Operations Committee Meeting
Wednesday, December 29, 2021 8:30 AM
Lower Platte North NRD Office
P.O. Box 126
Wahoo, NE 68066

1. UNFINISHED BUSINESS
   We have nothing to consider for unfinished business.
2. WILD NE AND OTHER PROGRAMS
   Currently, the tree removal contractor, Standing C Excavating, is working on the Wanahoo property and has made good progress.
   An email was sent to Pheasants Forever asking for a commitment to prescribe burn areas of Wanahoo in 2022. We have not burned for three years.
3. OPERATION & MAINTENANCE & OTHER ITEMS
   The O & M crew continues to remove trees from our recreation and project areas. We hauled rock (rip-rap) to Rawhide Ditch after a 36" culvert repair was completed. Closed the culvert gates on Clear Creek Ditch 1 that lead to the Platte River. Also servicing equipment.
   A. Wanahoo Stilling Basin - (FEMA)
      On Friday, Dec. 17th, FEMA gave the District verbal approval for the scope changes involving the dewatering wells and the basin floor. Griffin Dewatering mobilized on Dec. 15th but did not start the drilling operation until Monday, Dec. 20 because of equipment breakdown. They have 3 of the 5 wells drilled.

      We are conversing with NEMA/FEMA whether we need to present a more solid design plan for the basin floor which will cost more versus the band-aid approach in the current scope change (construction detail was not explained in detail). The more robust design is recommended by NDNR Dam Safety and would follow Federal Design Guidelines. (see Sotak Email attached)

      We will need to update our contract with FYRA to design and oversee the improvements to the basin floor and also decide if we want Valley Corp to do the floor repair or rebid the basin floor project. The basin floor improvements may not occur until mid 2022 but, we need to keep the pre-construction items moving forward.
      Last month the $89,607.86 cost was approved for converting the wells to pressure relief wells. Now there may be some cost savings that could lower that amount approximately $12,000, that may not be known until the well project is completed.
   B. NRD Owned Lots
      Heimann with assistance of Mountford and legal counsel Lausterer have developed two different easements (attached) for the 6 lots owned by the District at Thomas Lakes (see aerial). The easement developed for the four lots on the high ground will be permitted to use mobile/removable objects on the lots, whereas the two lots on the Clear Creek Levee will not permit any objects permanent or removable. The

easements have been forwarded on to the Corps of Engineers.
Next steps are an updated title search and a stake survey.

C. Wanahoo Relief Well Reconditioning
A RFQ/RFP was developed by Heimann and Olsson's. NDNR Dam Safety has reviewed with no comments. The final will be sent to Well Drilling Companies for bids to refurbish three wells and if successful an additional 4 wells. A site showing is scheduled for Thursday, January 20 at 11:00 am and bids are due March 1 at 4:00 pm. See attached.

D. Rawhide Ditch Culvert Repair
A 36" culvert with a flap gate tore/split. We had Thompson Construction repair it with a band for $1,610.00. The District added broken concrete below the culverts. See attached pictures.

4. ROCK AND JETTY
We have not received any inquiries for the program.

5. LAKE WANAHOO

A. Lake Wanahoo Permit Sales
For the month of December (as of 12/28), the District has received $3,830.00 in annual park permit revenue. The year by year breakdown for annual permits sold during the month of December is listed below. The District began selling 2022 annual permits on December 2nd.

B. Month	C. Monthly Total	D. YTD Total
E. December 2021	F. 3,830.00	G. 3,830.00
H. December 2020	I. 4,725.00	J. 4,725.00
K. December 2019	L. 4,470.00	M. 4,470.00
N. December 2018	O. 4,585.00	P. 4,585.00

Q. Lake Wanahoo Camping Revenue
For the month of December, the District received $2,438.00 in camping revenue at Lake Wanahoo. For the calendar year, camping revenue totals $118,152.11. The year by year breakdown for camping revenue during the month of December is listed below.

R. Month	S. Monthly Total	T. YTD Total
U. December 2021	V. 2,438.00	W. 118,152.11
X. December 2020	Y. 1,485.97	Z. 134,027.78
AA. December 2019	BB. 1,160.56	CC. 93,337.36

DD. Clint Johannes Education Building
During the month of December, the building was rented 15 times. Revenue for the month is $1,180.

EE. **Year**	FF. **Rentals**	GG. **Youth Rentals**	HH. **Rental Income**
II. **2020**	JJ. 118	KK. 14	LL. $8,240

MM. **2021**	NN. 184	OO. 27	PP. $12,840

6. INFORMATION AND EDUCATION

A. Information

1. Radio & eAds
   The Radio and E-ads for the first half of December featured the December 15th water reports deadline. The last half of December featured Wanahoo Park Permits available at the office and online (attached).
2. Analytics

3. **FACEBOOK**	4. **Total Reach**	5. **Engagements**	6. **Followers**
7. **December 1-27**	8. 2,159	9. 95	10. 1,299
11. **November**	12. 2,235	13. 30	14. 1,298
15. **October**	16. 1,311	17. 44	18. 1,297

19.

20. **TWITTER**	21. **Total impressions**	22. **Engagements**	23. **Followers**
24. **December 1-27**	25. 2,024	26. 114	27. 348
28. **November**	29. 3,008	30. 78	31. 345
32. **October**	33. 1,725	34. 40	35. 344

36.

Top Posts on Facebook and Twitter:

- Wahoo Creek Watershed draft plan available for public review
- Handplant trees and shrubs available for purchase
- Water Resources Technician position opening
- 2022 Wanahoo permits available
- December 15th water report deadline

37. **WEBSITE**	38. **Use**	39. **Traffic**	40. **Top Pages**	41. **Devic**

	rs	**Channel**		**es**
42. **December 1-27**	43. 830	44. Organic 52.1% Direct 33.7% Referral 10.4% Social 3.7%	45. Home Lake Wanahoo Downloads Staff Contact	46. Desktop 59.16% Mobile 39.16% Tablet 1.69%
47. **November**	48. 809	49. Organic 52.1% Direct 33.7% Referral 10	50. Home Lake Wanahoo Czechland Lake Downloads For	51. Desktop 50.31% Mobile 46.35

		.4% Social 3.7%	estry	% Tablet 3.34%
52. **October**	53. 1,160	54. Organic 62.3% Direct 21.5% Referral 8.9% Social 7.2%	55. Lake Wanahoo Home Czechland Lake Downloads Outdoor Recreation	56. Mobile 54.40% Desktop 43.10% Tablet 2.50%

57. **26 clicks from Facebook to our website and 6 clicks from Twitter to our website.**

58. News Channel Nebraska Advertising
The Information and Education Department video is completed and with the commitment to advertise, we will run the :60 commercial in January and February.

We would like to continue our great partnership with News Channel Nebraska since their viewing area covers most of our District. The following is a proposed schedule for early next year.

59. March	60. :30 Lake Wanahoo	61. News Sponsor $475

62. April	63. :30 I&E, :30 Projects, :30 Operations & Maintenance	64. News Sponsor $475
65. May	66. :30 I&E, :30 Projects, :30 Operations & Maintenance	67. News Sponsor $475

68.

B. Education

7. RURAL WATER SYSTEMS

WaterISAC and EPA, in cooperation with water sector associations, developed the attached advisory to present important information to the water sector on two recent cybersecurity advisories by the United States Government. On December 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the National Security Agency issued a joint advisory on Russian state-sponsored cyber operations against United States critical infrastructure (also attached). It complemented a December 15, 2021 CISA publication - Preparing For and Mitigating Potential Cyber Threats. These Advisories asserted that due to persistent cyber-threats from sophisticated actors, including nation-states and their proxies, critical infrastructure owners and operators should take immediate steps to strengthen their computer network defenses.

A. Colon System

Routine monthly sampling completed, meters read and billing cycle has been calculated. The bills will be mailed 1/3/22.

B. Bruno System

Routine monthly sampling completed, meters read and billing cycle has been calculated. The bills will be mailed 1/3/22.

C. Other

Bob Heimann

From: Mike Sotak <msotak@fyraengineering.com> on behalf of Mike Sotak
Sent: Sunday, December 26, 2021 9:01 AM
To: Eric Gottschalk; Chris Poole; bheimann@lpnnrd.org
Cc: Eric Suing
Subject: Apron Overlay Path Forward
Attachments: Board Update 10-11-21.pdf

LPNNRD:

Attached, please find the slide show I presented at the 11 October Board Meeting. During this presentation, we discussed doing a "quick fix" overlay to the damaged apron floor as well as a more sound solution that meets Federal design guidelines.

Tim Gokie at NDNR stated that while he would allow the quick fix, he also suggested that he would prefer to see a solution that meets current Federal design guidelines that are referenced in the .ppt slides.

I have no way of predicting how well a quick fix may last. It's a very unique situation and finding an apples to apples comparison of something similar in the past is not available. That, and given the feedback that Chris Poole has received from NEMA/FEMA, it seems likely that repairing it properly makes sense and will likely get funded.

The original fee for a quick design for this in the latest contract amendment was just for a quick fix. I need to get you a scope/fee estimate for the "proper" repair. As discussed at the 11 October meeting and as shown in the .ppt sides, that will take more design work.

So here is what needs to happen:

1. FYRA is coordinating w/ a subconsultant (Terracon) to perform anchor strength testing at the apron. This involves drilling anchors into the RCC apron and pulling them out at different strengths to test the ability to place anchors in the apron and at what depth. We reached out to them back in October, and have re-initiated those discussions based on Chris' latest feedback from NEMA/FEMA.
2. Once I know Terracon's costs, I will let you know. This will hopefully fit within the current contract amount w/ FYRA for design and extended construction observation.
3. Once the anchor strength tests are done, FYRA will prepare a new cost estimate and design/construction services fee for the work.

Regarding schedule, I hope to hear more from Terracon this week. I have been telling them that doing this during de-watering will make this most sense as they will be able to drain the basin and work easier. Terracon is letting me know if draining the basin is required for sure. So we hope to have this anchor test done during January when Valley Corp has de-watered the site and is working on the stilling basin completion.

Also regarding schedule, the design will not likely be completed/reviewed/approved until after Valley Corp has completed their current contracted work. Therefore, I emailed Chris to check w/ NEMA to see if they saw any issue w/ hiring another contractor, if that is even an option. Once we know the answer to that, we can decide how best to proceed...

Unrelated, I reached out to Tanner at Valley Corp again last week to check on the status of Change Order #2 review. I still have not heard back. I will try again tomorrow and let you know when I hear from them.

A reminder that I leave for vacation tomorrow and will be out of the country Dec. 27th – January 3rd. I will be checking email and hope to have phone service. But I do have a scuba dive planned during the Operations Committee, so will not be able to attend. Please feel free to forward this email to them ahead of time and see if they have any questions they would like answered ahead of the meeting, and I will do my best to get that done....otherwise, I think agreeing that the path forward discussed in this email is agreeable is probably all that CAN be done at this time.

