U.S. Department of Commerce

Securing the Information and Communications Technology and Services Supply Chain

(RIN 0605-AA51)

Regulatory Impact Analysis & Final Regulatory Flexibility Analysis

As required by Executive Order 12866, and the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq*., the Department of Commerce has prepared the following regulatory impact analysis (RIA) and final regulatory flexibility analysis (FRFA) for the interim final rule titled, "Securing the Information and Communications Technology and Services Supply Chain" (the Rule).

It is important to note that the estimates of the economic impact of this Rule are based on the best available information to the Department. Realized costs of the Rule will vary depending on a number of factors, such as the number of initial assessments and first consultations, as well as the number of transactions that are prohibited or mitigated. Nonetheless, this analysis represents the Department's best estimate of the economic impacts of the Rule, based on information currently available.

I. Regulatory Impact Analysis

Need for regulatory action

The reasons for and need for this action are articulated in the interim final rule, and are summarized here. As the Department of Homeland Security (DHS) noted in its "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report," (2019) (the ICT Supply Chain Report), at 6, "[Information and Communications Technology (ICT)] is one of the largest areas of economic activity on the planet." The U.S. Government and

critical infrastructure owners and operators of ICT contribute $500 billion annually in ICT investment.

Also, as noted in Executive Order 13873, “foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services.” DHS cautions that the market growth of ICT has increased the risk to the ICT supply chain, and the number of attacks on the ICT supply chain, such as through exploiting vulnerabilities in third-party software, hardware, and services, has increased over 50 percent annually over the last several years. ICT Supply Chain Report, at 6.

Currently, transactions involving Information and Communications Technology and Services (ICTS) that are designed, developed, manufactured, or supplied by certain foreign persons subject to the jurisdiction or direction of foreign adversaries are not reviewed or scrutinized by any U.S. entity. Moreover, private parties engaging in ICTS transactions with foreign parties consider only the private risks and may lack the information, expertise, and incentive to evaluate and internalize the potential National Security risks involved in ICTS transactions with foreign parties. In its ICT Supply Chain Report, DHS further noted that some private parties may in fact not disclose suspect suppliers or supplier behavior out of fear of putting themselves or others at risk, legally, from governments or other private entities. ICT Supply Chain Report, at 15. Consequently, as noted above, in recent years malicious actors have successfully: hijacked cellular devices, infected switch flash cards, pre-installed malware on end

user devices, sold counterfeit ICT to U.S. armed forces, and embedded malware within software security tools.

Recognizing that the market might not provide an optimal solution to the potential risk and harm to the ICTS supply chain, and that the general public is also potentially negatively impacted by these risks, whether they are realized or not, the President issued Executive Order 13873 in order to empower the Secretary of Commerce to create a mechanism to identify and review ICTS transactions, and potentially prevent or modify them, in order to counter the potential harms to the United States' infrastructure, citizens, economy, or industry that such transactions may present. This Rule implements that order and seeks to protect the safety and welfare of the United States and the ICTS supply chain.

Affected Entities

As ICTS is defined by this Rule, it includes any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including through transmission, storage, or display. Although the term ICTS is continually evolving with modernization, it broadly encompasses products and services under the Telecommunications and Computer sectors. Using research from Dun and Bradstreet's First Research, the Department estimates that the combined annual revenue of the Telecommunications industry (equipment manufacturing, services, and resellers) exceeds $670 billion. The U.S. computer manufacturing industry has combined annual revenue of about $24 billion.

To determine the industry sectors affected by the Rule, the Department conducted an in-depth analysis of the commodities and services that are considered to be part of the ICTS sector

and ICTS-related industries in the U.S. economy. The Department also considered characteristics such as the extent of outsourcing in telecommunications manufacturing, as impacted industries may import components manufactured by the six countries deemed to be adversaries for the purposes of the Executive Order.

The Department created a list of 35 ICTS sectors that include industries likely affected by the Rule from the North American Industrial Classification System (NAICS) (Table 1). Generally, the Department identified the Telecommunications sector as three subsectors: equipment manufacturers, services providers, and resellers. Equipment manufacturers include telecommunications equipment manufacturers that produce equipment used in telephone, data, broadcasting, and wireless communications networks. Companies in the telecommunications services sector operate and/or provide access to facilities for the transmission of voice and sound, data, text, and video via wired, wireless, and satellite networks. Resellers of telecommunication services purchase network access and capacity from telecommunication service providers and resell telecommunication services to household and business users.

