Project No.: P175403

Response to “Request for Comments Connected Cars – Workshop”

Submitted to:
Federal Trade Commission (FTC)

April 20, 2017

Prepared by:
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102

Tel 1 703 902 5000
Fax 1 703 902 3333

www.boozallen.com

April 20, 2017
Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street, SW
Suite 5610 (Annex A)
Washington, DC 20024

Subject: Response to: Request for Comments "Connected Cars – Workshop, Project No. 175403"

Dear Federal Trade Commission:

Booz Allen Hamilton Inc. (Booz Allen) is pleased to submit this response to the Request for Comments related to the planned Connected Cars Workshop in June of 2017.

Booz Allen has been supporting the United States Department of Transportation, the National Highway Traffic Safety Administration, and other related USDOT agencies on research, development, testing, and policy recommendations around connected vehicles and automated vehicles for 10 years. In addition, we have been supporting several automobile manufacturers in thinking about cybersecurity and data analysis in current and future vehicles. We look forward to the opportunity to continue our support in this area by participating and engaging with the FTC and NHTSA as part of the planned workshop this year. If you have any questions about our response, please contact Christopher Hill at hill_christopher@bah.com or 202-203-5411.

Sincerely,

Christopher Hill, PhD
Principal

BOOZ ALLEN HAMILTON INC.

TABLE OF CONTENTS

1.0 INTRODUCTION 1

2.0 RESPONSES TO FTC TOPICS OF INTEREST 1

2.1 What data do vehicles with wireless interfaces collect/store/transmit, and how is the data used and shared? 1

2.2 How do these vehicles integrate data into their functionality? How do consumers benefit from the collection and use of their information? 2

2.3 What are the current roles of vehicle manufacturers, parts suppliers, technology companies, and other stakeholders in collecting data and ensuring security? How are these roles expected to evolve? 3

2.4 What are the vehicle manufacturers' privacy and security policies and practices? How are those policies and practices communicated to consumers? What choices are consumers given about how their data is collected, stored, and used? Who owns the data? 4

2.5 What, if any, privacy and security harms can arise from connected vehicle manufacturers and their service providers' collection and use of data? What is the likelihood of such harms? 4

2.6 What privacy and security issues might arise from consumer operation of connected vehicles, including use of third-party aftermarket products that can plug into vehicle diagnostic systems, geolocation systems, or other data-generating aspects of connected vehicles? 5

2.7 What evidence exists regarding consumer perceptions of connected vehicles and their data collection and use practices? 6

2.8 What are the roles of the FTC, NHTSA, and other federal government agencies with regard to the privacy and security issues concerning connected vehicles? ... 6

2.9 What self-regulatory standards apply to privacy and security issues relating to connected vehicles? 7

3.0 BOOZ ALLEN EXPERIENCE AND EXPERTISE SUMMARY 8

1.0 Introduction

Booz Allen Hamilton (Booz Allen) commends the Federal Trade Commission (FTC) and National Highway Traffic Safety Administration (NHTSA) on working to explore and address consumer privacy and security concerns related to Connected Vehicles (CV) and Autonomous Vehicles (AV). As are most industries today, the transportation ecosystem is faced with increasing privacy and cybersecurity concerns. From private vehicles to commercial airlines, the connectivity of the ever-expanding Internet of Things (IoT) increases the vulnerability of the nation's transportation system to cyberattacks. Increasingly complex and connected transportation platforms and applications are beginning to collect enormous amounts of data that may encroach on the perceived privacy of transportation providers and users. Automakers are investing heavily into connected and automated vehicle research and development, and while great strides have been made to attend to the privacy and security implications of new technologies, more focus on security technology, process development, and testing is needed.

While federal agencies cannot solve all transportation-related cybersecurity and privacy issues through regulation, which may sometimes stifle innovation and the development of new privacy and security controls, agencies can act as trusted partners in developing awareness and providing guidance to protect against malicious cyberattacks and private information leaks. Public agencies can also provide invaluable support through facilitating collaboration among federal organizations, state and local entities, and private industry in relation to how to develop security and privacy controls and protections.

