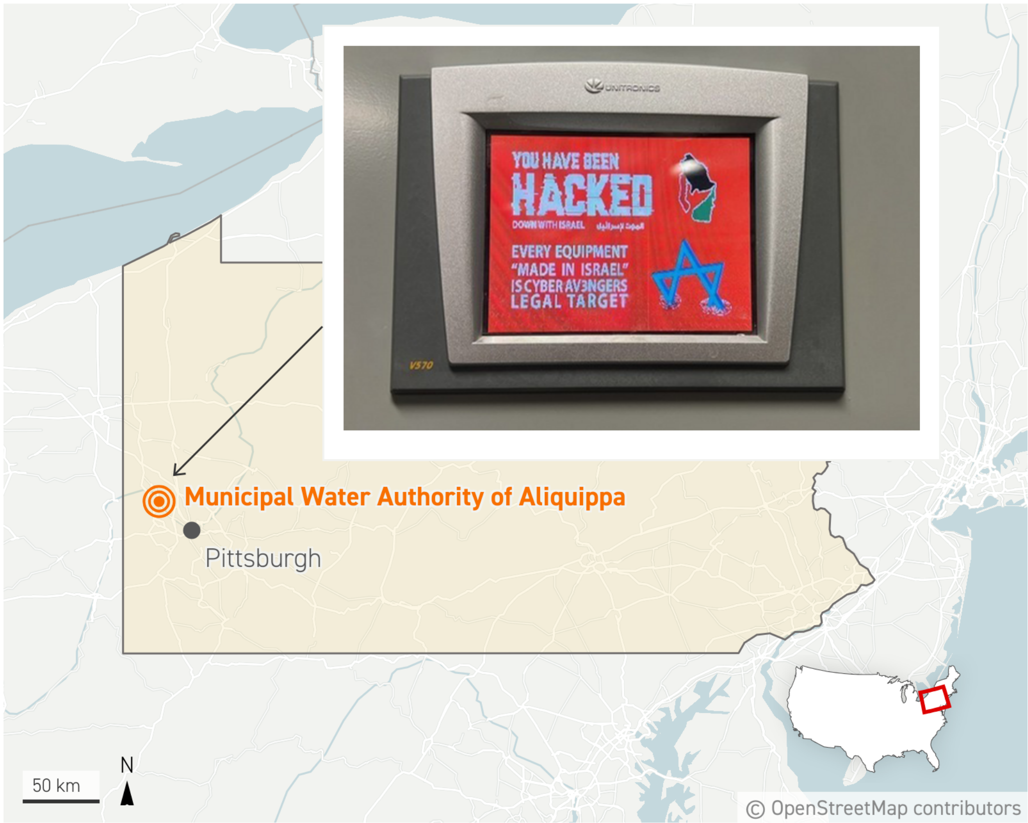
- **In November 2023, an Iranian cybercriminal group attacked Israeli-made equipment in multiple U.S.** water treatment facilities in retaliation for Israel's invasion of the Gaza Strip after the Oct. 7 Hamas assault.
- **The cyberattacks — which involved posting an anti-Israel message on monitors in the facilities** impacted but did not otherwise affect operations — prompted both the Biden administration and Congress to work to strengthen security at these facilities.
- **Congress is now considering legislation to increase the cybersecurity of the water sector, and the** Treasury Department sanctioned the alleged hackers behind the attacks.

HOW WE GOT HERE

The water sector has traditionally been one of the least secured areas of U.S. critical infrastructure, and cybercriminals and nation states alike have taken aim at water and wastewater centers through hacks in recent years — and following a recent burst of attacks, the federal government is looking to take action to secure these facilities against hackers.

The White House stepped up its focus on countering cyber threats to the water system early on in President Joe Biden's term in office, in particular following a hack of a water treatment facility in Oldsmar, Florida. However, the attention ratcheted up after Iranian cybercriminal group CyberAv3ngers hacked into Israeli-made equipment to post an anti-Israel message on monitors in several U.S. water facilities at the end of 2023, part of retaliation for U.S. support for Israel in its war with militant group Hamas.

