NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 20, ISSUE 1: OCTOBER 2018

CYBERSECURITY OF AUTONOMOUS SYSTEMS IN THE TRANSPORTATION SECTOR: AN EXAMINATION OF REGULATORY AND PRIVATE LAW APPROACHES WITH RECOMMENDATIONS FOR NEEDED REFORMS

Jeanne C. Suchodolski, JD, LLM

The past twenty-five years gave rise to increasing levels of automation within the transportation sector. From initial subsystems, like vessel satellite tracking and automobile chassis control, automation continues apace. The future promises fully autonomous devices such as unmanned aerial systems ("UAS") and self-driving cars ("UAV"). These autonomous and automatic systems and devices ("AASD") provide safety, efficiency, and productivity benefits. Yet AASD operate under continual threat of cyber-attack.

Compromised AASD can produce dire consequences in the transportation sector. The possible consequences extend far beyond financial harms to severe bodily injury or even death. Given both the prevalence of cyber threats and their potentially deadly consequences, the public holds a legitimate interest in ensuring that incentives exist to address the cybersecurity of such systems.

This paper examines both the private and public law mechanisms for influencing AASD cybersecurity behaviors in the transportation sector; and undertakes the first comprehensive comparison of existing agency regulatory schemes. The findings presented herein propose: (1) additional legislation to promote sharing of cyber event data; and (2) transportation sector regulatory best practices that require mandatory submission and review of cybersecurity plans by OEMs and service providers when compromise of their products or services threatens safety of life or critical infrastructure. None of the recommendations advanced herein require regulators to direct the adoption of any specific technical solution or specific cybersecurity standard. Thus, industry participants can remain nimble in the face of evolving cyber threats,

while ensuring public safety through what proves to be needed regulatory oversight.

I. INTRODUCTION

The U.S. Director of National Intelligence, Daniel Coats, stated in recent testimony before Congress that the United States public and private sectors are at continual risk of cyber-attack from both nation state and non-nation state actors.[1] Coats stressed that the threats "will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security . . . ."[2] Emerging technologies and novel applications of available technologies have the potential to threaten the nation's infrastructure, including the transportation sector.[3]

The past twenty-five years ushered in ever-increasing levels of automation within the transportation sector. From initial applications like ship and aircraft systems monitoring, to automobile traction control; automation continues apace. Current automatic systems now include more complex capabilities such as the ability to parallel park semi-autonomously.[4] Future systems promise fully autonomous unmanned aerial systems ("UAS") and self-driving cars. These automated and autonomous systems and devices ("AASD") have the potential to significantly improve safety while providing benefits in efficiency and productivity. Yet, compromised AASD can produce dire consequences in the transportation sector.

---

[1] *Open Hearing on Worldwide Threats*: Hearing Before the Select Comm. on Intelligence, 115th Cong. 16‑17 (2018) (statement of Daniel R. Coats, Director of National Intelligence), https://www.govinfo.gov/content/pkg/CHRG-115shrg28947/pdf/CHRG-115shrg28947.pdf.

[2] *Id*. at 16.

[3] *Id*. at 23.

[4] Aaron Turpen, *How self-parking car technology works: the first step to autonomous vehicles*, NEW ATLAS (Nov. 29, 2016), https://newatlas.com/how-self-parking-works/46684/.

These consequences extend far beyond financial harms to severe bodily injury or even death. Given both the prevalence of cyber threats and their potential safety of life consequences, the public has a legitimate interest in ensuring that the legal system includes mechanisms that address AASD cybersecurity.

According to a report by the Congressional Research Service, there are more than 50 federal laws relating to cybersecurity.[5] By the government's own admission, no overarching structural framework or organizing principles exist to unify this preponderance of legislation into a comprehensive approach to cybersecurity.[6] The majority of existing legislation seeks to secure the administrative systems, intelligence gathering, and defense capabilities of the United States. An additional subset of federal law delegates to specialized agencies, either directly or through broader more comprehensive mandates, the responsibility for oversight of non-federal critical infrastructure as well as for other non-federal sector-specific activities.

[5] ERIC A. FISHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 2-3 (2014), https://fas.org/sgp/crs/natsec/R42114.pdf; CALEB WATNEY & CYRIL DRAFFIN, R STREET POLICY NO. 118, ADDRESSING NEW CHALLENGES IN AUTOMOTIVE CYBERSECURITY 7 (2017), https://www.bafuture.org/sites/default/files/key-topics/attachments/Addressing%20Automotive%20Cybersecurity%20Nov%202017.pdf.

[6] FISHER, *supra* note 5, at 2.

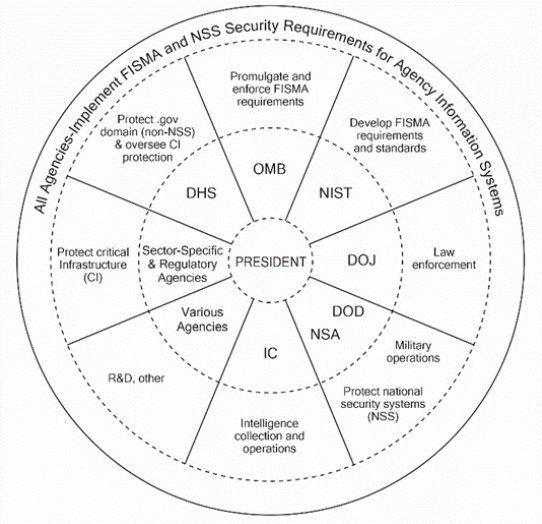

Figure 1: A Simplified Diagram Illustrating Agency Responsibilities for Regulating Cybersecurity

Figure 1 contains a simplified depiction of federal agency cybersecurity responsibilities, created by the Congressional Research Service.[7] As seen in the Figure, under current law all federal agencies have responsibility for securing their own systems. In the private sector, the Department of Homeland Security ("DHS") serves as the primary civil-sector cybersecurity agency. The National Institute of Standards and Technology ("NIST") develops cybersecurity standards and guidelines, while sub-agencies within the Department of Transportation and DHS retain responsibility for their sector-specific regulatory charges. In addition, the White House, through Presidential Directives and Executive Orders, can and does instruct federal agencies on specific cybersecurity actions and launches other cybersecurity improvements and initiatives.

In view of the escalating frequency and severity of cybersecurity breaches, and the cumbersome and disordered array of federal regulations designed to deal with them, many have called for legislative reform and additional regulatory oversight of the private

[7] *Id.* at 4.

sector.[8] Others argue that any such additional legislation and regulation is not only unnecessary, but likely to stifle innovation, introduce expensive and unnecessary overhead, and hinder access to beneficial goods and services.[9] Furthermore, logic suggests that regulatory intervention need not be necessary if private legal incentives for the desired cybersecurity behaviors already exist.

In at least one sector, the National Highway Traffic Safety Administration ("NHTSA") and its constituency has allied itself with the latter view, eschewing formal regulation of the cyber risks inherent with autonomous vehicles and espousing, instead, the use of optional industry guidelines.[10] Other agencies, such as the U.S. Coast Guard, adopt a slightly more aggressive posture: mandating certain cybersecurity related actions, while not specifying in detail the exact composition of those actions.[11]

This paper examines private and public law mechanisms to encourage AASD cybersecurity in the transportation sector. The analysis of private law mechanisms investigates the effectiveness of contractual agreements, insurance products, and product liability laws in influencing cybersecurity behaviors. The analysis of public law focuses primarily on regulations. Regulations are the tactical implementation of the broader statutory authority from which they derive and define the specific, detailed actions AASD providers and users must take. Furthermore, as illustrated by the NHTSA, statutory authority to regulate does not necessarily lead to the promulgation of regulations.

---

[8] *See id*. at 4–7.

[9] *See, e.g.*, WATNEY & DRAFFIN, *supra* note 5, at 11.

[10] *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 812 442, AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY 1 (2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

[11] *See* Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, 82 Fed. Reg. 32189 (proposed Jul. 12, 2017). *See generally* 33 C.F.R. pt. 105.

II. AN OVERVIEW OF AASD AND THEIR USE IN THE TRANSPORTATION SECTOR

AASD may comprise an entire vehicle, or a self-contained component or subsystem thereof. The degree of automation within AASD spans a wide range. At their least complex, AASD involve the simple automatic monitoring of a component or subsystem: for example, the tire pressure sensor and its companion alert system on a car. At their most complex, AASD include completely autonomous operations like self-driving cars. Between these two extremes lies automatic and autonomous systems such as flight management computers, ships' autopilots, and the vehicle chassis control used to manage road handling. The principal distinctions between an automatic system and an autonomous system are the degree of complexity and the impact on the overall operation and conduct of the apparatus of which it forms a part. For purposes of this paper, an automatic system, subsystem, component, or device is one capable of operating without external control or intervention (e.g. a tire pressure warning light), while an autonomous system is self-governing with logic that enables decision making independent of human intervention (e.g. an unmanned aircraft that delivers packages to your doorstep).[12] The consequences of a cyberattack depends in part upon the degree of automation as well as the function of the device or system automated.

AASD may be pre-programmed and exist independently of any external communications network. In contemporary applications, such configurations are becoming less and less common. The logic incorporated into AASD is often queried for stored information or periodically connected to external devices for the purposes of

[12] *See generally* SOC'Y OF AUTO. ENG'RS INT'L, J3016 201806, SURFACE VEHICLE RECOMMENDED PRACTICE: TAXONOMY AND DEFINITIONS FOR TERMS RELATED TO DRIVING AUTOMATION SYSTEMS FOR ON-ROAD MOTOR VEHICLES 2 (2018) (describing six levels of motor vehicle automation, ranging from no automation (level 0) to full driving automation (level 5)). While the cited source is in the specific context of motor vehicles, the definition provided above in the text is applicable to all devices and operations. For purposes of this paper it is only necessary to understand that the degree and complexity of automation may vary and that a distinction exists between an autonomous device and an automatic function.

performing updates and installing software patches. In the transportation sector, AASD also frequently receive inputs needed for their operation via communications links.

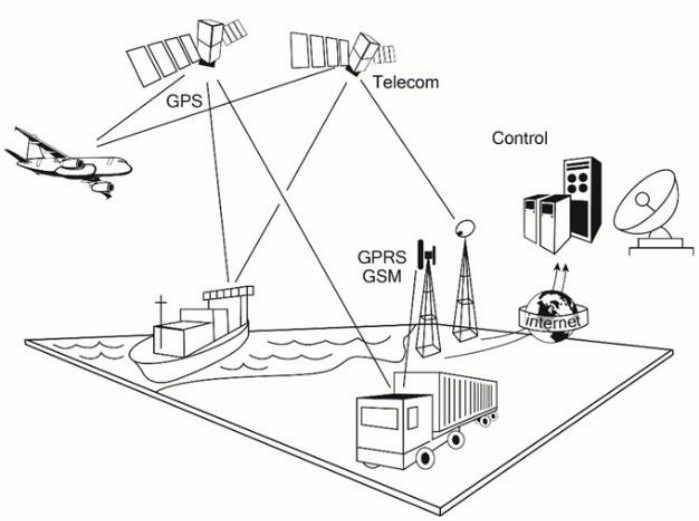

Figure 1: AASD Network Architecture

Figure 2 shows a top-level network architecture for connected AASD consisting of three segments: an end-user segment, a communications segment, and a control segment. The end-user segment includes automobiles, trucks, airplanes, ships, and the people who operate them. More specifically, the end-user segment includes a network node with equipment that transmits, receives, processes, and stores system data for use by the AASD or a human end user.

The communications segment, which may be comprised of a satellite communications network, a terrestrial wireless network, or a combination thereof, routes data and information to and from a data source or control facility and the AASD. When the communications segment includes satellite-based navigation, data, or communications services, the communications segment also includes space-based communications nodes. These space-based communications nodes comprise the satellite constellation and the onboard payload(s) that transmit and route data and information traffic. When the AASD communications segment includes a

cellular wireless communications network, the communications segment nodes comprise wireless cell towers, hotspots, or other wireless cellular equipment.

The third and final AASD network segment, the control segment, combines several functions distinct from the AASD end-user or the communications backbone itself. The control segment includes any terrestrial data source that supplies information to the AASD via the communications segment. The control segment also includes any terrestrial facility that monitors network configuration, bandwidth, power, and antennae as necessary to comply with the service objectives and licensing obligations of the satellite or cellular network. Some AASD applications, for example an autonomous vehicle, also employ a staffed control center to actively monitor AASD system performance. In critical situations, the control center can directly intervene in AASD operations or render assistance as appropriate.[13] In more common, less urgent situations, the control center collects information about any observed performance aberrations or software vulnerabilities and provides software updates to the end user segment.[14]

Whether AASD exist as discrete items or within a larger connected network, their componentry, operation, and communications backbones are all subject to cyber-attack. For ease of discussion, these attack vulnerabilities can be aggregated and summarized as follows:

a) Disruption or suppression of the radio frequency signals transmitted between AASD network nodes,

b) Compromising the integrity of the information conveyed between AASD nodes by altering the content, embedding content, or intercepting content, and

c) Compromising the internal operation of equipment such as, for example, data storage and retrieval tasks, or the communications functions executed at an AASD node.

Ironically, the increasing sophistication of AASD leave them even more susceptible to these attack vectors and exacerbates the

---

[13] WATNEY & DRAFFIN, *supra* note 5, at 2-4.

[14] *Id*.

resulting consequences. Inclusion of a greater number of machine-to-machine communications, interconnectivity, and autonomous operations reduces human oversight. As a result, unauthorized intrusions become more difficult to detect, and response interventions more difficult to effect than in previous designs. The growing proliferation of AASD also provides ever more access points through which harm can be wreaked.

Providers of AASD must now also manage the quality and security of constituent items provided by multi-national sources via a global logistics chain. Shared service models and the outsourcing of key operations add to the complex and interlocking nature of the modern supply chain. Numerous parties thus contribute to the design and operation of modern-day AASD. As the number of participants in AASD logistic chains grow, so too do the system vulnerabilities.[15]

Recent documented incidents leave no doubt that these vulnerabilities exist in reality and not as theoretical abstractions. A study reported in the *MIT Technology Review* documented the spoofing of shipboard Automatic Identification Systems ("AIS") to make fake vessels appear, real ships disappear, and to issue false emergency alerts.[16] An August 2017 report by BBC News documented numerous attacks on shipboard systems, including one where a hacker hacked into the satellite communications of a tanker ship at sea.[17] Although the hacker, a cybersecurity researcher, did no damage, the opportunity existed to alter software in the communications link, manipulate the ship's position reporting, or infect with malware the other shipboard systems connected to that network.[18]

---

[15] *See* DAVID LIVINGSTONE & PATRICIA LEWIS, SPACE, THE FINAL FRONTIER FOR CYBERSECURITY? 13-15 (2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[16] Tom Simonite, *Ship Tracking Hack Makes Tankers Vanish from View*, MIT TECH. REV. (Oct. 18, 2013), https://www.technologyreview.com/s/520421/ship-tracking-hack-makes-tankers-vanish-from-view/.

[17] Chris Baraniuk, *How Hackers are Targeting the Shipping Industry*, BBC NEWS (Aug. 18, 2017), http://www.bbc.com/news/technology-40685821.

[18] *Id*.

Cybersecurity incidents are not just limited to the maritime industry. In October of 2014, the weather satellite network of the National Oceanic and Atmospheric Administration suffered a disruption in service mere months after the OIG issued a report outlining the agency's vulnerability to attack.[19] At the 2017 CyberSat Summit in Tysons Corner, Virginia, experts from the Department of Homeland Security admitted they wirelessly hacked into the Department's own Boeing 757 aircraft while it sat on a tarmac.[20] A recent article by JC Reindl of the *Detroit Free Press* summarized the history of automobile cyber-hacks and admonished readers via the headline: "Car hacking remains a very real threat as autos become ever more loaded with tech."[21]

AASD are thus becoming increasingly embedded in the global infrastructure, actual attacks are occurring, and evolving system attributes are making cyber threats more likely. Yet, market forces and technological advancements are discouraging, rather than encouraging, the rigorous confrontation of these threats. The rapid pace of innovation makes certain markets highly competitive. In those markets, providers must constantly innovate and provide new

---

[19] *NOAA Confirms Cyberattack 'in Recent Weeks,'* NBC NEWS (Nov. 12, 2014, 8:28 PM), https://www.nbcnews.com/news/us-news/noaa-confirms-cyberattack-recent-weeks-n247446. *See generally* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF COM., OIG-14-025-A, SIGNIFICANT SECURITY DEFICIENCIES IN NOAA'S INFORMATION SYSTEMS CREATE RISKS IN ITS NATIONAL CRITICAL MISSION (2014), https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf; OFFICE OF INSPECTOR GEN., U.S. DEP'T OF COMMERCE, OIG-16-043-A, SUCCESSFUL CYBER ATTACK HIGHLIGHTS LONGSTANDING DEFICIENCIES IN NOAA'S IT SECURITY PROGRAM (2016), https://www.oig.doc.gov/ OIGPublications/OIG-16-043-A.pdf (finding that systems were vulnerable to attack because the weakness identified in the previous report had not been addressed, and also evaluating the agency's subsequent response to the attack).

[20] Calvin Biesecker, *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*, AVIONICS INT'L (Nov. 8, 2017), http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/.