Table 1. Information and Communications Technology and Services Sectors by 2017 NAICS Codes

List of Impacted Industries/Commodities		
Ct	**NAICS**	**Definition**
1	**334111**	Electronic Computer Manufacturing
2	**334112**	Computer Storage Device Manufacturing
3	**334118**	Computer Terminal and Computer Peripheral Equipment Manufacturing
4	**334210**	Telephone Apparatus Manufacturing
5	**334220**	Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing
6	**334290**	Other Communications Equipment Manufacturing
7	**334310**	Audio and Video Equipment Manufacturing
8	**334412**	Bare Printed Circuit Board Manufacturing
9	**334413**	Semiconductor and Related Device Manufacturing
10	**334416**	Capacitor, Resistor, Coil, Transformer, and Other Inductor Manufacturing
11	**334417**	Electronic Connector Manufacturing
12	**334418**	Printed Circuit Assembly (Electronic Assembly) Manufacturing
13	**334419**	Other Electronic Component Manufacturing
14	**334511**	Navigational, Measuring, Electromedical, and Control Instruments Manuf
15	**334513**	Instruments & Related Products to Manufacture, Display, & Control Industrial Process Variables
16	**334613**	Blank Magnetic and Optical Recording Media Manufacturing
17	**334614**	Software and other Prerecorded Compact Disc, Tape, and Record Reprod
18	**335921**	Fiber Optic Cable Manufacturing
19	**335929**	Other Communications and Energy Wire Manufacturing
20	**511210**	Software Publishers
21	**515111**	Radio Networks
22	**515112**	Radio Stations
23	**515120**	Television Broadcasting
25	**515210**	Cable and Other Subscription Programming
24	**517311**	Wired Communication Carriers
26	**517312**	Wireless Telecommunications Carriers (except Satellite)
27	**517410**	Satellite Telecommunications
28	**517911**	Telecommunications Resellers
29	**517919**	All Other Telecommunications
30	**518210**	Data Processing, Hosting, and Related Services
31	**519130**	Internet Publishing and Broadcasting and Web Search Portals
32	**541511**	Custom Computer Programming Services
33	**541512**	Computer Systems Design Services
34	**541513**	Computer Facilities Management Services
35	**541519**	Other Computer Related Services

Companies in the computer industry manufacture computers, such as mainframes, servers, personal computers (PCs), workstations, and mobile PCs (laptops, netbooks, and tablets), as well as computer peripheral equipment, including storage devices, terminals, biometric readers, and input/output devices such as printers, monitors, and keyboards.

Computer manufacturers typically assemble PCs from components bought from other manufacturers. Key components like motherboards are specially made for a product, while disk drives and other components may be off-the-shelf parts. Manufacturers of specialized devices like printers, monitors, and hard disk drives may also buy some components from outside vendors. The manufacture of some products requires highly sophisticated machinery.

According to the latest data from the Census Bureau, the 35 identified NAICS codes industries accounted for 4 percent of total employment and 8 percent of total annual payrolls in the United States in 2017.[1] For the 19 manufacturing sectors included in the list, they represented 4.2 percent of total manufacturing shipments, 18 percent of total manufacturing imports, 5.2 percent of total manufacturing employment, and 7 percent of total manufacturing payroll in the United States in 2016.[2]

Number of Affected Entities

The Department estimated both a lower and upper bound for the number of entities affected by the Rule. To derive the lower bound estimate, the Department first identified a core group of the most directly affected companies, then added members of the major industry

[1] Statistics of U.S. Business https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html
[2] Annual Survey of Manufactures https://www.census.gov/programs-surveys/asm.html

associations that the Department believes would be most directly affected by the Rule. Combining the core group of companies with the total membership of the directly affected associations resulted in nearly 262,000 companies being impacted by the Rule. The Department used Bloomberg to explore the relationships of these companies and found over 700 comparable firms to the core group of the most directly affected companies. This core group also included over 50 publicly listed companies, while Bloomberg reported quantified supplier and/or customer exposures (i.e., reported transactions) for over 2,400 suppliers and over 2,800 buyers for the publicly listed companies. Therefore, the Department estimates that approximately 268,000 companies will be directly impacted by this Rule.

