Compliance Maintenance Annual Report

Heart Of The Valley Metro Sewerage District

Last Updated: 6/12/2019 Reporting For: **2018**

DNR Response to Resolution or Owner's Statement

Name of Governing Body or Owner: Heart of the Valley Metropolitan Sewerage District

Date of Resolution or Action Taken: 2019-06-11

Resolution Number: 184

Date of Submittal: 6/12/2019

ACTIONS SET FORTH BY THE GOVERNING BODY OR OWNER RELATING TO SPECIFIC CMAR SECTIONS (Optional for grade A or B. Required for grade C, D, or F):

Influent Flow and Loadings: Grade = A

Permittee Response:

DNR Response:

Effluent Quality: BOD: Grade = A

Permittee Response:

DNR Response:

Good effluent BOD quality.

Effluent Quality: TSS: Grade = A

Permittee Response:

DNR Response:

Effluent TSS levels are below current limits.

Effluent Quality: Ammonia: Grade = A

Permittee Response:

DNR Response:

Good effluent Ammonia quality.

Effluent Quality: Phosphorus: Grade = A

Permittee Response:

DNR Response:

Effluent phosphorus levels are below current limits.

Biosolids Quality and Management: Grade = A

Permittee Response:

DNR Response:

Biosolids metal quality values are below the high quality limits.

Staffing: Grade = A

Compliance Maintenance Annual Report

Heart Of The Valley Metro Sewerage District

Last Updated: 6/12/2019 Reporting For: **2018**

Permittee Response:

DNR Response:

It appears that the preventative maintenance program is well managed.

Operator Certification: Grade = A

Permittee Response:

DNR Response:

Financial Management: Grade = A

Permittee Response:

DNR Response:

The equipment replacement fund has a good ending balance and the energy efficiency practices are strong.

Collection Systems: Grade = A

(Regardless of grade, response required for Collection Systems if SSOs were reported)

Permittee Response:

DNR Response:

The Department recognizes your efforts in controlling I/I in the sanitary sewer collection system. Please continue to address the issues.

ACTIONS SET FORTH BY THE GOVERNING BODY OR OWNER RELATING TO THE OVERALL GRADE POINT AVERAGE AND ANY GENERAL COMMENTS

(Optional for G.P.A. greater than or equal to 3.00, required for G.P.A. less than 3.00)

G.P.A. = 4

Permittee Response:

DNR G.P.A. Response:

The facilities appear to be well maintained and operated efficiently.

DNR CMAR Overall Response:

Thank you for submitting the Compliance Maintenance Annual Report (CMAR) in a timely manner. The report's G.P.A. shows the dedication of everyone involved in the management and maintenance of the WWTF and the sanitary sewer collection system.

DNR Reviewer: Van Gheem, Roy **Phone:** (920) 662-5191

Address: 2984 Shawano Avenue, Green Bay, WI 54313-6727 **Date:** 6/17/2019

FORT LAUDERDALE, Fla. (AP) —
A Florida city agreed to pay $600,000 in ransom to hackers who took over its computer system, the latest in thousands of attacks worldwide aimed at extorting money from governments and businesses.
The Riviera Beach City Council voted unanimously this week to pay the hackers' demands, believing the Palm Beach suburb had no choice if it wanted to retrieve its records, which the hackers encrypted. The council already voted to spend almost $1 million on new computers and hardware after hackers captured the city's system three weeks ago.
The hackers apparently got into the city's system when an employee clicked on an email link that allowed them to upload malware. Along with the encrypted records, the city had numerous problems including a disabled email system, employees and vendors being paid by check rather than direct deposit and 911 dispatchers being unable to enter calls into the computer. The city says there was no delay in response time.

Spokeswoman Rose Anne Brown said Wednesday that the city of 35,000 residents has been working with outside security consultants, who recommended the ransom be paid. She conceded there are no guarantees that once the hackers received the money they will release the records. The payment is being covered by insurance. The FBI on its website says it "doesn't support" paying off hackers, but Riviera Beach isn't alone: many government agencies and businesses do.
"We are relying on their (the consultants') advice," she said. The hackers demanded payment in the cryptocurrency bitcoin. While it is possible to trace bitcoins as they are spent, the owners of the accounts aren't necessarily known, making it a favored payment method in ransomware attacks.
Numerous governments and businesses have been hit in the United States and worldwide in recent years. Baltimore refused to pay hackers $76,000 after an attack last month. The U.S. government indicted two Iranians last year for allegedly unleashing more than 200 ransomware attacks, including against the cities of Atlanta and Newark, New Jersey. The men, who have not been arrested, received more than $6 million in payments and caused $30 million in damage to computer systems, federal prosecutors have said.
The federal government last year also accused a North Korean programmer of committing the "WannaCry" attack that infected government, bank, factory and hospital computers in 150 countries. He is also believed to have stolen $81 million from a Bangladesh bank. He also remains in his home country.
The FBI had no comment Wednesday on the Riviera Beach attack, but said 1,493 ransomware attacks were reported last year with victims paying $3.6 million to hackers — about $2,400 per attack. Some of those were against individuals.
Tom Holt, a Michigan State University criminal justice professor, said hackers often attack common and known vulnerabilities in computer systems. He said organizations' technology managers need to examine their systems for such flaws and teach their employees not to open suspicious email or click suspect links. The FBI says businesses also need to back up their data regularly on secure computers.
Holt said most attacks originate outside the U.S., making them difficult to police. He said many victims wind up like Riviera Beach: They pay their attacker because it is likely the only way to retrieve lost data.
"They might not pay the initial ransom that was suggested, but they may work with a third-party provider to negotiate the ransom down," Holt said.
He said in almost all cases, the attackers decrypt the computers after payment, allowing the victims to retrieve their data. He said the WannaCry attacks were an exception — the hackers took the money but often didn't release the data. Some private WannaCry decryption attempts were successful.

Kevin Skogman
Director of Operations and Maintenance
Heart of the Valley Metro. Sew. Dist.
Email: kevin.skogman@hvmsd.org
PH: 920-766-5731