Michael K. Sotak, P.E., D.WRE
12702 Westport Parkway, Suite 300 | Omaha, NE 68138
Phone: 402.502.7131 | Direct: 402.934.8328 | Cell: 402.850.6169
www.fyraengineering.com
msotak@fyraengineering.com

FYRA

LOWER PLATTE NORTH NRD

LAKE WANAHOO DAM

STILLING BASIN REPAIR

11 OCTOBER 2021

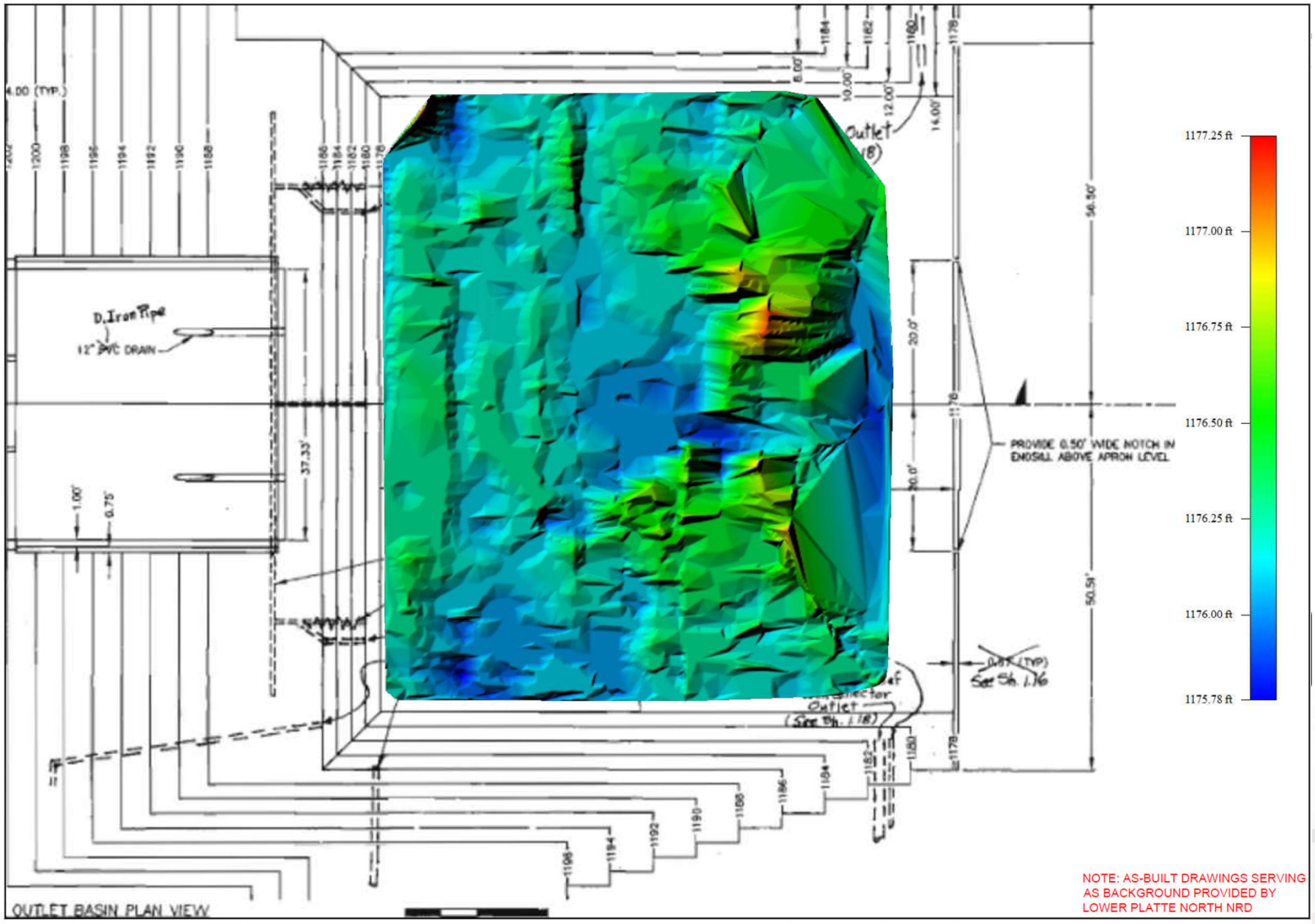
FYRA ENGINEERING

Presentation Agenda

1. Apron Repair Alternatives
2. De-watering/pressure relief wells
3. Decisions to be made
4. Future schedule

FYRA ENGINEERING

Apron Condition



FYRA ENGINEERING

How Do We Properly Fix It?

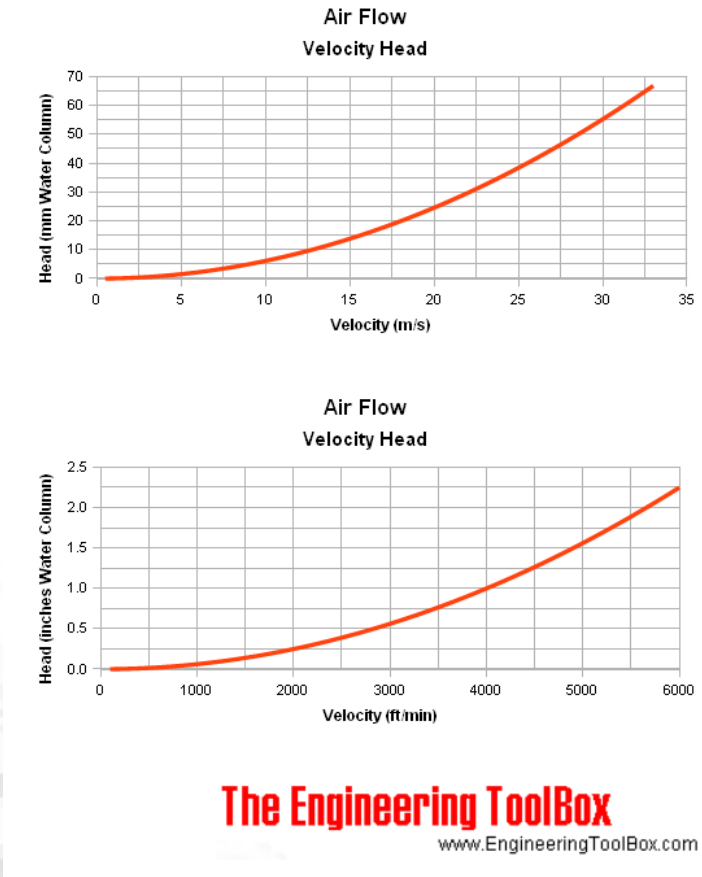
NDNR Requires that Solution Is:

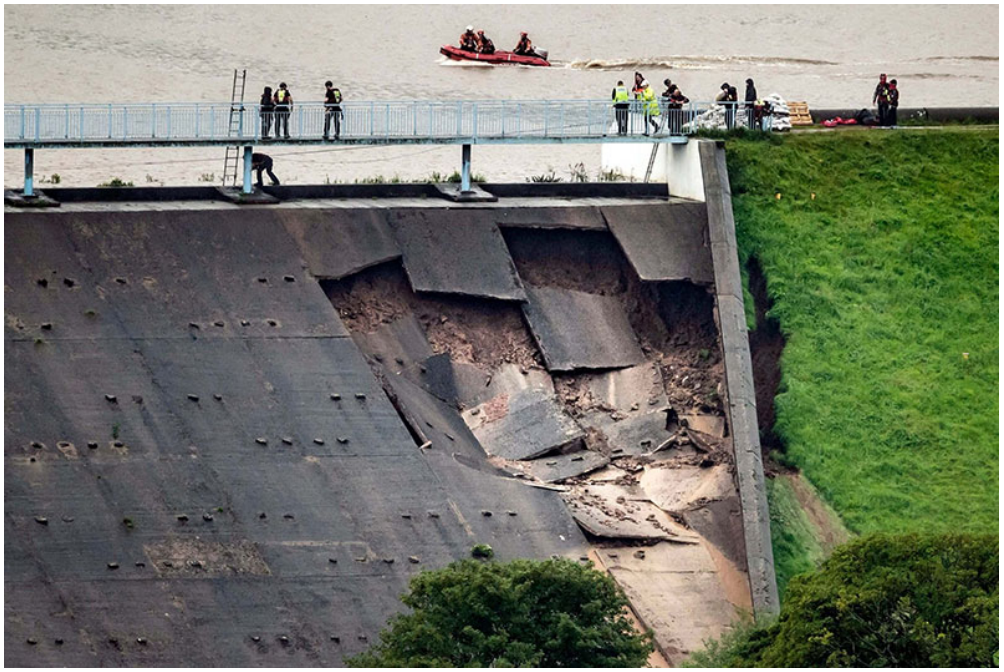
1. **R**obust
2. **R**edundant
3. **R**eliable

FYRA ENGINEERING

Design Considerations

1. Uplift



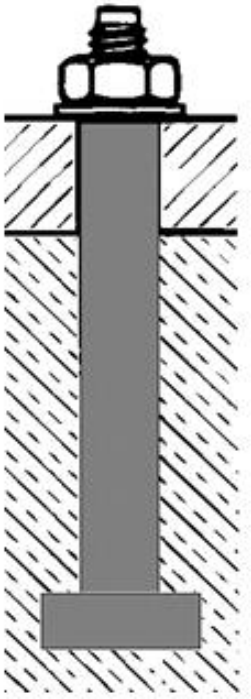


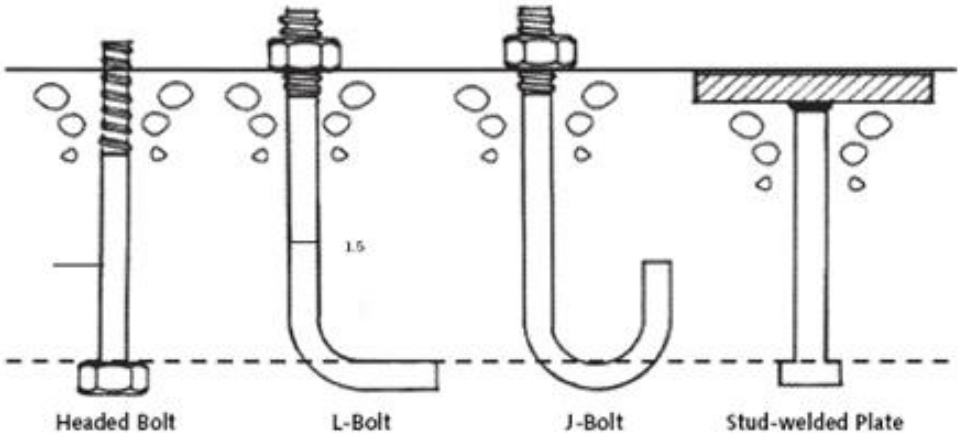
FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors

