RECLAMATION Managing Water in the West

February 2019 Upper Colorado Region



Four Corners Construction Office launches the Navajo-Gallup Water Supply Project Newsletter

By Pat Page, Four Corners Construction Office

The Four Corners Construction Office has released their second edition of the newly established Navajo-Gallup Water Supply Project Quarterly Newsletter. The newsletter will provide information on current and future construction activities, as well as present background information, answer frequently asked questions, and detail important facts pertaining to the project targeted to the people the project will directly impact.



2nd Quarter, January 2019 Navajo-Gallup Water Supply Project Newsletter.

The Navajo-Gallup Water Supply Project, or NGWSP, is the backbone of the Navajo Nation's 2010 Water Rights Settlement agreement on the San Juan River Basin in New Mexico. When completed, the project will consist of over 300 miles of pipeline, 2 water treatment plants, 19 pumping plants, and several million gallons of storage, and will provide a reliable and clean drinking water supply for 43 chapters within the Navajo Nation, the southwestern portion of the Jicarilla Apache Reservation, and the City of Gallup.

We recommend everyone take a minute to check out this new newsletter and hope you find the information presented to be interesting and useful. Should you have any questions regarding the Navajo-Gallup Water Supply Project, or have input on the newsletter, please contact Pat Page, Bureau of Reclamation NGWSP Project Manager, at (505) 324-5027, or email at ppage@usbr.gov.

You can also check out their website at https://www.usbr.gov/uc/rm/navajo/nav-gallup/index.html.

David Klein recognized by Regional Director

By Clint Stone, Regional Office



From left, Regional Director Brent Rhees presents the Upper Colorado Region Director's Honor Award plaque to Powerplant Supervisor David Klein with Power Office Manager Talmadge Oxford. Bureau of Reclamation photo by Clint Stone

Region Director Brent Rhees took the opportunity during the last Power Operations and Maintenance meeting to present the Upper Colorado Regional Director's Honor Award to Morrow Point Powerplant Supervisor David Klein in the regional office in Salt Lake City, January 30, 2018.

Join us in congratulating David on his recognition, the full award citation is below.

Upper Colorado Regional Director's Honor Award Presented to David L Klein

In recognition of his outstanding contributions as a Power Plant Supervisor for the Upper Colorado Region and the Bureau of Reclamation.

Mr. Klein serves as the Power Plant Supervisor for the Morrow Point Powerplant and Dam in the Upper Colorado Power Office in Montrose, Colorado. His contributions and leadership in this position resulted in significant accomplishments that improved personnel safety, facility reliability, and preservation of the unique history of the project and area. He pursued facility modernization projects that improved plant reliability while prioritizing personnel safety. One recent example is the replacement of the unit breakers and station service switchgear which now allows for operation and maintenance activities to be performed remotely without subjecting personnel to arc-flash hazards. Mr. Klein's success on the project served as an example throughout the Power Office

as other facilities are planning similar projects to improve safety and performance. He is currently pursuing replacement of the generator step-up transformer, which presents a significant fire and explosion hazard to personnel and equipment in the plant, with a sulfur hexafluoride (SF6) transformer that does not present fire or explosion hazards. When he first arrived at Morrow Point the gantry crane was not operable and critical maintenance activities could not be performed. He was integral to completing the project to repair the crane and shortly after commissioning used the crane to begin completing the backlog of maintenance. Mr. Klein also dedicated himself to preserving the history of the construction, maintenance and operation of Morrow Point as well as to the area surrounding the project. He researched Reclamation files for photos that document the history of the facility and displayed these prominently throughout the powerplant. His efforts will contribute to awareness of the history of the project and increase pride in the work personnel perform to maintain the facility far into the future. For his significant contributions to the Bureau of Reclamation and the citizens of the United States, David L. Klein is granted the Upper Colorado Regional Director's Honor Award.

"It Was an Accident Waiting to Happen"

By Johnny Mendoza, UCRO Safety Council

"It Was an Accident Waiting to Happen"

Some people prefer to learn their life lessons the hard way. For example, some individuals choose to ignore their issues in hopes that they will just go away. When we aren't addressing a problem early enough, it can become a full-blown crisis. But, some people argue that failure is okay, and, at the very least, we can learn from our mistakes. Right?

No. There is no room for error when it comes to managing your own personal safety and health.

Researchers estimate that for every death in the workplace caused by a safety failure, there were hundreds, if not thousands, of people who previously experienced close calls. In an accident investigation, people will typically say, "It was an accident waiting to happen," or in other words, everybody was aware of the hazard and nobody did anything about it. Just one person brave enough to communicate a problem could have made an impact for the deceased individual and for everyone who is left with the pain of loss.

Reclamation is providing training for every agency employee that teaches us the importance of being safe and healthy at work. Employees are learning what their responsibilities are according to the Safety and Occupational Health Program at Reclamation. Class participants practice communicating in front of an audience their safety concerns that they have witnessed in their own lives. We are convinced that the best way to foster a safe work environment is by communicating our safety concerns and by caring to look out for one another.

