About Skyline Technology Solutions

• Full service IT integrator, enterprise solutions provider and product development organization
• State & Local government, Federal, and commercial clients.
• Established 2004
• 300+ employees
• Privately held
• HQ outside of Baltimore, MD
• Over 300 clients nationwide
Transportation and Public Sector Customers

- TDOT (Department of Transportation, Tennessee)
- VDOT (Virginia Department of Transportation)
- MDOT (Maryland Department of Transportation)
- VITA (Virginia Information Technologies Agency)
- New York State Department of Transportation
- CHART (Connecticut High Access Roadway Transport, Transportation)
- Department of Transportation
- Pennsylvania Department of Transportation
- DelDOT (Delaware Department of Transportation)
- Penna Turnpike
- SCDOT (South Carolina Department of Transportation)
- Skyline Technology Solutions
How Mature is Your ITS Infrastructure?

- DOT Framework
- ITS Monitoring
  - Comprehensive ITS Management solution that understands the relations between all the components that make up the key transportation services.
- Cybersecurity
  - A transportation-infrastructure centric cybersecurity program to include 1) Governance, 2) Engineering, and 3) Ops
- Field Communication Architecture
  - Creating a common underlying communications leveraging the broad array of possible communications (technologies private fiber/wireless and leased services)
  - Support network function virtualization

<table>
<thead>
<tr>
<th>V2I, V2V</th>
<th>Integrated Corridors</th>
<th>Utilizing the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Vehicles</td>
<td>Centralized Systems</td>
<td>DSRC or 5G</td>
</tr>
<tr>
<td>Vehicle Data Collection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Five Levels of Vehicle Autonomy

- **Level 0**: No automation; the driver is in complete control of the vehicle at all times.
- **Level 1**: Driver assistance; the vehicle can assist the driver or take control of either the vehicle’s speed, through cruise control, or its lane position, through lane guidance.
- **Level 2**: Occasional self-driving; the vehicle can take control of both the vehicle’s speed and lane position in some situations, for example on limited-access freeways.
- **Level 3**: Limited self-driving; the vehicle is in full control in some situations, monitors the road and traffic, and will inform the driver when he or she must take control.
- **Level 4**: Full self-driving under certain conditions; the vehicle is in full control for the entire trip in these conditions, such as urban ride-sharing.
- **Level 5**: Full self-driving under all conditions; the vehicle can operate without a human driver or occupants.

*Source: SAE & NHTSA*
### Where Am I and What Do I Need To Do?

<table>
<thead>
<tr>
<th>Category</th>
<th>Novice</th>
<th>Beginner</th>
<th>Intermediate</th>
<th>Advance</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITS Management</strong></td>
<td>Deploy only</td>
<td>Spreadsheets for tracking</td>
<td>Basic availability monitoring</td>
<td>Capacity management</td>
<td>Strategic planning support</td>
</tr>
<tr>
<td><strong>Cybersecurity</strong></td>
<td>Default settings</td>
<td>Basic configuration</td>
<td>Governance model</td>
<td>Proactive monitoring, incident detection</td>
<td>Continuous cybersecurity posture enhancement</td>
</tr>
<tr>
<td><strong>Fiber/Assets</strong></td>
<td>Single purpose/ use fiber</td>
<td>Resource share fiber management</td>
<td>Geolocated fiber asset documentation</td>
<td>Fiber use and availability documentation</td>
<td>Strategic regional and commercial fiber use</td>
</tr>
<tr>
<td><strong>Interoperability</strong></td>
<td>Sole function ITS data/video for a TMC</td>
<td>Intra-agency data/video sharing</td>
<td>Intergovernmental data/video sharing (Traffic/First responders)</td>
<td>Inter-jurisdictional data/video sharing (partner DOTs)</td>
<td>“Open data” seamless-trusted data exchange</td>
</tr>
</tbody>
</table>
DOT Framework
DOT Framework

Traffic Networks
- Operational Technology
- Networks with field devices serving business functions
- Low rate of change
- Limited Internet Access

Business Networks
- Information Technology
- Network supporting users with office products
- High change
- Extensive Internet access

External Networks
- Traffic data consumers and producers
- Need controlled means for exchanging digital data
## Partner and Consumers Networks

<table>
<thead>
<tr>
<th>Internet</th>
<th>Traffic Networks</th>
</tr>
</thead>
</table>
| • Traffic data exchange (bi-directional) with the general public and partners | • Operational Technology  
  • Networks with field devices serving business functions  
  • Low rate of change  
  • Limited Internet Access |

<table>
<thead>
<tr>
<th>Partners</th>
<th>Business Networks</th>
</tr>
</thead>
</table>
| • Partners in multijurisdictional/modal regions benefit heavily from open data exchange with the State DOT’s. The communications touchpoint and data exchange formats vary widely | • Information Technology  
  • Network supporting users with office products  
  • High change  
  • Extensive Internet access |

