United States Government Accountability Office

Report to Congressional Requesters

March 2016

VEHICLE CYBERSECURITY

DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack

This Report Is Temporarily Restricted Pending Official Public Release.

GAO-16-350

GAO Highlights

Highlights of GAO-16-350, a report to congressional requesters

March 2016

VEHICLE CYBERSECURITY

DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack

Why GAO Did This Study

Over time, the amount of software code in vehicles has grown exponentially to support a growing number of safety and other features. However, the reliance on software to control safety-critical and other functions also leaves vehicles more vulnerable to cyberattacks.

GAO was asked to review cybersecurity issues that could impact passenger safety in modern vehicles. This report addresses, among other things, (1) available information about the key cybersecurity vulnerabilities in modern vehicles that could impact passenger safety; (2) key practices and technologies, if any, available to mitigate vehicle cybersecurity vulnerabilities and the impacts of potential attacks; (3) views of selected stakeholders on challenges they face related to vehicle cybersecurity and industry-led efforts to address vehicle cybersecurity; and (4) DOT efforts to address vehicle cybersecurity.

GAO reviewed relevant existing regulations and literature and interviewed officials from DOT; the Departments of Commerce, Defense, and Homeland Security; industry associations; and 32 selected industry stakeholders, including automakers, suppliers, vehicle cybersecurity firms, and subject matter experts. The experts were selected based on a literature search and stakeholder recommendations, among other things.

What GAO Recommends

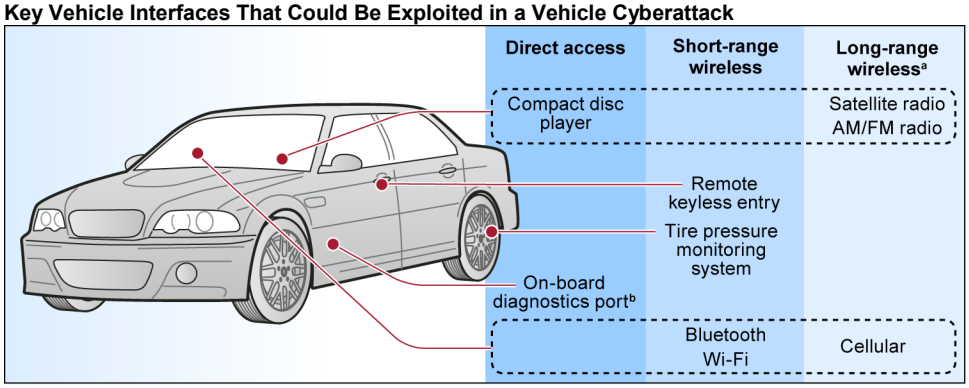
GAO recommends that DOT define and document its roles and responsibilities in response to a vehicle cyberattack involving safety-critical systems. DOT concurred with our recommendation.

View GAO-16-350. For more information, contact David J. Wise at (202) 512-2834 or wised@gao.gov.

What GAO Found

Modern vehicles contain multiple interfaces—connections between the vehicle and external networks—that leave vehicle systems, including safety-critical systems, such as braking and steering, vulnerable to cyberattacks. Researchers have shown that these interfaces—if not properly secured—can be exploited through direct, physical access to a vehicle, as well as remotely through short-range and long-range wireless channels. For example, researchers have shown that attackers could compromise vulnerabilities in the short-range wireless connections to vehicles' Bluetooth units—which enable hands-free cell phone use—to gain access to in-vehicle networks, to take control over safety-critical functions such as the brakes. Among the interfaces that can be exploited through direct access, most stakeholders we spoke with expressed concerns about the statutorily mandated on-board diagnostics port, which provides access to a broad range of vehicle systems for emissions and diagnostic testing purposes. However, the majority of selected industry stakeholders we spoke with (23 out of 32) agreed that wireless attacks, such as those exploiting vulnerabilities in vehicles' built-in cellular-calling capabilities, would pose the largest risk to passenger safety. Such attacks could potentially impact a large number of vehicles and allow an attacker to access targeted vehicles from anywhere in the world. Despite these concerns, some stakeholders pointed out that such attacks remain difficult because of the time and expertise needed to carry them out and thus far have not been reported outside of the research environment.

Key Vehicle Interfaces That Could Be Exploited in a Vehicle Cyberattack



Source: GAO analysis of stakeholder interviews and Checkoway et al, 2011. | GAO-16-350

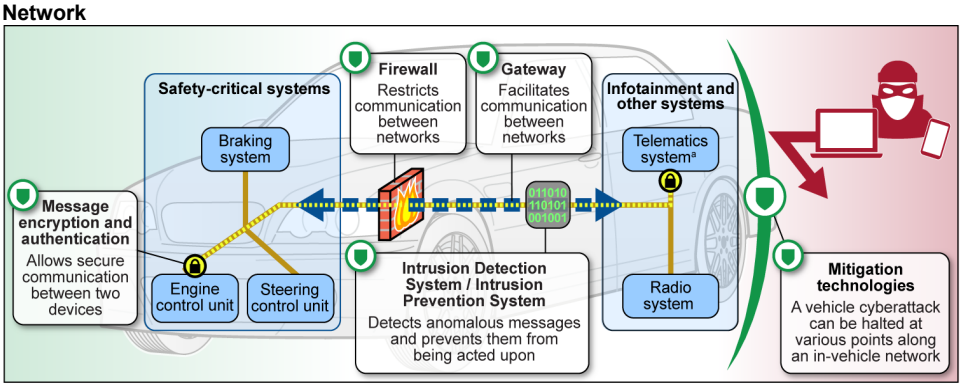
[a]In this context, long-range refers to access at distances over 1 kilometer.

[b]This port is mandated in vehicles by statute for emission-testing purposes and to facilitate diagnostic assessments of vehicles, such as by repair shops. 42 U.S.C. § 7521(a)(6).

Selected industry stakeholders, both in the United States and Europe, informed GAO that a range of key practices is available to identify and mitigate potential vehicle-cybersecurity vulnerabilities. For instance, the majority of selected industry stakeholders we spoke with (22 out of 32) indicated that—to the extent possible—automakers should locate safety-critical systems and non-safety-critical systems on separate in-vehicle networks and limit communication between the two types of systems, a concept referred to as "domain separation." However, some of these stakeholders also pointed out that complete separation

is often not possible or practical because some limited communication will likely need to occur between safety-critical and other vehicle systems. In addition, selected industry stakeholders we spoke to identified technological solutions that can be incorporated into the vehicle to make it more secure. However, according to stakeholders, many of these technologies—such as message encryption and authentication, which can be used to secure and verify the legitimacy of communications occurring along in-vehicle networks—cannot be incorporated into existing vehicles. Rather, such technologies must be incorporated during the vehicle design and production process, which according to stakeholders, takes approximately 5 years to complete.

Example of a Vehicle's Cybersecurity-Mitigation Technologies Shown along an In-Vehicle Network



Source: GAO analysis of stakeholder information. | GAO-16-350

[a]Vehicle "telematics systems"—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

Selected industry stakeholders identified several challenges they face related to vehicle cybersecurity. For instance, the lack of transparency, communication, and collaboration regarding vehicles' cybersecurity among the various levels of the automotive supply chain and the cost of incorporating cybersecurity protections into vehicles were the two most frequently cited challenges—mentioned by 15 and 13 of the 32 selected industry stakeholders, respectively. However, several industry-led efforts are planned and under way that, according to stakeholders, could potentially help automakers and parts suppliers identify and mitigate vehicle cybersecurity vulnerabilities and address some of the challenges that industry stakeholders face. For example, two U.S. industry associations have been leading the effort to establish an Automotive Information Sharing and Analysis Center (ISAC) to collect and analyze intelligence information and provide a forum for members to anonymously share threat and vulnerability information with one another. Selected industry stakeholders we spoke to, as well as DOT officials, generally expressed positive views regarding the potential effectiveness of an Automotive ISAC.

The Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) has taken steps to address vehicle cybersecurity issues but has not determined the role it would have in responding to a real-world vehicle cyberattack. For example, NHTSA added more research capabilities in this area and is developing guidance to help the industry determine when cybersecurity vulnerabilities should be considered a safety defect, and thus merit a recall; it expects to issue this guidance by March 31, 2016. Further, pursuant to a statutory mandate, NHTSA is examining the need for government standards or regulations regarding vehicle cybersecurity. However, officials estimated that the agency will not make a final determination on this need until at least 2018. Although NHTSA's stated goal is to stay ahead of potential vehicle-cybersecurity challenges, NHTSA has not yet formally defined and documented its roles and responsibilities in the event of a real-world cyberattack. Until it develops such a plan, in the event of a cyberattack, the agency's response efforts could be slowed as agency staff may not be able to quickly identify the appropriate actions to take.

Contents

Letter		1
	Background	6
	Remote Attacks Involving Safety-Critical Vehicle Systems Could Have the Greatest Impact on Passenger Safety	12
	A Variety of Key Practices and Technologies Are Available to Mitigate Vehicle Cybersecurity Vulnerabilities and the Impacts of Potential Attacks	20
	Stakeholders Face Challenges Related to Vehicle Cybersecurity, Some of Which May Be Addressed by Industry-Led Efforts	25
	DOT Has Made Progress in Addressing Vehicle Cybersecurity, but Has Not Yet Defined and Documented Its Roles and Responsibilities in Responding to a Vehicle Cyberattack	32
	Conclusions	43
	Recommendation	43
	Agency Comments	44
Appendix I	Objectives, Scope, and Methodology	47
Appendix II	Comments from the Department of Transportation	53
Appendix III	GAO Contact and Staff Acknowledgments	55

Tables

Table 1: Key Practices to Identify and Mitigate Vehicle Cybersecurity Vulnerabilities Identified by Industry Stakeholders	21
Table 2: Summary of Vehicle Security Layers and Examples of Technologies Identified by Stakeholders That Can Be Applied to Mitigate Impacts of Vehicle Cyberattacks	23
Table 3: Examples of Recently Completed and Ongoing National Highway Traffic Safety Administration (NHTSA) Vehicle Cybersecurity Research by Priority Area	33
Table 4: Selected Industry Stakeholders Interviewed	49

Figures

Figure 1: Depiction of Reduced Wiring Enabled by an In-Vehicle Communication Network 8
Figure 2: Average Lines of Software Code in Modern Luxury Vehicle Compared to Types of Aircraft 9
Figure 3: Key Interfaces That Could Be Exploited in a Vehicle Cyberattack 14
Figure 4: Example of a Potential Vehicle Cyberattack Launched through a Short-Range Wireless Interface, as Demonstrated by Researchers 16
Figure 5: Example of a Potential Vehicle Cyberattack Launched through a Long-range Wireless Interface, as Demonstrated by Researchers 17
Figure 6: Example of a Vehicle's Cybersecurity-Mitigation Technologies Shown along an In-Vehicle Network 24

Abbreviations

AUTOSAR	Automotive Open System Architecture.
CAN	controller area network
DHS	Department of Homeland Security
DOT	Department of Transportation
ECU	electronic control unit
FAST Act	Fixing America's Surface Transportation Act
FCA	Fiat Chrysler Automobiles
GM	General Motors
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	information technology
MAP-21	Moving Ahead for Progress in the 21st Century Act
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OBD-II	on-board diagnostics port
OTA	over-the-air
SAE	Society of Automotive Engineers
VRTC	Vehicle Research and Test Center

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 24, 2016

Congressional Requesters

Over the past decade, the amount of software code in passenger vehicles has increased significantly.[1] In today's vehicles, software code supports both core driving functions, such as braking and steering, as well as advanced safety and convenience features, including adaptive cruise control, forward collision-warning systems, and built-in navigation and Bluetooth systems. The amount of software code in vehicles is expected to continue to increase with the introduction of more advanced and automated features that have the potential to reduce crashes and save lives.[2] Despite the safety and convenience benefits offered by some electronically controlled systems, researchers and others have noted that as the lines of vehicle software code increase, so does the potential for cybersecurity vulnerabilities that could be exploited through vehicle cyberattacks or "hacking."

Since 2011, researchers have been demonstrating the feasibility of hacking into vehicles' electronic systems, including hacking from a remote location. For example, in July 2015, two researchers exploited software vulnerabilities in a Jeep Cherokee's" telematics" unit[3] to remotely take

[1]Passenger vehicles include passenger cars, vans, sport-utility vehicles, and pick-up trucks with a gross-vehicle weight rating of 10,000 pounds or less.

[2]NHTSA defines 5 levels of automation ranging

- from "no automation," in which the driver is in complete and sole control of the primary vehicle controls—brake, steering, throttle, and motive power—at all times,
- to "full self-driving automation," in which the vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for the entire trip.

[3]The term "telematics" refers to a technology that combines telecommunications and information processing in order to send, receive, and store information related to remote objects, such as vehicles. Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections. They provide a broad range of features, including some supporting safety (such as the ability to report a crash), diagnostics (such as the ability to receive early alerts of mechanical issues), and convenience (such as hands-free access to driving directions or weather).

control of safety-critical systems—including manipulating the brakes—without prior physical access to the target vehicle.[4] Shortly after this hacking demonstration was reported, the manufacturer Fiat Chrysler Automobiles (FCA) announced the recall of about 1.4 million impacted vehicles, including other models known to have similar vulnerabilities.

The Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) is responsible for overseeing recalls; developing, setting, and enforcing Federal Motor Vehicle Safety Standards and regulations; and conducting research that supports vehicle safety, including research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems.[5] Since 2011, part of this research has focused specifically on automotive cybersecurity, which is intended to ensure that vehicle systems and components that govern safety are protected from malicious attacks, unauthorized access, damage, or other factors that could interfere with safety functions.

In light of growing questions about the potential for vehicle cyberattacks, you asked us to review issues related to vehicle cybersecurity. This report examines:

- available information about the key cybersecurity vulnerabilities in modern vehicles that could impact passenger safety;
- key practices and technologies, if any, available to mitigate vehicle cybersecurity vulnerabilities and the impacts of potential attacks;
- views of selected stakeholders on challenges they face related to vehicle cybersecurity and industry-led efforts to address vehicle cybersecurity; and
- DOT efforts to address vehicle cybersecurity.

Although vehicle cybersecurity vulnerabilities, if found, could be exploited for various reasons, we focused on those vulnerabilities that could impact

[4]Although the researchers did not have prior physical access to the vehicle that was the subject of the hacking demonstration, they did have access to a test vehicle that had similar vulnerabilities to the targeted vehicle.

