IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

HUAWEI TECHNOLOGIES USA, INC., &
HUAWEI TECHNOLOGIES CO., LTD.,

Plaintiffs,

v.

UNITED STATES OF AMERICA, *et al.*,

Defendants.

Civil No. 4:19-cv-00159

DEFENDANTS' MOTION TO DISMISS OR,
IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
AND OPPOSITION TO PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

REGULATIONS

LEGISLATIVE MATERIALS

INTRODUCTION

As part of the National Defense Authorization Act ("NDAA") of 2019, Congress enacted Section 889, which restricts federal agencies from procuring, contracting with entities that use, or funding the purchase of certain telecommunications products of Chinese companies that Congress determined pose a substantial threat to U.S. national and informational security. Congress did so based on years of briefings, hearings, and other information-gathering addressing the cyber-threat posed by the Chinese government, including via Chinese technology companies subject to its influence. That record reflects Congress's understanding that our growing dependence on the Internet and Internet-connected technology makes the Nation's critical infrastructure, and Americans' personal and professional information, increasingly vulnerable to threats to our telecommunications systems. It also reflects longstanding and widespread concerns in the legislative and executive branches that two Chinese companies—Huawei Technologies and ZTE Corporation—have been aggressively seeking to expand into the U.S. telecommunications market and are uniquely positioned to be exploited by a foreign government already well-known for perpetrating cyber-attacks and -espionage against U.S. networks. In enacting Section 889, Congress sought to mitigate this potential for exploitation on U.S. networks.

Plaintiffs, Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. ("Huawei"), argue that Section 889 is not a risk-mitigation measure but rather legislative "punishment" prohibited by the Bill of Attainder Clause. *See* Pls.' Mot. for Summ. J. ("Pls.' Mot.") 10-28, ECF 27. In so arguing, Huawei fails to meaningfully address binding Fifth Circuit precedent, *SBC Commc'ns, Inc. v. FCC*, 154 F.3d 226, 233 (5th Cir. 1998), and all but ignores last year's decision in *Kaspersky Lab, Inc. v. DHS*, 909 F.3d 446, 458 (D.C. Cir. 2018), in which the D.C. Circuit rejected a bill of attainder claim nearly identical to Huawei's. In *SBC*, the Fifth Circuit recognized that regulatory restrictions on a company's business activities, similar to those at issue here, do not fall within the historical meaning of legislative

punishment, 154 F.3d at 243, and, importantly, that even statutes that impose historical punishments do not offend the Bill of Attainder Clause if the burdens they impose further "prophylactic" purposes and the legislative record does not contain "'smoking gun' evidence of punitive intent," *id.* at 242-43. That Section 889 furthers Congress's prophylactic purposes is clear: it serves to protect the telecommunications systems of federal agencies, contractors, and grant and loan recipients against Chinese cyber-threats by regulating the extent to which those systems will incorporate telecommunications products that carry substantial risk of exploitation by the Chinese government. A similar purpose motivated the passage of Section 1634 of the 2018 NDAA, which prohibited federal agencies from using the products of a Russian cybersecurity company due to the company's relationship to the Russian government. In light of Section 1634's prophylactic purpose, the D.C. Circuit easily dispensed with the company's bill of attainder claim, all the while considering and rejecting virtually every argument and legal theory that Huawei now advances in support of its claim. *See Kaspersky*, 909 F.3d at 453-64. The handful of "isolated references in [the] congressional debate" on which Huawei relies, *SBC Comm'ns*, 154 F.3d at 243—most of which it quotes out of context—fail to show punitive intent in light of all of the relevant information and do not refute the prophylactic nature of Section 889. Huawei may want to ignore *SBC* and *Kaspersky* given their obvious import for Huawei's attainder claim, but those decisions show that the Bill of Attainder Clause does not preclude Congress from addressing issues of national concern, including cybersecurity, simply because those issues emanate from a specifically identifiable source.

Huawei's attacks on Section 889 as a violation of due process and separation of powers principles fare no better. Huawei's due process argument is based on an erroneous standard—a purported rule against selective legislation—even though the Supreme Court has recognized the legitimacy of statutes that specifically identify and regulate parties or other subject matter. And a nearly identical separation of powers claim, based on the same authorities Huawei cites, was rejected

by the Fifth Circuit in *SBC*, 154 F.3d at 246—a fact Huawei fails to mention in its motion.

In sum, Huawei fails to establish any basis to strike down Section 889. The Court should dismiss this suit or, in the alternative, grant summary judgment to Defendants.

RESPONSE TO PLAINTIFFS' STATEMENT OF THE ISSUES

Defendants note that Plaintiffs overstate the scope of Section 889 and respectfully refer the Court to the text of the statute, in particular § 889(a)-(b), (f)(3), for an accurate statement of its application. Defendants submit the following as the statement of issues properly before the Court:

I. Whether Congress's enactment of Section 889, which prohibits federal agencies from procuring, contracting with entities that use, or funding the procurement of telecommunications equipment and services that pose a significant risk of cyber-exploitation by the Chinese government, violates the U.S. Constitution's prohibition on the passage of bills of attainder.

II. Whether Congress's enactment of Section 889 pursuant to normal legislative processes, and based upon years of briefings, reports, and testimony, comports with the Fifth Amendment to the U.S. Constitution.

III. Whether Congress's enactment of Section 889 comports with Congress's legislative authority under Article I of the U.S. Constitution.

BACKGROUND

As Huawei recognizes, Congress's concern that Huawei could be used by the Chinese government to target U.S. telecommunications networks did not develop overnight. *See* Pls.' Mot. 4-5. Lawmakers and numerous executive branch officials have been raising concerns about Huawei's potential to enable Chinese cyber-activity against U.S. networks for over a decade and have been acting over that time to mitigate the threat. When considered in light of the years'-long analysis and steady stream of governmental actions preceding it, Section 889 represents not only a considered response, but the logical next step, to further Congress's aim of ensuring that China is not given a strategic foothold in the networks of federal agencies, contractors, and grants and loan recipients (hereinafter "grantees") to the detriment of national and informational security at federal expense.

I. CONGRESSIONAL AND REGULATORY ACTIVITY LEADING UP TO THE ENACTMENT OF SECTION 889

A. Congressional and Executive Branch Concerns that Chinese Products on U.S. Networks Could Compromise U.S. National and Informational Security

An early indication of congressional concern with Huawei came in 2010, when a bipartisan group of lawmakers wrote a letter to the Chairman of the Federal Communications Commission ("FCC"), requesting information about the security of U.S. telecommunications networks in light of a proposed deal between Sprint, Cricket, Huawei and ZTE. *See* Compl. ¶ 41, ECF 1 (citing *Congressional Leaders Cite Telecommunications Concerns With Firms That Have Ties With Chinese Government* (Oct. 19, 2010)). In that letter, they observed that Huawei and ZTE were "aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure" and to service U.S. networks. Ex. 2 at 1. They cited a 2005 report from the RAND Corporation and a 2009 report by the Department of Defense ("DoD"), stating that Huawei has "significant ties to the Chinese military," as well as public reporting that both companies have received "billions of dollars in export financing and low- to no-interest 'loans' that needn't be repaid from the Chinese government." *Id.* They expressed concern that this financing would allow Huawei and ZTE to gain considerable market access by pricing out competitors, providing an opportunity for the Chinese government "to manipulate switches, routers, or software embedded in American telecommunications network[s] so that communications can be intercepted, tampered with, or purposely misrouted," thereby "pos[ing] a real threat to our national security." *Id.*; *see also* Chairman Mike Rogers & Ranking Member C.A. Dutch Ruppersberger, House Permanent Select Comm. on Intelligence ("HPSCI" or "the Committee"), 112th Cong., Investigative Rep. on the U.S. Nat'l Sec. Issues Posed by Chinese Telecomms. Cos. Huawei and ZTE, at 14, 27, 29 (2012) ("HPSCI Rep.") (noting China's market-distorting support), Ex. 3.

Around the same time, Congress was receiving reports from the U.S.-China Economic and

Security Review Commission ("U.S.-China Commission")[1] and DoD echoing similar concerns. The U.S.-China Commission reported that "[n]ational security concerns have accompanied the dramatic growth of China's telecom sector" and that "large Chinese companies ... are directly subject to direction by the Chinese Communist Party." Staff of U.S.-China Comm'n, 112th Cong., The Nat'l Sec. Implications of Invs. and Products from the People's Republic of China ("PRC") in the Telecomms. Sector, at 9 (2011) ("2011 USCC Telecomms. Rep."), Ex. 4. It also reported that Huawei was among a category of Chinese companies that, "though claiming to be private, are subject to state influence" and "enjoy favorable government policies that support their development." U.S.-China Comm'n, 112th Cong., 2011 Rep. to Congress, at 47, Ex. 5. DoD likewise conveyed its assessment that Chinese technology companies, including Huawei, "maintain close ties to the [People's Liberation Army]." Office of the Sec'y of Def., Annual Rep. to Congress: Military and Sec. Devs. Involving the PRC, at 42 (2011) ("2011 DoD Annual Rep."), Ex. 6.

In February 2011, the Committee on Foreign Investment in the United States ("CFIUS") issued a recommendation that Huawei voluntarily divest the assets it obtained in a 2010 deal with 3Leaf Systems, a U.S. computer technology firm, due to the national security implications of the transaction. *See* Compl. ¶ 42 (citing Ken Hu, "Huawei Open Letter," *Wall St. J.*, Feb. 5, 2011 (citing CFIUS recommendation)).[2] Huawei complied but also published an open letter denying any reason for security concerns with the company and requesting that the U.S. Government carry out a full

[1] The U.S.-China Commission, established by statute in the 2001 NDAA, Pub. L. No. 106-398, 114 Stat. 1654 (2000), is intended "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China." 22 U.S.C. § 7002(b)(2).

[2] CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the United States to assess their national security implications. *See* 50 U.S. Code § 4565. CFIUS's 2011 action was not the first against Huawei; CFIUS acted in both 2008 and 2010 to prevent Huawei's proposed investments in U.S. network security company 3Com and mobile communications company 2Wire, respectively. *See* 2011 USCC Telecomms. Rep., at 19, 29.

investigation into any concerns it had about Huawei. *Id.* Shortly thereafter, in November 2011, the HPSCI initiated a year-long investigation into "the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States." HPSCI Rep., at iv.

B. HPSCI Recommendations Against Using Huawei Telecommunications Equipment and Services

The Committee's investigation was premised on its concern that Chinese telecommunications companies with suspected ties to the Chinese government could provide a platform for a nation-state already well-known for perpetrating cyber-attacks and -espionage against the United States to conduct its cyber-activities. *See id.* at 2, 7. Such a platform, the Committee explained, could allow China "to exert pressure or control over critical infrastructure on which the country is dependent," such as "power grids or financial networks." *Id.* at 3. It could also give China access to sensitive governmental and proprietary information, including "negotiating or litigation positions," "expensive and time-consuming research and development," and "trade secrets," resulting in an "unfair diplomatic or commercial advantage over the United States." *Id.*

The Committee focused its work on Huawei and ZTE, in particular, because they were "the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States" and thus posed the greatest threat. *Id.* at 8. In the course of its investigation, the Committee identified several characteristics of the two companies that contributed to the security risks associated with using their products. First, the Committee noted that indigenous Chinese firms headquartered in China, like Huawei and ZTE, pose a greater risk of compromise because Chinese intelligence agencies have opportunities to tamper with their products throughout the design and manufacturing process. *Id.* at 3 (observing that during product development, "malicious hardware or software [could be] implant[ed] into critical telecommunications components and systems"). Second, the Committee observed that the risk was further exacerbated in the case of a company, like Huawei, that also offers services managing telecommunications

equipment, because the company's "authorized access" could be exploited "for malicious activity under the guise of legitimate assistance." *Id.* at 3-4 (noting that service providers have access to networks "for everyday updates to software and patches to glitches"). Third, the Committee explained that the companies' efforts to "control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes" could lead to a "lack of market diversity" of suppliers and dependence, thereby posing "a national concern for the United States." *Id.* at 2.

Fourth, the Committee found the security risks associated with Huawei and ZTE particularly concerning because of their histories of suspected ties to the Chinese government, *see id.* at 11, including, in the case of Huawei, reports of a history of financial support, the presence of the Chinese Communist Party Committee within the company, and links to the Chinese military, *id.* at 13-14, 22-23. On this score, the Committee explained that it was unable to make conclusive findings because the companies' responses to the Committee's inquiries were "inadequate and unclear." *Id.* at 12; *see also id.* at 12-13 (explaining that Huawei provided scant "internal documentation substantiating [its] answers" to the Committee's questions, a problem exacerbated by the Chinese government's "apparent control" over the information; "almost no information on the role of [the] Chinese Communist Party Committee within Huawei or specifics about how Huawei interacts in formal channels with the Chinese government"; and no "details of its dealings with the Chinese military or intelligence services"). "[G]iven the companies' repeated failure to answer key questions thoroughly and clearly, or support those answers with credible internal evidence," the Committee concluded that "the national-security concerns about their operations ha[d] not been ameliorated." *Id.* at 10.