Pittsburgh-area water authority was hacked last November



Source: Image courtesy of the Municipal Water Authority of Aliquippa
Jessie Blaeser/POLITICO

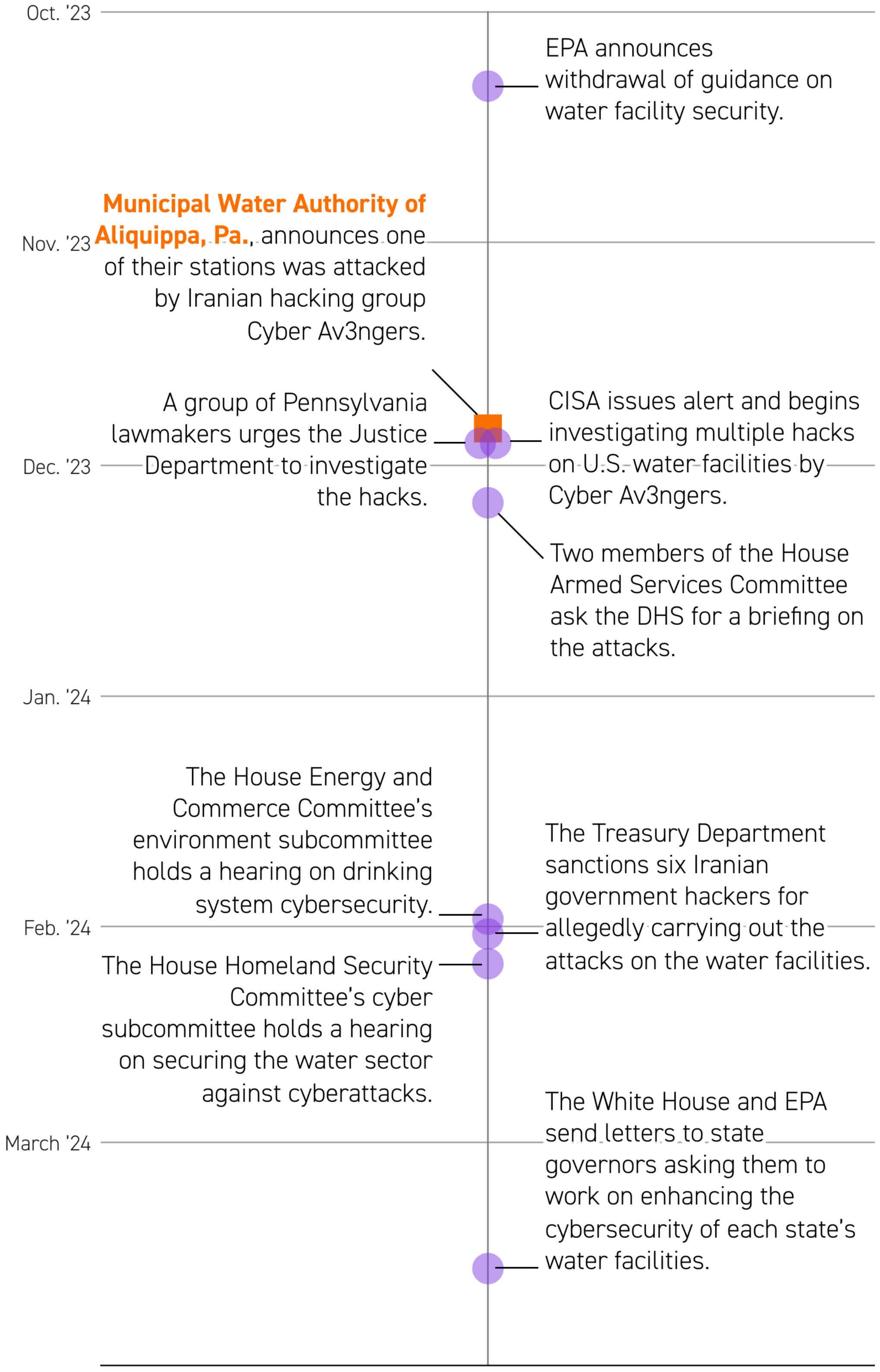
The Cybersecurity and Infrastructure Security Agency subsequently put out an alert warning of the attacks, stressing that none of the facilities saw impacts to water supply operations. Lawmakers were quick to pressure agencies including the Department of Justice and Department of Homeland Security to look into the attacks, and the Treasury Department announced sanctions against the Iranian nationals allegedly behind the strikes in February.

