Science and Technology Law Review

Volume 22 | Number 2 Article 3

2019

The Case for DHS to Classify the Internet of Things as Critical Infrastructure in the United States

Jessica G. Martz
jmartz2@masonlive.gmu.edu

The Case for DHS to Classify the Internet of Things as Critical Infrastructure in the United States

*Jessica G. Martz, J.D., LL.M.**

> Last year, when my refrigerator broke, the serviceman replaced the computer that controls it. I realized that I had been thinking about the refrigerator backwards: it's not a refrigerator with a computer, it's a computer that keeps food cold.
>
> – Bruce Schneier, Data and Goliath

> Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation's safety, prosperity, and well-being.
>
> – Presidential Policy Directive 21

There is a lot of talk about cybersecurity and critical infrastructure because of recent and growing threats over the last decade. Dams are an example of critical infrastructure in the United States, because they protect nearly half of the United States from being flooded, help irrigate American farmland, and generate electricity for a significant portion of the country.[1] Cybersecurity can impact dams if a malicious actor uses cyberspace to attack the sensors and controls that keep the dam functioning properly.[2] Iranian hackers, for instance, gained control of the floodgates to the small Bowman Avenue Dam located near the border of New York and Connecticut using a cellular modem.[3] The floodgate was automated earlier in the year to help regulate water level changes to prevent floods.[4] Thankfully, the dam was being repaired and was offline at the time of the cyberattack, so nothing happened.[5] Then, in September 2016, a denial of services attack created by

---

* L.L.M. Graduate, Spring 2019, Antonin Scalia Law School, George Mason University. Jessica Martz is also a judge advocate and an active duty Lieutenant Colonel in the United States Marine Corps. She is currently assigned to United States Cyber Command as a legal advisor wtihin the National Security Law Section. The views presented are those of the author and do not necessarily represent the views of the Department of Defense or its Components.

1. *Dams Sector*, U.S. Dep't Homeland Sec., https://www.dhs.gov/cisa/dams-sector (last visited Feb. 1, 2020).
2. *Hydropower Facilities: Vulnerability to Cyber Attacks*, Int'l Water Power & Dam Construction (Mar. 20, 2019), https://www.waterpowermagazine.com/features/featureunder-cyber-attack-7051600/.
3. Michael Chertoff, Exploding Data – Reclaiming Our Cyber Security in the Digital Age 53 (2018).
4. *Id.*
5. *Id.*

malware was launched using a botnet on a security blog website.[6] The Mirai malware allegedly infected 380,000 Internet of Things (IoT) devices by endlessly scanning the Internet, using default usernames and passwords for IoT devices that were susceptible.[7] Mirai caused disruptions in Internet communication traffic for hundreds of thousands of users and endangered the financial health of the victims of the attack because of the access the hackers gained to their personal information.[8] The Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI) recently warned nuclear and energy firms of hackers targeting their industry using "phishing" emails to get into their networks to engage in cyber espionage or create disruptions to the system.[9] These examples illustrate the weaknesses inherent in IoT devices and systems and how much of the American infrastructure relies on the IoT to function.

What exactly makes up the IoT? The DHS defines it as "network-connected devices, systems, and services" which "enable seamless connections among people, networks, and physical services."[10] The problem is that the IoT is becoming omnipresent across the United States without a security plan for the IoT.[11] It is hard to imagine walking down the street, moving through an office space, or sitting on public transportation without seeing several forms of the IoT, ranging from smartphones, smartwatches, or sensors on a bus that communicate to a network telling commuters when the bus will arrive, etc. Experts talk about the potential impact of the IoT as beneficial, but more recently, they raised the potential negative impact the IoT will have on American society because of the lack of security built into these devices.[12] Its potential negative impact will not be solved without action from the private sector and the federal government because one trillion IoT devices (for ex-

6. Lucian Constantin, *Smart Device Malware Behind Record DDoS Attack Is Now Available to All Hackers*, PCWorld (Oct. 3, 2016), https://www.pcworld.com/article/3126362/iot-malware-behind-record-ddos-attack-is-now-available-to-all-hackers.html.

7. *Id.*

8. *Id.*

9. Jim Finkle, *U.S. Warns Businesses of Hacking Campaign Against Nuclear, Energy Firms*, Reuters (June 30, 2017), https://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-businesses-of-hacking-campaign-against-nuclear-energy-firms-idUSKBN19L2Z9.

10. U.S. Dep't Homeland Sec., Strategic Principles for Securing the Internet of Things 2 (2016).

11. *See* John Bandler, Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security 211–12 (2017).

12. *See id.*

ample: smart TVs, scanners, and modems) are expected to be hooked up by the year 2025 across the globe.[13]

Despite all the talk, the federal government seems reluctant to regulate or raise awareness to the risks of the IoT in a meaningful and proactive way. Instead, the government is doing what it typically does when new technologies emerge—it waits and sees what happens, hoping that the private sector figures it out or the market and society forces it to adapt.[14] However, as the growing field of cybersecurity demonstrates, waiting is not the best course of action.[15] There is a lot of hope surrounding the benefits of the IoT. For example, the development of the smart grid should help reduce harmful emissions to the earth.[16] The IoT connected power grids can give every customer the amount of electricity desired without wasting energy.[17] There is no question that the IoT continues to bring the United States health, wealth, convenience, and efficiency, but with the benefits the IoT will bring to the American way of life also come the drawbacks because of bad actors who will exploit the IoT for their gain.[18] For example, malicious actors engaged in a cyberattack on Ukrainian power grids in 2015, leaving parts of the country without power.[19] In 2016, hundreds of thousands of IoT devices were hacked causing disruptions in access to Internet sites.[20] The IoT threatens personal safety and security, as well as the national critical infrastructure.[21] Presently, there are several federal agencies who manage certain aspects of the IoT, but many of these agencies overlap in their efforts.[22] What is needed is a single federal government agency tasked with regulating the IoT.