[5]49 U.S.C. Subtitle VI, 32101 et seq.

passenger safety.[6] For the purposes of this report, the term "modern vehicles" refers to passenger vehicles (i.e., automobiles) on the road today or currently in production.[7] We did not focus on cybersecurity vulnerabilities that may emerge as newer types of technologies, such as "connected vehicle" technologies, are introduced into vehicles in the future.[8]

To address these issues, we reviewed applicable federal laws and regulations, including requirements established in the Moving Ahead for Progress in the 21st Century Act (MAP-21) related to vehicle electronic systems.[9] We also identified and reviewed relevant research papers and publications. The reviewed citations were located through searches in bibliographic databases, including Transport Research International Documentation and SciSearch or relevant industry conferences. We also

[6]In addition to safety impacts, vehicle cyberattacks could have other impacts, such as privacy implications. For example, a cyberattack might involve the theft of personally identifiable information maintained in the vehicle, such as credit card information or e-mail addresses. However, such other impacts from vehicle cyberattacks are outside the scope of this review.

[7]Although our review is focused on vehicles on the road today, according to available research studies, vehicles manufactured before model year 2000 would be less vulnerable to cyberattacks, given that they have much less connectivity to external networks. According to the 2009 *National Household Travel Survey*, the average vehicle owned by U.S. households in 2009 was 9.4 years old and about 39 percent of all vehicles owned by U.S. households were more than 10 years old. See, Federal Highway Administration, *Summary of Travel Trends: 2009 National Household Travel Survey*, FHWA-PL-11-022 (Washington, D.C. June 2011). Vehicles currently in production include those that will be manufactured through model year 2020.

[8]"Connected vehicle" technologies—which include vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies—rely on data sent between vehicles, road infrastructure, and personal communication devices to improve safety by warning drivers and pedestrians of potential accidents. NHTSA issued an Advanced Notice of Proposed Rulemaking in August 2014 that would require vehicle manufacturers to install V2V technologies in new passenger cars and light trucks (79 Fed. Reg. 49270 (Aug. 20, 2014)) and plans to issue a draft rule on V2V in 2016, with the expectation that V2V technologies may be available in certain vehicle models as soon as 2017. According to DOT, V2I technologies are still developing and extensive deployment may occur over the next few decades. We have previously issued reports on V2V and V2I technologies. See GAO, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist*, GAO-14-13 (Washington, D.C.: Nov. 1, 2013) and GAO, *Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist*, GAO-15-775 (Washington, D.C.: Sept. 15, 2015).

[9]Pub. L. No. 112-141 § 31402, 126 Stat. 405 773 (2012).

reviewed reports and met with agency officials from DOT, the National Institute of Standards and Technology (NIST) within the Department of Commerce, the Department of Homeland Security (DHS), and the Defense Advanced Research Projects Agency within the Department of Defense. For example, we reviewed a series of reports on vehicle cybersecurity published by NHTSA in October 2014 and NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[10] In addition, we conducted semi-structured interviews with 32 selected industry stakeholders, including 8 automakers; 8 automotive parts suppliers; 3 vehicle cybersecurity firms that offer automotive cybersecurity products; and 13 subject matter experts, including 7 leading vehicle-cybersecurity researchers. Automakers were selected to ensure we had representation from each of the 3 major auto-producing regions of the world (the U.S., Europe, and Asia) and the two U.S. industry associations (the Alliance of Automobile Manufacturers and the Association of Global Automakers) that were jointly pursuing several efforts related to vehicle cybersecurity, such as the formation of an Automotive Information Sharing and Analysis Center (ISAC). We selected the top 5 automotive parts suppliers based on global sales in 2013 and other suppliers based on stakeholder recommendations.[11] We also interviewed 3 automotive cybersecurity firms that are offering vehicle cybersecurity products for new and existing vehicles based on stakeholder recommendations. The subject matter experts were identified through our literature search, relevant industry conferences, stakeholder recommendations, and our prior work on connected-vehicle technologies, and were considered subject matter experts based on their job titles and experience, technical papers and publications, contributions to relevant industry conferences (e.g., speeches, presentations, and organizing roles), and other significant contributions related to vehicle cybersecurity. Leading researchers were identified from the group of subject matter experts as

[10]NHTSA, *A Summary of Cybersecurity Best Practices*, DOT HS 812 075, (Washington, D.C.: October 2014); NHTSA, *Characterization of Potential Security Threats in Modern Automobiles*, DOT HS 812 074 (Washington, D.C.: October 2014); NHTSA, *National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles*, DOT HS 812 073, (Washington, D.C.: October 2014); NHTSA, *Assessment of the Information Sharing and Analysis Center Model*, DOT HS 812 076 (Washington, D.C.: October 2014); and NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.0* (Gaithersburg, MD: Feb. 12, 2014).

[11]One of the top 5 suppliers did not respond to our request for a meeting.

those with extensive applied research experience in vehicle cybersecurity.[12]

After conducting interviews with our 32 selected industry stakeholders, we summarized and analyzed their responses to identify themes relevant to each of our research objectives. The viewpoints gathered through our interviews with selected industry stakeholders represent the viewpoints of the individuals interviewed and cannot be generalized to a broader population. Our interviews with selected industry stakeholders were conducted, in part, during site visits in 2015 to Detroit, Michigan; Silicon Valley, California; Brussels, Belgium, and various locations within Germany. These site visit locations were selected largely based on the location of our selected industry stakeholders and to ensure we obtained a diverse range of perspectives, including those of U.S.-based and foreign companies. To assess DOT's efforts to address vehicle cybersecurity, we also reviewed (1) GAO's *Standards for Internal Control in the Federal Government;*[13] (2) NHTSA's documents regarding its strategic planning and vehicle cybersecurity-research priorities, including its *Priority Plan for Vehicle Safety and Fuel Economy 2015–2017*; (3) NHTSA's request for public comment on automotive electronic control systems safety and security issued in response to MAP-21 requirements;[14] and (4) a mandated report to Congress that summarized and analyzed the public comments NHTSA received, among other things.[15] We also visited NHTSA's Vehicle Research and Test Center (VRTC) in East Liberty, Ohio, to tour NHTSA's research facilities and observe ongoing vehicle-cybersecurity research and equipment demonstrations. Further details about our scope and methodology can be found in appendix I.

[12]In some cases, we spoke with more than one individual representing a research institute or center engaged in vehicle cybersecurity research. We considered the collective viewpoint of these individuals as one stakeholder.

[13]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). These standards provide the overall framework for establishing and maintaining an effective internal control system for the federal government.

[14]Sec. 31402(a)(2) of MAP-21.

[15]U.S. Department of Transportation, National Highway Traffic Safety Administration, *Report to Congress: Electronic Systems Performance in Passenger Motor Vehicles* (Washington, D.C.: December 2015).

We conducted this performance audit from February 2015 to March 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The number of annual fatalities and injuries due to motor vehicle crashes has declined from 42,836 fatalities and 2.8 million injuries in 2004 to 32,675 fatalities and 2.3 million injuries in 2014, although, according to NHTSA, the rate of decline has leveled off in recent years. The decline in fatalities and injuries over this time period is due in part to vehicle safety features, such as airbags. Automakers have also been installing a growing number of advanced technology features into vehicles to further improve passenger safety as well as to enhance driver and passenger convenience. For example, all vehicles manufactured starting in model year 2012 contain an electronic stability control feature that uses on-board sensors to detect and reduce skidding and automatically takes limited control from the driver to prevent the vehicle from leaving the roadway.[16] Similarly, some new vehicles offer forward collision warning and automatic emergency-braking systems that use on-board sensors and cameras to provide warnings to the driver and in some cases assist the driver to prevent a crash from occurring. As NHTSA attributed 94 percent of highway crashes to human error in 2013, such technologies could help continue the overall decline in motor vehicle fatalities over the past decade. Driver and passenger convenience technologies include built-in navigation systems, keyless entry and ignition systems, and wireless Bluetooth capabilities, among other features.

To support these and other advancements in technology, modern vehicles contain a number of electronic systems and components that have grown in number and complexity since they were first introduced into vehicles in the late 1970s. For example, a vehicle manufactured in the late 1970s contained basic electronic components to meet federal emissions regulations, and by the 1980s, the engines in most new vehicles were electronically controlled. Over time, these electronic

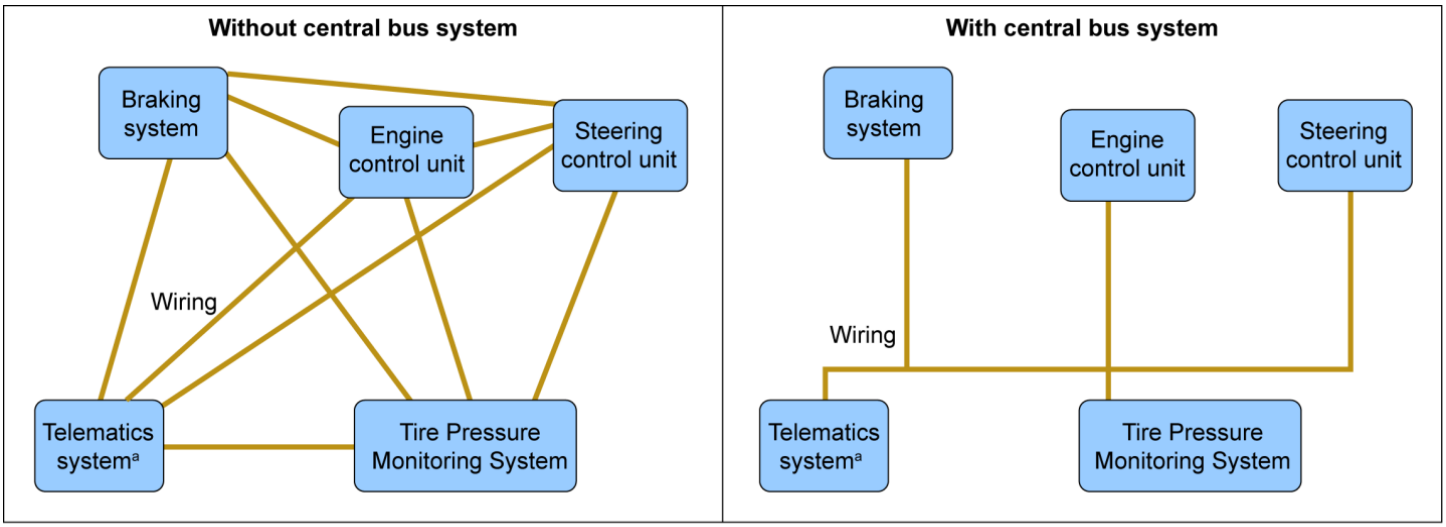
[16]79 Fed. Reg. 19178 (Apr. 7, 2014).

systems have begun to replace or control many of the traditional mechanical systems in vehicles. In 2009, NHTSA reported that a typical vehicle had around 50 embedded electronic control units (ECU) responsible for executing both core vehicle functions such as steering, as well as convenience and entertainment functions. By 2014 the agency estimated that a typical vehicle contained between 70 and 100 ECUs. In addition, over time, ECUs have evolved from controlling a single vehicle function and operating in isolation from other components, to controlling multiple vehicle functions and operating in conjunction with one another.

To facilitate communication among multiple ECUs without the need for complicated and extensive wiring systems, automakers began locating ECUs on in-vehicle communication networks, commonly referred to as buses or bus systems. According to NHTSA, the controller area network (CAN), which was first developed in 1985, has become the most commonly used in-vehicle communication network or bus; however, other types of networks are used by some automakers.[17] The CAN was designed to ensure that ECUs within the vehicle could reliably and expediently send messages to one another. The specific configuration of CAN and other in-vehicle communication networks can vary widely across automakers and even across different models produced by a single automaker, depending on the number and types of features within the vehicle. For example, automakers may locate all ECUs on a single in-vehicle network or include one network to support safety-critical vehicle functions, such as steering and braking, and another network to support convenience and entertainment systems. Figure 1 illustrates how in-vehicle communications networks reduce the need for wiring while facilitating communication among ECUs.

[17]Other in-vehicle communication networks used in modern vehicles include Ethernet, FlexRay, Local Interconnect Network, Media Oriented Systems Transport, and SAE-J1850. While networks generally serve the same function—connect and facilitate communication among ECUs—the rate at which they can process data and the amount of data that can be transmitted in each message vary. For example, whereas a CAN bus can carry messages with up to 8 bytes of data, FlexRay and Ethernet messages can be up to 254 bytes and 1,500 bytes respectively.

Figure 1: Depiction of Reduced Wiring Enabled by an In-Vehicle Communication Network



Source: National Instruments. | GAO-16-350

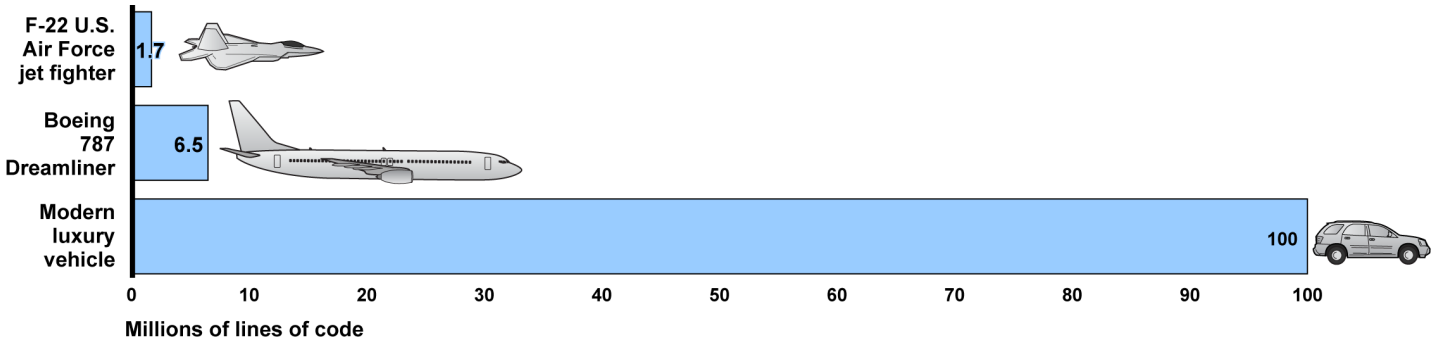
[a]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

While the shift from mechanical to electronically-controlled vehicle systems has helped improve the reliability and performance of certain vehicle features and allowed automakers to introduce new safety and "infotainment" features that are popular with consumers, it has also increased the potential for vehicles to be affected by cybersecurity breaches more commonly associated with the information technology (IT) and financial services industries. In particular, as the number of ECUs and electronic systems in vehicles has increased, the prevalence of software code in vehicles has also increased dramatically—and in some cases exponentially. DOT publications have indicated that a modern luxury vehicle could contain as much as 100 million lines of software code. In comparison, a Boeing 787 Dreamliner has about 6.5 million lines of software code (see fig. 2).[18] According to researchers and others, the use of software in vehicles is likely to increase as more advanced vehicle technologies and connected vehicle technologies are incorporated. As the

[18]We have previously reported on aviation cybersecurity issues. See GAO, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, GAO-15-370 (Washington, D.C.: Apr. 14, 2015) and GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221 (Washington, D.C.: Jan. 29, 2015).

lines of software code in vehicles increases, so does the potential for software errors, such as coding errors, and related vulnerabilities.