Cast-In Anchor

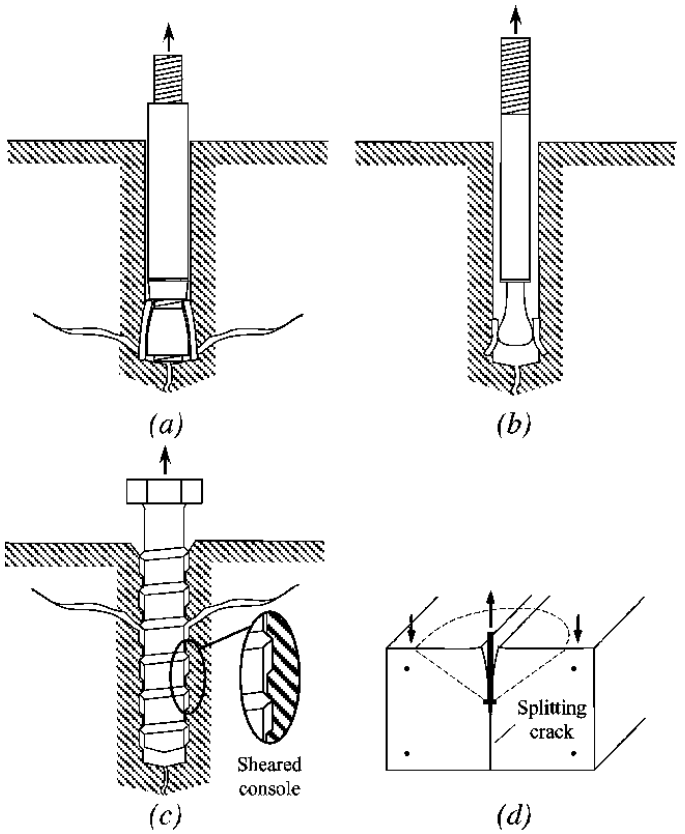




FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors



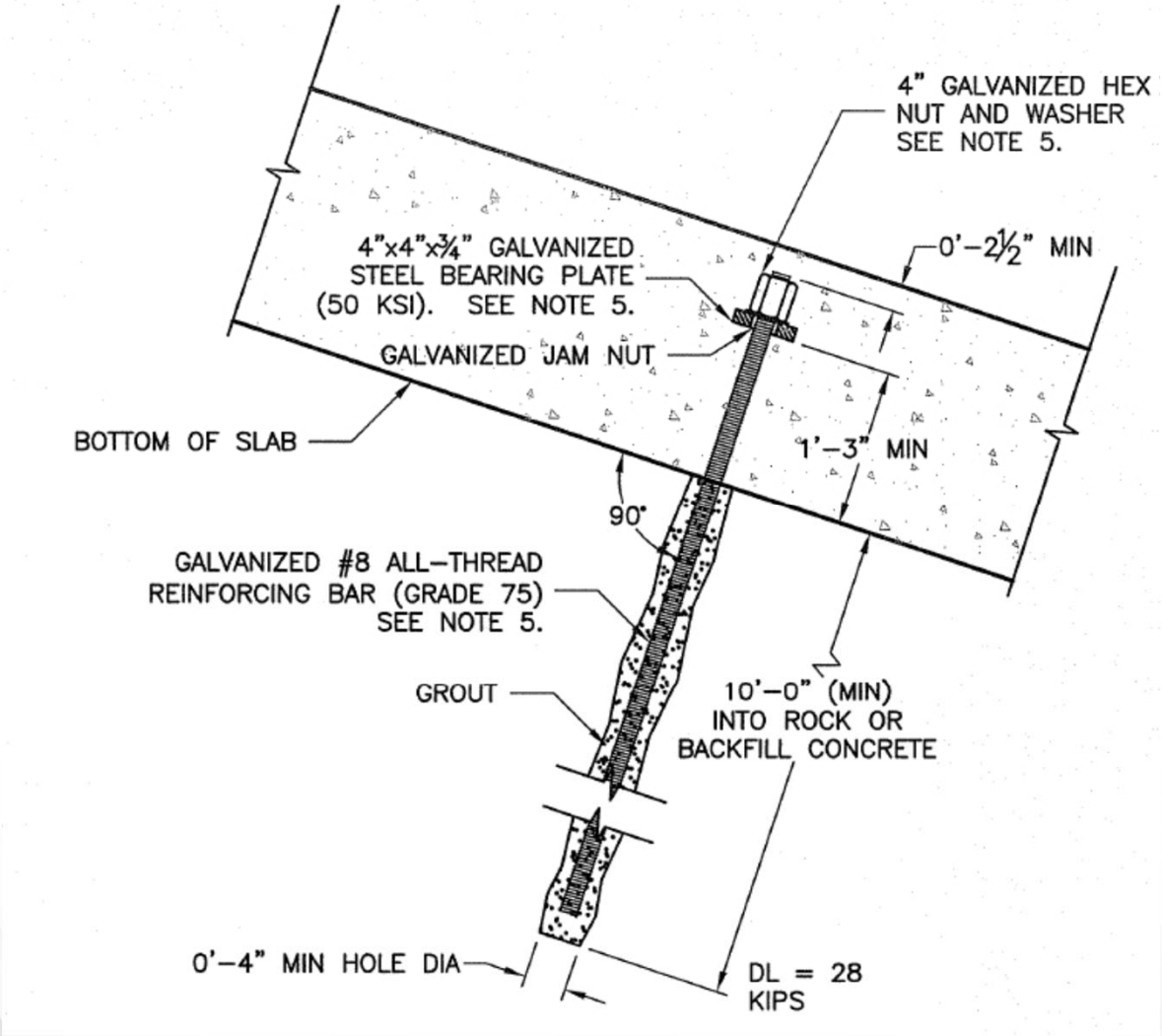
(a)

(b)

FYRA ENGINEERING

Design Considerations

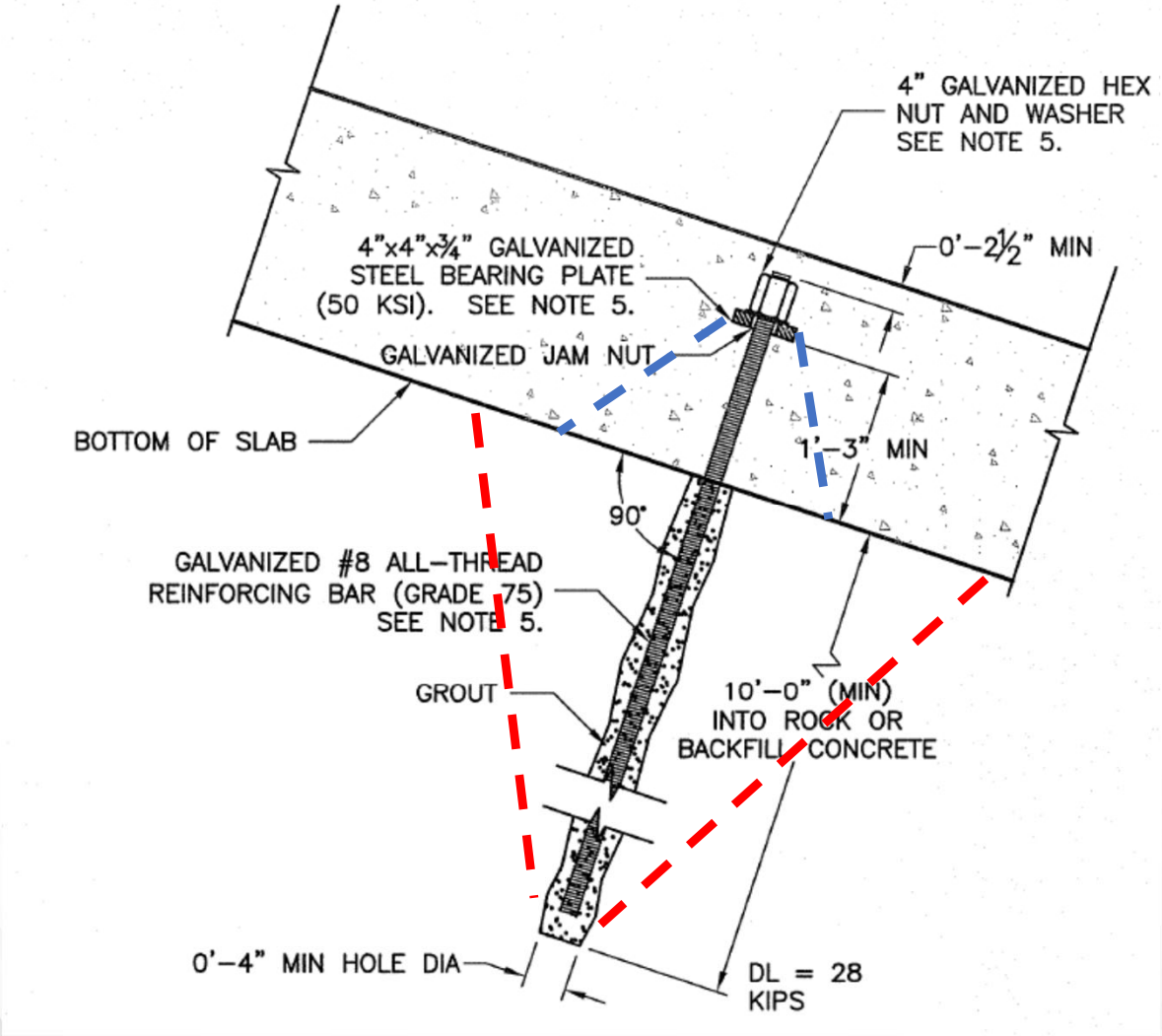
1. Uplift
2. Anchors



FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors



FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors

FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors

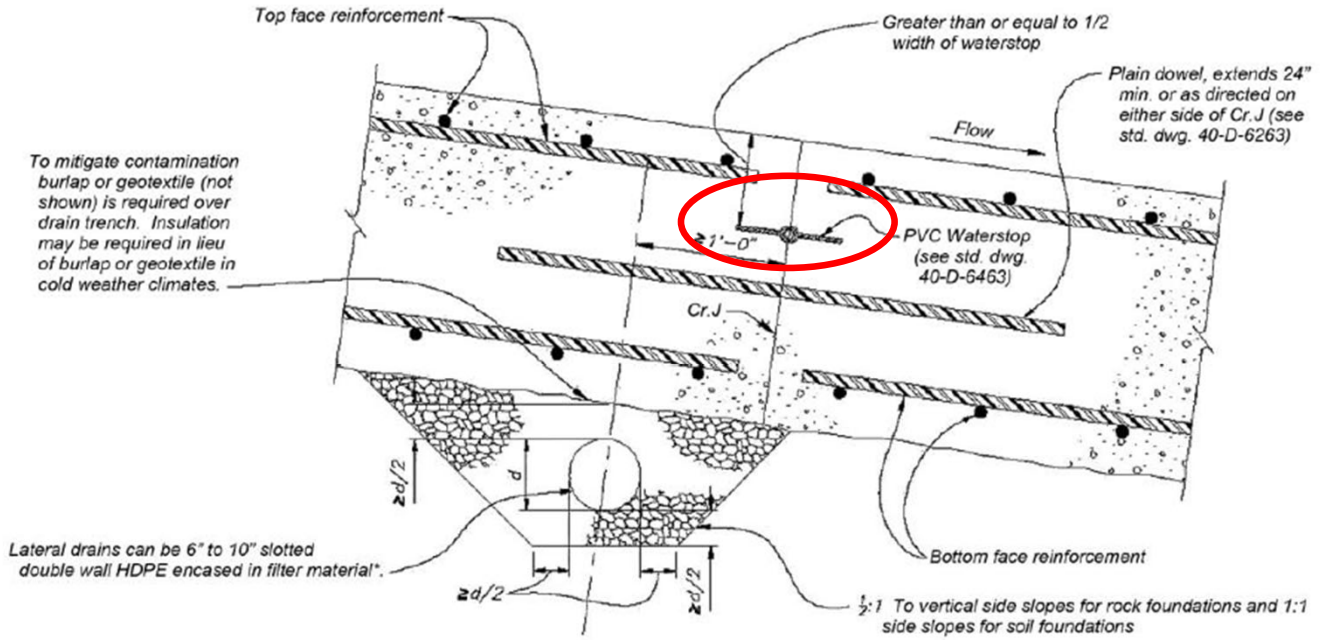
Design Considerations

1. Uplift
2. Anchors
3. Adhesion

FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors
3. Adhesion
4. Waterstops



CASE 1B: ROCK OR SOIL FOUNDATION WITHOUT FOUNDATION KEY – FLAT TO GRADUAL SLOPE – APPLICABLE FEATURE IS TERMINAL STRUCTURE (STILLING BASIN)

