International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 07 July 2022

DOI: 10.47191/ijsshr/v5-i7-18, Impact factor- 5.871

Page No: 2906-2913

The Federal Acquisition Supply Chain Act, the Solarwinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack

Donald L. Buresh, Ph.D., Esq.

Morgan State University

ABSTRACT: This essay explores the Federal Acquisition Supply Chain Act (FASCA) and the difference it would have made had it been a law during the SolarWinds cyber-attack. The Act is examined from a critical perspective to see what effect it would have had if it had existed when the attack occurred. The SolarWinds cyber attack is then discussed in some detail. In deciding what would have happened if the FASCA was a law at the time of the attack, the events are presumed to be the same as what took place. It was at the time when the cyber-attack information reached the Federal Acquisition Security Council (FASC) that the incident would likely have changed. The paper argues that there would be delays in the actions of the FASC due to the complexity of the bureaucracy involved. The article concludes that the projected outcome would differ from the actual outcome because the cyber-attack would have been handled administratively rather than legislatively in the proposed outcome. This difference may or may not have fostered mitigation of the cyber-attack.

KEYWORDS: Federal Acquisition Supply Chain Act , Federal Acquisition Security Council ,SolarWinds Cyber-Attack

Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
AR21-039A	Starburst
AR21-039B	TearDrop
CISA	Cybersecurity and Infrastructure Security Agency
Commerce	Department of Commerce
DHS	Department of Homeland Security
DNSA-CET	Deputy National Security Adviser for Cyber and Emerging Technology
DoD	Department of Defense
DoJ	Department of Justice
FASC	Federal Acquisition Security Council
FASCA	Federal Acquisition Supply Chain Act
FBI	Federal Bureau of Investigation
FIS	Russian Foreign Intelligence Service
GSA	General Services Administration
HSC	Homeland Security Council
ISA	Information Sharing Agency
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
SEC	Securities and Exchange Commission
SolarWinds	SolarWinds Corporation
UCG	Cyber Unified Coordination Group

The Federal Acquisition Supply Chain Act, the Solarwinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack

INTRODUCTION

The solar wind consists of charged electrons, protons, and alpha particles that emanate into the upper atmosphere of the Sun.[1] The heat from the solar wind warms Earth, making it inhabitable. Like solar winds, SolarWinds Corp. (SolarWinds) wanted to be the wind of life for organizations. The company's purpose was to bring life into government agencies and businesses by helping them manage their data. This paper aims to discuss the SolarWinds breach and compare the actual government reaction to what its reaction would have been had the various agencies affected by the breach conformed to the Federal Acquisition Supply Chain Act (FASCA).

The SolarWinds Cyber Incident

SolarWinds began in Tulsa, Oklahoma, co-founded by David and Donald Yonce.[2] [3] The name of the company's product is Orion.[4] The software helps governments and businesses maintain and manage their networks, systems, and information technology infrastructure.[5] The company is headquartered in Austin, Texas, with over 3,300 employees worldwide.[6] [7] SolarWinds was first publicly traded in May 2009.[8] As of December 2020, SolarWinds had about 300,000 customers, including various federal agencies and almost all Fortune 500 companies.[9] Approximately 33,000 public and private customers employed Orion.[10]

The SolarWinds attack began on September 12, 2019.[11] According to Temple-Raston, the malicious code verified whether the computer was running a 32-bit or 64-bit processor.[12] The software returned a 0 or a 1, depending on what was discovered.[13] The purpose of the code was to see if it was possible to modify SolarWinds' application.[14] Once the hackers understood they could engage in a supply chain attack, they began to infiltrate Orion.[15] A supply chain attack is a hacking technique where a cybercriminal places malicious code or components into a trusted software application.[16] The idea behind the SolarWinds attack was to infect a single supplier so that hackers could take over the supplier's distribution system and convert any hardware and software sold into Trojan horses.[17] With the malicious code in place, a hacker could infect many computers as SolarWinds provides its product to its customers.[18]

