epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL AVIATION ADMINISTRATION

Special Conditions: Garmin International, Textron Aviation Inc. Model 560XL; Airplane Electronic-System Security Protection From Unauthorized Internal Access

[Docket Nos. FAA-2018-0781; FAA-2018-0782]

January 7, 2019

By notice published November 21, 2018, the Federal Aviation Administration ("FAA") published final special conditions for Garmin G5000 avionics that allow internal and external connection "to previously isolated data networks, which are connected to systems that perform functions required for the safe operation of the airplane," and invited comments.[1]

EPIC submits these comments to the FAA to (1) express support for the FAA's decision to call attention to variances in safety regulations that create a risk of remote hacking; (2) establish that the risk of remote hacking of planes, drones, vehicles, and other Internet-connected devices is increasing; and (3) recommend that the FAA establish formal procedures to report and assess emerging cybersecurity risks.

[1] *Special Conditions: Garmin International, Textron Aviation Inc. Model 560XL; Airplane Electronic- System Security Protection From Unauthorized Internal Access*, 83 Fed. Reg. 58739-40 (Nov. 21, 2018), https://www.govinfo.gov/content/pkg/FR-2018-11-21/pdf/2018-25363.pdf;
Special Conditions: Garmin International, Textron Aviation Inc. Model 560XL; Airplane Electronic- System Security Protection From Unauthorized External Access, 83 Fed. Reg. 58740-42 (Nov. 21, 2018), https://www.govinfo.gov/content/pkg/FR-2018-11-21/pdf/2018-25362.pdf.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[2] EPIC has previously submitted comments to the FAA highlighting the security issues associated with the remote hacking of drones, noting that "hackers can exploit weaknesses in drone software to gain control of a drone's movement and other features."[3] Indeed, in EPIC's earliest comments to the FAA regarding drones, EPIC warned that "drone hacking can expose troves of sensitive data" and "poses a threat to the security of lawful drone operations."[4] In 2012, EPIC testified before the Homeland Security Committee on the "ease with which drones may be hacked" to "gain full control of a drone" or "intercept video and audio feeds[.]"[5] EPIC has also examined the security implications of connected vehicles, as well as the public safety issues arising from the Internet of Things.[6] EPIC has submitted numerous comments to federal agencies on security issues raised

[2] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[3] EPIC, Comments on the *Operation and Certification of Small Unmanned Aircraft Systems*, Federal Aviation Admin. Docket No. FAA-2015-0150, 13-14 (Apr. 24, 2015), https://epic.org/privacy/litigation/apa/faa/drones/EPIC-FAA-NPRM.pdf.
[4] EPIC, Comments on *Unmanned Aircraft System Test* Sites, Federal Aviation Admin. Docket No. FAA—2012—0252, 6 (May 8, 2012), https://epic.org/apa/comments/EPIC-Drones-Comments-2012.pdf.
[5] EPIC Association Litigation Counsel Amie Stepanovich, Testimony before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management, *Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?*, 4 (July 19, 2012), https://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf.
[6] EPIC, *Internet of Things (IoT)* (2018), https://epic.org/privacy/internet/iot/. *See, e.g.*, EPIC Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony- Nov- 18-2015.pdf; Brief of Amicus Curiae EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf; Marc Rotenberg, *Are Vehicle Black Boxes a Good Idea?*, THE COSTO CONNECTION (Apr. 2013), http://www.costcoconnection.com/connection/201304?pg=24#pg24; Marc Rotenberg, *Steer Clear of Cars That Spy*, USA TODAY (Aug. 18, 2011), http://usatoday30.usatoday.com/news/opinion/editorials/2011- 08-18-car-insurance-monitors-driving-snapshot_n.htm.

by networked vehicles,[7] including comments on the Federal Automated Vehicle Policy and the Federal Motor Vehicle Safety Standards.[8]

