Affidavit of Cybersecurity Compliance
NIST IR 7621, Section 2

State of _____ County of _____

1. My name is _____
2. I am authorized to act as the Chief Security Officer for _____
3. I am familiar with the cybersecurity standards published by the National Institute of Standards and Technology (NIST) in Interagency Report 7621, known as **NIST IR 7621**.
4. I certify that this business is in compliance with the following provisions of **NIST IR 7621**, **Section 2**.
5. Per **Section 2.1**, a business cybersecurity risk assessment was completed by _____ to identify risks, and to implement measures to reduce or eliminate the identified risks.
6. Per **Section 2.2**, ESET Internet Security suite is installed for **antivirus** and **antispyware** protection, and is set for auto-updates for virus signature database, automatic scans once per day, and is required for use by all employees at all times.
7. Per **Section 2.2**, Malwarebytes Anti-Malware is installed for **antimalware** protection and is run weekly.
8. Per **Section 2.2**, IObit Malware Fighter is installed for **antimalware** protection and is run weekly.
9. Per **Section 2.3**, a DSL modem/router is installed as a **hardware firewall**, using a strong password.
10. Per **Section 2.4**, ESET Internet Security suite includes a **software firewall**, which is enabled.
11. Per **Section 2.5**, all software updates to the Windows operating system and application software are installed promptly, with **auto-update** enabled, where available.
12. Per **Section 2.6**, backup copies of important data files are made on a regular basis.
    Daily on-site **auto-backup** is done with Acronis True Image to a removable USB flash drive.
    Hourly 256-bit AES **encrypted off-site backup** to out-of-state SpiderOak cloud storage is used for **disaster protection**. Several files are **tested** monthly to verify that backup is working properly.
    A recent data backup is stored on removable media in a fireproof safe for **disaster protection**.
13. Per **Section 2.7**, physical access to computers and the network is controlled by keeping equipment inside a **locked office**. Users require a **strong password** to log in. Computers automatically **log off** after 60 minutes of inactivity. During transportation, computers are kept in a **locked vehicle** with an armed alarm. In the field, computers must be supervised by the user and may not be left unattended.
14. Per **Section 2.8**, the **wireless network** in the office does not broadcast an **SSID**, has a **strong administrator password**, and does not use WEP encryption. **WPA-2 encryption** is used.
15. Per **Section 2.9**, employees must read the business **written information security policy** (WISP) and must sign a statement agreeing to follow the WISP. **Security training** is provided as needed by the Chief Security Officer, or a security consultant, or self-study training program, including a review of **NIST IR 7621**.
16. Per **Section 2.10**, each user is required to operate from a **separate user account**, with **limited privileges**. Only the **system manager** may have **full administrative privileges**. **Strong passwords** are required, at least 12 characters, using upper case, lower case, numbers and special characters.
17. Per **Section 2.11**, access to systems and data is limited to a **need to know** basis. Only the **system manager** is authorized to install software. All **financial transactions** are reviewed by the **Treasurer**.
18. Additional Security: ESET Internet Security includes **anti-phishing**, **antispam**, and **anti-ransomware**.
19. Additional Software: IObit Driver Booster is run monthly to keep **software drivers** up to date.
20. Additional Software: Advanced System Care, CCleaner and Glary Utilities are used for **maintenance**.

_____ _____
Chief Security Officer Date

Signed and sworn to (or affirmed) before me on this date _____, 20_____
by _____.

Notary Public _____ [Stamp]
My commission expires _____