The upper bound estimate is based on a count of firms that import significant amounts of the goods and services subject to review under the Rule. As noted above, using 2018 data available to the Department, the Department identified NAICS industries that imported $100 million or more ICTS goods or services using the 35 industries in table 1, indicated above. The Department then counted the number of firms in these industries using 2017 Census data. According to this analysis, there are approximately 4,533,000 firms that import a significant amount of goods and services potentially subject to review under the Rule. Thus, the Department estimates that the number of affected entities will be between 268,000 and 4,533,000 firms.

It is possible that some of the 268,000 to 4,533,000 affected firms do not source ICTS goods and services from the six foreign governments deemed to be adversaries for the purposes of this Executive Order. The Department is not aware of any data on country-level imports at the firm level that would allow the exclusion of entities that do not import ICTS goods and services from these six countries. However, in line 2 of Table 2 (and by extension, line 2 in Tables 3 and

4) the Department has estimated the share of potentially impacted entities likely to incur costs from the Rule. This estimate accounts for the fact that of the 268,000 to 4,533,000 potentially impacted entities, some number of those entities may not import ICTS goods and services from foreign adversaries.

Wage Rates in Relevant Labor Categories of Affected Entities

The Department understands that the administrative compliance burden borne by affected entities will depends on the wage rates for two labor categories: operational managers and lawyers. The Department estimates that most of the duties related to administrative compliance, including reading this Rule, developing and implementing a compliance plan, and complying with any national security investigations, will be performed by these types of employees.

The Department estimated the wage rates using May 2019 hourly wage estimates from the Bureau of Labor Statistics (BLS), doubled to account for overhead and benefits. According to BLS data, as of May 2019, operational managers earned $59.15 per hour on average, and lawyers earned $69.86 per hour on average. Thus, the Department estimates wage rates at approximately $118 per hour for operational managers, and $140 per hour for lawyers, inclusive of overhead and benefits, for all administrative compliance cost estimates in the following section.

The costs to the Government of implementing the Rule are similar, and specifically include the wages of attorneys and investigative agents needed to identify the transactions of concern and how best to investigate and pursue those. To enforce the Rule, the Department estimates that it will require the work of two special agents, both at the GS-13 level, one attorney

at the GS-15 level, and a half of a full time equivalent (FTE) employee to provide administrative and information services assistance. This staff would be engaged in the administration of the Rule, but particularly in the forms of serving subpoenas and investigating violations of the Rule. Other tasks, such as audits and similar activities, would be performed by other FTEs, and this estimate therefore only applies to the specific enforcement activities referenced. Note as well that the costs may vary because the total required work hours are uncertain, since the workload for enforcement for this type of executive order is unprecedented. Additionally, this estimate includes the costs of intelligence support for operations, which constitute $500,000 of the estimated per-case costs.

Administrative Compliance Burden on U.S. Companies

To assess the administrative compliance burden on U.S. companies, the Department organized its methodology into four sections: (1) learning about the Rule; (2) developing a compliance plan; (3) implementing a compliance plan; (4) compliance with national security investigations. The Department also considered other costs, such as compliance with mitigation agreements, which are addressed below.

Learning about the Rule

The first expected costs to businesses are those associated with business learning about the Rule, and what it requires. The Department expects that this task will largely be accomplished by the businesses' lawyers and operations managers. The Department's estimate for the cost to businesses of learning about the Rule is further derived from estimates of the number of firms potentially impacted by the Rule, the share of potentially impacted firms likely to devote time and resources to learning about the Rule, the number of hours needed to read and

learn about the Rule, and the wages of the employees tasked with learning about the Rule. Table 2 provides a detailed breakdown of the framework for estimating these costs.

