Affidavit of Cybersecurity Compliance
NIST IR 7621, Section 3

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 3**.
5. Per **Section 3.1**, computer users may not open email attachments, unless sender is a trusted source.
6. Per **Section 3.2**, users may not click on web links in email, instant messages or social media, unless it is a trusted link.
7. Per **Section 3.3**, users must use pop-up blocker on web browser, unless it is a trusted web site.
8. Per **Section 3.3**, users may not insert removable media from an unknown or untrusted source. Auto-Run must be disabled for USB ports, CDs and DVDs.
9. Per **Section 3.4**, users must use secure https browser connection for online transactions and banking. After online session, browser cache shall be deleted, including temp files, cookies and browsing history.
10. Per **Section 3.5**, employer shall conduct due diligence background check when hiring employees, including criminal history, sex offender, credit check, previous employer and credential verification.
11. Per **Section 3.6**, when online, users must use a standard user account, not an administrator account.
12. Per **Section 3.7**, users may not download software from untrusted websites. Website must be trusted or scanned by anti-malware software.
13. Per **Section 3.8**, users must complete continuing education in cybersecurity and information security, as directed by Chief Security Officer.
14. Per **Section 3.9**, old computers and digital media must be disposed of using secure delete or disk wipe to destroy data on hard disks, and secure file delete for flash drives. Old CDs, DVDs, floppy disks and paper documents must be shredded or incinerated.
15. Per **Section 3.10**, employees must protect against social engineering, and may not give personal or confidential information to any unauthorized person by phone, email, social media or other means.
16. Per **Section 3.11**, Chief Security Officer or other appointed person shall create an asset inventory of hardware, software and information, updated annually.
17. Per **Section 3.12**, encryption, such as Windows Encrypting File System (EFS), shall be used on sensitive and confidential information. Confidential files stored on removable media shall be encrypted.
18. Additional Security: _____

_____ _____

Chief Security Officer Date

Subscribed and sworn to or affirmed before me on this date _____, 20_____ by _____.

Notary Public _____ [Seal]