The Committee also noted that irrespective of the precise nature of the relationship between Huawei and ZTE and the Chinese government, the companies would nevertheless be required "to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security." *Id.* at 3, 47 n.17 (citing State-Security Law of

the PRC, Article 11 ("Where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual.")). And "[e]ven if the company's leadership refused such a request," the Chinese government could "recruit working-level technicians or managers in the[] companies" to carry out malicious activities. *Id.* at 3; *see also id.* at 2 (Chinese intelligence services "often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data").

The Committee issued its report in October 2012, containing its principal findings and recommendations. In light of the risks the Committee identified with respect to Huawei and ZTE, including the unresolved suspicion about the companies' ties to the Chinese government, and all of the information the Committee considered in the course of its investigation, the Committee concluded that "Huawei and ZTE cannot be trusted to be free of foreign state influence, and thus pose a security threat to the United States and to our systems." *Id.* at 45. It therefore recommended, *inter alia*, that:

- "U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts";
- "[G]overnment contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems"; and
- "Private-sector entities [should] ... consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services," with "U.S. network providers and systems developers [being] strongly encouraged to seek other vendors for their projects." *Id.*

C. Continued Warnings to Congress About the Security Risks Associated with Using Huawei Telecommunications Equipment and Services

In the years following the HPSCI Report, Congress continued to seek out information pertaining to the Chinese cyber-threat, including as to Huawei's and ZTE's role in China's cyber-strategy. Through that legislative fact-finding process, Congress received a multitude of briefings, reports, and testimony echoing the findings and recommendations in the HPSCI Report.

Reports to Congress continued to identify China as among the states posing the "greatest cyber threats to the United States." Daniel R. Coats, Dir. of Nat'l Intelligence ("DNI"), Stmt. for the Record: Worldwide Threat Assessment of the US Intelligence Cmty., at 5 (2018) ("2018 DNI Threat Assessment"), Ex. 7; Daniel R. Coats, DNI, Stmt. for the Record: Worldwide Threat Assessment of the US Intelligence Cmty., at 1 (2017) ("2017 DNI Threat Assessment"), Ex. 8. That threat is heightened by China's strategic insertion of Chinese companies into global telecommunications networks, including in the United States. In a February 2015 Counterintelligence Strategic P'ship Intelligence Note, the Federal Bureau of Investigation ("FBI") reported that "China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure." SPIN: 15-002, at 1 ("2015 FBI Note"), Ex. 9. The U.S.-China Commission similarly stated in its 2017 Annual Report to Congress that China's strategic approach involves domestic companies "achiev[ing] dominant positions in China, and then ... expanding to overseas markets." U.S.-China Comm'n, 115th Cong., 2017 Rep. to Congress, at 165, Ex. 10. That Huawei continued to be one of those companies was well-recognized. As the FBI explained, due to "the expanded use of Huawei" products "in US telecommunications ... networks," "the Chinese Government's potential access to US business communications is dramatically increasing," with China's intelligence services "operating as an advanced persistent threat to U.S. networks." 2015 FBI Note, at 1.

Reports to Congress also explained that China's practice of foreign and economic espionage had continued unabated, frequently targeting the U.S. Government, its contractors, and other providers of information and communications technology. *See* Interos Solutions, Inc., Supply Chain Vulnerabilities from China in U.S. Federal Info. and Commc'ns. Tech., at 27 (2018) ("Interos Rep."), Ex. 11.[3] Indeed, the DNI reported to Congress in 2018 that "[m]ost detected Chinese cyber

[3] The report was "prepared at the request of the [U.S.-China Commission] to support its deliberations." *See id.* at cover page.

operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide." 2018 DNI Threat Assessment, at 6. And given the United States' position as a "global center for research, development, and innovation across multiple high-technology sectors," DNI's National Counterintelligence and Security Center ("NCSC") explained that "[f]ederal research institutions [and] universities" are "regularly targeted by online actors seeking all manner of proprietary information." NCSC, Foreign Econ. Espionage in Cyberspace at 4 (2018) ("NCSC Rep."), Ex. 12.

As the Chinese cyber-threat continued, reports to Congress consistently highlighted that U.S. vulnerabilities were increasing due to the expanded use of, and significant advances in, information and communications technology. *See* James R. Clapper, DNI, Stmt. for the Record: Worldwide Threat Assessment of the US Intelligence Ctmy., at 1-4 (2016) ("2016 DNI Threat Assessment"), Ex. 13; 2017 DNI Threat Assessment, at 1-4; 2018 DNI Threat Assessment, at 5-6. Those reports explained that the 5th Generation of wireless technology, or "5G," promises to increase the speed and responsiveness of mobile communications while the number of Internet-connected devices beyond conventional computers and smartphones is expected to grow exponentially, leading to a veritable "Internet of Things" ("IoT"). *See* 2017 DNI Threat Assessment at 1-4. Among other things, the IoT is expected to integrate cyber technologies into "critical infrastructure in key sectors," meaning that "[c]yber threats pose also an increasing risk to public health, safety, and prosperity." *Id.* at 1; *see also* 2016 DNI Threat Assessment, at 1 (explaining that the incorporation of "[s]mart devices ... into the electric grid, vehicles—including autonomous vehicles—and household appliances ... can threaten data privacy, data integrity, or continuity of services"). At the same time, the inter-connected IoT will include "billions of potentially unsecured" points in our Internet infrastructure, "creat[ing] an incalculably larger exploitation space" for our adversaries. NCSC Report at 4; *see also* Interos Rep. at

v. (estimating that by 2021, there will be 25.1 billion IoT units installed, "decreasing the time required to breach" networks, even while the "time required to detect those breaches is not decreasing").

In light of these persistent threats and increasing vulnerabilities, FBI Director Christopher Wray stated during a 2018 hearing before the Senate Select Committee on Intelligence ("SSCI") that the FBI is "deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks." *Open Hearing on Worldwide Threats Before the SSCI*, 115th Cong., at 64-65 (2018) ("2018 SSCI Hearing"), Ex. 14. Doing so could "provide[] the capacity to exert pressure or control over our telecommunications infrastructure," to "maliciously modify or steal information," or "to conduct undetected espionage." *Id.* Then-NSA Director and Commander of U.S. Army Cyber Command Michael Rogers concurred with Wray, adding that government programs needed "to look long and hard at companies like this." *Id.* at 65.

Numerous officials within the executive branch—representing the intelligence community, law enforcement, and the military—warned Congress against the use of Huawei equipment and services in particular. Then-Deputy Secretary of Defense Robert Work stated during a House Armed Services Committee hearing in September 2015 that the Office of the Secretary of Defense would "absolutely not" use Huawei telecommunications equipment, and then-NSA Director Rogers, explained that such equipment is not used because the supply chain risk is "unacceptable." *Implementing the DoD Cyber Strategy Before the H. Comm. on Armed Servs.*, 114th Cong., at 32 (2015) ("2015 HASC Hearing"), Ex. 15. The DNI, along with the Directors of the FBI, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the NSA, and the CIA, all indicated in February 2018 hearing that they would not use Huawei or ZTE products and would not recommend that others do so either. 2018 SSCI Hearing, at 65. And soon-to-be NSA Director and Commander of U.S. Army Cyber Command Paul Nakasone, likewise testified that he "would not" use any Huawei, China

Unicom, or China Telecom products and "would not" recommend his family or friends do so. *Nomination of Lt. Gen. Paul M. Nakasone, U.S. Army, to be Dir. of the NSA and Chief of the Cent. Sec. Serv.: Hearing Before the SSCI*, 115th Cong. 19 (2018), Ex. 16.

Consistent with these recommendations, on December 12, 2017, Congress enacted a provision as part of the 2018 NDAA that prohibited DoD from procuring, or contracting with entities that use, any Huawei products to carry out its nuclear deterrence or homeland defense missions. *See* Pub. L. No. 115-91, § 1656, 131 Stat. 1283, 1761-62 (2017), ECF 28-1. Then in May 2018, DoD issued a directive, prohibiting exchanges on military bases from continuing to sell Huawei and ZTE devices based on DoD's assessment that they posed an unacceptable risk to DoD's personnel, information, and mission.[4] Later that year, Congress would take the next logical legislative step.

II. SECTION 889 OF THE 2019 NATIONAL DEFENSE AUTHORIZATION ACT

A. Introduction and Consideration of the Precursors to Section 889

Reflecting the longstanding cybersecurity concerns with China and the potential for the Chinese government to influence companies like Huawei and ZTE, in January 2018, Representative Conaway and Senator Cotton introduced the "Defending U.S. Government Communications Act" in the House and Senate, respectively. The bills provided that federal agencies would be prohibited from procuring, or contracting with entities that use, "as a substantial or essential component of any system," the equipment or services of Huawei, ZTE, or an entity the head of a federal agency "reasonably believes" is connected to the PRC. H.R. 4747, 115th Cong. (2018), ECF 28-2; S. 2391, 115th Cong. (2018), ECF 28-3. Both bills contained twelve legislative findings, citing many of the reports and testimony discussed above and reflecting the longstanding and widely-shared concerns

[4] *See* "Exchanges ordered to pull Chinese smartphones over security risks," Stars and Stripes (May 2, 2018), *available at* https://www.stripes.com/news/exchanges-ordered-to-pull-chinese-smartphones-over-security-risks-1.525026.

among Congress and the executive branch that "large Chinese companies ... are directly subject to direction by the Chinese Communist Party," *see* ECF 28-2 (Finding No. 2); that Huawei was one of those companies, *id.* (Finding No. 4); that the Chinese government may use the position of those companies to exploit "Chinese Government-supported telecommunications equipment on U.S. networks," *id.* (Finding No. 6); and that, as a result, Huawei products should be excluded from U.S. government systems and those of its contractors, *id.* (Finding No. 12 (citing the HPSCI Rep.); *see also id.* (Finding Nos. 8, 9, 14, 15 (citing the statements of high-level executive branch officials that they do not, and would not, use Huawei products)).

On April 12, 2018, the HASC held a hearing on defense authorizations, at which then-Secretary of Defense James Mattis testified that he did "not think [it would be] wise" to allow Huawei or ZTE to be part of DoD's supply chain. *See Hearing on NDAA for Fiscal Year 2019 and Oversight of Previously Authorized Programs Before the HASC*, 115th Cong., at 163 (2018), Ex. 17. The next day, Representative Thornberry introduced H.R. 5515, which became the 2019 NDAA. ECF 28-4.

During markup in the HASC, H.R. 5515 was revised to include a provision similar to the Defending U.S. Government Communications Act, along with three additional findings about the risks of Huawei and Chinese telecommunications products. *See* ECF 28-5 (citing the 2018 testimony of Dirs. Wray and Rogers and the February and March 2018 recommendations against using Huawei products by representatives of the intelligence community). The conference report also noted that the FCC had issued a notice of proposed rulemaking ("NPRM") in April 2018, to deny funding through the Universal Service Fund to purchase telecommunications equipment or services from companies "posing a national security threat to the integrity of communications networks or the communications supply chain" and specifically citing the risks posed by Huawei and ZTE. H.R. Rep.

No. 115-676, at 163 (2018), Ex. 18; *see* FCC, NPRM In the Matter of Protecting Against Nat'l Sec. Threats to the Comms. Supply Chain Through FCC Programs, FCC 18-42 (2018), Ex. 19.[5]

During the House's consideration of H.R. 5515, it adopted an amendment offered by Representative McCaul that extended the prohibition on federal agency procurement of covered equipment and services to federal grant and loan money. *See* 164 Cong. Rec. H4655 (May 23, 2018), Ex. 20. Rep. McCaul explained that the amendment was meant "to better safeguard State and local communications networks," in part by ensuring that the prohibition extended to federal dollars granted to State and local governments, which "play a major role in the protection of our Nation's security." *Id.* The House passed H.R. 5515 as part of the NDAA on May 24, 2018. ECF 28-8.

When the Senate considered H.R. 5515, it adopted an amendment proposed by Senator Cotton that, among other things, (1) clarified that the procurement prohibition would be limited to equipment that can "route or redirect user data traffic or permit visibility into any user data" traffic, and (2) provided that penalties originally imposed by the U.S. Department of Commerce on ZTE for selling restricted products to Iran in violation of U.S. export control laws would be reinstated under certain conditions. *See* 164 Cong. Rec. S3362 (June 7, 2018), Ex. 21. The Senate passed its version of H.R. 5515 on June 18, 2018, *see* H.R. 5515, 115th Cong. (2018), and during conference, the provision reinstating penalties on ZTE was eliminated, *see* H.R. Rep. No. 115-874, at 918-19 (2018), Ex. 22.