In addition, the House Homeland Security and Energy and Commerce committees held separate hearings in early 2024 on the cybersecurity of the water sector, and the White House and the Environmental Protection Agency sent a joint letter to state governors strongly urging them to prioritize securing water facilities against hackers.

One reason the letters were sent is that the EPA does not have strong authorities to ensure the cybersecurity of water and wastewater facilities. The agency was forced to withdraw a memorandum in early 2023 after pushback from several Republican-led states that would have required states to evaluate the cybersecurity of operational technology at water facilities.

Aliquippa hack kicked off flurry of activity to prevent further cyberattacks

Timeline of events related to cyber attacks at water utilities, Oct. 2023 through March 2024



EPA announces withdrawal of guidance on water facility security.

Municipal Water Authority of Aliquippa, Pa., announces one of their stations was attacked by Iranian hacking group Cyber Av3ngers.

A group of Pennsylvania lawmakers urges the Justice Department to investigate the hacks.

CISA issues alert and begins investigating multiple hacks on U.S. water facilities by Cyber Av3ngers.

Two members of the House Armed Services Committee ask the DHS for a briefing on the attacks.

The House Energy and Commerce Committee's environment subcommittee holds a hearing on drinking system cybersecurity.

The Treasury Department sanctions six Iranian government hackers for allegedly carrying out the attacks on the water facilities.

The House Homeland Security Committee's cyber subcommittee holds a hearing on securing the water sector against cyberattacks.

The White House and EPA send letters to state governors asking them to work on enhancing the cybersecurity of each state's water facilities.

Source: POLITICO reporting

Jessie Blaeser and Maggie Miller/POLITICO

WHAT'S NEXT

The Biden administration and Congress alike are looking to take further steps to secure the water sector against attacks from Iran and any other nation states or cybercriminals.

These include the introduction of new legislation to secure the water sector, such as one measure put forward by Reps. Rick Crawford (R-Ark.) and John Duarte (R-Calif.) that would establish a water risk and resilience organization to work with the EPA to enforce new cyber requirements for the water and wastewater sector. Another measure, introduced by Reps. Don Davis (R-N.C.), Zachary Nunn (R-Iowa), Angie Craig (D-Minn.) and Abigail Spanberger (D-Va.), would strengthen the cybersecurity of rural water facilities that often have less funds.

Sen. Ron Wyden (D-Ore.), chair of the Senate Energy and Natural Resources Committee's water subcommittee, vowed this year to take action to update and strengthen the Federal Energy Regulatory Commission's cybersecurity requirements for dams.

Inside the administration, Anne Neuberger, the deputy national security adviser for cyber and emerging technology, and EPA Deputy Administrator Janet McCabe met in March with state and local officials to encourage them to step up the cybersecurity of water systems. During those meetings they shared cybersecurity resources with the officials.

Neuberger asked that each state submit a plan to the White House by May 20 on how officials are addressing cyber vulnerabilities in their water and wastewater systems. In addition, the EPA is working to establish a Water Sector Cybersecurity Task Force to identify immediate ways to strengthen the cybersecurity of the nation's water systems.

POWER PLAYERS

- **The Cybersecurity and Infrastructure Security Agency:** The nation's cyber defense agency, housed within the Department of Homeland Security, launched an investigation into the cyberattacks on U.S. water facilities in late 2023.

- **The Environmental Protection Agency:** The sector-specific agency with authority over securing water and wastewater treatment centers

- **Anne Neuberger:** The White House deputy national security adviser for cyber and emerging technology, whose office has worked to step up the water sector's cybersecurity throughout Biden's time in office.

- **Rep. Chris Deluzio (D-Penn.):** The House representative for Pennsylvania's Municipal Water Authority of Aliquippa, the first facility that went public about being hit by the hackers in late 2023. Deluzio subsequently pushed the Justice Department to investigate the attacks.

- **Sen. Ron Wyden (D-Ore.):** The chair of the Senate Energy and Natural Resources Subcommittee on Water and Power is pushing to give the Federal Energy Regulatory Commission more cybersecurity authorities to regulate dams and the water sector.

