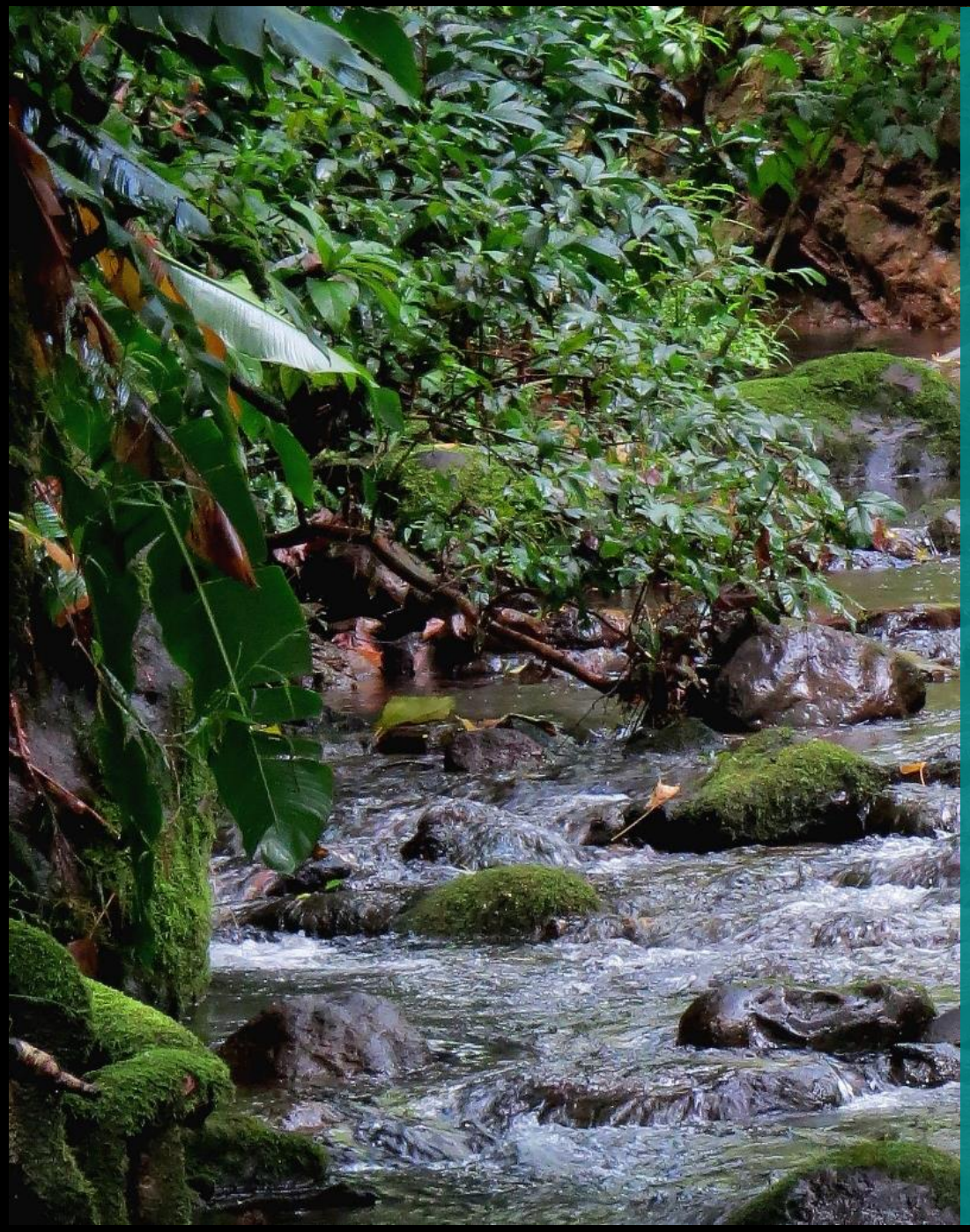


CYBERSECURITY TRENDS AND MITIGATIONS FOR THE WATER SECTOR

October 15, 2025

AGENDA

- Water sector attack trends
- Honolulu Board of Water Supply (BWS) attack trends
- Mitigations
- Cyber services