Table 2: Framework for Estimating Costs Associated with Learning about the Rule

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the Rule	268,000	4,533,000	Low estimate is based on a supply chain analysis of a core group of companies and members in industry associations directly affected by the Rule. High estimate is based on an analysis of industries that import significant amounts of the goods and services covered by the Rule.
2	Share of potentially impacted entities likely to devote time and resources to learning about the Rule	0.5	0.9	At the low end we estimate half of potentially impacted entities will devote time and resources towards learning about the Rule. This assumes a large number of potentially impacted entities do not source ICTS goods and services from countries deemed to be foreign adversaries. At the high end we estimate nearly all (90%) of potentially impacted entities will devote time and resources towards learning about the Rule.
3	Entities learning about the Rule	134,000	4,079,700	Line 1 * Line 2
4	Operations manager hours	2	2	This is an estimate of how long it is likely to take an operations manager to read and understand the Rule.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity	237	237	Line 4 * Line 5
7	Lawyer hours	10	10	This is an estimate of how long it is likely to take a lawyer to read and understand the Rule.

8	Lawyer hourly wage, doubled to account for benefits and overhead ($)	140	140	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
9	Lawyer cost per entity	1,397	1,397	Line 7 * Line 8
10	Total initial cost per entity to learn about Rule ($)	1,634	1,634	Line 6 + Line 9
11	Total initial cost to learn about Rule ($)	218,929,200	6,665,413,860	Line 3 * Line 10
12	Annualized cost per entity over 10 years at 7% rate ($)	233	233	Line 10 is a one time cost per firm to learn about the Rule. Line 12 annualizes that one time cost over 10 years at a 7% discount rate.
13	Annualized cost per entity over 10 years at 3% rate ($)	192	192	Line 10 is a one time cost per firm to learn about the Rule. Line 13 annualizes that one time cost over 10 years at a 3% discount rate.
13	Total annualized costs at 7% discount rate ($)	31,170,593	949,004,980	Line 3 * Line 12
14	Total annualized costs at 3% discount rate ($)	25,665,181	781,389,844	Line 3 * Line 13

Developing a Compliance Plan

Once companies learn about the Rule, they will need to develop compliance plans for their operations. Developing these plans include the costs associated with analyzing supply chain risks, determining how to manage those risks, and related due diligence for transactions subject to investigation under the Rule. Specifically, the Department anticipates that due diligence activities will include: 1) identifying the equipment, software and services procured in transactions potentially subject to investigation, prohibition, or mitigation under the Rule; 2) identifying the sources (companies, company owners, and countries) of any items in the supply chain identified in step 1; 3) analyzing the risks associated with the transactions identified above

being investigated and potentially prohibited; and 4) identifying alternative suppliers to prepare for the possibility of a transaction being prohibited, or that might be part of a mitigation agreement.

These anticipated costs were derived from the Department's experience and on comments received from industry, which indicated that they would likely need to perform these kinds of analyses and due diligence. To estimate the cost of developing a compliance plan, the Department estimated the number of firms likely impacted by the Rule, the share of potentially impacted firms likely to devote time and resources to developing a plan, the number of hours needed to develop a plan, and the wages of the employees tasked with developing a plan. A detailed breakdown of the framework for estimating these costs can be found in Table 3.

Table 3: Framework for Estimating Costs Associated with Developing a Plan

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the Rule	268,000	4,533,000	Low estimate is based on a supply chain analysis of a core group of companies and members in industry associations directly affected by the Rule. High estimate is based on an analysis of industries that import significant amounts of the goods and services covered by the Rule.
2	Share of potentially impacted entities likely to devote time and resources to developing a plan	0.3	0.7	We start with our estimate of entities that are likely to read and learn about the Rule of 50 to 90 percent. Entities that do not learn about the Rule are unlikely to develop a plan. In addition, some entities that learn about the Rule will not develop a plan, either due to resource constraints or because a system is already in place to be in compliance. Thus, these estimates are slightly lower than the 50 to 90 percent estimate in Table 2.

