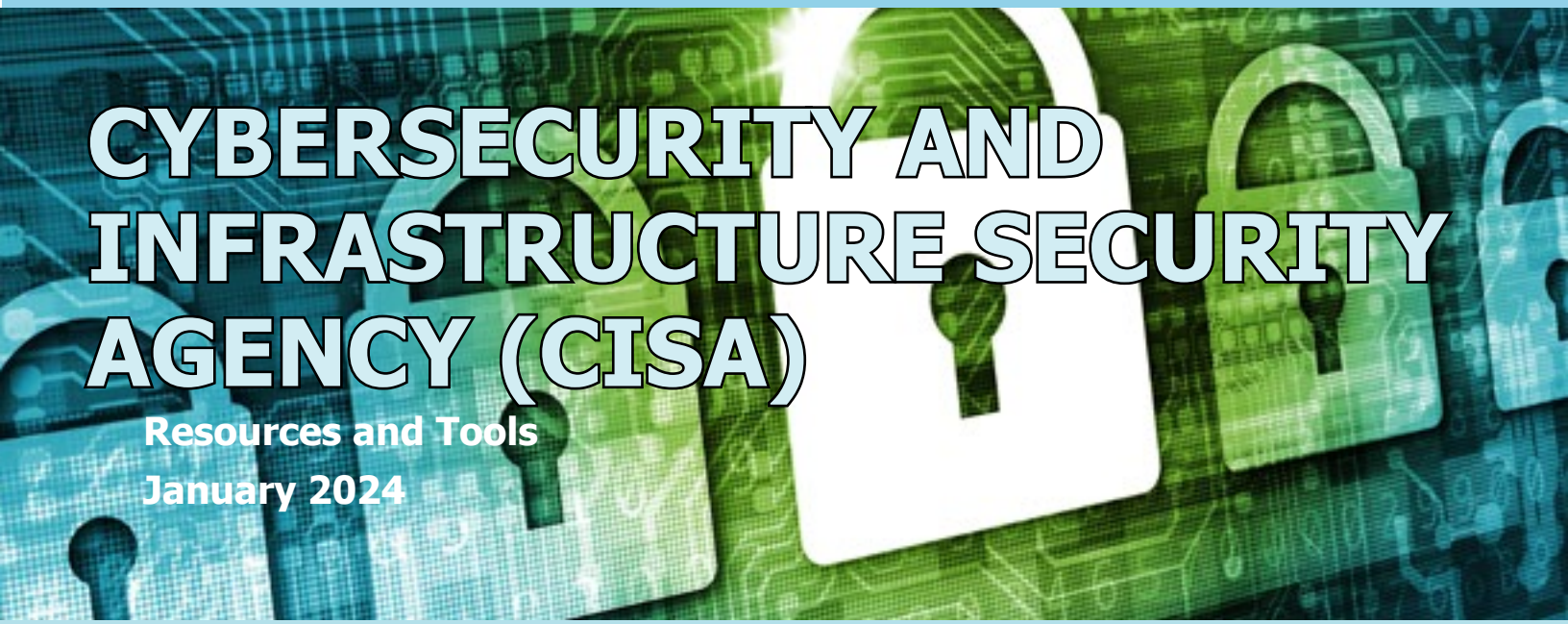
SPLASH Alert

ACWA JPIA Risk Management and Member Services Departments



CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

Resources and Tools

January 2024

In January 2024, CISA released two important publications that water and wastewater agencies may find beneficial.

Cybersecurity is a growing and evolving risk impacting the public sector, including water districts. Assisting our members with enhancing security and the ability of water systems to prevent, prepare for, respond to, and recover from cyber threats is key to maintaining a reliable and critical infrastructure. The **JPIA's Risk Management Department** monitors and shares cyber security and other water/wastewater security resources under *Section 26* on our *Risk Control Manual webpage*. Best management practices resources on unmanned aerial devices can be viewed and downloaded on our *Commitment to Excellence (C2E) Program webpage.*

Cyber Liability coverage is an essential component of the JPIA's risk management strategy. In Fall 2023, the **JPIA's Member Services Department** announced the complementary cybersecurity services of KYND and KnowBe4 for members participating in the JPIA's Liability Program. The implementation of KYND and KnowBe4 services will result in our member's reduced cyber vulnerabilities through regular monitoring of member domains and education and training in identifying attempted phishing attacks.

New CISA Resources

Cyber Incident Response Guide for the Water and Wastewater Sector – January 18, 2024. This guide was developed through a collaborative contribution from more than 25 Water and Wastewater sector organizations and co-sealed by CISA, FBI, and EPA. The guide outlines how water utility owners and operators can expect to work with federal partners as they prepare for, respond to, and mitigate the impact of a cyber incident.

Cybersecurity Guidance: Chinese-Manufactured UAS – January 17, 2024. This is a Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) resource that raises awareness of the threats posed by Chinese-manufactured Unmanned Aircraft Systems (UAS) and provides UAS cybersecurity recommendations that reduce risks to networks and sensitive information.

This guidance also provides additional resources to augment an organization's preparedness, response, and resilience.

The safe and secure integration of UAS or drones, into the national airspace system and across critical infrastructure organizations is essential to maintain the security and resilience of our national critical functions.

Additional Resources

CISA Resources and Tools webpage

CISA Be Air Aware webpage

JPIA Risk Control Manual Water/Wastewater Security webpage (see Section 26)

JPIA Commitment to Excellence Program Unmanned Aerial Devices (scroll down to Infrastructure, then Unmanned Aerial Devices)

JPIA Member Services Cybersecurity Resources webpage

JPIA Five: Expanding Cyber Resilience with KnowBe4 and KYND podcast