In February 2020, the hackers put malicious code into Orion, the SolarWinds' production software. In March 2020, SolarWinds distributed signed software patch updates to Orion that possessed the malicious code.[19] In November 2020, FireEye, a cybersecurity professional services firm, stated that it had found malicious code in its systems. On December 12, 2020, FireEye

---

[1] Nola Taylor Redd, *What Is Solar Wind?*, SPACE.COM (May 18, 2018), *available at* https://www.space.com/22215-solar-wind.html.
[2] Lori Hawkins, *SolarWinds Keeps on Growing*, STATESMAN NEWS NETWORK (Undated Dec. 12, 2018), *available at* https://www.statesman.com/business/employment/solarwinds-keeps-growing/JkhMoapafA0qdJvD5MFILM/.
[3] Liana B. Baker, Greg Roumeliotis, *SolarWinds Confirms It Is Exploring Strategic Alternatives*, REUTERS (Oct. 9, 2015), *available at* https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009.
[4] Saheed Oladimeji, *SolarWinds Hack Explained: Everything You Need to Know*, TECHTARGET (Jun. 16, 2021), *available at* https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.
[5] Id.
[6] Bloomberg Staff, *SolarWinds, Corp.*, BLOOMBERG (n.d.), *available at* https://www.bloomberg.com/profile/company/0OI:GR.
[7] Treva Lind, *SolarWinds blows into Post Falls*, SPOKANE JOURNAL OF BUSINESS (Sep. 22, 2011), *available at* https://www.spokanejournal.com/local-news/solarwinds-blows-into-post-falls/.
[8] Michael Novinson, *$286M Of SolarWinds Stock Sold Before CEO, Hack Disclosures*, THE CHANNEL CO.: CRN (Dec. 16, 2020), *available at* https://www.crn.com/news/security/-286m-of-solarwinds-stock-sold-before-ceo-hack-disclosures.
[9] Catalin Cimpanu, *SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack*, ZDNET (Dec. 14, 2020), *available at* https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/.
[10] Id.
[11] Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), *available at* https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[12] Id.
[13] Id.
[14] Id.
[15] Id.
[16] Andy Greenberg, *Hacker Lexicon: What Is a Supply Chain Attack?*, WIRED (May 31, 2021), *available at* https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.
[17] Id.
[18] Id.
[19] Vijay A. D'Souza, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, WATCHBLOG (Apr. 22, 2021), *available at* https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

informed SolarWinds that Orion was infected.[20] On December 13, 2020, FireEye issued a technical analysis of the malicious code in the Orion updates.[21] On December 14, 2020, SolarWinds told the Securities and Exchange Commission about the cyber-attack.[22] On December 15, 2020, Microsoft and its partners redirected and effectively prevented malicious network traffic from arriving at its intended destination address.[23]

The Congressional Response

On December 16, 2020, the National Security Council (NSC) staff invoked the Cyber Unified Coordination Group (UCG) that was made up of the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) that is supported by the National Security Agency (NSA).[24] On December 18, 2020, the CISA discussed the breach with Congress.[25] On December 23, 2020, CrowdStrike, a cybersecurity professional services company, released the CrowdStrike Reporting Tool. It is a software application that can identify cyber risks to the Microsoft Azure Active Directory.[26] The Microsoft Azure Active Directory is a cloud-based identity and management access service that assists employees when accessing internal and external resources.[27] On December 24, 2020, the CISA released Sparrow, a software application used to find malicious activity for Microsoft Azure and the Microsoft Office 365 cloud environments.[28] On December 31, 2020, Microsoft observed and reported on unusual internal company accounts and the viewing of unauthorized source code.[29]

On January 5, 2021, the CUG opined that the malicious code likely came from Russia.[30] However, at the time, President Trump stated that the SolarWinds hack could have originated from China without any evidence being made public.[31] China was previously the source in several high-profile hacks and may have been responsible for the attack.[32] [33]