3	Entities developing a plan	80,400	3,173,100	Line 1 * Line 2
4	Operations manager hours	80	80	This is an estimate of how long it is likely to take an operations manager to develop a plan for conducting supply chain risk management analysis and related due diligence for transactions that may be subject to investigation.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity	9,464	9,464	Line 4 * Line 5
7	Total initial cost to develop a plan	760,905,600	30,030,218,400	Line 3 * Line 6
8	Annualized cost per entity over 10 years at 7% rate ($)	1,347	1,347	Line 6 is a one time cost per firm to develop a plan. Line 8 annualizes that one time cost over 10 years at a 7% discount rate.
9	Annualized cost per entity over 10 years at 3% rate ($)	1,109	1,109	Line 6 is a one time cost per firm to develop a plan. Line 9 annualizes that one time cost over 10 years at a 3% discount rate.
10	Total annualized costs at 7% discount rate ($)	108,335,839	4,275,627,502	Line 3 * Line 8
11	Total annualized costs at 3% discount rate ($)	89,201,349	3,520,457,716	Line 3 * Line 9

Implementing the Plan

Once the impacted entities have learned about the Rule and developed their compliance plans, they will incur additional costs implementing the compliance plan. This would likely entail putting into action the steps outlined above. Specifically, for each transaction, the Department expects firms will identify equipment, software and the services potentially subject

to investigation, identify the sources of these items, analyze the risks associated with each transaction, and identify alternative suppliers.

Unlike the costs associated with learning about the Rule and developing a compliance plan, which are estimated to be onetime costs, the costs estimated for implementing the plan recur annually. This estimate for implementation costs is derived from estimates of the number of firms impacted by the Rule, the share of potentially impacted firms likely to implement a compliance plan, the number transactions potentially subject to the Rule that the average firm conducts annually, the number of hours needed to perform analysis and due diligence on each transaction, and the wages of the employees performing these tasks. A detailed breakdown of the framework for estimating these costs can be found in Table 4.

Table 4: Framework for Estimating Costs Associated with Implementing a Compliance Plan

Line	Item	Low Estimate	High Estimate	Basis for Estimate
1	Entities potentially impacted by the Rule	268,000	4,533,000	Low estimate is based on a supply chain analysis of a core group of companies and members in industry associations directly affected by the Rule. High estimate is based on an analysis of industries that import significant amounts of the goods and services covered by the Rule.
2	Share of potentially impacted entities likely to implement a plan	0.3	0.7	We expect all entities that develop a plan will implement the plan. Thus, these estimates are identical to those in Table 3.
3	Entities implementing a plan	80,400	3,173,100	Line 1 * Line 2
4	Number of transactions subject to	5	20	This is an estimate of the number of transactions likely to be subject to investigation in a given year. It is based

	the Rule per firm per year			on an estimate of the number of foreign suppliers at an average firm.
5	Operations manager hours to perform analysis and due diligence per transaction	2	2	This is an estimate of the number of hours we expect would be needed to perform analysis and due diligence for each transaction.
6	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
7	Operations manager cost per transaction	237	237	Line 5 * Line 6
8	Operations manager annual cost per entity ($)	1,183	4,732	Line 4 * Line 7
9	Total annual cost ($)	95,113,200	15,015,109,200	Line 3 * Line 8

Compliance with Investigations

Finally, the Department expects some firms will incur costs associated with compliance with investigations once they have been initiated. Under the investigatory provisions in this Rule, an investigation will include the following steps. First, the Secretary will make an initial assessment of whether an ICTS transaction falls under the scope of the Rule, and whether it may pose an undue risk of sabotage or subversion to the information and communications technology and services supply chain and critical infrastructure in the United States, or that pose an unacceptable risk to U.S. national security or the safety of U.S. persons. Second, for transactions that are initially determined to fall within the Rule's scope, and that the Secretary deems may pose an undue risk of sabotage or subversion to the information and communications technology and services supply chain and critical infrastructure in the United States, or that pose an unacceptable risk to U.S. national security or the safety of U.S. persons., parties to that transaction will receive a notice of the initial assessment and possibly an instruction to place the transaction in abeyance, while retaining all records relating to the transaction. Following the

initial assessment, the Secretary will consult with the appropriate agency heads, prior to making a preliminary determination of whether the transaction must be stayed pending further evaluation, mitigated if it is to continue, or prohibited. Notice of the preliminary determination will be sent to the parties involved, who will be allowed an opportunity to oppose the preliminary determination. Upon consideration of any information submitted in opposition to the preliminary determination, the Secretary, in consultation with the appropriate agency heads, will make a final determination of whether the transaction will be prohibited, not prohibited, or permitted pursuant to the adoption of mitigation measures.

