Attachment B

FPPC Form 700 System

Certification Submission for Local Agencies

Last Revised

10 January 2013

OVERVIEW

Since its ground-breaking launch in 2006, NetFile's FPPC Form 700 e-filing system has received and processed more than 67,000 Form 700 filings to date. Of those filings, nearly 25,000 have been filed electronically.

The NetFile FPPC Form 700 application ("SEI") is a shared, hosted, cloud-based system comprised of three major architectural components:

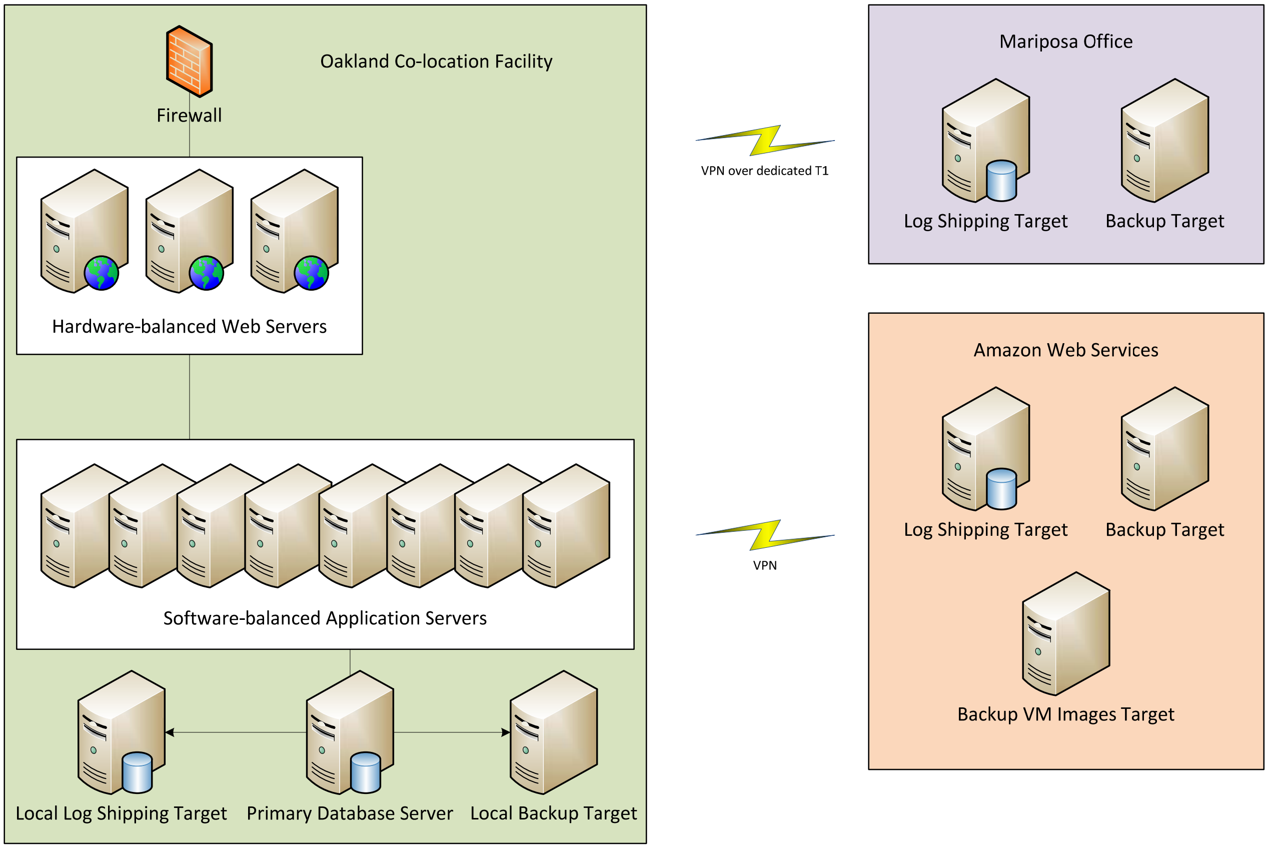
Admin: Provides features for local agency staff to create, track and correspond with filers