On January 13, 2021, the Deputy National Security Adviser for Cyber and Emerging Technology (DNSA-CET) was appointed and was held responsible for directing the response to the breach by the federal government.[34] On February 8, 2021, the CISA released the StarBurst (AR21-039A) and TearDrop (AR21-039B) reports, analyzing the Orion malware.[35] On February 17, 2021, the DNSA-CET stated that Russians were the likely threat actors, and nine federal agencies were affected.[36] On February 18, 2021, Microsoft reported that the threat actor could not access the company's code repositories.[37]

On February 23, 2021, SolarWinds, Microsoft, CrowdStrike, and FireEye testified before the Senate Intelligence Committee. On February 26, 2021, the House committees on Homeland Security and Oversight and Report held a joint hearing regarding the SolarWinds cyber-attack.[38] On March 10, 2021, the House Committee on Appropriations and the Homeland Security Subcommittee discussed updating the federal response to cybersecurity.[39] On March 18, 2021, the Senate Homeland Security and Governmental Affairs Committee held a similar hearing regarding the cyber-attack.[40] On the same day, the CISA released its Hunt and Incident Response Program, a software tool that permits entities to find indicators of malicious activity.[41] On April 15, 2021, the NSA, CISA, and the FBI opined that the Russian Foreign Intelligence Service (FIS) was the threat actor. Finally, on April 19,

[20] Id.
[21] Id.
[22] Id.
[23] Id.
[24] Id.
[25] Id.
[26] Id.
[27] Justin Hall, Kent Sharkey, Bill Anderson, & Alex Buck, *What is Azure Active Directory?*, MICROSOFT CORP. (Jun. 5, 2020), *available at* https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis.
[28] Vijay A. D'Souza, *supra*, note 18.
[29] Id.
[30] Id.
[31] Saheed Oladimeji, *supra*, note 4.
[32] *See generally*, CSIS Staff, *Significant Cyber Incidents*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (n.d.), *available at* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[33] Dorothy Denning, *How the Chinese Cyberthreat Has Evolved*, SCIENTIFIC AMERICAN (REPRINTED FROM THE CONVERSATION (Oct. 7, 2017), *available at* https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/.
[34] Vijay A. D'Souza, *supra*, note 19.
[35] Id.
[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] Id.
[41] Id.

2021, the NSC staff deactivated the Cyber UGC, noting that the lessons learned will improve the federal government's responses to malicious attacks.[42]

The Response of the Federal Agencies

From the timeline discussed above, the federal government conducted various agency and Congressional meetings discussing the SolarWinds attack and what could be done to defend against a future attack. One reason why the SolarWinds attack was noteworthy is that, according to CrowdStrike, the average *dwell time* in 2019 was 95 days or just over three months. In the SolarWinds attack, more than fourteen months passed before the attack was discovered.[43] The dwell time is the difference between when an attack is found and when an attacker initially gains access to a system.[44]

In responding to the attack, the early activities of the federal government included: (1) imposing new sanctions against Russian organizations; (2) ascribing the breach to the Russian FIS; and (3) distributing several interagency reports that highlighted technical information about the tools and methods employed by the Russian hackers (i.e., an NSA-CISA-FBI advisory and the CISA Malware Analysis Report).[45] The intelligence community designated the SolarWinds attack as an espionage campaign. The federal government stated that cyber-espionage campaigns should not attack private-sector computer systems because of the million in mitigation costs that threaten public safety.[46] The issue is that the federal government and its private contractors are so interlocked that cyber-attacking the federal government necessarily includes cyber-attacking private companies.