2.0 Responses to FTC Topics of Interest

2.1 WHAT DATA DO VEHICLES WITH WIRELESS INTERFACES COLLECT/STORE/TRANSMIT, AND HOW IS THE DATA USED AND SHARED?

Select automakers can stream or request data from vehicles via their telematics infrastructure (e.g., GM OnStar, Subaru STARLINK) and the rest of the industry is quickly following suit. These systems can collect Data Item Descriptions (DIDs) and Parameter IDs (PIDs) which can include odometer readings, part numbers, diagnostic trouble codes, specific driving behavior (e.g., hard braking events, trip information), and much more. Usually this type of data is available to the registered consumer through an online account. In regard to data sharing, OnStar's current privacy statement provides examples on how this data is currently shared with the GM family of companies, emergency service providers, business partners and independent third parties, service providers, where required by law, and business transfers. OnStar provides certain choices regarding how data is used and shared, such as for marketing or to determine insurance discount eligibility.

These types of data can be used to help detect cybersecurity incidents and anomalies through development of analytics-based vehicle Intrusion Detection Systems (IDS), which Booz Allen developed for a global automaker. Vehicle cyber analysts and engineers can use the purpose-built data stream's analytical engine with machine learning algorithms to gain an understanding of normal system behavior to then identify malicious and potentially fraudulent activity.

The potential NHTSA forthcoming regulation on mandating V2V communications ability (see NHTSA NPRM), if enacted, will have the eventual effect that all light vehicles on the road (upwards of 350 million currently) will be generating gigabytes of data every day. These data will be exchanged with other vehicles and roadside infrastructure, and possibly back end systems, such as Traffic Management Centers. How the data will be protected, who will own the data, where it

will be stored, and who will control or govern these security and privacy concerns are all areas that are still to be determined. As part of the NPRM, NHTSA worked with the auto industry to develop a security management system to ensure privacy by design and limited/controlled access to data. However, governance, oversight, and policies related to this system (SCMS) are still to be determined and the roles of different players in managing and operating it are also yet to be established. It is reasonable to expect that shared governance, with roles for all major stakeholders will be part of that eventual system.

Automated vehicles have the potential to further increase the collection, storage, and sharing of data. A wide variety of data types used by and generated by AVs are important to consider:

- Safety data (e.g., edge cases, near-misses, early warning reporting, crash reconstruction)
- System maintenance and monitoring (e.g., over-the-air firmware/software updates, prognostics),
- Traffic operations (e.g., speed harmonization, signal priority, routing, incident management), and
- Situational awareness (e.g., high definition maps, objects and events, cooperative localization).

These data may eventually be shared across industry, between public and private entities, or within a single company. New legal frameworks for data partnerships and privacy regulations will need to be developed to manage the complex data ecosystem necessary for maximizing the benefit of AV deployment and widespread adoption.

2.2 HOW DO THESE VEHICLES INTEGRATE DATA INTO THEIR FUNCTIONALITY? HOW DO CONSUMERS BENEFIT FROM THE COLLECTION AND USE OF THEIR INFORMATION?

Vehicles that are currently available to consumers integrate data into their functionality in a number of ways, usually to improve safety and performance of the vehicle, or to provide additional services to the user. It is important to note that most of this existing data integration does not adjust the course of a vehicle in motion. Consumer benefits currently available include enhanced mobility options, such as rerouting based on congestion, vehicle maintenance notifications, and lane change warnings, etc. Few makes and models also integrate automated controls based on the use of the data and the embedded applications.

In the future, autonomous vehicles, and automated operations within user-driven vehicles will take independent actions based on data from external sources (e.g., Signal Phase and Timing [SPaT] information from connected traffic signals, lane change warnings). Select vehicles equipped with sensors and radar are already taking action with input from the driver based on collected data. It is critical that vehicle systems have the ability to authenticate data used by the vehicle, from internal sensors and external sources, to act autonomously.

