Journal of Air Law and Commerce

Volume 82 | Issue 4 Article 5

2017

Cybersecurity in Aviation: Constant Vigilance Required

Hyattye O. Simmons

CYBERSECURITY IN AVIATION: CONSTANT VIGILANCE REQUIRED

HYATTYE O. SIMMONS*

I. THE SCOPE OF THIS ARTICLE[1]

"Aviation is proof that given the will, we have the capacity to achieve the impossible."[2]

In today's world, "it is imperative . . . [for] an efficient [and secure] . . . flow of goods and passengers"[3] that we find the "will" to develop, implement, and maintain reasonable and resilient cybersecurity in aviation. Given the scope of the aviation indus-

* Mr. Simmons is a former General Counsel of the Texas Secretary of State and of Dallas Area Rapid Transit (DART) (retired after twenty-four years of service, last five years as DART's General Counsel). Mr. Simmons currently serves as a Board Member and General Counsel for numerous non-profit corporations, including serving as General Counsel for the InfraGard National Members Alliance—a national alliance between the FBI and the private sector to help improve the security, preparedness, and resiliency of America's critical infrastructure. Mr. Simmons was the 2009 recipient of the Magna Stella Award for excellence in leadership and management for a non-profit or government agency from the Texas General Counsel Forum. Mr. Simmons is a 1984 graduate of the University of Texas at Austin School of Law. He received his Bachelor of Science in Government from Lamar University, where he completed a four-year program in two and a half years with High Honors. In 2017, he received the Lamar University Distinguished Alumnus Award.

[1] Caveat: The information contained in this article is provided for educational and informational purposes only, and the statements contained herein are solely the opinions of Hyattye O. Simmons or cited authorities. No copyright is claimed to original U.S. government works or original works by other authors.

[2] This quote has been attributed to Edward (Eddie) Vernon Rickenbacker (October 8, 1890—July 23, 1973) https://www.goodreads.com/quotes/519937-aviation-is-proof-that-given-the-will-we-have-the [https://perma.cc/7X4A-WD67]. Captain Rickenbacker was an American World War I "ace" fighter pilot and a World War I Medal of Honor recipient. *See generally Edward Rickenbacker*, THE AERODROME, http://www.theaerodrome.com/aces/usa/rickenbacker.php [https://perma.cc/3RR8-HVZQ]; *see also Medal of Honor Recipients*, U.S. ARMY CENTER OF MILITARY HISTORY, http://www.history.army.mil/moh/worldwari.html#RICKENBACKER [https://perma.cc/3XKP-C5NN].

[3] MARIA G. BURNS, LOGISTICS AND TRANSPORTATION SECURITY: A STRATEGIC, TACTICAL, AND OPERATIONAL GUIDE TO RESILIENCE xxv (2016).

try in the United States,[4] this article will analyze the nature of cybersecurity in three main areas: major cybersecurity issues, the importance of these issues, and recommended solutions.

II. MAJOR CYBERSECURITY ISSUES[5]

A. Aviation-Specific Cybersecurity Issues: The U.S. Government Accountability Office's[6] Critical Reviews of the Federal Aviation Administration's Cybersecurity Management of the National Airspace System

The Federal Aviation Administration (FAA), "an agency of the Department of Transportation, is primarily responsible for the advancement, safety, and regulation of civil aviation, as well as overseeing the development of the [nation's] air traffic control system," known as the National Airspace System (NAS).[7] "Over

---

[4] In 2014, air carriers in the United States performed almost 9 million aircraft departures, transported over 700 million "revenue passengers," and carried over 12 million "revenue tons" of freight and mail. *See* U.S. Dep't of Transp., *National Transportation Statistics*, 68 (2015), https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/NTS_Entire_15Q4_0.pdf [https://perma.cc/8465-WN9U]. During the same year, general aviation, which is defined as "all aviation other than military and scheduled commercial airlines," accounted for "$219 billion in total economic output in the United States." *See* Gen. Aviation Mfrs. Ass'n, *General Aviation Statistical Databook & 2015 Industry Outlook* 1 (2014), https://gama.aero/wp-content/uploads/GAMA_2014_Databook_LRes-LowRes.pdf [https://perma.cc/3F62-MTX7] . As an industry, "[b]ased on data collected during the last census in 2012, aviation . . . contributed $1.5 trillion in total [United States] economic activity . . . ." Matthew Lew et al., *Please Fasten Your Seat Belts: Managing Digital Risk to Support Aviation Innovation*, Deloitte, at 1, (Apr. 2015), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-aviation-cyber-risk-report-04222015.pdf [https://perma.cc/ZZL5-W9UL].

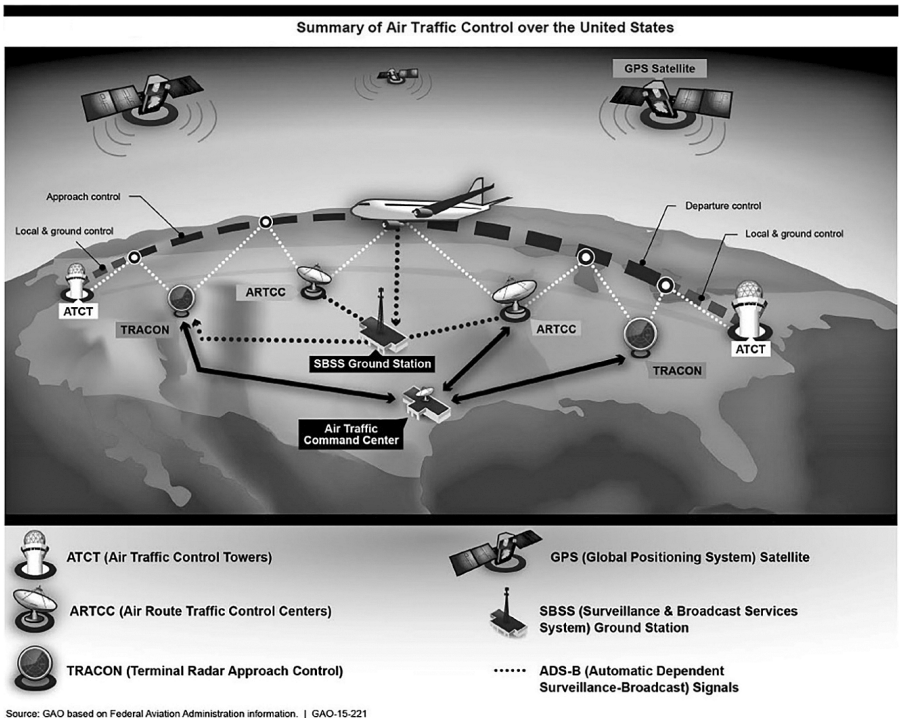
[5] Information and analysis contained in this section of the article is derived from non-classified, non-confidential, publicly available, and reliable sources.

[6] "The U.S. Government Accountability Office (GAO) is an independent, nonpartisan agency that works for Congress. Often called the 'congressional watchdog,' GAO investigates how the federal government spends taxpayer dollars. The head of GAO, the Comptroller General of the United States, is appointed to a 15-year term by the President from a slate of candidates Congress proposes." *About GAO*, U.S. Gov't Accountability Office, http://www.gao.gov/about/ [https://perma.cc/7HRL-KH8Y].

[7] U.S. Gov'T Accountability Office, GAO-15-221, Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems 3 (2015) [hereinafter GAO-15-221]. This system "includes more than 19,000 airports, nearly 600 air traffic control facilities, and approximately 65,000 other facilities, including radar . . . [and] ground-based navigation aids." *Id.* "The Department of Transportation's (DOT) operations rely on 463 information technology (IT) systems, nearly two-thirds of which belong to . . . FAA . . . . These systems represent an annual investment of approximately $3 billion—one of the largest IT investments among Federal civilian agencies. Moreover, the Department's financial IT

46,000 FAA personnel and approximately 608,000 pilots operate about 228,000 aircraft within the NAS, including up to 2,850 flights at any given moment."[8] As aircraft moves across the NAS, more than 500 air traffic control towers supervise flights, assisted by 160 Terminal Radar Approach Control facilities and twenty-two Air Route Traffic Control Centers (ARTCC).[9] The figure below provides a summary of air traffic control in the United States[10]:

Figure 1



systems are used to award, disburse, and manage approximately $117 billion in Federal funds annually." OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REP. FI-2016-001, FISMA 2015: DOT HAS MAJOR SUCCESS IN PIV IMPLEMENTATION, BUT PROBLEMS PERSIST IN OTHER CYBERSECURITY AREAS 2 (2015) [hereinafter REP. FI-2016-001].

[8] GAO-15-221, *supra* note 7, at 3.

[9] *Id.*

[10] *Id.* at 5 fig.1.

1. GAO's January 2015 Report on FAA's Information Security[11]

U.S. Congress members requested that the GAO[12] "review FAA's information security program."[13] The review's purpose "was to evaluate the extent to which FAA had effectively implemented information security controls to protect its air traffic control systems."[14] The GAO concluded that, although the "FAA took many steps to address . . . risks" in a large, complex, interconnected system like the NAS,[15] "weaknesses remain that challenge [ ] FAA in fulfilling its mission of ensuring the safety and efficiency of the nation's airspace operations."[16] Specifically, the GAO made the following cybersecurity-related findings:

- "Inadequately protected systems may be vulnerable to insider threats as well as the risk of intrusion by individuals or groups with malicious intent who could use their illegitimate access to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks."[17]
- The FAA's increased use of Internet Protocol technologies to communicate over interconnected computer networks "comes [with] increased risk: integrating critical infrastructure systems with information technology networks provides significantly less isolation from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats."[18]
- "FAA Did Not Consistently Control Access to NAS Systems."[19]

---

[11] *Id.* at 3.