Each of these steps has costs associated with it. The costs for some steps may be less than others; for example, there will be no direct costs to firms from the Secretary initiating an investigation. Additionally, the costs of retaining records may be minimal, since the requirement is only that they retain records they otherwise would in the normal course of business. The costs for other actions, however, many be significant; at one extreme, prohibiting a transaction may entail very high costs involved with unwinding a transaction, finding a new supplier, and negotiating a new contract, as necessary. Even mitigation agreements may result in additional costs for a transaction, since they may involve new negotiations for goods or services.

The Department's estimate of the cost to firms for these actions does not rely on estimates of the number of firms impacted by the Rule. Rather, it is derived from estimates of the number of investigations per year, the number of hours needed to comply with the investigations, and the wages of the employees tasked with complying with the investigations. A detailed breakdown of the framework for estimating these costs can be found in Table 5.

Table 5: Framework for Estimating Costs Associated with Compliance with Investigations

Line	Item	Low Estimate	High Estimate	Basis for Estimate
1	Number of investigations per year	1	250	Low estimate is based on the assumption that firms will likely avoid transactions that they deem to be at risk for investigation. High estimate is based on the assumption that the Department of Commerce devotes a high level of resources towards investigations
2	Operations manager hours to respond to and cooperate with each investigation	160	160	We estimate approximately one month of work.
3	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
4	Operations manager cost per investigation ($)	18,928	18,928	Line 2 * Line 3
5	Lawyer hours per investigation	160	160	We estimate approximately one month of work.
6	Lawyer hourly wage, doubled to account for benefits and overhead ($)	140	140	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
7	Lawyer cost per investigation ($)	22,355	22,355	Line 5 * Line 6
8	Total cost per investigation ($)	41,283	41,283	Line 7 + Line 4
9	Total annual cost ($)	41,283	10,320,800	Line 8 * Line 1

The Department has broken out the costs, using the methodology described above, to estimate compliance costs associated with the Rule's implementation. Costs categories are summarized in Tables 6 and 7. These costs are estimated to be between $1 billion and $52 billion, with a point estimate of $26 billion, in the first year following implementation of the Rule, and between $95 million and $15 billion, with a point estimate of $8 billion, in subsequent years. This implies annualized costs of between approximately $235 million and $20 billion,

with a point estimate of $10 billion, using a 7% discount rate, and annualized costs of between approximately $210 million and $19 billion, with a point estimate of $10 billion, using a 3% discount rate. Realized costs will depend on the factors described above, such as the number of transactions that are reviewed, the number of firms that will in fact change their behavior to comply with the Rule, and the number of transactions that are prohibited or mitigated as a result of the Rule.

Table 6: Estimates for the Cost of the ICTS Supply Chain Rule (Annualized at 7%)

Aggregate Costs to Businesses (Annualized at 7%)	Low Estimate	High Estimate	Point Estimate
1. Learning about the Rule (annualized at 7%)	$31,170,593	$949,004,980	$490,087,786
2. Developing a plan (annualized at 7%)	$108,335,839	$4,275,627,502	$2,191,981,671
3. Implementing the plan	$95,113,200	$15,015,109,200	$7,555,111,200
4. Compliance with potential investigations	$41,283	$10,320,800	$5,181,042
Total (annualized at 7%)	$234,660,915	$20,250,062,482	$10,242,361,699

Table 7: Estimates for the Cost of the ICTS Supply Chain Rule (Annualized at 3%)

Aggregate Costs to Businesses (Annualized at 3%)	Low Estimate	High Estimate	Point Estimate
1. Learning about the Rule (annualized at 3%)	$25,665,181	$781,389,844	$403,527,512
2. Developing a plan (annualized at 3%)	$89,201,349	$3,520,457,716	$1,804,829,533
3. Implementing the plan	$95,113,200	$15,015,109,200	$7,555,111,200
4. Compliance with potential investigations	$41,283	$10,320,800	$5,181,042
Total (annualized at 3%)	$210,021,013	$19,327,277,560	$9,768,649,287

Potential Economic Impact of the Rule

The economic impact of the Rule will depend on the industry sectors affected by the Rule and the extent to which these industries are dependent on imports, since the Rule seeks to create a framework to mitigate, prohibit and unwind particular ICTS transactions involving foreign adversaries.