In June and July of 2018, several Members of Congress expressed their views of the provision that would become Section 889. Senator Cotton explained that it was intended to prevent the use of Huawei and ZTE routers, switches, and other equipment that could "give the Chinese Government a backdoor into our first responder networks, our electric grid," and more. 164 Cong. Rec. S3896 (June

[5] The Universal Services Fund provides financial support to ensure telephone and Internet access for low-income individuals and rural, high-cost areas through qualifying telephone companies, healthcare providers, schools, and libraries. *See* https://www.fcc.gov/general/universal-service-fund (last visited July 3, 2019).

13, 2018), Ex. 23. He characterized it as "an important ... step" to protect "our national security and [Americans'] privacy" and to ensure that companies subject to Chinese influence "are not doing business with the Federal Government or any firms ... relying on U.S. taxpayer dollars." *Id.* at S3898.

Senator Van Hollen echoed those security concerns, reciting the HPSCI Report's statement that "'China has the means, opportunity, and motive to use telecommunications companies for malicious purposes,'" as well as FBI Director Wray's testimony that the Chinese government could exert its influence over companies with access to our telecommunications infrastructure to "'maliciously modify or steal information'" and "'conduct undetected espionage.'" *Id.* at S3897. He noted that "[t]he Pentagon recently prohibited the sale of [covered] devices on U.S. military bases" and that the FCC "[h]ad also proposed steps to discourage American companies from using products from Huawei and ZTE." *Id.* "It stands to reason," he said, that federal agencies "should not be purchasing this equipment that threatens our national security." *Id.*

Senator Blumenthal called the relevant provision a "practical security measure" to ensure that the equipment of companies subject to Chinese influence does not "enter[] the networks of the U.S. Government and its contractors for the safety and security of us all." 164 Cong. Rec. S3937 (June 14, 2018), Ex. 24. And Representative Hartzler observed that "[t]he Chinese Government is using every avenue at its disposal to target the United States, including expanding the role of Chinese companies in the U.S. domestic communications and public safety sectors." 164 Cong. Rec. H7703 (July 26, 2018), Ex. 25. "[T]o protect the U.S. government from [these] significant vulnerabilities," she explained that H.R. 5515 "prohibits Federal agencies from purchasing certain Chinese-made telecommunications and video surveillance equipment." *Id.*

B. Section 889 as Enacted

Against this backdrop, on August 13, 2018, Congress enacted, and the President signed into law, the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which included

Section 889. Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917-18, ECF 28-15. Section 889 as enacted does not contain legislative findings but retains the general structure of H.R. 5515, including its three principal prohibitions. First, the statute prohibits federal agencies from procuring or extending or renewing a contract to procure "any equipment, system, or service" if "covered telecommunications equipment or services" constitute "a substantial or essential component," or "critical technology," of any system. § 889(a)(1)(A). Second, it prohibits federal agencies from entering into, extending, or renewing a contract with an entity that uses any such "equipment, system, or service." § 889(a)(1)(B). Third, it prohibits federal loan or grant funds from being used to obtain any such "equipment, services, or systems." § 889(b).

"Covered telecommunications equipment or services" are defined to include, *inter alia*, telecommunications *equipment* produced by Huawei, ZTE, or their affiliates; telecommunications or video surveillance *services* provided by those entities, among others;[6] and telecommunications or video surveillance services provided by any other entity *using such equipment*. § 889(f)(3)(A), (C). Section 889 also permits the Secretary of Defense, in consultation with the DNI and the Director of the FBI, to apply the prohibitions in Section 889 to equipment and services provided or produced by an entity the Secretary "reasonably believes [is] owned or controlled by, or otherwise connected to, the [Chinese government]." § 889(f)(3)(D).

Section 889 clarifies the definition of "covered telecommunications equipment or services" by stating that the statute does not "cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles," § 889(a)(2)(B), (b)(3)(B), or prohibit an agency from contracting with an entity "to

[6] Section 889 defines covered telecommunications equipment to include "video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company" or their affiliates. *Id.* § 889(f)(3)(B). All three are Chinese companies headquartered in China.

provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements," § 889(a)(2)(A), (b)(3)(A).

The head of a federal agency may provide a time-delimited waiver of the first and second prohibitions if the agency head determines that the entity requesting the waiver has "a compelling justification" for needing the additional time and submits a plan to phase-out covered equipment or services from its systems. § 889(d)(1)(A)-(B). In addition, the DNI may provide a waiver if the Director determines it "is in the national security interests of the United States." § 889(d)(2).

DEFENDANTS' RESPONSE TO PLAINTIFFS' STATEMENT OF MATERIAL FACTS[7]

Pursuant to an agreed-upon schedule, ECF 25, adopted by this Court, ECF 26, the parties are filing cross-motions, including for summary judgment pursuant to Federal Rule of Civil Procedure 56.

1-3. Defendants do not dispute Plaintiffs' Facts Nos. 1-3.

4. Defendants do not dispute the first clause of Plaintiffs' Fact No. 4. The second clause of Plaintiffs' Fact No. 4 does not state a material fact, as Plaintiffs do not challenge any agency action.

5. Plaintiffs' Fact No. 5 does not state any material fact. Even if the economic and reputational harms Plaintiffs cite are accepted as true and are the result of Section 889, they do not constitute punishment for purposes of the Bill of Attainder Clause as a matter of law. And Plaintiffs have likewise not articulated facts setting forth a claim under the Due Process or Vesting Clauses.

ARGUMENT

I. SECTION 889 DOES NOT VIOLATE THE BILL OF ATTAINDER CLAUSE.

Article I of the U.S. Constitution prohibits Congress from passing "Bill[s] of Attainder." U.S. Const. art. I, § 9, cl. 3 ("No Bill of Attainder ... shall be passed."). The prohibition was meant to address the ancient parliamentary practice "of punishing without trial 'specifically designated persons

[7] Defendants have not provided an independent Statement of Facts, as this case involves purely legal questions and no genuinely disputed material fact.

or groups.'" *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 847 (1984) (quoting *United States v. Brown*, 381 U.S. 437, 447 (1965)).[8] A law thus violates the Bill of Attainder Clause only if it applies with "specificity" and imposes "punishment." *SBC Commc'ns*, 154 F.3d at 233.

The specificity element may be satisfied where a statute applies "either to named individuals or to easily ascertainable members of a group." *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 538 (1977). Specificity alone, however, does not render a statute a bill of attainder. *See id.* at 471-72 ("[T]he fact that [the Act] refers to appellant by name ... does not automatically offend the Bill of Attainder Clause."). Rather, "punishment is a necessary element of an unconstitutional bill of attainder." *SBC Commc'ns*, 154 F.3d at 235.[9]

A "punishment," in this context, is not merely a burden. *See Selective Serv.*, 468 U.S. at 851 ("That burdens are placed on citizens by federal authority does not make those burdens punishment."). "Figuratively speaking all discomforting action may be deemed punishment because it deprives of what otherwise would be enjoyed[,] [b]ut there may be reasons other than punitive for such deprivation." *Id.* To determine whether a statute imposes punishment for purposes of the Bill of Attainder Clause, courts look to: "(1) whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes; and (3) whether the legislative record evinces a congressional intent to punish." *Id.* at 852.

While courts weigh these factors together, "the second factor—the so-called 'functional

[8] Hereinafter, all internal citations, quotations, or alterations are omitted unless otherwise indicated.

[9] Defendants do not dispute that the specificity element is satisfied here, but satisfaction of that element is not dispositive, and Defendants note that in addition to specifically naming Huawei, Section 889 names four other Chinese companies and provides a procedure for the Secretary of Defense to designate additional companies as subject to Section 889's prohibitions. *See* § 889(f)(3)(A)-(B), (D). This shows Congress's intent to treat a particular problem, not to target a particular company for punishment. *See infra* § ARG.I.B.2.

test'—invariably appears to be the most important." *Kaspersky*, 909 F.3d at 455. As the Fifth Circuit has explained, even where a statute imposes a sanction falling within the historical meaning of punishment under the first factor, it is not a bill of attainder if it "reasonably can be said to further nonpunitive legislative purposes" under the second factor and the legislative record does not contain "'smoking gun' evidence of punitive intent" under the third. *SBC Commc'ns*, 154 F.3d at 242-43.

The party challenging a statute on attainder grounds bears the burden to "establish that the legislature's action constituted punishment and not merely the legitimate regulation of conduct." *Nixon*, 433 U.S. at 476 n.40. And because statutes are "presumed constitutional," *Heller v. Doe by Doe*, 509 U.S. 312, 320 (1993), "only the clearest proof [will] suffice" to invalidate a statute as a bill of attainder, *Communist Party of U.S. v. Subversive Activities Control Bd.*, 367 U.S. 1, 83 (1961).

Given these stringent standards, cases finding that a statute violates the Bill of Attainder Clause are "exceedingly rare." *Shankles v. Dir., TDCJ-ID*, 877 F. Supp. 346, 352 (E.D. Tex. 1995). The Supreme Court has invalidated statutes on attainder grounds only five times in this country's history, *see id.* (citing *Brown*, 381 U.S. 437; *United States v. Lovett*, 328 U.S. 303 (1946); *Pierce v. Carskadon*,, 83 U.S. (16 Wall.) 234 (1872); *Ex Parte Garland*, 71 U.S. (4 Wall.) 333 (1866); *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277 (1866)), with the Court's four major cases all involving Cold War or Civil War era enactments that barred flesh-and-blood individuals from participating in their chosen professions because "the legislature deemed [them] untrustworthy or subversive based on [their] political beliefs," (the "employment bar cases"), *Kaspersky*, 909 F.3d at 462-63.[10] By contrast, federal circuit courts have more recently rejected bill of attainder challenges to legislative restrictions on named entities relating to their business activities. The Fifth Circuit rejected one such bill of attainder challenge to line-of-business restrictions that precluded named operating companies from providing certain

[10] The statute at issue in *Pierce* involved access to the courts, not employment. *See* 83 U.S. at 235.

telecommunications equipment and services. *SBC Commc'ns*, 154 F.3d at 232. And just last year, the D.C. Circuit roundly rejected the attainder claim of a Russian cybersecurity company, Kaspersky Lab, challenging provisions of the 2018 NDAA that named Kaspersky and prohibited federal agencies from using its products. *See Kaspersky*, 909 F.3d 446.

Huawei does not meaningfully grapple with *SBC* and largely ignores the recent and highly analogous *Kaspersky* decision, instead attempting to analogize to the Supreme Court's employment bar cases from the Civil and Cold War eras. *See generally* Pls.' Mot. 10-27. But the statutes at issue in the employment bar cases are a far cry from Section 889, under which Huawei is not prevented from engaging in its global business, including in the United States. That conclusion is underscored by the more recent decisions, which firmly establish that Congress can restrict the federal procurement and funding of Huawei products where those restrictions reasonably can be said to further Congress's prophylactic purpose of protecting national and informational security and Huawei points to nothing close to the "unmistakable evidence of punitive intent" required to refute Congress's prophylactic purpose. *SBC Commc'ns*, 154 F.3d at 242-43. Congress's decision "to take its business elsewhere," *Kaspersky*, 909 F.3d at 463, and "to withhold funds from [Huawei] and its affiliates" in furtherance of legitimate legislative aims, *ACORN v. United States*, 618 F.3d 125, 137 (2d Cir. 2010), is not punitive, and Huawei fails to show otherwise under any of the three factors of the punishment test.

A. Section 889 Does Not Fall Within the Historical Definition of "Punishment."

The first, or historical, factor of the punishment test asks if a statute falls within the "checklist of deprivations and disabilities so disproportionately severe and so inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of [the Bill of Attainder Clause]." *Nixon*, 433 U.S. at 473. The classic example of such a sanction is a death sentence, but the Clause also encompasses statutes imposing "imprisonment, banishment, and the punitive confiscation of property by the sovereign." *Id.* at 473-74. To that list, the Supreme Court has made only one

addition: punitive employment bars. *Id.* at 474. As noted, in four instances, the Court struck down as bills of attainder statutes that "barr[ed] designated individuals or groups from participation in specified employments or vocations," *id.*, because Congress determined that they were "untrustworthy or subversive based on [their] political beliefs," *Kaspersky*, 909 F.3d at 462-63; *see also SBC Commc'ns*, 154 F.3d at 235-41 (discussing Supreme Court attainder jurisprudence).