[12] The Honorable John Thune, Chairman; The Honorable Bill Nelson, Ranking Member, Committee on Commerce, Science, and Transportation, United States Senate; The Honorable Bill Shuster, Chairman; The Honorable Peter DeFazio, Ranking Member, Committee on Transportation and Infrastructure, United States House of Representatives; The Honorable Frank A. LoBiondo, Chairman; The Honorable Rick Larsen, Ranking Member, Subcommittee on Aviation Committee on Transportation and Infrastructure, United States House of Representatives; and The Honorable John Katko, Chairman, Subcommittee on Transportation Security Committee on Homeland Security, United States House of Representatives. *Id.* at 35.

[13] GAO-15-221, *supra* note 7, at *GAO Highlights*, i. "Maintaining an effective information security program—one that quickly identifies and addresses vulnerabilities—is critical to ensuring continuity of operations and thwarting individuals who attempt to gain unauthorized access to systems and information." REP. FI-2016-001, *supra* note 7, at 2.

[14] GAO-15-221, *supra* note 7, at *GAO Highlights*, i.

[15] *See id.* at 3.

[16] *Id.* at 30.

[17] *Id.* at 7.

[18] *Id.* at 8.

[19] *Id.* at 13.

- "Although Control Mechanisms Were Put in Place, FAA Did Not Always Adequately Protect the Boundary of NAS Systems."[20]
- "FAA Did Not Consistently Implement Controls for Identifying and Authenticating Users of NAS Systems."[21]
- "FAA Did Not Always Ensure Users Were Properly Authorized to Access NAS Systems."[22]
- "Sensitive Data Were Not Always Sufficiently Encrypted."[23]
- "Changes to Network Systems and Software Were Not Always Properly Controlled."[24]
- "FAA Did Not Always Properly Control Changes to Network Devices or Ensure Key Systems Were Fully Patched."[25]
- "FAA Did Not Fully Implement Its Information Security Program."[26]
- "Identified Security Weaknesses Were Not Always Addressed in a Timely Fashion."[27]
- "NAS Incident Detection and Response Activities Were Limited."[28]
- "Contingency Plans Were Not Always Complete or Adequately Tested."[29]
- "Inadequate Agency-Wide Information Security Risk Management Processes Contribute to Weaknesses in Security Controls and Security Management."[30]

In its last conclusion, the GAO stated:

> Until FAA establishes stronger agency-wide information security risk management processes, fully develops its NAS information security program, and ensures that remedial actions are addressed in a timely manner, the weaknesses that we identified are likely to continue, placing the safe and uninterrupted operation of the nation's air traffic control system at increased and unnecessary risk.[31]

In a written response to the GAO's report, the FAA concurred with the GAO's recommendations for improving the NAS infor-

---

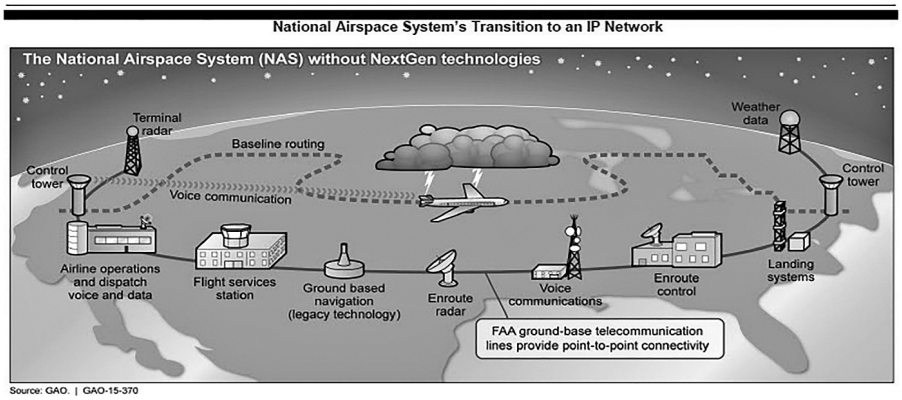
[20] *Id.* at 14.
[21] *Id.*
[22] *Id.* at 15.
[23] *Id.* at 16.
[24] *Id.* at 17.
[25] *Id.* at 18.
[26] *Id.* at 19.
[27] *Id.* at 23.
[28] *Id.* at 24.
[29] *Id.* at 25.
[30] *Id.* at 27.
[31] *Id.* at 31.

mation security.[32] The Department of Transportation "also stated that FAA recognizes the need to secure the NAS environment as part of the nation's critical infrastructure, and that FAA has taken several steps to improve NAS information security."[33]

2. GAO's April 2015 Report on FAA's Transition to "NextGen"[34]

"NextGen is a modernization effort begun in 2004 by FAA to transform the nation's ground-based [Air Traffic Control] system into a system that uses satellite-based navigation and other advanced technology . . . [which] will use an Internet Protocol (IP) based network to communicate."[35] The figures below show the "different parts of the NAS, the flow of information among them, and their transition to an IP-based network"[36]:

Figure 2



[32] *Id.* at 33, 39–40. Please note that besides the GAO's recommendations for improving the FAA's NAS information security, the GAO also made an additional 168 recommendations "in a separate report with limited distribution." *Id.* at 31–32.

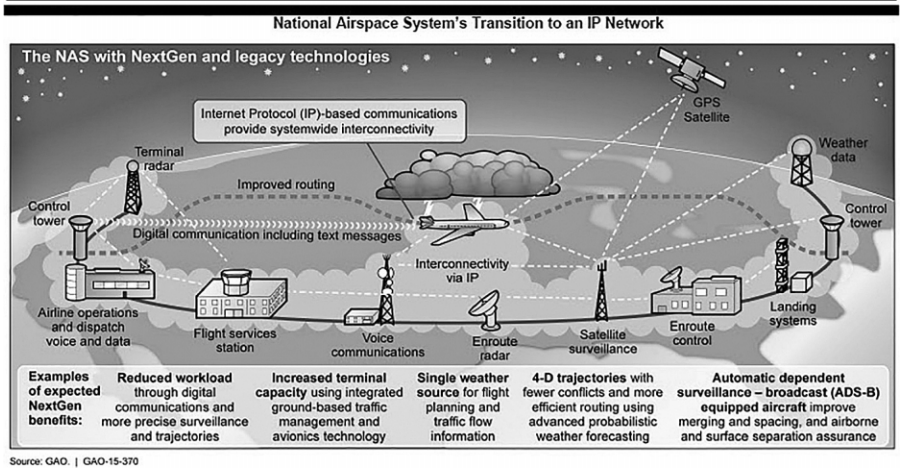
[33] *Id.* at 33.

[34] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-370, AIR TRAFFIC CONTROL: FAA NEEDS A MORE COMPREHENSIVE APPROACH TO ADDRESS CYBERSECURITY AS AGENCY TRANSITIONS TO NEXTGEN (2015) [hereinafter GAO-15-370].

[35] *Id.* at 4.

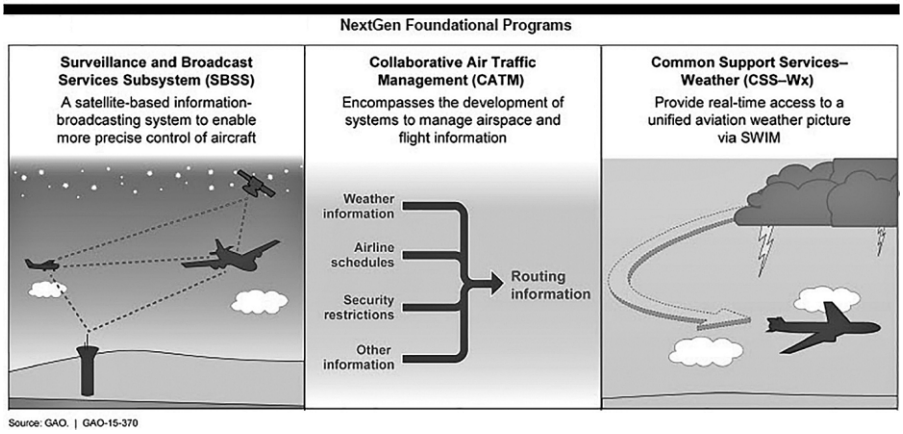
[36] *Id.* at 4–5.

Figure 3



As shown by the figure below, the Surveillance and Broadcast Services Subsystem (SBSS), the Collaborative Air Traffic Management (CATM), and the Common Support Services Weather (CSS-Wx) comprise three of the six NextGen foundational programs[37]:

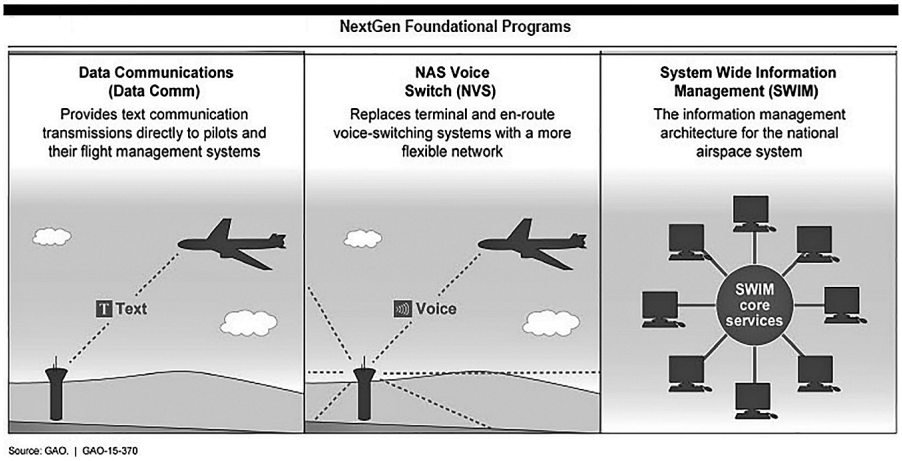
Figure 4



Data Communications (Data Comm), the NAS Voice Switch (NVS), and the System Wide Information Management (SWIM), as shown below, comprise the remaining three NextGen foundational programs[38]:

[37] *Id.* at 6–7.
[38] *Id.*

Figure 5



As with the January 2015 GAO review of the FAA, U.S. Congress members requested that the GAO[39] perform a review of the FAA, but this time the focus was on the FAA's cybersecurity efforts.[40] During the course of its review, the GAO found three significant cybersecurity challenges facing the FAA: "protecting [the] air traffic control [ ] information system, [ ]securing aircraft avionics used to operate and guide aircraft, and [ ]clarifying cybersecurity roles and responsibilities among multiple FAA offices."[41] With regard to the first cybersecurity challenge, protecting the air traffic control information system, the GAO made the following finding:

> New networking technologies connecting FAA's ATC [Air Traffic Control] information systems expose these systems to new cybersecurity risks, potentially increasing opportunities for systems to be compromised and damaged. Such damage could stem both from attackers seeking to gain access to and move among information systems, and from trusted users of the systems, such as controllers or pilots, who might inadvertently cause harm. FAA's

---

[39] The Honorable John Thune, Chairman; The Honorable Bill Nelson, Ranking Member, Committee on Commerce, Science, and Transportation, United States Senate; The Honorable Bill Shuster, Chairman; The Honorable Peter DeFazio, Ranking Member, Committee on Transportation and Infrastructure, United States House of Representatives; The Honorable Frank A. LoBiondo, Chairman; The Honorable Rick Larsen, Ranking Member, Subcommittee on Aviation Committee on Transportation and Infrastructure, United States House of Representatives; and The Honorable John Katko, United States House of Representatives. *Id.* at 44.