The SolarWinds breach is an example of threat actors exploiting cyber supply chain vulnerabilities. Recently, the Commerce Department distributed an interim final rule to fulfill the provisions of Executive Order 13873 on *Securing the Information and Communications Technology and Services (ICTS) Supply Chain*.[47] Based on Executive Order 13873, organizations should anticipate additional supply chain regulation, independent of whether a firm does business with the federal government.[48] [49] Government contractors will likely bear the burden of more federal regulation.[50] The federal government will likely demand baseline security enhancements, including mandatory two-factor authentication and encryption of sensitive data.[51] Two-factor authentication is a two-step process that employs two different authentication factors or methods to identify an individual.[52] By adding a layer of security, two-factor authentication makes it more difficult, but not necessarily impossible, for a cybercriminal to gain unauthorized access to a system.[53]

The Federal Acquisition Supply Chain Act

The Federal Acquisition Supply Chain Act (FASCA) is a comprehensive law where one federal organization coordinates various government agencies' supply chain security efforts.[54] The Act was signed into law on December 21, 2018.[55] To appreciate the value of the law, one must understand what the Act covers. A ***covered article*** is defined to be:

- Information technology as defined in 40 U.S.C. § 11101;
- Telecommunications equipment as defined in 47 U.S.C. § 153;
- The processing of information on a federal or non-federal; information system subject to the requirements Controlled Unclassified Information program or subsequent federal government programs for controlling unclassified information; and

[42] Id.
[43] Saheed Oladimeji, *supra*, note 4.
[44] Id.
[45] Morrison Foerster Staff, *U.S. Government Responds to SolarWinds Hack, Seeks to Establish New Norms for Cyber Espionage*, MORRISON FOERSTER (Apr. 19, 2021), *available at* https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack.html.
[46] Id.
[47] Id.
[48] Id.
[49] Dina Temple-Raston, *Biden Order To Require New Cybersecurity Standards In Response To SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 2021), *available at* https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att.
[50] Morrison Foerster Staff, *supra*, note 58.
[51] Id.
[52] Linda Rosencrance, Peter Loshin, & Michael Cobb, *Two-Factor Authentication (2FA)*, TECHTARGET (Last updated Jul. 2021), *available at* https://searchsecurity.techtarget.com/definition/two-factor-authentication.
[53] Id.
[54] *Federal Acquisition Supply Chain Security Act*, FEDERAL REGISTER (n.d.), *available at* https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.
[55] *Id.*

- Hardware, systems, devices, software, or services that possess embedded or incidental informational technology.[56]

In other words, a covered article is any information technology employed by the federal government. A ***source*** means any non-federal, supplier, or potential supplier of products or services.[57]

The important factors that FASCA uses include:

- Functionality and features of the covered article, including its source of data;
- The user environment where the covered article is installed or used;
- Security, authenticity, and integrity of covered articles and associated supply chains;
- The ability of a source to produce and deliver covered articles;
- Ownership of, control of, or influence over covered articles by a foreign government, parties owned or controlled by a foreign government, or other ties between a source and a foreign government;
- Implications for government missions or assets, national security, homeland security, or critical functions with the employment of the source or covered article;
- Potential or existing threats or vulnerabilities of federal systems, programs, or facilities;
- Capacity of the source or the federal government to mitigate risks;
- Credibility or confidence in available information employed for risk assessment;
- Any transmission of information or data by a covered article to a country outside the United States; and
- Any other information that would factor into a supply chain risk assessment, including any impact on federal agency functions or any information the FASC, an organization created by the FASCA, deems appropriate.[58]

The FASC is an executive branch interagency council that is chaired by a senior-level official from the Office of Management and Budget (OMB).[59] The FASC includes representatives from the General Services Administration (GSA), the Department of Homeland Security (DHS), the ODNI, the Department of Justice (DoJ), the Department of Defense (DoD), and the Department of Commerce (Commerce).[60]

Subpart B of the FASCA designated the Department of Homeland Security (DHS) as the information-sharing agency (ISA) to create and establish a supply chain risk management and information-sharing Task Force under the FASCA.[61] Under the law, the ISA facilitates and provides administrative support to the FASC Task Force, acting as a liaison to the FASC.[62] The purpose of the Task Force is to:

- Describe the ISA and the Task Force that will operate to support the FASC;
- Articulate how federal and non-federal organizations provide supply chain risk information to the FASC, including the handling, protection, and classification of information;
- Enunciate how supply chain risk information is shared under § 1326 of the Act, express recommendations issues by the FASC, and communicate covered procurement actions under § 4713 of the Act;
- Impart information to the FASC and executive agencies about removal orders and covered procurement actions; and
- Report to the FASC Chairperson any other appropriate processes and procedures of the FASC.[63]

Subpart B, § 201.202 of the Act lists the mechanics of submitting mandatory and voluntary information to the FASC and disseminating that information by the FASC.[64]

The Federal Acquisition Security Council

According to subsection 202(d) of FASCA, the FASC was required to generate first an interim rule and then a final rule to fulfill subchapter III of chapter 13 of title 41, U.S. Code.[65] On September 1, 2020, The FASC published the interim rule at 85 F.R. 54263.[66] Under the interim rule, entities were invited to submit comments on or before November 2, 2020.[67] Six organizations

[56] 41 U.S.C. § 201-1.101.
[57] *Id.*
[58] 41 U.S.C. § 201-1.300(b).
[59] *Federal Acquisition Supply Chain Security Act*, *supra*, note 54.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Federal Acquisition Security Council Rule*, FEDERAL REGISTER (Aug. 26, 2021), *available at* https://www.federalregister.gov/documents/2021/08/26/2021-17532/federal-acquisition-security-council-rule.
[66] *Id.*
[67] *Id.*

submitted comments.[68] The final rule addressed these comments along with feedback received from federal agencies.[69] The final rule corrected structural issues in the interim rule.[70]

The projected response under the FASCA is described in detail in Subpart B of the Act.[71] Regarding information sharing (§ 201-1.200 of the Act) by the ISA, paragraph (a) clarified that federal agencies and private organizations should submit information to the FASC by providing it to the ISA.[72] Paragraph (b) stated that the ISA, the FASC Task Force, and associated support personnel are responsible for receiving and disseminating the information on behalf of the FASC.[73] Paragraph (c) specified that the ISA was not responsible for providing physical facilities for the FASC.[74] Paragraph (d) explained the processes and procedures that the FASC implemented.[75] The final rule eliminated paragraph (e) of § 201-1.200 of the Act that required the ISA to identify resource gaps to the FASC.[76]

Under Subpart B, submitting information to the FASC (§ 201-1.201 of the Act), the final rule clarified paragraph (d), ensuring that its provisions only applied to the information provided by federal agencies.[77] There were two provisions in paragraph (d) of the interim rule. Paragraph (e) protected voluntary submission by non-federal entities in the final rule.[78] The second provision of the interim was designated as paragraph (f) in the final rule.[79] According to paragraph (f)(3) of the final rule, the FASC is not obliged to release a recommendation to a non-federal entity unless an exclusion or removal order was issued based on that recommendation and the affected non-federal entity was notified.[80]

The Projected Response Under FASCA

Based on the discussion above, if the FASCA had been in existence at the time of the SolarWinds attack, federal agencies would have shared their information about the attack. There would not have been Congressional meetings and reports generating, giving federal agencies guidance as to how to proceed. The procedures would have already been in place. The effects of the cyber-attack would have been handled administratively rather than legislatively.