Section 889 bears no resemblance to any of these historical forms of punishment. It is a regulatory measure, directed at the government's own purchasing decisions, that merely prohibits federal agencies from procuring, contracting with entities that use, or expending federal loan or grant funds to procure, substantial Huawei equipment or services[11] that could be exploited based on their ability to "route," "redirect," or "permit visibility into" telecommunications data. § 889(a)-(b). Section 889 does not sentence Huawei to death, imprison it, or confiscate its property. And to the extent the employment bar cases even apply to a multi-national corporation like Huawei, Section 889 plainly does not preclude Huawei from engaging in its chosen profession. Huawei nevertheless argues that Section 889 possesses certain characteristics indicative of historical bills of attainder, such that it imposes a disability on Huawei akin to an employment bar and banishment. *See* Pls.' Mot. 15-17. But both comparisons are inapt, as evidenced by the fact that courts have repeatedly rejected attempts to equate provisions that impose restrictions on private companies to punitive employment bars, *see, e.g., SBC Comm'ns*, 154 F.3d at 249; *Kaspersky*, 909 F.3d 446; *BellSouth Corp. v. FCC* (*"BellSouth II"*), 162 F.3d 678 (D.C. Cir. 1998); *BellSouth Corp. v. FCC* (*"BellSouth I"*), 144 F.3d 58 (D.C. Cir. 1998), and Huawei can cite no authority for its comparison of Section 889 to banishment, *see* Pls.' Mot. 15-17.

1. Section 889 Does Not Impose a Punitive Employment Bar.

[11] Hereinafter, if not otherwise indicated, Defendants, for brevity, refer to covered Huawei equipment and services as Huawei "products." In addition, while Defendants focus on Huawei's claims and thus Section 889 as it applies to Huawei, as mentioned, Section 889 applies to four other Chinese companies as well, *see* § 889(f)(3)(A)-(D), and much of the HPSCI Report also applies to ZTE.

"[A] wide valley separates" Section 889 "from the small handful of statutes that courts have found to be unconstitutional bills of attainder." *Kaspersky*, 909 F.3d at 463. *First*, "[b]ecause human beings and corporate entities are so dissimilar," any analogy between the acts at issue in the employment bar cases and Section 889 is "strained at best." *Kaspersky*, 909 F.3d at 462. Huawei does not contend at all with this distinguishing factor. *See* Pls.' Mot. 15-17. But the Supreme Court has emphasized that each bill of attainder case "turn[s] on its own highly particularized context," *Selective Serv.*, 468 U.S. at 852, and, accordingly, both the D.C. and Second Circuits have repeatedly explained that the differences between individuals and corporations must be taken into account in the bill of attainder analysis, *see Kaspersky*, 909 F.3d at 461 (calling the difference so "obvious" that it "must necessarily [be] take[n] into account"); *ACORN*, 618 F.3d at 137 ("'There may well be actions that would be considered punitive if taken against an individual, but not if taken against a corporation.'") (quoting *Consol. Edison Co. of N.Y. v. Pataki*, 292 F.3d 338, 354 (2d Cir. 2002) (noting that differences among individuals, corporations, and public utilities must be accounted for)). Indeed, two of the distinguishing characteristics of statutes historically deemed bills of attainder do not pertain in the case of a multinational corporation like Huawei.[12]

The distinction between individuals and corporate entities is an important one, first, because the Supreme Court extended "punishment" to include employment bars, in part, because the restrictions at issue "violated the fundamental guarantees of political and religious freedom." *BellSouth*

[12] In *SBC*, the Fifth Circuit "assum[ed] that the Bill of Attainder Clause applies to corporations," as well as individuals. 154 F.3d at 234. As noted in that case, however, the Supreme Court has not directly addressed the question, *see id.* at 234 n.11, and the history and application of the Clause—to individuals—as well as the Court's dicta, provide strong reason to suggest that the Clause does not, in fact, apply to multinational corporate entities like Huawei. *See, e.g., South Carolina v. Katzenbach*, 383 U.S. 301, 324 (1966) (explaining that "courts have consistently regarded the Bill of Attainder Clause of Article I and the principle of the separation of powers only as protections for individual persons and private groups"). In any event, if it is applied, it should be applied in a manner that takes account of the differences between individuals and corporations, as explained.

II, 162 F.3d at 686. That concern is simply not implicated here, *see Kaspersky Lab, Inc. v. DHS*, 311 F. Supp. 3d 187, 208 (D.D.C. 2018), *aff'd*, 909 F.3d 446 (D.C. Cir. 2018) ("A statute that does not apply to any individual but instead deprives a large multinational corporation of one of its many sources of revenue does not threaten anyone's personal rights or freedoms."), and Huawei does not seriously contend otherwise, *see* Pls.' Mot. 17 (making passing, unsupported assertion that Section 889 threatens Huawei's "rights of political association").

The distinction is also important because "the stain of a brand of infamy or disloyalty," characteristic of bills of attainder, matters to individuals in a way that it does not to corporations. *Kaspersky*, 909 F.3d at 461. Unlike "flesh-and-blood humans ... who, most likely, have but one country of citizenship," as well as "neighbors and colleagues and communities in whose good graces they hope to remain," corporate reputation "is an asset that companies cultivate, manage, and monetize." *Id.* "It is not a quality integral to a company's emotional well-being, and its diminution exacts no psychological cost." *Id.* Because corporations do not "feel burdens in the same way as living, breathing human beings," *id.*, the bill of attainder analysis does not apply to them in the same way, *see id.*; *see also ACORN*, 618 F.3d at 137 (recognizing same).

Contrary to Huawei's contentions then, Section 889 does not mark it with a "brand of infamy or disloyalty," Pls.' Mot. 17, like the statutes invalidated on attainder grounds that targeted individuals. At most, Huawei contends that Section 889 has "harmed [its] reputation *as a business*," Decl. of Kevin Lu ¶ 23, ECF 29-1 (emphasis added), by "casting [it] as a tool of the Chinese government," Pls.' Mot. 17.[13] But any reputational harm to Huawei's business interests due to Section 889 is different in kind

[13] Huawei attempts to rely on the purported reputational harm and embarrassment of its employees in arguing that Section 889 bears the marks of an historical attainder. *See* Pls.' Mot. 17 (citing, *inter alia*, Atha Decl. ¶ 6). Huawei's employees are not plaintiffs here, and they were not named in Section 889. For both reasons, any harm to them cannot support Huawei's bill of attainder claim. *See Kowalski v. Tesmer*, 543 U.S. 125, 130 (2004) (explaining general rule against raising the rights of third-parties).

from the harms imposed by the statutes at issue in the cases on which Huawei relies. For instance, Huawei's alleged reputational injury pales in comparison to the "costly injury to [the plaintiff]'s reputation" in *Foretich v. United States*, 351 F.3d 1198, 1223 (D.C. Cir. 2003), where the statute at issue "memorialize[d] a judgment by ... Congress that [the plaintiff] [wa]s guilty of horrific crimes," namely "criminal acts of child sexual abuse" against his own daughter. As the D.C. Circuit observed in *Kaspersky*, while "Section [889] may well cost [Huawei] some revenue, ... it stretches credulity to view what is ultimately a procurement decision as a brand of infamy or disloyalty." 909 F.3d at 463.

Second, unlike the statutes at issue in the employment bar cases, Section 889 does not preclude Huawei from engaging in its chosen profession. "[A]ll of the Supreme Court's employment ban cases have involved a legislative enactment barring designated individuals or groups from participation in specified employments or vocations." *Id.* at 462. Not so with Section 889. Although Huawei contends that Section 889 prevents it from "pursuing the avocation of [its] choice," Pls.' Mot. 15, its own statements undermine that contention. Huawei bills itself as a "global leader in information and communications technology products and services," Compl. ¶ 29, and the "first company to develop large-scale 5G commercial deployment capabilities," Huawei Investment & Holding Co., Ltd., 2018 Annual Rep. ("Huawei 2018 Rep."), at 3, Ex. 26.[14] Far from being "'exclu[ded] from ... [one] of the ordinary avocations of life,'" Pls.' Mot. 16 (quoting *Garland*, 71 U.S. at 377), Huawei operates in more than 170 countries and regions around the world, Huawei 2018 Rep., at 11.

Huawei complains that Section 889 "exclude[s] it ... from the trusted position of providing covered equipment to federal agencies." Pls.' Mot. 16. But a limitation on a company's customer base or product offerings does not prohibit individuals from serving in particular offices or engaging

[14] *See also* Kadri Kaska et al., NATO Cooperative Cyber Defense Centre of Excellence, Huawei, 5G and China as a Security Threat, at 7 (2019), Ex. 27 ("[Huawei] is currently the only company that can produce 'at scale and cost' all the elements of a 5G network, with its closest competitors Nokia and Ericsson not yet able to offer a viable alternative.").

in particular vocations altogether. *See Brown*, 381 U.S. 437 (barring communist party members from labor union offices); *Lovett*, 328 U.S. 303 (effectively terminating the government employment of three Communist party members); *Cummings*, 71 U.S. (4 Wall.) 277; *Garland*, 71 (4 Wall.) 333 (barring former confederate rebels from entry into clergy and law). Huawei's inability to contract with federal agencies to provide certain products (or to receive federal subsidization for the provision of those products) simply does not prevent Huawei from engaging in its chosen profession. *See Kaspersky*, 909 F.3d at 462 ("Because the federal government is far from Kaspersky's only client, section 1634 does not prevent [it] from engaging in its chosen profession.").

Instead, Section 889's prohibitions more closely resemble the "line-of-business restrictions on named corporations" that the Fifth Circuit upheld in *SBC*, *see* 154 F.3d at 233 (upholding Telecommunications Act of 1996 provisions prohibiting operating companies from providing certain telecommunications products without meeting statutory criteria), and that the D.C. Circuit has upheld repeatedly, *see Kaspersky*, 909 F.3d at 462-63 (upholding 2018 NDAA provision prohibiting the federal government from using Kaspersky products and requiring removal of Kaspersky software from federal networks); *BellSouth II*, 162 F.3d at 680-81 (upholding provisions similar to those upheld in *SBC*); *BellSouth I*, 144 F.3d at 65 (similar).[15] It is no answer that Section 889, according to Plaintiffs, "imposes a permanent disability on Huawei," unlike the provisions at issue in *SBC*. Pls.' Mot. 16. Under Section 889, the DNI may provide a waiver if he determines one "is in the national security interests of the United States." § 889(d)(2). And in any event, the indefinite nature of a restriction is not dispositive in the attainder analysis. *See SBC Commc'ns*, 154 F.3d at 238 (citing *Hawker v. New York*,

[15] Further, as the D.C. Circuit has explained, the Supreme Court "strongly suggested [in *Brown*] that line-of-business restrictions pose no bill of attainder concerns," *BellSouth I*, 144 F.3d at 65, and "has approved other line-of-business restrictions without ever suggesting that the restrictions constituted 'punishment,'" *BellSouth II*, 162 F.3d at 686 (citing cases).

170 U.S. 189, 196 (1898) (upholding indefinite prohibition of convicted felons from practicing medicine where the state was "not seeking to further punish a criminal, but only to protect its citizens from physicians of bad character")).[16] As the D.C. Circuit explained in rejecting the same argument in *Kaspersky*, "the Bill of Attainder Clause tolerates statutes that, in pursuit of legitimate goals such as public safety or economic regulation, prevent companies from engaging in particular kinds of business or particular combinations of business endeavors." 909 F.3d at 463. Such is the case here: to protect the telecommunications systems of federal agencies, contractors, and grantees, Section 889 reasonably restricts Huawei from obtaining federal contracts or subsidization to provide those entities with products that Congress determined pose substantial threats to national and informational security.

Huawei also contests that Section 889 "exclude[s] it … from providing [covered] equipment to a vast number of private entities that are government contractors and/or federal loan and grant recipients." Pls.' Mot. 16. But Huawei overstates the reach of Section 889. Aside from federal agencies, which are precluded from procuring covered Huawei products, "all other individuals and companies in the universe of potential clients remain free to buy and use [Huawei] products." *Kaspersky*, 909 F.3d at 457.[17] For entities wishing to obtain or extend contracts with federal agencies, Section 889 may dissuade them from using covered Huawei products, lest they be precluded from future federal contracting. But such an indirect effect on one line of Huawei's business does not

[16] *Id.* at 242 (citing *BellSouth I*, 144 F.3d at 65 ("Even measures historically associated with punishment—such as *permanent* exclusion from an occupation—have been otherwise regarded when the nonpunitive aims of an apparently prophylactic measure have seemed sufficiently clear and convincing.") (emphasis added); *Dehainaut v. Pena*, 32 F.3d 1066, 1071 (7th Cir. 1994) ("Even where a fixed identifiable group ... is singled out and a burden traditionally associated with punishment—such as *permanent* exclusion from an occupation—is imposed, the enactment may pass scrutiny under bill of attainder analysis if it seeks to achieve legitimate and non-punitive ends and was not clearly the product of punitive intent.") (same)).

