Administrative Report
May 18, 2023

COLLECTIONS

Collections have gone really well. Letters were sent out after statements letting people know they were either on the shut off-list (owing more than just 2022 Power), or on a future shut-off list (owing only 2022 Power). Most folks responded to these notices. Those who were shut-off and tagged out paid $25 fee. Current breakdown:

AGING:	DESCRIPTION:	AMOUNT:
Current	(2nd Half)	$427,096.10
1-30 Days	(Misc. Fees) Title $60 NSF Fee $15 Transfer Fees $140.60 Filters (Lat. 15) $354.91	$ 570.51
31-60 Days	(1st Half)	$112,842.43
61-90 Days	(2022 Power)	$ 12,078.75
Over 90 Days	(2022-pre)	$ 27,061.22
Open Credits		<$ 3617.73>
TOTAL DUE 5/16/23		**$ 580,072.65**

Historical A/R Balance	12/31/22	$ 186,478.85	(2022 Power)
	1/31/23	$ 154,479.69	
	2/28/23	$1,435,165.97	(2023 Assmt)
	3/31/23	$ 891,714,49	
	4/30/23	$ 604,098.51	

A few Intent to Foreclose notices went out (those back into bank ownership) and they have all responded with confirmation of payments before the end of this month. More will go out after I get the meter postcards out, hopefully next week.

ASSESSMENTS

There are still a few 2023 Assessments to go out. I am waiting on transfer acreages from the mapper.

METERS

Meter readings have started to come in. Notices will go out with meter postcards that effective June 1, if WEID has to read the meters there will be a $25 charge. The ones we will be targeting first are the subdivisions in Boardman (whose power bills are based upon usage) and the larger water users.

CYBERSECURITY

Wow, this is becoming a hot topic lately!! Fortunately, I have been accepted into a mentorship through the Multi-State Information Sharing and Analysis Center (MS-ISAC). This involves a 1-hour meeting once a month for the next year, or more as needed. Meetings are held remotely in Microsoft Teams. MS-ISAC exists for the benefit of agencies in the public sector (government and special districts) nationwide, and I first heard of them from SDAO. In this year's program, there are 293 mentees. There are 1-2 mentees per mentor this year. They try to match mentors with mentees near to their geographic location and in similar agencies. My mentor is the Cybersecurity Analyst for Clean Water Services (Hillsboro), and originally went through the program as a mentee for 2 years. He is a veteran of the Air Force and has basically worked in cybersecurity his whole career.

At first, I wondered what I had gotten myself into. There is another mentee with us. She just graduated from WSU with a degree in cybersecurity and has been doing an internship with a large school district in Washington. However, my mentor said that this was exactly where I needed to be; not only could I gain the knowledge I need to benefit WEID, but the other mentee would learn about setting up policies and procedures from the ground up, as her next job might be with an agency like ours, that has very little in place. I submitted a list of questions/issues that I was hoping to learn about this year. My questions and his answers (which formed the outline for our meeting earlier this month) are attached.

He said that smaller districts were potentially a more desirable target than larger ones, as the protocols and procedures in place tend to be more lax. One scenario is not that our server is hacked, but that our emails are hacked/emulated, and an infected email that looks like it has come from WEID is sent to a larger agency, who then clicks on the attachment and infects their computers. For example, emails with attachments are regularly sent between myself and the clerk's office.

CURRENT NEWS: Curry County OR was hit with ransomware in April from a Russian hacker known as "Royal." They first noticed problems on April 26. See attached news release. My mentor heard about the attack and let us know. I heard the breach most likely occurred on a machine that was not fully updated; it probably was brought onto their servers through an email with a link, that when clicked on loaded the ransomware onto the computer which then migrated to their server. As part of the process, their Microsoft 365 account(s) were also infected, and data and documents were either deleted or corrupted. This is especially painful for them, as about 2 years ago they digitized all their historical data. I am not sure what they did with the originals? We have talked about doing this with our historical records, but our plan is to send the originals to the State Archives, where they are still accessible, just not immediately (takes a week or 2).

My mentor has said that if copies of their response and recovery report become public, he can share his 2 cents; if they are not made public then he can't. I have asked for his opinion on what could have gone wrong and what WEID should do to prevent a similar attack. I expect to see his recommendations at some point, but he also has a full-time job besides the work he does for MS-ISAC. He is also working on a redacted version of his agency's policies and procedures for us to see.

With so many devices now attached to our network (4 computers, 10 smartphones, and 5 tablets) the potential for problems is only growing. I feel really fortunate to be a part of this program and what it will mean for WEID.