I. The FAA is Correct to Call Attention to Variances in Safety Regulations that Could Create a Risk of Remote Hacking

EPIC commends the FAA for recognizing the risks involved in emerging aircraft control technology and requesting public comment on an avionics design that allows both internal and external connection to previously isolated data networks.[9] As the agency notice states, "[t]his data network and design integration creates a potential for unauthorized persons to access the aircraft-control domain and airline information-services domain, and presents security vulnerabilities related to the introduction of computer viruses and worms, user errors, and intentional sabotage of airplane electronic assets (networks, systems, and databases) critical to the safety and maintenance of the airplane."[10]

Documents obtained by news media through Freedom of Information Act requests show the Department of Homeland Security ("DHS") Science & Technology Directorate has tested and found "viable attack vectors exist that could impact flight operations" as recently as 2017.[11]

---

[7] *E.g.*, EPIC, Comments on the *Federal Motor Vehicle Safety Standards: "Vehicle-to- Vehicle (V2V) Communications"*, Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2014-0022 (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA- V2V-Cmts.pdf; EPIC et al., Comments on the *Federal Motor Vehicle Safety Standards; Event Data Recorders*, Nat'l Highway Traffic Safety Admin., Docket No. NHTSA- 2012-0177 (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR- Cmts.pdf; *see generally* EPIC, *State Auto Black Boxes Policy* (2015), https://epic.org/state-policy/edr/; EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy* (2015), https://epic.org/privacy/edrs/.

[8] EPIC, Comments on the *Federal Automated Vehicle Policy*, Nat'l Highway Traffic Safety Admin., Docket No. 2016-22993 (Nov. 22, 2016), https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf/; EPIC, Comments on the Federal Motor Vehicle Safety Standards; V2V Communications, Nat'l Highway Traffic Safety Admin., Docket No. 2016-0126 (Apr. 12, 2017), https://www.epic.org/apa/comments/EPIC-NHTSA-V2V-Communications.pdf.

[9] 83 Fed. Reg. 58739; 83 Fed. Reg. 58740.

[10] 83 Fed. Reg. 58740.

[11] Aviation Cyber Initiative Research and Development, *ACI R&D Risk Summary and Report*, 5 (Apr. 10, 2017), https://www.documentcloud.org/documents/4495659-DHS-Document-Release-on-Aviation-Cybersecurity.html; Joseph Cox, *US Government Probes Airplane Vulnerabilities, Says Airline Hack Is 'Only a Matter of Time'*, Motherboard (June 6, 2018), https://motherboard.vice.com/en_us/article/d3kwzx/documents-us-government-hacking-planes-dhs.

Since commercial aircraft typically operate for 20 or more years, the Directorate assessed "15-20 more years of higher cyber vulnerability[.]"[12] According to one document, DHS anticipates "significant reluctance by the commercial world to expend resources to prevent penetration [and] attack."[13] The gravity of the risk and the difference in priorities between regulatory bodies and the private sector call for increased involvement of the FAA.

The documents obtained also included presentation slides from the U.S. Department of Energy's Pacific Northwest National Laboratory, stating, it is only "a matter of time before a cyber security breach on an airline occurs."[14] The Pacific Northwest National Laboratory presentation stressed the importance of all involved in the airline industry to understand and acknowledge the risks associated with airline cybersecurity because "effective cyber defense of aircraft will require: [c]ooperation[,] [i]nformation sharing[, and] [i]nformed and updated regulation/certification[.]"[15]

At a 2017 conference, Robert Hickey, a DHS official, stated that it took a mere two days to accomplish "remote, non-cooperative penetration" of a Boeing 757 "using typical stuff that could get through security and we were able to establish a presence on the systems of the aircraft."[16] Hacking of connected aircraft poses catastrophic risks.[17] A report from the Atlantic

---

[12] Dept. of Homeland Sec., *Aircraft Cyber Evaluation (ACE) ver. 8*, 6 (July 15, 2016), https://www.documentcloud.org/documents/4495659-DHS-Document-Release-on-Aviation-Cybersecurity.html; Joseph Cox, *US Government Probes Airplane Vulnerabilities, Says Airline Hack Is 'Only a Matter of Time'*, Motherboard (June 6, 2018), https://motherboard.vice.com/en_us/article/d3kwzx/documents-us-government-hacking-planes-dhs.