The first step is to assign this responsibility to the DHS, because it is the best suited for this responsibility based on its structure, resources, and its

13. Jason Corsello, *What the Internet of Things Will Bring to the Workplace*, WIRED, https://www.wired.com/insights/2013/11/what-the-internet-of-things-will-bring-to-the-workplace/ (last visited Feb. 2, 2020).

14. Joshua New, *Government Use of IoT Needs to Catch Up with the Technology*, FEDTECH (Apr. 3, 2018), https://fedtechmagazine.com/article/2018/04/government-use-iot-needs-catch-technology.

15. *Id.*

16. BRUCE SCHNEIER, DATA AND GOLIATH 18, 20 (2015).

17. BANDLER, *supra* note 11, at 211.

18. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-75, TECHNOLOGY ASSESSMENT: INTERNET OF THINGS – STATUS AND IMPLICATIONS OF AN INCREASINGLY CONNECTED WORLD (2017).

19. Finkle, *supra* note 9.

20. TECHNOLOGY ASSESSMENT: INTERNET OF THINGS – STATUS AND IMPLICATIONS OF AN INCREASINGLY CONNECTED WORLD, *supra* note 18.

21. U.S. DEP'T HOMELAND SEC., THE 2014 QUADRENNIAL HOMELAND SECURITY REVIEW 7–8 (2014).

22. *See id.* at 39–40.

mission to lead the efforts to regulate and help the private sector and other federal agencies supervise the IoT. The second step is for the DHS to designate the IoT as critical infrastructure for similar reasons that it recently designated the federal election system as critical infrastructure. Americans do not want bad actors hacking our elections, so it was appropriate to classify the election system as a critical infrastructure. Similarly, we do not want these individuals hacking our refrigerators, electric grids, cars, farming equipment, etc., or impeding our life, liberty, and pursuit of happiness. Federal elections take place typically every couple of years, but the IoT exists on a 24/7 basis. An alternative course of action is to have DHS lead a task force to study the challenges associated with the IoT and make findings and recommendations to the President and Congress. Another option is to have the DHS co-lead as a Sector-Specific Agency (SSA) over the IoT as critical infrastructure.

The current threat posed by the IoT is analogous to the problem that the Bush Administration faced after the terrorist attacks on September 9, 2001 (9/11)—how does the federal government best protect the American people and the American way of life? The DHS was the answer almost twenty years ago.[23] All these years later, they are the lead agency for critical infrastructure, cybersecurity, and protecting the homeland.[24] This Article is a call to action, and the DHS is the best agency to respond based on the precedent set most recently by designating the election system as critical infrastructure. Part I will provide background on the IoT, critical infrastructure, and why this is a DHS issue. Part II will analyze the reasons for and against making the IoT a critical infrastructure in the United States. Finally, Part III will make recommendations, and this article will conclude with the author's preferred recommendation.

I. BACKGROUND

A Government Accountability Office (GAO) study conducted in 2017 warned that the IoT is entrenched in American society in three ways: (1) Americans are becoming more connected to the Internet through personal devices; (2) companies use networks to improve business models and enhance safety in their industry; and (3) more cities and governments connect to cloud devices and use technologies to improve public transportation and other public services.[25] Although the IoT has great benefits, as pointed out in the beginning of this article, there are many security, safety, and privacy risks that come with the benefits. For instance, software updates get pushed to IoT devices (such as smartphones and other personal devices), but most people do not download the patch to their device, making their device vulnerable to

23. *See id.* at 13.

24. *Id.* at 14.

25. TECHNOLOGY ASSESSMENT: INTERNET OF THINGS – STATUS AND IMPLICATIONS OF AN INCREASINGLY CONNECTED WORLD, *supra* note 18.

hacking by malicious actors.[26] This problem is magnified because the IoT increases the number of devices susceptible to attack.[27] The United States is increasingly more dependent on networks that operate properly because the networks control activities that are essential to life, and therefore, according to the DHS, "IoT security is now a matter of homeland security."[28]

At first glance, the IoT may not seem to be a DHS issue. One might think the Department of Commerce (DOC) or the Federal Trade Commission (FTC) is better suited to regulate and manage the unwieldy group of private sector entities that produce and sell the IoT devices and technology. This assumption ignores the notion that malicious acts against IoT devices are a form of terrorism, and that cybersecurity is vital for IoT, as well as for the sixteen sectors classified as critical infrastructure.[29] One of the reasons the DHS was created after 9/11 was because there was no single agency that had the primary responsibility to protect the homeland in the United States.[30] One of the key missions immediately assigned to DHS was to ensure the security and safety of critical infrastructure.[31]

A. Key Players

1. The Department of Homeland Security

Multiple statutes and actions by the President indicate that the DHS is the primary agency responsible for leading the federal government's role in safeguarding critical infrastructure by making the IoT more safe and secure.[32] Examples include the requirement that the Special Assistant to the Secretary of Homeland Security is required to work with the private sector and assist in developing best practices to secure critical infrastructure.[33] There is also a Homeland Security Institute within DHS, and its duties include determining the "vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities."[34] Section 2 of the Homeland Security Act of 2002 defines "terrorism" as an act that "is dangerous to human life or potentially destructive of critical infrastructure or key resources."[35] It seems indisputable that hackers who try to disable dams

26. BANDLER, *supra* note 11, at 212.

27. *Id.*

28. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS, *supra* note 10.