[40] *Id.* at *GAO Highlights*, i.

[41] *Id.* at 11.

> ATC-related information systems are currently a mixture of old, legacy systems and new, IP-networked systems. FAA's legacy systems consist mainly of decades-old, point-to-point, hardwired information systems, such as controller voice-switching systems, that share information only within their limited, wired configuration. In contrast, FAA plans for NextGen call for the new information systems to be networked together with IP technology into an overarching system of interoperating subsystems . . . . [I]f one system connected to an IP network is compromised, damage can potentially spread to other systems on the network, continually expanding the parts of the system at risk . . . . We reported in January 2015 [in GAO 15-221] that FAA has taken steps to protect its ATC systems from cyber-based threats. However, we stated that significant security-control weaknesses remain that threaten the agency's ability to ensure the safe and uninterrupted operation of the national airspace system. We made numerous recommendations to address these weaknesses, and FAA has concurred with these recommendations.[42]

IP connectivity was also at the center of the threat for the second cybersecurity challenge, securing aircraft avionics:

> [M]odern communications technologies, including IP connectivity, are increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems. Aircraft information systems consist of avionics systems used for flight and in-flight entertainment [see figure [ ] below]. Historically, aircraft in flight and their avionics systems used for flight guidance and control functioned as isolated and self-contained units, which protected their avionics systems from remote attack. However, . . . IP networking may allow an attacker to gain remote access to avionics systems and compromise them . . . .[43]

---

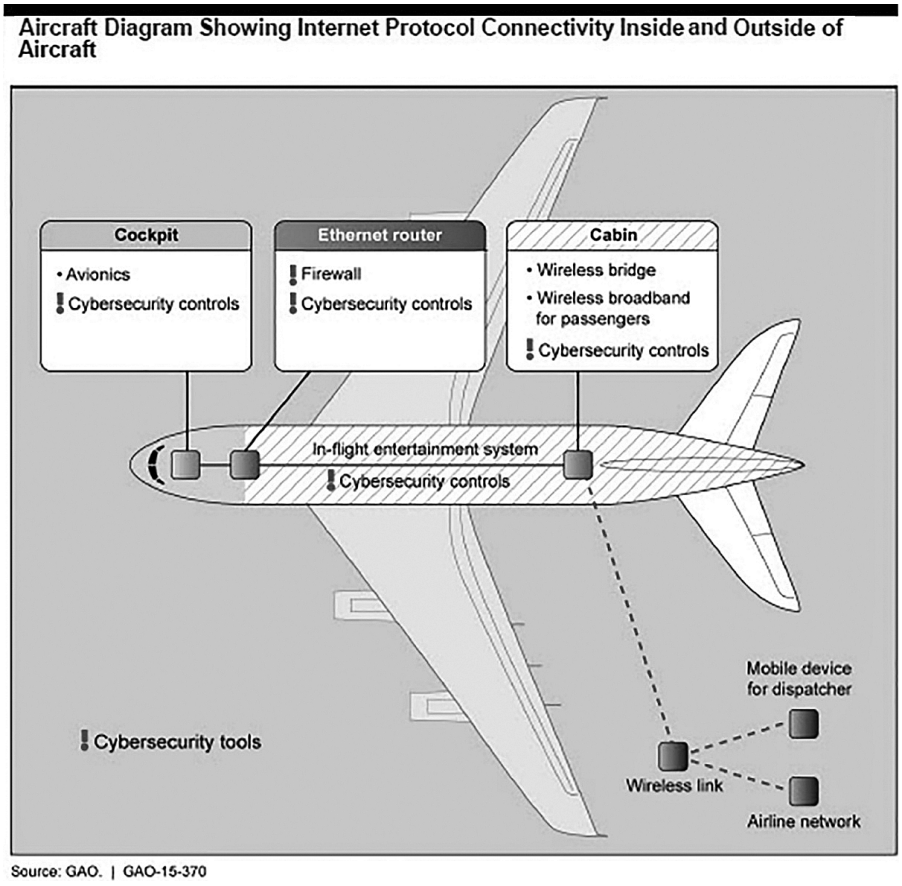
[42] *Id.* at 12–13. The GAO further found that the FAA is "designing and deploying an enterprise approach intended to strengthen the cybersecurity of its information systems." *Id.* at 14. Notwithstanding, the GAO found that the FAA could enhance its cybersecurity by adopting and implementing a "holistic threat model," which "could help FAA be more proactive in dealing with the rise of insider threats in federal agencies." *Id.* at 15–16. In making this last statement, the GAO referenced a 2014 FAA "malicious" incident:

> The 2014 malicious insider attack on FAA's Aurora, Illinois, enroute facility, while not facilitated through cyber means, destroyed ATC IP and point-to-point telecommunications lines, preventing ATC electronic communications and the gathering and use of flight data, such as radar data, to track aircraft, resulting in over $350 million in financial losses to airlines.

Id. at 16 n.22.

[43] *Id.* at 18. In response to this threat,

Figure 6



Lastly, with regard to clarifying cybersecurity roles and responsibilities, the GAO found that the FAA has taken steps to (1) "align [ ] cybersecurity orders and policies, as well as IT infrastructure and governance, with the changing needs of the

---

> FAA's Office of Safety began developing a [more comprehensive] airworthiness rule covering avionics cybersecurity in 2013 but determined more research was necessary before rulemaking could begin and halted the process. In December 2014, FAA tasked its Aviation Rulemaking Advisory Committee (ARAC) with submitting a report within 14 months of the March 2015 kickoff meeting that provides recommendations on rulemaking and policy, and guidance on best practices for information security protection for aircraft, including both certification of avionics software and hardware, and continued airworthiness.

Id. at 21.

NextGen cyber environment[,]" and (2) to "better coordinate its cybersecurity efforts."[44]

3. Epilogue to GAO's Reviews of FAA: Improvements[45] *Have Been Made, But More are Needed*

The FAA has taken steps to better protect the NAS, including NextGen, from cyberattacks. For example, as shown by the figure below, the six NextGen foundational programs are in the process of being made more secure[46]:

---

[44] *Id.* at 22. With regard to better coordination, the GAO noted that "FAA runs exercises that simulate cyber-attacks and are designed to increase internal collaboration and help clarify roles during such events." *Id.*

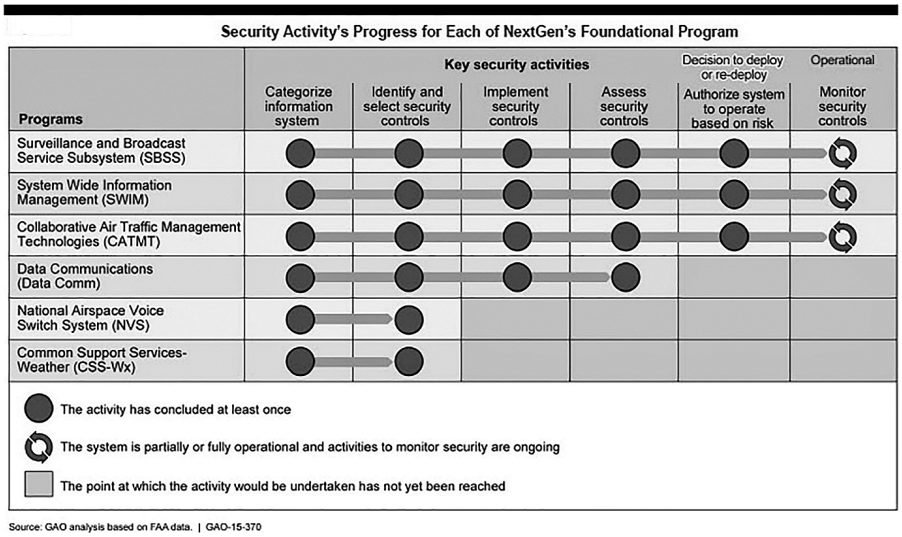
[45] In the process of writing this article, this author contacted the FAA to obtain its most current public response to the GAO's findings and recommendations. On January 5, 2016, Mark Allen, Chief of Staff, FAA NextGen (ANG), responded to my request by referencing the FAA's letter to GAO (dated Mar. 31, 2015) starting on page 48 of GAO-15-370. Below are excerpts from this letter:

> The Federal Aviation Administration (FAA) recognizes that cyber-based threats to federal information systems are becoming a more significant risk and are rapidly evolving and increasingly difficult to detect and defend against. We take this risk very seriously. We know that the Agency must be vigilant against the disruption of critical operations and infrastructure systems as more new internet-connected technologies are introduced into the National Airspace System (NAS). Accordingly, the FAA is committed to strengthening our capabilities to defend against new and evolving threats with a high degree of urgency . . . . It is also important to note that the FAA had already initiated a comprehensive program to improve the cybersecurity defenses of the NAS infrastructure, as well as other FAA mission-critical systems . . . . Recognizing the need to ensure an Agency-wide view and oversight of cyber-risk, the FAA established an Executive Cybersecurity Steering Committee (CSC) in November 2013 . . . . CSC priorities include the identification and correction of both existing and evolving vulnerabilities on all internet protocol-based systems and the establishment of an Agency-wide threat model for fiscal year 2016 . . . . The FAA established a Cyber Test Facility at the William J. Hughes Technical Center to enable thorough testing of cybersecurity capabilities to fully understand the impact, if any, before introducing them into our operational systems . . . . The FAA concurs with recommendations 1 and 3 [contained in GAO-15-370] and will implement the appropriate corrective actions by January 30, 2016. The Agency believes it has complied with the intent of recommendation 2.