[21] JC Reindl, *Car hacking remains a very real threat as autos become ever more loaded with tech*, USA TODAY (Jan. 15, 2018, 1:56 PM), https://www.usatoday.com/story/money/2018/01/14/car-hacking-remains-very-real-threat-autos-become-ever-more-loaded-tech/1032951001/.

offerings to remain viable.[22] The imposition of additional design requirements to address cybersecurity issues can retard the deployment of new capabilities and the exploitation of first-to-market opportunities.[23]

For these reasons, the Federal Communications Commission ("FCC") argues that the communications industry's cybersecurity practices fall short due to market failures.[24] In a report dated January 17, 2017, and issued prior to the current administration, the FCC cited evidence of three distinct types of market failures contributing to underinvestment in internet cybersecurity.[25] The first of these failures notes that imperfect information exists among network operators and system users. Network operators often lack information about attacks experienced by others and the effectiveness of deployed solutions in responding to those attacks.[26] The second notes that investment in cybersecurity practices varies as a function of market power. Markets with minimal competition leave consumers with little choice but to purchase services from a given provider regardless of the level of cyber-threat protection. [27] Conversely, as noted above, robust competition may penalize those who invest time and resources into cybersecurity by delaying introduction of their offerings into fast-moving markets. Finally, the FCC notes that cybersecurity best practices have both positive and negative externalities that disincentivize both service providers and end users from engaging in optimal levels of cyber countermeasures and behaviors.[28] The burgeoning Internet of Things ("IoT") and autonomous systems markets only exacerbate this investment shortfall as the negative externalities imposed upon third parties by

---

[22] *See* LIVINGSTONE & LEWIS, *supra* note 15, at 12.

[23] *Id*.

[24] DAVID SIMPSON, PUB. SAFETY & HOMELAND SEC. BUREAU, FCC, CYBERSECURITY RISK REDUCTION 40–51 (2017), https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/jan2017/cs2017_0017.pdf.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

cyber events provide little incentive for providers to avoid them.[29] While the FCC study focused specifically on the communications industry, the market failure issues and concerns raised therein are equally applicable to the larger AASD context.

Nonetheless, most transportation and communications industry segments do not believe dealing with cybersecurity threats requires additional legislation or regulation.[30] Industry participants argue many of the cybersecurity risks inherent in AASD can be mitigated via thoughtful engineering and design, personnel and vendor policies, and operations protocols as a matter of best practice. A significant subset of AASD providers additionally point to the dual-use nature of their product and service offerings. As suppliers to the federal government, these providers must satisfy the government's stringent security requirements, and therefore security in the private sector benefits without needing to impose additional oversight.[31]

The need for some sort of effective incentive to maintain cyber-vigilance and thwart attacks is of even greater importance in the transportation sector than in other portions of the economy. Unlike hacking of credit cards, personal information, or other data breaches, hacks of AASD can inflict bodily harm—even fatalities. The harms that can result from AASD breaches in the transportation sector thus are not limited to the financial. The systems on which AASD are

---

[29] *Id*. See Eli Dourado & Jerry Brito, *Is There a Market Failure In Cybersecurity?*, MERCATUS: TECH. POL'Y (Mar. 6, 2012), https://www.mercatus.org/publication/there-market-failure-cybersecurity, for a discussion of market failures and externalities in the cybersecurity context.

[30] *See, e.g.*, *Cybersecurity*, TELECOMM. INDUS. ASSOC., https://www.tiaonline.org/what-we-do/advocacy/policy-issues/cybersecurity/ (last visited Sept. 4, 2018) (stating that "[r]igid regulatory requirements cannot keep pace with rapidly evolving technologies and threats and require industry to comply with obsolete security requirements rather than addressing real-time threats, effectively making systems less secure"); *see also* Eric Kulisch, *Cybersecurity push may tie up autonomous-car legislation: Automakers, senators at odds over best approach*, AUTOMOTIVE NEWS (June 24, 2017, 12:01 AM), http://www.autonews.com/article/20170624/OEM11/170629894/cybersecurity-autonomous-legislation-sen-markey (describing automakers' resistance to proposed cybersecurity legislation).

[31] *See* Pete Roney, Chief Innovations Officer, Thales, Address at the Economist's A New Space Age Conference: The Data Race (Nov. 9, 2017).

employed carry persons on highways, through the air, and on the high seas. Their failure not only impacts these direct users but also the third-party bystander crossing the street, or child playing in a yard.[32] Often, the conversations surrounding the need for cybersecurity regulations trigger an all or nothing debate, and fail to recognize the distinctions between the degrees of automation, the severity of the consequences, and the resulting sliding scale of damage. Depending on the severity of consequences and safety of life considerations, different levels of regulatory oversight might be warranted.

This paper explores how existing private law mechanisms and public law mechanisms promote cybersecurity behaviors and motivate transportation sector AASD providers and users to take actions that reduce the risk and consequences of cyber-threats. More specifically, this paper explores the effectiveness of the following private law risk allocation mechanisms: contract law, insurance, and product liability. The effectiveness of these private law mechanisms, if sufficient, may obviate the need for formal regulation. Conversely, if these private law measures are weak or relatively ineffective at promoting cybersecurity behaviors, regulation is warranted as a matter of public safety. This paper also surveys the existing U.S. regulations that impact transportation sector cybersecurity and evaluates the manner in which current regulations promote the desired behaviors. From the entirety of this analysis, the appropriateness of (and opportunities for) additional legislation or private law solutions emerge.

---

[32] *See, e.g.*, Aarian Marshall & Alex Davies, *Uber's Self Driving Car Saw the Woman It Killed, Report Says*, WIRED (May 24, 2018, 3:38 PM), https://www.wired.com/story/uber-self-driving-crash-arizona-ntsb-report/ (describing the fatal collision of a self-driving car with a third-party pedestrian walking a bicycle). Although this tragic accident did not result from a cybersecurity breach, the event demonstrates that third parties are potential victims when AASD malfunction or behave in unanticipated ways.

III. PRIVATE LAW MECHANISMS FOR INFLUENCING AASD CYBERSECURITY

Private law mechanisms that encourage manufacturers and service providers to undertake cybersecurity behaviors include:

(a) Contractual agreements,

(b) Use of Cover, and

(c) Tort law via product liability.

The sub-sections below examine each in turn.

A. *Contractual Agreements*

Parties procuring or supplying AASD will always do so under some sort of written agreement that allocates the risk of cybersecurity events amongst the contracting parties. In two of the three markets considered, marine and aviation, a large mass market does not exist, making it difficult to examine a sample agreement or ascertain the relative bargaining strength of the supplier and consumer of services. Both parties to this type of transaction are likely to be highly sophisticated; and the manner in which AASD are operated and procured likely puts both parties in a position to efficiently mitigate certain types of potential harms. For example, a ship owner may be in the best position to reduce the risks stemming from any compromise of shipboard earth stations by adopting prudent watch standing practices, while the service provider is in the best position to mitigate the risks associated with data corruption by patching known software vulnerabilities.

However, in typical contracting terms, the AASD provider usually disclaims all financial harms such as incidental and consequential damages, as well as disclaiming all warranties.[33] Typical terms also severely limit the ability to recover damages.[34] Only with extreme difficulty or significant bargaining power will even a sophisticated purchaser of AASD be able to substantially revise such provisions. Thus, sales and support agreements are

---

[33] *See* MICHAEL OVERLY & JAMES KALYVAS, SOFTWARE AGREEMENTS LINE BY LINE 51-66 (Aspatore Books 2004).

[34] *See id*. at 63 (highlighting that most commercial software licenses limit recovery "to all or some portion of the fees paid for the software").

unlikely to influence the cybersecurity of AASD design or operation beyond that minimally necessary for the seller to exist in the marketplace.

In the third market segment, automotive, the contracting power resides almost exclusively with the Original Equipment Manufacturer ("OEM").[35] Neither suppliers nor end-users hold much sway over the allocation of risks in the subject agreements. Purchasers of automotive vehicles take the vehicle subject to the OEM's software license terms, or the pass-through licenses of the OEM's supplier, with no opportunity to negotiate on matters other than the vehicle price. Suppliers wish to access the lucrative aftermarket for spare parts and additional services that stem from being included in the OEM's vehicle offering.[36] In exchange for this advantageous market position, suppliers typically offer little resistance to the OEM's supplier agreements.[37] These OEM agreements generally seek to avoid both the costs of undertaking cybersecurity measures and the liabilities for any resulting harms, although there is evidence that some information technology suppliers have been able to negotiate these terms.[38] Nonetheless,

---

[35] A company that produces a product from component parts supplied by others. For example, an automobile manufacturer or airplane manufacturer.

[36] Omri Ben-Shahar & James J. White, *Boilerplate and Economic Power in Auto Manufacturing Contracts*, 104 MICH. L. REV. 958, 981‑982 (2006). While Ben-Shahar and White focused on Tier 1 suppliers, defined as "anyone who sells directly to an OEM," to the auto industry, *id*. at 955, they noted that the OEM's admit to using rigid boilerplate forms drafted in "a one-sided, self-serving manner." *Id*. at 981. The authors additionally note that suppliers will often invest significant sums for tooling and production in hopes that they will be able to support continued production and supply of service parts for the lifecycle of the vehicle. *See id*. at 963; *see also OEM Supplier Relations and Deregulation*, JET-TEK, https://jet-tek.com/aerospace-industry-direction/oem-supplier-relations-deregulation/ (last visited Sept. 6, 2018) (describing similar behaviors in the aerospace sector and noting that suppliers are willing to absorb significant investment costs to secure a position in the production supply chain and access to aftermarket revenue streams).

[37] Ben-Shahar & White, *supra* note at 36, at 981‑82 (noting suppliers are often "captives" of the OEMs).

[38] *Id*. at 960‑61, n.31 (noting that OEMs draft broad indemnity terms obligating suppliers to reimburse and defend the OEM against product liability claims).

contracting terms are still likely to be very favorable to the OEM and provide few contract incentives for the OEM to undertake cybersecurity measures on their own.[39] In those cases where an information technology provider has negotiated to provide a cap on liability or warranty claims, such terms limit the supplier's financial risk. Reason suggests that such provisions may also dampen the supplier's incentive to aggressively work cybersecurity issues generally as well as those specifically arising from the OEM's use case.

Additionally, in all transportation sectors, certain types of harm, including significant physical harms, may in fact be borne by third parties not a party to any AASD agreement. A seaman injured when his ship runs aground due to corrupted navigation data will not likely benefit from the damages and liability provisions contained within the shipping line's AASD contract. AASD contracts allocate the risks of financial harms, including third party financial liability, between the contracting parties.[40] Yet, the AASD agreement likely does nothing to allocate risks between third parties and the AASD suppliers or users, since those third parties do not exist as a party or intended beneficiary to the agreement.

B. *Insurance*

Parties providing and procuring AASD may wish to procure cover to ameliorate the losses suffered from cyber-threat events. Cover is most commonly obtained as an insurance product, but cover to protect against losses can also be attained via other financial instruments such as a bond, or maintenance of a cash reserve.[41]

However, Ben-Shahar & White also note that IT suppliers can sometimes secure more favorable terms that limit warranties and cap remedies at repair and replacement. *Id*. at 978.

[39] *Id*. at 960 (alleging that the OEM's one-sided contract terms are economically inefficient because the OEM has little incentive to avoid or address product quality issues directly; and further noting that the OEMs with the most self-serving contract language take the longest to identify and resolve a defect).

[40] *See, e.g.*, OVERLY & KALYVAS, *supra* note 33, at 51-66.

[41] *See, e.g.*, 46 C.F.R. § 540.24 (2018) (describing various types of financial vehicles available to operators of passenger vessels as proof of adequate financial responsibility for liabilities arising from death or injury to passengers).

When cover is procured via an insurance product, the underwriter would theoretically be incentivized to reward those behaviors that mitigate cyber-threats and reduce the probability of paying out a claim. Both aviation and maritime insurance contracts, however, specifically exclude cyber event coverage via standard pro-forma clauses.[42] The absence of insurance as a readily available form of cover means fewer financial resources exist to pay out claims made by third parties who suffer damage as a consequence of cyber-threats.

In the automotive industry, insurance providers appear to have a more progressive outlook, and appear to be prepping for the arrival of autonomous cars.[43] One study estimated that cybersecurity will be the greatest driver of premiums in the auto insurance segment,

---

[42] KATHERINE B. POSNER, TIM MARLAND & PHILIP CHRYSTAL, MARGO ON AVIATION INSURANCE APPENDIX: AVIATION POLICY FORMS, CLAUSES AND ENDORSEMENTS STANDARD CLAUSE AVN 48 (LexisNexis, 4th ed. 2016) (specifically excluding from coverage claims caused by "any malicious act or act of sabotage," however, none of the standard clauses or exclusions specifically mention cyber-attacks.); *see also* LLYOD'S MARKET ASSOCIATION, CYBER RISKS AND EXPOSURES: MODEL CLAUSES—CLASS OF BUSINESS REVIEW § 3 (Jan. 2018), https://www.google.com/url?sa=t&rct=j&q=&esrc =s&source=web&cd=1&ved=2ahUKEwiTlZHIr-HdAhXwITQIHXFzBCMQFjAAegQICRAC&url=http%3A%2F%2Fwww.lmalloyds.com%2FAsiCommon%2FControls%2FBSA%2FDownloader.aspx%3FiDocumentStorageKey%3Dc3910476-c5d4-47b1-bf3c-8b7e12e08299%26iFileTypeCode%3DPDF%26iFileName%3DCyber%2520Clauses%2520Review&usg=AOvVaw0lFlryOCXotAHBal-JdROA (noting that many aviation policies are "silent" regarding the coverage of cybersecurity claims but include the standard exclusion for " 'malicous acts and sabotage' (which potentially comprises cyber-attacks)" and for which additional coverage is available. The document additionally notes that clause CL380 is widely used in the marine industry to exclude cyber-attack coverage); *see also* Jonathon Saul & Carolyn Cohn, *Insurance gaps leave shipping exposed to growing cyber threats*, REUTERS (Jan. 12, 2017, 8:30 AM), https://www.reuters.com/article/us-shipping-insurance-cyber-idUSKBN14W1EA (confirming the maritime industry general practice as reported in the Margo text).

[43] *See* Werner Rapberger, *Markets Offering the Largest Cyber Security Insurance Opportunity*, ACCENTURE (Nov. 1, 2017) [hereinafter Rapberger, *Markets*], https://insuranceblog.accenture.com/markets-offering-the-largest-cyber-security-insurance-opportunity.

projecting a total of $64 billion by 2025.[44] These automobile policies anticipate underwriting coverage for ransomware, vehicle theft, unauthorized entry, and identity theft.[45] Of note, a review of these policies as described in the available literature appear to address only the economic harms suffered by the driver, and do not underwrite bodily injury to the driver or others resulting from the compromise of automotive AASD.

The availability and scope of policies to underwrite the cybersecurity risks faced by OEMs and automotive AASD suppliers also continues to evolve. As in the aviation and marine insurance markets, such risks are disclaimed by standard policy provisions and the ability to purchase riders expansive enough to cover risks beyond data breaches appears quite limited.[46] Although some insurance products such as AIG's CyberEdge offer a complete corporate insurance product, which includes protection against third party claims, the industry struggles to introduce new coverages.[47] Underwriters cite the following problems in assessing risk: a lack of data reporting actual events; and that the amount of data currently available is insufficient to support the actuarial processes.[48] Underwriters also live in fear that a single cyber hack or breach could result in a cascading and catastrophic accumulation of

---

[44] *Id*.

[45] *Id*.

[46] *See* Tony Chimino, *5 Types of Cyber Liabilities for Manufacturers*, 18 INDUSTRY TODAY, no. 3, 2015, at 30–37, https://industrytoday.com/article/5-types-of-cyber-liabilities-for-manufacturers/ (noting that general liability policies now typically exclude cyber risks requiring the purchase of separate, additional policies); Jayleen R. Heft, *7 Challenges Insurers Face in the Cyber Insurance Market*, PROPERTYCASUALTY360 (Mar. 8, 2017, 7:01 PM), https://www.propertycasualty360.com/2017/03/08/7-challenges-insurers-face-in-the-cyber-insurance/?slreturn=20180805001533 (noting that cyber insurance products are a "work in progress" and that existing products narrowly define the risks underwritten and ignore many of the cyber risks companies actually face).

[47] *See* Werner Rapberger, *The New Shape of Cyber Security Insurance – Meeting Evolving Threats Head On*, ACCENTURE (Nov. 8, 2017) [hereinafter Rapberger, *New Shape*], https://insuranceblog.accenture.com/the-new-shape-of-cyber-security-insurance-meeting-evolving-threats-head-on.

[48] *Id*.

claims.[49] Given these uncertainties, cover for cyber-related risks is usually comprised of non-standardized products that are not widely available—at least at the moment. Furthermore, even when available, studies note that only 50% of U.S. businesses obtain cyber risk insurance to cover either their business or their products.[50]

Insurance therefore does not exist as a mechanism to promote AASD cybersecurity because widespread underwriting of these risks does not exist. Thus, the opportunity for insurers to exert influence over AASD providers through counseling and oversight of the insured is essentially nonexistent for the transportation sector.

C. *Product Liability Tort Law*

Beginning in the late 1800s, courts began holding manufacturers and others liable for distributing defective products that cause injury.[51] The courts, and the later-enacted state product liability laws, enabled the pursuit of such claims under theories of negligence, strict liability, or breach of warranty.[52] Whether via common law or legislation, products liability law seeks the attainment of two public policy goals: (1) to compensate those injured by unsafe products; and (2) to provide incentives for manufacturers to take reasonable precautions in the design and manufacture of their products.[53] The later purpose recognizes that manufacturers are often the parties with the best opportunity and lowest cost to minimize or avoid any downstream harms resulting from the intended use of their products.[54]

Criticism of product liability law notes that such laws may not be necessary where consumers have both the information and the

---

[49] *Id*.