29. *See id.*

30. U.S. DEP'T HOMELAND SEC., PROPOSAL TO CREATE THE DEPARTMENT OF HOMELAND SECURITY 2 (2002).

31. *Id.* at 3.

32. *Id.*

33. Homeland Security Act of 2002, 6 U.S.C. § 112(c) (2018).

34. *Id.* § 192(c)(1).

35. *Id.* § 101(18)(A)(i).

and drown thousands or even millions of people are terrorists. The DHS leverages its law enforcement agencies and interagency partners to bring these terrorists to justice.[36] The DHS has more responsibilities than preventing terrorist attacks.

The Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection is required to "carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure of the United States."[37] He or she is also required to "develop a comprehensive national plan" and "recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government" as well as local government and private sector entities.[38] Additionally, the National Cybersecurity Act of 2014 amended the Homeland Security Act of 2002 by adding the task of creating a Cyber Incident Response Plan to the DHS.[39] This requires the DHS to coordinate with other federal agencies, local governments, and private sector "owners and [operators] of critical infrastructure" to share information and to develop plans that "address cybersecurity risks to critical infrastructure."[40] There is little doubt, based on legislation from Congress since 9/11, that the DHS carries the weight of critical infrastructure on their backs, but they have teammates to assist them.

The DHS is tasked with safeguarding critical infrastructure in the United States by coordinating with the private sector and SSAs.[41] An SSA is defined in the Cybersecurity and Infrastructure Security Agency Act of 2018, and the legislation places the responsibility of "providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment" on these SSAs.[42] SSAs coordinate with local governments, the private sector, and the DHS to protect critical infrastructure.[43] The Cybersecurity and Infrastructure Security Agency Act of 2018 also created the Cyber and Infrastructure Security

36. THE 2014 QUADRENNIAL HOMELAND SECURITY REVIEW, *supra* note 21, at 40.

37. 6 U.S.C. § 121(d)(2) (2018).

38. Homeland Security Act of 2002, Pub. L. No. 107–296 § 201(d), 116 Stat. 2135 (amended by 6 U.S.C. § 121(d)(5)–(6) (2018)).

39. The National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 § 7, 128 STAT. 3070 (codified at 6 U.S.C. § 149 (2014)).

40. *Id.*

41. ERIC A. FISCHER, CONG. RESEARCH SERV., IF10602, CYBERSECURITY: FEDERAL AGENCY ROLES 1 (2017).

42. Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 651(5) (2018).

43. *Id.*

Agency (CISA) within the DHS.[44] CISA will be discussed in greater detail later in this article.

President Obama reaffirmed the DHS as the lead agency to help the private sector safeguard critical infrastructure in Presidential Policy Directive 21 (PPD-21).[45] Since its inception, the DHS has been relied on to coordinate with several agencies and private sector partners on complex issues of national security and making the homeland safer.[46] That is exactly the type of mission capability set required to coordinate across the IoT private sector companies as well as the federal agencies that are tasked with each sector the IoT might fall within.[47] The purpose of the background section of this article is to provide definitions, identify the key players regarding the IoT in the public and private spheres, and discuss the relevant authorities and resources that support the thesis and recommendations of this article. The IoT is a DHS issue, and the DHS has the authority and capabilities to help the private sector, local governments, and other federal agencies meet the demanding task of safeguarding IoT to protect national security.[48]

The election system designation is a recent success in dealing with infrastructure that is vulnerable to hacking and cyber threats.[49] President Obama designated the election system as "critical" in January 2017 as a result of Russian interference with the 2016 national election.[50] Upon the President's designation, the DHS ordered the election infrastructure to be designated as critical infrastructure pursuant to PPD-21 and placed it within the existing Government Facilities Sector as a subsector.[51] This brought the election system across the United States within the critical infrastructure ecosystem. Some viewed the move as federal government overreaching into

44. *Id.* § 652.

45. Joseph Marks, *DHS Designates Election Systems Critical Infrastructure*, NEXTGOV (Jan. 26, 2017), https://www.nextgov.com/cybersecurity/2017/01/dhs-designates-election-systems-critical-infrastructure/134418/.

46. Rick Nelson, *Homeland Security at a Crossroads: Evolving DHS to Meet the Next Generation of Threats*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 1, 2013), https://www.csis.org/analysis/homeland-security-crossroads-evolving-dhs-meet-next-generation-threats.

47. *Id.*

48. U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY STRATEGY 13–14 (2018).

49. *See* Press Release, Dep't of Homeland Sec., Statement by Sec'y Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017).

50. Katie Bo Williams, *DHS Designates Election Systems as "Critical Infrastructure,"* THE HILL (Jan. 6, 2017), https://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure.

51. U.S. DEP'T HOMELAND SEC., FACT SHEET: DESIGNATION OF ELECTION INFRASTRUCTURE AS CRITICAL INFRASTRUCTURE (2017) [hereinafter FACT SHEET].

state and local government business.[52] Critics of this decision alleged this move would allow the Department of Justice and DHS access into polling locations that they would have no legal authority to access otherwise.[53] However, many viewed the move as a way of providing protection and resources to local governments during elections.[54] According to then-DHS Secretary Jeh Johnson, the inclusion of the election system within the critical infrastructure framework gives the election system "all the benefits and protections of critical infrastructure that the U.S. government has to offer."[55] Critical infrastructure sectors have the benefit of access to "classified threat information sharing, opportunities for additional training and various other tools aimed to help both public and private entities."[56] The precedent set by this change is that the President can announce something as critical, and then the DHS can order it as critical infrastructure. This precedent can support the DHS in designating the IoT as critical infrastructure.