Filer: Allows individuals to create, review, print, and e-file their Form 700 documents

Public: Displays filed documents to the public on the web

SUBMISSION REQUIREMENT #1 – Network Topology

NetFile Logical Network Diagram



Rev. 1/10/2013

SUBMISSION REQUIREMENT #2 - COI Form 700 Application

Development

All development/maintenance for the SEI application is performed in Windows 7 using Visual Studio 2010. All application code is written in ASP.NET and C# against the .NET 3.5 runtime.

Two third party libraries are used. First, for PDF rendering, we use iTextSharp. Second, for middleware data access, we use DataObjects.NET. The web application pages use code behind files that talk to data access libraries to retrieve and store data. Code integrity is maintained using the Perforce source control system.

Production

The deployed web application suite runs on Windows Server 2003 hosts, with a SQL Server 2008 R2 backend. The operating system for the primary database server is running Windows Server 2008 R2.

SUBMISSION REQUIREMENT #3 – Website

The website runs on Windows Server 2003, using IIS v6. Two web sites are configured, one for public access and the other for internal services. ASP.NET web applications are stored under virtual directories. The applications run under IIS app pools designed to maximize simultaneous users. The app pools will also auto restart on any detected issues to maximize uptime. Database caching is enabled up to 1GB on reads.

ASP.NET web services are used internally to communicate between the admin and filer components of the system. These web services endpoints are not exposed to the public internet, and require ASP.NET authentication. Secure web browsing is available using SSL certification from COMODO. The SSL encryption uses RC4 128 bit keys. System logging is performed through syslog and all messages are routed to a central logging database. Alerts are triggered on system errors or service outages and sent to NetFile support staff via email and text messages.

SUBMISSION REQURIEMENT #4 – Secured Authentication

Filers are uniquely identified by their private e-mail address, stored in the NetFile SEI database along with an internal identifier which is also unique. Filer account creation is controlled via the Admin application, which is administered by department-level Filing Liaisons or agency Administrators.

Passwords are randomly generated with a mix of lower and upper-case letters and numbers with a length of 8 characters. Special characters are also included. Filers may request a new randomly-generated password at any time through the Filer application.

SUBMISSION REQUIREMENT #5 – Security (network, system, application)

While NetFile does use Amazon Web Services for additional off-site storage of backup files, all other IT assets of the SEI system are owned and managed by NetFile.

The SEI system is located at the Oakland Co-location facility of Digital Realty Trust, a tier one data center. This ensures the highest level of facility-related support, such as power, cooling, and networking infrastructure for NetFile's servers. The facility is secure, with 24-hour security on site.

Primary network security for NetFile's collocation is provided by a High-Availablity pair of SonicWall NSA 2400 devices. These units act as our network firewall and intrusion detection system.

All communication between the collocation faciltity and NetFile IT staff is done through VPN connections.

SUBMISSION REQUIREMENT #6 – Security Operations (Industry Best Practices)

NetFile has been providing online e-filing and disclosure systems since 1998, before most of the rest of the world even though online disclosure was a real possibility. All of our software is carefully reviewed with security in mind – particularly regarding such popular attack vectors as SQL injection, buffer overflows, and server misconfigurations.

NetFile utilizes online and internal vulnerability scanning services, such as HackerTarget.com and Netsparker to scan its software on a per-build basis.

All software in the collocation network is updated on a continuous basis, to ensure all the latest security patches are deployed.

SUBMISSION REQUIREMENT #7 – Backup and Restore

SQL 2008 R2 Data

All transactional data and filing document data is stored in our primary SQL 2008 R2 database. Log shipping is utilized to maintain a hot standby database server at all times, also located in the Oakland facility. Log shipping is also performed to a hot standby database server located in our Mariposa office over the VPN. Additionally, log shipping is performed to a SQL 2008 instance hosted in Amazon Web Services as a failsafe.