[50] Rapberger, *Markets*, *supra* note 43.

[51] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 cmt. a (AM. LAW INST. 1998).

[52] *Id*.

[53] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1533-34 (2013), https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1.

[54] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 cmt. e, § 2 cmt. a.

opportunity to select those products they deem safer than others.[55] Manufacturers of safer products are therefore rewarded in the marketplace with a greater number of sales. These supply and demand market forces combine such that consumers purchase, and manufacturers also provide safety benefits at an economically efficient level.[56]

In the case of autonomous and automatic systems, however, the end users of such products may not be aware of the information needed to discriminate on this basis until after a potentially fatal accident has occurred. In addition, by design, the operation of autonomous and automatic systems is not transparent to even the most sophisticated of users. The consumers of such systems likely possess little practical information about how the system performs and may not even be aware of a cyber breach until well after the fact.[57] These unique aspects of AASD leave the purchasers of such systems with little opportunity to avoid the harms of cyber malfeasance on their own, other than by installing patches supplied by the manufacturer.[58] As a practical matter, end users may also possess little real marketplace choice if the entire industry underspends on preventing cybersecurity risks.[59] Therefore, holding

---

[55] *See generally* A. Mitchell Polinsky & Steven Shavell, *The Uneasy Case for Product Liability*, 123 HARV. L. REV. 1437 (2010), https://harvardlawreview.org/2010/04/the-uneasy-case-for-product-liability/.

[56] *Id*.

[57] *See, e.g.*, Steven Overly, *What we know about car hacking, the CIA and those WikiLeaks claims*, WASH. POST (Mar. 8, 2017), https://www.washingtonpost.com/news/innovations/wp/2017/03/08/what-we-know-about-car-hacking-the-cia-and-those-wikileaks-claims/?noredirect=on&utm_term=.596922bec42a (quoting cybersecurity researcher Chris Valasek: "It doesn't appear that any manufacturers currently have detection/prevention methods for such attacks," and noting that experts such as University of Michigan researcher Sam Lauzon and cybersecurity expert Yoni Heilbron believe it can be difficult to know when a vehicle has been hacked); *see also* Steve Tengler, *Top 10 Unspoken Automotive Cybersecurity Risks*, WARDSAUTO (Jul. 17, 2018), https://www.wardsauto.com/industry-voices/top-10-unspoken-automotive-cybersecurity-risks.

[58] Tengler, *supra* note 57.

[59] *See id*. (noting the business and financial challenges in providing automotive cybersecurity to consumers). See also Dourado & Brito, *supra* note 29, for a

manufacturers of AASD accountable for the harms resulting from insecure devices aligns with the public policy purpose of products liability law by encouraging investment in security measures by the party that can better assess the risk and more efficiently bear the burden.

Yet, most commentators remain skeptical that product liability principles can be successfully applied to insecure software and equipment.[60] The relative inability of private parties to allocate the risks of cybersecurity via contract and warranty claims has been noted previously above. Breach of warranty due to defective cyber-secure design is likely to have been explicitly disclaimed.[61]

Imposing products liability for defective software, data, and equipment via concepts of negligence or strict liability also remains problematic.[62] The core inquiry in such cases centers on whether the harm resulted from a product defect caused by either: a deficiency in the product's design, its manufacture, or in warnings about its inappropriate use.[63] Software code prone to hacking has typically been viewed as suffering from a design defect.[64] Furthermore, the possibility exists that firmware or chips containing malware supplied via a manufacturer's supply chain, or certain unanticipated instabilities in code operation might be considered a manufacturing defect to which strict liability attaches. Whatever the origin of the alleged defect, applying the current legal tests used to establish negligence in the design, or deficiencies in manufacture, pose significant difficulties in the context of software and cybersecurity.[65]

---

general discussion of how market failures can contribute to underspending on cybersecurity.

[60] *See generally* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913 (2017), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr.

[61] OVERLY & KALYVAS, *supra* note 33, at 52.

[62] Butler, *supra* note 60, at 915–16.

[63] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (AM. LAW INST. 1998).

[64] Butler, *supra* note 60, at 917.

[65] *Id*.

Two tests exist for establishing the existence of a design defect. The first adopts a risk vs. utility test to determine if the foreseeable harms could be avoided via adoption of a reasonable alternative design. This test rapidly devolves into a highly technical argument about whether the hack or resulting harm could have reasonably been avoided if the code were reasonably rewritten in an alternative manner.[66] The second, a consumer expectations test, examines whether the product performs safely when used as intended.[67] This second test, while more closely aligned with concepts of strict liability, can pose difficulties in application when the product is truly complex or poses obvious risks of use.[68]

A third source of products liability, the duty to warn, exists in the jurisprudence of more than half the states and in the *Third Restatement of Torts*.[69] This legal test also balances the risks vs. the burden of providing the warning. Courts are more likely to impose this duty when an ongoing relationship exists with the customer post-sale.[70] In the context of AASD, such warnings might include providing security patches, the supply of which serves to notify the user of a cyber vulnerability.

Optionally, the duty to warn could conceivably include a blanket warning that harm may result by not maintaining a vigilant watch over the performance of the system even though automated. This latter type of warning may be most effective in those transportation applications where professional licensed personnel such as pilots and ships' masters remain ultimately responsible for the overall vehicle operation. This type of warning may be ineffective or unjustified in driverless cars where one benefit of the product is to enable transportation for elderly or otherwise impaired drivers.

The duty to warn, even where it exists, may also give rise to counterproductive outcomes. For example, actually providing a security patch or a warning to operators about potential consequences of hacked systems, may perversely serve as a means

---

[66] *Id*.
[67] *Id*.
[68] *Id*.
[69] *Id*. at 918.
[70] *Id*.

for manufacturers to avoid liability for design defects that might have been avoided in the first place. Ultimately, the harm caused by cyber breaches results from the bad acts of a third party. But, no one today can claim that such acts are not foreseeable. And, manufacturers remain the parties best able to take actions that protect against these harms—exactly the type of behavior that products liability law is designed to incentivize.

Yet, even if liability can be established under the existing theories of product liability outlined above, there remains the issue of quantifying and proving harm. As a general rule under the *Restatement of Torts* and as adopted by several states, manufacturers are not liable for the economic harm suffered from use of the defective product.[71] This limitation on recovery "has long been viewed as an impediment to products liability" for defective software and systems.[72] In the transportation sector, such economic harms might include, for example, improper navigation performance that routes an aircraft or vehicle in such a manner that it consumes additional fuel or causes a rippling effect of transportation system delays; or an automobile rendered useless by ransomware. Application of the economic loss doctrine would not permit recovery of such pecuniary losses under the *Restatement of Torts,* even if such harms resulted from an insecure, defectively designed AASD.

Other types of losses, may however, be recoverable. In the transportation sector, many foreseeable harms are not economic and unfortunately include physical harm to tangible assets, such as an automobile, a ship, or an aircraft; as well as bodily or emotional harm to their occupants. Moreover, these same types of harm could potentially be inflicted upon innocent bystanders. At present, the law is unclear on whether these types of damages resulting from cyber breaches of a defective product can be recovered, although proposed changes to the Restatement favors recovery for damage to tangible property or physical injury arising from insecure devices.[73]

---

[71] *Id*. at 919.
[72] *Id*. at 920.
[73] *Id.* at 921.

Product liability law as an incentive for hygienic cyber-security behaviors thus holds much promise, but the state of its development is immature. Not all types of harms suffered, even though potentially significant, can be recovered. Additional limitations on the effectiveness of product liability law arise not only from the difficulty of proving defective design in this context, but in the ability of manufacturers to use warnings and subsequent software patches to avoid liability. This latter outcome may perversely result in underinvestment in the initial cybersecurity design.

IV. PUBLIC LAW: CYBERSECURITY REGULATION OF AASD

Given the difficulties faced by private law in encouraging and achieving a desired level of cybersecurity behaviors, a reasonable alternative lies in the promulgation of regulations via the public sector. But, this approach also remains fraught with difficulties. Cybersecurity regulation within the transportation sector exists as a multitude of separate regulatory approaches by specialist executive branch agencies with no overarching coherent federal approach, and only limited inter-agency coordination.[74]

The sections below contain a detailed review of the current transportation sector-specific regulations and those that bear upon its cybersecurity. Regulations contain the detailed implementation of the broader statutory authority from which they derive and define the particular actions AASD providers, manufacturers, and users must undertake. And, as noted previously above, agencies sometimes refrain from promulgating cybersecurity regulations even when they are statutorily enabled to do so. A survey of relevant agency regulations therefore enables a comparison of the various regulatory frameworks and identifies opportunities for reform.

More specifically, the sections below contain a detailed review of the regulations promulgated by the following federal agencies. The FCC Rules control the provision and use of the satellite telecommunications systems and terrestrial wireless networks that

[74] FISHER, *supra* note 5.

form the communications backbone of a connected AASD.[75] The U.S. Coast Guard promulgates rules pertaining to maritime operations.[76] The Federal Aviation Administration ("FAA") promulgates rules pertaining to aircraft operations, and the National Highway Transportation Safety Administration promulgates rules pertaining to manufacture and sale of autonomous surface vehicles.[77] Potential utilization of remote sensing data by AASD make the National Oceanic and Atmospheric Administration (NOAA) regulatory framework also of interest.[78]

A. *Rules Applicable to All Connected AASD: FCC Regulations*

The FCC regulations relevant to AASD address the telecommunications components of the AASD communications segment. As shown in Figure 2 above, many AASD connect to a communications backbone for purposes of receiving and transmitting data and control information. In most applications, the communications segment connects to the internet or a dedicated communications circuit via cellular wireless communications. Increasingly, AASD communications segments include mobile satellite services ("MSS"), especially in remote areas or over the high seas. All MSS and wireless service providers must comply with the licensing, technical, and operating regulations promulgated by the FCC, regardless of the specific type or use of the mobile service. The FCC regulations also implement and mandate compliance with

---

[75] *See* 47 U.S.C. § 151 (2018) (describing the authority of the FCC to regulate radio services generally).

[76] 14 U.S.C. § 2(3) (2018).

[77] 49 U.S.C. §§ 106, 40101 (2018) (establishing the FAA and defining its policy objectives respectively); 14 C.F.R. ch. I (containing the aviation safety regulations); 49 U.S.C. §§ 105, 30101 et seq. (providing the basis and framework for the National Highway Transportation Safety Administration enforcement authority over motor vehicles).

[78] For example, satellite remote sensing data of fields and crops, coupled with GPS data, can enable a farmer's equipment to precisely modulate the amount of fertilizer and water applied to locations within a field. *See, e.g.*, P. C. Scharf, et al., *Remote Sensing for Nitrogen Management*, 57 J. SOIL & WATER CONSERVATION 518 (2002), https://pdfs.semanticscholar.org/5513/8b91a9fe6bf475541e374500d218cfe4724f.pdf.

the ITU Radio Regulations and the radio provisions of all international treaties to which the United States is a party.[79] Thus, to the extent FCC regulations and the ITU Radio Regulations mandate cybersecurity protections, any requirements will be applicable to all operators of AASD regardless of type.

1. *FCC Regulation of MSS*

The International Telecommunications Union ("ITU"), classifies mobile satellite services ("MSS") into five separate subcategories of service: maritime mobile satellite service ("MMSS"); land mobile satellite service ("LMSS"); aeronautical mobile satellite service ("AMSS"); personal mobile satellite service (PMSS); and broadcast mobile satellite service ("BCMSS").[80] Of these broad categories, MMSS, LMSS, and AMSS are the most relevant to implementation of AASD in the transportation sector.

The licensing provisions of 47 CFR Part 25 address the initial licensing of MSS systems and apply separate criteria to the licensing of space stations and earth stations.[81] Appendices A-1 and A-2 contain tables summarizing the specific FCC licensing regulations applicable to MSS. These regulations primarily operate to ensure that equipment will transmit within the assigned frequency band without harming others' use of the radio spectrum. Additional regulations address system ownership and restrict communications with non-U.S. satellites.[82] While the regulations reduce cybersecurity threats by constraining the number of interfaces with non-U.S. persons and systems, the purpose of these regulations is not cybersecurity, but the oversight of market competition and compliance with U.S. treaty commitments.

---

[79] *See, e.g.*, 47 C.F.R. § 80.86.

[80] Int'l Telecomm. Union [ITU], Radio Reg. art. 1.19–1.60, *Section III – Radio Services*, *in* Volume 1 Radio Regulations: Articles, Chapter 1: Terminology and Technical Characteristics, at 9–13 (2016).

[81] 47 C.F.R. § 25.

[82] *See* 47 C.F.R. §§ 25.135, .137, .143, .149 (restricting communications with non-U.S. satellite systems); 47 C.F.R. § 20.5 (documenting citizenship requirements).

Other operational requirements applicable to all types of satellite communications can be found in Subpart D of 47 CFR Part 25. Certain of these general operating provisions are relevant to cybersecurity best practices. For example, 47 CFR § 25.271 requires operators of transmitting stations to stand watch at all times whenever the station is transmitting.[83] Transmitting facilities must be protected against both unauthorized access and unauthorized operations whenever an operator is not present at the station.[84] Within the 1.5/1.6 GHz frequency bands, mobile earth stations must include features that ensure the station accesses the communications network subject to the frequency use priority rights of others.[85] Mobile earth stations operating within these bands must also transmit a unique terminal identification code upon any attempt to access the network and must be configured to immediately inhibit its transmissions upon receiving a channel shut off command or upon loss of channel assignment and control information.[86] These requirements, while intended to preserve the frequency sharing schemes between primary and secondary uses of the spectrum, do afford some measure of protection should hackers attempt to initiate unauthorized use of MSS earth stations because these requirements either thwart unauthorized access or make unauthorized access detectable.

Later chapters of the FCC regulations apply more specific Rules to operation of MMSS, VMSS, and AMSS.[87] The FCC requires operators of all ship earth stations, and all aircraft earth stations to be licensed and to display such license.[88] Operator licenses are not required for automobile receive-only earth stations. Although certain licenses are granted automatically by rule, foreign

[83] 47 C.F.R. § 25.271.
[84] 47 C.F.R. § 25.271(d).
[85] 47 C.F.R. § 25.287.
[86] *Id.*
[87] See 47 C.F.R. pts. 80, 87, 90, for maritime, for aviation, and private land mobile services respectively.
[88] See 47 C.F.R. §§ 80.51, .13, for ships and 47 C.F.R. §§ 87.19, .103, for aircraft.

governments and their representatives cannot obtain earth station licenses.[89]

Ships subject to the Communications Act or the Safety Convention are also subject to annual inspection of their shipboard communications equipment.[90] Additional operating rules define communications protocols to ensure that a single station does not unduly monopolize the operating frequency.[91] In the aviation environment, the FCC places additional physical controls upon operations of the transmitter. Specifically, 47 CFR § 87.143 states that transmitters must be installed such that only authorized users have access and airborne transmitters must be able to be switched off by the operator.[92]

2. *FCC Regulation of Mobile Radio Services*

A review of the FCC's wireless network ownership and operator regulations reveals approaches and issues similar to those outlined above in connection with MSS. As in the case of MSS, the FCC requires a license to operate the service.[93] Ownership of the wireless network is only available to U.S. citizens and corporations controlled by U.S. entities.[94] Carriers having more than sixteen employees must also file an annual employment report, but this report merely documents the demographics and diversity of the carriers' personnel.[95] The required employment report does not reach matters of interest to cybersecurity such as vetting or credentialing of those employees.[96]

---

[89] See 47 C.F.R. §§ 80.13, .15, for ships and 47 C.F.R. § 87.19, for aircraft. Note that alien persons and corporations cannot obtain an aircraft earth station license because the regulations prohibit foreign governments, foreign persons, and foreign corporations from holding station licenses.

[90] 47 C.F.R. § 80.59.

[91] *See, e.g.*, 47 C.F.R. § 80.141 (specifying shipboard radio communications protocols and technologies to prevent an open or "hot" mike); 47 C.F.R. § 87.185 (specifying communications protocols for aircraft).

[92] 47 C.F.R. § 87.143.

[93] 47 C.F.R. § 22.107.

[94] *See* 47 U.S.C. §§ 20.5, 310 (documenting citizenship requirements).

[95] 47 C.F.R. § 1.815; FCC Form 395.

[96] *Id.*

Additional Rules govern the technical performance of the wireless network and its equipment. Wireless network terminals, including end-user and intermediate communications nodes and equipment, must satisfy technical requirements that prevent harm to the public switched telephone network, and interference with others' lawful use of spectrum.[97] The FCC additionally requires certification that the wireless communications equipment complies with these technical conditions.[98] The cell towers and their radio equipment which form component parts of the wireless network are also regulated by the FCC.[99] Cellular radio facilities (i.e. radio stations/towers) must be registered with the FCC and comply with rigid technical specifications.[100] Via these Rules, much like in MSS, the FCC specifies the technical performance of the radio equipment and antennae to ensure lawful use of the spectrum and that transmissions do not interfere with others' lawful use of the airwaves. Much of the FCC's remaining rule-making regarding mobile services centers on tariffs, roaming, and spectrum allocation.[101]

3. *Other FCC Cybersecurity Policy and Guidance*

The FCC maintains a Public Safety and Homeland Security Bureau that encourages MSS and wireless service providers to implement the security countermeasures developed by the agency's Communications Security, Reliability, and Interoperability Council.[102] This Council, composed of industry participants, endeavors "to make recommendations to the [FCC] that promote the

---

[97] *See* 47 C.F.R. § 20.15(a); 47 C.F.R. pt. 68.