2. IoT and the Private Sector

Within the private sector of IoT manufacturers, there is a wide range of the scope of security features companies are willing to provide to their consumers, not to mention updates to those features. Most of the IoT is controlled by the private sector, but the government shares a duty with the private sector to address the IoT security.[57] The IoT is not defined in a statute, but the common consensus is that the IoT encompasses "stand-alone devices"[58]—technology and devices that communicate with the Internet or networks.[59] Incidentally, the term IoT was created a long time ago by a supply chain manager to track parts using radio frequency identification.[60] Some today call the IoT machine-to-machine devices because the machines are

52. Williams, *supra* note 50.

53. Hans A. von Spakovsky, *Why Does DHS Want to Designate Election Booths: Critical Infrastructure?*, THE HERITAGE FOUND. (Aug. 17, 2016), https://www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure.

54. Williams, *supra* note 50.

55. *Id.*

56. *Id.*

57. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS, *supra* note 10, at 4.

58. BANDLER, *supra* note 11, at 64.

59. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS, *supra* note 10, at 1.

60. BANDLER, *supra* note 11, at 211.

communicating with each other.[61] The IoT includes items Americans use every day such as smartphones, computers, refrigerators, coke machines, thermostats, and fitness watches.[62]

3. Other Federal Agency Partners

In 2013, President Obama issued PPD-21 on Critical Infrastructure Security and Resilience.[63] The general purpose of PPD-21 was to showcase the President's expectations of federal agencies in promoting "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[64] PPD-21 established DHS as the lead agency for critical infrastructure security and named other agencies to serve as SSAs for sixteen sectors of critical infrastructure.[65] The other federal agencies tasked by PPD-21 to serve as SSAs for critical infrastructure are the: (1) Department of Defense (DOD) (Defense Industrial Base); (2) Department of Energy (Energy); (3) Department of Treasury (Financial Services); (4) Department of Agriculture (Food and Agriculture); (5) General Services Administration (Government Facilities); (6) Department of Health and Human Services (Food and Agriculture; Healthcare and Public health); (7) Department of Transportation (Transportation Systems); and (8) Environmental Protection Agency (Waste and Wastewater Systems).[66] Some of these agencies co-share the responsibility of their sector with another agency or with the DHS.[67] The President assigned the SSAs the role of using their "institutional knowledge" within their sector to "strengthen the security and resilience of critical infrastructure," serve as the federal expert to the private sector on issues within their sector, and help with incident management.[68] The Secretary of the DHS is tasked with leading the other SSAs, as well as other federal entities to identify threats to critical infrastructure.[69]

---

61. Louise Frenzel, *The Internet of Things and Machine-to-Machine Communications Emerge as Internet Drivers*, NUTS AND VOLTS MAG. (June 2014), https://www.nutsvolts.com/magazine/article/june2014_OpenComm.

62. Corsello, *supra* note 13.

63. Directive on Critical Infrastructure Security and Resilience, 2013 PUB. PAPERS 106–115 (Feb. 12, 2013).

64. *Id.* at 106.

65. *Id.* at 108.

66. *Id.* at 109–10.

67. *See id.*

68. *Id.* at 107.

69. Directive on Critical Infrastructure Security and Resilience, *supra* note 63, at 108.

B. Legal Authority

Presently, no federal legislation exists to regulate the IoT.[70] However, that could change this year, as Congress will attempt to reintroduce the Internet of Things Cybersecurity Improvement Act of 2019 (a rebooted draft of the 2017 version that failed to pass into law).[71] The bill focuses on security standards and gives the National Institute of Standards and Technology (NIST) the task of creating the mandated security standards.[72] The bill will also address "device configuration, identity management, firmware updates, and other categories."[73] Although the legislation will apply to devices sold to the federal government, the hope is that IoT manufacturers will decide to create all of their products in compliance with the NIST standards, thus benefiting individual consumers as well.[74] Legislation is one piece to ringing in the new era of technological innovation but awareness is still a vital component. According to Bruce Schneier, there is currently no financial incentive for manufactures to build security into their products, and so it is time for Congress to protect the American people.[75] Designating the IoT as critical infrastructure can accomplish the task of raising awareness of its importance and vulnerabilities related to the critical infrastructure that relies on it.

II. CRITICAL INFRASTRUCTURE

Critical infrastructure is defined by statute in the USA PATRIOT Act as "systems and assets," regardless of "whether physical or virtual," that are "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[76] As briefly mentioned earlier, there are sixteen sectors of critical infrastructure in the United States. PPD-21 designated the following sectors as critical infrastructure: (1) Chemical; (2) Commercial Facilities; (3) Communications; (4) Critical Manufacturing; (5) Dams; (6) Defense Industrial Base; (7) Emergency Services; (8) Energy; (9) Financial Services; (10) Food and Agriculture; (11) Government Facilities; (12) Healthcare and Public Health; (13) Information Technology; (14) Nuclear Reactors, Materials and Waste;

70. Todd Wilbur, *New Legislation Poised to Make IoT More Secure in 2019*, IoT Evolution (Mar. 26, 2019), https://www.iotevolutionworld.com/iot/articles/441718-new-legislation-poised-make-iot-more-secure-2019.htm.