Id. at 48–49.

[46] *Id.* at 30 fig.2.

Figure 7



Notwithstanding, there remains significant room for improvement.[47] Once accomplished, the end result of these improve-

---

[47] This report contained the following recommendations for FAA improvement:

> To better ensure that cybersecurity threats to NextGen systems are addressed, the Secretary of Transportation should instruct the FAA Administrator to take the following three actions.
>
> - As a first step to developing an agency-wide threat model, assess the potential cost and timetable for developing such a threat model and the resources required to maintain it.
> - Incorporate the Office of Safety into FAA's agency-wide approach by including it on the Cybersecurity Steering Committee.
> - Given the challenges FAA faces in meeting OMB's guidance to implement the latest security controls in NIST's revised guidelines within one year of issuance, develop a plan to fund and implement the NIST revisions within OMB's time frames.

Id. at 41. For more areas in which the FAA needs improvement, *see* GAO-15-221, *supra* note 7, at 31–32; *see also* REP. FI-2016-001, *supra* note 7, at 10, 13, 15–16, 18–20, 24–28, 30–31, 38. In one of its findings, the GAO determined that the FAA's SBSS, one of NextGen's foundational programs, did not "Sufficiently Assess Key Controls Prior to Deployment." GAO-15-370, *supra* note 34, at 35. This contributed to a system outage:

> [I]n August 2010, an engineer made an error while implementing a system change that caused the network to shut down, which prevented surveillance data transmitted through the hub from reaching FAA control centers. As a result, air traffic controllers could not use SBSS surveillance data to help separate aircraft in the affected locations for nearly 16 hours. A report produced by the SBSS contractor after the outage identified that the outage had occurred be-

ments will be a safer and more secure NAS and aviation industry for this country.[48]

B. Other Major Cybersecurity Issues

The aviation industry is also "exposed to more familiar cyber risks" as a result of its dependence on technology.[49] Boeing, one of the world's largest aerospace companies and a leading manufacturer of commercial jetliners, summarized the aviation industry's dependence on technology as follows:

> Networks are embedded in our economies and our political and social lives. These networks and information systems hold information of immense value, and they control the machinery that provides our critical services and impact our everyday lives from banking to travel. While this interconnectedness creates immense economic value, we now realize it has the potential of being a major source of risk to commerce and our nation.[50]

For example, "[e]-commerce is the aviation industry's primary sales platform. With the development of sophisticated online sales channels and rewards programs, airlines have become in-

---

> cause of shortcomings in the processes and controls for managing and controlling changes to the system . . . . FAA officials stated the outage has been thoroughly investigated to ensure that the SBSS program and the contractor learned from the experience, and that remedial actions were taken to strengthen the controls.

GAO-15-370, *supra* note 34, at 35–36.

[48] While its reviews focused on the FAA, the GAO's analysis and findings could be utilized by other entities within the aviation industry to improve their cybersecurity. For example, adoption and implementation of a "holistic threat model" could enhance any entity's cybersecurity. *See* GAO-15-370, *supra* note 34, at 15. The concept of applying a "holistic approach" to aviation cybersecurity is not new: "While overcoming current cyber security concerns require technical expertise, *the aviation security community should address this new security landscape holistically* and aim for cyber resilience, rather than merely plugging gaps in the current cyber security architecture deployed in the aviation systems." Martin Siu et al., *Aviation Cyber Security: A New Security Landscape*, J. Aviation Mgmt., at 74 (2014) (emphasis added) http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/AviationCyberSecurity_A_NewSecurityLandscape.pdf [https://perma.cc/Q7ZZ-F4SM]. The Journal of Aviation Management is an annual publication by the Singapore Aviation Academy, the training arm of the Civil Aviation Authority of Singapore. *About Us*, Sing. Aviation Acad., http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/About_Us/?__locale=en [https://perma.cc/45RC-32KV].

[49] Matthew Lew et al., *supra* note 4, at 3.

[50] The Boeing Company, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Nat'l Inst. Standards & Tech. 1, 4 (Apr. 8, 2013) https://www.nist.gov/sites/default/files/documents/2017/06/01/040813_boeing_part2.pdf [https://perma.cc/SVR3-4PDV].

creasingly reliant on Internet-based data exchange to transact and promote their businesses."[51] This increased use of technology in the aviation industry has been motivated "by the drive towards achieving greater efficiency, reduction in the use of manpower, and greater use of IT to reduce cost and increase synergies between and amongst stakeholders."[52] While this "electronic connectivity" has immense economic value, as previously noted, it also has major risks:

> Loyalty program IDs and payment card information (PCI) are used to link consumers to their reservations, and may be stored and accessed by a range of other services, including executive club memberships, seat upgrades, and baggage check-in services, across a range of devices like in-airport kiosks, consumer handheld devices and gate agent kiosks. A gate agent or automated kiosk can access a customer's entire profile and itinerary using one piece of personal identification information (PII). A cyber breach involving a single identifier, or a rudimentary social engineering attack . . . could threaten passenger safety, and expose airlines to new sources of potential liability.[53]

Accordingly, "cyber threats such as computer viruses and more malicious deliberate attacks on [aviation] computer systems[54] by hackers and other adversaries are not new occurrences."[55] As shown by the diagrams below, this type of cybersecurity threat continues to grow[56]:

---

[51] Matthew Lew et al., *supra* note 4, at 3.

[52] Bernard Lim, *Aviation Security: Emerging Threats from Cyber Security in Aviation—Challenges and Mitigations*, J. AVIATION MGMT. 81, 83 (2014) http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/EmergingThreats_CyberSecurityinAviation_ChallengesandMitigations.pdf [https://perma.cc/TWS9-W7P3].

[53] Matthew Lew et al., *supra* note 4, at 3.

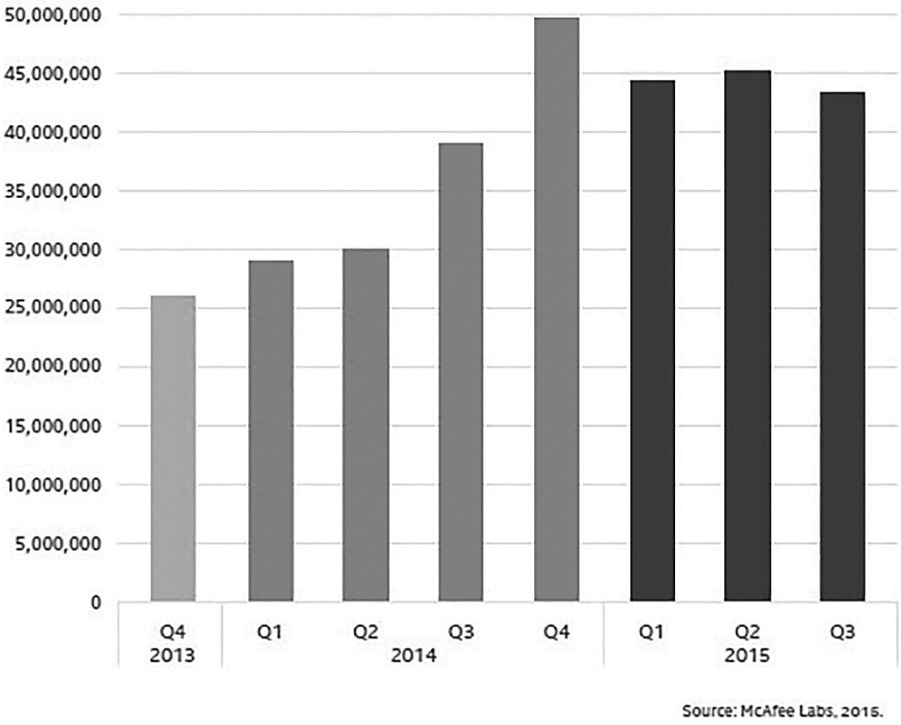
[54] TRANSP. RES. BD., *Guidebook on Best Practices for Airport Cybersecurity*, AIRPORT COOP. RES. PROGRAM, Rep. 140, at 1 (2015), http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pdf [https://perma.cc/AP7Y-QJ3M].

> The technology that may be affected is not limited to the desktop computers, servers, and network devices that compose typical information technology (IT) infrastructure. Flight information display systems (FIDS), airfield lighting controls, heating and ventilation systems, baggage handling systems, access control devices, and a broad range of other mission-critical systems rely on digital technology that may be vulnerable to attack. Since these systems are often not regarded as computing devices, cybersecurity protective measures are often not applied.

[55] Lim, *supra* note 52, at 83.

[56] *McAfee Threats Report: November 2015*, MCAFEE 1, 49–53 (2015), http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-nov-2015.pdf

Figure 8
New Malware



[https://perma.cc/JCN5-3ULH]. McAfee, one of the leading companies providing global digital security solutions (i.e., anti-malware, antispyware, and antivirus) and now a standalone company, (*see generally*, *A Brand New McAfee Commits to Building a Safer Future*, MCAFEE (Apr. 3, 2017), https://www.mcafee.com/mx/about/newsroom/press-releases/press-release.aspx?news_id=20170403006682 [https://perma.cc/Q85L-JSN6]), found that every "hour more than 7.4 million attempts were made (via emails, browser searches, etc.) to entice our customers into connecting to risky URLs[; every] hour more than 3.5 million infected files were exposed to our customers' networks[; and every] hour an additional 7.4 million potentially unwanted programs attempted installation or launch." *Id.* at 3.