[98] *See, e.g.*, 47 C.F.R. § 68.201 (requiring certification by either a Telecommunications Certification Body or self-certification via a declaration of conformity); 47 C.F.R. § 68.218 (requiring that the responsible party warrants compliance with the applicable technical rules and regulations for interconnection with the public switched network).

[99] *See* 47 C.F.R. § 17.

[100] *See* 47 C.F.R. § 17.5, 22.150.

[101] *See* 47 C.F.R. pt. 20.

[102] *See, e.g.*, FCC, DA 17–799, FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ENCOURAGES IMPLEMENTATION OF CSRIC SIGNALING SYSTEM 7 SECURITY BEST PRACTICES (2017) [hereinafter FCC, FCC'S BEST PRACTICES], https://apps.fcc.gov/edocs_public/attachmatch/DA-17-799A1.pdf.

security, reliability, and resiliency of the Nation's communications systems."[103] The Council currently convenes three Working Groups, each Group focused on making recommendations regarding a single narrow sub-topic related to the Council's larger mission statement. Working Group 3, "Network Reliability and Security Risk Reduction," is the only current Working Group with a mandate specifically encompassing communications network cyber-security issues.[104] More specifically, the Working Group 3 identifies and examines security risks to: wireless protocols, the design and implementation of 5G networks, and IoT devices.[105] While from time to time, the Council, via this Working Group provides reports to the FCC , for reasons discussed further below, the FCC merely issues guidance that encourages, but does not require compliance with the Group's recommendations. Recently, for example, the FCC issued a Public Notice encouraging communications service providers to implement a recommended best practice to counter a known exploitation of the carrier system signaling protocols used by the network infrastructure.[106] Since these best practices are just suggestions by the FCC, compliance is entirely voluntary and not enforced.

4. *Summary and Analysis of FCC Cybersecurity Regulations*

This review of the FCC Rules governing the MSS and cellular networks that form the AASD communication backbone reveals that the existing FCC Rules do not address cybersecurity directly. Rather, the Rules primarily function to *ensure that an operator's legitimate use of their own systems does not interfere with or compromise the use of another's communication system.* As such, a significant percentage of the Rules focus primarily on technical configurations, antenna specifications, design tolerances, and

---

[103] *Communications Security, Reliability and Interoperability Council VI*, FCC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council (last updated Jul. 17, 2018).

[104] FCC, CSRIC VI WORKING GROUP DESCRIPTIONS 2 (2018), https://www.fcc.gov/files/csric6wgdescriptions3-2018docx (last updated Sept. 2, 2018).

[105] *Id*. at 3.

[106] FCC, FCC'S BEST PRACTICES, *supra* note 102.

operator protocols. Certain of the Rules, such as physical access requirements and preventing open mikes, may have ancillary positive impacts on cyber security although that outcome is not their primary purpose.

Although the FCC Rules do not currently address cybersecurity directly, under the previous administration, the FCC asserted that it had the statutory authority to make these types of Rules if it desired to do so.[107] As of this writing, however, the FCC only exerts oversight of cybersecurity behaviors during its review of potential telecommunications merger partners.[108] The agency explained its lack of rulemaking in this area in its January 2017 position paper by noting that additional study is needed before the Agency promulgates cybersecurity regulations.[109]

In point of fact, legitimate questions exist about the FCC's previous claim that its statutory authority extends to oversight of cybersecurity for cellular and satellite networks. More specifically, FCC Commissioner Michael O'Rielly recently wrote that he believes the FCC's cyber authority to be "extremely limited."[110] O'Rielly criticized previous Chairman Wheeler and others for the elastic interpretation of the FCC's enabling statute advanced in the 2017 position paper: an interpretation that would justify cybersecurity oversight of the communications infrastructure by the FCC.[111] Current FCC Commissioners do not agree on the agency's ability or inability to regulate cybersecurity matters. In recent testimony before Congress, FCC Chair Pai stated the agency lacked the authority to lead on cybersecurity.[112] But later in the same

---

[107] SIMPSON, *supra* note 24, at 40–51.

[108] *See id*. at 27–28 (citing *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Assign or Transfer Control of Licenses and Authorizations*, MB Docket No. 15-149, Memorandum Opinion and Order, 31 FCC Rec. 6327, 6519-20, ¶ 424 (2016) (Charter Merger Order)).

[109] *See* SIMPSON, *supra* note 24, at 52.

[110] Michael O'Rielly, *Abusing Section 1*, FCC: FCC BLOG (Feb. 21, 2018, 4:05 PM), https://www.fcc.gov/news-events/blog/2018/02/21/abusing-section-1.

[111] *See id.*

[112] *Hearing Before the S. Comm., Scien. & Transp. Comm., on FCC Oversight*, 115th Cong. (2018) (Statement of Ajit Pai, FCC Chair, & Jessica

hearing, FCC Commissioner Jessica Rosenworcel disagreed stating that the agency had an existing duty as public servants to engage in cybersecurity oversight and additional legislation was not needed.[113] As a consequence of this ambiguity, Democrats in Congress want new legislation to not only grant the FCC the necessary statutory authority, but to explicitly instruct the agency to proactively issue cybersecurity regulations for the communications networks it oversees.[114]

In 2017, Representative Yvette Clark (D) of New York introduced HR 1335, the Cybersecurity Responsibility Act of 2017. The draft legislation directs the FCC to issue new rules to secure communications networks from cyber risks.[115] As of this writing, September 2018 the bill has been introduced in the House and referred to the Subcommittee on Communications and Technology with no further action taken.[116] Thus, the creation of additional cybersecurity requirements for MSS and cellular networks remains unlikely given both the current administration and the existing statutory ambiguity.

Nonetheless, the FCC continues to proactively work with industry groups to better understand market conditions, legal and technical constraints, and cybersecurity best practices via the Communications Security, Reliability, and Interoperability Council. In 2015, the Council's Working Group 4 collaborated with multiple telecommunications industry segments to promote voluntary compliance with the NIST cybersecurity risk framework.[117]

Rosenworcel, FCC Comm'r), https://www.c-span.org/video/?c4744670/ fcc-commissioners-disagree-authority-cybersecurity-problems.

[113] *Id*.

[114] Kieren McCarthy, *FCC under fire for trying to ditch cybersecurity*, REGISTER (Mar. 10, 2017, 10:36 PM), https://www.theregister.co.uk/2017/03/10/fcc_under_fire_for_ditching_cybersecurity/.

[115] Cybersecurity Responsibility Act of 2017, H.R. Doc. No. 1335, 115th Cong. § 2(b) (2017) (citing 6 U.S.C. § 131 (2017)).

[116] *See H.R. 1335 - Cybersecurity Responsibility Act of 2017*, *All Actions H.R.1335*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/house-bill/1335/all-actions (last visited Sept. 4, 2018).

[117] COMMC'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, FCC, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES, WORKING GROUP 4:

Working Group 4 also documented that telecommunications providers found sharing of event and threat information to be a best practice for cyber risk mitigation.[118] Working Group 5 was therefore subsequently tasked with developing recommendations to encourage sharing of cybersecurity information amongst telecommunications industry participants.[119] Although Working Group 5 identified several mechanisms currently utilized by industry participants to share cyber threat information, several barriers to actually sharing that information exist.[120] Specifically, companies expressed a reticence to share attack information with regulators and each other for fear of liability, the imposition of future regulation, or subsequent disclosure by competitors.[121]

Precedent for enabling companies to confidentially report cyber-related incidents with liability protection exists. The Department of Homeland Security ("DHS") encourages private citizens and entities to voluntarily report significant cybersecurity events and to seek assistance in responding to those events.[122] Per Presidential Policy Directive PPD-41, to the extent allowed under federal law,

---

FINAL REPORT 4 (2015) [hereinafter COUNCIL IV, FINAL REPORT 4], https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[118] *Id.* at 29, 413.

[119] COMMC'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL V, FCC, WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING FINAL REPORT 3 (2017) [hereinafter COUNCIL V, FINAL REPORT 3], https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

[120] *Id*. at 13–19.

[121] *Id*.

[122] Directive on United States Cyber Incident Coordination, PPD-41, 2016 DAILY COMP. PRES. DOC. 494 (Jul. 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. In his Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, President Trump directed further study into the cyber risk management by private operators of critical infrastructure; and also directed an assessment of international cyber threat information sharing, but this order does not appear to alter existing guidance for the voluntary sharing of non-critical infrastructure cyber events as established by PPD-41. See Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 16, 2017), at sections 2(c) and 3(c) respectively.

the Department endeavors to keep such information confidential and not disclose it to others.[123] Working Group 5 thus recognized that DHS plays the lead role in coordinating the dissemination of cyber threat information and recommended that the FCC refrain from duplicating these efforts.[124]

Yet, the DHS cyber event reporting regime as currently executed does not fully address the barriers to information sharing identified by Working Group 5. The process implemented by the Presidential Directive is distinct from and does not contain many of the statutory protections found within the cyber event disclosure provisions of the Homeland Security Act of 2002. Section 214 of that Act provides a mechanism for voluntarily disclosing cyber event information to DHS, when such an event impacts "critical infrastructure and protected systems."[125] Disclosures made under this statutory provision prohibit disclosure under the Freedom of Information Act, prevent the use of that information in regulatory enforcement, and bar the information from use in any civil lawsuit.[126] Since only disclosures pertaining to critical infrastructure are covered under this statute, not every voluntary disclosure of cyber events receives the benefit of these statutory protections. MSS and cellular systems do not typically fall within the critical infrastructure definition. Hence, information voluntarily reported to the FCC or DHS about cyber incidents involving those systems often do not enjoy the protections of the Homeland Security Act, and must rely on the much more limited protections afforded under PPD-41.

The proposed Cybersecurity Responsibility Act of 2017, HR 1335, would elevate communications networks generally, including all types of satellite mobile communications networks, to "critical infrastructure and protected systems" as that term is defined in sections 2(4) and 212(6) of the Homeland Security Act of 2002.[127] Adoption of this measure resolves the reporting dilemmas raised by mobile communications companies and their suppliers. Since the

---

[123] PPD-41 at § III.

[124] *See* COUNCIL V, FINAL REPORT 3, *supra* note 119, at 4.

[125] Homeland Security Act of 2002, § 214, 6 U.S.C. § 133 (2012).

[126] *Id*.

[127] Cybersecurity Responsibility Act of 2017, H.R. 1335, 115th Cong. § 2(b) (citing 6 U.S.C. § 131 (2015)).

bill also includes provisions that would expand the FCC's regulatory authority, the bill is unlikely to pass.

B. *Cybersecurity Regulation of AASD in the Maritime Transportation Sector*

On the high seas, ships employing AASD must utilize over-the-horizon communications services such as MSS as their AASD communications backbone. Mobile satellite services for shipborne uses have the longest history of operational deployment of all MSS applications. These services thus also comprise the largest share of the total MSS market.[128] Most notable among maritime MSS service providers is the industry's first, Inmarsat.[129] Created in 1979 as a non-profit intergovernmental organization, Inmarsat's original mandate was to establish and operate a satellite communications network for ocean vessels.[130] Initially, the organization offered only satellite radio-telephony services for safety of life at sea, but the organization—since privatized—now offers many additional services ranging from media entertainment and broadband internet to ship security status and position tracking.[131] The growing demand for these maritime broadband products encouraged competitors to offer their own similar suite of satellite services.[132] Other mobile satellite applications widely available in the marine sector include: global satellite navigation, weather imagery, emergency locator beacons, logistics and cargo management, internet connectivity, and

---

[128] *See* BRYCE SPACE & TECH., SATELLITE INDUSTRY ASSOCIATION, 2017 STATE OF THE SATELLITE INDUSTRY REPORT (2017); *Mobile Satellite Services Market Size and Forecast*, HEXA RESEARCH, https://www.hexaresearch.com/research-report/mobile-satellite-services-market; Peter B. de Selding, *Comsys Survey Sees No Letup in Maritime Market Growth*, SPACE NEWS (Mar. 25, 2015), https://spacenews.com/comsys-survey-sees-no-letup-in-maritime-market-growth/; *Mobile Satellite Services Market worth $5.62 Billion by 2019*, MARKETSANDMARKETS, https://www.marketsandmarkets.com/PressReleases/mobile-satellite-services.asp (last visited Apr. 12, 2018).

[129] *About Us*, INMARSAT, https://www.inmarsat.com/about-us/ (last visited Sept. 9, 2018).

[130] *Id*.

[131] *Maritime*, INMARSAT, https://www.inmarsat.com/maritime/ (last visited Apr. 30, 2018).

[132] *See* de Selding, *supra* note 128.

satellite-based implementations of the Automatic Identification System ("AIS").

The AIS is an automatic tracking system used to broadcast ship position information to other ships and to vessel traffic management services. The AIS service thus plays a critical role in separating marine traffic and avoiding collisions. U.S. regulations implementing the International Maritime Organization Safety of Life at Sea ("SOLAS") requirements mandate AIS aboard all passenger ships carrying more than 150 passengers, commercial ships greater than 65 feet in length, certain commercial tugs and fishing vessels, and vessels carrying dangerous cargo.[133]

Near shore, the AIS utilizes VHF[134] line of sight radio transmissions received directly by the vessel traffic management ground stations as well as by the nearby ships.[135] On the open ocean, AIS line of sight VHF signals can no longer be received directly by shore stations, but newer technologies enable companies such as ORBCOMM,[136] exactEarth,[137] Spire,[138] and Spacequest[139] to offer satellite-AIS services. Pending SOLAS mandates for long range tracking, and their corresponding U.S. regulatory requirements

---

[133] 33 C.F.R. § 164.46.

[134] Very High Frequency ("VHF") is the designation for the range of radio frequency electromagnetic waves between 30 to 300 megahertz (MHz). Radio waves in the VHF band travel by line of sight. *See generally* JOHN S. SEYBOLD, INTRODUCTION TO RF PROPAGATION 9–10 (2005).

[135] *How AIS Works*, USCG NAVIGATION CENTER (Sept. 8, 2016), https://www.navcen.uscg.gov/?pageName=AISworks.

[136] *Networks: Satellite AIS*, ORBCOMM, https://www.orbcomm.com/en/networks/satellite-ais (last visited Apr. 12, 2018).

[137] *exactEarth Now Operating the Single Largest Satellite AIS Constellation*, EXACTEARTH (Oct. 10, 2017), http://www.exactearth.com/media-centre/recent-news/352-exactearth-now-operating-the-single-largest-satellite-ais-constellation.

[138] *Operate Intelligently More Data, More Often*, SPIRE, https://spire.com/data/maritime/ (last visited Sept. 6, 2018).

[139] *Global Satellite AIS Data*, SPACEQUEST, http://www.spacequest.com/s-ais (last visited Sept. 6, 2018).

ensure that these systems will become a universal safety and traffic separation tool and an integral component of maritime AASD.[140]

A modern ship therefore includes numerous earth stations connecting to multiple mobile satellite services. Some of these earth stations provide critical safety functionality such as emergency notifications and tracking. Others deliver satellite navigation and weather data as an alternative source of information for ship operations. Mobile satellite services also provide non-critical communications and entertainment capability. The maritime sector has integrated MSS into routine operations more than any other sector, and thus has a larger cyber threat footprint.

The United States Coast Guard has responsibility for protecting the nation's maritime interests, port security, and licensing of vessels and ships' personnel. The Coast Guard formally recognized the risks that cybersecurity challenges present to these missions in 2015 when it officially released its "Cyber Strategy" policy.[141] As articulated in the agency's 2017 budget, by implementing this strategy, the Coast Guard seeks to "coordinate cyber regulatory and technical assistance activities across Federal, state and local maritime industry stakeholders."[142] According to Lieutenant Commander H. Lars McCarter, director of the Coast Guard Cyber Operations Center, "[b]ecause the Coast Guard's missions include counterterrorism, anti-piracy, national security, and law enforcement against criminal organizations, it and its stakeholders potentially face greater danger of cyber-attack than other potential U.S. targets."[143] Commander Nick Wong, charged with implementing the industry portion of the cyber strategy, further

---

[140] *See* 33 C.F.R. pt. 169 (describing requirements for long range tracking of certain U.S. flagged vessels). Satellite AIS is one means of satisfying these requirements.

[141] J.R. Wilson, *Cybersecurity within the Coast Guard*, DEFENSEMEDIANETWORK (Feb. 27, 2017), https://www.defensemedianetwork.com/stories/cybersecurity-within-the-coast-guard.

[142] U.S. COAST GUARD, POSTURE STATEMENT, 2017 BUDGET IN BRIEF, 2015 PERFORMANCE HIGHLIGHTS, https://www.uscg.mil/Portals/0/documents/budget/2017_Budget_in_Brief.pdf.