NATION STATE ACTORS

- Chinese State Sponsored Activities
  - Prepositioning access for later
  - Volt Typhoon water compromises
    - Hawaii
    - Massachusetts
    - Likely more undisclosed
  - Uses zero days and known vulnerabilities, default/weak passwords
  - Other Typhoon actors use different tactics

Star Advertiser

Monday, October 13, 2025 84° Today's Paper

Chinese hackers targeting assets in Hawaii

By Peter Boylan

Dec. 17, 2023

A water utility and other government and private assets in Hawaii have been targeted this year by hackers working for China's People's Liberation Army who are looking for ways to undermine U.S. military capabilities in the Asia-Pacific.

HTTPS://WWW.CISA.GOV/TOPICS/CYBER-THREATS-AND-ADVISORIES/NATION-STATE-CYBER-ACTORS/CHINA

HACKTIVISTS

- Cyber Av3ngers initially portrayed themselves as hacktivists
  - Really affiliated with Iran's Islamic Revolutionary Guard Corps
  - Targeting of Israeli hardware
  - supplanted existing ladder logic files with their own, renamed devices likely to forestall owner access, reset software versions to older versions, disabled upload and download functions, and changed the default port numbers[1]
- TwoNet (pro-Russian) attacked a water treatment honeypot
  - Observed defacement, process disruption, manipulation, and evasion

[1] HTTPS://WWW.CISA.GOV/NEWS-EVENTS/CYBERSECURITY-ADVISORIES/AA23-335A

CYBERCRIMINALS

- Typically motivated by money
  - Loss of operations, personal information, sensitive data, etc.
- Recent notable examples
  - Veolia North America
    - Billing system degradation and theft of personal information
  - Southern Water (UK)
    - Theft of personal information, corporate/HR information, customer information
  - American Water
    - Billing/customer account systems offline for 7 days

BWS OBSERVATIONS

- Identity (attacker in the middle)
- Phishing
- Third party compromise

MITIGATIONS

- Multi-factor authentication
- User training
- Understanding your vendors and their access
- Patch systems
  - Recent Cisco ASA zero-day attacks[1]
  - Requires you understand what you have
- Ensure logging is enabled and centralized
- Take advantage of the following services

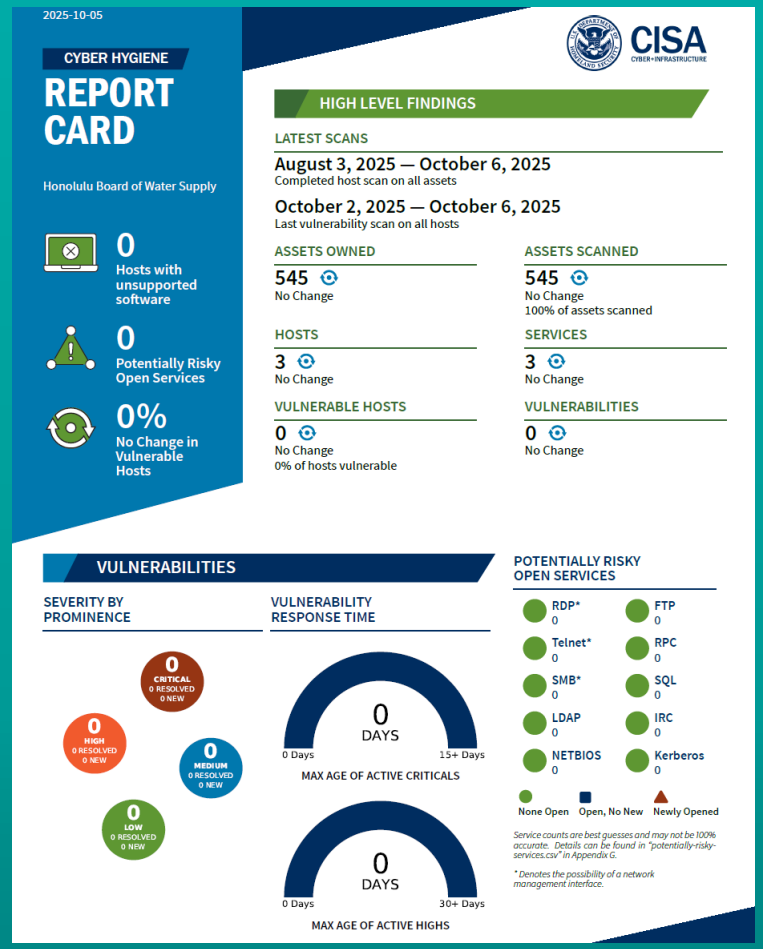
[1] HTTPS://WWW.CISA.GOV/NEWS-EVENTS/DIRECTIVES/ED-25-03-IDENTIFY-AND-MITIGATE-POTENTIAL-COMPROMISE-CISCO-DEVICES

