## Impacts Assessment to Prepare for Future Transportation System

| Impact Area: Cybersecurity for Vehicle to Infrastructure (V2I) Communications |
| Description |

Vehicle-to-infrastructure communication, or V2I, is the term for wireless communication between connected vehicles (CV) and digital systems linked to transportation infrastructure, usually through communication devices installed near roadways, called roadside units. Vehicle-to-infrastructure communication can utilize dedicated short-range commutations (DSRC), cellular technology or sometimes Wi-Fi.¹

Many experts expect automated vehicles to also use connected vehicle technology. V2I communication could enhance automated vehicle safety, especially in areas with variable rules of the road such as school zones or work zones, and improve the flow of traffic by integrating data about transportation infrastructure, traffic conditions and signal timing with automated driving system behavior.

While emerging transportation technologies could help reduce crashes, congestion, and greenhouse gas emissions, increased utilization of advanced computing systems and software also increases the potential for cyberattacks. Cybersecurity breaches in a CV system could pose immediate safety risks and lead to crashes or other dangerous situations on the road. Because many of the regularly transmitted CV messages include speed and position data, this information could be used to track a specific user, violating the individual’s privacy. In addition, cybersecurity breaches could undermine trust in CV systems; if drivers cannot trust information received through V2I messages, they will be less likely to take action based on those messages, diminishing the safety and efficiency benefits of CV technology.

The U.S. Department of Transportation (US DOT) has identified four elements to securing connected vehicle systems, including vehicle cybersecurity, infrastructure cybersecurity, ITS architecture and standards security, and communications.

---

¹ *Connected Vehicle Impacts on Transportation Planning, Technical Memo #5: Case Studies, US DOT*
security.\textsuperscript{2} The federal government has sole authority to establish cybersecurity standards for vehicles and equipment. This impact assessment examines communications security.

As noted above, DSRC is not the only technology that can be utilized for V2I communications. However, most security research to date has focused on DSRC. In 2018, the Center for Transportation Research noted that DSRC is inherently resilient to some kinds of cyber based attacks. However, the same report notes that, similar to Wi-Fi, it can be susceptible to a wide range of attacks that could result in denial of service, loss of confidentiality, or degraded system integrity. The report acknowledges that more research is necessary to understand these attacks and design compensating measures.\textsuperscript{3}

While no single technology can provide security against all types of attacks, cryptographic systems will assuredly play a major role in ensuring the trustworthiness of V2I communications. To that end, the US DOT and partner organizations have created a proof-of-concept communications security system\textsuperscript{4}, called the Security Credential Management System (SCMS), designed to be used in federal CV pilots. The SCMS uses a public key infrastructure (PKI)-based authentication method to create, manage, distribute, use, store and revoke digital certificates. In the proof-of-concept project, the SCMS issues multiple digital certificates to users and constantly alters the certificates to preserve privacy. The certificates contain no information that could be used to identify individuals or pieces of equipment, but serve as system credentials so that other users can trust their messages. However, a full-scale deployment will require more research, investment and a business model that will sustain the SCMS over time.

The US DOT has identified lessons learned and considerations for an SCMS deployment. Ongoing considerations include how on-board units (OBUs) can trust certificates from more than one authorized entity, the rules specifying how certificates are issued and retired over time, the manner in which certificates

\textsuperscript{2} How the U.S. Department of Transportation Is Protecting The Connected Transportation System from Cyber Threats
\textsuperscript{3} Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems
\textsuperscript{4} National Security Credential Management System – SCMS Baseline Summary Report, US DOT, January 2018
<table>
<thead>
<tr>
<th>Certainty/potential time horizon</th>
<th>V2I technology is already being tested, including in Oregon. The extent to which automated vehicles will be deployed with or will require V2I features is highly uncertain. Deployments of V2I technology will require cybersecurity systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Co-benefits/advancing established goals</strong></td>
<td>To deploy V2I technology, the security of the communications has to be ensured. Securing V2I communications is essential to prevent attacks that, if successful, could lead to crashes and other dangerous road incidents. It is also essential to protect the privacy of individual users. Generally speaking, securing V2I communications is essential to prevent loss of trust in CV systems and ensure the full potential safety and traffic management benefits of CVs are realized.</td>
</tr>
<tr>
<td><strong>Barriers</strong></td>
<td>It is uncertain whether V2I communications will rely on DSRC or 5G technology, which has prevented both private companies and public agencies from investing in CV infrastructure. To date, published research regarding cybersecurity for V2I communications has focused on DSRC technology. It is also uncertain what level of government will have authority to implement and oversee the cybersecurity of V2I communications. For example, laws and regulations defining misbehavior that results in certificate revocation could be set by the federal government or by states and local governments. In either case, multiple departments and multiple levels of government will likely need to coordinate inspections and incident response and to enforce compliance with CV requirements. A full-scale, secure SCMS system would require an ownership and governance model that ensures effective governance and consistent funding. Otherwise, there could be issues with availability and inconsistent services, resulting in varying security, privacy and device standards across components and geographic areas. This could negatively impact interoperability, but it could also create vulnerabilities and expose the system to interference.</td>
</tr>
</tbody>
</table>