Full backups of the SQL data is performed nightly with two copies of the backup files maintained at the Oakland facility. Copies of the full backups are sent nightly to our Mariposa office and Amazon S3 storage. Backups stored in S3 are encrypted.

A minimum of ten days of complete backups are maintained.

Machine Images and Configuration Data

Backup VM images and configuration data files (such as firewall and load balancer configurations) are made after configuration changes to the affected VM/device. These backups are stored in Oakland and Amazon S3.

Source Code

All NetFile source code related to the SEI system is hosted in Perforce. A full backup of the Perforce data is made nightly and copied to multiple locations in the Oakland facility and Mariposa office.

SUBMISSION REQUIREMENT #8 – Business Continuity and Planning / Disaster Recovery

The NetFile SEI system is designed to provide a significant amount of fail-over redundancy without creating exorbitant costs for our clients. Designing the system to provide a reasonable level of planned fault-tolerance includes:

- Dual HA SonicWall NSA 2400 firewall appliances
- Multiple network switches with every server having at least two NIC adapters
- Kemp Technologies Load-balancing systems configured in an HA pair
- Multiple web servers, load balanced by the Kemp units
- Multiple application/processing servers, balanced by our software processes

The only 'single point of failure' in the entire SEI system is the primary SQL 2008 database server. The database server itself is as fault tolerant as any single Intel-based server can be with multiple power supplies and RAID 10 SSD disk arrays.

If any single device or server apart from the SQL database server failed, NetFile's users should not even be able to notice.

Should the SQL database server fail, NetFile IT staff can remotely reconfigure the system to use the hot standby SQL server (with the log shipped data, so it is fully up to date even as the failure of the primary server occurs) within ten minutes.

If there was a more extensive disaster, such as a major earthquake destroying the city of Oakland, the SEI system could be running again within a maximum of six hours with provisioned Amazon EC2 instances. We're currently in the process of evaluating several different backup solutions to reduce our maximum potential outage duration.

SUBMISSION REQUIREMENT #9 – System Access

NetFile staff will contact FPPC IT staff to provide appropriate user credentials.

REQUIRED SYSTEM FEATURE CHECKLIST

1. *E-mail notification of filing*
   YES. All e-filing submissions to NetFile's SEI system receive an e-mail indicating success or failure of the submission.

2. *Electronic confirmation number*
   YES. All e-filings accepted by NetFile's SEI system are issued a unique filing ID. This ID is listed on the Public portal and rendered onto the PDF representation of the e-filing.

3. *Electronic signature (date/time stamp)*
   YES. All e-filings accepted by NetFile's SEI system are time-stamped, and can be related back to an individual's private e-filing credentials.

4. Extractable COI data in a common file format
   YES. All e-filings generated or accepted by NetFile's SEI system are XML data documents, which pass through a PDF rendering process for presentation and printing purposes.

5. *Auto-populate filer information*
   YES. Previous year e-filings auto-populate the following year form. Additionally, changes to a filer's departments or positions during the year are available for easy selection into the new form, along with the previous year's departments and positions.

6. *Previous year filings*
   YES. A filer is able to review, reprint or amend any previous filing they have created using the SEI system.

7. *Public website available 24x7x365*
   YES. NetFile's web portals into the SEI system are always available.

8. *FPPC Pamphlet Online*
   YES. FPPC-provided manuals and instructions are readily available to all filers while using the system.

9. *System assistance hotline*
   YES. Local cities and counties using the NetFile SEI system provide telephone help desk support to their filers.

10. *Online password management*
    YES. Filers or agency administrators may reset their passwords at any time.

11. *Account registration process*
    YES. NetFile provides local agencies with helpful documentation and procedures along with on-site training seminars that have worked well for other jurisdictions to achieve a high percentage of initial e-failing adoption by their filers. Additionally, NetFile imports personnel database records to initially populate the Admin system.