Figure 9
Total Mobile Malware

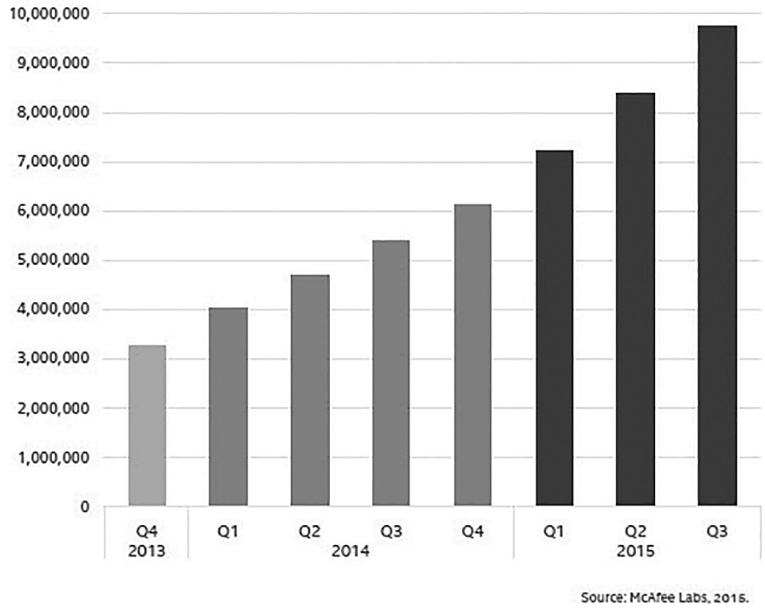
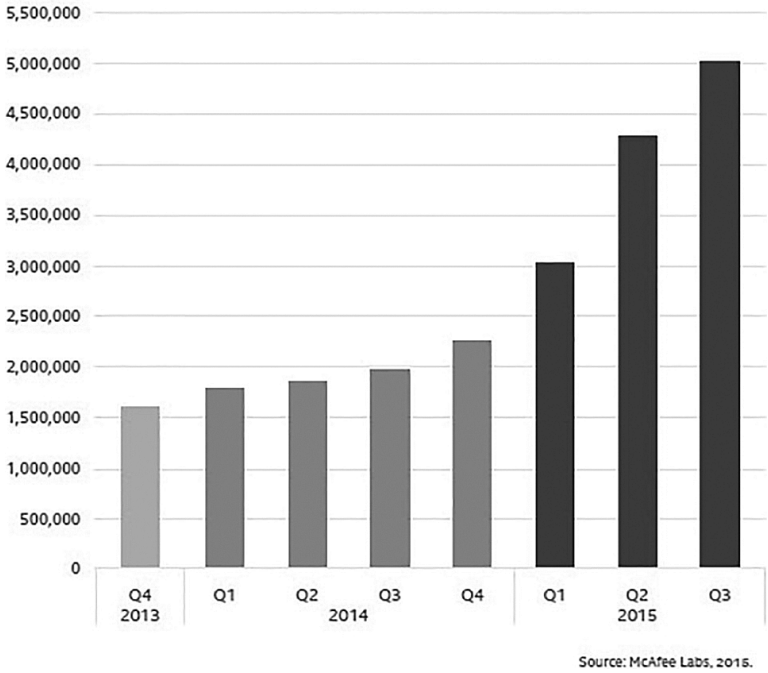


Figure 10
Total Ransomware



In addition to this trend,[57] cybercriminals continue to develop inventive methods of finding their victims,[58] including the deployment of new types of cyber threats:

> [These new threats include a] new breed of fileless malware, which evades detection by hiding in the Microsoft Windows registry and deleting all traces of its infection from the file system . . . , poor coding practices for mobile app cloud security . . . [which increased the risk of] exposure of user data in the cloud, [and the] return of macro malware, primarily through sophisticated spam [e-mail] campaigns and clever macros that remain hidden even after they have downloaded their payloads.[59]
>
> [Furthermore, cloud] computing will also provide tremendous resources to [cybercriminals] in the form of computing and storage capacity, plus the ability to appear and disappear at the click of a mouse. Law enforcement organizations will find it challeng-

---

[57] The amount of money that cybercriminals are collecting from these activities is staggering. For example, with regard to just one type of ransomware, "the CryptoWall Version 3 ransomware family, . . . has generated in excess of $325 million in ransom payments . . . ." *Id.* Ransomware "is a type of malware that prevents or limits users from accessing their [computer] system [or data] . . . [until] its victims [pays money] through certain online payment methods." *Definitions: Ransomware*, TREND MICRO (2017), http://www.trendmicro.com/vinfo/us/security/definition/Ransomware [https://perma.cc/4H49-BLLA].

> The word malware comes from the words "malicious software." It is an umbrella term for any piece of software, script or code designed by its creators to perform specific routines or have specific behaviors that have undesirable results for the affected users of a computer system or a network. These undesirable results include anything from annoying popup ads or messages, disruption of normal computer operations, to the exposure of personal or confidential data. Malware encompasses computer viruses, Trojans, worms, spyware, backdoors, and other malicious software.

Threat Encyclopedia: Malware, TREND MICRO (Oct. 9, 2012), http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/malware [https://perma.cc/M2XG-ASAK].

[58] For example, in a "watering hole" cyber-attack, the cybercriminal researches the "web habits" of a targeted group or organization. Once the cybercriminal has identified a website that is frequently visited by the targeted group, the cybercriminal infects the website with malware: the goal being to infect the computer (and computer systems of the organization) when a member of the targeted group visits the "tainted" website. *See Watering Hole Attacks*, SYMANTEC (2012), https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf [https://perma.cc/HX6B-BAR2]. During one "significant watering hole attack, [the cybercriminals] took advantage [of a web site] vulnerability . . . and coupled [malware] with a specific piece of software produced by [the] legitimate vendor." Symantec, *Internet Security Threat Report*, 20 ISTR 1, 66 (2015), http://www.symantec.com/security_response/publications/threatreport.jsp [https://perma.cc/K8FD-C93L].

[59] *McAfee Threats Report: November 2015*, *supra* note 56, at 3.

> ing to shut down an entire cloud service provider for the behavior of [a few] criminal clients, so it will be necessary to go after other criminal resources, such as their Bitcoin wallets,[60] to put them out of business.[61]

Finally, "[w]ith the continued growth of the global civil aviation industry, the increasing number of air [travelers], development of new, larger and more modern airports as well as the introduction of new and more sophisticated aircraft,"[62] the aviation industry will have to develop new methods of handling the never ending increase of the "cyberattack surface."[63] As shown by the figure below, "more users, more data, more devices, and more clouds [are] creating a perfect security storm of threats and vulnerabilities"[64]:

---

[60] Correspondingly, to go after the "illegal wealth" obtained by cybercriminals, on April 1, 2015, President Obama issued Executive Order 13694, titled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*:

> I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.

Exec. Order No. 13694, 80 Fed. Reg.18,077 (Apr. 1, 2015) ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities").

In accordance with this Executive Order, on December 31, 2015, the U.S. Department of Treasury issued final regulations to govern its application and enforcement. *See* Cyber-Related Sanctions Regulations, 80 Fed. Reg. 81,752 (Dec. 31, 2015) (to be codified at 31 C.F.R. pt. 578).

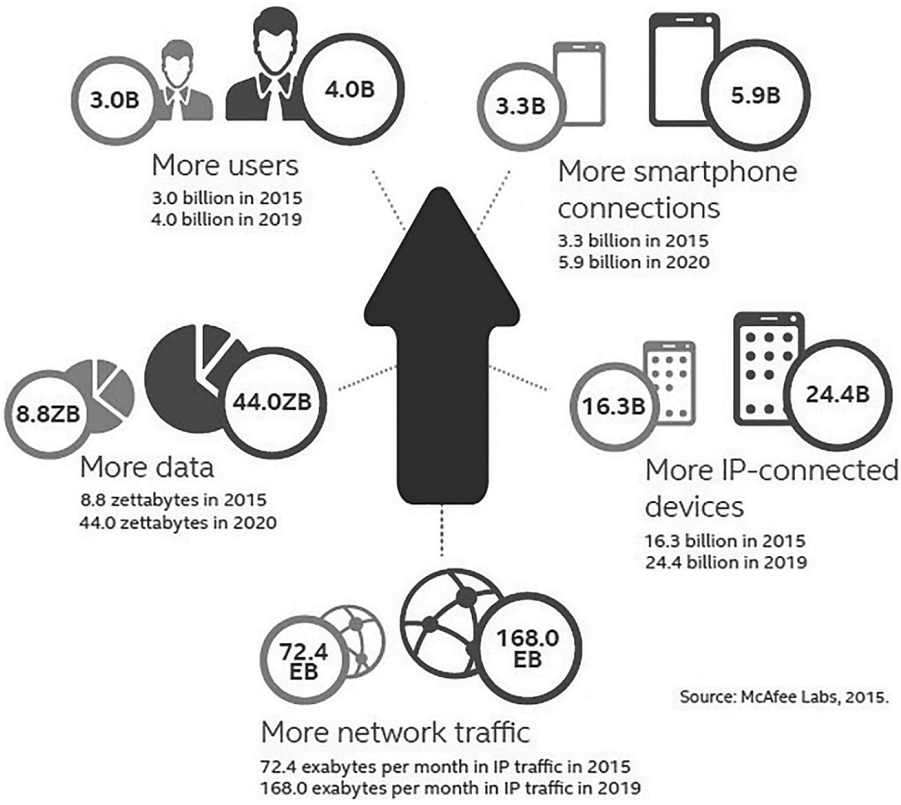
[61] *2016 Threats Predictions*, MCAFEE, at 16 (2016), http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf [https://perma.cc/9QEM-VV4D].