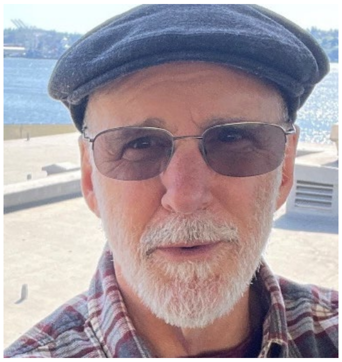
SPEAKER BIOS

Margarita Dronov is a licensed Professional Engineer (PE) for the City of Rancho Cordova, California. Within Public Works Stormwater & Drainage, she assists with regulatory compliance, land development drainage reviews, and maintenance of stormwater facilities (open waterways, pipes, and drainage pump stations). She enjoys working with a great team to deliver stormwater capital projects that improve public safety and quality of life. Margarita earned a Master of Science degree in Civil & Environmental Engineering from Stanford through the National Science Foundation's Graduate Research Fellowship Program. Her bachelor's degree is from California State University, Sacramento.

Gregg Fishmann is the Board Vice President and Director of the Sacramento Municipal Utility District (SMUD). Gregg was first elected to the SMUD Board of Directors in January 2015 and represents Ward 3, which includes East Sacramento, much of the Arden-Arcade area, and the Campus Commons, College Glen, and Rosemont neighborhoods, as well as parts of Carmichael, Florin, Fruitridge and Vintage Park.

Gregg has been a clean energy advocate for much of his career. As a former SMUD employee, he promoted wind and solar energy when they were in their infancy. At the California Independent System Operator, he led public engagement efforts supporting new wind energy farms in California. As President of the SMUD Board in 2018, he led the utility in passing its Integrated Resource Plan, hailed by the California Energy Commission as "... an ambitious road map for lowering greenhouse gas emissions in the Sacramento region."

In his varied career, Gregg was a news reporter and anchor at KFBK and KGO Radio, a public information officer at SMUD and the California Independent System Operator (California ISO), and communications coordinator for the California State Association of Counties. He currently works at Sacramento Regional Transit as the Senior Community Relations Officer. Gregg is a graduate of California State University, Sacramento with a bachelor's degree in journalism.



Don Hodge is the Safe Drinking Water Information System Coordinator in the Drinking Water Section for the U.S. Environmental Protection Agency (EPA) Region 9. Don Hodge has held several data management and program coordination positions at EPA's Region 9 office in San Francisco beginning in 1994. Since 2014, he has served as the SDWIS Federal Coordinator for Region 9, managing the migration of data from state-level drinking water programs to the federal Safe Drinking Water Information System. He has also worked as a systems administrator for the US Consulate in Frankfurt, Germany, as a hardware/software technical writer in the San Francisco bay area, and as a wildland firefighter for the US Forest Service in northern California. He holds a Masters of Computer Information Systems degree from Boston University and lives and works in Marin county.

Rita Gass is the Chief Technology and Innovation Officer for the City of Rancho Cordova, California. Rita's background in government service spans over two decades, encompassing a wide range of roles within state, local and federal government agencies. She's worked for the Secretary of State, providing election and cyber-security solutions for California's 58 counties. Under her leadership, there were zero reported critical incidents in the 2016 and 2018 elections.

Most recently, she was CIO at the California Employment Development Department where she stepped in during a challenging time and fixed many problems, including reducing fraud and backlogs.

Evan Jacobs is Vice President for Business Development, Communications and External Affairs for California and Hawaii American Water. Evan got his start in the water industry in 2003 when he began consulting for American Water on local public policy issues. Previously, Evan served as an external affairs manager for American Water in Northern California, New Mexico and Texas and as the director of communications and government affairs for California American Water. During the 2012-2016 drought, Evan managed California American Water's state drought response team and led successful efforts to achieve a 26 percent reduction in water use. He serves on the boards of California Water Association and several Groundwater Sustainability Agencies in Yolo, Sacramento, and Sonoma Counties. Evan met his wife when they attended Trinity College in Hartford, CT and now lives in Davis, CA.

Raef Porter is the Transportation and Climate Change Program Manager for the Sacramento Metropolitan Air Quality Management District. Raef has a background in transportation, land use, climate change, and business that showcases his strong interest in helping to build sustainable, equitable, and efficient systems.

Prior to working for the Air District, Raef was the Executive Director of the Del Paso Boulevard Partnership. He worked closely with local residents, property and business owners, community-based organizations, partner agencies, and the City of Sacramento to build and implement a collective vision for the business corridor.