[17] Huawei has been the subject of various other congressional and executive actions and proposals, including, as Defendants have pointed out, actions by DoD, the FCC, and the Commerce Department. To the extent any of those actions restrict Huawei's interactions with the private sector, they are not attributable to Section 889.

equate to an employment bar. *See, e.g., Fresno Rifle & Pistol Club, Inc. v. Van De Kamp*, 965 F.2d 723, 728 (9th Cir. 1992) (where California statute imposed permitting requirements on firearms designated "assault weapons" but did not preclude their continued manufacture or sale, any economic harm to covered manufacturers was "indirect" and did not amount to historical punishment). And any "competitive disadvantage" Huawei may suffer "when marketing and attempting to sell" covered products to federal contractors or grantees, *see* Lu Decl., ¶¶ 12, 17, is not "so disproportionately severe and so inappropriate to nonpunitive ends" that it "unquestionably" falls within the category of disabilities and deprivations recognized as historical punishments under the Bill of Attainder Clause, *Nixon*, 433 U.S. at 473. *See, e.g., Selective Serv.*, 468 U.S. at 853 (statute denying financial aid to male students who failed to register for the draft was not a bill of attainder where "[n]o affirmative disability or restraint [wa]s imposed" and Congress inflicted "nothing approaching the ... disabilities historically associated with punishment"); *ACORN*, 618 F.3d at 137 (not an attainder where "plaintiffs [we]re not prohibited from any activities; they [we]re only prohibited from receiving federal funds to continue their activities").

Third, Section 889 is unlike the statutes found by the Supreme Court to be punitive employment bars because it does not constitute, and is not based upon, any trial-like adjudication that Huawei is guilty of past wrongdoing. *De Veau v. Braisted*, 363 U.S. 144, 160 (1960) ("The distinguishing feature of a bill of attainder is the substitution of a legislative for a judicial determination of guilt."). Huawei attempts to rely on the legislative findings in earlier versions of Section 889 to argue that Congress, "in effect, tried Huawei" and "found it guilty of being a bad actor subject to Chinese government influence." Pls.' Mot. 22. But Congress routinely makes particularized legislative findings to support its policy choices without offending the Bill of Attainder Clause. *See, e.g., SeaRiver Mar. Fin. Holdings, Inc. v. Mineta*, 309 F.3d 662 (9th Cir. 2002) (upholding provision of Oil Pollution Act of 1990 that set forth detailed findings about the Exxon Valdez oil spill and excluded the owners and operator

of the Exxon Valdez from the Prince William Sound); *Am. Commc'ns Ass'n, C.I.O., v. Douds*, 339 U.S. 382, 387 (1950) (rejecting bill of attainder claim, in part, based on Congress's legislative findings in the Labor-Management Relations Act). Doing so does not amount to a trial-like adjudication of guilt indicative of a bill of attainder, as the Ninth Circuit found in rejecting a nearly identical argument. *See Fresno Rifle*, 965 F.2d at 727 (rejecting gun manufacturers' argument that "the legislature tried them and found their products to be 'assault weapons'" where California legislature made findings including that the named plaintiffs' firearms constituted "assault weapons").

Moreover, Plaintiffs repeatedly emphasize that Congress did not conclusively determine that Huawei was guilty of wrongdoing, *see* Pls.' Mot. 4; Compl. ¶ 47, which underscores that Section 889 is not premised on any trial-like adjudication of Huawei's past conduct, but rather is targeted at mitigating the prospective cyber-threat posed by Huawei's expanding deployment into U.S. networks and potential for influence by the Chinese government. While the substance of Congress's earlier findings reflect its recognition of the view, stated publicly over a span of years in numerous reports and by high-level officials in the executive branch, that Huawei is suspected of having ties to the Chinese government, that is not the end of the matter. Congress did not enact Section 889 to "sanction[]" Huawei because of any such ties, as Plaintiffs suggest. Pls.' Mot. 22. Rather, Congress enacted Section 889 based on its judgment that those potential ties make Huawei's products particularly susceptible to the *prospective* threat of wrongdoing by *the Chinese government*—especially in light of increasing vulnerabilities due to the transition to 5G and the IoT. Congress is afforded substantial leeway in making such "predictive judgments," *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 195 (1997), and its exercise of that judgment here, in light of longstanding cybersecurity concerns, does not offend the Bill of Attainder Clause, *see SBC Commc'ns*, 154 F.3d at 247 (statute not a bill of attainder where it "may well constitute a legislative judgment that the [operating companie]s currently

have an inherent and natural potential to restrain competition by virtue of their local market power").[18]

2. Section 889 Does Not Impose a Punishment Akin to Banishment.

Huawei also makes passing comparisons of Section 889 to the historical punishment of "banishment." Pls.' Mot. 16-17. Respectfully, Section 889 is nothing like the historical punishment of banishment. Banishment, or exile, is the "[c]ompelled removal or banishment from one's native country." Black's Law Dictionary (10th ed. 2014). It has "traditionally been associated with deprivation of citizenship, and does more than merely restrict one's freedom to go or remain where others have the right to be: it often works a destruction of one's social, cultural, and political existence." *SeaRiver*, 309 F.3d at 673. Claims of banishment therefore typically arise in cases involving denaturalization, denationalization, and deportation proceedings. *See Poodry v. Tonawanda Band of Seneca Indians*, 85 F.3d 874, 902 (2d Cir. 1996).

In light of this context, it is questionable whether banishment applies to corporations at all. *See SeaRiver*, 309 F.3d at 673 (seeming to assume so but noting that banishment typically "refers to individuals"). In any event, nothing in Section 889 serves to "banish" Huawei from the United States. The statute does not destroy Huawei's social, cultural, or political existence in this country. And it does not remove Huawei from the United States (or any subdivision thereof). Huawei USA is headquartered in Plano, Texas, Compl. ¶ 8, and nothing in Section 889 precludes Huawei from continuing to engage in much of its business with the private sector, or even to contract with the government to provide products not covered by Section 889.

Huawei nevertheless argues that the "vast restrictions and constitutional burdens" imposed by

[18] The evidence of the longstanding national security concerns about Huawei on the part of the executive branch and Congress serves as an additional indicator that Section 889 does not have the hallmarks of a bill of attainder. Far from "cater[ing] to the momentary passions of a free people, in times of heat and violence," *Nixon*, 433 U.S. at 480 n.45, Congress enacted Section 889 only after lengthy and thoughtful consideration.

Section 889 constitute "attempts to 'banish' Huawei from the [United States]," Pls.' Mot. 15, and pose a "serious threat to [its] ability to continue to do business" in this country, *id.* at 17. But Huawei's suggestion that Congress *attempted* to banish it is itself a concession that Congress did no such thing. Huawei cites no authority for the proposition that a purported *threat* to the business vitality of a company could rise to the level of "a fate universally decried by civilized people." *Trop v. Dulles*, 356 U.S. 86, 102 (1958).[19] And any adverse effect resulting from the business restrictions imposed by Section 889 is hardly punishment of the severest kind rising to the level of a bill of attainder. *See ACORN*, 618 F.3d at 137 (denying attainder claim where plaintiff argued it would be "drive[n] close to bankruptcy" and suffer "corporate death sentence" without federal funds); *SBC Commc'ns*, 154 F.3d at 243 n.27 (denying attainder claim where act imposed criteria difficult but not "impossible" to meet).

B. Section 889 Furthers Nonpunitive Legislative Purposes.

Notably, even if Huawei could show that Section 889 imposes an historically punitive sanction (it cannot), Section 889 nonetheless does not violate the Bill of Attainder Clause. As the Fifth Circuit explained in *SBC*, the Supreme Court has developed a "prophylactic exception," such that even where a statute falls within the historical meaning of punishment, absent "'smoking gun' evidence of punitive intent," 154 F.3d at 243, it does not constitute a bill of attainder so long as it "serve[s] a nonpunitive purpose" under the functional test, *id.* at 242-43 (citing *BellSouth I*, 144 F.3d at 65 (recognizing exception); *Dehainaut*, 32 F.3d at 1071 (same)). Huawei does not even acknowledge this prophylactic exception in its opening brief, but the exception is fatal to Huawei's bill of attainder claim.

[19] Huawei's unsupported assertions that Section 889 poses a "serious threat to [its] ability to continue to do business" in the United States, Pls.' Mot. 17 (citing He Aff. ¶ 20, ECF 29-6; Lu Decl. ¶ 24 (stating unsupported beliefs)), are undermined by the fact that despite the passage of Section 889, Huawei's 2018 sales revenue surpassed $100 billion, up nearly 20% from the prior year. *See* Huawei 2018 Rep., at 3. Huawei does not cite any information regarding its U.S. business in support of its assertions that Section 889 poses a "potentially life-threatening 'exclusion,'" Pls.' Mot. 17, and its overall sales growth suggests that it is not a business faltering as a result of Section 889.

The functional test asks "whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *SBC Commc'ns*, 154 F.3d at 242. While the burdens imposed by a statute must be reasonably "tailored ... to an appropriate end," *id.* at 243, "the question is not whether a burden is proportionate to the objective, but ... whether [its] is so disproportionate that it belies any purported nonpunitive goals," *Kaspersky*, 909 F.3d at 455. Thus, a statute belies its nonpunitive aims only where there is a "significant," *Kaspersky*, 909 F.3d at 455, or "grave," *ACORN*, 618 F.3d at 138, imbalance between the burden imposed and the purported nonpunitive purpose. Because the burdens imposed by Section 889 reasonably further its aims to protect the telecommunications systems of federal agencies, contractors, and grantees from Chinese cyber-threats and to ensure the responsible expenditure of federal funds, it functions as a prophylactic, not a punitive, measure.

1. The Nonpunitive Legislative Purposes of Section 889 are Apparent.

The text of Section 889, along with its legislative history and the context in which it was enacted, demonstrate Congress's principal nonpunitive purpose: to further national and informational security by protecting the networks of federal agencies, contractors, and grantees from the threat of cyber-attacks and -espionage by the Chinese government via companies in a position to exploit those networks.[20] This prophylactic purpose is readily discernable from the text of Section 889. Rather than punishing Huawei for past conduct, the statute has a prospective focus, prohibiting the future

[20] The text and legislative history of Section 889 show that Congress had an ancillary purpose of ensuring that federal tax dollars were not spent to procure, or otherwise further propagate on U.S. networks, products that pose the aforementioned Chinese cyber-threat. *See* § 889(a)-(b); 164 Cong. Rec. S3898 (stmt. of Sen. Cotton) (characterizing Section 889 as "an important ... step" to ensure that companies subject to Chinese influence "are not doing business with the [f]ederal [g]overnment or any firms ... relying on U.S. taxpayer dollars"); *id.* at S3897 (stmt. of Sen. Van Hollen) (explaining that Section 889 "prohibit[s] U.S. taxpayer dollars from being spent to purchase any equipment from Huawei or ZTE"). This is, of course, an appropriate legislative aim, *see ACORN*, 618 F.3d at 137 (recognizing Congress's authority to ensure federal funds are spent responsibly), and the furtherance of that aim is reflected in the statute's restrictions on federal procurement and funding.

procurement of Huawei products and phasing out reliance on those products. *See* § 889(a)-(b) (prohibiting federal agencies from entering into, renewing, or extending covered contracts and from expending loan or grants funds to procure covered products). Its focus on cybersecurity threats is also apparent, as it applies only to telecommunications equipment that can "route or redirect user data traffic or permit visibility into any user data," as well as services using such equipment, *id.*—precisely the types of technological capabilities that could provide a platform for cyber-attacks and -espionage, *see, e.g.,* 2015 FBI Note at 2 (explaining that because routers and switches enable Internet communications to be properly routed, "[t]he Internet of the United States could theoretically be brought down or severely disrupted" if they were disabled). And the statute's aim to counter the particular cyber-threat from China is evidenced by its application to the telecommunications products of five Chinese companies headquartered in China (and their subsidiaries and affiliates), § 889(f)(3)(A)-(B), as well as those of any company the Secretary of Defense "reasonably believes" is connected to the Chinese government, § 889(f)(3)(D).

The statute's focus on the particular products that pose cyber-threats, as well as the national security waiver provision, provide further evidence of Section 889's nonpunitive, prophylactic purpose. The statute does not constitute a "permanent blacklisting of Huawei," as Plaintiffs suggest. Pls.' Mot. 24. It prohibits the procurement of only those telecommunications products that constitute "substantial" or "essential" parts of any system and then, only equipment that can "route," "redirect," or "permit visibility into" user data. § 889(a)(1)-(2), (b)(1), (b)(3)(B). And the DNI may provide a waiver if he determines one "is in the national security interests of the United States." § 889(d)(2). That Congress did not apply Section 889's prohibitions to all Huawei products and included a waiver provision further demonstrates that Congress sought, not to punish Huawei, but to address the particular, most acute threat.