FYRA ENGINEERING

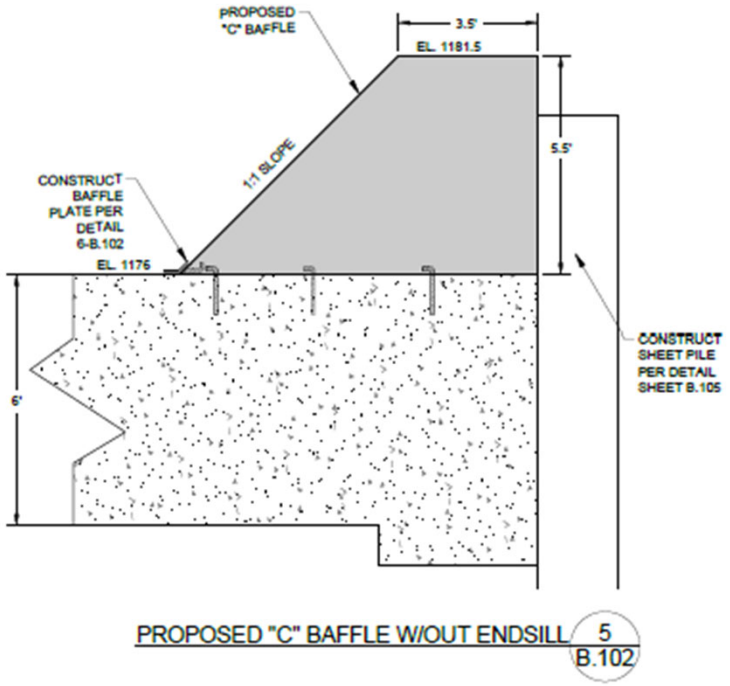
Design Considerations

1. Uplift
2. Anchors
3. Adhesion
4. Waterstops

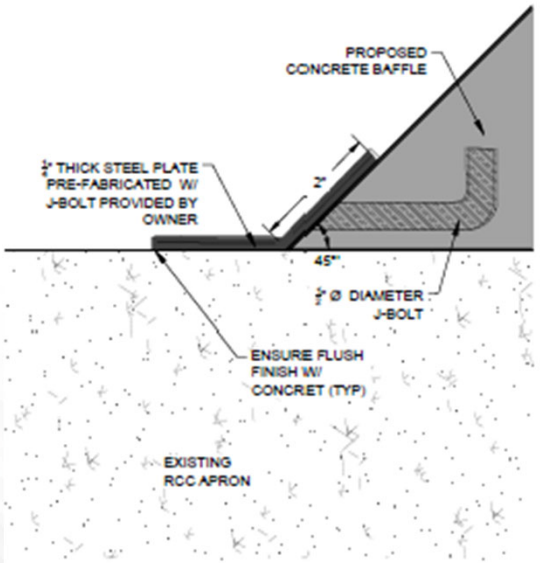
FYRA ENGINEERING

Design Considerations

1. Uplift
2. Anchors
3. Adhesion
4. Waterstops
5. Baffles



PROPOSED "C" BAFFLE W/OUT ENDSILL 5 B.102



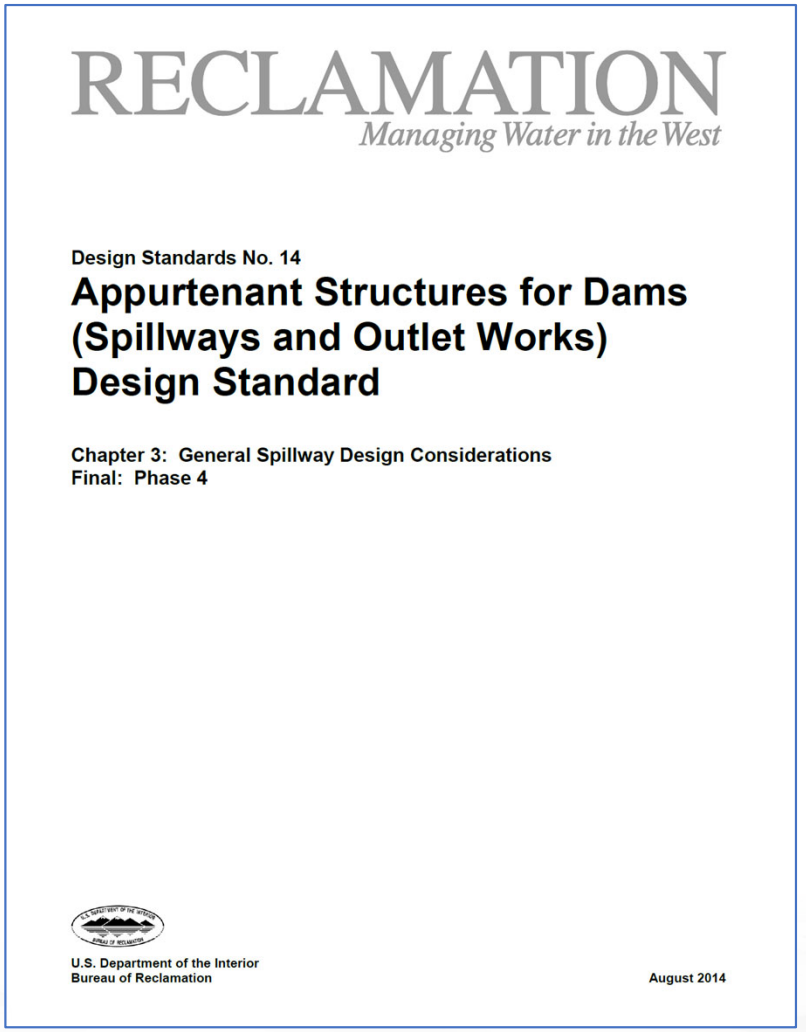
BAFFLE PLATE 6 B.102

FYRA ENGINEERING

Design Guidance

NDNR notes poor condition of many concrete slabs in dams across Nebraska.

Suggests using USBR guidance for a RRR apron overlay.


RECLAMATION
Managing Water in the West

Design Standards No. 14

Appurtenant Structures for Dams (Spillways and Outlet Works) Design Standard

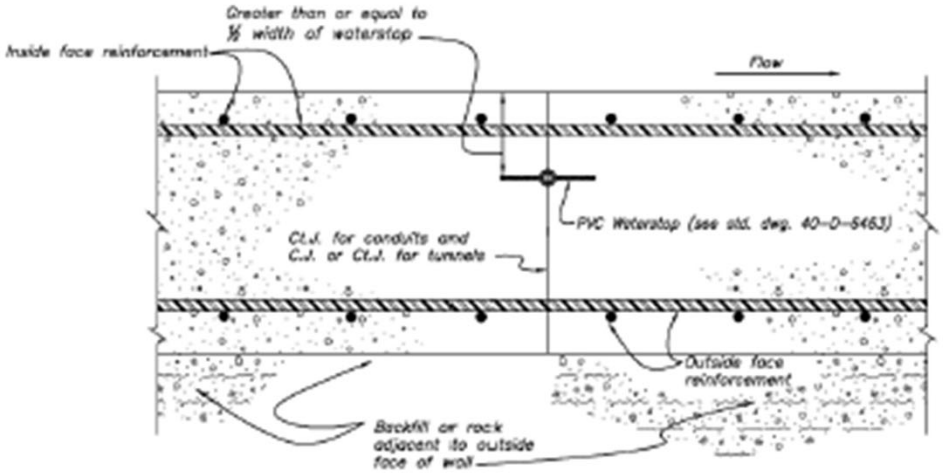
Chapter 3: General Spillway Design Considerations
Final: Phase 4

U.S. Department of the Interior
Bureau of Reclamation

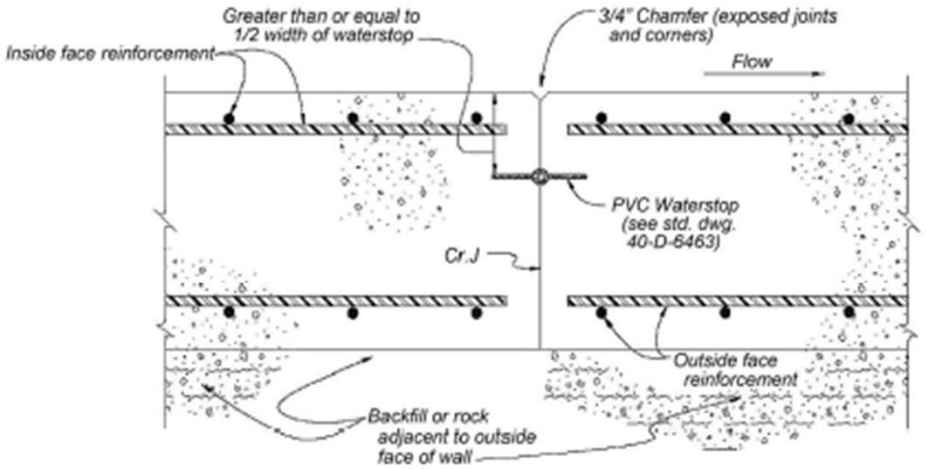
August 2014

FYRA ENGINEERING

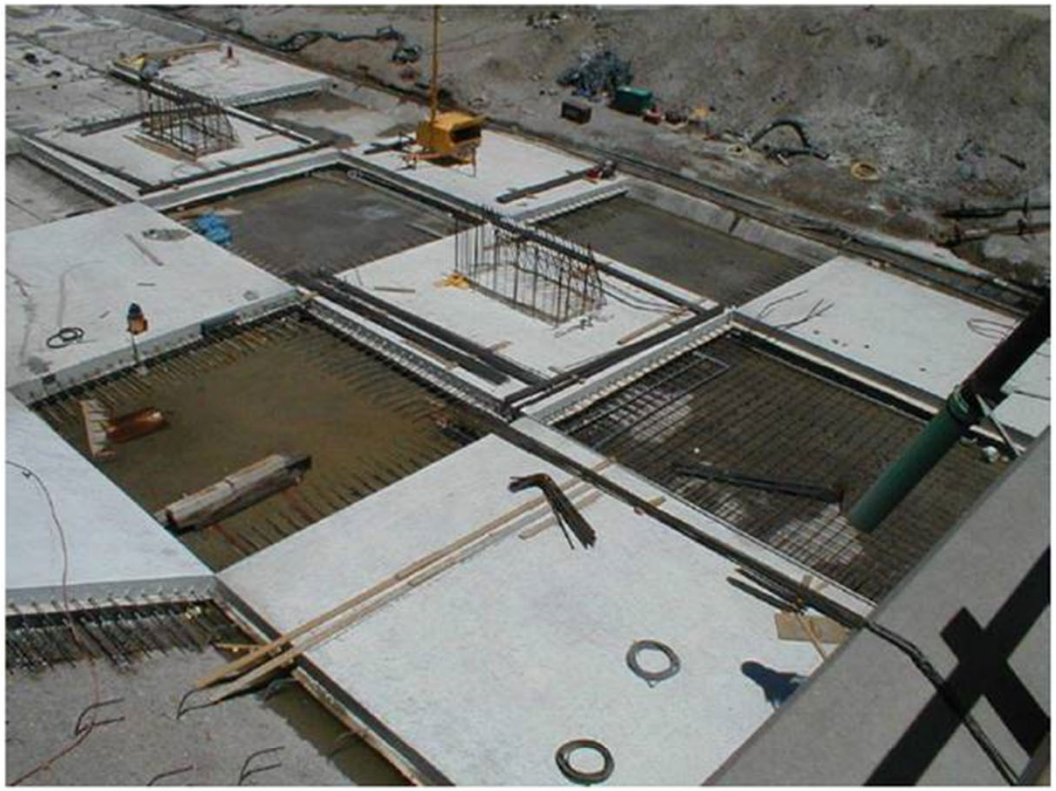
Design Guidance



FLOW SURFACE CONDUIT OR TUNNEL – LATERAL (TRANSVERSE) CONTROL JOINT (Ct.J) THRU CONDUIT AND CONSTRUCTION JOINT (C.J.) OR Ct.J. THRU TUNNEL – APPLICABLE FEATURE IS CONVEYANCE FEATURE



FLOW SURFACE WALL – LATERAL (TRANSVERSE) CONTRACTION JOINT (Cr.J) THRU WALL – APPLICABLE FEATURES ARE CONVEYANCE FEATURE (INLET STRUCTURE AND CHUTE), CONTROL STRUCTURE, AND TERMINAL STRUCTURE (STILLING BASIN)



FYRA ENGINEERING

Design Alternatives

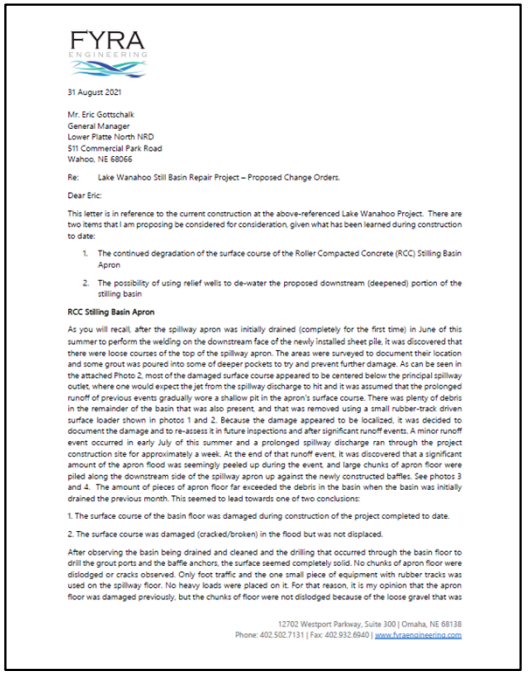
1. Follow all applicable guidance
2. Apron "Wear Surface"
3. Do Nothing

FYRA ENGINEERING

Other Alternatives

1. Follow all applicable guidance
2. Apron "Wear Surface"
3. Do Nothing

At this time, the best course of action is to repair the basin floor. And while some design work needs to be done, it is estimated that a minimum 8" thick course of reinforced concrete anchored to the existing spillway floor will take approximately 250 CY of concrete and 30,000 lbs of steel reinforcement and would cost approximately $480,000.00 to construct (including engineering). As mentioned above, there is design work to be done and potential cost savings to be realized, but guessing conservatively, this should be close, given unit prices given in the bidding process.