As automated capabilities within vehicles become more widespread across multiple makes and models, and more V2V and V2I connectivity comes online, more opportunities for data collection, storage, transmission, and usage will arise. The data have many potential functional applications that produce benefits, including:

- Increased safety through improving situational awareness (e.g., identifying objects and events), defects in vehicle systems, and communal learning of security and performance threats and vulnerabilities

- Improved mobility and energy consumption through optimizing traffic management and vehicle performance
- Reducing cost through decentralized computing and sensing of the environment, i.e., less onboard processor and sensor requirements

How the data will be integrated and protected are issues that will need clear processes and safeguards.

2.3 WHAT ARE THE CURRENT ROLES OF VEHICLE MANUFACTURERS, PARTS SUPPLIERS, TECHNOLOGY COMPANIES, AND OTHER STAKEHOLDERS IN COLLECTING DATA AND ENSURING SECURITY? HOW ARE THESE ROLES EXPECTED TO EVOLVE?

Right now, these roles are not clearly defined and differ among the automakers and their supply chains. Who has the responsibility and authority to take on various data and privacy protection roles will need to be clearly defined and encompass the end to end design and management of data security and privacy protections. Given that the federal government has not passed a rule or mandate around how data is to be used and protected in these environments, the responsibility has by default fallen to the auto manufacturers. However, the extent of action and data privacy and protection policies differ across the various companies that are contending with the issue and implementing new connected systems within vehicles.

Organizations and consortia such as the Alliance of Automobile Manufacturers (Auto Alliance) and the Automotive Information Sharing and Analysis Center (Auto-ISAC), which Booz Allen helped to stand-up and continues to support, are helping to clarify the cybersecurity and privacy roles and responsibilities of automakers to enhance cybersecurity awareness and coordination across the global automotive industry. While each supplier and technology company within the automotive supply chain has an inherent responsibility to design security and privacy controls within their products and components, roles and responsibilities within each automaker's supply chain may differ based on their unique strategies and business models.

The Federal government can help to shape these roles and responsibilities through:

- Ensuring consumer privacy in a required environment (e.g., V2V communications rule)
- Providing guidelines and best practices (e.g., National Institute for Standards and Technology (NIST) Risk Management Framework (RMF), NHTSA Cybersecurity Best Practices for Modern Vehicles)
- Supporting research and development for early innovation and bringing systems beyond initial concepts
- Providing support for standards development
- Support adoption of technologies, standards, frameworks, and processes with pilot programs and other deployments
- Convening stakeholders, such as in the FTC and NHTSA Connected Cars Workshop
- Managing certain types of data, such as crash data and early warning reporting

We expand on the Federal role in Section 2.8.

2.4 WHAT ARE THE VEHICLE MANUFACTURERS' PRIVACY AND SECURITY POLICIES AND PRACTICES? HOW ARE THOSE POLICIES AND PRACTICES COMMUNICATED TO CONSUMERS? WHAT CHOICES ARE CONSUMERS GIVEN ABOUT HOW THEIR DATA IS COLLECTED, STORED, AND USED? WHO OWNS THE DATA?

In November 2014, the Association of Global Automakers (Global Automakers), the Auto Alliance, and associated members committed to a set of Privacy Principles related to customer data based on the FTC's Fair Information Practice Principles (FIPPs). These principles represent a proactive effort by the industry to commit to a consistent approach to privacy protection. The companies that adopted this framework committed to following seven fundamental elements: transparency; choice; respect for context; data minimization, de-identification, and retention; data security; integrity and access; and accountability. These principles are further expanded within the agreed upon framework. Of course, automakers also follow guidance from other regulatory bodies, such as the Federal Communications Commission, as their products increasingly cross regulatory responsibility boundaries.

Some OEMs are beginning to engage directly with consumers on how data is collected, stored and used – per the Privacy Principles. For example, according to the OnStar privacy statement, GM provides the consumer options to opt out of sharing certain types of data. These types of statements and options should be the standard across the industry and specifically disclosed to the buyer during the vehicle purchasing process.

There is still a gap in terms of data ownership. While the automakers are working toward the new Privacy Principles, ownership of the data generated by the vehicle operator/owner has still not been fully addressed.