With that said, the existence of the FASCA and the FASC would not have prevented the SolarWinds cyber-attack from occurring. The SolarWinds attack began with a tiny code strip on September 12, 2019.[81] There is nothing that the FASC could have done, or the existence of the FASCA could have prevented that would have avoided the code that checked whether the computer was running a 32-bit or 64-bit processor from being inserted into the SolarWinds software. Neither the FASCA nor the FASC could have stopped the infected software patch to Orion from being propagated to SolarWinds' client base. The FASC would not have assisted FireEye on December 13, 2020, when it informed SolarWinds of the malicious software in the Orion update. Finally, the presence of the FASC would not have aided SolarWinds when it informed the Securities and Exchange Commission (SEC) of the cyber-attack. The SEC is an independent agency of the federal government that was created in the aftermath of the Wall Street Crash of 1929.[82] The primary purpose of the SEC is to enforce the law against market manipulation.[83]

The critical issue is that the SEC is an independent federal government agency. The SEC is not part of the FASC. The FASC would likely not get involved once it was informed of the cyber-attack. Recall that on December 16, 2020, the NSC staff triggered the UCG that consisted of CISA, the FBI, and the ODNI that the NSA supports.[84] The CISA reports to the DHS, the FBI is part of the DoJ, and the ODNI is a principal advisor to the President, the NSC, and the Homeland Security Council (HSC) for intelligence matters. Based on the levels of bureaucracy highlighted in the previous paragraph, it is evident that there may be significant administrative delays in conveying information about the cyber-attack to the FASC. Simply stated, there are many bureaucratic levels for the information to traverse. There is a distinct possibility that at any given level, and for any relevant federal

[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] Dina Temple-Raston, *supra*, note 11.
[82] Investor.gov Staff, *The Laws That Govern the Securities Industry*, SECURITIES AND EXCHANGE COMMISSION (n.d.), available at https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry.
[83] *Id.*
[84] Vijay A. D'Souza, *supra*, note 19.

agency, the flow of information could crawl forward or even come to a standstill. This would be an unfortunate circumstance, but a situation that could likely occur.

The other way the FASC could receive information about the cyber-attack is via the private sector. On December 13, 2020, FireEye issued a technical analysis of the malicious software contained in the Orion patches.[85] On December 15, 2020, Microsoft and its partners redirected and prevented malicious network traffic from infecting its intended destination address.[86] FireEye, Microsoft, or both companies independently or jointly could have informed the FASC of the cyber-attack. Finally, SolarWinds could have updated the FASC about the attack on its initiative.

Once the FASC had learned of the attack, it could have administratively disseminated the information to its membership. However, going down the bureaucratic hierarchy may be just as byzantine as navigating up the bureaucratic maze. In other words, there may be delays that a federal agency experiences when receiving information from FASC. Also, different federal agencies may receive cyber-attack information at different rates of speed. There is also a possibility that the mainstream and alternative media would report the SolarWinds cyber-attack. If this sequence of events happens, federal agencies could gather the information from the press, thereby making the information flow from FASC communication channels unnecessary.

CONCLUSION

As can be readily seen, many possibilities could happen even if the FASCA and the FASC existed when the SolarWinds cyber-attack occurred. FASC would suffer significant recognition lags due to the bureaucratic hierarchy. The implementation lag could also be significant, as FASC organizations may insist on implementing solutions to the cyber-attack based on their peculiar or unique missions or constraints. Finally, the action lags could be substantially diverse depending on their mitigation plans and performance nuances.

There is no easy answer here. The existence of additional layers of bureaucracy when analyzing the FASC from a critical perspective seemingly ensures that delays in recognition, implementation, and action will come to pass. The issue is the balance between flexibility in decentralization and the rigidity due to bureaucratic machinations. There is no royal road to success. Although pundits may extol the virtues of the FASCA and the FASC, it may turn out that cybersecurity supply chain issues are hard to crack, where things are not as easy as they seem. The FASCA was signed into law on December 21, 2018.[87] It is a young law. Time will tell how effective it is and will be.

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: Not applicable.