CYBER SERVICES – FEDERAL

- Cybersecurity and Infrastructure Security Agency (CISA)
  - Federal agency that is the National Coordinator for Critical Infrastructure Security and Resilience. CISA works with partners at every level to identify and manage risk to the cyber and physical infrastructure
- Offers both Cyber and Physical services (free!)

CISA SERVICES EXAMPLES

- Cyber Hygiene
  - Web Application Scanning
- Cyber Assessments/Hunts
- Known Exploited Vulnerabilities Catalog
- Tabletop Exercises
- Frameworks
  - Cross-Sector Cybersecurity Performance Goals



2025-10-05

CYBER HYGIENE

REPORT CARD

Honolulu Board of Water Supply

CISA CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

August 3, 2025 — October 6, 2025
Completed host scan on all assets

October 2, 2025 — October 6, 2025
Last vulnerability scan on all hosts

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

ASSETS OWNED
545
No Change

ASSETS SCANNED
545
No Change
100% of assets scanned

HOSTS
3
No Change

SERVICES
3
No Change

VULNERABLE HOSTS
0
No Change
0% of hosts vulnerable

VULNERABILITIES
0
No Change

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW
0 HIGH 0 RESOLVED 0 NEW
0 MEDIUM 0 RESOLVED 0 NEW
0 LOW 0 RESOLVED 0 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days — 15+ Days
MAX AGE OF ACTIVE CRITICALS

0 DAYS
0 Days — 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0
FTP 0
Telnet* 0
RPC 0
SMB* 0
SQL 0
LDAP 0
IRC 0
NETBIOS 0
Kerberos 0

None Open · Open, No New · Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

CYBER SERVICES – FEDERAL

- Environmental Protection Agency (EPA)
- Sanitary surveys don't require comprehensive cyber evaluations
  - March 2023 Cybersecurity Rule
  - Free cybersecurity evaluation
- H.R. 2594 - To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector
  - Requires cyber assessments by WRRO/third party not less frequently than every 5yrs
  - Requirements no later than 270 days after establishment

CYBER SERVICES – FEDERAL

- Federal Bureau of Investigation (FBI)
  - Honolulu Field Office

SERVICES – ORGANIZATIONS

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Offers managed services and intelligence reports
- Federal funding not renewed presumably in favor of CISA

