Report: Security Measures for Cloud-Based Phone System

Overview

During the Administration and Public Works Committee on June 6, 2023, the Committee raised concerns over the security of having a cloud-based phone system. Specifically, the Committee decided to move forward with the proposal on the condition that the Department collect further information regarding IT Voice's security measures and the safety of having Yealink phones at the Wildwood Municipal Building.

Experience

IT Voice (formerly VoicePro Networks) has been providing telecommunication services to the City of Wildwood since 2008/2009. IT Voice also provides telecommunication services to the following Cities:

- Overland, MO
- Pevely, MO
- Bel-Ridge, MO
- Breckenridge Hills, MO
- Black Jack, MO
- Jennings, MO
- Pagedale, MO
- St. John, MO

Data Centers

The Department received further information from IT Voice regarding the location of their servers. The Department can confirm that all of IT Voice's servers are located within the United States. The data centers (DCs) that host their services are in Dallas/Ft. Worth, Texas, and Grand Rapids, Michigan. Both of IT Voice's data centers are Class-5 data centers. The Department has provided an overview of the tier system used to classify data centers.

Each tier (1-5) represents an increasing level of redundancy and availability, with higher tiers offering more robust and fault-tolerant infrastructure. While there is no universally standardized definition for each tier, the following general characteristics are typically associated with each tier:

- Tier 1: Basic capacity components and infrastructure. It offers a single path for power and cooling distribution and has an expected availability of around 99.671% (about 28.8 hours of downtime per year).
- Tier 2: Adds some redundancy to Tier I with the introduction of additional infrastructure components. It provides redundant power and cooling systems, allowing for scheduled

maintenance without impacting operations. The expected availability is around 99.741% (about 22 hours of downtime per year).

- Tier 3: Provides a concurrently maintainable infrastructure with redundant capacity components. It ensures that maintenance can be performed without disruption to IT operations and offers multiple independent paths for power and cooling. Tier III facilities typically achieve an expected availability of 99.982% (about 1.6 hours of downtime per year).
- Tier 4: With a fully redundant infrastructure, a Tier 4 data center meets and exceeds all of the requirements of the aforementioned three tiers. Not only do these data centers, preferred by enterprise corporations, provide 99.995% uptime per year (less than 0.5 hours of downtime per year), they also are complete with at least 96-hour power outage protection. The redundancies built into Tier 4 data centers are made to ensure that the system can function normally even if one or more pieces of equipment fail. Everything is redundant, including generators, cooling units, power sources, and more, so that another system can immediately take over in the event that another fails.
- Tier 5: Tier 5 is a relatively new standard in data center requirements. Tier 5 data centers must meet the same standards as Tier 4, plus several additional ones. For example, they must be able to run forever without water, have outside air pollutant detection (and be capable of initiating a protective response), have permanently installed stored energy system monitors, securable server racks, and much more. Furthermore, Tier 5 data centers are required to run on local, renewable power projects.

The DNA of the underlying tech beneath the EMBRACE (IT Voice) platform, Netsapiens, is a mature and secure technology, and is the soft-switch architecture (physical software and digital programming that allow soft-switches to function) for many providers that make it their core SIP switching solution. An SIP switch is a signaling protocol used for multimedia communication sessions, such as voice calls, video calls, and instant messaging. The Department would like to highlight the fact that wide-scale adoption of this platform makes it very robust and lessens the zero-day exposures (hackers discover a software vulnerability before the vendor becomes aware of it) that many lessor-deployed solutions may suffer from.

Yealink Phones

If IT Voice's cloud-based phone system proposal is approved, IT Voice will be providing Yealink T54W phones free of charge to the City of Wildwood. The safety and suitability of Yealink T54W phones, or any other technology equipment, for governmental agencies depend on various factors, including security considerations and risk assessments. While Yealink is a reputable global manufacturer of communication devices, it is important to evaluate specific factors related to the phones and their usage in governmental settings.

When evaluating the safety and suitability of technology devices for governmental use, the focus should be on the security measures implemented in the device itself, as well as the protection of data transmitted and stored by the device. The Department would like to note that Yealink is a

Chinese company, and it is possible that some of the phone's components are manufactured in China. However, it is crucial to note that the country of origin does not inherently determine the security or safety of a device. Many technology products used by governmental agencies, including those from reputable manufacturers, may have components sourced from different countries.

The Department consulted with the Federal Communications Commission regarding the list of communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. Specifically, this list is covered By Section 2 of The Secure Networks Act. This list can be found by visiting https://www.fcc.gov/supplychain/coveredlist.

Section 1.50002 of the Commission's rules directs the Public Safety and Homeland Security Bureau to publish a list of communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, based exclusively on any of four sources for such a determination and that such equipment or services possess certain capabilities as enumerated in section 2(a) of the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609). This list was last updated on September 20, 2022. Please see the equipment and services included in the "Covered List" below:

- Telecommunications equipment produced by **Huawei Technologies Company**, including telecommunications or video surveillance services provided by such entity or using such equipment.
- Telecommunications equipment produced by **ZTE Corporation**, including telecommunications or video surveillance services provided by such entity or using such equipment.
- Video surveillance and telecommunications equipment produced by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.
- Video surveillance and telecommunications equipment produced by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.
- Video surveillance and telecommunications equipment produced by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

- Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.
- International telecommunications services provided by **China Mobile International USA Inc.** subject to section 214 of the Communications Act of 1934.
- Telecommunications services provided by **China Telecom (Americas) Corp**. subject to section 214 of the Communications Act of 1934.
- International telecommunications services provided by **Pacific Network Corp** and its wholly-owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.
- International telecommunications services provided **by China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.

While it is important for municipalities to conduct their own risk assessments and evaluate specific security requirements, Yealink is currently not listed on the Federal Communications Commission's "Covered List." Yealink phones can provide a safe and reliable communication solution for municipalities in the U.S. when implemented with proper security measures and best practices. It is crucial for the City to ensure network security, implement appropriate access controls, regularly update firmware, and follow recommended security guidelines to maximize the safety of its communication systems. If approved, the City will work with its IT Vendor, ThrottleNet, Inc., and IT Voice to ensure the safe and secure implementation of the cloud-based phone system. At this time, Yealink phones are not recognized as a severe security thread by the federal government and both of IT Voice's data centers are located within the U.S. That being said, the Department believes that the Yealink T54W phones are acceptable for use at the Wildwood Municipal Building.