Employees have shared many vivid stories of safety lessons that they have learned, and we want to continue to share some of these lessons:

- Think through what you are doing at all times and be aware of your surroundings.
- Inspect government-owned vehicles at the time you are selecting a vehicle to reserve and before driving the vehicle. Complete Form 7-2633 Motor Vehicle Safety Inspection Checklist and report any issues to Virginia Thurgood in the Fleet Department.
- If you drive a vehicle for work, you are required to complete the Annual Motor Vehicle Operator's Certification https://intra.uc.usbr.gov/bss/gen/7-2632.pdf.
- Anticipate the actions of other drivers and be prepared to take responsive actions.
- Using a cell phone while driving and driving while drowsy can be fatal.
- Have an accident reporting kit (SF-91 Motor Vehicle Accident Report and two copies of SF-94 Statement of Witness) in your briefcase if you are in a government-rented vehicle.
- Remember that you are publicly representing the Federal Government when you are in a government-owned vehicle.
- Do not use an unbalanced or wheeled object to stand on. Use a ladder and make sure there is someone watching out for you.
- Hold on to stairwell handrails to avoid slipping and falling because waxed flooring can become slippery.
- Keep office refrigerators clean and immediately remove any rotting food.
- Clean up any ice that falls on the floor because it will melt and create a slip hazard.
- Be aware of your surroundings when leaving a federal building, especially at night.
- Take into consideration the environmental conditions in which you are walking and the shoes that you are wearing.
- When crossing the street look out for cars that may not see you, even if you have the right of way.
- Ask for safety training if you need it.
- Use ear plugs or noise-cancelling headphones in noisy environments, even outside of work.
- Never leave a space heater unattended.
- Use proper form when lifting heavy objects so you can protect the health of your back.
- Request Job Hazard Analyses before visiting a facility so that you will arrive prepared. Visitors are never exempt from wearing required personal protective equipment because they failed to prepare.
- Never ignore the safety experts to meet a personal deadline.
- Be prepared by having emergency plans in place for your family, pets, and neighborhoods.

While we believe that communicating with your supervisor or the safety officer about your safety concerns is an effective way to identify and eliminate any accidents that are waiting to happen, we know that some people will prefer to report their concerns through other methods, such as the Health & Safety Hazard reporting form found on the intranet at https://intra.usbr.gov/ssle/safety/hazard.



Thank you for caring about your safety and health.

IT Security Corner – Did I get Hacked?

By John Strongo, Regional Information System Security Officer

The Bureau of Reclamation continually monitors the network for malicious files and suspicious activities but, just like driving a car, sooner or later you may have an accident no matter how secure you are. Below are clues to help figure out if you have been hacked and, if so, what to do. The sooner you identify something bad has happened, the more likely you can fix the problem.

Clues You Have Been Hacked

 Your anti-virus program generates an alert that your system is infected. Make sure it is your anti-virus software generating the alert, and not a pop-up window from a website trying to fool you into calling a number or installing something else. Not sure? Open your anti-virus program.



- You get a pop-up window saying your computer has been encrypted and you have to pay a ransom to get your files back.
- Your browser is taking you to all sorts of websites that you did not want to go to.
- Your computer or applications are constantly crashing or there are icons for unknown apps or strange windows popping up.
- Your password no longer works even though you know it is correct.
- Friends ask you why you are spamming them with emails that you know you never sent.
- There are charges to your credit card or withdrawals from your bank account you never made.

How to Respond

If you suspect you have been hacked, the sooner you act the better. If the hack is work related, do not try to fix the problem yourself; instead, report it to your UC IT Security team immediately (ibr4ucrditsec@usbr.gov). If it is a personal system or account that has been hacked, here are some steps you can take:

- Change Your Passwords: This includes not only changing the passwords on your computers and mobile devices, but for your online accounts. Do not use the hacked computer to change your passwords; use a different system that you know is secure. If you have a lot of accounts, start with the most important ones first. Can't keep track of all your passwords? Use a password manager.
- Financial: For issues with your credit card or any financial accounts, call your bank or credit card company right away. Use a trusted phone number to call them, such as from the back of your bank card, your financial statements, or visit their website from a trusted computer. In addition, consider putting a credit freeze on your credit files.
- Anti-virus: If your anti-virus software informs you of an infected file, follow the
 actions it recommends. Most anti-virus software will have links you can follow to
 learn more about the specific infection.
- Reinstalling: If you are unable to fix an infected computer or you want to be surer
 your system is safe, reinstall the operating system. Do not reinstall from backups;
 instead, backups should only be used for recovering your personal files. If you
 feel uncomfortable rebuilding, consider using a professional service to help you.
 Or, if your computer or device is old, it may be easier to purchase a new one.
 Finally, once you have rebuilt your system or purchased a new one, make sure it
 is updated and enable automatic updating whenever possible.
- Backups: A key step to protecting yourself is to prepare ahead of time with regular backups. Many solutions will automatically back up your files daily or hourly. Regardless of which solution you use, periodically check that you are able to restore those files. Quite often, recovering your data backups is the only way you can recover from being hacked.
- Law Enforcement: If you feel in any way threatened, report the incident to local law enforcement. If you are the victim of identity theft and are based in the United States, then visit https://www.identitytheft.gov.

Article attributed from SANS Security Awareness at https://www.sans.org/security-awareness-training/resources/am-i-hacked

In Transition

Lisa lams – Information Resources Division Manager – Upper Colorado Regional Office



PhotoWe are pleased to announce that we have finalized the recruitment process for the Upper Colorado Region -Information Resources Division Manager.

Please join us in congratulating the new UC/IRD Manager, Lisa lams. We didn't have to look far in our recruitment! Lisa has been with the UC Region for several years, including supervisory roles in Public Affairs and IRD. She will be leaving her position as, Chief IT Customer Support & Web Group. The benefit for us, is that she will remain with the Region!

Lisa is well suited to lead the UC/IRD into a future of change, challenge, and opportunity.

Again, please welcome Lisa to her new role as the IRD Manager for the Upper Colorado Region!