Figure 2: Average Lines of Software Code in Modern Luxury Vehicle Compared to Types of Aircraft



Source: Battelle. | GAO-16-350

According to NHTSA, in the context of motor vehicles, cybersecurity is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation. Although no vehicle cyberattacks impacting passenger safety have been reported outside of the research environment, our previous work has shown that the sources of cyber-threats vary in terms of the types and capabilities of the actors, their willingness to act, and their motives.[19] For example, *hackers* break into networks for the thrill of the challenge, bragging rights in the hacker community, and monetary gain, among other reasons, whereas *botnet operators* use a network of compromised, remotely-controlled systems to, among other things, coordinate attacks, such as denial-of-service attacks that prevent the authorized use of networks, systems, or applications by exhausting resources. Still others, such as *nations* may use cyber tools for information-gathering and espionage activities, while *terrorists* may seek to cause harm or damage public morale and confidence.

[19]For example, see GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

Responsibility for ensuring the security of vehicle systems and components spans across the automotive supply chain and occurs throughout the vehicle development cycle. For example, automakers define core vehicle design requirements, including software system requirements, to automotive parts suppliers. In turn, automotive parts suppliers assemble vehicle systems and often rely on lower-level suppliers, such as chip manufacturers, to obtain the specific parts (i.e., hardware) for the vehicle systems. Each supplier is responsible for testing and validating its specific product and certifying that its product meets automaker specifications. Automakers may incorporate components from multiple suppliers to assemble the vehicle and are ultimately responsible for validating that safety-critical systems meet minimum performance requirements and operate as intended.

Within DOT, NHTSA is the primary agency responsible for vehicle safety. NHTSA's mission is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes. NHTSA developed Federal Motor Vehicle Safety Standards, which establish the minimum performance requirements for certain safety features, such as brakes and air bags, to which automakers must conform and certify compliance.[20] NHTSA also conducts research in support of vehicle safety programs. The Office of Vehicle Safety Research conducts research in the areas of crashworthiness, crash avoidance, and electronic controls research. The electronic controls research—which includes research in the areas of electronics reliability, automated vehicles, and cybersecurity—is conducted by the Electronics Systems Safety Research Division[21]and is also supported by VRTC, the agency's in-house laboratory, in East Liberty, Ohio. In fiscal year 2015, the Office of Vehicle Safety Research had a budget of $29 million, of which $2.5 million was dedicated to electronics and vehicle cybersecurity research. According to NHTSA officials, as of July 2015, five full-time staff were dedicated to vehicle cybersecurity, automation, and electronics research. In addition, NHTSA has research under way related to cybersecurity for connected-vehicle

[20]49 U.S.C. § 30111. Federal Motor Vehicle Safety Standards provide objective criteria by which an automobile can be tested to see if it meets the minimum standard for motor vehicle performance. Federal Motor Vehicle Safety Standards are grouped into three main categories—crash avoidance, crashworthiness, and post-crash integrity.

[21]NHTSA established the Electronic Systems Safety Research Division in January 2012 as part of the Office of Crash Avoidance.

technologies, which, as previously mentioned, are expected to provide safety benefits by deterring crashes.

Several recent laws and legislative proposals have included provisions related to vehicle cybersecurity. For example, MAP-21—which was signed into law in July of 2012—directed NHTSA to, among other things, complete an examination of the need for safety standards with regard to electronic systems in passenger motor vehicles and to consider various topics, such as the security needs for those electronic components to prevent unauthorized access.[22] The act also required NHTSA to seek public comment in conducting its examination and to issue a report to Congress on the highest priority areas for safety with regard to electronic systems.[23] In addition, the Fixing America's Surface Transportation Act (FAST Act), enacted in 2015, requires DOT to submit a report to Congress on the operations of the Council for Vehicle Electronics, Vehicle Software and Emerging Technologies (Electronics Council), [24] which was established in MAP-21 to provide a forum for research, rulemaking, and enforcement officials to coordinate and share information internally on advanced vehicle electronics and new technologies.[25] Legislative proposals related to ensuring vehicle cybersecurity have also been introduced by members of Congress. For example, if passed, the Security and Privacy in Your Car Act of 2015 would require NHTSA to establish a "cyber dashboard" that displays an evaluation of how well each automaker protects the security and privacy of vehicle owners and would require automakers to adhere to government standards for vehicle cybersecurity.[26] The Security and Privacy in Your Car Study Act of 2015 would require NHTSA, along with some other federal agencies, to conduct a study to determine the appropriate standards for the regulation of vehicle cybersecurity.[27]

[22]Pub. L. No. 112-141 § 31402, 126 Stat. 773.

[23]Pub. L. No. 112-141 § 31402(a)(2).

[24]Pub. L. No. 114-94 § 31402, 129 Stat. 1312 (2015).

[25]Pub. L. No. 112-141 § 31401(a).

[26]Security and Privacy in Your Car Act of 2015, S. 1806. 114th Cong. (2015).

[27]Security and Privacy in Your Car Study Act of 2015, H.R. 3994. 114th Cong. (2015).

Finally, other federal agencies and foreign governments have also conducted cybersecurity research, particularly as it relates to connected-vehicle technologies, which are expected to increase the need for security protections.[28] For example, the European Union sponsored two major projects examining the security of connected-vehicle technology communications. These projects resulted in guidelines for the various security elements needed for the deployment of connected-vehicle technologies, such as message integrity, privacy protection, and misbehavior detection.[29]

Remote Attacks Involving Safety-Critical Vehicle Systems Could Have the Greatest Impact on Passenger Safety

Cyberattacks through Direct and Remote Access Are Possible, but Remote Attacks Are of Most Concern to Stakeholders

Based on our analysis of research and industry stakeholder views, modern vehicles contain multiple interfaces—connections between the vehicle and external networks—that if not properly secured, can become entry points—or attack paths—for cyber attackers.[30] Some of these interfaces can only be accessed through direct contact with the vehicle, while others can be accessed remotely through short- and long-range wireless channels.

[28]For example, although this report focuses on DOT efforts, DHS, NIST, and the Defense Advanced Research Projects Agency in the Department of Defense also have some efforts that broadly relate to vehicle cybersecurity. According to officials, these agencies are working to coordinate their efforts.

[29]These two projects are the E-safety Vehicle Intrusion-protected Applications, or EVITA project, and Preparing Secure Vehicle-to-X Communication Systems, or PRESERVE project.

[30]In this report, we will refer to those who would hack vehicles with malicious intentions as cyber attackers. We will refer to those conducting vehicle hacks in an effort to identify vulnerabilities—so that automakers can address them—as researchers.

Cyberattacks through Direct Access

Selected industry stakeholders we interviewed identified several vehicle interfaces that can be compromised through direct, physical access to a vehicle (see fig. 3). Of these potential direct interfaces, most of the selected industry stakeholders in our review (24 out of 32) expressed concerns about attacks exploiting cybersecurity vulnerabilities through the on-board diagnostics (OBD-II) port. This port is mandated in passenger vehicles by regulation for emissions-testing purposes and to facilitate diagnostic assessments by auto dealers, repair shops, and car owners.[31] In addition to being prevalent in modern vehicles, this port also provides direct and largely unrestricted access to in-vehicle communication networks. Thus, it can provide an attacker with sufficient access to compromise the full range of a vehicle's systems, including safety-critical systems, such as the brakes and steering wheel. However, because accessing the OBD-II port and other direct interfaces generally requires direct access to the vehicle,[32] such attacks would require attackers to target one vehicle at a time, thereby limiting the impact of a successful attack.

Cyberattacks through Remote (Short- and Long-Range Wireless) Access

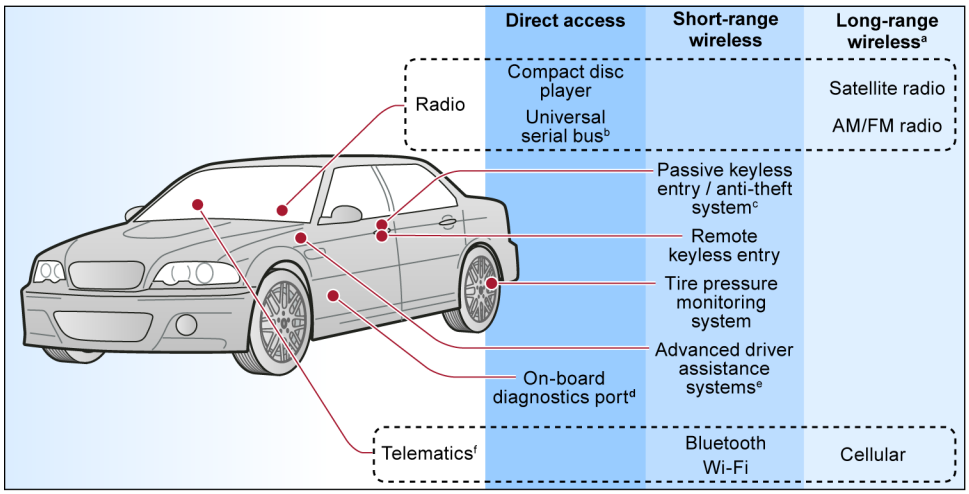
Selected industry stakeholders we interviewed identified several main interfaces that could be used to undertake a remote cyberattack through short- or long-range wireless channels, such as built-in Bluetooth and cellular-calling capabilities (see fig. 3). The majority of these industry stakeholders (23 out of 32) agreed that remote attacks are the most concerning for passenger safety. Such attacks could involve multiple vehicles and cause widespread impacts including passenger injuries or fatalities. For example, two stakeholders told us that through remote attacks, cyber attackers could theoretically achieve massive attacks of multiple vehicles simultaneously. Half of the selected industry stakeholders (16 out of 32) emphasized that long-range wireless interfaces, such as cellular connections on the telematics unit, are especially concerning. Through such interfaces, the cyber attacker could theoretically exploit vulnerabilities to access the target vehicles from

[31]The Clean Air Act Amendments of 1990 and its accompanying regulations, which are enforced by the U.S. Environmental Protection Agency, mandated that beginning with the 1996 Model Year, all light-duty vehicle and trucks for sale in the U.S. must be equipped with an OBD-II port. 42 U.S.C. § 7521(a)(6). Prior to this, an earlier version of this port had been in use in California since 1988.

[32]In some cases, the OBD-II port could be accessed remotely, as we will discuss later in this section.

anywhere in the world and take control over the vehicles' safety-critical systems.

Figure 3: Key Interfaces That Could Be Exploited in a Vehicle Cyberattack



Source: GAO analysis of stakeholder interviews and Checkoway et al, 2011. | GAO-16-350

[a]In this context, long-range refers to access at distances over 1 kilometer.

[b]Universal Serial Bus (USB) storage devices are used to store text, video, audio, and image information. By inserting such devices into the vehicle's USB port, users can access stored information through the vehicle's radio or other media systems.

[c]These systems can prevent the car from operating unless the correct key is present, as verified by the presence of the correct radio-frequency identification tag.

[d]This port is mandated in vehicles by regulation for emission-testing purposes and to facilitate diagnostic assessments of vehicles, such as by repair shops.

[e]These systems use on-board sensors and other cameras to assist the driver in undertaking certain functions, such as changing lanes or braking suddenly.

[f]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

Researchers have played a key role in publicly demonstrating that remote vehicle cyberattacks that impact safety are possible, because of vulnerabilities in modern vehicles. For example, in a hacking demonstration[33] first reported in 2011, researchers from the University of Washington and University of California San Diego first demonstrated the

[33]We will refer to vehicle hacking conducted by researchers as hacking demonstrations, and will refer to vehicle hacking with malicious intent, such as causing harm, as cyberattacks.

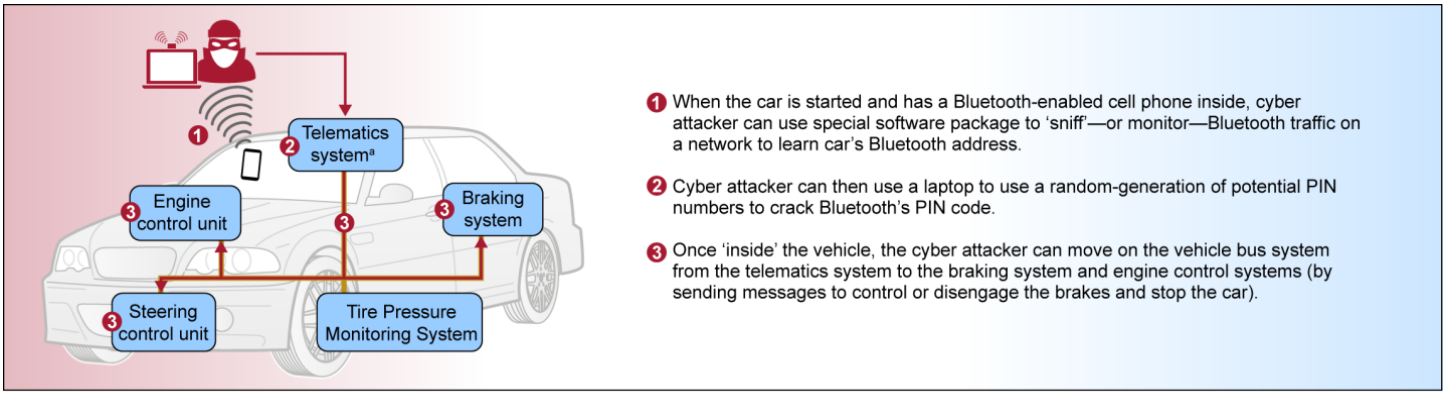
ability to remotely attack multiple vehicles' safety-critical systems through short- and long-range wireless channels without physical access to the target vehicles.[34] In this demonstration, the researchers studied two General Motors (GM) vehicles, gaining an in-depth understanding of the vehicles' systems, including the software code underlying various vehicle components and the CAN messages used to send commands between the ECUs that control the vehicle's systems. After gaining access to a target vehicle's CAN bus by exploiting software vulnerabilities in multiple wireless interfaces—including GM's OnStar telematics system and the Bluetooth unit—the researchers were able to inject messages onto the vehicle's CAN bus to take physical control over the vehicle, such as controlling the display on the speedometer, shutting off the engine, and controlling the brakes.