In addition to the statutory text, the legislative record of Section 889 shows that Congress was

taking preventive action to protect the networks of federal agencies, contractors, and grantees in response to the national and informational security threat posed by China's cyber-activities. The precursors to Section 889, introduced in both the House and Senate, were entitled, the "Defending U.S. Government Communications Act." *See* H.R. 4747, 115th Cong. (2018); S. 2391, 115th Cong. (2018). As explained, findings in those bills cited longstanding and widely shared concerns among Congress and the executive branch about cybersecurity threats from the Chinese government and companies potentially subject to its influence, including Huawei, and the widespread recommendation that Huawei equipment should be excluded from sensitive systems. *See supra* § BG.II.A.

Those concerns were echoed by Members of both the House and Senate. Their statements reveal that Section 889 was responding to reports and testimony indicating that the Chinese government has the means, motive, and opportunity "'to use telecommunications companies for malicious purposes.'" 164 Cong. Rec. S3897 (stmt. of Sen. Van Hollen (quoting HPSCI Rep.); *see also id.* (quoting similar 2018 testimony of FBI Dir. Wray); *supra* § BG.II.A (setting forth similar statements by Senators Cotton and Blumenthal and Representative Hartzler). The statements also indicate that Section 889 was passed "to protect the U.S. government from [those] significant vulnerabilities," 164 Cong. Rec. H7703 (stmt. of Rep. Hartzler), as well as "State and local communications networks," 164 Cong. Rec. H4655 (stmt. of Rep. McCaul). As Senator Blumenthal summed it up: Section 889 is a "practical security measure" to ensure that the products of companies with ties to the Chinese government do not "enter[] the networks of the U.S. Government and its contractors for the safety and security of us all." 164 Cong. Rec. S3938.

Although Huawei purports to be "independent of the Chinese government," Pls.' Mot. 4, it does not deny that it is subject to Chinese laws. In fact, Huawei admits that an internal Communist Party Committee exists within Huawei because "party committees are required by Chinese law to exist in all companies in China." HPSCI Rep., at 23. And Huawei does not suggest that it is unreasonable

for Congress to have been concerned about the potential for the Chinese government to use the position of Chinese companies and its influence over them to direct cyber-activity at U.S. information systems, especially in light of particular concerns that have been raised about Huawei, *see supra* § BG.I.B (describing, *inter alia*, that Huawei has received extensive financial support from the Chinese government).[21] Nor does it suggest that it is not a legitimate goal to attempt to protect those systems from state-backed cyber-threats.

Yet, Huawei maintains that, rather than addressing this widely-recognized security threat, it is "reasonable to conclude"—based in part on the fact that "Section 889 does not facially identify its own *actual* purpose"—that Section 889 was really aimed at punishing Huawei. Pls.' Mot. 17 (citing *Nixon*, 433 U.S. at 476; *Foretich*, 351 F.3d at 1221; *Kaspersky*, 909 F.3d at 456). Huawei gets the standard and the burden of proof backwards. As the Fifth Circuit has explained, Huawei, not the government, bears the burden of establishing that the "terms" and "legislative history" of Section 889 "demonstrate[] the 'smoking gun' evidence of punitive intent necessary to establish a bill of attainder." *SBC Commc'ns*, 154 F.3d at 243; *see also Nixon*, 433 U.S. at 476 n.40 (challenging party must establish that Congress's action "constituted punishment and not merely the legitimate regulation of conduct"). Thus, Huawei errs in seeking to impose a clear statement rule, requiring that a statute explicitly state its purpose to survive an attainder challenge. In fact, the statute at issue in *Kaspersky*, which disallowed federal use of Kaspersky products, did not include such a statement, and the court relied heavily on the historical context in which Congress enacted the statute in rejecting the company's bill of attainder claim. *See id.* at 457. Moreover, in *Foretich*, the D.C. Circuit explicitly rejected the argument that a court should confine its review to the "face" of a statute, "divorced from the legislative process that

[21] Indeed, Huawei criticizes Section 889 as underinclusive because it does not cover products from "other telecommunications companies that are from or do business in China—even though the Chinese government *could also seek to influence those companies*." Pls.' Mot. 21 (emphasis added).

produced it"—"particularly ... in the [bill of attainder] context," 351 F.3d at 1215. There is thus no basis for Huawei's suggestion that the court discard the statutory text and legislative record of Section 889—both of which inexorably point to the provision's prophylactic purposes.

2. The Burdens Imposed by Section 889 are Reasonably Tailored to Its Purposes.

The burdens imposed by Section 889 are also sufficiently tailored to its prophylactic purposes. The Supreme Court has warned that Congress must be given sufficient leeway in making policy decisions, lest the bill of attainder analysis "cripple the very process of legislating." *Nixon*, 433 U.S. at 470. Congress is therefore not required to "precisely calibrate the burdens it imposes to ... the threats it seeks to mitigate." *Kaspersky*, 909 F.3d at 460; *see also SBC Comm'ns*, 154 F.3d at 243 (upholding statute in the absence of "substantial doubt [about] the fit of [its] tailoring"). A statute does not fail the functional test unless it is "significantly overbroad," such that it "pil[es] on ... additional, entirely unnecessary burden[s]," *Kaspersky*, 909 F.3d at 455, 460, or so underinclusive that it "seemingly burdens one among equals," *id.* at 456. The standard is a high one because the inquiry remains whether the statute is so punitive that it "belies any purported nonpunitive goals." *Foretich*, 351 F.3d at 1222.

As explained, the congressional concerns animating Section 889 were that it would be detrimental to national and informational security to allow Chinese technology companies to be in a position where they could be used by China to exploit U.S. telecommunications systems. Section 889 therefore contains specific provisions addressing the companies that pose the most acute threat, *see* § 889(f)(3)(A)-(B), due to concerns about their ties to the Chinese government and, in Huawei's case, its positioning and largely unique capacity to provide the full range of telecommunications equipment and services, *see supra* § BG.I.B, as well as broader provisions, permitting the Secretary of Defense to address similar threats in the future, § 889(f)(3)(D), and the DNI to provide a waiver if one is in the national security interests of the United States, *see id.* § 889(d)(2). By holistically addressing the cyber-threat posed by Chinese-government-linked companies—both now and in the future—Section 889

functions like a permissible statute regulating entities "in certain inherently conflicted positions," rather "than an impermissible [punishment] censuring or condemning any man or group of men for their personal conduct." *SBC Commc'ns*, 154 F.3d at 243. Congress also reasonably tailored Section 889 to the specific cyber-threat posed by expressly exempting from its prohibitions products that could not be used to intercept, modify, or spy on network communications. *See* § 889(a)(2)(B), (b)(3)(B) (excluding products that cannot "route or redirect user data traffic or permit visibility into any user data"). These provisions show a clear and coherent nexus between the restrictions imposed under Section 889 and its prophylactic purposes.

Huawei posits that Section 889 is both overbroad and underinclusive, but Huawei falls well short of demonstrating that Section 889 "pil[es] on ... additional, entirely unnecessary burden[s]." *Kaspersky*, 909 F.3d at 460. And in arguing that Section 889 is underinclusive, Huawei misapprehends the nature of the inquiry and otherwise advances arguments that have been rejected previously.

a. Section 889 is not significantly overbroad.

Huawei's overbreadth arguments fall into two general categories: arguments that the prohibitions in Section 889 are overbroad in the scope of their application and, relatedly, arguments that Congress could have adopted narrower, less burdensome alternatives than the framework it did. *See* Pls.' Mot. 17-22, 24-26. This hairsplitting approach to bill of attainder review runs afoul of the Supreme Court's warning against "crippl[ing] the very process of legislating." *Nixon*, 433 U.S. at 470. The Bill of Attainder Clause does not command such a result. *See id.*

Huawei's scope-related arguments are principally three. *First*, Huawei argues that Section 889 is overbroad because it applies to federal agencies, contractors, and grantees that have no connection to "national defense." Pls.' Mot. 19. Aside from its placement in the NDAA, nothing in the text or legislative history of Section 889 suggests it was intended to be limited to national defense. As Huawei notes, the 2018 NDAA, which Congress passed the year before it enacted Section 889, already

prohibited DoD from procuring, or contracting with entities that use, Huawei products to carry out its nuclear deterrence or homeland defense missions. *See id.* at 5. Section 889 had a different aim, applying government-wide to protect critical telecommunications infrastructure based on Congress's well-documented concerns that the cyber-threat from China extends beyond the defense sector, implicating national security (including economic security) and informational security (including governmental and private information, such as proprietary business information, trade secrets, and research results). *See supra* § BG.I.B. One need look no further than the 2014 breach of U.S. Office of Personnel Management ("OPM") databases to see that a cyber-attack on a civilian agency and the contractor supporting it can have far-reaching national security and privacy implications. *See* Maj. Staff, H. Comm. on Oversight & Gov't Reform, Rep. on the OPM Data Breach, at v-vii (2016), Ex. 28 ("attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals").

Second, Huawei argues that Section 889 is overbroad because it applies to federal contractors that use Huawei products even if they "have no potentially compromising connections to [government information] systems" or use covered products for functions "unrelated to their government contracts." Pls.' Mot. 20. But federal contractors routinely work side-by-side with federal employees and not only *do* connect to government information systems, but often provide support to those systems. *See* 2018 DNI Threat Assessment at 6 (explaining that the products and services of "cleared defense contractors or IT and communications firms ... support government and private sector networks worldwide"). Even where they do not have access to government information *systems*, they may nonetheless process, store, or transmit, sensitive government *information*, not to mention personal and proprietary business information, the storage and dissemination of which the government may not always control and Congress reasonably sought to protect. *See* Interos Rep., at vi. ("Nefarious actors linked to China have targeted the networks of private sector entities and private sector

government contractors in order to obtain sensitive government information and to exploit vulnerabilities within federal information systems."). And even where a contractor uses Huawei products for functions wholly unrelated to those being performed for the government, *see* Pls.' Mot. 20, government operations are nevertheless at risk of disruption based on the potential for Chinese government interference with the operations of the contractors on which the government relies.[22]

Third, Huawei argues that Section 889 is overbroad because its restriction on loan and grant funds applies "even if the recipient has no interaction with government information systems." Pls.' Mot. 20. For starters, state and local governments *are* large recipients of loan and grant funds, *see* 164 Cong. Rec. H4655 (stmt. of Rep. McCaul), and the covered products they purchase with federal funds will interact with their information systems. Moreover, because Congress unquestionably has the authority to ensure that the federal funds it appropriates are spent responsibly in furtherance of broader national security goals, *see ACORN*, 618 F.3d at 137, it can leverage its spending power to shield state and local networks from the same cyber-threats facing federal networks. And it can ensure that federal funds are not being used to promote the use of unsecure telecommunications products to support critical functions like building out broadband Internet access to rural communities;[23] expanding access to health care for medically underserved populations through telehealth technology;[24] increasing the use of mobile device technology in classrooms;[25] and investing in smart

[22] Moreover, even if Section 889's prohibitions apply to a subset of contractors whose use of Huawei products would not present these risks, the fact that a statute is not perfectly tailored to Congress's purpose does not make it punitive. *See Kaspersky*, 909 F.3d at 456.

[23] U.S. Dep't of Agric., Reconnect Loan and Grant Program: Program Overview, https://www.usda.gov/reconnect/program-overview (last visited June 26, 2019).

[24] Health Res. & Servs. Admin., Telehealth Programs, https://www.hrsa.gov/rural-health/telehealth/index.html (last reviewed May 2019) (explaining the provision of care to persons geographically distant from their provider through telecommunications technology).

[25] *See* 20 U.S.C. 7119(a)(2)(B) (permitting local educational agencies to spend federal funds on "building technological capacity and infrastructure," including "purchasing devices, equipment, and software applications").

technologies to regulate electric grids efficiently[26]—to name just a handful of the ongoing and recent programs being funded through federal grants and loans.

In addition to its scope arguments, Huawei asserts that Section 889 is overbroad because Congress could have adopted "narrower, less burdensome approaches." Pls.' Mot. 25. But Huawei's alternative approaches would either not adequately serve the purposes of Section 889 or would not reduce the burden on Huawei. Huawei proposes that Congress could have prohibited federal agencies, contractors, and grantees from using covered equipment only if it fails to satisfy "specified design and engineering standards" or "independent security testing." *Id.* As explained, however, Congress's overriding concern about Huawei stemmed not necessarily from faulty aspects of particular equipment, but rather the comparatively high risk of its products being exploited by the Chinese government. The HPSCI thus rejected—after a careful and detailed analysis—the same alternatives Huawei proposes here. *See* HPSCI Rep., at 4-7. Not only did the HPSCI conclude that Huawei's proposals would "fall short of addressing security concerns given the breadth and scale of the U.S. telecommunications market," it explained that given the potential for future exploitation—through, for example, "everyday updates to software and patches to glitches"—no amount of equipment standardization or testing would sufficiently mitigate the threat from an untrusted provider. *Id.* Given the wide latitude afforded Congress to choose between policy alternatives, it "does not matter that Congress arguably could have enacted different legislation in an effort to secure federal networks, because it cannot be legitimately suggested that the risks ... were so feeble that no one could reasonably assert them except as a smoke screen for some invidious purpose." *Kaspersky*, 909 F.3d at 459.