[13] Dept. of Homeland Sec., *Aircraft Cyber Evaluation (ACE) ver. 8*, 9 (July 15, 2016), https://www.documentcloud.org/documents/4495659-DHS-Document-Release-on-Aviation-Cybersecurity.html

[14] Pac. Nw. Nat'l Laboratory, *PNNL Results & Findings*, 3 (Jan. 10, 2018), https://www.documentcloud.org/documents/4495659-DHS-Document-Release-on-Aviation-Cybersecurity.html; Joseph Cox, *US Government Probes Airplane Vulnerabilities, Says Airline Hack Is 'Only a Matter of Time'*, Motherboard (June 6, 2018), https://motherboard.vice.com/en_us/article/d3kwzx/documents-us-government-hacking-planes-dhs.

[15] *Id.*

[16] Calvin Biesecker, *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*, Avionics International (Nov. 8, 2017), https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/.

[17] Kate O'Flaherty, *How To Hack An Aircraft*, Forbes (Aug. 22, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/.

Council in November 2017, found that "the aviation industry's rapid technological adoption of hardware, software, and a complex supply chain have dramatically increased both the attack surface of systems that could be affected and the potential ways of affecting them."[18]

Advances in technology can offer safer solutions for pilots and passengers, but robust cybersecurity protection is essential. The range of threats for air travel expands with these advances, so regulation must keep pace. In London, Gatwick airport was shut down for three days due to unauthorized unmanned aircraft systems hovering over the premises, and "confusion still hangs over the investigation[.]"[19] And in 2016, there were more than 50 reports of GPS interference at Manila International Airport alone.[20]

II. The FAA Should Establish Reporting Procedures for Cybersecurity Threats

As required by the FAA Extension, Safety, and Security Act of 2016, the agency must develop "a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the national airspace system [and] civil aviation[.]" 49 U.S.C. § 44903 note Aviation Cybersecurity (a)(1). The act required the Administrator to "identify and address cybersecurity risks associated with… the modernization of the national airspace system;… the automation of aircraft, equipment, and technology; and… aircraft systems." 49 U.S.C. § 44903 note Aviation Cybersecurity (a)(2)(A)(i)-(iii).

The agency should also report on vulnerabilities related to connected aircraft. In particular, FAA reports should include test results of aviation cybersecurity techniques, any

[18] Pete Cooper, *Aviation Cybersecurity—Finding Lift, Minimizing Drag*, Atlantic Council, 33 (Nov. 2017), https://www.atlanticcouncil.org/images/Aviation_Cybersecurity_web_1107.pdf.
[19] Jamie Grierson, *Gatwick returns to normality but drone threat remains*, Guardian (Jan. 4, 2019), https://www.theguardian.com/world/2019/jan/04/gatwick-returns-to-normality-but-drone-threat-remains.
[20] Kate O'Flaherty, *How To Hack An Aircraft*, Forbes (Aug. 22, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/; International Civil Aviation Organization, Regional Preparatory Group Meeting for WRC-2019, *GPS Interference/Signal Degradation in Manila, Philippines Affecting Flight and ATM Operations*, 1 (Mar. 28, 2017).

incidents of unauthorized access to aircraft, and assessments of industry standards for the sector. The Inspector General listed FAA Cybersecurity as a Top Management Challenge, drawing particular attention to "wireless technologies on aircraft" and "airlines' use of IoT."[21] The report stated the "FAA has not resolved its longstanding cybersecurity issues."[22]

EPIC appreciates the efforts of the FAA to highlight the cybersecurity risks raised by this very specific situation, but it is clear the FAA needs to move quickly and address the potential cybersecurity risks faced by the airline industry as a whole.

III. Conclusion

Connected aircraft pose serious security risks, and the FAA is right to include public comment in addressing those risks, but expanded reporting is necessary to respond appropriately to the risks and to comply with the directives of the FAA Extension, Safety, and Security Act of 2016.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow

[21] U.S. Dep't of Trans., Ofc. of Inspector Gen., *DOT's Fiscal Year 2018 Top Management Challenges*, 36 (Nov. 15, 2017), https://www.faa.gov/about/plans_reports/media/fy_2018_ig_top_management_challenges.pdf.
[22] *Id.*