FYRA ENGINEERING

31 August 2021

Mr. Eric Gottschalk
General Manager
Lower Platte North NRD
511 Commercial Park Road
Wahoo, NE 68066

Re: Lake Wanahoo Still Basin Repair Project – Proposed Change Orders.

Dear Eric:

This letter is in reference to the current construction at the above-referenced Lake Wanahoo Project. There are two items that I am proposing be considered for consideration, given what has been learned during construction to date:

1. The continued degradation of the surface course of the Roller Compacted Concrete (RCC) Stilling Basin Apron
2. The possibility of using relief wells to de-water the proposed downstream (deepened) portion of the stilling basin

RCC Stilling Basin Apron

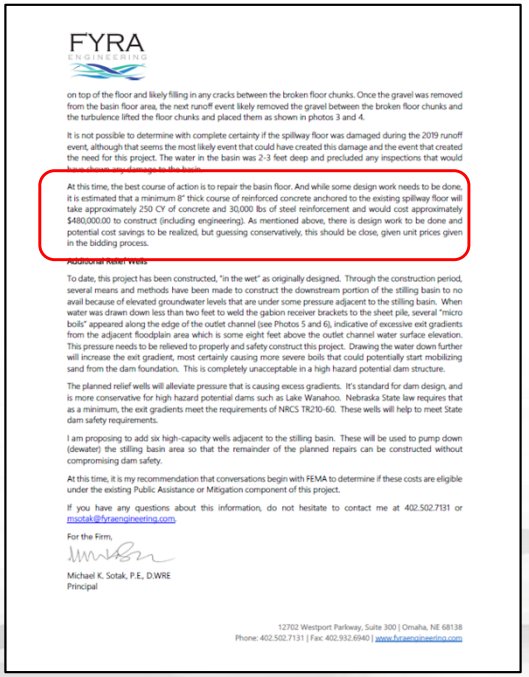
As you will recall, after the spillway apron was initially drained (completely for the first time) in June of this summer to perform the welding on the downstream face of the newly installed sheet pile, it was discovered that there were loose courses of the top of the spillway apron. The areas were surveyed to document their location and some grout was poured into some of deeper pockets to try and prevent further damage. As can be seen in the attached Photo 2, most of the damaged surface course appeared to be centered below the principal spillway outlet, where one would expect the jet from the spillway discharge to hit and it was assumed that the prolonged runoff of previous events gradually wore a shallow pit in the apron's surface course. There was plenty of debris in the remainder of the basin that was also present, and that was removed using a small rubber-track driven surface loader shown in photos 1 and 2. Because the damage appeared to be localized, it was decided to document the damage and to re-assess it in future inspections and after significant runoff events. A minor runoff event occurred in early July of this summer and a prolonged spillway discharge ran through the project construction site for approximately a week. At the end of that runoff event, it was discovered that a significant amount of the apron flood was seemingly peeled up during the event, and large chunks of apron floor were piled along the downstream side of the spillway apron up against the newly constructed baffles. See photos 3 and 4. The amount of pieces of apron floor far exceeded the debris in the basin when the basin was initially drained the previous month. This seemed to lead towards one of two conclusions:

1. The surface course of the basin floor was damaged during construction of the project completed to date.

2. The surface course was damaged (cracked/broken) in the flood but was not displaced.

After observing the basin being drained and cleaned and the drilling that occurred through the basin floor to drill the grout ports and the baffle anchors, the surface seemed completely solid. No chunks of apron floor were dislodged or cracks observed. Only foot traffic and the one small piece of equipment with rubber tracks was used on the spillway floor. No heavy loads were placed on it. For that reason, it is my opinion that the apron floor was damaged previously, but the chunks of floor were not dislodged because of the loose gravel that was

12702 Westport Parkway, Suite 300 | Omaha, NE 68138
Phone: 402.502.7131 | Fax: 402.932.6940 | www.fyraengineering.com



FYRA ENGINEERING

on top of the floor and likely filling in any cracks between the broken floor chunks. Once the gravel was removed from the basin floor area, the next runoff event likely removed the gravel between the broken floor chunks and the turbulence lifted the floor chunks and placed them as shown in photos 3 and 4.

It is not possible to determine with complete certainty if the spillway floor was damaged during the 2019 runoff event, although that seems the most likely event that could have created this damage and the event that created the need for this project. The water in the basin was 2-3 feet deep and precluded any inspections that would have shown any damage to the basin.

At this time, the best course of action is to repair the basin floor. And while some design work needs to be done, it is estimated that a minimum 8" thick course of reinforced concrete anchored to the existing spillway floor will take approximately 250 CY of concrete and 30,000 lbs of steel reinforcement and would cost approximately $480,000.00 to construct (including engineering). As mentioned above, there is design work to be done and potential cost savings to be realized, but guessing conservatively, this should be close, given unit prices given in the bidding process.

Additional Relief Wells

To date, this project has been constructed, "in the wet" as originally designed. Through the construction period, several means and methods have been made to construct the downstream portion of the stilling basin to no avail because of elevated groundwater levels that are under some pressure adjacent to the stilling basin. When water was drawn down less than two feet to weld the gabion receiver brackets to the sheet pile, several "micro boils" appeared along the edge of the outlet channel (see Photos 5 and 6), indicative of excessive exit gradients from the adjacent floodplain area which is some eight feet above the outlet channel water surface elevation. This pressure needs to be relieved to properly and safety construct this project. Drawing the water down further will increase the exit gradient, most certainly causing more severe boils that could potentially start mobilizing sand from the dam foundation. This is completely unacceptable in a high hazard potential dam structure.

The planned relief wells will alleviate pressure that is causing excess gradients. It's standard for dam design, and is more conservative for high hazard potential dams such as Lake Wanahoo. Nebraska State law requires that as a minimum, the exit gradients meet the requirements of NRCS TR210-60. These wells will help to meet State dam safety requirements.

I am proposing to add six high-capacity wells adjacent to the stilling basin. These will be used to pump down (dewater) the stilling basin area so that the remainder of the planned repairs can be constructed without compromising dam safety.

At this time, it is my recommendation that conversations begin with FEMA to determine if these costs are eligible under the existing Public Assistance or Mitigation component of this project.

If you have any questions about this information, do not hesitate to contact me at 402.502.7131 or msotak@fyraengineering.com.

For the Firm,

Michael K. Sotak, P.E., D.WRE
Principal

12702 Westport Parkway, Suite 300 | Omaha, NE 68138
Phone: 402.502.7131 | Fax: 402.932.6940 | www.fyraengineering.com

FYRA ENGINEERING

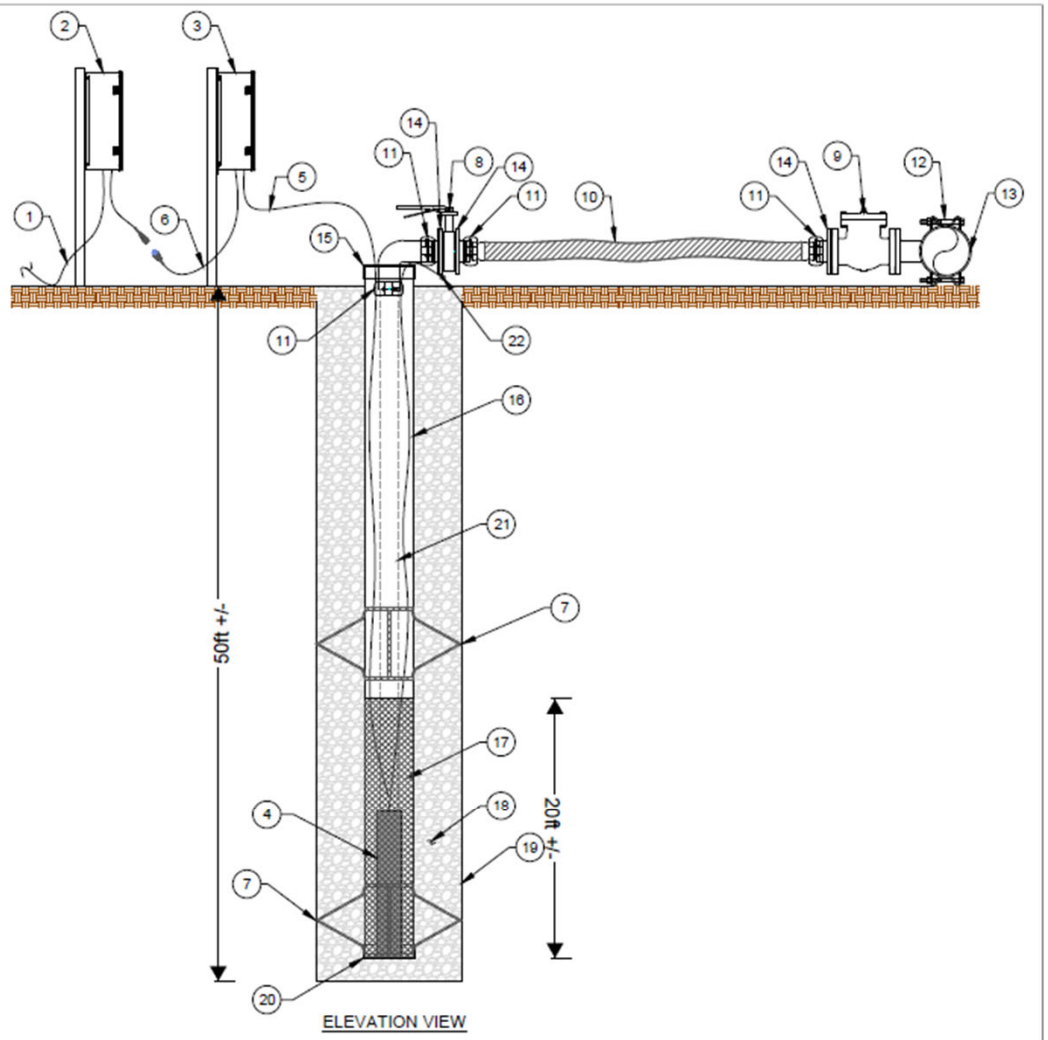
De-Watering/Pressure Relief Wells

1. De-watering required to complete stilling basin repair project.
2. Existing pressure relief wells in dam were tested for suitability for de-watering in mid-August
3. Existing PRWs did not provide enough drawdown for de-watering needs
4. On September 1st, a new de-watering plan was proposed consisting of six new wells
5. Cost of de-watering to be born by Contractor

FYRA ENGINEERING

De-Watering/Pressure Relief Wells

MATERIAL LIST — BELOW LIST IS TYPICAL; MATERIAL SUBSTITUTIONS MADE AS APPROPRIATE			
NO.	QTY.	U.O.M	EQUIPMENT
1	1	EA	ELECTRICAL DISTRIBUTION CABLE (BY OTHERS)
2	1	EA	JUNCTION BOX w/ 30AMP WEATHER TIGHT TWISTLOCK CONNECTOR (BY OTHERS)
3	1	EA	PUMP CONTROL BOX
4	1	EA	SUBMERSIBLE TURBINE PUMP (7.5HP, 460V, 3 PHASE)
5	1	EA	PUMP CABLE
6	1	EA	PIGTAIL w/ 30AMP WEATAHER TIGHT TWISTLOCK PLUG- TO CONNECT CONTROL BOX TO JUNCTION BOX
7	-	EA	CENTRALIZER (AS REQUIRED)
8	1	EA	BUTTERFLY VALVE, SUPPORTED TO PREVENT EXCESS WEIGHT ON ELBOW
9	1	EA	FLANGED CHECK VALVE
10	1	LF	HOSE,
11	4	EA	COUPLING
12	1	EA	STEEL TAPPING SLEEVE
13	1	EA	DISCHARGE PIPE
14	3	EA	FLANGE X GROOVE ADAPTER
15	1	EA	WELL CAP,
16	1	EA	PVC CASING (12")
17	1	EA	WELLSCREEN (12")
18	1	EA	WELLPACK (Pea Gravel or similar)
19	1	EA	BOREHOLE (32")
20	1	EA	PVC BOTTOM CAP
21	1	EA	RISER PIPE-
22	1	EA	SAFETY CABLE FOR PUMP RETRIEVAL



ELEVATION VIEW

GRIFFIN DEWATERING L.L.C.
5906 CLINTON DRIVE
HOUSTON, TX 77020
TEL: (713) 676-8000
FAX: (713) 676-8080
E MAIL: griffin@griffindewatering.com
WEBSITE: www.griffindewatering.com

REV.	DESCRIPTION	DATE	BY	APPVD.

