County of Fairfax, Virginia

To protect and enrich the quality of life for the people, neighborhoods and diverse communities of Fairfax County

# SURVEY RESULTS
## *Secure Internet Connectivity*

November 21, 2013

## SUMMARY

On behalf of Fairfax County Courts, the Center for Legal & Court Technology (CLCT)[1], sponsored by the College of William and Mary Law School, conducted a blind survey of Federal, state, and local courts to determine if and to what extent secure internet connectivity such as VPN (Virtual Private Network) is being utilized.  Fairfax County Courts are one of the original affiliate members of the CLCT.

The survey collected information on how courts are using secure internet connectivity to access and share court and case information.  A total of 63 courts from across the country and Canada responded to the 8 question survey.  Exactly 58 of the 63 respondents reported that they are currently utilizing some type(s) of secure internet connection technology for sharing court and case information.  The results of the survey are provided within.

## RESULTS

The survey responses varied in the level of details, but support that courts have become more reliant and dependent on the use of the internet and electronic exchange of information.  Each question is summarized below:

1. *<u>Is your court using secure connectivity over the internet?</u>*

   Yes – 92%<br>
   No – 8%

2. *<u>Please elaborate?</u>*

   The majority of the courts use some form of secure internet connectivity, such as VPN Client (Virtual Private Network), to allow access to their court and case information.  A small subset of respondents did not know what method they used to remotely access their data.

| ***Types Reported*** | |
|---|---|
| 1. | VPN Client (Virtual Private Network) |
| 2. | SSL Website/Webserver (Secure Sockets Layer) |
| 3. | Citrix |
| 4. | Secure email |

[1] *The Center for Legal & Court Technology (CLCT) is an entrepreneurial public service organization at the College of William & Mary Law School and a joint initiative of William & Mary and the National Center for State Courts.  CLCT's mission is to improve the administration of justice through the use of technology.  For more information:  http://www.legaltechcenter.net/*

| ***Types Reported*** |
|---|
| 5. Internet Court website postings |
| 6. Extensive Infrastructure supporting external users |
| 7. Unknown |

3. *Describe for what purpose(s) secure internet connectivity has been used?*

The majority of the courts stated they use secure internet connectivity for a wide variety of purposes, as stated below:

| **Purposes Reported** |
|---|
| 1. Access to case management systems |
| 2. Access to court internal domain from any internet connected computer |
| 3. Access to email, network files, and web |
| 4. Allow access by employees |
| 5. Allow remote review of documents |
| 6. Support users via remote desktop |
| 7. Allow transmission of information through public facing web applications such as e-Filing |
| 8. Receive credit card and court payments |
| 9. Share confidential data |
| 10. Allow access for volunteer legal entities who provide free legal services |
| 11. Allow access by large news media agencies |
| 12. Allow access by justice partners including public defenders, state's attorney, sheriff |
| 13. Allow access by approved business partners |
| 14. Allow access to court systems |
| 15. Allow advisements matters for local inmates and from out of town inmates |
| 16. Remote interpretation |
| 17. Allow access to accused persons for their own court case materials such as public viewing |
| 18. Allow court-only intranet access |
| 19. Allow access to confidential and non-confidential court documents |
| 20. Allow online search for court cases |
| 21. Allow access to desktop applications |
| 22. Receive disposition records from 90 counties, and forward to four authorized state entities |
| 23. Receive and resubmit court metrics |

4. *Does your court interact with other facilities or staff (court and non-court) outside of the Courthouse by using secure connectivity over the internet?*

Yes – 78%
No – 22%

5. *Please describe?*

Overall, the survey found that courts provide access to the court staff, and other non-court entities such as the public, attorneys, state agencies, business partners, justice partners (including public defenders, state's attorney, and sheriff), inmates, accused persons, and large news media agencies.

The British Columbia courts shared how they are successfully piloting a system using secure connectivity that allows access to confidential data from multiple, remote sites. They stated that clients are able to securely and easily access legal documents, case information, client histories, discharge dates and medical appointments. They are in the process of expanding the technology to include nine correctional centers, 55 community corrections offices, and 40 counsel offices.

6. *Problems or Issues*

A subset of courts shared the following types of problems or issues encountered with using secure internet connectivity over purposes of accessing their court and case information:

| ***Problems or Issues*** |
|---|
| 1. Cloud connectivity variances |
| 2. Business processes not worked out in advance |
| 3. Inadequate bandwidth for remote interpreters |
| 4. Awkwardness and slowness of connection, and connection difficulties |
| 5. Managing the number of requests for gaining access to the system |
| 6. Inadequate staff for supporting the technology |
| 7. Issues with certificates, and keeping VPN up to date |
| 8. Issues with Internet Service Providers (ISPs) |
| 9. No problems |
| 10. Unknown |

7. *Levels of Security*

A subset of respondents reported the following levels of security in place and if they were considered sufficient from intrusion or outside vulnerabilities for using secure internet connectivity for purposes of accessing their court and case information:

| ***Levels/Effectiveness of Security Levels*** |
|---|
| 1. Multiple layers: VPN, firewall, mainframe, multiple DMZs is considered sufficient |
| 2. High security levels (not clearly defined). No guarantees with respect to sufficiency to prevent intrusions. |
| 3. Cisco infrastructure is considered sufficient |
| 4. Government network utilizing traditional firewall provisioning |
| 5. Third-party vendor with quarterly internal security audits and certificate maintenance |
| 6. Secured internet with firewalls |
| 7. High level of security interferes with the use of some protocols including cloud-based utilities and Skype. Unsure if sufficient. |
| 8. Keep servers up to date, web servers do not have internal network permissions, web services data access only, web servers do not connect to case management databases, |

| ***Levels/Effectiveness of Security Levels*** |
|---|
| monitor web logs for suspicious activity. Respondent states that while no system can ever be un-hackable, we do everything we can to minimize security holes. |
| 9. Use of password rotations, strong password requirements, virus and malware protection, scan all incoming and outgoing files, keep hardware current with patches and software updates, access only through file server for some applications. Not considered sufficient until the addition of regular third-party scans and threat assessments. |
| 10. Dual factor authentication provides additional security layer, also utilize interactive monitoring. |
| 11. Use of external devices and their personal user accounts potentially exposes the system to compromised data (i.e., non-court devices may be improperly secured). Respondent concerned security is insufficient. |
| 12. A number of respondents did not know the extent and sufficiency of the security. |

## 8. *Lessons Learned*

A subset of courts shared the following lessons learned with using secure internet connectivity for purposes of accessing their court and case information:

| ***Lessons Learned*** |
|---|
| 1. Preferable for courts to own their own server, and control their own security |
| 2. Analyzing, then remediate security/intrusion vulnerabilities, malicious content and data leakage |
| 3. Utilize encryption/decryption technologies |
| 4. Recommend remote access through WAN for securing court data |