The researchers also showed that by exploiting vulnerabilities in the implementation of a telematics system—which connects participating vehicles via a cellular connection to a backend server maintained by the automaker—it would be possible to compromise multiple vehicles simultaneously. In this demonstration, the researchers exploited vulnerabilities in the communication protocols of GM's OnStar system in order to send commands to the CAN buses of their two test vehicles.[35] For safety reasons, the researchers only sent commands to take control of their test vehicles and only when these vehicles were in secured environments. However, if carried out by a cyber attacker, such an attack could have safety impacts on multiple vehicles. The researchers also demonstrated vulnerabilities in several other interfaces—including the Bluetooth unit—that could be exploited to send messages on the CAN bus and thereby take control over the vehicle's safety-critical systems (see fig. 4 for an overview of the researchers' hacking demonstration involving the Bluetooth unit).

[34]See Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, Proceedings of the USENIX Security Symposium (San Francisco, CA: August 2011).

[35]Many other major automakers besides GM offer such telematics services. For example, others include Ford's Sync, Toyota's Safety Connect, Lexus' Enform, and FCA's UConnect.

Figure 4: Example of a Potential Vehicle Cyberattack Launched through a Short-Range Wireless Interface, as Demonstrated by Researchers



Source: GAO analysis of Checkoway et al, 2011. | GAO-16-350

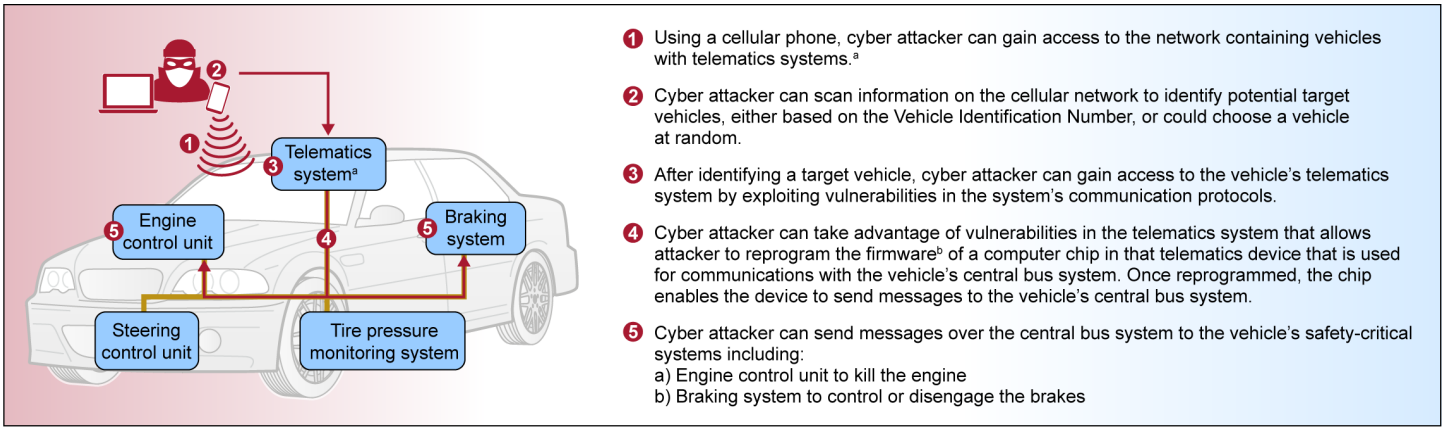
[a]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

In another example—the aforementioned Jeep Cherokee hacking demonstration reported in 2015—researchers exploited several vulnerabilities that allowed them to remotely disable a vehicle's engine and in some cases control the brakes and steering.[36] Similar to the 2011 GM demonstration, the researchers closely studied a test vehicle to understand its systems—including the characteristics of its software code and CAN messages—and showed it would be possible to remotely attack target vehicles with the same vulnerabilities as the test vehicle. Also, the researchers showed that it would be possible to exploit vulnerabilities in the implementation of a telematics system to target multiple vehicles participating in the telematics service. This demonstration involved multiple steps and identified a chain of vulnerabilities related to the vehicle's network architecture, the telematics unit, and the cellular provider's implementation of the vehicle's telematics service (see fig.5 for an overview of this hacking demonstration).[37]

[36]See whitepaper on this hacking demonstration: Charlie Miller and Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (Aug. 10, 2015).

[37]The demonstration led to the recall of about 1.4 million vehicles, initiated by FCA in response to a request from NHTSA. In addition, the cellular provider Sprint strengthened its network access protocols for that telematics service. NHTSA also initiated a safety defect investigation into the UConnect telematics unit found in the test vehicle and the target vehicles, which is manufactured by Harmon.

Figure 5: Example of a Potential Vehicle Cyberattack Launched through a Long-range Wireless Interface, as Demonstrated by Researchers



Source: GAO analysis of Miller and Valasek, 2015. | GAO-16-350

[a]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

[b]"Firmware" is the combination of a hardware device and the computer instructions and data that reside as read-only software on that device.

In addition, researchers have demonstrated that wireless telematics devices that consumers can plug into OBD-II ports to provide vehicle data to third parties, such as insurance companies, contain vulnerabilities that can be exploited remotely. By using these devices—often referred to as "dongles"—consumers may qualify for decreased insurance rates. Also, these dongles can provide older vehicles lacking built-in wireless interfaces with connectivity, allowing consumers to access telematics features—such as long-range cellular connectivity—that would otherwise only be available through purchasing a modern vehicle with a built-in telematics unit. Since, as previously mentioned, the OBD-II port connects directly to the key in-vehicle systems, an attack on such dongles could enable an attacker to take control of safety-critical systems and turn what was formerly a direct attack path into a remote attack path. For example, a recent demonstration showed that a particular manufacturer's dongles can be discovered online and then compromised by a remote attacker.[38] The researchers were able to exploit vulnerabilities of the dongle,

[38]See Ian Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage, *Fast and Vulnerable: A Story of Telematic Failures,* USENIX Workshop on Offensive Technologies (Washington. D.C.: August 2015).

allowing them to send messages to the vehicle's CAN buses, including messages to remotely apply and disable the brakes. Other demonstrations have shown similar vulnerabilities in other dongles.

Notably, each of the above hacking demonstrations illustrate that some overarching characteristics of the CAN bus make it more likely that a vehicle cyberattack launched through any interface—including non-safety-critical systems, such as the telematics unit—could impact safety. Specifically, these hacking demonstrations highlight a major security weakness of CAN: it assumes that any message on the bus is sent from a trusted sender, so messages are not secured or restricted in any way. In other words, these demonstrations help illustrate that because of the CAN's design, there is no way to know whether a given message on the CAN bus originates from a legitimate source or from a cyber attacker. As previously noted, the CAN was designed in 1985, which was long before vehicles were connected to external networks and vehicle cybersecurity was an issue facing the auto industry. Despite its inherent security weaknesses, CAN is the most commonly used bus system in the auto industry today.

Stakeholders Acknowledge That Remote Attacks Are Difficult to Execute, but Expressed Concern about the Future Potential for Such Attacks

While the possibility that remote cyberattacks could occur outside the research environment is concerning, some of the selected industry stakeholders we spoke to (8 out of 32) have also pointed out that attacks comparable to the hacking demonstrations described above would be complex to execute. Specifically, most of these stakeholders noted that such attacks would likely require a high level of hacking sophistication, including specialized knowledge. For example, as previously mentioned, the researchers involved in the GM and Jeep hacking demonstrations had prolonged access to test vehicles, which they used to closely study the vehicles' systems and key components. In another example, representatives from a cybersecurity firm noted that one very difficult step in such demonstrations is figuring out how to create authentic-looking messages that will be accepted and acted upon by the vehicle's ECUs. In addition, one leading researcher predicted that those who would execute remote cyberattacks would be those with previous experience hacking into other computer systems; for someone with no such experience, hacking into a vehicle remotely would be very difficult.

To date, there have been no remote cyberattacks with safety impacts reported outside of the research environment. In addition, determining the risk that such a remote cyberattack will occur in the near future is challenging, especially because of the difficulty of predicting the actions of

cyber attackers and since modern vehicles' designs vary widely (with some vehicle makes and models more vulnerable than others to such an attack). However, most selected industry stakeholders we interviewed (26 out of 32) expressed concerns that real-world attacks with safety implications could occur in the near future, particularly as automakers begin deploying autonomous (i.e., self-driving) vehicles and connected-vehicle technologies.[39] For instance, some stakeholders expressed concerns that as vehicles become increasingly autonomous–and assume control of more functions traditionally controlled by the driver such as steering and braking—it could become easier for remote cyberattacks to reach vehicles' safety-critical systems. This is because autonomous vehicles' systems will be tightly linked and highly responsive to inputs from external systems, such as sensors and the Global Positioning System, much more so than they currently are today. Also, DOT and the auto industry are planning to implement connected-vehicle technologies in coming years.[40] These technologies are envisioned to further connect vehicles to one another and infrastructure, such as traffic signals, to increase safety overall. For example, vehicle-to-vehicle technologies would allow nearby vehicles to share data, such as information on vehicle speed and location, to warn drivers of and thereby help prevent imminent collisions.[41] However, some stakeholders expressed concerns that cyber attackers could exploit vulnerabilities in the larger wireless networks used to facilitate these technologies to remotely cyberattack multiple vehicles simultaneously and take control over their safety-critical systems, which could result in accidents or other safety impacts.

[39]Autonomous vehicles would control steering, acceleration, and braking without a driver's input.

[40]See GAO-14-13 and GAO-15-775.

[41]See GAO-14-13.

A Variety of Key Practices and Technologies Are Available to Mitigate Vehicle Cybersecurity Vulnerabilities and the Impacts of Potential Attacks

Key Practices Used by Other Industries Are Available for Use in the Auto Industry

Selected industry stakeholders informed us that a range of key practices are available to identify and mitigate potential cybersecurity vulnerabilities in vehicles.[42] For instance, stakeholders frequently cited key practices used by other industries with a longer history of cybersecurity concerns, such as the IT industry's use of penetration testing and code reviews (see table 1). In addition, when NHTSA published *A Summary of Cybersecurity Best Practices* in 2014, it drew from existing practices used in other industries, including the IT, aviation, telecommunications, industrial control systems, energy, medical devices, and financial payments industries.[43] Although the key practices identified by NHTSA were generally broader, higher-level practices than those identified by our selected industry stakeholders, there were some similarities. For example, both NHTSA and our selected industry stakeholders emphasized the importance of risk assessments in mitigating cybersecurity vulnerabilities.

According to some stakeholders we interviewed, the auto industry's adoption of cybersecurity key practices varies by company and some companies are farther along with respect to following key practices than others. Some stakeholders pointed to the relative newness of cybersecurity in the automotive realm to explain why some companies

[42]For the purposes of this report, stakeholder-identified key practices are defined as concepts and approaches that can help identify and mitigate vehicle cybersecurity vulnerabilities, as opposed to specific technologies, which are discussed in the next section.

[43]NHTSA, *A Summary of Cybersecurity Best Practices*, DOT HS 812 075 (Washington, D.C.: October 2014).

are still building up their organizational capacity to address cybersecurity issues and developing or refining cybersecurity practices. In addition, some stakeholders also opined that until very recently some companies—primarily automakers—have been reluctant to accept vehicle cyberattacks as a real threat and take the necessary steps in response.

Table 1: Key Practices to Identify and Mitigate Vehicle Cybersecurity Vulnerabilities Identified by Industry Stakeholders

Key practice[a]	Description
Conduct risk assessments	Assess threats and vulnerabilities related to vehicles' electronic systems, including the potential impacts if known vulnerabilities are exploited, to inform and prioritize cybersecurity protections.
Incorporate security-by-design principles	Consider and build in cybersecurity protections starting in the early vehicle-design phases.
Create domain separation for in-vehicle networks	To the extent possible, locate safety-critical systems (i.e., steering, braking, etc.) and non-safety-critical systems on separate in-vehicle networks and limit communication between the safety-critical and non-safety-critical domains.
Implement a layered approach to security	Incorporate cybersecurity protections at multiple vehicle layers (e.g., at the electronic control unit level and the in-vehicle network level) to create multiple hurdles for cyber attackers and reduce the impact of a cyber breach.
Conduct penetration testing	Employ skilled assessors/evaluators who can simulate real-world vehicle cyberattacks in an attempt to identify ways to circumvent and defeat the vehicle's cybersecurity protections.
Conduct code reviews	Employ skilled assessors/evaluators to systematically examine the vehicle's software code so that any mistakes overlooked in the initial development phase can be addressed.
Develop over-the-air update capabilities	Establish mechanisms to remotely and securely update vehicle software and firmware[b] over the life of the vehicle in response to identified vulnerabilities.

Source: GAO analysis of stakeholder interviews. | GAO-16-350

[a]These key practices are organized based on the vehicle development process, beginning with the vehicle concept and design phases and ending with the vehicle operation and maintenance phase.

[b]"Firmware" is the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

One of the key practices mentioned most frequently—by 23 of the 32 selected industry stakeholders we interviewed—related to developing capabilities to conduct remote, over-the-air (OTA) updates of vehicle software and firmware (see table 1). Some of these stakeholders pointed to OTA updates as an essential piece of automakers' response capabilities as they would allow automakers to quickly and effectively respond to cybersecurity incidents if and when they occur. However, based on our interviews, only a few automakers have OTA update

capabilities, and only one—Tesla—can update all systems, including safety-critical and non-safety critical systems, on a fleet-wide basis remotely. Representatives from one automaker explained that their company does not yet conduct OTA updates because this capability involves hiring new staff and developing a whole new IT infrastructure to ensure that these updates do not become a new remote attack path into their vehicles.

The concept of domain separation was also identified as a key practice by the majority of selected industry stakeholders we spoke with (22 out of 32). Several automakers informed us that their companies have been following this key practice for 7 or more years. For example, one German automaker informed us that the company adopted this practice in the late 1990s as more functions in the vehicle became electronically controlled and infotainment systems and telematics units were introduced into vehicles; however, company representatives explained that the company's initial motivation was to ensure system stability, not to mitigate vehicle cyberattacks. In addition, several stakeholders suggested that the FCA hacking demonstration might not have had such significant safety impacts if the Jeep model involved had exhibited a greater degree of domain separation. Despite general agreement that domain separation can be a very effective mitigation strategy, some stakeholders pointed out that complete isolation or segregation is often not possible or practical because some limited communication will likely need to occur between safety-critical and non-safety-critical systems. For example, in some vehicles the infotainment system needs to receive information regarding the vehicle's speed to keep the volume at a consistent level.