2.5 WHAT, IF ANY, PRIVACY AND SECURITY HARMS CAN ARISE FROM CONNECTED VEHICLE MANUFACTURERS AND THEIR SERVICE PROVIDERS' COLLECTION AND USE OF DATA? WHAT IS THE LIKELIHOOD OF SUCH HARMS?

There are two basic categories of potential security and privacy harm to the consumer arising from vehicle connectedness: 1) wireless intrusion into the actual vehicle or communication transmissions to extract information or inject false information and 2) leaks or unauthorized extraction of consumer data (e.g., trip information, driving behavior) in the automakers back end systems. The most serious harms can arise from actual intrusions into a vehicle. Security researchers have displayed the ability to hack vehicles (e.g., Jeep[1], Tesla[2]) and manipulate vehicle systems while in operation. This could potentially lead to hackers taking over a vehicle to cause physical harm to the driver and passengers of the hacked vehicle, or other drivers and pedestrians. In this category, a more likely concern is the installation of ransomware which could require payment to the hacker to release the vehicle back to the owner or operator. Other likely scenarios could be the manipulation of sensors and systems to eavesdrop on the consumer by activating a vehicle microphone and/or camera or the extraction of vehicle-linked consumer data such as contact information and/or payment information. While these new vulnerabilities and threats may not be the direct result of data collection and use (as the question is posed), the new connected systems that collect and use data introduce new attack vectors. The table below contains a non-exhaustive list of potential threats or avenues of attack on a connected vehicle.

---

[1] Greenberg, A. (August 1, 2016). "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse." Wired. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[2] Peterson, A. (September 20, 2016). "Researchers Remotely Hack Tesla Model S." Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/

Connected Vehicle Threats
An attacker learns information using a non-invasive attack such as a side channel attack and/or cryptanalysis of algorithms and signed messages.
An attacker learns information using an invasive software attack such as malware (available on Internet for example) that exploits vulnerabilities in algorithms and software.
An attacker learns physically protected restricted information from connected systems, such as private keys, using a physical attack.
An attacker replays system message at a different (than original) time and/or location.
An attacker modifies the sensor inputs on a single vehicle before the vehicle uses them to generate and send system messages.
An attacker modifies the sensor inputs to multiple vehicles before the vehicles use them to generate and send system messages. (For example, by GPS spoofing).
An attacker uses learned system information or communications transmissions to track a vehicle.
An attacker installs malware on a vehicle that prevents receiving, or making use of, or providing user interaction based on system messages.
An attacker uses connected vehicle sensors as an attack vector on the rest of the vehicle.

Less of an immediate safety concern but more probable is the inadequate protection of or inadvertent release of consumer data from an automaker's back end systems, data storage platforms, and data sharing relationships. There is potential for a consumer's PII, specific trip information, travel habits, driving behavior, and more to be accidently shared or maliciously extracted. These types of hacks and data spills are already commonplace among the consumer industry (e.g., payment system hacks) and even government (e.g., OPM data hack).

2.6 WHAT PRIVACY AND SECURITY ISSUES MIGHT ARISE FROM CONSUMER OPERATION OF CONNECTED VEHICLES, INCLUDING USE OF THIRD-PARTY AFTERMARKET PRODUCTS THAT CAN PLUG INTO VEHICLE DIAGNOSTIC SYSTEMS, GEOLOCATION SYSTEMS, OR OTHER DATA-GENERATING ASPECTS OF CONNECTED VEHICLES?

Privacy and security issues are much the same as those listed in 2.5, except additional risks are taken when using aftermarket systems and parts for a vehicle that was engineered without those systems and parts in mind. When introducing a line of communication into and out of a vehicle, no matter the interface, there will be additional risks to consumer privacy and security. Third-party aftermarket products, such as those that plug into the OBD-II port (e.g., Verizon Hum+, Progressive Snapshot), bring about new security and privacy questions that should not necessarily be grouped with factory vehicle privacy and cybersecurity considerations. These aftermarket products are not designed or controlled by the automakers. Securing aftermarket systems and products should be considered as a separate case from securing factory vehicles and protecting consumer data as these systems can add additional attack vectors into the vehicle while also streaming data to someone other than the automaker.

