SB 3 Section 4 Facts

- **FACT:** Drones controlled by smartphones and other internet-connected devices provide a path for drone data egress and storage, allowing for intelligence gathering on U.S. critical infrastructure.[1]

- **FACT:** While ensuring that network-connected devices are up to date with the latest patches and firmware is critical for the secure operation of any information and communications technology device, updates controlled by Chinese entities could introduce unknown data collection and transmission capabilities without the user's awareness. That data might be accessed by the People's Republic of China (PRC).[2]

- **FACT:** As drones and their peripheral devices such as docking stations are incorporated into a network, the potential for data collection and transmission of a broader type—for example, sensitive imagery, surveying data, facility layouts—increases. This new type of data collection can allow foreign adversaries like the PRC access to previously inaccessible intelligence.[3]

- **FACT:** President Biden, President Trump, the FBI, the Department of Homeland Security and Congress (both Republicans and Democrats) have stated and implemented policies that these Chinese made drones pose significant risks.

- **FACT:** The United States Congress passed, and the President signed, a bill that bans the use of Chinese and Russian made drones by federal agencies.[4]

- **FACT:** These drones have been found by experts to contain "backdoors" built into their software that allow the Chinese intelligence services to access the drones and all of the drone's data without the user knowing.
    - DJI's Products Terms of Use[5] agreement incorporates by reference DJI's privacy policy, which states that DJI "collect[s] information about you directly from you, from third parties, and automatically through your use of the DJI Products. . . . When you choose to upload your photos, videos or other content using DJI

---

[1]CISA, *Cybersecurity Guidance on Chinese-Manufactured UAS*. Accessed February 28, 2024: https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf

[2]CISA, *Cybersecurity Guidance on Chinese-Manufactured UAS*. Accessed February 28, 2024: https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf

[3]CISA, *Cybersecurity Guidance on Chinese-Manufactured UAS*. Accessed February 28, 2024: https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf

[4]Congress, *All Information (Except Text) for S.473 - American Security Drone Act of 2023*. Accessed February 28, 2024: https://www.congress.gov/bill/118th-congress/senate-bill/473/all-info

[5]DJI, *DJI UAS Products Terms of Use*. Accessed March 5, 2024: https://www.dji.com/terms.

Products and Services, including text content relating thereto, we may collect and store such content, including EXIF data relating to the photo or video."[6]
    - DJI admits that it "may disclose your information to our parent company, affiliates and subsidiaries," which includes to the People's Republic of China as DJI is a Chinese Military Company.[7]
    - Additionally, all of the data produced by the drones is potentially compromised when put onto American servers.[8]

- **FACT:** DJI was designated a "Chinese Military Company" by the Department of Defense.[9]
    - A Chinese Military Company is defined in Public Law 116-283 – this means the company is controlled by the Chinese Military.

- **FACT:** Encrypted software does not protect data on Chinese drones.
    - The security risks linked to Chinese-made drones cannot be addressed by security software updates. The drone hardware itself is the risk.

- **FACT:** Even if the Chinese will not use the information that they collect to physically invade the United States, does not mean that they will not engage in cyberattacks on critical infrastructure or give this information to a hostile actor who will attack America.[10]
    - Sensitive Ukrainian information was given to the Russians that was collected by Chinese drones prior to the full invasion of Ukraine two years ago.

- **FACT:** The Chinese Communist Party has hacked into critical American infrastructure—including communications, energy, transportation, water for the sole purpose of disabling and destroying our critical infrastructure, and thus deter our ability to marshal military might, in the event of a conflict over Taiwan.[11]
    - The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party reported that the Chinese will be ready to launch their attack against Taiwan in the next three years.

---

[6]DJI, DJI Privacy Policy. Accessed March 5, 2024: https://www.dji.com/policy
[7]DJI, DJI Privacy Policy. Accessed March 5, 2024: https://www.dji.com/policy
[8]CISA, *Cybersecurity Guidance on Chinese-Manufactured UAS*. Accessed February 28, 2024: https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf
[9]https://media.defense.gov/2024/Jan/31/2003384819/-1/-1/0/1260H-LIST.PDF
[10]CISA, *Cybersecurity Guidance on Chinese-Manufactured UAS*. Accessed February 28, 2024: https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf
[11] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/1.31.24%20Hearing%20Transcript.pdf