Other key practices that were mentioned by several selected industry stakeholders, but less frequently than those described in table 1, include having dedicated organizational resources specifically focused on cybersecurity, such as creating new cybersecurity divisions or high-level managerial positions, and developing responsible disclosure policies that facilitate communication and collaboration with researchers and other third parties who may identify vehicle cybersecurity vulnerabilities. For example, some stakeholders noted that responsible disclosure policies are used by large IT companies, such as Microsoft, to encourage researchers and others to report any software vulnerabilities that they identify in the company's products.

Mitigation Technologies Can Be Incorporated at Multiple Vehicle Security Layers

Selected industry stakeholders informed us of several technologies that can help automakers and parts suppliers mitigate vehicle cybersecurity vulnerabilities and the impacts of potential cyberattacks (see table 2). As noted above, these stakeholders identified "implementing a layered approach to security" as a key practice. In other words, they noted that vehicle cybersecurity is enhanced as mitigation technologies are added at more layers, including the ECU layer, the in-vehicle network layer (e.g., CAN bus), and the external interfaces layer (e.g., telematics unit). In addition, in its white paper *NHTSA and Vehicle Cybersecurity*, NHTSA states that a layered approach to vehicle cybersecurity reduces the probability of attack and mitigates the potential ramifications of a successful intrusion.

Table 2: Summary of Vehicle Security Layers and Examples of Technologies Identified by Stakeholders That Can Be Applied to Mitigate Impacts of Vehicle Cyberattacks

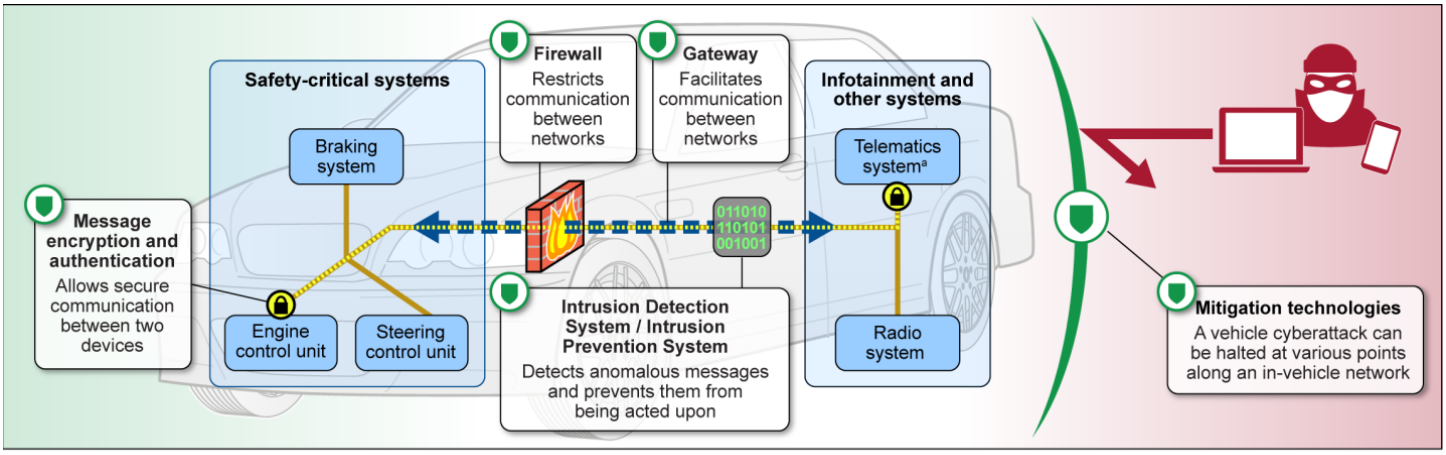
Security layer	Overview of protection	Example technologies that can help achieve protection
Electronic control unit (ECU)	Protect integrity of ECU software and hardware	• **Hardware security module/trust anchor:** Piece of hardware, such as a computer chip, that has undergone additional rigorous testing to eliminate flaws to ensure that communications it facilitates can be trusted. • **Microkernel:** Very small portion of software securely designed with limited, yet critical functionality. It is useful when a single ECU with multiple functionalities needs to send trusted messages to other ECUs.
In-vehicle networks	Protect integrity of critical ECU messages transmitted across in-vehicle networks	• **Gateway:** Device that interconnects and enables communication between two or more networks, including multiple internal vehicle networks and internal and external networks (e.g., gateways help facilitate the separation of safety-critical and non-safety-critical in-vehicle networks). • **Firewall:** System that controls and limits communication between two or more networks, including multiple internal vehicle networks and internal and external networks. Firewall systems can sit on gateways and block any messages not on a pre-determined list of approved messages (i.e., "white list"). • **Message authentication and encryption:** Coding techniques that verify the legitimacy of message senders and receivers. These techniques can be used to secure communications among ECUs on higher-bandwidth internal vehicle networks, such as Ethernet, or to secure communications between the vehicle and the automaker's backend server. • **Intrusion detection and prevention system:** Software that monitors network messages and analyzes them for signs of possible incidents. Intrusion prevention systems also attempt to stop detected possible incidents, ideally before the target is reached.
External interfaces	Secure interfaces that facilitate the vehicles' communications with external networks and devices (e.g., the telematics unit which facilitates cellular connectivity)	

Source: GAO analysis of stakeholder interviews and the National Institute of Standards and Technology reports. | GAO-16-350

Notably, most of the technologies identified by selected industry stakeholders we spoke with cannot be added on existing vehicles; rather, they must be incorporated into the vehicle design and production process, which as we describe later in this report, takes approximately 5 years to complete. The one exception is intrusion detection and prevention

systems: several companies that are marketing these products for in-vehicle networks informed us that they have also developed aftermarket versions of their products that can be incorporated onto existing vehicles. In addition, most of the technologies identified by stakeholders serve to mitigate the inherent security weakness of CAN, which is that messages transmitted over a CAN bus are generally free flowing and not secured or restricted in any way. For example, a firewall placed between two in-vehicle networks can be set up to prevent the passage of any message that is not on a pre-determined list of approved messages (i.e., a "white list"). Figure 6 below depicts how firewalls and some of the other technologies listed in the table above can help mitigate vehicle cyberattacks.

Figure 6: Example of a Vehicle's Cybersecurity-Mitigation Technologies Shown along an In-Vehicle Network



Source: GAO analysis of stakeholder information. | GAO-16-350

[a]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

Based on our interviews with selected industry stakeholders, automakers are still determining whether and how to implement some technologies that can help identify and mitigate vehicle cybersecurity vulnerabilities and reduce the impacts of potential cyberattacks. For example, several stakeholders expressed skepticism about the usefulness and effectiveness of intrusion detection and prevention systems—especially detection-only systems—and stated that these systems merit further testing before they are widely deployed on in-vehicle networks. In

addition, as noted above, CAN has become the most commonly used in-vehicle network that facilitates communication among ECUs. However, one mitigation option—message authentication and encryption[44]—cannot be easily incorporated onto CAN buses, as CAN does not provide sufficient bandwidth to host these protections.[45] Some stakeholders informed us that this option is more feasible for higher-bandwidth networks, such as Ethernet, but noted that these networks are currently less prevalent than CAN and likely to remain less prevalent for some time given the costs associated with vehicle re-designs.

Stakeholders Face Challenges Related to Vehicle Cybersecurity, Some of Which May Be Addressed by Industry-Led Efforts

Stakeholders Identified Several Challenges Facing the Industry Related to Vehicle Cybersecurity

The most frequently cited set of challenges facing the industry in ensuring vehicle cybersecurity—mentioned by 15 of the 32 selected industry stakeholders we spoke with—was the lack of transparency, communication, and collaboration regarding vehicles' cybersecurity among the various players in the automotive supply chain, as described in the following examples.

- Several parts suppliers informed us that the security requirements they receive from automakers often lack sufficient context about the

[44]Encryption techniques protect data by transforming ordinary data into code form for the purposes of security of privacy. Authentication techniques verify the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a particular information system or network.

[45]Bandwidth is the data rate or frequency range of a communications system. The higher the bandwidth, the greater the amount of data that can be transmitted in a given time period.

broader component or system. For example, one supplier stated that, ideally, automakers should provide specific security requirements (e.g., "encrypt data X using encryption mechanism Y"), as well as their higher-level system functionality, security, and protection goals, such as "ensure data confidentiality of function Z." Suppliers stated that with sufficient information, they could more readily identify potential cybersecurity issues and recommend alternative protections and enhancements.

- Some stakeholders also noted that it can be difficult for automakers to oversee and exert control over suppliers' software code. They explained that because suppliers' code is proprietary, the automakers do not have access to it and suppliers are reluctant to share it. One subject matter expert noted that as a result, all the automakers can really know about the code is how it performs when tested under certain conditions. In addition, one automaker noted that it can be especially challenging to exert control over third parties that manufacture dongles that plug into the OBD-II port for vehicle tracking and other purposes. They explained that while dongles have been shown to compromise vehicle cybersecurity, automakers are unable to set security requirements for these devices, as dongle manufacturers are not technically part of the automotive supply chain.

Highlighting the lack of transparency and collaboration that exists among the players in the automotive supply chain, one leading researcher we spoke with stated that "the most important and interesting commonality" with respect to the vulnerabilities identified in his research was that the vulnerabilities were located precisely at the interfaces where software code written by different supply chain players has to interact.

Another set of challenges cited by 13 of the 32 selected industry stakeholders was the cost of incorporating cybersecurity protections into vehicles. Some stakeholders informed us that profit margins for passenger vehicles are relatively narrow;[46] as a result, even seemingly small modifications to enhance cybersecurity—such as using hardware with added security protections—can potentially be cost prohibitive to

[46]According to the National Automobile Dealers Association, in 2014, net pretax profit at new car dealerships as a percentage of total sales (including sales in the new- and used-vehicle, service, and parts departments) was 2.2 percent and the average retail-transaction price of new cars and light trucks was $32,618.

some automakers.[47] Yet, according to some stakeholders, some automakers will likely have to pursue larger-scale changes—such as redesigning their in-vehicle communication networks—to significantly enhance the cybersecurity of their vehicles. Although many stakeholders declined to provide specific cost estimates, there was general agreement that these larger-scale changes would comprise a major upfront expense, which ultimately contributes to automakers' continued reliance on legacy systems with inherent security weaknesses, such as CAN.[48] In addition, stakeholders noted that automakers may not be able to pass the costs of cybersecurity protections onto consumers as they can with other features, such as connectivity and convenience features. As a result, automakers will have to balance the cost of cybersecurity protections against the risks facing vehicles and consumers' willingness to pay.

Some stakeholders (13 of 32) also identified challenges related to the auto industry's historical lack of cybersecurity expertise and companies' efforts to build up their expertise in this area. According to stakeholders, the existing pool of candidates with the specific mix of knowledge and skills needed to design and validate secure vehicle systems is small. One automaker explained that due to the shortage of automotive cybersecurity professionals, the company often has to decide whether to hire hardware and software professionals and teach them cybersecurity or cybersecurity professionals and teach them hardware and software. In addition, one leading researcher mentioned that the lack of automotive cybersecurity professionals in particular—combined with a shortage of cybersecurity professionals more broadly—produces competition for top talent both within the industry and with major technology companies, such as Google. However, automakers are taking some steps to address these

[47]According to one parts supplier we spoke with, the cost of a silicon computer chip can range from 50 cents to 5 dollars depending on the protections added. SAE (Society of Automotive Engineers) International—a standards development organization for the auto industry—has a Vehicle Electrical Hardware Security Task Force that is currently working to define and standardize the categories and characteristics of hardware security mechanisms that could be utilized to enhance vehicle cybersecurity, according to an SAE International member involved in this effort.

[48]According to a 2014 report by Frost and Sullivan, incorporating cybersecurity protections into vehicle electronic systems—including the costs associated with system design and engineering, hardware and software security features, and implementation—would increase costs per vehicle by 3 to 5 percent. However, the industry is currently exploring enhancements to CAN, such as CAN with flexible data-rate (CAN-FD), which could address the bandwidth limitations of CAN and could reduce costs associated with the re-design of in-vehicle networks that currently support CAN.

challenges. For example, several automakers informed us that they have begun partnering with colleges and universities to develop college curriculums that better meet their needs, and several U.S. and foreign automakers have opened technology and research and development centers in Silicon Valley, in part to be closer to the area's high concentration of IT and cybersecurity professionals.

Finally, 12 of the 32 selected industry stakeholders we spoke with informed us that the auto industry's long product development cycle creates challenges related to ensuring vehicle cybersecurity. According to some of these stakeholders, vehicles are designed approximately 5 years before they roll off of the assembly line. As a result, to the extent that automakers incorporated cybersecurity protections in their 2015 model year vehicles, these protections would have been based on technology—as well as threat information—available in 2010. One stakeholder suggested that this lag can make it easier for cyber attackers to understand and breach vehicles' cyber protections and more difficult for automakers to ensure their vehicles are protected against the latest known threats. Other challenges that were mentioned by several selected industry stakeholders, but less frequently than those cited above, include identifying and assessing vehicle cybersecurity threats and risks and measuring the performance and effectiveness of cybersecurity protections. For example, stakeholders noted that there are no widely accepted cybersecurity performance metrics, and it is difficult to prove that a vehicle with up to 100 million lines of code is secure. According to one stakeholder, testing every line of code in a vehicle would take several months, which is not feasible or practical.

Several Industry-Led Efforts Are Under Way That Could Help Address Some Challenges Related to Vehicle Cybersecurity

Auto industry stakeholders pointed to several industry-led efforts that could potentially improve automakers' and parts suppliers' ability to identify and mitigate vehicle cybersecurity vulnerabilities, as described below. As noted above, the adoption of key practices to identify and mitigate vehicle cybersecurity vulnerabilities currently varies significantly across the auto industry. As a result, several stakeholders told us that the main benefit of these and other industry efforts will be to help level the playing field across the industry. However, in some cases, stakeholders identified more specific benefits and goals associated with the various efforts that may help to address some of the key challenges facing the industry described above. For instance, stakeholders noted that efforts focused on incorporating cybersecurity into vehicle-design and engineering processes could help facilitate more productive conversations between automakers and their suppliers by creating shared

expectations and a common language for discussing vehicle cybersecurity issues and requirements.

Automotive Information Sharing and Analysis Center

The effort to establish an Information Sharing and Analysis Center (ISAC) for the auto industry is being led by two U.S. industry associations—the Alliance for Automobile Manufacturers and the Association of Global Automakers—and their members.[49] Similar to ISACs created for other industries, such as the Financial Services ISAC, the Automotive ISAC is intended to serve as a central hub for intelligence collection and analysis and provide a forum for members to anonymously share threat and vulnerability information with one another. According to representatives from the Association of Global Automakers, the ISAC—a U.S. entity that supports members that operate globally—began operations at the end of 2015. They also informed us that the Automotive ISAC's membership will initially be limited to automakers so that these companies, which are highly competitive, can acclimate to the new organization and establish and maintain the level of trust and cooperation necessary for a successful ISAC. However, the goal is to expand the ISAC's membership to include other stakeholders, such as parts suppliers, as soon as practically possible.