The automaker can only do so much to protect the vehicle from cyberattacks while also protecting unique data generated by the vehicle and consumer. The manufacturer cannot control the actions of the owner, just like it cannot control the driving habits of the operator. As long as vehicle manufacturers take steps to secure vehicle systems and protect consumer generated data per guidance being developed by SAE, NHTSA, and other organizations, this is the most that can be done by the manufacturer to ensure adequate security and privacy protection. However, manufacturers can take steps to discourage and limit these threats by invalidating portions of warranties when certain vehicle systems have been modified and implementing firewalls that limit data inputs as well as data extraction by plug-in aftermarket systems. Right-to-repair laws and the openness required for the OBD-II port will continue to pose unique security considerations. These laws and standards may need to be reassessed, from a cybersecurity perspective, given

the leaps in implemented vehicle technology and connected systems (internal and external to the vehicle).

2.7 WHAT EVIDENCE EXISTS REGARDING CONSUMER PERCEPTIONS OF CONNECTED VEHICLES AND THEIR DATA COLLECTION AND USE PRACTICES?

While most consumers do not put a lot of thought into cybersecurity and privacy concerns with connected vehicles, the increasing press coverage of vehicle hacks, such as the Jeep hack, and almost daily hacks of connected systems in other industries are causing more concern. The steadily increasing availability of automated features are welcome safety features in the eyes of most consumers. However, the public is more cautious in their comfort levels with ceding operational control to vehicles with increasing levels of automation (i.e., SAE levels 3, 4, and 5) due to concerns with technology maturity and cybersecurity.

Privacy seems to be less of a concern for most consumers. Results from previous NHTSA V2V Public Acceptance Market Research Focus groups stated, "Privacy was less of a concern than we predicted; participants rationalized that they are already being tracked on a daily basis (cell phones, Google, etc.), but were uneasy about where this might all go." Consumers understand that their data is being collected, but the concern is more of how and with whom it is shared. Of course, consumers still demand privacy of data such as PII and the content of communications, but seem less concerned with sharing of data that provides them direct benefits (e.g., sharing location data to receive faster routes when considering traffic in navigation applications).

2.8 WHAT ARE THE ROLES OF THE FTC, NHTSA, AND OTHER FEDERAL GOVERNMENT AGENCIES WITH REGARD TO THE PRIVACY AND SECURITY ISSUES CONCERNING CONNECTED VEHICLES?

The perspective on the role of government in cybersecurity differs based on the industry and stakeholder, especially in regard to mandated regulations for cybersecurity and privacy. Most automakers do not want mandated cybersecurity regulation but have a favorable position for high-level federal guidance on cybersecurity and privacy, support in research and development, standards development participation, and pilot deployment support. However, state and local governments may favor regulation to ease their burden on managing ITS and related cybersecurity. For the most part, the industry prefers to develop their own standards through organizations such as the Society of Automotive Engineers (SAE) or Institute of Electrical and Electronics Engineers (IEEE), with input and collaboration from the USDOT and other federal agencies. There are currently multiple collaborative efforts (refer to 2.9) to develop standard security control guidance that can be applied to most of the industry.

While the automotive industry seems to agree on the role of federal agencies in vehicle cybersecurity and privacy, the industry differs in opinion on the role of government regulation in external or independent security research and management of the CV Security Credentials Management System (SCMS). For example, during the NHTSA Vehicle Cybersecurity Roundtable (January 19, 2016), select OEMs stated that it should be illegal for "white hat" hackers and security researchers to search for and exploit vehicle cybersecurity vulnerabilities. Other OEMs at the roundtable noted that independent security researchers could be helpful in identifying and patching vulnerabilities. This is likely an area that could benefit from some defined regulations or guidance for security researchers, particularly around disclosure of vulnerabilities and potential threats. Also, automakers differ on the preferred level of USDOT involvement in managing and overseeing the SCMS. Some automakers would like to run their own Certificate Management Entities (CMEs), while others prefer that NHTSA or another external organization handle certificate management.