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

75. Bruce Schneier, *New IoT Security Regulations*, Schneier on Security (Nov. 13, 2018), https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html.

76. USA PATRIOT Act, 42 U.S.C. § 5195c(e) (2017).

(15) Transportation Systems; and (16) Water and Wastewater Systems.[77] Out of the sixteen sectors, the DHS is primarily responsible for eight (Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Emergency Services, Information Technology, and Nuclear Reactors, Materials, and Waste) and jointly responsible for two (Government Facilities and Transportation Systems) with other federal agencies, totaling ten sectors in which the DHS has a leadership role in protecting critical infrastructure.[78] NIST may be the leader for developing standards for manufacturers of the IoT to follow, but the DHS is the one responsible for ensuring that regardless of standards for the IoT,[79] the critical infrastructure of the United States which relies detrimentally on the IoT is secure.[80] It is the DHS that will testify before Congress to explain what went wrong and what lessons were learned if there is a major attack on critical infrastructure in the United States. NIST is not likely to testify.[81]

A. Authority to Identify Critical Infrastructure

PPD-21 gives the Secretary of Homeland Security the authority to "[i]dentify and prioritize critical infrastructure."[82] The Secretary exercised this authority in 2017 to designate the election systems as critical infrastructure, so, arguably, the same could be done for the IoT.[83] PPD-21 also requires the "Secretary of Homeland Security to periodically evaluate the need for and approve changes to critical infrastructure sectors."[84] If the Secretary of Homeland Security wants to make changes to a critical infrastructure sector, the Secretary "shall consult with the Assistant to the President for Homeland Security and Counterterrorism" before making the change.[85] It is unclear from news reports surrounding the designation of the election system as critical infrastructure if the Secretary of the DHS consulted with the Assistant to the President for Homeland Security and Counterterrorism, but this was likely mooted by President Obama's announcement that the election systems are critical.[86] In addition to PPD-21, Congress charged the Director of CISA

77. Directive on Critical Infrastructure Security and Resilience , *supra* note 65, at 114–15.

78. *Id.*

79. Wilbur, *supra* note 70.

80. *See, e.g.*, Directive on Critical Infrastructure Security and Resilience, *supra* note 63.

81. *See generally id.*

82. *Id.* at 108.

83. Williams, *supra* note 50.

84. Directive on Critical Infrastructure Security and Resilience, *supra* note 63, at 114.

85. *Id.*

86. *See, e.g.,* Williams, *supra* note 50.

to "lead cybersecurity and critical infrastructure security programs, operations, and associated policy" on behalf of CISA in the Cybersecurity and Infrastructure Security Act of 2018.[87] CISA is unquestionably the DHS's lead agency to defend critical infrastructure in the United States against malicious cyberattacks.[88]

B. Challenges: Resources, Awareness, and Enforcement

Adding IoT to the critical infrastructure framework within the United States will require additional resources in the form of funding and personnel. One of the responsibilities of SSAs is to make training and funding available to the private sector and local governments who seek out the SSA for their expertise.[89] Classifying the IoT as critical infrastructure will raise awareness of the vulnerabilities in the IoT and how that directly relates to critical infrastructure.[90] This in turn could see the private sector become more willing to seek funding, training, and assistance from SSAs voluntarily. This may become more likely if Congress makes NIST set standards for the IoT manufacturers. The DHS and CISA could also act as a co-SSA with another federal agency over the IoT and therefore mitigate the costs associated with being a single SSA.

Bringing the IoT within the federal critical infrastructure framework goes a long way in raising awareness to the public and private sector that the federal government is concerned about the vulnerabilities inherent in the IoT. However, there are other options that do not include federal government involvement. States could update their existing data breach and privacy laws to require manufacturers of the IoT devices to make their products harder targets for cyberattacks.[91] States can also require the manufacturers provide

87. Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652(c)(1) (2018).

88. *About CISA*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/cisa/about-cisa (last visited May 5, 2019).

89. U.S. DEP'T OF HOMELAND SEC., GOVERNMENT FACILITIES SECTOR-SPECIFIC PLAN 11 (2015).

90. *Infrastructure Security*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/topic/critical-infrastructure-security (last visited Feb. 2, 2020) (stating that one of the main focus areas include facilitating critical infrastructure vulnerability assessments); *see Critical Infrastructure Vulnerability Assessments*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/cisa/critical-infrastructure-vulnerability-assessments (last visited Feb. 2, 2020) (stating that the Department conducts specialized field assessments to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on the nation's critical infrastructure).

91. *See, e.g.*, Nicole Lindsey, *New IoT Security Laws Seek to Protect Consumers from Hacks of Internet-Connected Devices*, CPO MAG. (May 10, 2019), https://www.cpomagazine.com/data-protection/new-iot-security-laws-seek-to-protect-consumers-from-hacks-of-internet-connected-devices/.

notice to their customers about the risks of using their products and how to mitigate those risks.[92] The issue of IoT safety and security could be left to the private sector to resolve.[93] However, the problem with leaving the consumer to contend with the IoT manufacturers on their own is, as Bruce Schneier stated, that there is no financial incentive to fix the problem.[94]

Additionally, there is still the issue of the federal government's reliance on the IoT. What happens when a manufacturer of a certain type of network printer that a government agency uses goes out of business? Who is responsible for updating the software on the printers to prevent them from being hacked and then used to hack into other devices on the network where the printers are connected? These questions have no clear answers but are the ones that seem to be the aim of Congress's current bill on the IoT.[95] Without government regulation and supervision, there are too many drawbacks to leaving things to the private sector and consumers to figure out on their own.