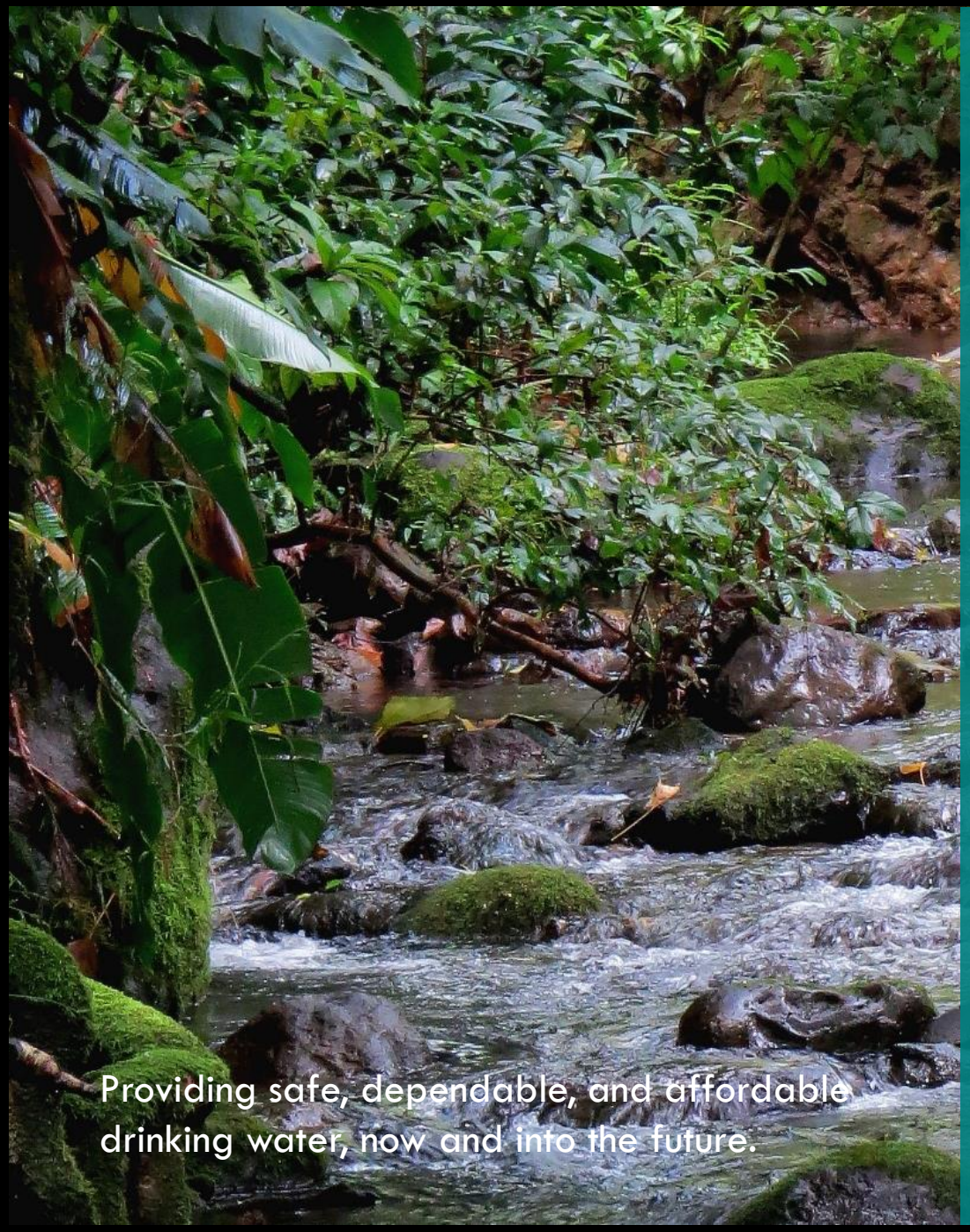
MS-ISAC®

SERVICES – ORGANIZATIONS

- Water Information Sharing and Analysis Center (Water-ISAC)
- Focused on intelligence instead of services
  - Cyber
  - Physical
  - Terrorism

SERVICES – ORGANIZATIONS

- American Water Works Association (AWWA)
- Provides tools, professional development, intelligence and other reports and publications
  - Specific to cyber - Water Sector Cybersecurity Risk Management Guidance Version 4.0



Mahalo!

Scott Wong
Honolulu Board of Water Supply
Information Technology Division
Cybersecurity Office
swong3@hbws.org