Federal agencies can choose from a wide spectrum of approaches to use to meet automotive safety, security, and privacy objectives. The range of approaches spans from promulgating regulations (prescriptive), to publishing guidance and/or policies, to recommended best practices, to deference to industry practices (not at all prescriptive), among others. Federal automotive cybersecurity regulations will likely limit innovation and competition. Also, cybersecurity is a moving target. Vehicle cybersecurity regulations mandated in 2018 would likely be outdated and possibly completely obsolete by 2020. However, federal agencies should provide guidance and best practices on how to secure vehicle systems. There are already numerous security standards, while not completely automotive focused, that automakers can reference while designing security into their vehicle systems. The federal agencies should also collaborate with the Auto-ISAC to develop new guidance and updated best practices based on new technology, threats, and mitigation strategies. In regard to privacy, federal agencies could potentially take a stronger regulatory stance. For example, the government could mandate the disclosure of data collection information to consumers and the ability to opt out of data collection activities where possible.

2.9 WHAT SELF-REGULATORY STANDARDS APPLY TO PRIVACY AND SECURITY ISSUES RELATING TO CONNECTED VEHICLES?

There are many self-regulatory organizations and standards available for automakers to reference when considering privacy and security controls for CV/AV. The key is assessing risk through evaluating the impact of threats and potential mitigation activities to inform the development of a privacy and security strategy. The following list contains examples of a few existing self-regulatory organizations and standards, of which many automakers are already contributing members.

- IEEE Vehicular Technology and Intelligent Transportation Systems Societies
  - IEEE 1609.2 WAVE-Security Services for Applications and Messages (V2X communications security)
- SAE Vehicle Electrical System Security Committee
  - SAE 3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
  - SAE 3101, Hardware-Protected Security Requirements for Ground Vehicles
- Auto-ISAC
  - Automotive Cybersecurity Best Practices focused on security by design, risk assessment and management, threat detection and protection, incident response, collaboration and engagement with appropriate third parties, governance, awareness and training
- Auto Alliance and Global Automakers
  - Privacy Principles (discussed in 2.4)
- NIST
  - Framework for Cyber-Physical Systems
- Cyber-Physical Systems Task Force formed by auto researchers and engineers through the U.S. Council for Automotive Research (USCAR) as a means of providing the National Science Foundation's cyber-physical systems initiative with insight into automotive security solutions
- Automotive Consortium for Embedded Security (ACES), organized and operated by the Southwest Research Institute
- National Telecommunications and Information Administration's (NTIA) Multi-stakeholder Collaboration on Vulnerability Research Disclosure, which aims to improve coordination between industry cybersecurity stakeholders and security researchers

Regarding internal systems and the sharing of data, there are a plethora of resources that an organization can use to develop information security programs to protect against hacks and data spills – in addition to guidance from SAE and the Auto-ISAC. A few examples include:

- NIST Risk Management Framework
- ISO 15408, Common Criteria for Information Technology Security Evaluation
- Control Objectives for Information and Related Technologies (COBIT)

3.0 Booz Allen Experience and Expertise Summary

Booz Allen leverages some of the deepest and broadest cybersecurity capabilities in the industry. The firm's cyber expertise includes a 20-year history in providing cybersecurity services protecting critical infrastructure, in both the federal and commercial sectors. Booz Allen has provided long term support to the USDOT on all aspects of connected and automated vehicle and data programs, including the development of a security system and privacy/security requirements for the USDOT CV mandate and for the Tampa CV Pilot. The firm also has extensive expertise in back end transportation systems, and management of large database access, such as the CV Operational Data Exchange. We have also researched vehicle event data recorder technologies, costs, and benefits.