TYPICAL DEWATERING WELL DETAIL

-

TYPICAL DEWATERING WELLS w/6" AND LARGER DISCHARGE

DRAWN: DW

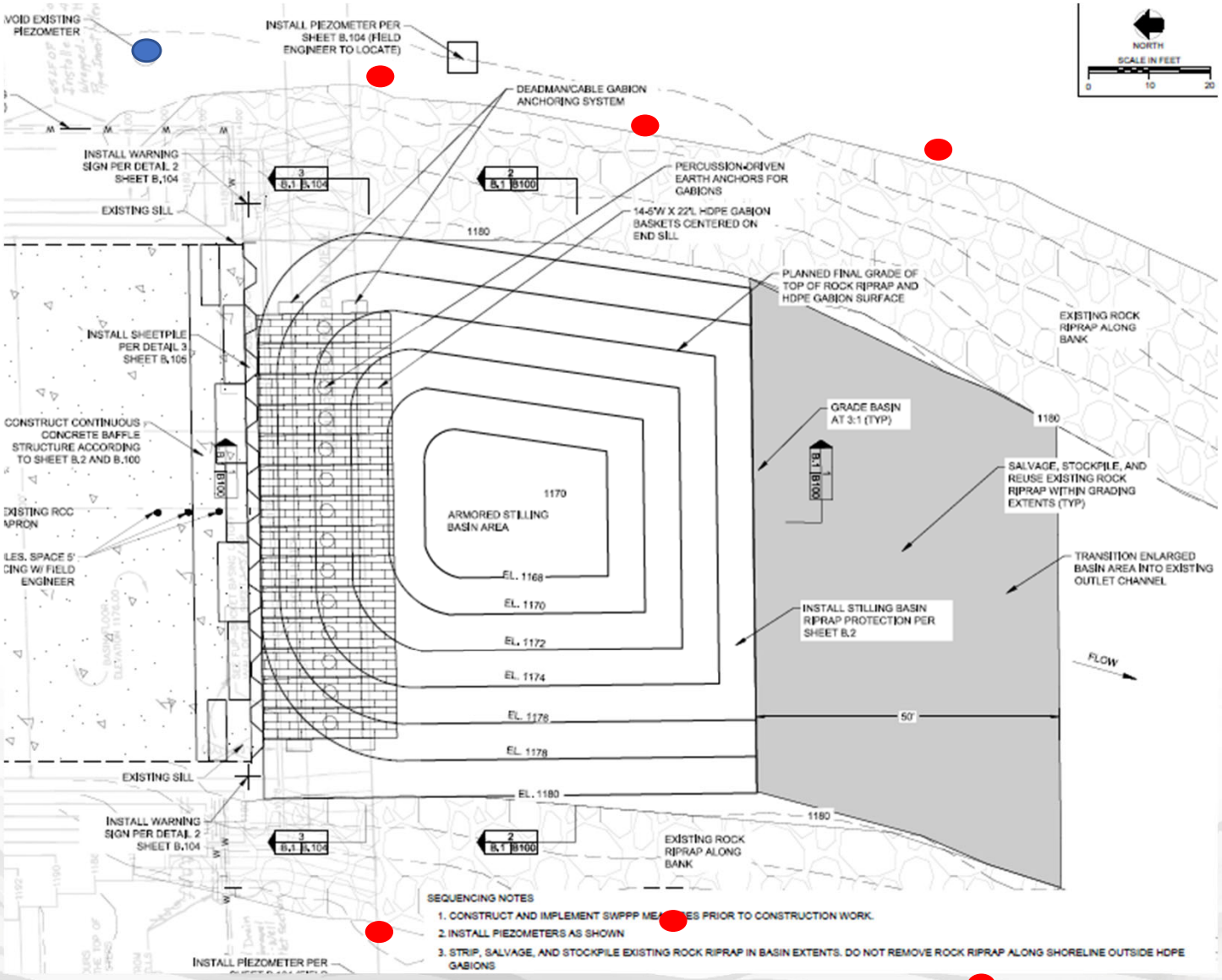
SCALE: N.T.S.

DATE: 09/01/2021

DWG: 02

FYRA ENGINEERING

De-Watering/Pressure Relief Wells



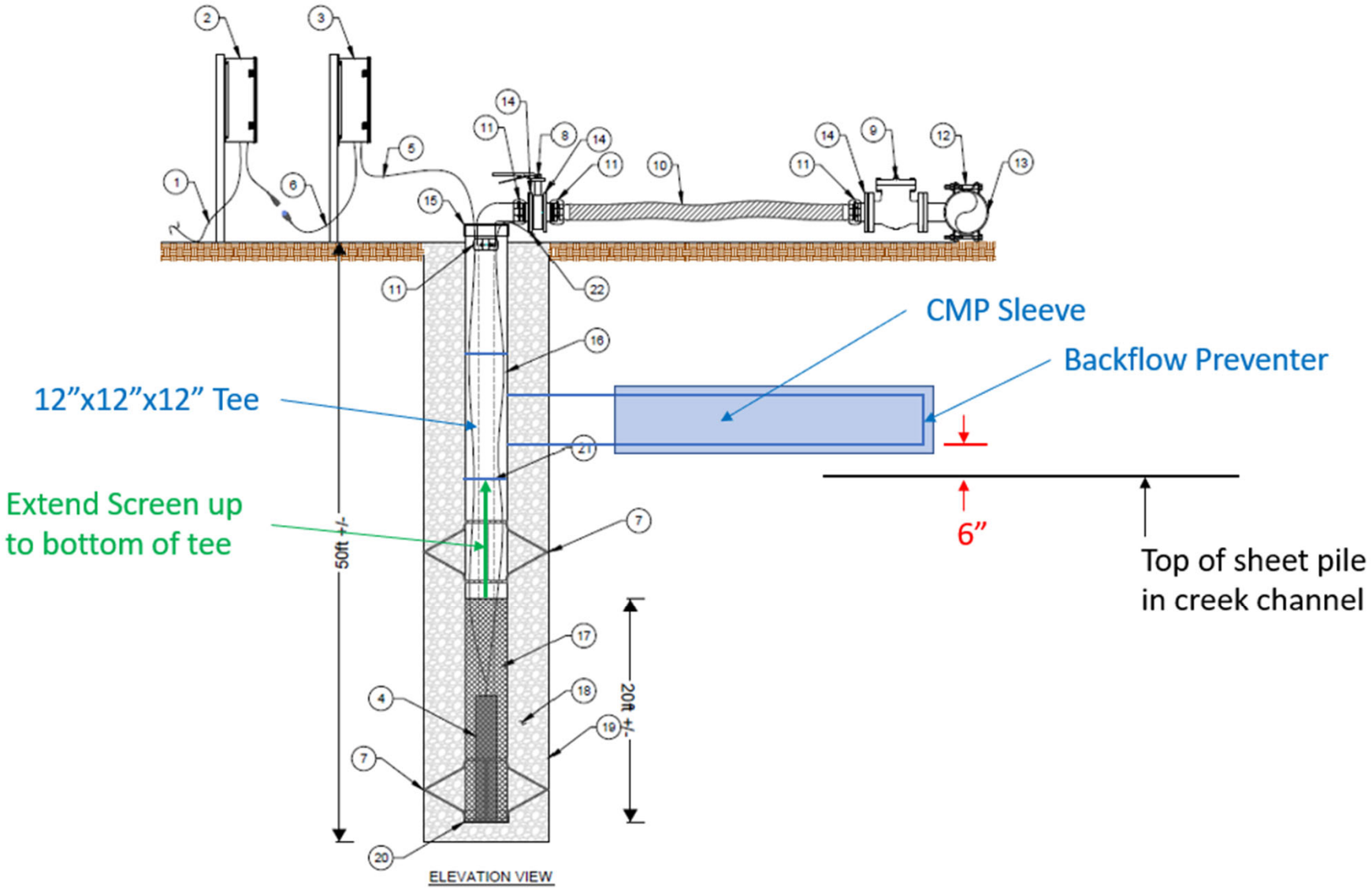
FYRA ENGINEERING

De-Watering/Pressure Relief Wells

1. Additional PRWs below Lake Wanahoo Dam have been identified as a need in recent observations
2. Through early September, coordination with Contractor to see if wells can be converted from de-watering to pressure relief after they are used to construct remainder of current project.
3. Changes to wells have been identified and an additional cost is being prepared by Contractor

FYRA ENGINEERING

De-Watering/Pressure Relief Wells



Next Steps

1. Decision on apron overlay from NRD
2. Cost of “upgraded” apron overlay from FYRA
3. Get Cost from Contractor on Apron
4. Get Cost from Contractor on well transition
5. Coordination with NEMA/FEMA
6. Well materials 2-3 weeks out from final approval, more if stainless steel is used
7. Upgraded apron will require additional design time

FYRA ENGINEERING

OPERATION, MAINTENANCE AND, PERMANENT FLOWAGE EASEMENT
LOWER PLATTE NORTH NATURAL RESOURCES DISTRICT
WESTERN SARPY/CLEAR CREEK FLOOD REDUCTION PROJECT

In consideration of ONE DOLLAR ($1.00) and other valuable consideration received, [Name new owner] ("OWNERS" AND "TENANTS" whether one or more, hereinafter being referred to collectively as "GRANTORS") hereby grant to Lower Platte North Natural Resources District, a political subdivision of the State of Nebraska, (hereinafter referred to as "the DISTRICT") and its successors and assigns, including the UNITED STATES ARMY CORPS OF ENGINEERS (hereinafter referred to as the "CORPS"), and their successors, officers, agents, employees and contractors, a permanent and assignable operations, maintenance, flowage and saturation easement (hereinafter referred to as "the EASEMENT") in, on, under, over and across the following tract of land in Saunders County, Nebraska, to wit:

> All of Lot 49 (& 50) Thomas Lakes Subdivision, a Subdivision located in Section 18, Township 13 North, Range 10 East of the 6th P.M., as surveyed, platted and recorded in Saunders County, Nebraska,

(Hereinafter referred to collectively as "the EASEMENT AREA").

Pursuant to the EASEMENT, the DISTRICT and CORPS shall have the perpetual power, privilege right and authority to intermittently overflow, saturate and submerge the surface and sub-surface of the EASEMENT AREA with flood waters and sediment occurring as the result of the construction, operation, maintenance, repair and replacement of the levees and other works of improvement directly or indirectly comprising the CORPS' WESTERN SARPY/CLEAR CREEK FLOOD REDUCTION PROJECT (hereinafter referred to as "the PROJECT"), by whatever name called, in or on adjacent or nearby lands. The DISTRICT shall further have the right, although not the obligation, to access the property for operation and maintenance purposes relating directly or indirectly to the PROJECT.

The EASEMENT shall be subject to the following additional provisions, to-wit:

1. No structures (whether for human habitation or otherwise) shall be constructed or maintained on or in the EASEMENT AREA; and no excavations shall be conducted, nor landfill placed on or in the EASEMENT AREA

2. The consideration given for the EASEMENT shall constitute payment in full for all prior, present and/or future damages sustained by GRANTORS and their heirs, successors and assigns by reason of the exercise of any of the rights or privileges herein expressly granted or reasonably implied.

3. The EASEMENT shall be deemed to run with the land and shall be binding upon and inure to the benefit of the parties to this instrument and their heirs, successors, and assigns. The GRANTORS and their successors or assigns shall be obligated to coordinate all construction activities conducted with the EASEMENT AREA with the DISTRICT AND CORPS in order that they can determine if such activities are prohibited because they would adversely impact the levee system.

