WATER RESOURCES INCIDENT – APRIL 12, 2023

On Wednesday, April 12, 2023, in the early morning hours (approximately 4am) CrowdStrike® Falcon services began noticing possible nefarious script and command-line activity on a critical water resource server. CrowdStrike® Falcon is an endpoint cybersecurity product installed on all servers and workstations touching the County's network by ADP.

Shortly before 8am, ADP staff began receiving a series of serious high priority alerts through ADP's cyber-security center from CrowdStrike® indicating what appeared to be a significant and persistent threat attack on this Water Resource server.

CrowdStrike® observed, what appeared to be nefarious activity, attempting to access and control the server. Given the persistent nature of the attack, CrowdStrike® elevated the incident to "Critical", automatically blocked its execution, isolated the server's communication, and put in motion a series of procedures and instructions for ADP to further isolate and protect the County's network infrastructure.

ADP personnel immediately notified Water Resources of the attack, blocked all inbound Water Resource domain traffic, removed Water Resources from all shared ISP switches, and began a deep scan of all County systems to ensure that the County's environment, under ADP control, was secure and unaffected.

It appears that the Water Resource server in question is an end of life/end of support server operating Microsoft Exchange for Water Resources which was not properly service patched by Water Resources. This vulnerability likely permitted the exploitation of an outside actor to externally penetrate the server through Exchange and attempt to run a series of tasks or commands through PowerShell scripting. The server was ultimately powered off by Water Resource staff preventing any further analysis by ADP or CrowdStrike®.

As of now, there is no indication that the attack bridged beyond Water Resources and they remain off-line awaiting remediation. CrowdStrike® and ADP were successful in containing the attack with no disruption to other County services or systems under ADP control.

Due to the fact that the penetrated server was not under the control or oversight of ADP, an emergency meeting of the ADP Board was called for Thursday, April 13, 2023 at noon in the Real Estate Appraisal conference room in the Courthouse Annex to discuss the issue.