Unfortunately, it will be hard to legislate the IoT to a point where we can all sit back and relax. Even if Congress were to pass legislation tomorrow that required manufacturers to provide regular security updates to their customers, it will still be on the customer to affirmatively apply the updates to keep their device more secure. It seems that the only way to force consumers to update their devices would be to make it a crime to not update a device, which seems very un-American. Perhaps Judge Easterbrook was right when he argued that regulating cyberspace makes as much sense as creating a "law of the horse."[96] The point is that it is difficult to regulate IoT because of the problem of identifying who is doing bad things to the IoT. Unlike using eyewitnesses to catch a thief who robbed a bank, it is very hard to catch a cybercriminal robbing the personal information off someone's Apple Watch, for example, because typically, there are no witnesses or a clear data trail leading to the criminal actor.[97] Lawmakers and scholars have made different arguments for and against regulating the Internet and the IoT for at least a couple of decades. Despite the lack of consensus among experts, there are laws and policies that the DHS can rely on in facing the IoT and critical infrastructure security threat.

In addition to relying on the legal definition of "critical infrastructure" in the Homeland Security Act, the DHS can leverage some existing initiatives to raise awareness to concerns over the security of the IoT and how that

92. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 137 (2014).

93. SCHNEIER, *supra* note 16, at 191.

94. *Id.* at 193.

95. *See* Wilbur, *supra* note 70.

96. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 501 (1999).

97. *See id.* at 511.

relates to national critical infrastructure.[98] This can be done without making the changes to the existing sixteen SSAs. For example, CISA recently issued a document describing the National Critical Functions which are defined as "[t]he functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[99]

There are IoT devices that connects to some components of government and private sector systems that are critical to national security, the economy, and public health or safety. Public transportation is an example of a National Critical Function Set that is very likely connected to an IoT device.[100] Sensors on a bus, for instance, communicate to the personal devices of travelers to tell the travelers when the bus will arrive at its designated stop. A disruption to this system of communication as a result of hackers can cause major disruptions to traffic and the lives of those who rely on the transportation to get where they need to go. Additionally, many Americans walking around with defibrillators in their hearts that function using sensors that connect the person with a network which keeps their heart functioning properly. Similarly, individuals with diabetes benefit from insulin pumps that dispense the correct amount of insulin at the right time into their blood, so they keep their insulin above levels leading to ketoacidosis and possibly death. The government and private sector are increasingly moving to cloud storage servers to reduce their infrastructure and costs to store data for these types of devices. The examples of how the IoT supports the National Critical Functions are endless. CISA can re-approach the same interagency partners and the private sector they engaged with to create this framework and raise the issue of how the IoT fits into these principles.

The biggest drawback to the proposal to have the DHS classify the IoT as critical infrastructure and then designate itself as the lead SSA or co-SSA over the IoT is that it may not be enough to proactively safeguard the IoT from hackers. Classifying something as critical infrastructure makes federal resources available and certainly draws national attention to its importance.[101] However, without an accountability mechanism to deter and bring malicious actors to justice, providing money and resources could be woefully insufficient. However, it could be the catalyst to show that the law needs to catch up with the technology and its vulnerabilities. The FTC and state gov-

98. THE PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., U.S. DEP'T HOMELAND SEC., NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS 4 (2014) [hereinafter NSTAC REPORT].

99. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T HOMELAND SEC., NATIONAL CRITICAL FUNCTIONS: AN EVOLVED LENS FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 1 (2019).

100. *See id.* at 3.

101. *See* Williams, *supra* note 50.

ernments are the only mechanisms that currently have authority to address data security breaches in the United States.[102] Because there is no federal statute that regulates data security or the IoT, the FTC is limited to bringing penalty actions against companies under the Federal Trade Commission Act for failing to create or maintain adequate security standards to protect consumers.[103] However, the FTC's pursuit of these companies for "unfair" or "deceptive acts or practices affecting commerce" have been criticized for aggressively pursuing actions outside of the jurisdiction of the FTC Act.[104] Another enforcement mechanism is state data-breach notification laws. Unfortunately, most of these laws are only triggered when certain types of "personal information" is stolen, such as a person's full name, social security number, or bank account number.[105] These laws fail to address the issue of reliance and vulnerability of critical infrastructure connected to the IoT.

The United States is fortunate that there have not been more attacks on the IoT (like the Mirai attack and the attack on the dam between New York and Connecticut[106]) while the law and policies in the United States catch up to the technology. However, it is likely that time is running out on our luck.

III. RECOMMENDATIONS

A. The DHS Should Designate the Internet of Things as Critical Infrastructure and Serve as SSA or Co-SSA for the Internet of Things

The first recommendation for which this article advocates is that the IoT should be designated as critical infrastructure, and the DHS should be the lead agency responsible for safeguarding the IoT because of how dependent existing critical infrastructure is on the IoT. The IoT is critical infrastructure as defined by the USA PATRIOT Act because it is vital to security of the United States as a result of the public and private sector's reliance on the IoT for an endless list of essential aspects of daily life.[107] Leadership is needed in safeguarding American critical infrastructure, including the IoT, because technology is outpacing safeguards and the law.[108]

The IoT connects devices and machines across each of the SSAs, and, dangerously, each of the SSAs is growing more reliant on devices and systems that fall within the IoT. A good example of this danger is the Stuxnet virus, allegedly planted by the United States with the help of Israel into the

102. *See* Peppet, *supra* note 92, at 136.