[62] Lim, *supra* note 52, at 83.

[63] *2016 Threats Predictions*, *supra* note 61, at 7–8.

[64] *Id.* at 7. The "Growing Cyberattack Surface" figure, while its author, McAfee Labs, does not explicitly state, is assumed to be demonstrating worldwide data and usage growth. This figure also mentions two uncommon (to the average technology user) units of digital information storage: "exabytes" and "zettabytes." One exabyte (EB) is equal to approximately 1 billion gigabytes (GB) of data, and one zettabyte (ZB) is equal to approximately 1 trillion gigabytes. *See* Charles Arthur, *What's a Zettabyte? By 2015, the Internet Will Know, Says Cisco*, THE GUARDIAN (June 29, 2011, 6:20 PM), http://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco [https://perma.cc/ZCT5-J8NL]. To put this in perspective, one exabyte amounts to "36,000 years of HD-TV video" while one zettabyte would be the equivalent of thirty-six million years of HD-TV video. *Id.*

Figure 11
The Growing Cyberattack Surface



III. WHY SHOULD YOU CARE ABOUT CYBERSECURITY?

A. We Are Family: Protecting People, Infrastructure, and Goods

"The actors within the aviation ecosystem have a cohesive interest [in] ensuring . . . cybersecurity[,]"[65] the protection of "efficient [and secure] flow of goods and passengers[,]"[66] and of the aviation infrastructure[67] in which they travel. No matter the

---

[65] The Boeing Company, *supra* note 50, at 14.

[66] Burns, *supra* note 3, at xxv.

[67] In addition to aircraft, the airports themselves require protection because

> Airports are vital national resources. They serve a key role in transportation of people and goods and in regional, national, and international commerce. They are where the nation's aviation system connects with other modes of transportation and where federal responsibility for managing and regulating air traffic operations inter-

role (i.e., federal government, state government, local government, manufacturer, airline, contractor, law firm, employee, customer,[68] attorney, etc.), if you participate in the "aviation ecosystem," then this is your responsibility.

B. Avoiding the "Greatest Illusion"

"The greatest trick the Devil ever pulled was convincing the world he didn't exist."[69] The greatest illusion cybercriminals have created is convincing the world that they only attack large organizations. Symantec™, "a global leader in providing security, storage and systems management solutions,"[70] has reported that, while data breaches have netted cybercriminals hundreds of millions[71] of identities,[72] "the median number of identities stolen . . . [was] 7,000 in 2014. Using the median [is] . . . helpful . . . since it ignores the extreme values caused by the notable . . . [large data breach] . . . events that resulted in the largest numbers of identities' being exposed."[73] In short, in 2014, "[sixty] percent of all targeted attacks struck [were] small- and medium-sized organizations. These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices . . . . This puts not only the businesses, but also their business partners [and clients], at higher risk."[74] Thus, "[c]yber theft, cyber extortion, mobile device loss, misappropriation of confidential business information, and unauthorized

---

> sects with the role of [the private sector], state and local governments.

Guidebook on Best Practices for Airport Cybersecurity, *supra* note 54, at Airport Cooperative Research Program (copyright page).

[68] If customers are going to bring their own electronic devices (BYOD) into the "aviation ecosystem," then they should be responsible for maintaining a reasonable level of cybersecurity on these devices.

[69] The Usual Suspects (Gramercy Pictures 1995).

[70] *See Corporate Fact Sheet*, Symantec (2013), http://www.symantec.com/content/en/ca/about/media/Symantec_Corporate_Fact_Sheet.pdf [https://perma.cc/7DGH-ZEWZ].

[71] According to the Privacy Rights Clearinghouse, 121,544,707 records had been breached in 2015 as of Aug. 25, 2015. *Data Breaches*, Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach/new (last visited Oct. 12, 2017) [https://perma.cc/YH6G-XNZ9].

[72] Top 3 Sectors Breached in 2014 and Number of Identities Exposed: (1) Retail Sector, 205,446,276; (2) Financial Sector, 79,465,597; and (3) Computer Software Sector, 35,068,405. *See Watering Hole Attacks*, *supra* note 58, at 82.

[73] Symantec, Internet Security Threat Report, 19 ISTR 1, 13 (2014), www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf [https://perma.cc/P5G5-6S8M].

[74] *Watering Hole Attacks*, *supra* note 58, at 6.

disclosures of protected information are real and present dangers for organizations of all sizes and across all industries."[75]

C. Maintaining Client Confidences

"Both the fiduciary relationship existing between lawyer and client and the proper functioning of the legal system require the preservation by the lawyer of confidential information of one who has employed or sought to employ the lawyer,"[76] regardless of whether the information is tangible or digital:

> Rule 1.1 of the Model Rules of Professional Conduct admonishes that "a lawyer shall provide competent representation to a client." The rule defines "competent representation" as requiring "the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." . . . And commentary to the rules states that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[77]

This ethical duty also extends to the attorney's use of assistants and third parties.[78] Applying these principals to cybersecurity, there is an ethical duty for attorneys to provide a reasonable

---

[75] Peter Sloan, *The Reasonable Information Security Program*, 21 Rich. J.L. & Tech. 2, 2 (2014), http://jolt.richmond.edu/v21i1/article2.pdf [https://perma.cc/5DXG-CERH].

[76] Tex. Disciplinary Rules Prof'l Conduct R. 1.05 cmt. 1.

[77] Rose L. Romero et al., *Data Privacy Issues*, Essentials of Bus. L. Course 1, 5 (2015) (citations omitted).

[78] For example, Tex. Disciplinary Rules Prof'l Conduct R. 5.03 (Responsibilities Regarding Nonlawyer Assistants) states, in part: "With respect to a non-lawyer employed or retained by or associated with a lawyer . . . a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer . . ." Tex. Disciplinary Rules Prof'l Conduct R. 1.05. Comment 1 provides further clarification on the attorney's ethical duties:

> Lawyers generally employ assistants in their practice . . . . Such assistants act for the lawyer in rendition of the lawyer's professional services. A lawyer should give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product.

Id. at cmt. 1. In Tex. Comm. on Prof'l Ethics, Op. 572 , the issue was whether a lawyer may, without the client's express consent, send client's privileged information to an independent contractor hired by the lawyer to perform services in connection with the client's representation. Tex. Comm. on Prof'l Ethics, Op. 572 (2006). The Ethics Committee concluded that a lawyer may disclose privileged information to an independent contractor "if the lawyer reasonably expects

infrastructure for the protection of their client's confidential information and to use due diligence in the protection of this information when access to it is given to independent contractors.[79]

D. Complying with the Law

Given its reliance upon e-commerce, the aviation industry collects and uses personal information.[80] "Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of . . . [statutorily protected personal] information,"[81] with each jurisdiction[82] having its own provisions for determining the type of information to be protected, how and when notice is to be given, and whether encryption is required.[83]

---

that the confidential character of the information will be respected by the independent contractor." *Id.*

[79] A similar conclusion, but after a different legal analysis, was reached by Jill D. Rhodes & Vincent I Polley, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals 6 (2013).

[80] *See* Matthew Lew et al., *supra* note 4, at 3.

[81] *Security Breach Notification Laws*, Nat'l Conf. of St. Legislatures (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/S2DB-7SGJ].

[82] The reader of this article is strongly encouraged to research and carefully review personal information privacy laws applicable to their area of practice. For general discussion of federal and state personal information privacy laws, see Sloan, *supra* note 75, at 7–25.

[83] For example, Texas is one of the forty-seven states with breach notification laws. Specifically,

> A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Tex. Bus. & Com. Code Ann. § 521.053(b) (West 2009). The State of Texas then broadly defines "sensitive personal information" as:

> (2) "Sensitive personal information" means . . . :
>
> (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and *the items are not encrypted:*
>
> (i) social security number;
>
> (ii) driver's license number or government-issued identification number; or
>
> (iii) account number or credit or debit card number in combination with any required security code, access

E. Minimalizing the Financial Impact of a Data Breach: "An Ounce of Prevention is Worth a Pound of Cure"[84]

In the *2015 Cost of Data Breach Study: United States*,[85] a benchmark research sponsored by IBM and independently conducted by the Ponemon Institute, it was found that forty-nine percent of data breaches involved a malicious or criminal attack, nineteen percent were the result of negligent employees,[86] and thirty-two

---

code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:
(i) the physical or mental health or condition of the individual;
(ii) the provision of health care to the individual; or
(iii) payment for the provision of health care to the individual.

Tex. Bus. & Com. Code Ann. § 521.002 (West 2009) (emphasis added). Lastly, the State of Texas imposes a legal duty on Texas businesses to protect "sensitive personal information":

> Sec. 521.052. Business Duty to Protect Sensitive Personal Information
> A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

Tex. Bus. & Com. Code Ann. § Sec. 521.052 (West 2009).

[84] Benjamin Franklin, Goodreads, https://www.goodreads.com/quotes/247269-an-ounce-of-prevention-is-worth-a-pound-of-cure [https://perma.cc/TPF7-LC47].

[85] *2015 Cost of Data Breach Study: United States*, Pomenon Inst. 1, 8 (2015) [hereinafter *Ponemon U.S. Data Breach*], https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF [https://perma.cc/JQ7H-RAXB].

[86] The *2015 Data Breach Investigations Report*, a study conducted by Verizon™ with contributions from seventy corporate and governmental organizations from around the world, found three main categories of internal error (data breach) incidents:

- 30% of incidents: "D'oh!"—Sensitive information reaching incorrect recipients;
- 17% of incidents: "My bad!"—Publishing nonpublic data to public web servers;
- 12% of incidents: "Oops!"—Insecure disposal of personal and medical data.