[143] Wilson, *supra* note 141.

explains that the Coast Guard must address cyber threats originating from equipment failure and operator errors as well as from nefarious actors.[144] For these reasons, he prefers the term, "cyber risk management," to describe the Coast Guard's approach to maritime industry cyber threats.[145]

According to Commander Wong, one key goal in the risk management endeavor is clarifying what cyber threat activity the maritime industry must report.[146] Maritime operators already face mandatory reporting requirements for marine casualties and pollution and safety issues, and it is clear the Coast Guard wishes to interpret its rule-making authority to encompass reporting of cyber threats.[147] The Maritime Transportation Security Act of 2002 directed the Coast Guard and the maritime industry to develop security plans for the protection of critical maritime infrastructure.[148] Coast Guard regulations implementing this legislation now require mobile offshore drilling units, cargo vessels greater than 100 gross tons, tankers, and certain passenger vessels to keep records of and report security breaches and incidents to the Department of Homeland Security.[149]

In December of 2016, the Coast Guard issued policy guidance specifically placing certain cybersecurity events within the scope of security incidents that must be reported.[150] The policy guidance further directed that such incidents be reported to the Department of Homeland Security National Cybersecurity and Communications Integration Center, thereby awarding operators the liability and confidentiality protections previously identified above.[151] Paragraphs 3(A)(ii), (iii), and 3(B)(vi) of the policy guidance details

---

[144] *Id*.
[145] *Id*.
[146] *Id*.
[147] *Id*.
[148] 46 U.S.C. §§ 70101–70132 (2016).
[149] 33 C.F.R. §§ 104.235(b), 101.305 (2018).
[150] P. F. THOMAS, U.S. COAST GUARD, U.S. DEP'T OF HOMELAND SEC., CG-5P POLICY LETTER NO. 08-16, REPORTING SUSPICIOUS ACTIVITY AND BREACHES OF SECURITY (2016), http://www.maritimedelriv.com/storage/app/media/Agencies/USCG/USCG_Guidance/CG_5P_Policy_Letter_08_16_SAR.pdf.
[151] *Id*.

the metes and bounds of the cybersecurity events that do and do not merit reporting as follows:

> A. . . . .
>
> ii . . . .
>
> d) Intrusion into telecommunications equipment, computer, and networked systems linked to security plan functions (e.g., access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS;
>
> e) Instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers that are linked to security plan functions; and/or
>
> f) Any denial of service attacks that adversely affect or degrade access to critical services that are linked to security plan functions.
>
> iii. Note that routine spam, phishing attempts, and other nuisance events that do not breach a system's defenses are NOT BoS. Furthermore, breaches of telecommunications equipment, computer, and networked systems that clearly target business or administrative systems unrelated to safe and secure maritime operations are outside the U.S. Coast Guard's jurisdiction . . . .
>
> B. . . . .
>
> vi. The Coast Guard recognizes that the cyber domain includes countless malicious but low-level events that are normally addressed via standard anti-virus programs and similar protocols. Operators should only report events that are out of the ordinary in terms of sophistication, volume, or other factors which, from the operator's perspective, raise suspicions.[152]

Those same vessels subject to the aforementioned event reporting requirements are required by regulation to conduct Vessel Security Assessments[153] and develop Vessel Security Plans.[154] A Vessel Security Assessment (VSA) is "an analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations."[155] Rule 104.300

---

[152] *Id*. at 3–4.
[153] 33 C.F.R. §§ 104.300, .305 (2018).
[154] 33 C.F.R. §§ 104.400–.415.
[155] 33 C.F.R. § 101.105.

(d) (11) specifically states that preparation of the assessment should draw upon expertise in evaluating "[r]adio and telecommunications systems, including computer systems and networks . . . ."[156] The existing regulation thus implicitly directs evaluation of cybersecurity threats.

Additional security requirements specified by the rule contribute to the mitigation of cyber threats. Specifically, the regulations contain numerous provisions mandating personnel credentialing, security training, and physical access controls to sensitive locations.[157] In addition, vessel operators must appoint a Chief Security Officer, whose duties include completion of Vessel Security Assessments and Plans, as well as periodic audits.[158] One maritime industry security expert estimates that these security requirements will impact 10,300 U.S. Flag and SOLAS vessels and about 70 foreign flagged and non-SOLAS vessels at a total cost of $1.368B.[159]

The Coast Guard regulatory approach to cybersecurity focuses not on equipment specifications, technical performance, or earth station design. Rather, the holistic approach mirrors the risk management approach of the NIST framework. The reach of the regulations extends, however, only to the vessels and specific surface operations under the Coast Guard's jurisdiction, and hence only to those operations over which the vessel owner/operator has direct control. These regulations do not address potential risk vectors arising from the integrity of the space segment, or from third party suppression or corruption of valid message traffic.

C. *Cybersecurity Regulation of AASD in the Aviation Sector*

Similar to the maritime industry, all aviation regulation exists within an overarching framework of international treaties and understandings administered by an IGO, the International Civil Aviation Organization (ICAO). The FAA has primary responsibility

---

[156] 33 C.F.R. § 104.300(d)(11).

[157] 33 C.F.R. §§ 104.200, .225, .265.

[158] 33 C.F.R. §§ 104.210, .215, .415.

[159] JONATHON K. WALDRON & ANDREW W. DYER, JR., MARITIME SECURITY HANDBOOK: IMPLEMENTING THE NEW U.S. INITIATIVES AND REGULATIONS 50 (2005).

for promulgating regulations that implement U.S. aviation treaty obligations and ICAO agreements, and for exercising domestic oversight of aviation activities. In contrast to the maritime domain, which relies heavily on automation but has yet to experience significant use of autonomous craft, existing FAA regulations specifically address both manned and unmanned aircrafts.

1. *FAA Regulation of Manned Aircraft Systems and Operations*

Use of AASD in the aviation sector includes both discrete systems and connected AASD. Like their maritime counterparts, aircrafts flying over the high seas and in remote areas must use MSS. AMSS services include: satellite communications with air traffic control, private communications channels with airline operations, internet and cellular services for passengers, data uplink and downlink of passenger/customer service information and billing, inflight entertainment data, data links for navigation and weather information, and inflight uplink of aircraft telemetry to enhance aircraft reliability. In the wake of the mysterious loss of Malaysian Airlines Flight 370, aircraft on oceanic routes must include a means of continuously broadcasting their position via AMSS/ADS-B out by 2021.[160] Over the landmass of the United States, connected AASD can utilize cellular networks using repurposed bandwidth originally set aside for mobile aeronautical communications.

[160] U.N., Int'l Civil Aviation Org., States Make Further Progress through ICAO to Help Avoid Recurrence of MH370-Type Disappearances (Mar. 8, 2016), https://www.icao.int/Newsroom/Pages/States-Make-Further-Progress-through-ICAO-to-Help-Avoid-Recurrence-of-MH370-Type-Disappearances.aspx. For aircraft subject to U.S. airworthiness requirements or operating in U.S. Class A airspace, the requirements for automatic position reporting are to be implemented by 2020.

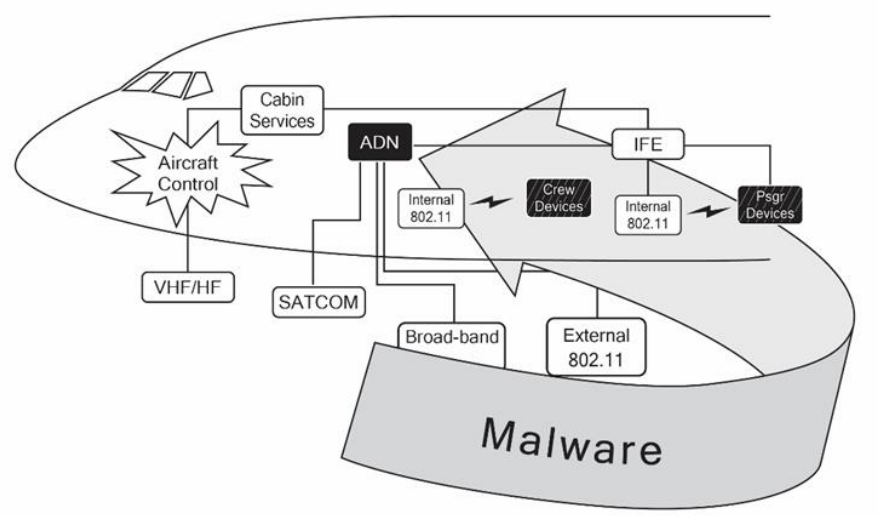

Figure 2: Aircraft Communications Networks and Services

Figure 3 diagrams typical data and telecommunications systems and networks aboard a modern large aircraft per the DOT Volpe Transportation Center.[161] The ADN, or Aircraft Data Network, denotes an industry consensus standard specification for aircraft data network design promulgated by the Airlines Electronics Engineering Committee, for example, ARINC 664. Although most aircrafts place flight critical and non-flight critical services on separate data networks, as Figure 3 shows, the DOT believes that significant cyber security issues remain because of the potential for interconnectivity of aircraft communications links.

The FAA regulatory approach differs fundamentally from that taken by its sister transportation agencies. FAA regulations may be broadly classed into the following types: those pertaining to operations, those pertaining to certification of personnel, those pertaining to airport facility design and security, and those

[161] See MICHAEL G. DINNING, DEP'T OF TRANSP., INTRODUCTION TO CYBERSECURITY ISSUES FOR TRANSPORTATION 19 (2011), https://www.ahcusa.org/uploads/2/1/9/8/21985670/s111207_dinning_overviewof_transportation_cyber_issues.pdf, for the image Figure 3 is based upon.

pertaining to the certification of aircraft and aircraft software and equipment. The FAA does not appear to have adopted the holistic cybersecurity approach articulated by the Coast Guard in the maritime domain. This statement does not mean the FAA is insensitive to cybersecurity issues or that its regulatory structure lacks similar elements. When compared to the maritime domain, however, the aviation industry evolved in a way that places a greater emphasis on the certification of the aircraft and component subsystems.

The FAA grants various certifications that enable personnel, equipment, and services to be introduced into the aviation ecosystem. More specifically, the FAA issues:

> (a) Licenses for pilots, flight attendants, mechanics, and dispatchers; as well as credentialing of certain key airport and other aviation personnel,[162]
>
> (b) Production certificates and parts manufacturing authority for airframe producers and spare and component parts manufacturers,[163]
>
> (c) Airworthiness certificates for aircraft,[164]
>
> (d) Operator certificates for airlines and certain other operations,[165]
>
> (e) Certification of airports and navigation equipment,[166] and
>
> (f) Supplemental Type Certificates and Technical Standard Orders which enable modification of an aircraft from its original configuration by adding or removing equipment.[167]

Several of the certification regulations specify precise requirements or technical rules for issuance and compliance. For example, twin engine aircraft certification rules require flight tests that demonstrate the aircraft can take off on one engine and clear an obstacle of a specified height.[168] In many cases, however, the FAA specifies certification requirements using industry consensus

---

[162] 14 C.F.R. pts. 60–68 (2018) (containing the licensing requirements for all Airmen).

[163] 14 C.F.R. pt. 21.

[164] 14 C.F.R. pts. 23, 25–27, 29, 31, 33, 35–36, 39.

[165] 14 C.F.R. pts. 110, 119, 125, 137.

[166] 14 C.F.R. pts. 150, 153, 157, 161, 170–71.

[167] 14 C.F.R. §§ 21.91–.101, .111–.120, .601–.621.

[168] 14 C.F.R. § 23.2120.

standards such as ARINC and RTCA.[169] In addition, industry consensus standards bodies such as the Society of Automotive Engineers (SAE), the International Airline Transport Association (IATA), and Aeronautical Radio, Inc. (ARINC) play a significant role in defining the design parameters and safety guidelines underpinning the certification process. Although the FAA incorporates and works cooperatively with consensus standards bodies, the agency retains via testing and review a measure of oversight to the acceptability and ultimate adoption of the resulting standards.

Fundamentally, an aircraft does not go into service, nor a part installed thereon, without technical review by the FAA via the certification process. Of particular importance are the FAA's software design guidelines as documented in Advisory Circular AC 20-115D.[170] This Advisory Circular cites an industry standard published by the RTCA as DO-178C, and recognizes that standard as an acceptable means, but not the only means, for establishing the airworthiness (certification requirements) of AASD software. The FAA classifies software according to the criticality of the function it performs.[171] Class A software includes flight control systems, the failure of which results in catastrophic harm including possible fatalities.[172] Class D and E software includes non-flight safety critical applications such as customer convenience internet connections that, if compromised, have little or no safety effect.[173] For each class of software, the Advisory Circular specifies a set of

---

[169] *See, e.g.*, YANN-HANG LEE, ET AL., FED. AVIATION ADMIN., U.S. DEPT. OF TRANSP., DOT/FAA/AR-05/52, SAFETY AND CERTIFICATION APPROACHES FOR ETHERNET-BASED AVIATION DATABUSES (2005), https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/05-52_Ethernet.pdf (noting several ARINC consensus standards).

[170] SUSAN J. M. CABLER, FED. AVIATION ADMIN., U.S. DEPT. OF TRANSP., AC NO: 20-115D, AIRBORNE SOFTWARE DEVELOPMENT ASSURANCE USING EUROCAE ED-12( ) AND RTCA DO-178( ) (2017), https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-115D.pdf.

[171] *Id.*

[172] *Id.*

[173] *Id.*

performance and fault tolerant objectives that must be met.[174] At higher levels of software classification the achievement of those objectives must be independently verified by persons other than those who coded the software.[175]

> Despite the robust oversight afforded by the certification and software design process, the interconnectivity of the aircraft AASD as shown in Figure 3 still leaves it vulnerable to cyber-threats. In 2014 the FAA responded by issuing policy guidance on the certification of aircraft and equipment. That guidance states that connectivity to "non-governmental" services not otherwise accredited for secure operations may trigger additional certification steps.[176] In particular, the FAA will issue special conditions for the certification of aircraft or systems that directly connect to external services and networks under the following conditions: (a) The external service is non-governmental; (b) The aircraft system receives information from the non-governmental service or network; and (c) The failure effect classification of the aircraft system is "major" or higher.[177]

AASD systems that only receive data from the aircraft and do not transmit data to the aircraft are exempt from these provisions.[178] The FAA explicitly states that this policy guidance does not constitute additional regulation. Yet the FAA fails to provide examples of special conditions or describe how the design of impacted AASD will be evaluated.

The policy guidance as understood thus addresses at least those AASD cyber-vulnerabilities arising from the receipt by the aircraft of a corrupted signal or inaccurate data carried by such a signal. It is less clear how well the guidance addresses the fault tolerance of component equipment aboard the aircraft, or how resistant this equipment should be to the introduction of malware.

Notably, the policy guidance leaves untouched existing FAA Rules and Orders pertaining to field loadable software, digital

---

[174] *Id*.

[175] *Id*.

[176] SUSAN J. M. CABLER, FED. AVIATION ADMIN., U.S. DEPT. OF TRANSP., PS-AIR-21.16-02, ESTABLISHMENT OF SPECIAL CONDITIONS FOR CYBER SECURITY (2014), https://www.icao.int/cybersecurity/SiteAssets/FAA/PS-AIR-21.16-02.pdf.

[177] *Id*.

[178] *Id*.

signatures and certificates for loadable software, FAA Order 8100.49 pertaining to design approval for software, and Spec 42 defining industry standards for digital information security.[179] These standards specify the fault tolerant and fail-safe design and operating characteristics of software embedded within equipment, according to the criticality of its function. Through these additional mechanisms, the FAA mitigates the risk of improper operation of aircraft equipment due to cyber malfeasance.

Despite the rigor of the certification process and the policy guidance, those processes do not mitigate or anticipate all threats. In November of 2016, the FAA received a report from the agency's Aviation Rulemaking Advisory Committee.[180] That report, which was not made public, is believed to have cited additional cybersecurity concerns and to have recommended the partitioning of onboard aircraft data networks into separate domains.[181] For example, noncritical networks such as in-flight entertainment, would be implemented on a separate data network from the AMSS data network used for communications with air traffic control. Modern designs currently utilize this best practice, but regulations do not mandate its use.

Threats from suppliers are not dealt with explicitly, other than possibly via apart through a production certificate. For example, software may be designed and certified in compliance with FAA guidance, but testing may not reveal malware embedded by suppliers and set to execute at a later date. The detection of such unauthorized code depends on the robustness of the testing protocols, and the manufacturer's voluntary supplier qualifications and oversight.

The FAA approaches the accreditation of aviation professionals in a manner similar to that used by the Coast Guard in the maritime domain. Personnel with the potential to impact aviation safety are

---

[179] *Id.* at 1.

[180] Woodrow Bellamy III, *Senators Reintroduce Aircraft Cyber Security Legislation*, AVIONICS (Mar. 24, 2017), http://www.aviationtoday.com/2017/03/24/senators-reintroduce-aircraft-cyber-security-legislation/.

[181] *Id.*

both vetted and acredited directly by the Agency or as part of the certification requirements of their employer.[182] In addition to the FAA regulations governing the certification of pilots, mechanics, dispatchers, flight attendants, and other key operations personnel, FAA airport design criteria also mandate physical controls to limit access to the airport and aircraft environment.[183] These accreditation regulations and controls provide the ancillary benefits of reducing cyber threats by restricting physical access to vulnerable aircraft systems and prescreening personnel working in the vicinity of AASD once installed.

2. *Unmanned Aircraft Systems and Operations*

In the FAA Modernization and Reform Act of 2012, Congress mandated that the FAA safely and expediently integrate unmanned aircraft systems (UAS) into the national airspace system.[184] In response, the FAA defined three classes of UAS:

> (a) unregulated hobbyist or recreational activities for aircraft weighing less than fifty-five (55) pounds,[185]
>
> (b) regulated commercial UAS operations for remote-piloted aircraft weighing less than fifty-five pounds,[186] and
>
> (c) Section 333 exemptions required for unmanned aircraft fifty-five pounds or greater, or for other deviations from any regulation governing UAS and their operations.[187]

Only one of these aforementioned classes of UAS is truly pertinent to cyber security concerns. Small, commercial UAS operations under Part 107 or hobbyist activities must be conducted with the aircraft in visual sight.[188] Thus, other than utilization of GPS

---

[182] *See* 14 C.F.R. pts. 60–68 (2018) (regarding Airmen); *see also* 14 C.F.R § 139.203 (citing certain personnel training, record keeping, and access controls required for airport certification).