103. *See id.*

104. *Id.* at 136–37.

105. *Id.* at 137–38.

106. *See* CHERTOFF, *supra* note 3; *see* Constantin, *supra* note 6.

107. USA PATRIOT Act, 42 U.S.C. § 5195c(e) (2017).

108. *See* Peppet, *supra* note 92, at 133.

Natanz uranium enrichment facility in Iran.[109] The worm was allegedly planted through external hard drives used by unknowing employees of the plant.[110] The virus went undetected from 2009 to 2010 and eventually broke out of the Natanz facility and infected systems across the globe.[111] Its primary goal was to delay the nuclear development of Iran by tricking employees at the plant into believing that everything at the plant was operating normally when, in fact, the virus was causing centrifuges to "spin out of control."[112] If something like this is employed against a power grid, a nuclear power plant, or a dam, the effects could be catastrophic and deadly, which is why the DHS needs to elevate the IoT to critical infrastructure status.

The DHS has the legal authority to designate the IoT a critical infrastructure under PPD-21. The designation process for the election system is an example of DHS's authority to designate systems of national import to the critical infrastructure framework.[113] The IoT meets the definition of "critical infrastructure" found within the USA PATRIOT Act because it is a physical and a virtual system that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[114] It is a vital system because "network-connected technologies"[115] "enable seamless connections among people, networks, and physical services" across all aspects of security, national economic security, and national public health or safety.[116] Water, power, financial systems, and military technologies and networks are all reliant on the IoT for daily operations.[117] Even minor disruptions to these IoT networks and devices could cause major disruptions and endanger the public safety.

This course of action is arguably the most aggressive of all the recommendations, but any harshness from its zeal could be softened if the President called the IoT "critical" in the same way that President Obama classified the election system as "critical."[118] President Trump seems amenable to advanc-

109. Michael B. Kelley, *The Stuxnet Attack on Iran's Nuclear Plant was 'Far More Dangerous' than Previously Thought*, BUS. INSIDER (Nov. 20, 2013), https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

110. *See id.*

111. *See id.*

112. *Id.*

113. *See* Williams, *supra* note 50.

114. USA PATRIOT Act, 42 U.S.C. § 5195c(e) (2017).

115. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS, *supra* note 10, at 2.

116. *Id.*

117. *See id.*

118. *See* Williams, supra note 50.

ing technologies to keep America in the race for Artificial Intelligence and other emerging technologies, so he may not be opposed to such a recommendation coming from the DHS Secretary.[119] Another way to mitigate the criticism that might come from designating the IoT as critical infrastructure is to get buy-ins from the other SSAs and the private sector before making the designation official. Practically, this would take significant time and resources away from the CISA mission by devoting personnel to liaise with the SSAs and private sector.

Another criticism of this approach is that Congress intends to pass the Cybersecurity and Infrastructure Security Act of 2019, and, if successful, the goal of bringing awareness to the security vulnerabilities of the IoT may be mooted by the legislation.[120] NIST seems to be the agency of choice to set standards. Congress could give the FTC jurisdiction to enforce the standards, and then there would be little point in raising the IoT to critical infrastructure status.

The answer to these criticisms is that NIST is made for setting standards for emerging technologies, and DHS's mission is to protect the homeland from cyberattacks and other forms of terrorism. DHS should focus on preventing and responding to attacks on the IoT, because these attacks are likely also attacks on a sector with critical infrastructure. NIST does not prevent and respond to anything.[121] They do not have law enforcement capabilities, but the DHS does.[122]

B. The DHS Should Create Internet of Things Subsectors Within Every Critical Infrastructure That Connects to the Internet of Things

When the election system was designated a critical infrastructure, it did not receive its own sector.[123] Instead, it fell within the Government Facilities sector as a subsector.[124] The same could be done for the IoT and it could either be placed in a single sector such as Information Technology, or it could be made a subsector of any SSA that relies on the IoT for daily operations. The DHS has the authority to designate systems as critical infrastructure, so it has the legal authority to make such a move. If it is preferable to place the IoT as a subsector within a single SSA, it will be challenging deciding which SSA IoT falls within since it could fall under several SSAs. It is arguably less difficult to place the IoT as a subsector across several SSAs,

119. *See* NSTAC Report, *supra* note 98, at 7.

120. *See id.* at 25.

121. *See id.* at 13.

122. *See id.*

123. *See* Fact Sheet, *supra* note 51.

124. *See id.*

because the DHS has relationships with the other SSAs and can coordinate with them to determine which rely on the IoT for daily activities.

Each SSA uses the IoT, and therefore, each are as vulnerable as the device being used within the IoT. This course of action gives the DHS more flexibility and arguably brings less controversy by designating the IoT as a critical infrastructure subsector rather than its own sector. This also allows the IoT to fall in on an existing and well-established sector which brings the benefits of experience and staffs that are accustomed to the SSA system. The downside is the challenge of deciding if a single SSA takes on the IoT or if several SSAs do. A second challenge is determining which SSA or SSAs take on the IoT.