Verizon Enterprise Solutions, *2015 Data Breach Investigations Report*, Verizon 1, 49 (2015), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf [https://perma.cc/8CBL-BFB6]. In the *2015 Insider Threat Industry Report* (a collaborative effort of Bitglass™, Dell Software™, Fasoo™, LightCyber™, HEAT Software™, ObserveIT™, Palerra™, RES Software™, Sergeant Laboratories™, SpectorSoft™, Vectra Networks™, and Watchful Software™ in association with the Information Security Community on

percent involved system glitches that included both IT and business process failures. Furthermore, it was determined that every year for the last ten years, the indirect costs of a data breach (i.e., what a business spends on existing internal resources to deal with the data breach) have exceeded the direct cost of a data breach (i.e., what a business spends to minimize the consequences of a data breach).[87] Implementation of a reasonable data security infrastructure[88] can reduce the cost per lost record caused by a data breach by more than thirty percent.[89] The *2015 Cost of Data Breach Study: Impact of Business Continuity Management*[90] found that the implementation of a business plan that identified the cyber risks, threats, and vulnerabilities that could impact the business and then established a framework for building organizational resilience and effective response to the "cyber event" had the following effects:

- 27% reduction in the mean time to identify a data breach;
- 41% reduction in the mean time to contain a data breach;
- 28% decrease in the likelihood of a data breach over the next two years.[91]

LinkedIn™), it was found that "[p]rivileged users, such as managers [, officers, and owners] with access to sensitive information, pose the biggest insider threat . . . . This [was] followed by [current and former] contractors . . . consultants . . . , and . . . employees . . . ." Crowd Research Partners, *Insider Threat: Spotlight Report*, INFO. SEC. REP. 3, 8 (2015), http://crowdresearchpartners.com/portfolio/insider-threat-report/ [https://perma.cc/VLB7-WX9M]. Additionally, this report noted that there was a "rise in insider attacks . . . mostly due to a combination of three factors: insufficient data protection strategies and solutions . . . , the proliferation of sensitive data moving outside the firewall on mobile devices . . . , and lack of employee training and awareness . . . ." *Id.* at 12. Accordingly, a "reasonable information security program" must address and, to the extent possible, provide an effective plan to minimize these internal risks. *Id.* at 3.

[87] *Ponemon U.S. Data Breach*, *supra* note 85, at 14.

[88] This "security infrastructure" would include, but not be limited to, an "incident response plan and team in place, extensive use of encryption, . . . employee training," and business continuity management and IT leadership. *Id.* at 9.

[89] *Id.*

[90] *2015 Cost of Data Breach Study: Impact of Business Continuity Management*, PONEMON INST. 1, 1 (2015) [hereinafter *Ponemon Impact Study*], http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03074usen/SEW03074USEN.PDF [https://perma.cc/YG28-N5GS]. This was another benchmark research sponsored by IBM and independently conducted by the Ponemon Institute. *Id.*

[91] *Id.* at 1.

IV. RECOMMENDED SOLUTIONS: IMPLEMENTATION AND USE OF A RESILIENT CYBERSECURITY INFRASTRUCTURE FRAMEWORK AND COLLABORATIVE SHARING OF CYBERSECURITY INFORMATION

A. A Framework for Improving Critical Infrastructure Cybersecurity

Cybersecurity threats place the "nation's security, economy, and public safety and health at risk."[92] To address these risks, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, on February 12, 2013.[93] This Executive Order required the National Institute of Standards and Technology (NIST) to develop a voluntary cybersecurity framework: "a set of industry standards and best practices to help organizations manage cybersecurity risks."[94] On February 12, 2014, the NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity*.[95] The core of this framework consists of five concurrent and continuous functions which represent the lifecycle of an organization's management of cybersecurity risk: identify, protect, detect, respond, and recover.[96] In the context of the NIST cybersecurity framework, these core elements have the following meaning:

> *Identify*: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities; . . .
> *Protect*: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services; . . .
> *Detect*: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event; . . .
> *Respond*: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event; . . . [and]
> *Recover*: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[97]

---

[92] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, at 1 (U.S. Dep't of Commerce 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/696P-8ZHK].

[93] *Id.*; *see also* Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) ("Improving Critical Infrastructure Cybersecurity").

[94] *Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 92, at 1.

[95] *Id.*

[96] *Id.* at 4.

[97] *Id.* at 8–9.

Similarly, Peter Sloan[98] proposes that an organization develop and implement a "reasonable information security program" in which the entity[99]:

- [I]dentif[ies] the types of information in its possession, custody, or control for which it will establish security safeguards ("Protected Information");
- [A]ssess[es] the anticipated threats, vulnerabilities, and risks to the security of Protected Information;
- [E]stablish[es] and maintain[s] appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of Protected Information;
- [A]ddress[es] the security of Protected Information in its third-party relationships;
- [R]espond[s] to detected breaches of the security of Protected Information; and
- [P]eriodically review[s] and update[s] its policies and controls for the security of Protected Information.[100]

B. Application of a Framework for Improving Critical Infrastructure Cybersecurity to the Aviation Industry

> Introducing new technologies without robust cybersecurity measures in place presents a risk to the [aviation] industry, in light of evolving cyber threats . . . . For this reason, all aviation industry stakeholders must fully understand the risks to their networks and control systems from cyber threats and take steps to close the gaps and potential vulnerabilities . . . .[101]

With these words, the American Institute of Aeronautics and Astronautics (AIAA)[102] issued its *Framework for Aviation Cyber-*

---

[98] Mr. Sloan is an employee with the Information Governance Group, LLC, and a member of The Sedona Conference, Working Group I (Electronic Document Retention and Production) and Working Group XI (Data Security and Privacy Liability). *See Peter Sloan*, Info. Governance Grp., LLC, https://infogovgroup.com/who-we-are/peter-sloan-professional-bio/ [https://perma.cc/BU9G-8LV5]; *see also Peter B. Sloan*, The Sedona Conf., https://thesedonaconference.org/bio/sloan-peter [https://perma.cc/59BA-PUT6].

[99] Sloan, *supra* note 75, at 4–5, 25–92.

[100] *Id.* at 4–5.

[101] *The Connectivity Challenge: Protecting Critical Assets in a Networked World—A Framework for Aviation Cybersecurity*, Am. Inst. of Aeronautics & Astronautics 1, 7 (2013), https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf [https://perma.cc/L7ER-GNQ2].

[102] According to AIAA:

> With more than 30,000 individual members from 88 countries, [it] . . . is the world's largest technical society dedicated to the global

security six months after President Obama issued Executive Order 13636,[103] *Improving Critical Infrastructure Cybersecurity*,[104] but six months before the NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity*.[105] In summary, the AIAA's *Framework for Aviation Cybersecurity* requested the aviation industry to adopt the following cybersecurity framework:

- Establish common cyber standards for aviation systems;
- Ensure a cybersecurity culture;
- Understand the threat;
- Understand the risk;
- Communicate the threats and assure situational awareness;
- Provide incident response;
- Strengthen the defensive system;
- Define design principles;
- Define operational principles;
- Conduct necessary research and development; and
- Ensure that government and industry work together.[106]

Notwithstanding the efforts of AIAA, the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* has been more recently applied to the aviation industry in the United States.[107] For example, the Transportation Research Board (TRB), one of the major divisions of the National Research Council and a part of the National Academy of Sciences, published in 2015 its

---

> aerospace profession. Created in 1963 by the merger of the two great aerospace societies of the day, the American Rocket Society (founded in 1930 as the American Interplanetary Society), and the Institute of the Aerospace Sciences (established in 1933 as the Institute of the Aeronautical Sciences).

About AIAA, AM. INST. OF AERONAUTICS & ASTRONAUTICS, http://www.aiaa.org/AboutAIAA/ [https://perma.cc/9TJP-5A9E].

[103] Prior to issuance of Exec. Order No. 13636, in 2012, the Boeing Company published in its online industry magazine an "information security strategy" designed "to protect an airline's information and technology assets." Robert Rencher et al., *Securing Airline Information on the Ground and in the Air*, QTR_03 AERO 1, 25–28 (2012), http://www.boeing.com/commercial/aeromagazine/articles/2012_q3/5/ [https://perma.cc/Z4A2-539V]. "Boeing's holistic cyber security aviation framework is designed to address both airborne and ground-based cyber threats. The aviation industry benefits from the availability of a cyber security information resource that provides a protected venue for exchanging sensitive security information." *Id.* at 28. After the issuance of Exc. Order No. 13636, Boeing issued a written response applauding the Order and providing NIST with their vision of how the new cybersecurity framework should be designed. THE BOEING COMPANY, *supra* note 50, at 4–113.

[104] *See* Exec. Order No. 13636, *supra* note 93.

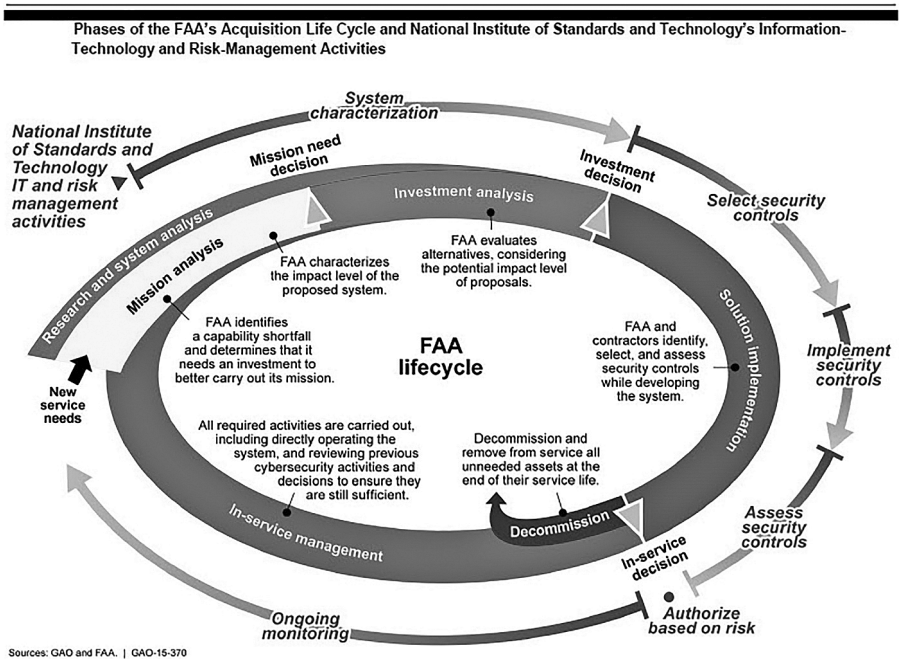
[105] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 92.