<table>
<thead>
<tr>
<th>External Networks</th>
<th></th>
</tr>
</thead>
</table>
| • Traffic data consumers and producers  
  • Need controlled means for exchanging digital data |
DOT Business/Enterprise Networks

**DOT Business/Enterprise Network**
- Corporate applications (Office suite, etc)
- Sometimes used to interconnect DOT Traffic Regions/Districts
- Sometimes leveraged as the secure conduit between traffic networks and partner/Internet networks
- Cybersecurity governed by “traditional” cyber-best practices

**Traffic Networks**
- Operational Technology
- Networks with field devices serving business functions
- Low rate of change
- Limited Internet Access

**Business Networks**
- Information Technology
- Network supporting users with office products
- High change
- Extensive Internet access

**External Networks**
- Traffic data consumers and producers
- Need controlled means for exchanging digital data

---

Internet
- Public

Partners
- Jurisdictions
- Media
- Public Safety

DOT Business/Enterprise Network

---

SKYLINE TECHNOLOGY SOLUTIONS
### Traffic Networks

#### Traffic Network
- Usually regional/district dedicated networks
- **Heart of traffic management** – A TMC leveraging their ATMS to conduct vehicle traffic management
- **Field Communications Infrastructure** – Internet Protocol (IP) Everywhere
  - Fiber – switching/routing/MetroE
  - Private Wireless
  - Lease services (TDM/EVPL/LTE/5G/MPLS/...)
- **Field Devices** – IoT before there was IoT (IP versus Non-IP)
  - Camera
  - Lane Control System
  - Speed/weather sensor
  - DMS
  - Other

#### Traffic Networks
- **Operational Technology**
- Networks with field devices serving business functions
- Low rate of change
- Limited Internet Access

#### Business Networks
- **Information Technology**
- Network supporting users with office products
- High change
- Extensive Internet access

#### External Networks
- Traffic data consumers and producers
- Need controlled means for exchanging digital data
TRAFFIC/ITS NETWORK - Journey from Operations/Public Information to Public Safety

**Region/District Traffic/ITS Networks**

**Infrastructure**
- TMC/TOC
  - ATMS
  - Traffic Management
- Field Comms architecture
  - Private (IP/Non-IP)
    - Fiber
    - Wireless
  - Leased – TDM, EVPL, LTE/5G,…
- Field devices/IoT
  - Camera
  - Speed Sensors
  - DMS

**Challenges**
- Operations Challenges
  - Public Communications
  - Reporting
- Siloed architecture
  - Limited scalability
  - Costly resiliency and redundancy
  - Limited capacity
  - Underleverage assets
- Limited Asset Management
  - (scale/growth)
  - Infrastructure health
  - Device availability
  - Wide range of devices
  - Untrusted

**Opportunities**
- Automated/enhanced traffic event detection and traffic management
  - “Local compute” for traffic management
- Comprehensive and secure communications architecture
- Secure data exchange with partners
- Ubiquitous bandwidth
- Scalable Asset Management
  - Infrastructure Health
  - Service-based availability
  - Wide range of devices
  - Secure field infrastructure

**ITS Monitoring**
- ITS Monitoring

**Cybersecurity**
- Cybersecurity
ITS Monitoring
ITS Management Leveraging the ITIL Framework

**Today**
- Cybersecurity concerns
- Limited Network Management
- No Data for Analysis
- Super Hero Support
- Highly Reactive

**Future Innovation:**
- Fiber Asset Management Services
- Video Interoperability & Analytics
- Connected Vehicle Data Hub
- Basic Safety Messages (BSM), SPaT Data Analytics & Applications

**Starting Foundation:**
- Deploy Monitoring, ITIL
- Proactive Asset Lifecycle Management
- Improved Security
- Automation
- Standardization & Rationalization

**Today**
- Cybersecurity concerns
- Limited Network Management
- No Data for Analysis
- Super Hero Support
- Highly Reactive

**CHAOTIC**
- Work is ad-hoc
- Users provide notification
- No infrastructure management

**REACTIVE**
- Component view
- Firefighting
- Alerting
- Formal Incident Management
- Technology silos

**Predictive**
- Workload view
- Prevent and prevent performance problems
- Trending
- Standardized tools

**Service**
- Service view
- Reports at service level
- SLAs in place
- Planning for capacity availability

**Value**
- Business process view
- Reports in business terms
- Measure process and efficiency
- Continual Service Improvement (CSI)
Cybersecurity
Cybersecurity - Do you know where your #2 Key is?

