ONWASA

MEDIA RELEASE

FOR RELEASE: **Monday, October 15, 2018, 7:30am**
CONTACT: **Jeffrey Hudson, CEO**
910-455-0722 (*CURRENTLY ONLY METHOD*)

CYBER-CRIMINALS TARGET CRITICAL UTILITY IN HURRICANE-RAVAGED AREA

In the wake of the Hurricane Florence disaster, ONWASA, a critical water utility has been specifically targeted by cyber-criminals. ONWASA's internal computer system, including servers and personal computers have been subjected to a sophisticated ransomware attack that has left the utility with limited computer capabilities. Customer information was not compromised in the attack. However, many other databases must be recreated in their entirety. The utility is coordinating with the Federal Bureau of Investigation, the Department of Homeland Security, the State of North Carolina, and a several technology security companies.

The safety of the public's water supply and the area's environment is not in danger. The crisis is technological in nature.

On October 4th ONWASA began experiencing persistent virus attacks from a virus known as EMOTET, a polymorphic malware. The virus was initially thought to be under control, but when it persisted ONWASA brought in outside security specialists. The specialist continued to work the problem with ONWASA Information Technology (IT) staff. At what may have been a timed event, the malware launched a sophisticated virus known as RYUK at approximately 3am on Saturday, October 13th.

An ONWASA IT staff member was working at 3am and saw the attack. IT staff took immediate action to protect system resources by disconnecting ONWASA from the internet, but the crypto-virus spread quickly along the network encrypting databases and files. The attack is similar in nature to those experienced by Atlanta, Georgia and Mecklenburg County, North Carolina. Information on the Mecklenburg attack may be found at: jhttps://www.nbcnews.com/news/us-news/north-carolina-officials-refuse-pay-ransomware-hackers-following-expert-advice-n827481

ONWASA had multiple layers of computer protection in place, including firewalls and malware/anti-virus software. The defenses of the computer systems at the main office were penetrated. ONWASA has received one email from the cyber-criminals, who may be based in a foreign country. The email is consistent with ransomware attacks of other governments and corporations. Ransom monies would be used to fund criminal, and perhaps terrorist activities in other countries. Furthermore, there is no expectation that payment of a ransom would forestall repeat attacks. ONWASA will not negotiate with criminals nor bow to their demands. The FBI agrees that ransoms should not be paid. ONWASA will undertake the painstaking process of rebuilding its databases and computer systems from the ground up.

The lack of computing ability will affect the timeliness of service from ONWASA for several weeks to come. Initially, the utility will operate manually at all plant and office locations. Water and wastewater service to homes and businesses will not be interrupted. Customers may continue to make credit card payments by phone, at ONWASA's kiosk locations (by check, cash, or credit card), and in person at the main office at 228 Georgetown Road, Jacksonville. Satellite Offices in Holly Ridge, Swansboro, and Richlands have the capability of processing credit card payments by phone and very limited other services. Service orders, account creation, connections, disconnections, development review, backflow program, engineering, and human resources will utilize manual processes until the computer systems are restored. While phone service remains, email service has been interrupted for most of the utility.

A team of local, state, and federal agencies are cooperating to restore the utility and bring the criminals to justice.

###