Booz Allen is also an established partner in helping civil, defense, and commercial clients incorporate vehicle automation throughout their missions, such as:

- Supporting US DOT's Automation program, including efforts on technology forecasting, technical standards planning and development, and safety assurance
- Supporting the National Academies in developing CV/AV deployment guidance for states and localities
- Providing automated vehicle systems engineering and deployment support to defense and security clients, including Army, Air Force, DHS, Coast Guard, and others
- Developing unmanned ground and aerial platforms for a broad range of defense, civil, and commercial applications through our Robotics Lab in Arlington, VA
- Supporting CV/AV energy efficiency projects at the Department of Energy

Our team includes experts that sit on CV/AV related professional committees at IEEE, SAE, and Transportation Research Board. Members of our team have crafted CV/AV privacy and security legislation and served as legislative liaisons with the Government Accountability Office on CV/AV privacy and security studies.

In recent years, Booz Allen has become a trusted cybersecurity partner to automakers, with insight and expertise on numerous manufacturers, OEMs.

- Launched and operationalized the Auto-ISAC
- Worked with Auto-ISAC members to develop industry best practices for vehicle cybersecurity
- Worked with multiple automotive OEMs to assess and design vehicle cybersecurity programs

Booz Allen is investing over $8M a year in Cyber Innovations that will help address the rapidly changing landscape of cybersecurity, including a major investment in securing Cyber-Physical Systems (CPS), blended ecosystems of information technology and operational technology systems, that will rapidly grow within the transportation industry. Example resources include:

- Cyber Assurance Testing Lab – virtually-connected network of centers and labs equipped with unique tools and expertise needed to counter 21st century cyber threats. This network's capabilities include four service areas: advanced cyber analytics, computer network defense, product testing and evaluation, and comprehensive cyber training
- Dark Labs – an elite team of security researchers, penetration testers, and reverse engineers that develop advanced cyber tradecraft and tools, and teach this tradecraft in the classroom
- Cyber4Sight and ThreatBase – customized, comprehensive cyber protection solutions using a combination of on-site threat monitoring, threat-base knowledge, 24x7 intelligence analysis, continuous monitoring and other tools to keep organizations ahead of the next attack, including a repository of cyber threat intelligence on threat actors, actor relationship finders, link and timeline analysis, metadata ingestion and tagging, and pattern recognition
- Over 400 professional hackers with a variety of niche subject matter expertise across the embedded, RF/wireless, network, and mobile domains
- Extensive reach back capability to over 5,000 cybersecurity experts with a variety of specialized skills

Summary of Privacy and Security Experience in the Health Domain

Booz Allen supports health-related policy and requirements development, researches and addresses privacy and security concerns, and participates in multiple meetings as privacy and security subject matter experts. Example client engagements include:

- Defense Health Agency (DHA)
  - Led the development and deployment of the Compliance Risk Assessment Program, an approach that transitions DHA from multiple single-focus assessments to one comprehensive assessment that integrates requirements from the Privacy Act and the HIPAA Privacy and Security Rules
  - Supported the development of a Risk Management Program, including the annual performance of a HIPAA Security Risk Assessment, driven by the requirements in the HIPAA Security Rule and DoDI 8580.02
  - Currently updating the HIPAA risk assessment process to incorporate the DoD RMF, the Privacy Overlay, and the transition to NIST SP 800-53 controls
  - Researched and analyzed regulations applicable to the Cerner's Electronic Health Record (EHR), Virtual Lifetime Electronic Record (VLER), and Health Information Exchange (HIE) initiatives
  - Drafted privacy and security policies identified by the Privacy Office as necessary to appropriately implement emerging technologies
  - Responded to ad hoc inquiries from the Services and military treatment facilities with respect to privacy implications presented by emerging technologies
- U.S. Department of Veterans Affairs
  - Supported the protection of patient data exchanged with the VA, a critical step in successfully managing beneficiary information and care between the Military Health System (MHS) and the VA
  - Increased interoperability and HIE, combined with the urgency of managing patient care, has changed the landscape of care and information management at the MHS
  - Monitored developments concerning this issue in support of the DHA Privacy Office's need to balance the requirement for increased availability of data while ensuring the confidentiality of patient information