[183] See 14 C.F.R. pt. 139, for airport certification requirements.

[184] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 (2012).

[185] 14 C.F.R. §§ 101.41, .43.

[186] 14 C.F.R pt. 107.

[187] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 333, 126 Stat. 11, 75–77.

[188] 14 C.F.R. § 107.31 (requiring the remote pilot in command or visual observer to have the unmanned aircraft in visual sight at all times unless a waiver

navigation services, such operations are unlikely to be consumers of AMSS or otherwise coupled to a communications network. Although their flight control systems are highly automated, the hazards resulting from compromise of these aircraft are likely benign. UAS operations conducted under Section 333 exemptions or under a certificate of operation, however, may extend beyond visual line of sight or be of such a size and scale that they do not constitute a connected AASD as shown in Figure 4.[189]

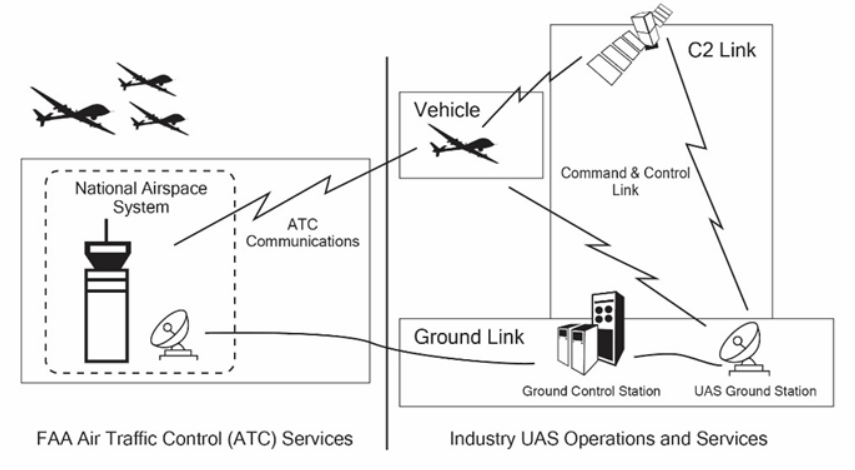

Figure 3: Components of Connected UAS

While many larger UAS are operated as government aircraft subject to special additional sensitivities and regulations beyond the scope of this paper, several, civil, applications of such large UAS presently exist. Private commercial UAS operations include: long-duration scientific monitoring, land and crop surveys, pipeline and

is obtained). In addition, current UAS rely on line of sight radio communications for aircraft control.

[189] See SUSAN J. M. CABLER, FED. AVIATION ADMIN., CYBERSECURITY & MITIGATIONS (2017), https://www.faa.gov/uas/resources/event_archive/2017_uas_symposium/media/Workshop_2_Cybersecurity.pdf, for the image Figure 4 is based upon.

powerline monitoring, and airborne communications relays.[190] Future use of such systems will continue to expand to potentially include the delivery of medicines and other goods, or the transport of people.[191] Therefore, the cybersecurity of their equipment and operations presents a legitimate concern.

Like manned aircraft systems, both the unmanned aircrafts and its operations must each comply with applicable regulations. For large UAS, three pathways to aircraft certification exist. An unmanned aircraft may receive type certification and a standard airworthiness certificate just like any manned aircraft.[192] The unmanned aircraft can opt to receive a special airworthiness certificate in the experimental category under 14 CFR § 21.191, if the anticipated use involves research and development, crew training, or market surveys.[193]

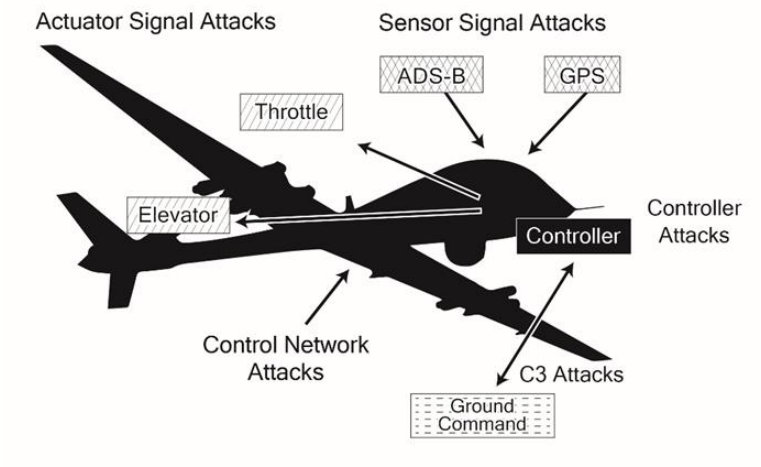

Figure 4: UAS Cyber-Vulnerability Overview

---

[190] *A Civil Future for Unmanned Aircraft Systems*, NASA (Aug. 3, 2017), https://www.nasa.gov/aeroresearch/programs/iasp/uas/civil-future-for-uas.

[191] *See, e.g.*, KITTY HAWK, https://kittyhawk.aero/ (last visited Sept. 4, 2018) (proposing a semi-autonomous personal aircraft and an air taxi).

[192] 14 C.F.R §§ 21.17(b), .25.

[193] FED. AVIATION ADMIN., PUBLIC GUIDANCE FOR PETITIONS FOR EXEMPTION FILED UNDER SECTION 333 at 1 (2014) [hereinafter SECTION 333], https://www.faa.gov/uas/beyond_the_basics/section_333/how_to_file_a_petition/media/section333_public_guidance.pdf.

The certification of both the aircraft and its onboard systems is therefore similar to that described above for manned aircraft, including the applicability of special conditions as mandated by PS-AIR-21.16-02. However, the FAA acknowledges that the risk calculus embedded within the regulations and policy guidance for manned aircrafts may not scale appropriately for unmanned aircrafts.[194] Figure 5 illustrates the vulnerabilities of large UAS to cyber-attacks and security deficiencies.

As shown in Figures 4 and 5, several potential risks exist when the UAS relies on command signals or operation and critical data received or provided via AMSS.[195] As in the maritime and manned aeronautical systems domains, these risks include jamming or interference with the signal, corruption of the data embedded within the signal, and corruption of the onboard systems which process such signals. Each of these vulnerabilities could adversely impact the aircraft's ability to aviate, navigate, or communicate. In a manned aircraft, however, a human pilot can directly observe and intervene in aircraft operations with less data latency than a remote pilot can. A human pilot may also possess a greater number of options for directly controlling the aircraft, overriding autonomous systems, or supplanting signal data with their own observations. Conversely, in certain UAS operations, such as those occurring at low level in remote or unpopulated areas, the consequences of such vulnerabilities may not pose a hazard to life or property at all. For these reasons, the FAA appears to implicitly acknowledge that the risk exposure for UAS differ from manned aircraft and that cyber risk policies appropriate for manned aircraft might not be appropriate for UAS.[196] Therefore, although aircraft and equipment certification processes remain a valid mechanism for addressing cyber-security issues within a UAS, management of cybersecurity risks must place additional emphasis on mitigation practices during flight operations.

---

[194] CABLER, *supra* note 189.
[195] *Id.*
[196] *Id.*

Civil operators of unmanned aircraft, not otherwise covered by the small UAS operating rules of Part 107, must petition for a Certificate of Waiver or Authorization[197] or obtain a certificate of operation to legally conduct operations.[198] The requirements for obtaining a certificate of operation are the same as those previously discussed in connection with the regulations governing certification of manned aircraft operations.[199] Certification of Waiver and Authorization constitutes ad-hoc applications for relief from certain FAA regulations or airworthiness certification requirements.[200] Thus, the precise content of these applications varies between applicants and the operations they envision. A review of a sample Section 333 Certificate of Authorization (COA) application reveals that the applicant must describe the actions to be taken in the event that communications links are lost either with the aircraft or between the remote pilot, air traffic control, or members of the flight crew.[201] The information requested by the sample application therefore addresses the risks due to the jamming or complete loss of a communications signal, but does not address the corruption of data transmitted by such signal. Nor does the suggested application specifically address the possibility that malware aboard the aircraft might corrupt the processing of the received data, or cause the transmission of the erroneous data. Unlike in the maritime domain, there does not appear to be a formal discussion, requirement, or emphasis on securing access to key aircraft systems once those systems are approved as part of the aircraft certification.[202]

---

[197] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 333, 126 Stat. 11, 75–77 (2012).

[198] 14 C.F.R. pts. 91, 135, 121. The author notes that some UAS proposals include the transport of persons.

[199] *Id*.

[200] SECTION 333, *supra* note 193, at 4.

[201] *Sample: FAA UAS Civil COA Request Form*, FED. AVIATION ADMIN., https://www.faa.gov/uas/beyond_the_basics/section_333/how_to_file_a_petition/media/FAA_UAS_Civil_COA_Request_v2.pdf (last visited Aug. 17, 2018).

[202] The omission of this type of information from the sample application does not preclude the FAA from requesting it if the agency deems it necessary to fully evaluate the safety of the proposed operation.

3. *Proposed Legislation and Additional Rules*

In May 2017, Senators Edward Markey and Richard Blumenthal introduced legislation titled Cybersecurity Standards for Aircraft to Improve Resilience Act of 2017 (aka. Cyber AIR Act). The Bill requires that air carriers, aircraft manufacturers, and aircraft equipment manufacturers disclose to the FAA any "attempted or successful cyberattack" against any aircraft or ground support system.[203] Notably, the Bill does not address the potential liability of such a disclosure, nor does the Bill mandate disclosure via the Department of Homeland Security's existing process. As previously noted, the sharing of cyber-threat information among ecosystem participants can be beneficial in defending the larger system against attack. Industry participants, however, remain concerned that such information could subject them to liability, regulatory sanction, or the manipulations of an untrustworthy competitor.[204] The Bill as drafted is unlikely to illicit the support and cooperation of the aviation community for these reasons.

The Bill additionally requires that all electronic entry points to the aircraft or ground systems be hardened against cyber-attack and that such measures be periodically evaluated for effectiveness, and changes be made to such measures if warranted by the evaluation results.[205] Such a broad regulation may be too divorced from tailoring the measure to the risk presented. For example, an unmanned aircraft operating over the ocean waters of the United States, may present no risk of harm even if compromised by a cyber incident.

Finally, the Bill requires the FAA to work with the FCC, The Department of Homeland Security, and The National Intelligence Community to incorporate cybersecurity requirements into requirements for an air carrier operating certificate or an aircraft production certificate.[206] As discussed above, existing FAA rules

---

[203] Cybersecurity Standards for Aircraft to Improve Resilience Act of 2017, S. 679, 115th Cong. § 3(a) (2017).

[204] *See, e.g.*, COUNCIL V, FINAL REPORT 3, *supra* note 119; Eamon Javers, *Cyberattacks: Why Companies Keep Quiet*, CNBC (Feb. 25, 2013, 1:45 PM), https://www.cnbc.com/id/100491610.

[205] S. 679 § 4(b).

[206] S. 679 § 4(b)(2).

focus predominately on certification of the aircraft and aircraft subsystems, and on the aviation operations themselves. Certain FAA rules, such as PS-AIR 21.16-02, do not rise to the level of formal regulation. None of the FAA cybersecurity rules discussed pertain to the operating certificate of the airline or the aircraft manufacturer. Including such entities within the scope of the cyber regulatory scheme would enable a more comprehensive approach along the lines of that advocated by the Coast Guard in the maritime domain. Such an approach would expand the focus of cybersecurity beyond the physical realm of the aircraft and its systems to include risks present in production and in the physical operating environment of the aircraft. At present, the Bill has been introduced with no action taken.[207]

D. *Cybersecurity Regulation of AASD in the Automobile Industry*

The regulation of cybersecurity for surface transportation belongs to various constituent agencies within the U.S. Department of Transportation.[208] The Federal Motor Carrier Safety Association makes rules related to commercial vehicle operations "largely focused on addressing human driver training, issues of human driver fatigue, hours of service, rest and meal stops."[209] As such, this

---

[207] The Cyber AIR Act has been introduced in the Senate as S.679 and in the House as H.R. 2997. The Senate bill has been referred to Committee. *S.679 - Cyber AIR Act*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/679?q=%7B%22search%22%3A%5B%22S.679%22%5D%7D&r=1 (last visited Feb. 20, 2018). The House has issued a Committee Report and the matter has been calendared. *See H.R.2997 - 21st Century AIRR Act*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/house-bill/2997/all-actions?q=%7B%22search%22%3A%5B%22H.R.+2997%22%5D%7D&r=1 (last visited Feb. 20, 2018).

[208] *See* 49 U.S.C. ch. 1 (2018) (establishing the DOT and its constituent agencies); U.S. DEP'T OF TRANSP., COMPREHENSIVE MANAGEMENT PLAN FOR AUTOMATED VEHICLE INITIATIVES 3 (2018), https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/317351/usdot-comprehensive-management-plan-automated-vehicle-initiatives.pdf.

[209] Eric Miller, *Chao Tells Automated Vehicle Summit DOT "3.0" Guidance Could be Issued in Early Summer*, TRANSP. TOPICS (Mar. 1, 2018, 7:15 PM), https://www.ttnews.com/articles/chao-tells-automated-vehicle-summit-dot-30-

agency manages vehicle safety primarily through workplace rules and human factors. One can therefore reasonably believe its influence on the cybersecurity of vehicular transportation is negligible at this time. The Federal Railroad Administration is tasked with enforcing the nation's railroad safety laws via rail safety regulations.[210] This agency only recently began surveying the industry to better understand the future of AASD within the rail system.[211] The Federal Highway Administration conducts research and promulgates regulations pertaining to highway design, traffic control devices, and highway-related aspects of pedestrian safety.[212] Although this agency concerns itself with the cybersecurity of the roadway infrastructure, the agency largely works in cooperation with its sister agency the National Highway Traffic Safety Administration (NHTSA) in such efforts.[213] The National Highway Traffic Safety Administration is the agency with responsibility for all motor vehicle safety regardless of the degree of automation.[214]

Congress recognized the potential to create a jumble of uncoordinated cybersecurity regulatory efforts within the surface transportation sector. In March 2018, Congress passed legislation directing the Department of Transportation to develop a comprehensive plan to better manage initiatives pertaining to

---

guidance-could-be-issued-early-summer (quoting Steven Bradbury, DOT general counsel); *see* 49 U.S.C. § 113 (2000).

[210] 49 U.S.C. § 103 (2011).

[211] Automation in the Railroad Industry, 83 Fed. Reg. 12,646 (proposed Mar. 22, 2018). FRA spokesperson Warren Flatau told *Railway Age* that "Secretary Chao is placing considerable emphasis on autonomous vehicle development, and prospective use of automation technologies across all modes of transportation" and that "[t]his solicitation is part of U.S. DOT efforts to advance the safe deployment of such technologies." William C. Vantuono, *FRA RFI: "Automation in the Railroad Industry,"* RAILWAY AGE (Apr. 2, 2018), https://www.railwayage.com/regulatory/fra-rfi-automation-railroad-industry/.

[212] 49 U.S.C. § 104(c)(1) (2000).

[213] INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFFICE, *How the U.S. Department of Transportation is Protecting the Connected Transportation System from Cyber Threats*, U.S. DEP'T TRANSP., https://www.its.dot.gov/factsheets/cybersecurity.htm (last visited Sept. 9, 2018).

[214] 49 U.S.C. § 105 (1994).

AASD.[215] In response, the Department of Transportation published its *Comprehensive Management Plan for Automated Vehicle Initiatives*, and promised to issue in the later months of 2018 an additional document titled: *Preparing for the Future of Transportation: Automated Vehicles 3.0*.[216] When developing this latest document, the Department plans to build upon the policy and regulatory approaches currently articulated in NHTSA *Automated Driving Systems 2.0: A Vision for Safety* .[217] Because of the degree of economic activity surrounding autonomous cars, and the influence the NHTSA exerts on current and future DOT cybersecurity policy, this section focuses its analysis on the NHTSA AASD regulatory scheme.

In its oversight of motor vehicle safety, the NHTSA employs a combination of two regulatory tools: Federal Motor Vehicle Safety Standards (FMVSS) and recall of unsafe vehicles.[218] In practice, automobile manufacturers self-certify that they comply with the FMVSS before placing an automobile into public use.[219] The NHTSA then randomly tests deployed vehicles to verify compliance with the FMVSS.[220] If tests reveal that a manufacturer's vehicle is noncompliant or presents a safety hazard, then the agency exercises its authority to recall the vehicle.[221] In actuality, the agency initiates

---

[215] The Consolidated Appropriations Act, Pub. L. No. 115-141 (2018), provided $100 million "to remain available until expended, for a highly automated vehicle research and development program to fund planning, direct research, and demonstration grants for highly autonomous vehicle (HAV) technologies and advanced driver-assistance systems (ADAS). . . . Of the total amount provided, up to $500,000 shall be available to the Secretary to develop a comprehensive plan to better manage departmental initiatives related to automated vehicles . . . ." 164 CONG. REC. H2875 (2018) (statement of Rep. Frelinghuysen).

[216] U.S. DEP'T OF TRANSP., *supra* note 208, at 9.