In addition, Raef spent over 15 years at the Sacramento Area Council of Governments working on land use, climate change, and transportation related projects. As the Climate and Energy Team Manager, Raef oversaw projects on electric vehicles, climate adaptation, climate mitigation, transportation innovation, transportation funding, and air quality mitigation.

Raef has lived in Sacramento for 20 years, and with his family and friends owns a small business.

NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER

2024 Energy, Environment & Natural Resources (EENR) Committee Roster

Leadership

- Chair Ruth Grendahl, Council Member, City of Apple Valley, MN
- Vice Chair Laura Dent, Vice Mayor, City of Harrisonburg, VA
- Vice Chair Brian Jones, Council Member, City of Union City, GA

Members

- Kathryn Abbott, Councilmember, Village of Pinecrest, FL
- Bessye Adams, Council Member - At Large Place 7, City of Grand Prairie, TX
- Taishya Adams, Council Member, City of Boulder, CO
- Valerie Amor, Energy Manager, City Manager Office, City of Alexandria, VA
- David Anderson, Council Member, City of Dover, DE
- Salette Andrews, Councilmember, City of Wilmington, NC
- Anne Barrington, Council Member, Town of Parker, CO
- Mila Besich, Mayor, Town of Superior, AZ
- Alex Bollin, Planner I, City of Southfield, MI
- Deborah Calvert, Council Member, City of Minnetonka, MN
- Bradley Carter, Councilman, City of Oklahoma City, OK
- TJ Cawley, Mayor, Town of Morrisville, NC
- Arlene Chin, Councilmember, City of Tempe, AZ
- Margaret Clark, Mayor Pro Tem, City of Rosemead, CA
- Kristi Douglas, Councilmember, City of Commerce City, CO
- Carrie Anne Downey, Council Member, City of Coronado, CA
- Jennifer Duff, Councilmember, City of Mesa, AZ
- Danielle Duran, Intergovernmental Affairs Manager, Los Alamos County, NM
- Rick Elumbaugh, Mayor, City of Batesville, AR
- Junior Ezeonu, Councilmember, City of Grand Prairie, TX
- Dalia Fadl, Principal Civil Engineer, City of Rancho Cordova, CA
- Lindsay French, Council Member, City of Kansas City, MO
- Thomas Good, Commissioner, City of Pembroke Pines, FL
- Clay Goodman, Council Member, City of Buckeye, AZ
- Lance Haynie, Government Affairs Director, City of Santa Clara, UT
- Alan Hew, Council Member, City of College Park, MD
- Chris Herron, Councilmember, City of Lenexa, KS
- Abbie Kamin, Council Member, City of Houston, TX
- Debbie Kring, Councilmember, City of Mission, KS
- Lorraine Koss, Council Member, City of Cocoa, FL
- Mina Layba, Legislative Affairs Manager, City of Thousand Oaks, CA
- Laura Mork, Councilmember, City of Shoreline, WA

- David Newman, Mayor Pro Tem, City of Thousand Oaks, CA
- Meeka Owens, Council Member, City of Cincinnati, OH
- Nick Palumbo, Alderman, City of Savannah, GA
- Johnnie Parks, Council Member, City of Broken Arrow, OK
- Billy Pearson, Council Member, City of Lincoln, AL
- Susan Persis, City Commissioner, City of Ormond Beach, FL
- Jenni Pompi, Council Member, City of Greenbelt, MD
- Leslie Pool, Council Member, City of Austin, TX
- Gabe Quinto, Council Member, City of El Cerrito, CA
- Joe Rasco, Mayor, Village of Key Biscayne, FL
- Jessica Sandgren, Councilmember, City of Thornton, CO
- Julie Sayers, Mayor, City of Lenexa, KS
- Andrew Sensi, Infrastructure Project Manager II, City of New Orleans, LA
- Patricia Showalter, Mayor, City of Mountain View, CA
- Ellen Smith, Council Member, City of Oak Ridge, TN
- Katrina Thompson, Mayor, Village of Broadview, IL
- Becky Tuttle, Council Member, City of Wichita, KS
- Kimberly Wilburn, Council Member, City of Minnetonka, MN
- Kevin Wilk, Council Member, City of Walnut Creek, CA