Selected industry stakeholders we spoke with, as well as DOT officials, generally expressed positive views regarding the potential effectiveness of an Automotive ISAC. However, some expressed skepticism regarding the ISAC's potential effectiveness. For example, one stakeholder stated that the ISAC's effectiveness could be limited given the sensitivity of the information that will need to be shared among competitors and the significant heterogeneity in vehicles' electronic architectures, parts, and components.

Society of Automotive Engineers' Vehicle Cybersecurity Guidelines

SAE (Society of Automotive Engineers) International—a standards development organization for the auto industry comprised of engineers and other technical professionals—established two taskforces led by representatives from the U.S. automakers that have been working since 2012 to develop recommended practice documents related to vehicle cybersecurity. According to SAE representatives, the taskforce focused on vehicle hardware security is still in the process of developing its draft

[49]NHTSA also facilitated the development of the Automotive ISAC by issuing a report that assessed the ISAC model for use in the auto industry and sending formal letters that urged automakers' executives to form an ISAC, among other things.

product; however, the taskforce that is focused on identifying and addressing cybersecurity risks during the vehicle's design process has recently completed its draft of SAE J3061: *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. This guidebook, which was issued in January 2016, provides an overarching framework and basic guiding principles for incorporating cybersecurity protections into the design of vehicle systems, among other things. Selected industry stakeholders we spoke with were generally supportive of SAE's efforts to develop recommended practice documents.

Design and Engineering Process Standard for Cybersecurity

In July 2015, German automakers informed us that they were working with the International Organization for Standardization (ISO) to develop a voluntary design and engineering process standard, similar to ISO 26262, that is focused on vehicle cybersecurity.[50] One stakeholder involved in this effort told us that the standard would help automakers and parts suppliers speak a common language and ensure that all stakeholders are asking themselves similar questions when designing their systems and determining appropriate levels of cybersecurity protections. Another stakeholder told us that a critically important aspect of this standard is that it would allow for variation and flexibility with respect to the types and methods of cybersecurity protections, as it would not mandate the use of specific technologies. Many selected industry stakeholders we spoke with indicated that they would support the development of this type of voluntary design and engineering process standard. Two German companies said that they have already incorporated elements of this proposed standard into their existing processes.

In November 2015, one German automaker involved in the ISO effort informed us that—given the similarities between the intent of SAE's *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* and the proposed ISO standard—SAE and ISO have agreed to jointly develop a robust, international standard for cybersecurity that will build upon the work already completed by SAE. Despite widespread support for both the SAE and ISO efforts, some stakeholders mentioned that the standards development process can be slow and that it can often take several years to achieve consensus and finalize a standard.

[50]ISO 26262 is a voluntary industry standard focused on road vehicles' functional safety. The standard establishes uniform practices for achieving specific levels of safety integrity in complex, safety-related systems comprised of electrical, electronic, and software elements.

AUTOSAR (Automotive Open System Architecture) Partnership

Since 2003 companies involved in the AUTOSAR (Automotive Open System Architecture) partnership—which was founded by German automotive companies and now includes 7 of the 8 automakers and 6 of the 8 parts suppliers we interviewed—have been working on a set of specifications to manage the growing complexities associated with the development of vehicle software.[51] More specifically, the partnership aims to standardize the basic software functionality of automotive ECUs and increase the transferability and reuse of vehicle software across manufacturers and product lines, among other things. Although AUTOSAR's goals are broader than ensuring vehicle cybersecurity, representatives informed us that the partnership has developed some specifications related to vehicle cybersecurity. For instance, AUTOSAR has several specifications that pertain to the use of message encryption and authentication techniques and recently issued a specification aimed at protecting the integrity of ECU messages transmitted across in-vehicle communication networks. According to AUTOSAR representatives, one of the main benefits of the partnership for automakers and parts suppliers is the reduction in costs associated with software development and testing. Other benefits of the partnership include the assurance that all applicable standards and requirements—including any future cybersecurity standards and requirements—have and will be incorporated into AUTOSAR specifications and the increase in product quality due to the use of standard specifications.

[51]In addition to automakers and parts suppliers, AUTOSAR includes partners from the electronics, semiconductor, and software industries. For a complete list of current partners see www.autosar.org/partners/current-partners/.

DOT Has Made Progress in Addressing Vehicle Cybersecurity, but Has Not Yet Defined and Documented Its Roles and Responsibilities in Responding to a Vehicle Cyberattack

NHTSA Has Established a Vehicle Cybersecurity Research Program

According to NHTSA officials, efforts to specifically consider vehicle cybersecurity have been under way over the last 5 years. Specifically, the agency modified its Vehicle Safety Research organization in recognition that vehicle cybersecurity represents a safety concern. In January 2012, NHTSA created a new Electronic Systems Safety Research division—which conducts research on electronics reliability, automated vehicles, and cybersecurity—within the Vehicle Safety Research's Office of Vehicle Crash Avoidance. Within this new division, NHTSA established a cybersecurity research program in 2012 and set goals for it, including: developing tools to enable applied research in this area, fostering industry's development of new solutions, and gathering facts to inform potential future federal policy and regulatory decisions.[52] Cybersecurity research has become one of NHTSA's highest safety research priorities[53] and falls into four main areas, as summarized in table 3. Some of this research is conducted by NHTSA's staff. For example, its VRTC conducts NHTSA's sensitive and quick turn-around cybersecurity research projects, according to officials. Other research is conducted through contracts with

[52]In addition, DOT's Intelligent Transportation Systems Joint Program Office conducts research on connected-vehicle technologies, including electronics and cybersecurity research that is managed by NHTSA's Vehicle Safety Research staff.

[53]For example, in its *Priority Plan for Vehicle Safety and Fuel Economy, 2015 - 2017*, NHTSA identified gaining a comprehensive understanding of cybersecurity and reliability for safety-critical vehicle electronic systems as one of seven priority research areas.

DOT's Volpe Center and other research institutions.[54] NHTSA officials informed us that the agency has used the results of its completed research to inform industry about its efforts and to form the basis for additional research currently under way or planned. The officials expect more reports to be issued in 2016 as additional research projects are completed.

Table 3: Examples of Recently Completed and Ongoing National Highway Traffic Safety Administration (NHTSA) Vehicle Cybersecurity Research by Priority Area

Research area	Description	Examples of completed, ongoing, and planned research by area
Protective and preventive measures and techniques	Research into methods that could prevent a cyberattack, such as isolating safety-critical systems, message encryption, and using gateways and firewalls.	**Completed research** In 2014, NHTSA issued reports that: • Summarized cybersecurity best practices that could be leveraged by the auto industry;[a] • Outlined a modeling approach to assess potential cybersecurity threats in modern vehicles;[b] and • Applied the National Institute of Standards and Technology Cybersecurity Risk Management Framework to modern vehicles.[c] **Ongoing research** In 2015, NHTSA initiated contracted research into effective firewall and gateway technologies for vehicles.
Real-time intrusion detection systems	Research into the feasibility and effectiveness of systems that are designed to detect and respond in real time to mitigate the potential adverse effects of intrusions.	**Ongoing research** In 2015, NHTSA initiated contracted research on vehicle intrusion detection and prevention systems.

[54]For example, NHTSA maintains Indefinite Delivery Indefinite Quantity (IDIQ) contracts with the University of Michigan Transportation Research Institute, Virginia Tech Transportation Institute, and Battelle. As IDIQ contractors, these institutions have been selected to conduct research on behalf of NHTSA related to vehicle electronics, including on vehicle cybersecurity. IDIQ contractors are responsible for preparing proposals in response to specific task orders issued by NHTSA. NHTSA then selects from among these proposals and awards the task order to one of the research institutions.

Research area	Description	Examples of completed, ongoing, and planned research by area
Effectiveness of industry's responses to identified vulnerabilities	Applied investigatory research into how well specific stakeholders have responded to an identified vulnerability. Broad research on effective ways to respond to vulnerabilities, including key practices from other industries.	**Completed & ongoing research** In recent years, VRTC staff have recreated hacking demonstrations (such as the Jeep demonstration) to help NHTSA determine the extensiveness of the vulnerability in other vehicles and assess the impact vulnerabilities may have on vehicle safety. **Ongoing research** In October 2015, NHTSA initiated contracted research on secure firmware[d] updates—both through direct vehicle access and wireless over-the-air updates.
Assessment of solutions	Research to assess proposed solutions (such as those suggested by industry and researchers) and to provide feedback for continuous improvement.	**Completed research** In 2014, NHTSA issued a report focused on assessing the applicability of the Information Sharing and Analysis Center (ISAC) model for the automotive sector.[e] **Ongoing research** According to officials, NHTSA continues to promote and monitor progress of the Automotive ISAC and to research additional proposed solutions.

Source: GAO Summary of DOT research. | GAO-16-350

[a]NHTSA, *A Summary of Cybersecurity Best Practices*, DOT 812 075 (Washington, D.C.: October 2014).

[b]NHTSA, *Characterization of Potential Security Threats in Modern Automobiles*, DOT HS 812 074 (Washington, D.C.: October 2014).

[c]NHTSA, *National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles*, DOT 812 073 (Washington, D.C.: October 2014).

[d]Firmware is the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

[e]NHTSA, *Assessment of the Information Sharing and Analysis Center Model*. DOT HS 812 076 (Washington, D.C.: October 2014).

Most selected industry stakeholders we spoke to (25 out of 32) were aware that NHTSA is conducting vehicle cybersecurity research, but their opinions differed about whether NHTSA is appropriately focusing and prioritizing its research. Of those stakeholders who discussed NHTSA's research in this area, the majority (10 out of 18) told us that its research focus and prioritization are appropriate. For example, according to some stakeholders in our review, the research reports NHTSA issued in 2014 provide helpful background on the issue of vehicle cybersecurity. Specifically, representatives from one automaker told us that they use the report on characterizing vehicle cybersecurity threats to make their own determinations about how to respond to identified vulnerabilities. However, six selected industry stakeholders told us that NHTSA could improve its research prioritization in this area. For example, two stakeholders noted that NHTSA has not dedicated enough resources to

this important issue. In another example, two other stakeholders stated that NHTSA's efforts to recreate the Jeep Cherokee hacking demonstration are not useful since such efforts are more reactive than proactive. However, VRTC staff told us that recreating this hacking demonstration allowed them to determine that the initial steps that FCA took to mitigate the vulnerabilities were not successful and additional steps needed to be taken.

NHTSA officials told us that their ability to conduct additional research is in part dependent on funding and resources the agency receives for vehicle cybersecurity and other priority research areas. In recent years, the agency has requested an increase in funding to support additional staff in the Office of Vehicle Safety Research, in part to conduct additional cybersecurity research, but actual funding received was lower than requested. For example, in fiscal year 2015, NHTSA requested $36.8 million for the Office of Vehicle Safety Research but received $29 million; this sum was about a $4 million decrease from the $32.5 million the Office received for fiscal year 2014. NHTSA officials told us that due to the 2015's funding being lower than requested, they had to make difficult decisions and forgo other planned projects in order to carve out the $2.5 million that was ultimately dedicated to electronics and vehicle cybersecurity research in fiscal year 2015. This amount was still a decrease from the $2.7 million dedicated to this area in fiscal year 2014.[55] Despite lower funding levels, officials told us they have been able to leverage resources from other programs, such as by using test vehicles for the New Car Assessment Program for cybersecurity research.[56] To build on its ongoing research, the agency's fiscal year 2016 budget requested $1 million for additional space and new equipment at VRTC, as

[55]In fiscal year 2015, NHTSA's Office of Vehicle Safety dedicated $2.5 million in total to electronics and cybersecurity research, which includes research related to electronics reliability, automated vehicles, and vehicle cybersecurity. Of this total, $0.9 million was dedicated specifically to vehicle cybersecurity research. In addition, DOT's Intelligent Transportation Systems Joint Program Office dedicated $2.5 million in fiscal year 2015 toward electronics and cybersecurity, as part of its research on connected-vehicle technologies, and requested $3.6 million for such research in fiscal year 2016.

[56]Under the New Car Assessment Program, which began in 1978, NHTSA provides consumers with information about crash protection, rollover safety, and crash avoidance technologies beyond what is required by law. The program aims to encourage market forces that prompt vehicle manufacturers to make safety improvements to new vehicles and provide the public with objective information on the relative safety performance of vehicles.

well as $4.1 million to enhance a program on vehicle electronics and emerging technologies. In addition to the applied research it conducts, officials also told us that they attend cybersecurity conferences where researchers present findings on vehicle cybersecurity vulnerabilities and participate in various working groups, such as serving as a liaison on SAE International committees, to enhance their understanding of vehicle cybersecurity issues. Finally, NHTSA collaborates in relevant research efforts led by other federal agencies. For example, it participates in two ongoing efforts by DHS: one effort involving seven major automakers which is focused on researching intrusion detection systems and secure over-the-air updates for vehicles, among other issues, and another effort focused on ensuring the cybersecurity of government-owned vehicles.

NHTSA Is Developing Guidance to Help Ensure Consistent Responses to Vulnerabilities

In November 2015, NHTSA officials informed us that they were developing guidance to help automakers understand the agency's determinations—and to assist automakers in making their own determinations—regarding the types of vehicle cybersecurity vulnerabilities that would constitute a safety defect and, therefore, merit a recall.[57] According to NHTSA officials, the differing conclusions reached by NHTSA and FCA regarding the need for a recall in the aftermath of the Jeep Cherokee hacking demonstration, underscored the need for this guidance.[58] While the guidance is not yet complete, NHTSA officials informed us that they intend to create a document that provides a framework and educates the industry on the methodology NHTSA uses and the factors it considers when assessing risks associated with cybersecurity vulnerabilities in order to make safety defect and recall determinations. According to NHTSA officials, factors such as the number of affected vehicles, frequency of occurrence, likelihood of exploitation, and the resulting hazard level (i.e., impacts to safety-critical systems) can

[57]The term "defect" is defined by the Motor Vehicle Safety Act (49 U.S.C. § 301-02(a)(2)) as "any defect in performance, construction, a component, or material of a motor vehicle or motor vehicle equipment."