4. GRANTORS covenant and agree that OWNERS own the EASEMENT AREA and have good right to convey the EASEMENT over the same; that the EASEMENT AREA is free and clear of all liens and encumbrances except easements of record for public roads and highways, public utilities, railroads, and pipelines; and that GRANTORS will warrant and defend the DISTRICT'S title to the EASEMENT against the lawful claims and demands of all persons whomsoever.

5. TENANTS covenant and agree that their lease over the EASEMENT AREA is and shall be subordinated to the EASEMENT.

6. Any use of the EASEMENT AREA shall be subject to Federal and State laws whether with respect to pollution or otherwise.

7. The EASEMENT shall not be construed to pass to the DISTRICT a fee simple interest or title to the property.

8. Any amendments to this instrument will be subject to approval of the DISTRICT.

9. GRANTORS warrant that no verbal or written representations or inducements have been made or given by the DISTRICT, or by any of its officers, agents, or employees, other than as may be recited in this instrument.

Executed by GRANTORS on this _____ day of _____, 2022

_____
[Name]

_____
[Name]

STATE OF NEBRASKA)
) SS
COUNTY OF _____)

The foregoing instrument was acknowledged before me this _____ day of _____, 2022, by [Insert name]

_____
Notary Public

OPERATION, MAINTENANCE AND, PERMANENT FLOWAGE EASEMENT
LOWER PLATTE NORTH NATURAL RESOURCES DISTRICT
WESTERN SARPY/CLEAR CREEK FLOOD REDUCTION PROJECT

In consideration of ONE DOLLAR ($1.00) and other valuable consideration received, [Name new owner] ("OWNERS" AND "TENANTS" whether one or more, hereinafter being referred to collectively as "GRANTORS") hereby grant to Lower Platte North Natural Resources District, a political subdivision of the State of Nebraska, (hereinafter referred to as "the DISTRICT") and its successors and assigns, including the UNITED STATES ARMY CORPS OF ENGINEERS (hereinafter referred to as the "CORPS"), and their successors, officers, agents, employees and contractors, a permanent and assignable operations, maintenance, flowage and saturation easement (hereinafter referred to as "the EASEMENT") in, on, under, over and across the following tract of land in Saunders County, Nebraska, to wit:

> All of Lot (41 – 44) Thomas Lakes Subdivision, a Subdivision located in Section 18, Township 13 North, Range 10 East of the 6th P.M., as surveyed, platted and recorded in Saunders County, Nebraska,

(Hereinafter referred to collectively as "the EASEMENT AREA").

Pursuant to the EASEMENT, the DISTRICT and CORPS shall have the perpetual power, privilege right and authority to intermittently overflow, saturate and submerge the surface and sub-surface of the EASEMENT AREA with flood waters and sediment occurring as the result of the construction, operation, maintenance, repair and replacement of the levees and other works of improvement directly or indirectly comprising the CORPS' WESTERN SARPY/CLEAR CREEK FLOOD REDUCTION PROJECT (hereinafter referred to as "the PROJECT"), by whatever name called, in or on adjacent or nearby lands. The DISTRICT shall further have the right, although not the obligation, to access the property for operation and maintenance purposes relating directly or indirectly to the PROJECT.

The EASEMENT shall be subject to the following additional provisions, to-wit:

1. The only allowable structures shall be removable/mobile and maintained on or in the EASEMENT AREA; and no excavations shall be conducted, nor landfill placed on or in the EASEMENT AREA

2. The consideration given for the EASEMENT shall constitute payment in full for all prior, present and/or future damages sustained by GRANTORS and their heirs, successors and assigns by reason of the exercise of any of the rights or privileges herein expressly granted or reasonably implied.

3. The EASEMENT shall be deemed to run with the land and shall be binding upon and inure to the benefit of the parties to this instrument and their heirs, successors, and assigns. The GRANTORS and their successors or assigns shall be obligated to coordinate all construction activities conducted with the EASEMENT AREA with the DISTRICT AND CORPS in order that they can determine if such activities are prohibited because they would adversely impact the levee system.

4. GRANTORS covenant and agree that OWNERS own the EASEMENT AREA and have good right to convey the EASEMENT over the same; that the EASEMENT AREA is free and clear of all liens and encumbrances except easements of record for public roads and highways, public utilities, railroads, and pipelines; and that GRANTORS will warrant and defend the DISTRICT'S title to the EASEMENT against the lawful claims and demands of all persons whomsoever.

5. TENANTS covenant and agree that their lease over the EASEMENT AREA is and shall be subordinated to the EASEMENT.

6. Any use of the EASEMENT AREA shall be subject to Federal and State laws whether with respect to pollution or otherwise.

7. The EASEMENT shall not be construed to pass to the DISTRICT a fee simple interest or title to the property.

8. Any amendments to this instrument will be subject to approval of the DISTRICT.

9. GRANTORS warrant that no verbal or written representations or inducements have been made or given by the DISTRICT, or by any of its officers, agents, or employees, other than as may be recited in this instrument.

Executed by GRANTORS on this _____ day of _____, 2022

_____
[Name]

_____
[Name]

STATE OF NEBRASKA)
) SS
COUNTY OF _____)

The foregoing instrument was acknowledged before me this _____ day of _____, 2022, by [Insert name]

_____
Notary Public


Thomas Lakes NRD Lots
Yellow = NRD Lots
Red = approx. center line levee
Legend
Lot 41
Lot 42
Lot 44
Lot 49
Lot 50
Cedar Ln
Thomas Lk
Google Earth
© 2018 Google
N
900 ft

DECEMBER 29, 2021

REQUEST FOR BID FROM WELL DRILLERS

CLEANING AND RECONDITIONING OF RELIEF WELLS ON THE LAKE WANAHOO DAM

The Lower Platte North NRD is the owner of the Lake Wanahoo Dam located north of Wahoo, NE and built in 2010. The dam stores a 662-acre reservoir and is classified as a high hazard dam. At the toe of the downstream side of the dam there are 46 pressure relief wells of which approximately 29 flow water. Over the last few years, the trend is showing a decrease in velocities from the wells, it's likely the well are beginning to clog and need to be cleaned. Clogging can be caused by soil intrusion into the well pack, chemical deposits, or biological deposits. The amount and type of clogging will dictate the cleaning method, such as mechanical cleaning like scrubbing and pumping-and-surging or can extend to more complex cleanings using chemicals that disinfect the wells.

- ✓ We would like pressure relief wells 22A, 34, 35 cleaned and if successful wells 23, 24, 25 and 31 cleaned as well. (See attached Olsson Pressure Relief Well and Instrumentation sheet for well locations and lengths)
    - Note: Well 31 is located near the Principal Spillway and additional attention should be considered by contractor regarding site access for this location.
- ✓ Each pressure relief well including the aggregate filter packs should be cleaned and redeveloped. Cleaning should extend along the entire well length.
- ✓ The cleaning of each well should include an initial and final pump test that will be compared to the original test performed on the wells. Mechanical well cleaning may include, but not limited to, mechanical scrubbing and pumping-and-surging. See attached Olsson Relief Well Detail Sheet for details on the construction, dimensions, and materials for the relief wells. All cleaning methods should follow the guidelines listed in the EPA's Manual for Water Well Construction Practices. The cleaning process should include:
    - Testing Pumping for a minimum of 4 hours. Rate should be incrementally increase to 150 gall/min.
    - Mechanical Cleaning: Mechanical scrubbing and pumping-and- surge blocking the entire length of well. Bailing out of material from the base of the well after scrubbing and pumping/surge blocking.
    - Another Test Pumping for a minimum of 4 hours. Rate should be incrementally increase to 150 gall/min.
- ✓ Vibrating wire piezometer measurements should be taken before and after the well cleaning. To be completed by NRD consultant.

- ✓ Find included in this packet a) Pressure Relief Well Results Chart, Vibrating Wire Piezometer Monitoring Report, Individual Relief Well Velocity graphs, Olsson Pressure Relief Well and Instrumentation sheet, and Olsson Relief Well Detail Sheet.

Lower Platte North NRD is requesting a bid from qualified well drilling companies for this project. A site showing will be held on Thursday, January 20 at 11:00 am in the parking area downstream side of the dam, on the southeast side (behind John Deere) weather permitting.

Please quote a price/well for the first three wells and either extend that price for the next four or quote a new bid for the next four.

Bid Price:

Mobilization $_____

Mechanical Cleaning and Pumping Per/Well $_____
-Hours planned for mechanical cleaning _____

Total $_____

Additional Mechanical Cleaning Per/Hour (if needed) $_____

Additional Pumping Per/Hour (if needed) $_____

Please send your sealed bid to Lower Platte North NRD, PO Box 126, Wahoo, NE 68066 by 4:00 pm March 1, 2022.
If you have questions, contact Bob Heimann at 402-443-4675 or bheimann@lpnnrd.org

Sincerely,

Bob Heimann
O & M Manager


Rediscover the Outdoors
Lake Wanahoo NRD Recreation Area
permits are now available!
To purchase a permit, please visit
the NRD Office in Wahoo, or order
online at www.lpnnrd.org
LOWER PLATTE NORTH
Natural Resources District

December 20, 2021

U.S. ENVIRONMENTAL PROTECTION AGENCY-WaterISAC ADVISORY

To: Water and Wastewater Systems, SLTT Governments and Private Sector Stakeholders

(TLP:AMBER) Cybersecurity Recommendations in Consideration of the CISA/FBI/NSA Advisory on Russian State-Sponsored Cyber Operations Against U.S. Critical Infrastructure

On December 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the National Security Agency (NSA) issued a joint advisory on Russian state-sponsored cyber operations against United States critical infrastructure (see attachment for advisory AA21-350B).

What is the Purpose of the CISA/FBI/NSA Joint Advisory?

The joint advisory describes commonly observed tactics, techniques, and procedures; detection actions; incident response guidance; and mitigations. It is intended to help critical infrastructure reduce the risk presented by these threats and to encourage the adoption of a heightened state of awareness during the holidays (a time when many disconnect from work).

The joint advisory complemented a December 15, 2021 CISA Insights publication - Preparing For and Mitigating Potential Cyber Threats. It asserted that due to persistent cyber-threats from sophisticated actors, including nation-states and their proxies, critical infrastructure owners and operators should take immediate steps to strengthen their computer network defenses. These actors have the capability to leverage network access for targeted operations with the potential to disrupt critical infrastructure functions.

What Actions are Recommended for Water and Wastewater Systems?

Water and wastewater system owners and operators should review the attached joint advisory and assess how to apply the recommended detection, incident response, and mitigation actions to their operations. Key actions for water and wastewater systems include the following:

1) **Require Strong, Unique Passwords.** Malicious cyber actors repeatedly use stolen or easily guessed credentials. Consider forcing a global reset of all passwords in your environment before staff begin taking time off.
2) **Implement Multi-Factor Authentication.** After changing passwords, make implementing multi-factor authentication (MFA) a priority. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into your systems.
3) **Address known exploited vulnerabilities.** This could include patching and/or additional controls such as network segmentation to protect vulnerable devices that cannot effectively be patched. CISA maintains a catalog of Known Exploited Vulnerabilities that utilities are encouraged to review to identify vulnerable systems. Also, prioritize network segmentation to prevent unauthorized access to your operational technology (OT) systems from the internet and to reduce connectivity between OT and vulnerable information technology (IT) systems.
4) **Surge Support.** Identify surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity.

5) **Network/Systems Awareness.** Be alert for unusual behavior in OT and IT systems, such as unexpected reboots of digital controllers and other OT hardware and software, and delays or disruptions in communication with field equipment or other OT devices. Enhance logging to investigate anomalous activity – including collecting more logs and increasing storage capacity and retention time.
6) **Backup Data.** Implement and test data backup procedures on both IT and OT networks and ensure copies of backups are isolated (stored offline) from the network.
7) **Incident Response Plans.** Create, maintain, and exercise a cyber incident response and continuity of operations plans.
8) **Manual Operations.** Have a resilience plan that addresses how to operate your system if you lose access to or control of critical OT or IT systems – including the ability to sustain manual operations for extended periods.