[217] *Id.*

[218] WATNEY & DRAFFIN, *supra* note 5, at 10.

[219] *Id*.

[220] *Id*.

[221] *Id*.

few recall cases.[222] The manufacturers self-initiate most recalls before the agency needs to exercise its recall authority.[223]

To date, the agency has not issued any FMVSS regarding cybersecurity.[224] In 2017, the NHTSA published industry guidance concerning the regulation of autonomous vehicles and vehicles containing automated systems.[225] That guidance specifically eschews promulgation of formal regulations in favor of voluntary compliance with 12 priority safety design elements.[226]

Safety design element 7 addresses cybersecurity matters.[227] In its guidance to industry, the agency "encourages," but does not mandate, certain practices.[228] Specifically, NHTSA encourages entities to design automation using "established best practices for cyber vehicle physical systems," including those established by NIST, the Society of Automotive Engineers (SAE), the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center, and other relevant agencies.[229] The agency further encourages entities to document their compliance with such standards as well as their design choices in mitigating cyber risks.[230] But notably, unlike the Coast Guard's approach, the agency does not *require* such actions—even for systems that might impact safety of life. The agency only advocates for submission of a *voluntary* safety self-assessment.[231] Thus, the regulated entity has complete discretion over whether to engage in any of these recommended behaviors—or not.

Also noteworthy is the distinction between the FAA's regulatory approach to aircraft and aviation systems and that taken by The Department of Transportation its sister agency, NHTSA, with

---

[222] *Id*.
[223] *Id*.
[224] *Id*.
[225] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 10.
[226] *Id*. at 1.
[227] *Id*. at 11.
[228] *Id*. at 1, 11.
[229] *Id*. at 11.
[230] *Id*.
[231] *Id*. at 16.

respect to surface vehicles. Although the FAA exercises its oversight via mandatory regulation, policy guidance, and advisory circulars; every aircraft, manned or unmanned, must either come within a Rule exemption or meet certification standards and obtain an airworthiness certificate *prior* to entering service.[232] Individual systems and pieces of equipment must also meet certification standards either via a Technical Standards Order, or Supplemental Type Certificate before being installed on an aircraft.[233] The NHTSA would, presumably, not permit a patently unsafe automated vehicle from entering into service, but its exclusive reliance on its recall authority is remarkable.

In the past, use of the recall authority coexisted with an enforceable FMVSS. In the realm of cybersecurity, however, none exist. The agency's justification for its approach is therefore also noteworthy. The NHTSA states that the purpose of the voluntary guidance is: "to support the automotive industry, the States, and other key stakeholders . . . ."[234] Although safety is acknowledged in passing as an agency responsibility, the Department of Transportation's voluntary guidance does not explicitly reference the agency's congressional mandate to provide "fast, *safe*, efficient, and convenient transportation."[235] The agency's other stated objective *vis a vis* the public is to support public trust and confidence in the safety of AASD by encouraging, but not requiring, the regulated entities to disclose voluntary self-assessments and their methodologies for achieving safety.[236]

The stated justification for this somewhat laissez faire approach is to promote the introduction of potentially life-saving automation while not impeding the innovation necessary to achieve it.[237] Commenters have noted other possible benefits to this approach.

---

[232] 14 C.F.R. ch. I (2018).

[233] 14 C.F.R. pt. 21.

[234] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 10, at 1.

[235] *Id*. at 18, 25 (mentioning "safety" as something existing within the purview of the agency as opposed to the states). See 49 U.S.C. § 101(a) (2012) (emphasis added), for the statutory text.

[236] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 10, at 25.

[237] *Id*. at i–ii.

Specifically, this approach allows for diverse responses to cybersecurity threats and prevents the emergence of a cyber monoculture where vulnerabilities are uniform across the system.[238]

Despite these potential advantages, the agency's sole reliance on voluntary compliance with consensus standards also has numerous drawbacks. Voluntary industry standards, although advanced by those with specialized technical expertise, leave no voice for the consumer or the public in their formation. Additionally, in certain technical fields, such as telecommunications, consensus standards bodies have sometimes earned a reputation for being unwieldy political entities capable of being captured and controlled by a savvy player or one with a dominant intellectual property position[239] Thus, the technical solutions adopted by such groups may or may not be the optimal approach to the problem addressed. Furthermore, merely encouraging compliance with a standard is a far cry from requiring that a device actually attains the performance achievable via that standard.

No doubt in other sectors, such as aerospace, policy standards bodies have successfully worked to advance common understandings of technically appropriate solutions to shared problems. The FAA has routinely turned to ARINC, the RTCA, the SAE, and other standards bodies for solutions to stated problems.[240] But, the FAA employs consensus standards in an entirely different manner than NHSTA. The FAA utilizes consensus standards as an acceptable means to demonstrate conformance with an existing safety rule.[241] This approach also enables the public to comment on

---

[238] *See* WATNEY & DRAFFIN, *supra* note 5, at 12.

[239] With over 15 years' experience representing various entities in the formation of consensus standards, and the licensing of technology necessary for adoption of such standards, I stand by this assessment.

[240] See *supra* notes 168–69 and accompanying text, describing the use of RTCA standards in the certification of aircraft software and Ethernet based aircraft systems.

[241] *See, e.g.*, Accepted Means of Compliance; Airworthiness Standards: Normal Category Airplanes, 83 Fed. Reg. 21,850 (proposed May 11, 2018) (requesting comments on the use of 30 published consensus standards as a means for demonstrating compliance with the aircraft certification requirements of 14 C.F.R. pt. 23). The FAA Administrator found after review that these consensus

the suitability of the standard since it forms a part of the agency's rule making activities.[242]

In the realm of motor vehicles, however, the NHTSA merely encourages voluntary compliance with consensus standards in a manner decoupled from any FMVSS, the agency's rulemaking process, or agency verification of compliance.[243]

Presumably, the consensus standards cited by the NHTSA could also serve as a basis for establishing negligent design in product liability cases. A failure to adhere to an acceptable consensus standard may be grounds for establishing a negligent design unless the automaker could document a rationale for the deviation. It is noteworthy, however, that the NHTSA guidance strongly discourages states from implementing their own regulations.[244] The NHTSA document states: "NHTSA strongly encourages States not

---

standards, promulgated by the American Society for Testing and Materials (ASTM), were "an acceptable means, but not the only means" of demonstrating compliance with 14 C.F.R. pt. 23. Fed. Aviation Admin., *FAA Publishes Means to Comply with Part 23*, U.S. DEP'T TRANSP. (June 11, 2018), https://www.faa.gov/news/updates/?newsId=90566.

[242] Accepted Means, *supra* note 241.

[243] *See generally* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, Circular A-119, FEDERAL PARTICIPATION IN THE DEVELOPMENT AND USE OF VOLUNTARY CONSENSUS STANDARDS AND IN CONFORMITY ASSESSMENT (2016), ACTIVITIES, https://obamawhitehouse. archives.gov/omb/circulars_a119 (containing guidance to federal agencies on selecting and using voluntary consensus standards in lieu of government unique standards and assessing private sector conformance with voluntary standards). Section 4(a) defines a "voluntary consensus standard" as one created using a development process having certain defined attributes. A "voluntary consensus standard" is therefore to be distinguished from "voluntary compliance with a standard." The former term describes the process by which the standard was created while the latter term defines whether adherence to the standard bears any relation to regulatory compliance. Although OMB Circular A-119 clearly articulates a government policy favoring agency adoption of consensus standards in regulatory oversight functions, the NHTSA use of standards differs significantly from that employed by the FAA. The FAA uses voluntary consensus standards as an optional means of demonstrating compliance with a Rule and in a manner clearly consistent with the framework of OMB Circular A-119. The NHTSA merely encourages voluntary adoption of voluntary consensus standards.

[244] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 10, at 3, 18, 20, 21.

to codify this Voluntary Guidance (that is, incorporate it into State statutes) as a legal requirement for any phases of development, testing or deployment of ADSs [Automated Driving Systems]."[245] While acknowledging elsewhere that the regulation of liability remains with the States, strict adherence to this admonition would prevent states from formally incorporating the voluntary guidelines and standards into any formal definition of defective design. Such a prohibition would effectively gut the ability for product liability law to serve as an incentive for the desired cyber-secure behaviors.

The totality of the NHTSA approach, especially when contrasted with the regulatory approaches taken by other agencies, suggests a regulatory body captured by the industry it is intended to regulate. For perhaps this reason, or in response to the specific drawbacks noted above, current legislation pending in Congress would make the now voluntary self-assessment of compliance with these standards compulsory while prohibiting the States from levying additional design standards.[246] In addition, each proposed bill requires mandatory cybersecurity plans from automobile manufacturers documenting their process for identifying and mitigating vulnerabilities to cyber-attack.[247] The regulatory scheme advanced by the proposed legislation tracks the regulatory scheme implemented by the Coast Guard in the maritime domain, and appears to be a reasonable compromise to compel and ensure automakers actually work through cybersecurity issues in a

---

[245] *Id*. at 18.

[246] *See* AV Start Act, S. 1885, 115th Cong. (2017); H.R. 3388, 115th Cong. (2017) (requiring that manufacturers of highly automated vehicles develop written cybersecurity and privacy plans for such vehicles prior to offering them for sale, and also mandating that the Department of Transportation require safety assessment certifications for the development of a highly automated vehicle or an automated driving system). The proposed legislation also amends 49 U.S.C. § 30103 (b) to preempt any State laws or regulations regarding the design or construction of automated vehicles.

[247] *Id*. The proposed legislation is an attempt to amend Chapter 301, subtitle VI of 49 U.S.C. by inserting a new section, § 30130 Cybersecurity of automated driving systems. See H.R.3388, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/3388/summary/00, for the language as specifically proposed.

comprehensive way. In addition, this approach would ensure that cyber failures potentially impacting safety of life are presented in a manner over which the agency can exert its oversight authority prior to the occurrence of an accident.

The voluntary guidelines advanced by NHTSA also address disclosure of cyber incidents. Entities are encouraged to report to the Automotive Information and Analysis Center, or other relevant organizations, all discovered incidents, threats, exploits, and vulnerabilities from internal testing, consumer reporting, or external research.[248] This private industry group, formed in 2015, established a global information sharing community to track vehicle cyber-security risks.[249] According to the group's web-pages, membership encompasses over 99 percent of light-duty vehicles in North America, with over 30 global original equipment manufacturers and suppliers.[250] Information submitted to this industry collaborative is anonymized and shared with other members, a key component of the collaborative architecture being the confidentiality of the disclosing member.[251] No government agency or law enforcement organization has access to the submitted data without the approval of the disclosing party, although the agency claims that it will work cooperatively with the government on a need-to-know basis and with the approval of the industry member.[252] Presumably, the information could be subpoenaed. Such a process is not only costly and time consuming, but also implies that some aggrieved party has already suffered a harm for which redress is sought.

The Department of Transportation therefore recognizes the benefits that collaborative learning brings to the reduction of cyber vulnerabilities, but has introduced a significant barrier to its own edification of ongoing trends and developments. The data remains entirely within the complete control of a private industry group with no obligation to share its findings, observations or research with the government. Unlike the system for critical infrastructure in use at

---

[248] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 10, at 11.

[249] *Frequently Asked Questions*, AUTO-ISAC, https://www.automotiveisac.com/faqs/ (last visited Apr. 29, 2018).

[250] *Id*.

[251] *Id*.

[252] *Id*.

DHS, the government possesses no mechanism that provides visibility into emergent cyber-security issues or the effectiveness of the aggregate industry response. Yet again, such disclosures are only voluntary and not mandatory. As a result, the safety decision making function has been completely ceded to the industry participants. Unlike aviation, the driving public is left without any meaningful independent arbiter of or enforcer of the necessary safety behaviors. The significance of this position cannot be understated. Unlike previous iterations of automotive automation, cyber compromise of current AASD doesn't just create consumer inconvenience, it impacts safety of life.

E. *Remote Sensing: NOAA Licensing and Operating Rules*

The remote satellite sensing systems licensed by NOAA are indirectly relevant to the regulation of AASD in the transportation sector. AASD may consume processed data and services provided by remote sensing technology but they currently do not directly communicate with or process the raw data output from such systems.[253] Contemporary remote sensing systems downlink the observed data back to a fixed base ground station for further data processing and subsequent distribution to the end user or AASD.[254] An examination of the cybersecurity regulations pertaining to remote sensing systems is meritorious primarily as an investigation into an alternative cybersecurity regulatory scheme, although corruption of the remote observation data provided to the AASD is also of concern.

Operators of commercial space-based remote sensing satellite systems must obtain a license from the U.S. National Oceanic and Atmospheric Administration pursuant to the National and Commercial Space Programs Act.[255] Review of the specific license

---

[253] *The Use of Satellite Remote Sensing to Study the Human Dimensions of Global Environmental Change*, CIESIN, http://www.ciesin.org/TG/RS/RS-home.html (last visited Sept. 6, 2018); *The Technology of Satellite Remote Sensing*, CIESIN, http://www.ciesin.org/TG/RS/sattech.html (last visited Sept. 6, 2018).

[254] *See supra* note 253.

[255] 51 U.S.C. §§ 60101–26 (2012).

requirements documented in the corresponding regulations finds cybersecurity addressed via two separate provisions.[256] The first, most directly applicable provision, mandates that all licensees submit a "Data Protection Plan," describing the licensee's plan to protect data and information through the entire cycle of tasking, operations, processing, archiving and dissemination.[257] "At a minimum, this includes appropriate protection of communications links and/or delivery methods for tasking of the satellite, downloading of data to a ground station . . . , and delivery of data from the satellite to the licensee's central data storage facilities."[258] In 2008, NOAA published informal guidance in the form of a "Licensee Data Protection Plan Template," that outlines in greater detail the types of information licensees should include in their plans.[259] Table 1 documents the key elements to be included.

Spacecraft	**Communications Links to/from Spacecraft**	**Ground Segment**	**Entire System**
Orbits	No. of Channels	Physical site and physical access controls to site	Description of system architecture
Equipment performance capabilities	Frequency of and data conveyed via each channel	Personnel security	Overview of data protection strategy

[256] *See* 15 C.F.R. pt. 960.

[257] *Id.* § 960.11(b)(13).

[258] *Id.* § 960.3.

[259] COMMERCIAL REMOTE SENSING REGULATORY AFFAIRS, NAT'L OCEANIC & ATMOSPHERIC ADMIN., NOAA LICENSEE DATA PROTECTION TEMPLATE (2002), https://www.nesdis.noaa.gov/CRSRA/files/DPP%20Template.pdf.

Pointing capability	Encryption used on each channel	Data storage and protection practices	Methods for complying with U.S. Government requests for and allowable uses of data.
	Encryption key management plan	Data transmittal process to end users	
	Description of how data is processed from raw to enhanced state	Security and encryption to end users	

Table 1: NOAA Data Protection Plan Template

Examination of the plan elements reveals that the anticipated protection schemes address protections to ensure the proper acquisition and dissemination of the data. Specific elements of the plan pertaining to the performance and pointing characteristics of spacecraft sensors address masking sensitive troop movements, and complying with statutory obligations concerning sensing of Israel.[260] Elements of the plan requiring encryption of data and control signals not only protect against unauthorized collection of data, but also seek to prevent against access to the data by unauthorized persons.

[260] *See* 15 C.F.R. pt. 960, app. 1, § IV(4) (2018); Nat'l Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104-201, § 1064(a), 110 Stat. 2422, 2653 ("A department or agency of the United States may issue a license for the collection or dissemination by a non-Federal entity of satellite imagery with respect to Israel only if such imagery is no more detailed or precise than satellite imagery of Israel that is available from commercial sources."). The Department of Commerce makes the determination as to the allowable level of precision. As part of the licensing process, NOAA requires the applicant's data plan to identify how the proposed system will restrict the collection and dissemination of imagery of Israel at the required resolution. *See About the Licensing of Private Remote Sensing Space Systems*, NOAA CRSRA LICENSING, https://www.nesdis.noaa.gov /CRSRA/licenseHome.html (last modified Jul. 27, 2018, 9:00:22 EDT).

Absent from the plan, therefore, are any of the comprehensive, NIST-like, analyses that identify and mitigate cyber-security risks unrelated to data collection and use. For example, the plan template and regulations neither suggest nor require controls of the suppliers and services providers or any risk analysis of same. The plan template neither suggests nor requires positive mitigation of risks that the spacecraft could be damaged or lost due to the corruption of onboard equipment. The plan template does not address the possibility that an encrypted and correctly formatted control signal might be received by the spacecraft that commands it to operate in an undesired or even self-destructive way. The encryption of transmitted packets, site access, and personnel security as required by the plan do mitigate this risk, but these steps fail to account for additional sources of risk. Specifically, the acquisition of ground antennae and ground station operations by secondary suppliers removes the owner/operators of the satellite from direct oversight of certain operational aspects. The remote data service provider does not appear to be required to mandate either by contract or other means the protection of encryption keys or the appropriate access to data as applicable. Review of some publicly searchable plans indicates plan details do not reach this depth of holistic risk assessment and mitigation.

