Engineering, Operations, & Technology Committee

Cyber Threat Briefing

Item 6c

December 8, 2025

Presented by: Jake Margolis

Item 6c

Cybersecurity Quarterly Update

Subject

Cyber Threat Briefing for the Engineering Operations and Technology Committee

Purpose

Provide the Board and key Metropolitan leaders with current information on cyber risks, and Metropolitan defensive actions

Next Steps

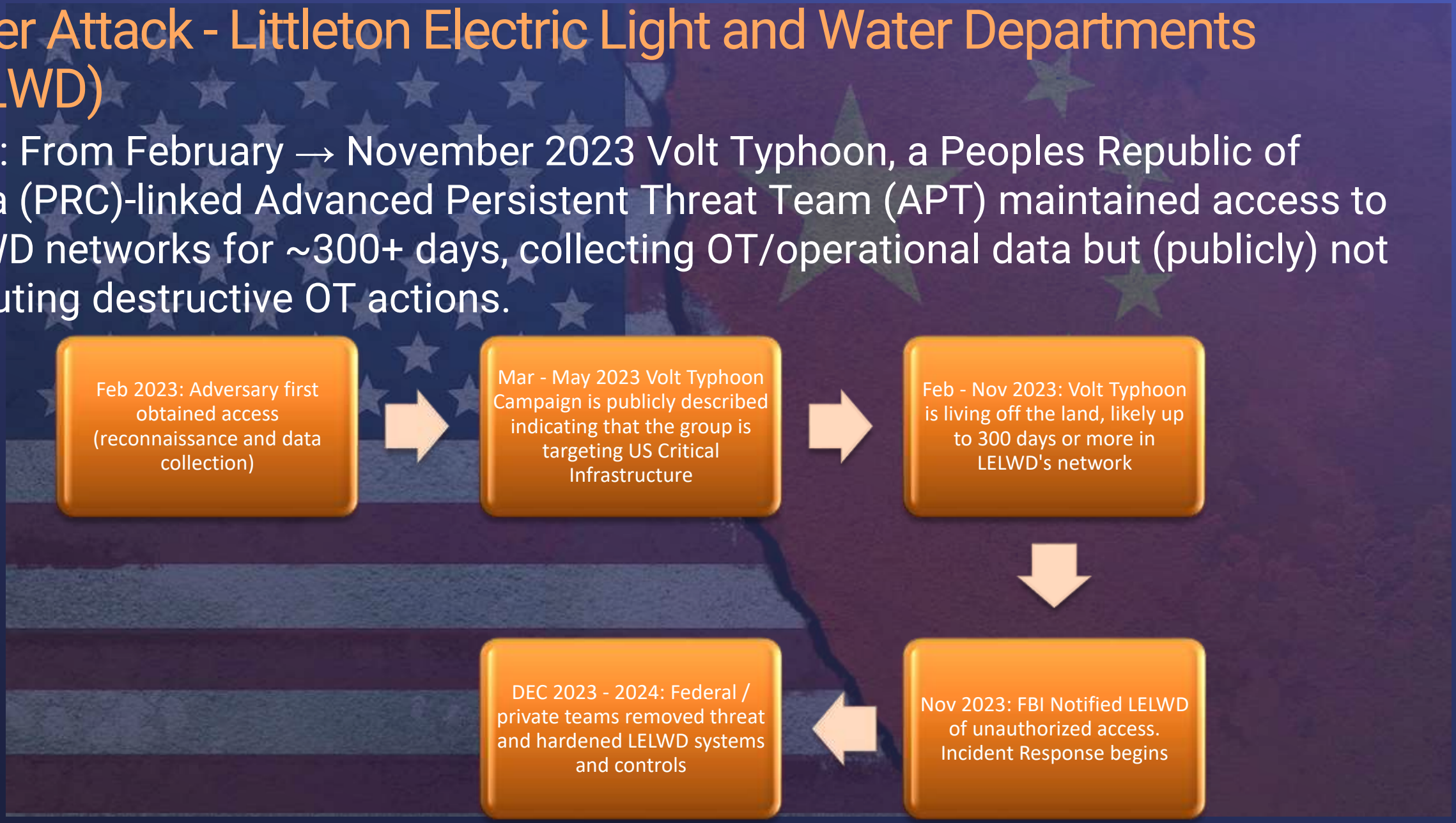
Receive feedback and the guidance of Metropolitan leadership

Agenda

- Littleton Electric Light and Water Departments (LELWD) Cyber Attack Overview
- Who is Volt Typhoon
- Tactic, Technique, Procedure (TTP) Living off the Land (LOTL)
- CLOSED SESSION

Cyber Attack - Littleton Electric Light and Water Departments (LELWD)

What: From February → November 2023 Volt Typhoon, a Peoples Republic of China (PRC)-linked Advanced Persistent Threat Team (APT) maintained access to LELWD networks for ~300+ days, collecting OT/operational data but (publicly) not executing destructive OT actions.



LELWD Root Cause

- **Initial access via a vulnerable internet-facing FortiGate firewall / SSL-VPN** — Volt Typhoon exploited a known FortiOS SSL-VPN vulnerability (Fortinet issued patches/PSIRT advisories in 2022–2024). Public reporting indicates the LELWD FortiGate device had not been updated and remained vulnerable, enabling remote code execution/vector for initial compromise.
- **Managed-service provider (MSP) patching gap / operational oversight** — industry reporting and LELWD statements indicate the firewall firmware had not been patched by the MSP that managed the device, creating an exploitable window months after the vendor fix.
- **Post-compromise tradecraft favored credential-centric and LOTL behavior** — once inside, the actor used living-off-the-land techniques

Who is Volt Typhoon?

- A PRC-linked, state-sponsored activity cluster (publicly tracked as “Volt Typhoon”) that focuses on quietly pre-positioning inside critical-infrastructure networks (routers, VPNs, MSP/cloud suppliers) to harvest credentials and retain options for disruption or coercion later.
- First detailed public writeup by Microsoft (May 24, 2023); U.S. government agencies (CISA/NSA/FBI/DHS) published joint advisories in early 2024 (Feb 7, 2024) after follow-on investigation and disclosures. Law-enforcement disrupted associated malicious infrastructure in Jan 2024.


THE METROPOLITAN WATER DISTRICT OF
SOUTHERN CALIFORNIA
1928