How Can I Learn More About the CISA/FBI/NSA Joint Advisory?

WaterISAC and EPA, in conjunction with water sector associations, will hold a TLP:AMBER webinar on the dates/times listed below to present and discuss the joint advisory. The webinar is intended for water and wastewater system owners and operators, along with state, local, tribal, and territorial (SLTT) government officials and private sector organizations that directly support water and wastewater system operations. Registration links for the webinar are provided. For those unable to join live, the webinar will be recorded and posted to the WaterISAC website for members and trial members.

- Date 1: Wednesday, December 29, 2021, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/8355582904364747792
- Date 2: Wednesday, January 5, 2022, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/5595566826088940559

Additional Resources

- Protecting Against Malicious Cyber Activity before the Holidays (White House; 12/16/21)
- Joint Cybersecurity Advisory Ongoing Cyber Threats to U.S. Water and Wastewater Systems (CISA, FBI, NSA, EPA; 10/14/21)
- WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- U.S. EPA Cybersecurity Best Practices for the Water Sector
- AWWA Resources on Cybersecurity

WaterISAC Incident Reporting
WaterISAC encourages all utilities that have experienced malicious or suspicious activity to email analyst@waterisac.org, call 866-H2O-ISAC, or use the confidential online incident reporting form. Reporting to WaterISAC helps utilities and stakeholders stay aware of the threat environment of the sector.

TLP:AMBER Definition: *Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.*

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:AMBER

Product ID: A20-350B

December 16, 2021

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

SUMMARY

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

Actions critical infrastructure organizations should implement to immediately strengthen their cyber posture.

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Implement multi-factor authentication.
- Use antivirus software.
- Develop internal contact lists and surge support.

1. **Be prepared**. Confirm reporting processes and minimize personnel gaps in IT/IO security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.

2. **Enhance your organization's cyber posture**. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. **Increase organizational vigilance**. Stay current on reporting on this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

CISA, the FBI, and NSA encourage critical infrastructure organization leaders to review CISA Insights: Preparing for and Mitigating Cyber Threats for information on reducing cyber threats to their organization.

TECHNICAL DETAILS

Note: this advisory uses the MITRE ATT&CK® for Enterprise framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks. Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials.

In some cases, Russian state-sponsored cyber operations against critical infrastructure organizations have specifically targeted operational technology (OT)/industrial control systems (ICS) networks with

destructive malware. See the following advisories and alerts for information on historical Russian state-sponsored cyber-intrusion campaigns and customized malware that have targeted ICS:

- ICS Advisory ICS Focused Malware – Havex
- ICS Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
- ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure
- Technical Alert CrashOverride Malware
- CISA MAR HatMan: Safety System Targeted Malware (Update B)
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)

Russian state-sponsored APT actors have used sophisticated cyber capabilities to target a variety of U.S. and international critical infrastructure organizations, including those in the Defense Industrial Base as well as the Healthcare and Public Health, Energy, Telecommunications, and Government Facilities Sectors. High-profile cyber activity publicly attributed to Russian state-sponsored APT actors by U.S. government reporting and legal actions includes:

- **Russian state-sponsored APT actors targeting state, local, tribal, and territorial (SLTT) governments and aviation networks, September 2020, through at least December 2020.** Russian state-sponsored APT actors targeted dozens of SLTT government and aviation networks. The actors successfully compromised networks and exfiltrated data from multiple victims.
- **Russian state-sponsored APT actors' global Energy Sector intrusion campaign, 2011 to 2018.** Russian state-sponsored APT actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
- **The Russian General Staff Main Intelligence Directorate's (GRU's) Main Center of Special Technologies (GTsST) campaign against Ukrainian critical infrastructure, 2015 and 2016.** GTsST or Unit 74455 has previously been attributed as Sandworm Team by Mandiant, VOODOO BEAR by CrowdStrike, and ELECTRUM by Dragos. GTsST actors conducted a cyberattack against Ukrainian energy distribution companies, leading to multiple companies experiencing unplanned power outages in December 2015. The actors deployed BlackEnergy malware to steal user credentials and used its destructive malware component, KillDisk, to make infected computers inoperable. In 2016, GTsST actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware specifically designed to attack power grids.

For more information on recent and historical Russian state-sponsored malicious cyber activity, see the referenced products below or the CISA webpage cisa.gov/Russia.

- Joint FBI-DHS-CISA CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint NSA-FBI-CISA CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
- Joint FBI-CISA CSA Russian APT Actors Compromise U.S. Government Targets

- Joint CISA-FBI CSA APT Actors Chaining Vulnerabilities against SLTT, Critical Infrastructure, and Elections Organizations
- CISA's webpage Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- CISA Alert Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors
- CISA ICS: Alert Cyber-Attack Against Ukrainian Critical Infrastructure

Table 1 provides common, publicly known TTPs employed by Russian state-sponsored APT actors, which map to the MITRE ATT&CK for Enterprise framework, version 10. **Note**: these lists are not intended to be all inclusive. Russian state-sponsored actors have modified their TTPs before based on public reporting.[1] Therefore, CISA, the FBI, and NSA anticipate the Russian state-sponsored actors may modify their TTPs as they deem necessary to reduce their risk of detection.

Table 1: Common Tactics and Techniques Employed by Russian State-Sponsored APT Actors

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used `cmd.exe` to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.

Tactic	Technique	Procedure
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database `ntds.dit`.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed "Kerberoasting," whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

For additional enterprise TTPs used by Russian state-sponsored APT actors, see the ATT&CK for Enterprise pages on APT29, APT28, and the Sandworm Team, respectively. For information on ICS TTPs see the ATT&CK for ICS pages on the Sandworm Team, BlackEnergy malware, CrashOveride malware, BlackEnergy's KillDisk component, and NotPetya malware.

DETECTION

Given Russian state-sponsored APT actors demonstrated capability to maintain persistent, long-term access in compromised enterprise and cloud environments, CISA, the FBI, and NSA encourage all critical infrastructure organizations to:

- **Implement robust log collection and retention.** Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior described in this advisory. Depending on the environment, examples include:
    - Native tools such as M365's Sentinel.
    - Third-party tools, such as Sparrow, Hawk, or CrowdStrike's Azure Reporting Tool (CRT), to review Microsoft cloud environments and to detect unusual activity, service principals, and application activity. **Note**: for guidance on using these and other detection tools, refer to CISA Alert Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.
- **Look for behavioral evidence or network and host-based artifacts** from known Russian state-sponsored TTPs. See table 1 for commonly observed TTPs.
    - To detect password spray activity, review authentication logs for system and application login failures of valid accounts. Look for multiple, failed authentication attempts across multiple accounts.
    - To detect use of compromised credentials in combination with a VPS, follow the below steps:
        - Look for suspicious "impossible logins," such as logins with changing username, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user's geographic location.
        - Look for one IP used for multiple accounts, excluding expected logins.
        - Look for "impossible travel." Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins). **Note**: implementing this detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting into networks.
        - Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the `ntds.dit` file from a domain controller.
        - Look for suspicious privileged account use after resetting passwords or applying user account mitigations.
        - Look for unusual activity in typically dormant accounts.
        - Look for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity.

- For organizations with OT/ICS systems:
    - Take note of unexpected equipment behavior; for example, unexpected reboots of digital controllers and other OT hardware and software.
    - Record delays or disruptions in communication with field equipment or other OT devices. Determine if system parts or components are lagging or unresponsive.

INCIDENT RESPONSE

Organizations detecting potential APT activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
3. Collect and review relevant logs, data, and artifacts.
4. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
5. Report incidents to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Note: for OT assets, organizations should have a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment. Refer to the Mitigations section for more information.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA, the FBI, and NSA encourage critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch (FCEB) agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

Note: organizations should document incident response procedures in a cyber incident response plan, which organizations should create and exercise (as noted in the Mitigations section).

MITIGATIONS

CISA, the FBI, and NSA encourage all organizations to implement the following recommendations to increase their cyber resilience against this threat.

Be Prepared

Confirm Reporting Processes and Minimize Coverage Gaps

- Develop internal contact lists. Assign main points of contact for a suspected incident as well as roles and responsibilities and ensure personnel know how and when to report an incident.
- Minimize gaps in IT/OT security personnel availability by identifying surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity—critical infrastructure organizations should proactively protect themselves by minimizing gaps in coverage.
- Ensure IT/OT security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any identified IOCs and TTPs for immediate response. (See table 1 for commonly observed TTPs).

Create, Maintain, and Exercise a Cyber Incident Response, Resilience Plan, and Continuity of Operations Plan

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
- Ensure personnel are familiar with the key steps they need to take during an incident and are positioned to act in a calm and unified manner. Key questions:
    - Do personnel have the access they need?
    - Do they know the processes?
- For OT assets/networks,
    - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
        - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
    - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
    - Implement data backup procedures on both the IT and OT networks. Backup procedures should be conducted on a frequent, regular basis. Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.

- In addition to backing up data, develop recovery documents that include configuration settings for common devices and critical OT equipment. This can enable more efficient recovery following an incident.

Enhance your Organization's Cyber Posture

CISA, the FBI, and NSA recommend organizations apply the best practices below for identity and access management, protective controls and architecture, and vulnerability and configuration management.

Identity and Access Management

- Require multi-factor authentication for all users, without exception.
- Require accounts to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access.
- Secure credentials. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
  - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
  - Disable the storage of clear text passwords in LSASS memory.
  - Consider disabling or limiting New Technology Local Area Network Manager (NTLM) and WDigest Authentication.
  - Implement Credential Guard for Windows 10 and Server 2016 (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - Minimize the AD attack surface to reduce malicious ticket-granting activity. Malicious activity such as "Kerberoasting" takes advantage of Kerberos' TGS and can be used to obtain hashed credentials that attackers attempt to crack.
- Set a strong password policy for service accounts.
- Audit Domain Controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
  - Secure accounts.
  - Enforce the principle of least privilege. Administrator accounts should have the minimum permission they need to do their tasks.
  - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
  - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).

Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor or malware. Use network monitoring tools and host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly

useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

- Enable strong spam filters.
    - Enable strong spam filters to prevent phishing emails from reaching end users.
    - Filter emails containing executable files to prevent them from reaching end users.
    - Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.

Note: CISA, the FBI, and NSA also recommend, as a longer-term effort, that critical infrastructure organizations implement network segmentation to separate network segments based on role and functionality. Network segmentation can help prevent lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by taking into account criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

Vulnerability and Configuration Management

- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Prioritize patching known exploited vulnerabilities, especially those CVEs identified in this CSA, and then critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
    - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
    - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.
- Use industry recommended antivirus programs.
    - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
    - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.

- Disable all unnecessary ports and protocols
  - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control (C2) activity.
  - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Ensure OT hardware is in read-only mode.

Increase Organizational Vigilance

- Regularly review reporting on this threat. Consider signing up for CISA notifications to receive timely information on current security issues, vulnerabilities, and high-impact activity.

RESOURCES

- For more information on Russian state-sponsored malicious cyber activity, refer to cisa.gov/Russia.
- Refer to CISA Analysis Report Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services for steps for guidance on strengthening your organizations cloud security practices.
- Leaders of small businesses and small and local government agencies should see CISA's Cyber Essentials for guidance on developing an actionable understanding of implementing organizational cybersecurity practices.
- Critical infrastructure owners and operators with OT/ICS networks, should review the following resources for additional information:
  - NSA and CISA joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
  - CISA factsheet Rising Ransomware Threat to Operational Technology Assets for additional recommendations.

REWARDS FOR JUSTICE PROGRAM

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's Rewards for Justice Program. You may be eligible for a reward of up to $10 million, which DOS is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact +1-202-702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details refer to rewardsforjustice.net/malicious_cyber_activity.

CAVEATS

The information you have accessed or received is being provided “as is” for informational purposes only. CISA, the FBI, and NSA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, the FBI, or NSA.

REFERENCES

[1] Joint NCSC-CISA UK Advisory: Further TTPs Associated with SVR Cyber Actors
https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors