Submission Requirements

1. **Network Topology / Visio:**
   A network diagram that describes the connections of a computer network which may be physical or logical. The information in this diagram (or layout) can consist of physical location, network and system devices (brand/model), cabling, and a basic understanding of how data flows from source to destination.

2. **COI Form 700 Application:**
   A description of the software application and system application. This information should include development platform and programming language, hardware operating system, type of database, middleware, plug-ins, 3rd party add-ons, and other technologies that make up the entire useable application.

3. **Website:**
   A description of how the website is setup, type of operating system, web services, secured web tunnel, and encryption level (i.e. 2048-bit SSL encryption, SHA1-2-3, soft token, etc.). Use of trusted certificates (VeriSign and Entrust), and not the internal system/server generated.

4. **Secured Authentication:**
   Describe how a user (or filer) can be uniquely identified and login securely to access website filing information, including user identification, account creation process, password format or scheme, password recovery/reset.

5. **Security (network, system, application):**
   Describe the purpose of each Information Technology security component, device, and software that ensures the security of data transmittal is reliable and the integrity of data was not compromised (i.e. layered network security, enterprise-level firewalls, redundancies, Intrusion Prevention System (IPS), network isolation (subnet), database encryption, etc.).

   An operational description of network systems and application process to ensure industry best practices has been applied and is being proactively managed (i.e. network vulnerability scans, web scans, system hardening, code reviews, patch management, Anti-Virus updates, etc.).
7. **Backup and Restore:**
   An operational description of the backup and restore process which includes Information Lifecycle Management (ILM) and off-site storage (i.e. policies, incremental, differential, full backup, etc.).

8. **Business Continuity & Planning / Disaster Recovery (BCP/DR):**
   A description of the process, policies and procedures that are required to maintain business continuance when a disaster occurs. Part of the description is to define the disaster recovery method in order to return business to normal operations within a period of time (cold site, warm site, active/hot site, etc.).

9. **System Access**
   A user account and password will be submitted to the FPPC for purposes of testing and review.

**Required System Features / Business Operations**

1. Electronic email notification of filing
2. Electronic confirmation #
3. Electronically filed signature (date/time stamp)
4. Extractable COI data (using common file format – CSV, TXT, XML, etc.)
5. Auto-populate filer’s information
6. Previous year’s filings
7. Public website accessible 24x7x365
8. FPPC Pamphlet online
9. System Assistance Hotline (local County)
10. Online password management
11. Account Registration Process