Huawei also posits that Congress should have left it to the executive branch to decide whether

[26] U.S. Dep't of Energy, Smart Grid Investment Grant Program, https://www.smartgrid.gov/recovery_act/overview/smart_grid_investment_grant_program.html (last visited June 26, 2019).

Huawei should be subject to Section 889's restrictions pursuant to the administrative process set forth therein for designation of future companies, § 889(f)(3)(D) (authorizing DoD, in consultation with the DNI and FBI Director, to designate additional companies as subject to Section 889). It is entirely permissible, however, for Congress to have dealt first with those Chinese companies posing the most acute cyber-threats, while concurrently enacting a process to handle companies later determined to present similar threats. *See Nixon*, 433 U.S. at 472 (upholding act that preserved only former-President Nixon's materials, while establishing a process to determine how to preserve those of future officials, because only Nixon's materials "demanded immediate attention"). And, in any event, Huawei fails to explain how the process it purports to seek would result in a less burdensome outcome. DoD reported as early 2011 that Huawei "maintain[s] close ties to the PLA." 2011 DoD Annual Rep., at 42. The Deputy Secretary of Defense testified in 2015 that the Secretary's office would "absolutely not" use Huawei products. 2015 HASC Hearing, at 32. At the same hearing, then-Commander of U.S. Cyber Command testified that Huawei products are not used because they pose an "unacceptable" supply chain risk. *Id.* And the DNI, as well as the Directors of the FBI and DIA, among others, all indicated in a 2018 hearing that they would not use Huawei products. 2018 SSCI Hearing, at 65. In the face of this testimony, and the significant evidence before Congress, Huawei provides no reason to think the administrative process it requests would result in anything other than the restrictions it is presently subject to. Where that is the case, the existence of an alternative process does not render Section 889 impermissibly overbroad. *See Kaspersky*, 909 F.3d at 458 (rejecting argument that the procedural safeguards of the federal debarment process were a less burdensome alternative where plaintiff failed to show how they "would have ultimately forestalled" a similar outcome).

b. Section 889's application is not underinclusive.

Huawei's arguments that Section 889 is underinclusive are equally unpersuasive. Huawei first posits that Section 889 is underinclusive because it permits the continued use of Huawei products by

federal agencies, while prohibiting only future procurements, and allows federal grantees to purchase Huawei products so long as they do not use federal funds to do so. Pls.' Mot. 21. In essence, Huawei asks the Court to second-guess Congress's policy choices and argues that Section 889 is punitive because the choices it made burden Huawei *too little*. That is nonsensical and misapprehends the nature of the inquiry with respect to underinclusiveness.

To be sure, the functional inquiry asks "whether the challenged statute can be reasonably said to further nonpunitive goals," but that inquiry is conducted in view of the "*burdens* imposed." *Selective Serv.*, 468 U.S. at 852-54 (emphasis added); *see also SBC Commc'ns*, 154 F.3d at 243 (evaluating whether Congress "tailored the burdens imposed to an appropriate end"). The inquiry is then focused on "whether the burden is so disproportionate that it belies any purported nonpunitive goals," *Kaspersky*, 909 F.3d at 455—in other words, whether the entity named in the statute is burdened *too much*. Thus, in evaluating whether a statute is "underinclusive" for purposes of the functional test, courts look to whether the statute burdens the named entity more than others in the same position, *see SBC Commc'ns*, 154 F.3d at 243 (assessing whether there was reason to apply "additional burdens" to named companies and not others with local market power); *see also Kaspersky*, 909 F.3d at 456 (statute is underinclusive "when [it] seemingly burdens one among equals"). They do not conduct a free-wheeling exploration of the statute's efficacy untethered from any analysis of the burdens it imposes.

Even if such an inquiry were conducted, there is no merit to Huawei's argument that Section 889's prohibitions are impermissibly "underinclusive" to the extent they do not require agencies to break contracts with Huawei immediately, or grantees to cease using Huawei's products. *See* Pls.' Mot. 20-21.[27] For starters, Congress's measured approach is certainly "not so disproportionate that it belies

[27] As noted, such an alternative would hardly seem to have been less burdensome on Huawei. Indeed, the plaintiffs in *Kaspersky* argued that the retrospective application of the statute at issue there, which required federal agencies to remove already-purchased Kaspersky products from their systems, demonstrated that the statute had a punitive purpose and posited that a restriction limited to future

any purported nonpunitive goals." *Kaspersky*, 909 F.3d at 455. Even with the limitations Huawei identifies, Section 889 considerably mitigates cybersecurity risk as to federal procurement and grant-making by, for example, ensuring that federal agencies do not continue to rely on contractors that use Huawei products as a substantial part of their systems and that federal grants are not promoting the use of Huawei products to provide critical services or to support critical infrastructure. *See supra* § ARG.I.B.2.a. Moreover, Congress's approach in Section 889 reflects the character of the threat. Congress recognized that cybersecurity includes ensuring adaptability by, *inter alia*, maintaining a diversity of telecommunications suppliers to avoid becoming dependent on one supplier for products that could be compromised or cut off. *See supra* § BG.I.B.[28] It was perfectly reasonable for Congress to decide not to subsidize, through federal procurements and funding, the expanded adoption and dependence on Huawei products that it determined are vulnerable to exploitation.

Huawei also argues that Section 889 is underinclusive because it "singles out" Huawei for punishment, Pls.' Mot. 16, and that instead, Congress should have passed a "generally applicable law[]," *id.* at 27, that imposes the same restrictions on "many other telecommunications companies that are from or do business in China," *id.* at 21. The Supreme Court has explained, however, that a law is not an unconstitutional attainder by virtue of its specificity, and there is no requirement that Congress pass only laws that are generally applicable. *See Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 239 (1995) ("While legislatures usually act through laws of general applicability, that is by no means their only legitimate mode of action.... Even laws that impose a duty or liability upon a single individual or firm are not on that account invalid...."). Such a requirement would leave Congress powerless to

contracts would have been a less burdensome alternative. *See Kaspersky*, 909 F.3d at 458.

[28] Huawei's Global Security Officer acknowledged that managing cyber-risk includes "instill[ing] diversity" and that "Huawei's desire to be an end-to-end provider for whole network solutions does not align" with such efforts to maintain a diversity of supply. HPSCI Rep., at 47 n.22.

address national security threats directly whenever the person or entity posing the threat is specifically identifiable. The courts have therefore roundly—and rightly—rejected such an irrational result. *See Bank Markazi v. Peterson*, 136 S. Ct. 1310, 1328 (2016) (citing cases).[29] Indeed, in *Kaspersky*, the D.C. Circuit upheld against a bill of attainder claim a statute that prohibited the use of a single company's products, given Congress's security concerns about that specific company. *See* 909 F.3d at 459.

Moreover, as explained above, Congress had good reason to apply Section 889 to Huawei (and the other named companies) first, while providing for additional designations in the future. While Huawei and ZTE "may not be the only two companies" posing risks to U.S. telecommunications systems, "they are the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States." HPSCI Rep., at 8. Huawei itself touts its stature and, in particular, the diversity and power of its offerings, ranging from the provision of smart phone devices to the management of physical platforms, like buildings, factories, production lines, and utilities. *See* Huawei 2018 Rep., at 20. Congress also recognized that "vertically integrated industry giants like Huawei and ZTE provide a wealth of opportunities" for mischief, whether during product development or in the provision of software updates or other support services, HPSCI Rep., at 3—opportunities that are only increasing with the ever-expanding IoT, *see supra* § BG.I.C. Moreover, numerous experts and executive branch officials warned Congress, in reports and testimony spanning more than a decade, of Huawei's potential ties to, and obligation to cooperate with, the Chinese government. *See id.* It was therefore "rational" for Congress to identify Huawei specifically in acting to address the specified threat. *SBC Commc'ns*, 154 F.3d at 243 (finding it "rational

[29] Indeed, as discussed below, while Huawei relies heavily on Chief Justice Warren's statements in *Brown*, as well as Justice Breyer's concurrence in *Plaut*, in support of its theory that Congress is limited to enacting only "generally applicable laws," Pls.' Mot. 27, 33, the Fifth Circuit has called *Brown* "somewhat aberrant," *SBC Comm'ns*, 154 F.3d at 242, and specifically rejected such an "amorphous" theory, explaining that the argument set forth in Justice Breyer's concurrence was "squarely and specifically contradicted" by the six-vote majority in *Plaut*, *see id.* at 246.

to subject [operating companies] to additional burdens" because they could "exercise bottleneck control" over long-distance calls in more cases than other companies). And the inclusion of a provision permitting DoD to apply the prohibitions in Section 889 to future companies with ties to the Chinese government underscores that the statute's purpose is to counter a persistent threat, not to punish a particular company. *See Nixon*, 433 U.S. at 472; *Kaspersky*, 909 F.3d at 459-60 (noting significance of broader provision directing further study of the Russian cyber-threat and the possibility of Congress expanding the statute's prohibition to other companies); *Fresno Rifle*, 965 F.2d at 724 (where statute provided process for future designations of "assault weapons," purpose was not to punish the named manufacturers but to control types of weapons).

C. The Legislative Record of Section 889 Does Not Show Congressional Intent to Punish.

Where Huawei fails to show that Section 889 constitutes legislative punishment under either of the first two factors, Huawei cannot substantiate its attainder claim based on the third factor because it falls well short of identifying the "unmistakable evidence of punitive intent" required to do so. *SBC Commc'ns*, 154 F.3d at 243. The third, or "motivational," factor asks "whether the legislative record evinces a congressional intent to punish." *Selective Serv.*, 468 U.S. at 852. With respect to this factor, the Supreme Court has cautioned that "[j]udicial inquir[y] into Congressional motives [is] at best a hazardous matter" and that "the presumption of constitutionality" that attaches to a congressional enactment "forbids ... [a] reading of the statute's setting which will invalidate it over that which will save it." *Flemming v. Nestor*, 363 U.S. 603, 617 (1960). Accordingly, "only the clearest proof" will render a statute unconstitutional based on congressional intent. *Id.* "[I]solated statements" do not suffice. *Selective Serv.*, 468 U.S. at 856; *see also SBC Commc'ns*, 154 F.3d at 243 (similar).

As discussed, the text and legislative record of Section 889 demonstrate that Congress's motive in enacting Section 889 was prophylactic, not punitive. The HPSCI Report expressed congressional concerns that the use of Huawei products on U.S. networks could be exploited by the Chinese

government to the detriment of national and informational security. *See supra* § BG.I.B. Similar concerns were echoed in numerous governmental and expert reports and at various committee hearings. *See* § BG.I.C. And nine senior executive branch officials indicated in congressional testimony that they do not, and would not, use Huawei products due to the security risks they pose. *See id.* In the months leading up to the passage of Section 889, these concerns, reports, and testimony were cited in earlier versions of Section 889 and by Members on the House and Senate floors. *See* § BG.II.A. The text of the statute as enacted shows Congress was seeking to address these concerns by targeting the products most vulnerable to the threat of Chinese government exploitation. *See* § BG.II.B. "While it is always risky trying to determine congressional intent," *In re Miller*, 570 F.3d 633, 639 n.12 (5th Cir. 2009), here, the thrust of Congress's motivation is clear: Congress passed Section 889 to address longstanding concerns that Huawei products on U.S. networks could be exploited by the Chinese government to the detriment of national and informational security at federal expense.

In the face of all this evidence, Huawei largely relies on the statements of five Senators to support its view that Congress's motivation for enacting Section 889 was really "to punish Huawei for its alleged misdeeds and ties to the Chinese government and Communist party." Pls.' Mot. 23. That Huawei is straining to find evidence of punitive intent is evidenced by the fact that the majority of the statements it cites are taken out of context. To better understand the context surrounding the statements that Plaintiffs cite, some unpacking is in order. In June of 2018, the U.S. Government and ZTE reached a superseding settlement agreement, part of which suspended penalties the Commerce Department had imposed on ZTE two months prior for violating U.S. export control laws. *See* 83 Fed. Reg. 34825 (July 23, 2018), 17644 (Apr. 23, 2018). The Senate version of the NDAA originally included a provision to reinstate those penalties and undo the superseding settlement agreement. *See* H.R. Rep. No. 115-874, at 918-19 (2018). That Senate provision was struck in conference, *see id.*, and Section 889 as enacted does not include it, *see* ECF 28-5. The majority of the statements Plaintiffs cite

to support the supposed "*unmistakable* intent to punish *Huawei*," Pls.' Mot. 23 (emphasis added), actually relate to an earlier Senate provision responding to risks posed by *ZTE*, *see id.* (same) (citing 164 Cong. Rec. S3897 (highlighted "death penalty" statement of Sen. Cotton actually referring to earlier ZTE provisions); *id.* (highlighted "slap on the wrist" statement of Sen. Van Hollen referring to same); *id.* at S3938 (highlighted statement of Sen. Blumenthal about violations of U.S. law referring to same); ECF 28-10 at 83 (highlighted "hammer" statement of Sen. Schumer referring to same), *see* 164 Cong. Reg. S3396 (June 11, 2018)).[30] Read in context, these statements do not suffice to establish congressional intent to punish *Huawei*, where they were not directed at Huawei and refer to a provision Congress ultimately omitted from the statute. *See, e.g., Council of & for the Blind of Delaware Cty. Valley, Inc. v. Regan*, 709 F.2d 1521, 1530 (D.C. Cir. 1983) (explaining that "the version of [the statute] ultimately adopted by Congress reflects ... legislative intent").