Imports accounted for over 50 percent of the total supply of 6 out of 14 ICT sectors, as shown in Table 8. The sector with the greatest single share of U.S. supply accounted for by imports was *Audio and video equipment manufacturing* at 91 percent. Among communications equipment, 77 percent of total *Broadcast and wireless communication equipment supply*, and 60 percent of total *Telephone apparatus manufacturing* supply in the United States, originated abroad. For most computer related equipment and components on the list--notably, *Electronic computer manufacturing* and *Computer terminals, other computer peripheral equipment manufacturing*--imports accounted for over 80 percent of supply. By contrast, for *Printed circuit assembly (electronic assembly) manufacturing*, less than 10 percent of U.S. supply originates abroad. (Table 8)

Table 8. Value of Imports as a Share of U.S. ICT Supply in 2018

BEA Code	Description	Total
334111	Electronic computer manufacturing	86%
334112	Computer storage device manufacturing	52%
334118	Computer terminals, other computer peripheral equipment manufacturing	81%
334210	Telephone apparatus manufacturing	60%
334220	Broadcast and wireless communications equipment	77%
334290	Other communications equipment manufacturing	27%
334300	Audio and video equipment manufacturing	91%
33441A	Other electronic component manufacturing	44%
334413	Semiconductor and related device manufacturing	44%
334418	Printed circuit assembly (electronic assembly) manufacturing	1%
334511	Search, detection, and navigation instruments manufacturing	11%
334513	Industrial process variable instruments manufacturing	32%
334610	Manufacturing and reproducing magnetic and optical media	15%
335920	Communication and energy wire and cable manufacturing	32%
	Total	**58%**

Source: DOC calculations.

U.S. imports of ICT related goods were supplied by a relatively small number of exporting nations. Fifteen foreign exporters (14 individual countries plus the European Union) accounted for at least 95 percent of total U.S. ICT related goods imports in 2018.

Combined, the six nations named by the Secretary as foreign adversaries for the purpose of the Executive Order accounted for over one-half of U.S. imports of *Electronic computer manufacturing, Computer terminals and other computer peripheral equipment manufacturing, Telephone apparatus manufacturing,* and *Broadcast and wireless communications equipment* (Table 9).[3] All four of these sectors have products for which over 50 percent of U.S. imports originated from names adversaries. The named adversaries also accounted for over 40 percent of U.S. imports of *Other communications equipment manufacturing, Communication and energy wire and cable manufacturing,* and *Other electronic component manufacturing.*

Table 9. Shares of ICT and Related Equipment Imports in 2018 From Adversary Nations

	Partners -> China, Cuba, Iran, North Korea, Russia, Venezuela		Combined Share
U.S. BEA Industry Codes	**334111**	Electronic computer manufacturing	58.0%
	334112	Computer storage device manufacturing	13.7%
	334118	Computer terminals, other computer peripheral equipment manufacturing	53.2%
	334210	Telephone apparatus manufacturing	67.3%
	334220	Broadcast and wireless communications equipment	64.2%
	334290	Other communications equipment manufacturing	42.3%
	334300	Audio and video equipment manufacturing	49.3%
	33441A	Other electronic component manufacturing	45.6%
	334413	Semiconductor and related device manufacturing	15.8%
	334418	Printed circuit assembly (electronic assembly) manufacturing	19.7%
	334511	Search, detection and navigational instruments manufacturing	12.1%
	334513	Industrial process variable instruments manufacturing	11.8%
	334610	Manufacturing and reproducing magnetic and optical media	4.6%
	335920	Communication and energy wire and cable manufacturing	42.4%

[3] The trade data by partner used here includes imports for final consumption and imports used by firms in their production process.

Source: DOC calculations.