- It’s not just 13-year-old kids hacking your DMS you should concerned about
- ITS infrastructure continues to transition from Operations/Public Information to Public Safety
- Security by obscurity is not a strategy

The number of “things” on the roadside will continue to grow exponentially.
Cybersecurity Approach

Lifecycle, Not Projects

- Develop a customized roadmap for your organization, and then work that roadmap.
- If you already have a roadmap, Skyline can support initiatives from your roadmap throughout the Cybersecurity Lifecycle.
Cybersecurity Approach

Gap Analysis
- On any pre-existing cyber program or policy.
- Adhere to: NIST RMF; NIST 800-171; PCI DSS; HIPAA

Asset and Vulnerability Management -
- Analysis of vulnerabilities to determine the proper scope and approach necessary to fortify the IT infrastructure.

Policy Development
- Utilize risk management framework and common standards such as: NIST, CIS Top 20, ISO 27001

Adoption and Implementation
- Training and communications to educate users of new standards and practices.

Monitor and Evaluation
- Ensure long-term compliance
- Annual updates to policies, technology and documentation.
Developing a Roadmap
Do You Know Where Your IT Assets Are? No, Seriously...

**CIS Controls™**

<table>
<thead>
<tr>
<th>Basic</th>
<th>Foundational</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Inventory and Control of Hardware Assets</td>
<td>7 Email and Web Browser Protections</td>
<td>17 Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>2 Inventory and Control of Software Assets</td>
<td>8 Malware Defenses</td>
<td>18 Application Software Security</td>
</tr>
<tr>
<td>3 Continuous Vulnerability Management</td>
<td>9 Limitation and Control of Network Ports, Protocols, and Services</td>
<td>19 Incident Response and Management</td>
</tr>
<tr>
<td>4 Controlled Use of Administrative Privileges</td>
<td>10 Data Recovery Capabilities</td>
<td></td>
</tr>
<tr>
<td>5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
<td>20 Penetration Tests and Red Team Exercises</td>
</tr>
<tr>
<td>6 Maintenance, Monitoring and Analysis of Audit Logs</td>
<td>12 Boundary Defense</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13 Data Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 Controlled Access Based on the Need to Know</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15 Wireless Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16 Account Monitoring and Control</td>
<td></td>
</tr>
</tbody>
</table>

Center for Internet Security
https://www.cisecurity.org/
Field Communications
Architecture
Field Communications Architecture

Challenge

• Untrusted, limited capacity, security, owned, leased, maturity
• Purpose built solutions, lack of fiber valuation and utilization, siloed architecture, lack of redundancy and resilience.

Opportunity

• Resources Share
  • Maximizing the State’s roadways for establishing the State’s Information Highways
  • 5G Carrier’s need access what can you acquire?
• Architecture
  • Underlay – Creating a common underlying communications leveraging the broad array of possible communications (technologies private fiber/wireless and leased services)
  • Overlay – Support network function virtualization – Ability to logically support and securely separate disparate business functions, such as Tolling, DSRC, Lane Control Systems, other ITS functions.
One Maryland Broadband Network

Challenges

• 3rd largest Stimulus Program ($158M) Development and implementation
• Multi-governmental (150+ organizations) communications architecture
• +1,200 miles of fiber build and
• +1,000 State, County, K-12, Higher Ed, Libraries locations
Underlay versus Overlay

Attributes
- Fiber
- Locations
- Devices
- Providers
- Services
- Customers
- Business functions
Anatomy of an Asset

Fiber
- Where is it? Path - geographic
- How many strands?
- What other fiber is it connected to?

Links
- A and Z End
- Purpose (customer)
- Fiber Quality (distance/dB loss/...)

Customers
- Communications hardware
- Devices
## Where Am I and What Do I Need To Do?

<table>
<thead>
<tr>
<th></th>
<th>Novice</th>
<th>Beginner</th>
<th>Intermediate</th>
<th>Advance</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITS Management</strong></td>
<td>Deploy only</td>
<td>Spreadsheets for tracking</td>
<td>Basic availability monitoring</td>
<td>Capacity management</td>
<td>Strategic planning support</td>
</tr>
<tr>
<td><strong>Cybersecurity</strong></td>
<td>Default settings</td>
<td>Basic configuration</td>
<td>Governance model Hardened based device templates</td>
<td>Proactive monitoring, incident detection</td>
<td>Continuous cybersecurity posture enhancement</td>
</tr>
<tr>
<td><strong>Fiber/Assets</strong></td>
<td>Single purpose/ use fiber</td>
<td>Resource share fiber management</td>
<td>Geolocated fiber asset documentation</td>
<td>Fiber use and availability documentation</td>
<td>Strategic regional and commercial fiber use</td>
</tr>
<tr>
<td><strong>Interoperability</strong></td>
<td>Sole function ITS data/video for a TMC</td>
<td>Intra-agency TMC data/video sharing (Traffic/First responders)</td>
<td>Intergovernmental data/video sharing (Traffic/First responders)</td>
<td>Inter-jurisdictional data/video sharing (partner DOTs)</td>
<td>“Open data” seamless-trusted data exchange</td>
</tr>
</tbody>
</table>
Thank You