Huawei is thus left to rely on what can only be characterized as a "smattering" of legislative statements insufficient to establish punitive intent, *ACORN*, 618 F.3d at 141 (finding statements of nearly ten legislators allegedly showing punitive intent to be insufficient "smattering"). *See* Pls.' Mot. 23. Among the Senators Huawei identifies as having punitive intent, the overall emphasis of their statements throughout the legislative record was that the use of Huawei's products created a risk of cyber-interference by the Chinese government and that action needed to be taken to address that vulnerability. *See* ECF 28-10 at 82 (stmt. of Sen. Rubio) (explaining that Huawei's "links to the Chinese government and Communist Party" "pose a serious threat to Americans' national security" because its products "are used for espionage and intellectual property theft"); ECF 28-11 at 87 (S3897) (stmt. of Sen. Cotton) (explaining that allowing Huawei "products into our country's critical communications

[30] Similarly, Huawei cites statements of Senators Schumer and Rubio that are not referring to the NDAA at all. *See* Pls.' Mot. 22 (citing ECF 28-6 at 54 (Schumer referring to FCC measure)); *id.* at 23 (citing ECF 28-13 at 94 (Rubio referring to proposed restrictions on buying U.S. products)).

infrastructure"—"[w]hether it is routers, switches, or any other kind of equipment"—"would give the Chinese Government a backdoor into our first responder networks, our electric grid, and a lot more than that"). And even if the isolated statements of a handful of Senators could be read to suggest that *they* were motivated to punish Huawei, such "isolated references in congressional debate" are insufficient to establish that Congress—"as a whole"—was so motivated. *SBC Commc'ns*, 154 F.3d at 243. To the contrary, where the text of Section 889 and the legislative record as a whole clearly manifest Congress's prophylactic purposes, even the handful of senatorial statements Huawei cites, no matter how spun, fall well short of "the 'smoking gun' evidence of punitive intent necessary to establish a bill of attainder." *SBC Commc'ns*, 154 F.3d at 243.

II. SECTION 889 DOES NOT VIOLATE THE DUE PROCESS CLAUSE.

Huawei also fails to show that Section 889 deprives the company of its rights under the Fifth Amendment's Due Process Clause. Huawei does not specify whether its due process claim is rooted in an alleged violation of substantive or procedural due process. Whatever the theory, precedent shows that either avenue is foreclosed here. Procedural due process claims are unavailable as to congressional statutes because the legislative process set forth in Article I of the Constitution is all that is due a plaintiff adversely affected by a federal law. *See Bi-Metallic Inv. Co. v. State Bd. of Equalization*, 239 U.S. 441, 445 (1915) (rights of those affected by statutes "are protected in the only way that they can be in a complex society, by their power, immediate or remote, over those who make the rule"); *cf. Atkins v. Parker*, 472 U.S. 115, 130 (1985) ("A welfare recipient is not deprived of due process when the legislature adjusts benefit levels.... The legislative determination provides all the process that is due."). As for substantive due process, the Supreme Court has long ago settled that economic regulations like section 889 are subject to rational basis review and presumed constitutional. *Williamson v. Lee Optical of Okla., Inc.*, 348 U.S. 483, 487-88 (1955) ("The day is gone when this Court uses the Due Process Clause of the Fourteenth Amendment to strike down state laws, regulatory of business

and industrial conditions, because they may be unwise, improvident, or out of harmony with a particular school of thought."). Huawei does not even try to argue that Section 889 fails this deferential standard. *See, e.g.*, *Cornerstone Christian Schs. v. Univ. Interscholastic League*, 563 F.3d 127, 139 (5th Cir. 2009) (under rational basis review, a regulation must be upheld "if there is any reasonably conceivable state of facts that could provide a rational basis" for the regulation).

Huawei's Fifth Amendment claim hinges entirely on the contention that Section 889 is "selective legislation." Pls.' Mot. at 28–29. Huawei's position is untenable. As discussed, the Supreme Court has rejected as "flawed" the "assumption that legislation must be generally applicable" or that there is "something wrong with particularized legislative action." *Bank Markazi*, 136 S. Ct. at 1327; *see also SBC*, 154 F.3d at 232 (upholding statute imposing line-of-business restrictions on named corporations). The *Bank Markazi* Court approvingly cited authorities upholding "as a valid exercise of Congress' legislative power diverse laws that governed one or a very small number of specific subjects." *Id.* at 1328. *Bank Markazi* involved a very particularized statute indeed: it "designate[d] a particular set of assets and render[ed] them available to satisfy the liability and damages judgments underlying a consolidated enforcement proceeding that the statute identifies by the District Court's docket number." *Id.* at 1317. Yet, the legislation survived constitutional scrutiny. And contrary to Huawei's argument, Pls.' Mot. 31, neither the Supreme Court's statements in *Plaut*, *see* 514 U.S. at 239 n.9, nor *Bank Markazi*, 136 S. Ct. at 1316-17, were limited to private bills, *i.e.*, laws providing benefits to specified individuals. Both cases establish that Congress can legislate with specificity without violating the Constitution, including the Due Process Clause.[31]

[31] Indeed, a due process claim on this basis makes little sense where punishment is a necessary element to make out a bill of attainder and it is not enough that a statute applies to specific individuals. *See Nixon*, 433 U.S. at 471-72. If due process prohibited specific statutes, it would seem to render the Bill of Attainder Clause superfluous. Unsurprisingly, the Supreme Court has never held that a bill of attainder, or a specific statute that does not operate as punishment, violates due process due to its specificity alone.

III. SECTION 889 DOES NOT VIOLATE THE VESTING CLAUSES.

Lastly, Huawei argues that Section 889 violates separation-of-powers principles because in passing Section 889, Congress exercised powers assigned by the vesting clauses to the executive and judicial branches. The only authority Huawei marshals in support of its amorphous theory are two quotations plucked from decades-old Supreme Court cases, divorced from their relevant context. Pls.' Mot. at 32-33 (quoting *Fletcher v. Peck*, 10 U.S. 87, 136 (1810); *Brown*, 381 U.S. at 443). Beyond these context-free quotations, Huawei merely cites legal commentaries and concurring opinions from Supreme Court justices, notably Justice Breyer's one-Justice concurrence in *Plaut*, 514 U.S. at 241.

The Fifth Circuit heard just such an argument, based on the same authorities, over 20 years ago and soundly rejected it—a fact Huawei fails to mention. The Court of Appeals in *SBC* heard the argument that the allegedly problematic aspects of the statute under challenge, including its "specificity" and its "near-punitive nature," "when added together somehow amount[ed] to a separation-of-powers violation that is greater than the sum of its parts." *SBC Commc'ns*, 154 F.3d at 246. The court held that such an "amorphous" theory "must fail" and, in so holding, rejected reliance on the identical authorities Huawei attempts to invoke now:

> Although this argument finds appealing rhetorical support in the more sweeping statements of some of the Court's older cases, including particularly the admonition offered by Justice Marshall in *Fletcher* and seconded by Chief Justice Warren in *Brown* that "[i]t is the peculiar province of the legislature to describe general rules for the government of society; the application of those rules to individuals in society would seem to be the duty of other departments," *see Brown,* 381 U.S. at 446 ... it is squarely and specifically contradicted by *Plaut*. In that case, Justice Breyer raised a very similar argument in his one-vote concurrence.... Justice Scalia's six-vote majority opinion soundly rejected it.... *Id.* at 246.

Moreover, the Supreme Court has held that this kind of argument rests on an "archaic view of the separation of powers as requiring three airtight departments of government." *Nixon*, 433 U.S. at 443. Instead, "the proper inquiry focuses on the extent to which" the actions of one branch prevents another "from accomplishing its constitutionally assigned functions" and "[o]nly where the potential for disruption is present must we then determine whether that impact is justified by an

overriding need to promote objectives within the constitutional authority of Congress." *Id.* Section 889 does not prevent the other branches from accomplishing their constitutionally assigned functions, and Huawei fails to explain how it could be construed to. By contrast, the results of the other cases Huawei cites are fully consistent with that rule, as well as the fact that those cases involved particular and well-defined constitutional rules that were violated by the statutes under challenge. *Zivotofsky ex rel. Zivotofsky v. Kerry*, 135 S. Ct. 2076, 2096 (2015) (holding "the power to recognize foreign states resides in the President alone" and "[t]o allow Congress to control the President's communication in the context of a formal recognition determination is to allow Congress to exercise that exclusive power itself"); *Bowsher v. Synar*, 478 U.S. 714, 722-23 (1986) ("direct congressional role in the removal of officers charged with the execution of the laws" violates the separation of powers in light of the Constitution's express provision for the removal of U.S. officers only upon impeachment and conviction by the House and Senate); *I.N.S. v. Chadha*, 462 U.S. 919, 957-58 (1983) (legislative veto is inconsistent with "the express procedures of the Constitution's prescription for legislative action," which exist to "check" both the executive and legislative branches). In enacting Section 889, Congress did not exercise any authority expressly assigned to another branch or impede another branch from accomplishing its functions and thus did not violate the separation of powers.

IV. THE NAMED AGENCY DEFENDANTS SHOULD BE DISMISSED.

The seven named agency defendants should be dismissed for the independent reason that Huawei brings "a facial challenge to the constitutionality of section 889," Pls.' Mot. 9, and do not challenge an action of any of the agencies. *See Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 62 (2004).

CONCLUSION

For the foregoing reasons, the Court should dismiss Plaintiffs' Complaint, Fed. R. Civ. P. 12(b)(6), or, in the alternative, grant summary judgment to Defendants on all claims, and deny Plaintiffs' motion for summary judgment, Fed. R. Civ. P. 56(a).

Dated: July 3, 2019

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

JOSEPH D. BROWN
United States Attorney

JAMES GILLINGHAM
Assistant U.S. Attorney
Eastern District of Texas
110 N. College Avenue; Suite 700
Tyler, Texas 75702
E-mail: James.Gillingham@usdoj.gov
(903) 590-1400
(903) 590-1346 (fax)
Texas State Bar # 24065295

JOSHUA M. RUSS
Assistant U.S. Attorney
Eastern District of Texas
101 Park Blvd.; Suite 500
E-Mail: Josh.M.Russ@usdoj.gov
(972) 509-1201
(972) 509-1209 (fax)
Texas State Bar # 24074990

DIANE KELLEHER
ERIC R. WOMACK
Assistant Branch Directors

/s/ Emily Newton
EMILY SUE NEWTON (Va. Bar No. 80745)
JAMES R. POWERS (TX Bar No. 24092989)
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Washington, DC 20005
Telephone: (202) 305-8356
Fax: (202) 616-8470
E-mail: emily.s.newton@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

HUAWEI TECHNOLOGIES USA, INC., & HUAWEI TECHNOLOGIES CO., LTD.,

Plaintiffs,

v.

UNITED STATES OF AMERICA, *et al.*,

Defendants.

Civil No. 4:19-cv-00159

[PROPOSED] ORDER

Having carefully considered the motion for summary judgment filed by Plaintiffs, Huawei Technologies USA, Inc. and Huawei Technologies Co., Ltd., and the motion to dismiss or, in the alternative, for summary judgment and opposition to Plaintiffs' motion for summary judgment filed by Defendants, the United States of America and Emily Webster Murphy, Administrator of the General Services Administration, Alexander Acosta, Secretary of the U.S. Department of Labor, Alex Azar II, Secretary of the U.S. Department of Health and Human Services, Betsy DeVos, Secretary of the U.S. Department of Education, Sonny Perdue, Secretary of the U.S. Department of Agriculture, Robert Wilkie, Secretary of the U.S. Department of Veterans Affairs, and David L. Bernhardt, Secretary of the U.S. Department of the Interior, and for good cause shown, it is hereby:

ORDERED that Plaintiffs' motion for summary judgment is **DENIED**, and further

ORDERED that Defendants' motion to dismiss [for summary judgment] is **GRANTED**.