REFERENCES

1) Nola Taylor Redd, What Is Solar Wind?, SPACE.COM (May 18, 2018), available at https://www.space.com/22215-solar-wind.html.
2) Lori Hawkins, SolarWinds Keeps on Growing, STATESMAN NEWS NETWORK (Undated Dec. 12, 2018), available at https://www.statesman.com/business/employment/solarwinds-keeps-growing/JkhMoapafA0qdJvD5MFILM/.
3) Liana B. Baker, Greg Roumeliotis, SolarWinds Confirms It Is Exploring Strategic Alternatives, REUTERS (Oct. 9, 2015), available at https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009.
4) Saheed Oladimeji, SolarWinds Hack Explained: Everything You Need to Know, TECHTARGET (Jun. 16, 2021), available at https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.
5) Bloomberg Staff, SolarWinds, Corp., BLOOMBERG (n.d.), available at https://www.bloomberg.com/profile/company/0OI:GR.
6) Treva Lind, SolarWinds blows into Post Falls, SPOKANE JOURNAL OF BUSINESS (Sep. 22, 2011), available at https://www.spokanejournal.com/local-news/solarwinds-blows-into-post-falls/.

[85] *Id.*
[86] *Id.*
[87] *Federal Acquisition Supply Chain Security Act*, *supra*, note 54.

7) Michael Novinson, $286M Of SolarWinds Stock Sold Before CEO, Hack Disclosures, THE CHANNEL CO.: CRN (Dec. 16, 2020), available at https://www.crn.com/news/security/-286m-of-solarwinds-stock-sold-before-ceo-hack-disclosures.
8) Catalin Cimpanu, SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack, ZDNET (Dec. 14, 2020), available at https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/.
9) Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Attack, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), available at https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
10) Andy Greenberg, Hacker Lexicon: What Is a Supply Chain Attack?, WIRED (May 31, 2021), available at https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.
11) Vijay A. D'Souza, SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic), WATCHBLOG (Apr. 22, 2021), available at https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
12) Justin Hall, Kent Sharkey, Bill Anderson, & Alex Buck, What is Azure Active Directory?, MICROSOFT CORP. (Jun. 5, 2020), available at https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis.
13) Vijay A. D'Souza, supra, note 18.
14) Saheed Oladimeji, supra, note 4.
15) See generally, CSIS Staff, Significant Cyber Incidents, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (n.d.), available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
16) Dorothy Denning, How the Chinese Cyberthreat Has Evolved, SCIENTIFIC AMERICAN (REPRINTED FROM THE CONVERSATION (Oct. 7, 2017), available at https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/.
17) Vijay A. D'Souza, supra, note 19.
18) Saheed Oladimeji, supra, note 4.
19) Morrison Foerster Staff, U.S. Government Responds to SolarWinds Hack, Seeks to Establish New Norms for Cyber Espionage, MORRISON FOERSTER (Apr. 19, 2021), available at https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack.html.
20) Dina Temple-Raston, Biden Order To Require New Cybersecurity Standards In Response To SolarWinds Attack, NATIONAL PUBLIC RADIO (NPR) (Apr. 2021), available at https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att.
21) Morrison Foerster Staff, supra, note 58.
22) Linda Rosencrance, Peter Loshin, & Michael Cobb, Two-Factor Authentication (2FA), TECHTARGET (Last updated Jul. 2021), available at https://searchsecurity.techtarget.com/definition/two-factor-authentication.
23) Federal Acquisition Supply Chain Security Act, FEDERAL REGISTER (n.d.), available at https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.
24) 41 U.S.C. § 201-1.101.
25) 41 U.S.C. § 201-1.300(b).
26) Federal Acquisition Supply Chain Security Act, supra, note 54.
27) Federal Acquisition Security Council Rule, FEDERAL REGISTER (Aug. 26, 2021), available at https://www.federalregister.gov/documents/2021/08/26/2021-17532/federal-acquisition-security-council-rule.
28) Dina Temple-Raston, supra, note 11.
29) Investor.gov Staff, The Laws That Govern the Securities Industry, SECURITIES AND EXCHANGE COMMISSION (n.d.), available at https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry.
30) Vijay A. D'Souza, supra, note 19.
31) Federal Acquisition Supply Chain Security Act, supra, note 54.