The legal basis for this recommendation is nearly the same as it was for the first recommendation. The DHS has the authority to designate the IoT a critical infrastructure pursuant to the authorities given to the Department under PPD-21. The IoT meets the definition of "critical infrastructure" found within the USA PATRIOT Act because it is a physical and a virtual system that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[125] It is a vital system because "network-connected technologies" "enable seamless connections among people, networks, and physical services," across all aspects of security, national economic security, and national public health or safety.[126]

This course of action is arguably a middle ground between the first recommendation and the next recommendation. It would still be helpful to follow the precedent set by President Obama in 2017 with the election system and have President Trump classify the IoT as "critical."[127] However, this is not required by PPD-21, and the DHS has the authority to add systems of critical infrastructure as long as it consults with the Assistant to the President for Homeland Security and Counterterrorism.[128] Also, as stated under the first recommendation, gaining buy-in from the other SSAs and the private sector before making the designation official would help mitigate any criticisms from the public and across the SSAs.

In terms of practical considerations, a lot more coordination will be required on the part of the DHS and that most likely that would fall in the lap of CISA. More coordination would be required to determine whether to go with IoT as a subsector of one or of many SSAs. This will likely take about the same time to set up as the first recommendation because the first recom-

125. USA PATRIOT Act, 42 U.S.C. § 5195c(e) (2017).

126. Strategic Principles for Securing the Internet of Things, *supra* note 10, at 1.

127. Williams, *supra* note 50.

128. *See* Directive on Critical Infrastructure Security and Resilience, *supra* note 63.

mendation will create a new SSA which will in turn have to come up with its own Sector-Specific plan pursuant to PPD-21.

C. CISA Should Lead an Interagency Task Force Across the SSAs to Create Findings and Recommendations on How to Protect Critical Infrastructure and the Internet of Things

As the chosen leader of the SSAs, the DHS should engage with the other SSAs to form an IoT interagency task force[129] that studies: (1) how reliant the SSAs are on the IoT; (2) what safeguards are currently used to protect against cyberattacks on the IoT that the SSAs use; and (3) what impact an individual consumer's IoT device could have on critical infrastructure if it were hacked (examples: a router at a family residence, printer at a business, or an apple watch being used by a federal employee while at work).

It would be prudent to examine how dependent each SSA is on the IoT before breaking the IoT out either as its own SSA or as a subsector within existing SSAs. The drawback to this recommendation is that the United States is running out of time before bad actors find a way to engage in a major cyberattack on critical infrastructure using the IoT. Studies take time to perform, and this one will take a significant amount of coordination and research across the SSAs and the private sector to get the findings and recommendations that will translate to solutions regarding the next steps in safeguarding American critical infrastructure and their rapidly growing reliance on the IoT.

The Cybersecurity and Infrastructure Security Agency Act of 2018 mandates that the Secretary of the DHS coordinate with the SSAs to create a national plan for securing key resources and critical infrastructure and to recommend measures necessary to protect key resources and critical infrastructure in coordination with SSAs, local governments, and the private sector.[130] This recommendation is arguably permitted by this provision and the DHS can delegate this task to its critical infrastructure expert, CISA.

A similar idea was proposed in 2014 by the National Security Telecommunications Advisory Committee (NSTAC) in a report on the IoT to the President of the United States.[131] The NSTAC recommended that the DHS, DOD, and DOC work together on a task force to identify the risks posed by the IoT and update federal programs to fill gaps in security procedures designed to address the risks posed by the IoT.[132] This recommendation takes from that proposal and modifies it from a DHS, DOD, and DOC task force and moves it to the SSAs, which are experts across more federal agents that are vulnerable as a result of growing reliance on the IoT. Currently, the SSAs

129. *See* NSTAC Report, *supra* note 98, at 24.

130. Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652(e)(1) (2018).

131. *See* NSTAC Report, *supra* note 98, at ES-4.

132. *See id.*

include the: (1) DHS; (2) DOD; (3) Department of Energy; (4) Department of Treasury; (5) Department of Agriculture; (6) Department of Health and Human Services; (7) General Services Administration; (8) Department of Transportation; and (9) Environmental Protection Agency.[133] There is no question that each of these SSAs rely heavily on the secure and safe functioning of the IoT and, therefore, have a vested interest in working together to come up with solutions to improve the security of the IoT. The Secretary of the DHS has the authority to direct these agencies to work with the DHS on this initiative. However, the DHS should leverage the Director of CISA to execute the mission of standing up a task force, because CISA is the component within DHS that is already coordinating with the SSAs on issues regarding critical infrastructure and cybersecurity as part of its daily duties.

IV. CONCLUSION AND PREFERRED RECOMMENDATION

After consideration, the author prefers the second recommendation: the DHS should create IoT subsectors within every critical infrastructure that connects to the IoT. The rationale for advocating for this recommendation over the other two is that the United States may be running out of time before malicious actors figure out a way to send malware to an IoT device that infects thousands of other devices and ultimately compromises American critical infrastructure. For this reason, the third recommendation is the least preferred, because it delays action through studying the problem we already know exists. Further, the first recommendation seems too drastic. The IoT impacts so many different SSAs, it makes more sense to spread the IoT subsector across multiple SSAs so that each will invest in helping other SSAs, other federal and state agencies, as well as the private sector. If one SSA is given the task, it allows the other SSAs to assume that they are off the hook so-to-speak.

Regardless of which, if any, of these recommendations are studied or used, this article calls the DHS to action on leading a federal effort to identify and take steps to mitigate the security risks that the IoT poses. CISA seems well-suited to take on the task of coordinating across federal, state, and local entities as well as the private sector as well as the SSAs, because they do this currently in their role as the lead agency managing cybersecurity and critical infrastructure security.

133. Cybersecurity and Infrastructure Sec. Agency, *Critical Infrastructure Sectors*, U.S. Dep't Homeland Sec., https://www.dhs.gov/cisa/critical-infrastructure-sectors (last visited Feb. 2, 2020).