[58]NHTSA requested that FCA undertake a recall, based on its conclusion that the vulnerabilities could result in unauthorized remote control of vehicle systems, thereby increasing the risk of a crash. In addition, NHTSA officials noted that because the hacking researchers planned to publish details of their findings, this could allow others—possibly with less hacking expertise—to replicate this demonstration and exploit the identified vulnerabilities. While FCA complied with the recall request, it argued that it was conducting this recall "out of an abundance of caution," since "no safety defect had been found."

be important when assessing risk and making safety defect determinations; these and other factors will be explained in the guidance. For example, the officials noted that NHTSA would be particularly concerned with identified vulnerabilities that would enable a cyber attacker to manipulate the safety-critical systems of multiple vehicles. In January 2016, NHTSA officials informed us that they expect the guidance to be issued by March 31, 2016.[59]

Several industry stakeholders we spoke with—including automakers and industry associations—told us that this type of guidance would be helpful and is needed. For example, representatives from one industry association told us that absent guidance, automakers could monitor NHTSA's actions and recall decisions over time to get clarity on what factors NHTSA considers important in making safety defect determinations; however, conducting such monitoring of NHTSA's actions is not efficient. In addition to being helpful to the industry, such guidance could also help NHTSA respond to identified vulnerabilities more consistently. For example, several stakeholders noted that while NHTSA requested that FCA conduct a recall in response to the 2015 Jeep Cherokee hacking demonstration, it did not request a recall in response to the GM hacking demonstration in 2011, despite the fact that both demonstrations revealed similar vulnerabilities that allowed researchers to remotely control the vehicle's safety-critical functions. NHTSA officials informed us that due to staffing changes that have occurred since 2011, they could not confirm why the two similar hacking demonstrations were handled differently. However, they noted that the Jeep Cherokee researchers planned to publicly report more details about the identified vulnerabilities than the GM researchers had reported; and that the release of such details could have allowed cyber attackers to replicate the Jeep Cherokee demonstration.

[59]In January 2016, NHTSA and 18 automakers issued *Proactive Safety Principles* stating their intention to work collaboratively to further enhance safety, by, for example, working to mitigate cybersecurity threats that could present unreasonable safety risks. This effort would include establishing best practices to foster enhanced cybersecurity resiliency and effective remediation, developing means to engage with cybersecurity researchers, and continuing to support and evolve the Automotive ISAC. See DOT, *Proactive Safety Principles* (January 2016).

NHTSA Has Established a Vehicle Electronics Council and Is Assessing the Need for Vehicle Cybersecurity Standards and Regulations

NHTSA is taking steps in response to the requirements set forth in MAP-21, including establishing an Electronics Council and assessing the need for vehicle cybersecurity standards and regulations.[60] As directed by MAP-21, NHTSA established an Electronics Council in 2012 to coordinate and share information on a broad array of topics related to vehicle electronics and emerging technologies, including cybersecurity.[61] More specifically, NHTSA officials informed us that the Council's mission is to broaden, leverage, and expand the agency's expertise in vehicle electronics to continue ensuring that these technologies enhance vehicle safety. NHTSA officials told us that the Council's membership includes staff from NHTSA's Office of Vehicle Safety Research and other offices responsible for the agency's vehicle safety work.[62] However, NHTSA's Chief Counsel was also designated as a member to ensure that the agency fully understands its rulemaking and oversight authority regarding electronics-related issues. According to NHTSA officials, the Council holds bimonthly meetings, which NHTSA Associate Administrators attend; the Council also periodically briefs NHTSA's Administrator. NHTSA officials also informed us that the Council's meetings can serve as a forum for collaboration between the agency and industry stakeholders. For example, they said that the Council sometimes invites outside subject matter experts to share information with NHTSA during its bimonthly meetings, or recommends other training by such experts that would be helpful for NHTSA staff to attend.

Although NHTSA has taken some steps to examine the need for safety standards for electronic control systems as required by MAP-21,[63] which could include government standards related to vehicle cybersecurity, officials informed us the agency's examination is still ongoing.[64] As part of its examination, NHTSA is considering establishing process standards,

[60]Pub. L. No. 112-141 §§ 31401(a) and 31402, 126 Stat. 405, 773.

[61]As previously mentioned, the FAST ACT also requires DOT to submit a report to Congress on the operations of the Council. Pub. L. No. 114-94 § 24201.

[62]The four NHTSA offices responsible for vehicle safety are the Office of Vehicle Safety Research, Office of Enforcement, Office of Rulemaking, and the National Center for Statistics and Analysis.

[63]Pub. L. No. 112-141 § 31402(a).

[64]In the current discussion, we will refer to standards set by NHTSA as government standards, to differentiate these from voluntary industry standards.

which would prescribe specific processes for developing vehicle electronic systems. This step would be a departure from NHTSA's current approach of developing performance standards, such as the Federal Motor Vehicle Safety Standards, which set a specific level of performance but do not prescribe specific methods that must be used to meet a given standard. In October 2014, NHTSA issued a request for public comment to help inform its examination of the need for safety standards for electronic control systems, including the need for cybersecurity standards.[65] Among other things, NHTSA requested comments on available performance standards and process standards, such as ISO 26262, that could potentially be adapted and incorporated into government standards to address vehicle cybersecurity. In January 2016, NHTSA issued a report that summarized its analysis of the public comments it received, including industry stakeholders' thoughts on the need for voluntary industry standards as well as government standards pertaining to vehicle cybersecurity.[66] In this report, NHTSA noted that most of the 40 stakeholders that submitted comments agreed that vehicle cybersecurity is a dynamic, complex problem that may not be effectively addressed with the use of "static" or "prescriptive" government standards.

Half of the selected industry stakeholders we spoke with (16 out of 32) also expressed doubts about the effectiveness of "static" or "prescriptive" government standards to address vehicle cybersecurity, since threats are constantly changing and such standards could become outdated quickly. In addition, some stakeholders expressed concerns that regulations could result in unintended negative consequences for cybersecurity, similar to several existing laws and regulations. For example, as noted above, the OBD-II port—which many stakeholders identified as a key entry point for vehicle cyberattacks—is mandated by regulation for diagnostic and testing purposes. As a result, several automakers told us that they have limited ability to restrict access to in-vehicle networks and systems provided by the port; however, one informed us that it was exploring what types of OBD-II port restrictions and protections would be legally allowed. Two automakers also expressed concerns about potential negative

[65]NHTSA, *Request for Comment on Automotive Electronic Control Systems Safety and Security*, Docket No. NHTSA-2014-0108. 79 Fed. Reg. 60574 (Oct. 7, 2014).

[66]U.S. Department of Transportation, National Highway Traffic Safety Administration, *Report to Congress: Electronic Systems Performance in Passenger Motor Vehicles* (Washington, D.C.: December 2015).

impacts for vehicle cybersecurity that could stem from recent changes to regulations implementing the Digital Millennium Copyright Act.[67] In general, this act prohibits access to and circumvention of protections associated with digital copyrighted materials;[68] however, in 2015, the act's regulations were amended to include exemptions for vehicle software accessed for diagnostic and repair purposes and "good faith" research.[69] For example, one industry association that opposed the change stated that increasing access to vehicle software will make it harder for automakers to develop effective protections for their vehicles' cyber systems. However, two leading researchers we interviewed opined that these changes will help mitigate cybersecurity vulnerabilities, as they will allow more researchers to identify vulnerabilities without fear of legal action.

On the other hand, some selected industry stakeholders (13 out of 32) told us that voluntary industry standards alone would be insufficient for ensuring vehicle cybersecurity and that thus some government standards and federal oversight will be needed. For example, one subject matter expert suggested that—contrary to current self-certification practices that are common in the auto industry[70]—NHTSA should establish an oversight body to evaluate automakers' compliance with any cybersecurity-related standards it issues and verify that these standards are being met.[71] In addition, another expert noted that this kind of oversight process could help promote the use of best practices while also providing NHTSA with additional assurance that the automotive supply chain is secure. Both

[67]Pub. L. No. 105-304. 112 Stat. 2860 (1998) and its implementing regulations under 37 C.F.R. Part 201.

[68]17 U.S.C. § 1201(a)(1).

[69]Exemptions to the Digital Millennium Copyright Act went into effect on October 28, 2015. 80 Fed. Reg. 65944 (Oct. 28, 2015). However, the particular exemptions for vehicle software cannot be initiated earlier than 12 months after the effective date of the regulation, or before October 28, 2016. 37 CFR 201.40(b)(6).

[70]The auto industry currently self-certifies compliance with the Federal Motor Vehicle Safety Standards and is not subject to a verification or certification process undertaken by NHTSA. Once a standard is in effect, NHTSA tests and monitors vehicles and equipment to ensure that they meet the relevant safety standards.

[71]GAO has previously reported on risk-based safety management systems in other industries, including aviation. See for example, GAO, *Aviation Safety: Additional Oversight Planning by FAA Could Enhance Safety Risk Management,* GAO-14-516 (Washington, D.C: June 25, 2014).

experts noted that as part of this process, NHTSA could turn to qualified independent third parties to assess whether automakers are taking the proper steps for vehicle cybersecurity.

According to NHTSA officials and the agency's *Priority Plan for Vehicle Safety and Fuel Economy, 2015-2017*, the agency plans to complete its initial research on vehicle cybersecurity in 2016 and also announce an agency decision about next steps pertaining to vehicle cybersecurity and other issues related to electronic control systems. The decision could be to conduct more research, initiate a rulemaking, issue guidance, or some combination thereof. As of July 2015, officials estimated that the agency was about 3 years away from making a final determination about the need for additional government standards or regulation in this area; thus, such a final determination is not expected until at least 2018. NHTSA officials explained that this time frame is necessary in part, because they expect several research projects that are planned and under way to help inform their decision. In addition, NHTSA officials informed us that as they determine the need for regulations, they want to better understand alternative steps such as the development of voluntary industry standards that could be taken to address this issue.

NHTSA Has Not Yet Defined and Documented Its Roles and Responsibilities in Responding to a Vehicle Cyberattack

In its whitepaper *NHTSA and Vehicle Cybersecurity*, NHTSA states that its goal is to "be ahead of potential vehicle cybersecurity challenges, and seek ways to address or avoid them altogether." As described above, NHTSA has made progress in many areas in an effort to proactively address potential cybersecurity threats to vehicle safety-critical systems; however, NHTSA has not yet formally defined and documented the agency's role and responsibilities in the event of a real-world vehicle cyberattack and how the agency's response actions would be coordinated with other federal agencies. Given that NHTSA and selected industry stakeholders we spoke with generally agreed that the threat of a vehicle cyberattack will increase as autonomous and connected-vehicle technologies are deployed in the coming years, such a response plan may be particularly important for NHTSA to develop proactively, before the threat environment significantly changes. Until such a plan is developed, NHTSA's response efforts—regardless of the threat environment in which an attack is carried out—could be slowed as agency staff and other stakeholders may not be able to quickly identify the appropriate actions that NHTSA should take. In addition, the lack of such a response plan is inconsistent with federal standards for internal control, which—among other things—are intended to help agencies in managing change associated with shifting environments and evolving

demands and priorities.[72] Under these federal standards, agencies are required to appropriately and clearly document their internal controls, which include the policies, plans, methods, and procedures used to meet agency missions, goals, and objectives; and assess risks.

NHTSA officials offered several roles and responsibilities they believe the agency would have in response to a vehicle cyberattack involving safety-critical systems, including quickly contacting the appropriate industry personnel and determining what actions need to be taken, such as regulatory or enforcement action, a Direct Final Rule,[73] or other action. In addition, NHTSA officials told us that the agency would also validate the feasibility of the cybersecurity threat or event at its VRTC and take steps to ensure that any new information regarding threats and vulnerabilities is reflected in NHTSA's research program. However, NHTSA officials told us that these roles have not been outlined in a formal response plan yet, in part because the agency currently lacks clarity regarding other roles and responsibilities it may have to fulfill in the event of an attack. For example, according to NHTSA officials, it is currently unclear whether NHTSA or DHS would be "the responsible agency" in charge of the government's response if a large-scale vehicle cyberattack on safety-critical systems were to occur.

According to NHTSA officials, the agency is working with other federal agencies, such as DHS, to clarify the roles and responsibilities of the various agencies that would be involved in responding to a vehicle cyberattack. NHTSA officials informed us that these interagency discussions are still ongoing and could not provide a time frame as to when they expect the discussions—and subsequently, a plan outlining NHTSA's roles and responsibilities in the event of an attack—to be completed. However, NHTSA officials stated that obtaining clarification on its roles and responsibilities in the event of a cyberattack on safety-critical

[72]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999) and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[73]In June 2015, NHTSA established Direct Final Rule rulemaking procedures for use in adopting amendments to its regulations on which the agency expects it would receive no adverse public comment were it to publish them as proposals in the *Federal Register*. Adoption of the procedures is intended to expedite the promulgation of routine and noncontroversial rules by reducing the time and resources necessary to develop, review, clear, and publish separately proposed and final rules.

vehicle systems is a priority for the agency, and in their view, a response plan would be a useful tool for the agency to develop.

Conclusions

In recent years, researchers have played an instrumental role in demonstrating that remote vehicle cyberattacks with safety implications are possible and increasing overall awareness about vehicle cybersecurity issues among consumers, the media, and the general public. Despite awareness of risks related to vehicle cybersecurity since at least 2011, the auto industry and NHTSA have only recently sharpened their focus on this issue. As this report describes, NHTSA has taken several important steps since 2012 to address vehicle cybersecurity, including establishing a vehicle-cybersecurity research program and soliciting industry input on the need for government and voluntary industry standards. However, NHTSA does not anticipate making a final determination on the need for government standards until 2018 when additional cybersecurity research is expected to be completed. In addition, several industry efforts to address vehicle cybersecurity—such as the development of an Automotive ISAC and a voluntary design and engineering process standard for cybersecurity—are still in their early stages. As such, some of these government and industry efforts to address vehicle cybersecurity are unlikely to provide many benefits for vehicles already operating on the roads today or those currently in the design and production stages.

Given that NHTSA and industry stakeholders expect the threat of a vehicle cyberattack to increase in the coming years as autonomous and connected-vehicle technologies are deployed, it will be important for NHTSA to continue to take proactive steps in the interim to ensure that it is meeting the agency's goal of being ahead of vehicle cybersecurity challenges. The agency's planned guidance outlining when cybersecurity vulnerabilities constitute safety defects should help ensure consistent responses when cybersecurity vulnerabilities are identified. However, until NHTSA defines and documents the agency's role and responsibilities in the event of a real-world vehicle cyberattack affecting safety-critical systems, it may not be in a position to quickly and effectively respond should a threat materialize.

Recommendation

To enhance the agency's ability to effectively respond in the event of a real-world vehicle cyberattack, the Secretary of Transportation should direct NHTSA to:

- work expeditiously to finish defining and then to document the agency's roles and responsibilities in response to a vehicle cyberattack involving safety-critical systems, including how NHTSA would coordinate with other federal agencies and stakeholders involved in the response.