Despite these apparent gaps in the data plan template, the second of the two NOAA licensing regulations may indirectly address those security items left unspecified by the template itself.[261] Rule 960.11 requires that operators of remote sensing satellites maintain operational control of the satellite from the United States at all times.[262] Operational control is defined to mean "the ability to operate the system or override commands issued by any operations center or station."[263] Wherein "[o]perate means to manage, run, authorize, control, or otherwise affect the functioning of a remote sensing space system, directly or through an affiliate or subsidiary. This includes: (1) Commanding, controlling, tasking, and

[261] *See* 15. C.F.R. § 960.11 (2006).
[262] *Id*.
[263] 15 C.F.R. § 960.3 (2006).

navigation of the system; or (2) Data acquisition, storage, processing, and dissemination."[264] Additional licensing instructions direct the applicant to describe those methods used to ensure the integrity of operations including positive control of the space system, operations centers, and ground stations.[265] There appears little more needed to establish this capability beyond the type of information required by the data protection plan. This Rule, however, may serve as an additional authority to strengthen license requirements in response to the changing cybersecurity threat environment.

Additional NOAA regulatory provisions bear upon cybersecurity, although not directly. Licenses for commercial remote systems are also subject to review by the Department of State, the Department of Defense, the Department of the Interior, and the Intelligence Community.[266] These additional agencies may review the licensing package for compliance with "international obligations, foreign policy concerns, or national security concerns."[267] Such reviews might flag additional cyber-security issues; however, the scope of such reviews and their particulars remain ambiguous.

V. CONCLUSIONS AND RECOMMENDATIONS

Private law incentives to compel cyber-secure behaviors in the transportation sector exist but are insufficient to achieve vigilance. Unequal bargaining power and broad disclaimers of warranties and liabilities limit meaningful negotiation over the allocation of cyber-security risks via contact. Insurance, which could serve as a mechanism to incentivize cybersecurity through oversight of risk mitigation practices, typically excludes cyber-related incidents from coverage. Hence, insurers do not exert much influence in promoting cyber-secure design and best practices.

Product liability law remains a promising avenue for incentivizing the manufacturers of AASD to engage in design and

---

[264] *Id*.
[265] 15 C.F.R. pt. 960, app. 1, § IV(4).
[266] 15 C.F.R. pt. 960, app. 2, § A(2).
[267] *Id*.

production behaviors that both reduces exposure to and mitigates the consequences of cyber-security events. Product liability law is maturing, but proving that the harm resulted from a faulty design or failure to warn remains difficult and problematic. The formal advocacy of adherence to voluntary consensus standards by some agencies should be augmented by either:

(a) allowing those consensus standards with which an agency encourages voluntary compliance to serve as admissible evidence of competent design, a deviation from which can serve as a rebuttable basis for product liability under state laws; and clearly stating use of standards for this purpose is not federally preempted, or

(b) promulgating formal safety regulations that allow conformance with the cited standard to serve as one mechanism for compliance with the rule; and wherein failure to comply with the formal regulation could then serve as a basis for product liability under state laws.

Manufacturers and the providers of services are in the best positions to anticipate, prevent, and mitigate the harms of cyber malfeasance by others. Product liability law should therefore be clarified and strengthened, perhaps at least through proposed updates to the restatement.

Given the relatively weak ability of private law mechanisms to incentivize cyber-secure behaviors, turning to public law solutions such as legislation and regulation appears appropriate. Existing U.S. regulations, however, are a jumble of varied approaches by different oversight agencies. A review of the regulations pertinent to AASD in the transportation sector reveals very different regulatory choices among agencies in five key areas of cybersecurity oversight.

Table 2 compares the different approaches taken by each of the relevant agencies. Close inspection of Table 2 exposes that one entire segment of an interconnected AASD lacks any cybersecurity regulatory oversight whatsoever. The absence of any FCC statutory authority to exercise cybersecurity oversight means that there are no compulsory behaviors related to the communications backbone of any AASD. This omission is the most notable in the space component of any satellite communications network. While other agencies may lack the ability to regulate the communications

network, they can, and often do, regulate the terrestrial end user terminals and the processing of data provided by such networks. Communications nodes and data sources in orbit however, are not beyond the reach of hackers. Only new legislation can address this key omission in oversight of the nation's communication infrastructure as a component of AASD.

	Incident Reporting	Submission of Comprehensive Cybersecurity Plan	Licensing or Certification of Key Personnel	Specified Cybersecurity Practices	Verification of Compliance
FCC	X Encouraged to use DHS voluntary process	X	Licensing of Carriers	X	X
FAA	Few are mandatory via DHS process otherwise no	Some – if 'special conditions' apply for certification	Credentialing and licensing of: Airmen Airport personnel Mechanics Dispatchers Operators Aircraft and parts manufacturers	Some via: Advisory Circulars Industry consensus standards referenced in STCs, TSOs and other certification requirements	Safety Inspections Review prior to certification
USCG	Mandatory via DHS process and regulation	Mandatory: Vessel security assessments Vessel security plans	Credentialing and licensing of: Ship's personnel Vessels	NIST risk framework	Periodic Inspections and audits Fines and other penalties for non compliance
NHTSA	Voluntary via industry trade association	Voluntary	X	Voluntary compliance with industry consensus standards	Voluntary self-assessments Recall authority
NOAA	X	Mandatory - Data plan	X	As stated in guidelines for preparation of data plans	Data plan subject to audit

Table 2: Comparison of Regulatory Approaches in Five Key Areas of Cybersecurity

The corollary to these observations also means that no single agency will ever have a sufficient span of authority to manage system and equipment cyber threats across all AASD network segments. This fact indicates the desirability for some degree of alignment and coordination of approaches across agencies. Although the Department of Homeland Security and the Coast Guard engage in efforts to share cybersecurity best practices and strategies across federal agencies, such laudable work results only in exchanges of information and cannot by itself ensure a synergistic approach to cybersecurity regulation of AASD as a networked

system of systems.[268] Congress may wish to consider formally directing such agency collaboration either via legislation or via exercise of its oversight authority. Such actions would promote coordinated and synergistic cybersecurity regulations without unduly compromising continued innovation, or disregarding the industry-specific nuances of the particular oversight agency. Existing differences in regulatory approaches arise more from regulatory legacy and less from industry-unique circumstances that warrant these distinctions.

The needed and recommended additional steps, as outlined below also recognize the need to distinguish between cyber risks that potentially impact safety of life and those that do not. A different level of safety oversight should be required of the former, while the later, although not insignificant, can be developed with less regulatory scrutiny. Specifically, as a result of the review and analysis undertaken herein, the following legislative/regulatory recommendations are made.

A. *Legislation Regarding Disclosure of Cyber-security Events*

Industry participants all articulate a need for mechanisms to share cyber-threat events without fear of liability, regulatory retaliation, or competitor abuse. Only certain limited subsets of the AASD ecosystem, defined as "critical infrastructure," can participate in the Department of Homeland Security voluntary

---

[268] *See, e.g.*, Maureen D. Johnson, *Department of Homeland Security Efforts: Implementing Cybersecurity Initiatives Throughout the Federal Government*, 71 COAST GUARD J. SAFETY & SECURITY SEA, PROC. MARINE SAFETY & SECURITY COUNCIL, no. 4, Winter 2014–2015, at 52, https://homeport.uscg.mil/Lists/Content/Attachments/1544/Proceedings.CyberSecurity.Vol71_No4_Wint2014.pdf (describing various efforts to share cybersecurity policies, information, and best practices across multiple agencies); DEP'T OF HOMELAND SEC. & DEP'T OF TRANSP., TRANSPORTATION SYSTEMS SECTOR-SPECIFIC PLAN 15 (2015), https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (suggesting, as a collaboration of federal agencies, broad strategies for managing security, including cyber security, within the transportation sector, articulating aspirational goals, and "encourage[ing] unity of effort in cybersecurity initiatives and greater efficiency in evaluating cyber threats, vulnerabilities, and consequences").

programs for sharing such information inclusive of its statutory liability protections.[269] The definition of "critical infrastructure" under the Homeland Security Act is too narrow to encompass all transportation AASD activity of interest because that definition concerns itself solely with items that, when compromised, have a direct and debilitating impact on national security or public health.[270] Therefore, as discussed previously above, while portions of the aviation and maritime sectors come within the definition of "critical infrastructure, " this definition also operates to exclude significant elements of the AASD communications backbone, the automobile industry, and other AASD sub-elements that do not by themselves directly bear on national security or public health. Industries and AASD network components excluded from the definition of "critical infrastructure" do not enjoy the cyber event disclosure protections provided by § 214 of the Homeland Security Act.

The reluctance to share event data for fear of regulatory retaliation, competitor abuse of the data, and production in discovery therefore persists. The additional voluntary disclosure process enabled by Presidential Directive PPD-41 does not sufficiently address these concerns. Private industry voluntary disclosure organizations are an additional and valuable alternative, but do not necessarily provide the government with the comprehensive "big picture" intelligence needed to protect the country and make sound regulatory and legislative decisions. The current reporting mechanisms therefore tend to under-report incidents and retard the private sector's responses and adaptations to emerging threats.

Given the potential benefits to industry participants, the insurance sector, and the public, a unified system for sharing cyber-

---

[269] *See* Homeland Security Act of 2002, Pub. L. No. 107–296, § 214, § 116 Stat. 2135, 2152-55; 6 U.S.C. § 133 (2012).

[270] *See* Pub. L. No. 107–296, § 2(4), § 116 Stat. 2140; 6 U.S.C. § 101(4); 42 U.S.C. § 5195c(e) (2012) ("'[C]ritical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

event data responsive to these concerns should be implemented. Legitimate concern exists that blanket exemption from liability or regulatory enforcement could lead to abuse of the disclosure system as a means of avoiding accountability for avoidable harms. The NASA aviation incident safety reporting mechanism is instructive here. That system, in which aviation participants voluntarily disclose safety-related incidents and mishaps within a specified time interval, has been instrumental in spotting emerging safety concerns and issuing timely alerts and recommended responses.[271]

The Department of Homeland Security Act should be amended to either expand the definition of "critical infrastructure" to include the components of AASD used in the transportation sector, or optionally establish a mechanism whereby all participants wishing to disclose cyber-security events can do so free of liability under certain conditions. Under the second, more expansive option, the disclosure system should be exempt from the Freedom of Information Act, and it should be confidential and share information with others only in an anonymized and aggregated manner unless otherwise permitted by the disclosing party. Much like the NASA aviation safety incident reporting, the party sharing information via this mechanism should be shielded from regulatory repercussions for the events disclosed under certain conditions. Candidate provisions for a more expansive disclosure process might include protection from regulatory repercussions and from disclosure of the submitted material in a civil lawsuit, provided the following conditions are true:

(a) The disclosed event did not result from the criminal or willful negligence of the disclosing party,

(b) The disclosure documenting the event was submitted within a specified time frame.

(c) The disclosing party has on file with the appropriate regulatory agency, a comprehensive cyber-security risk mitigation

---

[271] *See* Linda Connell, Address at the ATEC Safety Reporting Seminar in Tokyo, Japan: Aviation Safety Reporting System (Jan. 11, 2011); LINDA CONNELL, NASA, AVIATION SAFETY REPORTING SYSTEM (2011), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140000574.pdf.

plan developed in accordance with relevant agency guidelines or a consensus standard acceptable to the agency,

(d) The disclosure as submitted will not be produced in a civil lawsuit alleging third party liability in cases where the event disclosed did not result in the loss of life, serious bodily harm, or permanent disability of a third party, and

(e) The disclosing party will be shielded from regulatory repercussions even in cases involving the violation of any applicable agency rule, so long as that violation was not willful or criminal, and the disclosure was submitted within the specified time limit.

The unified disclosure mechanism outlined above would encourage divulging cyber event information and would establish a predictable set of rules consistent in all industry sectors. The Department of Homeland Security is likely the best choice to continue to serve as custodian of this information given their existing mandate. Optionally, a third, non-regulatory agency or private party could serve this function.

B. *Mandatory Submission and Review of Cybersecurity Plans for OEMs and Service Providers in the Transportation Sector where Failure or Compromise of Products and Services Has Potential Safety of Life or Critical Infrastructure Consequences.*

Only the maritime sector, via Coast Guard regulation, *requires* entities to submit a comprehensive cyber-security plan.[272] When AASD cyber failures or attacks have the potential to impact safety of life, this relinquishing of safety oversight cannot be justified. Requiring submission of a comprehensive plan does not equate to over-specifying the technology or mitigating actions to be taken under such a plan. The agency, as in the case of the NHTSA, can point to multiple sources of best practices for developing a plan, but construction and filing of a plan should be *mandatory* in safety of life relevant circumstances. Leaving plan development in the realm of a voluntary activity means that there is no assurance that plans

[272] 33 C.F.R. §§ 104.300, .305, .400 (2018).

will even be developed, let alone that their quality is satisfactory, or that the plan covers all appropriate threats.

The only reasonable alternative to the above position, certification of manufacturers, and certification that parts and equipment have been designed using acceptable best practices or technical standards; imposes an even greater burden on industry. As in aviation, this model may be the best path for assuring industry achieves a minimum level of safety before putting a part or AASD into commerce. The FAA has shown that it can retain its regulatory oversight while industry remains free to promote and adopt appropriate consensus standards regarding cybersecurity certification requirements. When safety of life issues exist, deviation from this general practice should not be the norm. In the case of self-driving automobiles, the estimated savings in lives lost to traffic accidents --by one account as many as tens of thousands each year— may justify the expediency of substituting certification for another type of compulsory approach.[273] The NHSTA's existing voluntary approach puts the public in harm's way. The NHSTA voluntary approach abdicates the agency's responsibility to safeguard members of the public who reasonably are not knowledgeable or sophisticated enough to perform this function in the marketplace.

Even with the FAA's strong oversight activity, gaps in cybersecurity oversight exist. With the possible exception of operator and production certificates, the FAA does not require submission of a comprehensive cybersecurity plan. Requiring such plans of all participants whose AASD have possible safety-of-life impacts if compromised would ensure those participants at least identify and address cybersecurity risks.

C. *Concluding Remarks*

The recommendations made herein thus ensure critical segments of any AASD are subject to cybersecurity oversight and that the key elements of a cybersecurity regulatory scheme are in place across all relevant agencies. The recommendations provided above do not direct agencies to require the adoption of any specific technical cybersecurity actions. Agencies remain free to define for themselves

[273] *See* WATNEY & DRAFFIN, *supra* note 5, at 1–2.

or otherwise establish independent sources of cybersecurity best practices. The recommended approach thus also avoids calcification around a fixed set of remediations and enables a diversity of solutions to continuously evolve. By following these recommendations, industry participants can therefore remain nimble in the face of evolving cyber threats, while ensuring public safety through what proves to be needed regulatory oversight.[274]

[274] As this article was being finalized for print, President Trump signed the FAA Reauthorization Act on October 5, 2018. FAA Reauthorization Act of 2018, Pub. L. No. 115-254. This law directs the FAA to take several steps regarding cybersecurity and AI. *See id.* at §§ 548, 575, 731.

APPENDIX: SUMMARY OF FCC REGULATIONS RELATING TO LICENSING AND OPERATION OF MSS

GENERAL REQUIREMENTS	ABOARD AIRCRAFT (ESAA)	ABOARD VESSELS (ESV)	VEHICLE MOUNTED (VMES)
47 CFR §§ 25.115 and 25.130 Applicants must file Form 312 plus Schedule B	47 CFR §25.227 • Technical specifications for preventing RF interference • Frequency coordination • ESAA must be self-monitoring and capable of automatic shut off if transmission parameters exceeded • Each ESAA subject to monitoring and control and 24/7 capability to disable transmission via command	47 CFR §25.221 and §25.222 Similar to those specified for aircraft ESAA	47 CFR §25.226 Similar to those specified for aircraft ESAA
Transmitting Earth Stations 47 CFR §25.203			
Receive only Earth Stations 47 CFR §25.131 Station must be registered.			
Non-voice/non GEO MSS 47 CFR §25.135 * no interference with other systems * must comply with operational conditions placed upon the systems with which they operate * US approved space station communications only			
Access to non- US satellite networks 47 CFR §25.137 requires additional approval, analysis of competitive environment and listing of all countries in which communications with the US earth station will originate or terminate			
§25.216 All mobile stations must not interfere with aircraft radio navigation satellite service			

Table A-1: MSS Earth Station Licensing Requirements

GENERALLY	ANCILLARY TERRESTIAL COMPONENTS	NON-VOICE, NON GEO	TECHNICAL REQUIREMENTS	DIGITAL AUDIO RADIO	1.6/2.4 GHz and 2 GHz MSS
47 CFR §§ 25.114 Applicants must file Form 312 plus Schedule S	47 CFR § 25.149 • Applies to operation in the 1.5/1.6 GHz and 1.6/2.4 GHz bands • Must demonstrate non-interference with other uses • Must use licensed equipment • Must show compliance with personnel safety precautions	47 CFR §25.142 • must set forth "all pertinent and technical aspects of the system" • must demonstrate non-interference with other systems • (b)(4) must prioritize distress traffic and can't charge for same • cannot interchange traffic that's been otherwise denied to another US company	47 CFR §25.210 documents antenna and beam design and performance	47 CFR §25.144 • Must document system description • Must cover contiguous 48 states • only licensees can operate terrestrial repeaters	47 CFR §25.143 • must be Non GEO constellation for 1.6/2.4 GHz operations • mandatory regions of geographic coverage to include min and max latitudes and coverage over certain US States and territories • must demonstrate no interference with other users of spectrum • prioritization of distress and safety traffic • cannot interchange traffic that's been otherwise denied to another US company
47 CFR §25.170 (a) must file an annual report to include any space station not available for service or not performing per specifications					
47 CFR § 25.172 must file info on the telemetry, call signs and tracking of earth command stations					

Table A-2: MSS Space Station Licensing Requirements