[106] *The Connectivity Challenge*, *supra* note 101, at 5–6, 9.

[107] *Guidebook on Best Practices for Airport Cybersecurity*, *supra* note 54, at 10–14.

Guidebook on Best Practices for Airport Cybersecurity in which the TRB used the NIST's Framework to help it create cybersecurity recommendations for airports.[108] In a related use of an NIST security framework (as shown by the figure below),[109] the FAA has incorporated the NIST's *Risk Management Framework*[110] for federal information systems into its Acquisition Management System (AMS)[111]:

Figure 12



C. A Resilient Cybersecurity Infrastructure Framework

"[W]e need to accept that we will never eliminate all risk,[112] that nothing is permanently safe."[113] Therefore, a cybersecurity

---

[108] *Id.*

[109] GAO-15-370, *supra* note 34, at 26.

[110] *See* Nat'l Inst. of Standards & Tech., *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, at 5–9, (U.S. Dep't of Commerce 2010), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf [https://perma.cc/KME2-ULLF].

[111] This is most likely for the purpose of resolving GAO's finding that the Surveillance and Broadcast Service Subsystem "Did Not Sufficiently Assess Key Controls Prior to [program] Deployment." GAO-15-370, *supra* note 34, at 35.

[112] "The reality is that security breaches may be inevitable no matter how diligently an organization safeguards its information." Sloan, *supra* note 75, at 2.

[113] *2016 Threats Predictions*, *supra* note 61, at 9.

infrastructure framework must be designed to enable an organization to rapidly recover from the unexpected. In other words, the framework must be resilient: "The term 'resilience' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[114] Consequently, as "part of Executive Order 13636 [*Improving Critical Infrastructure Cybersecurity*], the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community or C^3 (C Cubed) Voluntary Program."[115] The purpose of this program is to assist the critical infrastructure sectors[116] and organizations in their use of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.[117] One element of the "C Cubed" program is the option for an organization to participate in a Cyber Resilience Review (CRR)[118]: "The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational *resilience* and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals."[119] By utilizing the assessment generated by the CRR, an organization

---

[114] Press Release, The White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013) [hereinafter (PPD)-21], https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/F6J7-VKZL].

[115] U.S. Comput. Emergency Readiness Team, *Critical Infrastructure Cyber Community Volunteer Program*, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/ccubedvp (last visited Oct. 13, 2017) [https://perma.cc/JCW4-5BTT].

[116] In (PPD)-21, the President identified sixteen critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. (PPD)-21, *supra* note 114. For more details on each sector, see *Critical Infrastructure Sectors*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-sectors (last visited Oct. 13, 2017) [https://perma.cc/5E3C-TF4D].

[117] *Critical Infrastructure Cyber Community Volunteer Program*, *supra* note 115.

[118] U.S. Comput. Emergency Readiness Team, *Assessments: Cyber Resilience Review (CRR)*, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/ccubedvp/self-service-crr (last visited Oct. 13, 2017) [https://perma.cc/QFM4-6D4E].

[119] *Id.* (emphasis added); *see also Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks*, U.S. DEP'T OF HOMELAND SEC. (Feb. 2016), https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-ramework-crosswalk.pdf [https://perma.cc/R3GN-4N26].

has the ability to evaluate the resiliency of its cybersecurity infrastructure framework before a critical event occurs.

D. Ensuring that Government and Industry Work Together[120]: Collaborative Sharing of Cybersecurity Information Under the Cybersecurity Act of 2015

On December 18, 2015, H.R. 2029, the Cybersecurity Act of 2015, was signed into law as part of Consolidated Appropriations Act of 2016[121]: The Cybersecurity Act of 2015 "encourages private companies to voluntarily share information[122] about cyber threats with each other as well as the government. Firms that participate in the information sharing will receive liability protection."[123] By enabling the collaborative sharing of cyber-

---

[120] *See The Connectivity Challenge*, *supra* note 101, at 6, 9.

[121] *See* Consolidated Appropriations Act 2016, Cybersecurity Act of 2015, Pub. L. No. 113-114, 129 Stat. 2242 (2015).

> The Cybersecurity Act of 2015 represents a compromise between the House and Senate intelligence committees and the House Homeland Security Committee. It includes various components of three separate information sharing bills: H.R. 1560 and H.R. 1731, passed by the House in [ ] 2015, and S. 754, passed by the Senate in October [of] 2015.

Rita Tehan, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, Cong. Research Serv. 1, 3 (last modified June 23, 2017), https://www.fas.org/sgp/crs/misc/R43317.pdf [https://perma.cc/N2XS-DYAH]. This analysis comes from a report written by the Congressional Research Service (CRS). "[CRS] works exclusively for the United States Congress, providing policy and legal analysis to committees and Members of both the House and Senate, regardless of party affiliation." *Congressional Research Centers*, Lib. of Cong., https://www.loc.gov/crsinfo/ (last visited Oct. 13, 2017) [https://perma.cc/4HDV-2BXP].

[122] Prior to this enactment, on February 13, 2015, the President issued Executive Order Number 13691 (titled *Promoting Private Sector Cybersecurity Information Sharing*) to enhance the sharing of cybersecurity information. Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb 20, 2015).

[123] Tehan, *supra* note 121. Specifically, with regard to the federal government's sharing of cyber threat information, this Act states:

> Sec. 102. DEFINITIONS
> (14) NON-FEDERAL ENTITY.—
> (A) In General.—Except as otherwise provided in this paragraph, the term "non-Federal entity" means *any private entity*, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).
> (B) Inclusions.—The term "non-Federal entity" includes a government agency or department of the District of Columbia. . . .
> (C) Exclusion.—The term "non-Federal entity" does not include a foreign power . . .
> Sec. 103. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

security information between government and the private sector, the Cybersecurity Act of 2015 enhances aviation's (and the country's) ability to fight cyber-attacks:

> The optimal approach to securing aviation defense is for the government and industry to collaborate, sharing threat data and sensitive information. Providing a forum where industry stakeholders can receive and share threat data would increase the speed at which threats can be mitigated across the aviation system. This gives all parties involved an opportunity to share effective countermeasures against specific attacks and adversaries.[124]

> (a) In General.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—
> (2) the *timely sharing with* relevant Federal entities and *non-Federal entities* of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level;
> (3) the *timely sharing with* relevant Federal entities and *non-Federal entities*, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;
> (4) the *timely sharing with* Federal entities and *non-Federal entities*, if appropriate, of information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats.

Consolidated Appropriations Act 2016, *supra* note 121, at §§ 102(14), 103(2)–(4) (emphasis added). With regard to private sector cyber-related information shared with the federal government, Section 105 (d)(1) states that providing such information "shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection." *Id.* at § 105(d)(1). Section 104(e)(1) of the Act also provides an antitrust exemption: "It shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide cyber [information] . . . for cybersecurity purposes under this [Act]." *Id.* at §104(e)(1).

[124] *The Connectivity Challenge*, *supra* note 101, at 12.

IV. CONCLUSION

If "eternal vigilance is the price of liberty,"[125] then without constant vigilance cybersecurity is just an illusion of the moment.[126]

"The importance of the aviation industry to the nation's economy cannot be understated. The growth rate of civil aviation has outpaced the overall growth of the U.S. national economy."[127] As a result of this increased growth and the never-ending dependence upon technology, "[cybersecurity] threats to civil aviation operations have become more sophisticated and challenging to deal with."[128] While cybersecurity improvements have been made to the nation's aviation systems,[129] many more security enhancements are needed.[130] In the final analysis, cybersecurity is more than just "implementing a checklist of requirements—cybersecurity is managing cyber risks[131] to an ongoing and acceptable level,"[132] with the ability to rapidly recover from the unexpected.[133] A resilient NIST cybersecurity framework provides a scalable method of accomplishing this task. Notwithstanding, given the ever-changing landscape of cyber threats,[134] more is required: cybersecurity collaboration[135] and constant vigilance.

---

[125] This quote is generally attributed to Thomas Jefferson. *But see Eternal Vigilance is the Price of Liberty*, THIS DAY IN QUOTES (Jan. 28, 2015), www.thisdayinquotes.com/2011/01/eternal-vigilance-is-price-of-liberty.html [https://perma.cc/TYD8-F634].

[126] *See* Hyattye O. Simmons, *Cyber Security and Data Privacy*, 23 TEX. MINORITY COUNS. PROGRAM 1, 1 (2015).

[127] *See* Matthew Lew et al., *supra* note 4, at 1.

[128] Lim, *supra* at note 52, at 81.

[129] *See* GAO-15-370, *supra* note 34, at 30.

[130] *See id.* at 41; GAO-15-221, *supra* note 7, at 31–32; *see generally* REP. FI-2016-001, *supra* note 7.

[131] Ethical and statutory duties, together with best business practices, require that the attorney be able to understand, analyze, evaluate, design, and create a reasonable cyber-security framework for the protection of their clients.

[132] C3 Voluntary Program, U.S. DEP'T OF HOMELAND SEC. (Mar. 2015), https://www.us-cert.gov/sites/default/files/c3vp/smb/CCubedVP_Outreach_and_Messaging_Kit_SMB.pdf (citing *Cyber Risk Management Primer for CEOs of Small & Mid-size Businesses* page) [https://perma.cc/EWV6-U6M8].

[133] *See* (PPD)-21, *supra* note 114.

[134] *See 2016 Threats Protections*, *supra* note 61; *McAfee Threats Report*, *supra* note 56.

[135] Consolidated Appropriations Act 2016, Cybersecurity Act of 2015, Pub. L. No. 113-114, 129 Stat. 2242 (2015).