---

5 Full-Scale Security Credential Management System (SCMS) Deployment: Workshop Read Ahead

6 Full-Scale Security Credential Management System (SCMS) Deployment: Workshop Read Ahead
Depending on the ownership and governance model, industry competitors may need to participate in the system and would need to work together to ensure the system operates effectively and safely. One example is the payment card industry (PCI), in which competing companies (such as Visa and Mastercard) established a council to set privacy and security standards, run training programs, and annually certify adherence to the standards.

Additional research is required to address some of the cybersecurity vulnerabilities of CV systems, especially vulnerabilities related to interference and confidentiality.

<table>
<thead>
<tr>
<th><strong>Impact to infrastructure owner/operator</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>State and local governments that operate network connected roadside infrastructure already have requirements for implementing security measures. The ability to receive messages from external entities such as a connected vehicle creates additional cybersecurity complexity. The federal government has taken primary responsibility for deploying a security credential management system for CV technology; although development of a system is proceeding slowly. State and local governments will need to implement SCMS technology for infrastructure points where V2I communications is enabled, but this is not possible until national standards and a sustainable business model are defined. Regulating and overseeing cybersecurity for the vehicle end of V2V or V2I communications will likely remain the responsibility of the federal government. However if federal standards don’t develop fast enough to meet needs, state and local governments could be required to take an expanded role in securing V2I and V2V communications.</td>
</tr>
<tr>
<td>Any state or local role in V2I communications security would require building organizational capacity, including hiring and training staff and investing in new systems. State and local agencies would also likely need to establish an ongoing source of funding for efforts related to V2I communications security because outdated CV communications technology could create cybersecurity risks. Contracts with companies with cybersecurity expertise may be required to audit systems and review agency cybersecurity procedures.</td>
</tr>
</tbody>
</table>
| Relevant national guidance/key decision makers | The Intelligent Transportation Systems Joint Program Office (ITS JPO) and the National Highway Traffic Safety Administration (NHTSA) partnered with the automotive industry and security experts through the Crash Avoidance Metrics Partnership (CAMP) to create the SCMS proof-of-concept communications security system for connected vehicles pilots and other federally-funded V2X efforts. The goals for the SCMS project include defining a governance strategy for a full-scale SCMS, establishing an SCMS manager and hierarchy, and identifying roles and responsibilities for all the system participants.\(^7\)  

Another research effort is the European Commission’s Cooperative Intelligent Transportation System Trust Model concept. This concept envisions an infrastructure which provides redundancy and interoperability, allowing for more flexibility in expanding and decentralizing its operations. Initial next steps will include development of a working prototype at the European level. Work on design and implementation of the prototype have already begun.\(^8\) |
|---|---|
| Next steps | Monitor US DOT’s SCMS project for updates and observe AV pilots where the SCMS is used for lesson learned. Implementing CV infrastructure that is compliant with national standards that develop is important for achieving interoperability.  

Develop plans for hiring and developing a workforce with the technical expertise to design, deploy, and maintain V2I equipment and to monitor and mitigate cybersecurity risks. |

---

\(^7\) [Full-Scale Security Credential Management System (SCMS) Deployment: Workshop Read Ahead](https://example.com)  
\(^8\) [European Commission: Intelligent Transportation Systems – Cooperative, Connected and Automated Mobility (CCAM)](https://example.com)