Agency Comments

We provided a draft of this report to the Departments of Transportation (DOT), Homeland Security, Defense, and Commerce for review and comment. We received written comments from DOT, which are reprinted in appendix II.

DOT concurred with our recommendation to define and document NHTSA's roles and responsibilities in response to a vehicle cyberattack involving safety-critical systems. DOT also noted that the agency has been actively involved in research and collaborative efforts to address vehicle cybersecurity issues. DOT cited some recent actions by NHTSA to address vehicle cybersecurity vulnerabilities, including convening a public roundtable on vehicle cybersecurity and finalizing the *Proactive Safety Principles* agreement in January 2016. Through this agreement, NHTSA and 18 automakers committed to work together to develop a collaborative, data-driven process to advance safety objectives, including mitigating cybersecurity threats.

The Departments of Homeland Security, Defense, and Commerce reviewed our report, but did not have any comments.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretaries of Transportation, Homeland Security, Defense, and Commerce, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or wised@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix III.

David J. Wise
Director, Physical Infrastructure Issues

List of Requesters

The Honorable Barbara Comstock
Chairwoman
The Honorable Daniel Lipinski
Ranking Member
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
House of Representatives

The Honorable Fred Upton
Chairman
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Larry Bucshon, M.D.
House of Representatives

The Honorable Ted W. Lieu
House of Representatives

The Honorable Joe Wilson
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to examine: (1) available information about the key cybersecurity vulnerabilities in modern vehicles that could impact passenger safety; (2) key practices and technologies, if any, available to mitigate vehicle cybersecurity vulnerabilities and the impacts of potential attacks; (3) views of selected stakeholders on the challenges they face related to vehicle cybersecurity and industry-led efforts to address vehicle cybersecurity; and (4) the Department of Transportation's (DOT) efforts to address vehicle cybersecurity.

To address all of our objectives, we reviewed technical papers, reports, and other documentation relevant to the cybersecurity of modern vehicles published by DOT's National Highway Traffic Safety Administration (NHTSA).[1] For example, we reviewed a series of reports on vehicle cybersecurity published by NHTSA in October 2014.[2] We also interviewed officials from several NHTSA offices, including the Office of Vehicle Safety Research and Office of Enforcement and the Volpe National Transportation Systems Center. In addition, we reviewed previous GAO reports related to connected-vehicle technologies, information technology (IT), and cybersecurity, and identified and reviewed relevant research papers and publications. The reviewed citations were located through searches in bibliographic databases, including Transport Research International Documentation and SciSearch, or relevant industry conferences. We used three research papers to inform our findings regarding the potential for remote vehicle

[1]For the purposes of this report, the term 'modern vehicles' refers to vehicles on the road today or currently in production. Vehicles currently in production include those that will be manufactured through model year 2020. We did not focus on cybersecurity vulnerabilities that may emerge as connected-vehicle technologies are introduced into vehicles. Although our review is focused on vehicles on the road today, vehicles manufactured before model year 2000 would be less vulnerable to cyberattacks, given that they have much less connectivity to external networks. According to the 2009 National Household Travel Survey, the average vehicle owned by U.S. households in 2009 was 9.6 years old and about 41 percent of all vehicles owned by U.S. households were more than 10 years old. See, Federal Highway Administration, *Summary of Travel Trends: 2009 National Household Travel Survey*, FHWA-PL-11-022 (Washington, D.C.: June 2011).

[2]NHTSA, *A Summary of Cybersecurity Best Practices*, DOT HS 812 075, (Washington, D.C.: October 2014); NHTSA, *Characterization of Potential Security Threats in Modern Automobiles*, DOT HS 812 074, (Washington, D.C.: October 2014); NHTSA, *National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles*, DOT HS 812 073, (Washington, D.C.: October 2014); and NHTSA, *Assessment of the Information Sharing and Analysis Center Model*. DOT HS 812 076, (Washington, D.C.: October 2014).

cyberattacks to impact passenger safety.[3] We reviewed and summarized these research papers to identify the main steps of the hacking demonstrations and discussed them with the researchers to obtain additional information and clarification about the demonstrations.

In addition, we conducted semi-structured interviews with 32 selected industry stakeholders, including 8 automakers, 8 automotive parts suppliers, 3 automotive cybersecurity firms offering vehicle cybersecurity products, and 13 subject matter experts, including 7 leading researchers (see table 4).[4] These interviews informed all four of our objectives. Automakers were selected to ensure we had representation from each of the 3 major auto-producing regions of the world (the U.S., Europe, and Asia) and the two U.S. industry associations (the Alliance of Automobile Manufacturers and the Association of Global Automakers) that were jointly pursuing several efforts related to vehicle cybersecurity, such as the formation of an Automotive Information Sharing and Analysis Center (ISAC). We also sought to include automakers that were considered leaders in vehicle cybersecurity as well as those that had been the subjects of cybersecurity hacking demonstrations. We selected the top 5 automotive parts suppliers based on global sales in 2013 and other suppliers based on stakeholder recommendations.[5] We also interviewed 3 automotive cybersecurity firms that are offering vehicle cybersecurity products for new and existing vehicles based on stakeholder recommendations. The subject matter experts were identified through our literature search, relevant industry conferences, stakeholder recommendations, and our prior work on connected-vehicle technologies, and were considered subject matter experts based on their job titles and experience, technical papers and publications, contributions to relevant

[3]Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, *Comprehensive Experimental Analyses of Automotive Attack Surfaces,* Proceedings of the USENIX Security Symposium (San Francisco, CA: August 2011); Charlie Miller and Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (Aug. 10, 2015); and Ian Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage, *Fast and Vulnerable: A Story of Telematic Failures*, USENIX Workshop on Offensive Technologies (Washington. D.C.: August 2015).

[4]Selected industry stakeholders were those that we anticipated would have the most in-depth knowledge of vehicle cybersecurity developments based on their area of expertise or position in the market (e.g., automakers and parts suppliers).

[5]One of the top 5 suppliers did not respond to our request for a meeting.

industry conferences (e.g., speeches, presentations, and organizing roles), and other significant contributions related to vehicle cybersecurity (e.g., contracted to conduct vehicle cybersecurity research for federal agencies). We identified leading researchers from the group of subject matter experts as those with extensive applied research experience in vehicle cybersecurity.[6] After conducting our interviews with selected industry stakeholders, we summarized and analyzed their responses to identify themes relevant to each of our research objectives, such as themes regarding the main vehicle interfaces that could be used to undertake vehicle cyberattacks. The viewpoints gathered through our interviews with selected industry stakeholders represent the viewpoints of the individuals interviewed and cannot be generalized to a broader population.

Table 4: Selected Industry Stakeholders Interviewed

Stakeholder
Automakers
BMW
FCA US LLC
Ford
General Motors
Honda
Mercedes-Benz Passenger Car Development, Germany
Tesla Motors, Inc.
Volkswagen
Automotive parts suppliers
Aeris Communications
Bosch
Continental
Denso
Infineon
Lynx Software
Magna International
Panasonic Automotive Systems Company of America

[6]In some cases, we spoke with more than one individual representing a research institute or center engaged in vehicle cybersecurity research. We considered the collective viewpoint of these individuals as one stakeholder.

Stakeholder
Automotive cybersecurity firms
Argus Cyber Security
Arilou Technologies
TowerSec
Subject matter experts
Dr. Andrew Brown Jr., P.E., FESD, FSAE, NAE (ret. Delphi Automotive)
Daniel Chilcott, Formerly at Virginia Tech Transportation Institute, Center for Automated Vehicle Systems
Joshua Corman, I am the Cavalry
Karl Heimer, AutoImmune[a]
Stylianos Kaminaris, Battelle, Cyber Innovations Business Unit
Christoph Krauss and Andreas Fuchs, Fraunhofer Institute for Secure Information Technology[a]
Praveen Narayanan, Frost and Sullivan
Stefan Savage and Tadayoshi Kohno, Center for Automotive Embedded Systems Security[a]
Greg Shannon, Christopher King, Mark Sherman, Daniel Klinedinst, and Art Manion, Carnegie Mellon University, Software Engineering Institute, CERT Division[a]
Craig Smith, Theia Labs[a]
Chris Valasek, Uber Advanced Technologies Center[a]
Andre Weimerskirch, University of Michigan Transportation Research Institute[a]
William Whyte, Security Innovation

Source: GAO. | GAO-16-350

[a]Leading researchers.

To identify the key vehicle cybersecurity vulnerabilities in modern vehicles that could impact passenger safety and key practices and technologies that could mitigate these vulnerabilities, we interviewed officials from other federal agencies involved in vehicle cybersecurity research or cybersecurity efforts more broadly. These agencies included: the National Institute of Standards and Technology (NIST) within the Department of Commerce, the Department of Homeland Security's Science and Technology Directorate, and the Defense Advanced Research Projects Agency within the Department of Defense. We also reviewed documents published by NIST, such as its *Framework for Improving Critical Infrastructure Cybersecurity*,[7] and based on stakeholder

[7]NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Gaithersburg, MD: Feb. 12, 2014).

recommendations, interviewed representatives from several IT and telecommunication firms to identify key mitigation practices and technologies. To address our objective on challenges and industry-led efforts related to vehicle cybersecurity, we also interviewed representatives from entities involved in those efforts, including representatives from the Alliance of Automobile Manufacturers, the Association of Global Automakers, AUTOSAR,[8] the National Council of ISACs, and Society of Automotive Engineers International.[9]

To assess DOT's efforts to address vehicle cybersecurity, we reviewed applicable federal laws and regulations—such as the Moving Ahead for Progress in the 21st Century Act (MAP-21) and the Fixing America's Surface Transportation Act (FAST Act)—including their requirements for NHTSA pertaining to vehicle electronics and cybersecurity.[10] We also reviewed GAO's *Standards for Internal Control in the Federal Government*[11] and NHTSA documents regarding the agency's strategic planning and vehicle cybersecurity research priorities, including its *Priority Plan for Vehicle Safety and Fuel Economy 2015-2017*; request for public comment on automotive electronic control systems safety and security issued in response to MAP-21 requirements;[12] and mandated report to Congress that summarized and analyzed the public comments it received, among other things.[13] We also visited NHTSA's Vehicle Research and Test Center (VRTC) in East Liberty, Ohio, to tour NHTSA's research facilities and observe ongoing vehicle cybersecurity research and equipment demonstrations. In addition to our VRTC site visit, we

[8]AUTOSAR is an acronym for Automotive Open System Architecture.

[9]The interviews mentioned in this paragraph were conducted in addition to our interviews with the 32 selected industry stakeholders described above.

[10]Pub. L. No. 112-141 § 31402, 126 Stat. 773 (2012) and Pub. L. No. 114-94. 129 Stat. 1312 (2015).

[11]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999) and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). These standards provide the overall framework for establishing and maintaining an effective internal control system for the federal government.

[12]Docket No. NHTSA-2014-0108. 79 Fed. Reg. 60574 (Oct. 7, 2014).

[13]U.S. Department of Transportation, National Highway Traffic Safety Administration, *Report to Congress: Electronic Systems Performance in Passenger Motor Vehicles* (Washington, D.C.: December 2015).

conducted the stakeholder interviews described in this appendix, in part, during site visits in 2015 to Detroit, Michigan, to meet with U.S. automakers, among other stakeholders; Silicon Valley, California, to meet with Tesla, technology firms, and parts suppliers; and Brussels, Belgium, and various locations within Germany to obtain international perspectives on vehicle cybersecurity from a variety of stakeholders—including automakers, parts suppliers, government officials, and subject matter experts.

We conducted this performance audit from February 2015 to March 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Transportation

U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

MAR 8 2016

David J. Wise
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Mr. Wise:

A key Department of Transportation (DOT) priority is enhancing vehicle cybersecurity to mitigate cyber threats that could present unreasonable safety risks to the public. The Department, together with its operating administration, the National Highway Traffic Safety Administration (NHTSA), is actively engaged in vehicle cybersecurity research and employs a proactive and collaborative approach with stakeholders to protect vehicle owners from cybersecurity risks. Recent actions we have taken to address vehicle cybersecurity vulnerabilities include the following:

- Examined the need for safety standards with regard to electronic systems in passenger motor vehicles, including "security needs for those electronic components to prevent unauthorized access." In January 2016, DOT submitted its findings to Congress and identified, among other matters, new research opportunities which, pending the availability of resources, would explore data elements and data recording trigger points for capturing record-of-data in cases of suspected electronics malfunctions and cybersecurity hacking attempts.[1]

- Convened a public vehicle cybersecurity roundtable meeting[2] attended by vehicle manufacturers, suppliers, technology companies, industry experts, security researchers, technology leaders in related industries, and other government agencies to facilitate discussion on key vehicle cybersecurity topics. For example, one topic included the best ways to capitalize efforts from other environments while applying them to distinct aspects of the auto industry. During this January 2016 meeting, stakeholder groups identified actionable steps that the vehicle manufacturing industry may take to effectively and expeditiously address vehicle cybersecurity challenges.

- Finalized a historic agreement with 18 automakers in January 2016, on proactive safety principles. The signatories agreed to work together to develop a collaborative, data–

[1] Report to Congress: "Electronic Systems Performance in Passenger Motor Vehicles," December 2015, http://www.nhtsa.gov/staticfiles/laws_regs/pdf/Electronic-Systems-Performance-in-Motor%20Vehicles.pdf
[2] http://www.nhtsa.gov/Research/Crash+Avoidance/NHTSA+Vehicle+Cybersecurity+Roundtable

driven, science–based process, consistent with the law, to advance safety objectives including, mitigating "cyber threats that could present unreasonable safety risks."[3]

Upon review of the draft report, we concur with the recommendation regarding clarifying and documenting NHTSA's roles and responsibilities in response to a vehicle cyberattack involving safety critical systems. The Department will provide a detailed response to this recommendation within 60 days of the final report's issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if you would like to obtain additional details.

Sincerely,

Jeff Marootian
Assistant Secretary for Administration

[3] https://www.transportation.gov/briefing-room/proactive-safety-principles-2016

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

David Wise, 202-512-2834 or WiseD@gao.gov

Staff Acknowledgments:

In addition to the contact named above, the following individuals made important contributions to this report: Nabajyoti Barkakati and Gregory C. Wilshusen (Directors); Nancy Lueke (Assistant Director); Jessica Bryant-Bertail; West Coile; Pamela Davidson; Charlotte Hinkle; David Hooper; Thomas Johnson; Jaclyn Nidoh; Josh Ormond; Malika Rice; and Amy Rosewarne.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.