“Leveraging the Internet to Securely Broker Data”
Pennsylvania Justice Network (JNET)
July 14, 2015
Eric Webb, Executive Director JNET
Pennsylvania Justice Network

- JNET provides criminal justice and public safety practitioners with access to critical data in a prompt, secure and efficient manner

- 34,000 users from federal, state, and municipal agencies

- Web-based, mobile-friendly

- Information is protected by policy, advanced authentication, secure connectivity and role-based entitlements
JNET provides secure access to an extensive set of data sources:

- Administrative Office of Pennsylvania Courts
- Juvenile Court Judges’ Commission
- Pennsylvania Board of Probation and Parole
- Pennsylvania Commission on Crime & Delinquency
- Pennsylvania Commission on Sentencing
- Pennsylvania Department of Corrections
- Pennsylvania Department of Health
- Pennsylvania Department of Human Services
- Pennsylvania Department of Transportation
- Pennsylvania State Police
- Pennsylvania Labor & Industry
PennDOT Records available on JNET

- Driver Information and Demographics
- Certified Driver’s History
- Certified Vehicle Abstract
- License / Registration Police Pick Ups
- Vehicle Inspection and Emission Records
- PennDOT Photo ID examples
- Inspection Decals examples
- JNET Traffic Stop
- JNET Address Search
- JNET Photo Search
Network Security

Past

Secure Circuit

Present

Secure Circuit

Future

Secure Circuit

Internet
- JNET has moved all of our secure portal applications to the internet
- User applications are secured using TLS encryption (JNET’s Access Manager)
- FIPS 140-2 compliant (NIST standard)
By clicking Login, I hereby agree and understand:

1. That I am an authorized JNET user and I will use JNET for official purposes only as defined by JNET Policy and Procedures;
2. That personal use of JNET is strictly prohibited;
3. That all transactions in JNET are logged and audited;
4. That I will not disseminate JNET derived data to unauthorized individuals.
5. That use of JNET is governed by JNET Policies and Procedures, and violations may result in the suspension of my access to JNET.
6. That use of any JNET application protected by a user Digital Certificate and derives Pennsylvania State Police CLEAN/NCIC data is governed by PSP CLEAN Administrative Regulations, and violation of CLEAN Administrative Regulations may result in the suspension or revocation of my access to both JNET and CLEAN and may lead to criminal prosecution.

If you have problems logging in, please contact the JNET Help Desk at ra-jnethelpdesk@pa.gov or 1-877-327-2465.
Roll based access
2,716 locations

<table>
<thead>
<tr>
<th>Role</th>
<th>Assigned To</th>
<th>Source</th>
<th>Effective Date</th>
<th>Expiration Date</th>
<th>Initial Request Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Enhancement Administration</td>
<td>Eric Webb</td>
<td>User Assigned to Role</td>
<td>Feb 3, 2010</td>
<td></td>
<td>Request generated by policyDriver DN: JNET-IDV-PROD\jnet\services\Idm361\IDV2JNET Location: vnd.nds.stream://JNET-IDV-PROD\jnet\services\Idm361\IDV2JNET\Input\HandleRoles\Xml\Data:108</td>
<td>Completed</td>
</tr>
<tr>
<td>Business Partners CSX Sponsor - CSX</td>
<td>Eric Webb</td>
<td>User Assigned to Role</td>
<td>Nov 17, 2010</td>
<td></td>
<td>add sponsor and registrar to csx</td>
<td>Completed</td>
</tr>
<tr>
<td>Business Partners CSX Sponsor - CSX</td>
<td>Business Partners CSX Sponsor - CSX</td>
<td>Role Relationship</td>
<td>Nov 17, 2010</td>
<td>Assigned by IDV2JNET Pub Create Rule</td>
<td></td>
<td>Completed</td>
</tr>
<tr>
<td>Certificate Management</td>
<td>Eric Webb</td>
<td>User Assigned to Role</td>
<td>Feb 3, 2010</td>
<td></td>
<td>Request generated by policyDriver DN: JNET-IDV-PROD\jnet\services\Idm361\IDV2JNET Location: vnd.nds.stream://JNET-IDV-PROD\jnet\services\Idm361\IDV2JNET\Input\HandleRoles\Xml\Data:108</td>
<td>Completed</td>
</tr>
</tbody>
</table>
• Migrating from x.509 digital certificates for users, to One-Time-Password (OTP) solution.
• OTP meets FBI CJIS requirements
• OTP’s limited life span makes it less susceptible to misuse
• Alleviates browser compatibility issues
In 2014, JNET began publishing services over the internet using x.509 digital certificates.

Services are facilitated using a FIPS 140-2 compliant web-service appliance.

Certificates must be maintained and synchronized between JNET and business partners.

When necessary, site to site VPN (IPSec) tunnels are used to secure services.
Enterprise Information Security Office (EISO)

- EISO analyzes application-based traffic ([www.jnet.pa.gov](http://www.jnet.pa.gov)) for threats or patterns
- JNET uses EISO’s code scanning tools independently to mitigate code weaknesses
- JNET applications are submitted and assessed through EISO’s Commonwealth Application Certification and Accreditation (CA²) process
Questions?

Contact Information
Eric Webb
717-346-7355
ewebb@pa.gov