The overall impact of the Rule will be determined by which ICT products and transactions are included and by the countries designated as foreign adversaries. For transactions involving products and services covered by the Rule, the impact will be the greatest for industries that intensively use ICT products imported from designated foreign adversaries in their production processes. Mitigation and prohibition measures may involve substituting those products with inputs from other sources, potentially at a higher cost. There may be upstream impacts as domestic producers of the restricted import may experience reduced competition and a greater demand for their products, resulting in higher prices for the upstream producers. However, the increased price for the upstream products will then increase the production costs for firms in the affected sectors. Thus, the restriction of imports from adversarial nations will likely increase production costs of these firms as they substitute higher priced alternatives for restricted imports.

In addition, other firms in the same industry, even those which did not engage in transactions affected by the Rule, may face higher production costs as they compete for a reduced supply of available inputs. As these firms' input costs increase, the prices of their products may also increase, resulting in fewer sales, a smaller quantity produced, and lower profits. As a result, an entire industry subject to a designated transaction may experience a loss of producer surplus and lower profits.

The impacts of the Rule are not confined to the firms in the industries that produce the products subject to the Rule. Users of ICT products, whether they be consumers of final products or firms downstream purchasing ICT as intermediate inputs, may face higher prices for the products they purchase. For consumers, the higher prices result in lower consumer surplus. For

the downstream firms, costs of production and the prices of their products may increase, and the quantity produced may decline.

The potential impact on an industry's supply chain can be illustrated with an example for the *Broadcast and wireless communications equipment* industry. Other ICT industries that rely on this industry for intermediate inputs are the *Broadcast and wireless communications equipment, Telephone apparatus manufacturing,* and *Other communication equipment manufacturing* industries. In addition, industries outside the ICT sector that use inputs produced by the *Broadcast and wireless communications equipment* industry include *Guided missile and space vehicle manufacturing*, and *Automatic environmental control manufacturing*.

Similarly, the outputs of the *Telephone apparatus manufacturing* industry are used as inputs by several industries, such as *Wired telecommunications carriers, Wireless telecommunications carriers (except satellite), Satellite and telecommunications resellers,* and *All other telecommunications.*

In addition to the costs associated with higher prices for inputs, there are other costs that could be associated with the Rule. For example, if a system can be shut down by the Federal government, investors (public and private) will likely to take extra time to ensure that the system they are purchasing or designing has a low risk of being subject to the Rule at any point in the future. The additional time spent in evaluating and potentially modifying purchases or designs could result in delays in the completion of projects. These delays could also impose costs on consumers, who might have to continue to use outdated systems while the testing and analysis is underway. Moreover, delays may result in investors requiring a higher expected return before

providing financial backing for potentially risky products or technology, thereby increasing the cost of acquiring and or producing a system.

Consequently, if the Rule resulted in restricted imports in the affected sectors, higher prices and lower consumer and producer surplus is likely to arise among many inter-related industries as higher priced goods replace imports from designated adversaries.

Benefits of the Rule

ICTS has become integral to the daily operations and functionality of U.S. critical infrastructure, as well as many, if not most, of U.S. industry. Moreover, ICTS accounts for a large part of the U.S. economy. Accordingly, if vulnerabilities in the ICT supply chain—composed of hardware, software, and managed services from third-party vendors, suppliers, service providers, and contractors—are exploited, the consequences can affect all users of that technology or service, potentially causing serious harm to critical infrastructure, U.S. Government operations, and disrupting the U.S. and the global economy. These harms are already occurring. As noted in Executive Order 13873, "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services."

More specifically, U.S. entities – persons, companies, and governments - purchasing and incorporating ICTS equipment, and using ICTS services such as network management or data storage, provided by foreign adversaries can create multiple opportunities for foreign adversaries to exploit potential vulnerabilities in the ICTS. That, in turn, could cause direct and indirect harm

to both the immediate targets of the adverse action and to the U.S. as a whole. While attacks can originate from remote foreign sources, incorporation of a foreign adversary's software, equipment, and products into domestic ICTS networks, as well as the use of use of foreign cloud, network management, or other services, greatly increases the risk that potential vulnerabilities may be introduced, or that they may be present without being detected. These potential vulnerabilities are often categorized under the general concepts of threats to privacy, data integrity, and denial of service.

In the area of privacy, foreign actors are known to exploit the sale of software and hardware to introduce vulnerabilities that can allow them to steal critical intellectual property, research results (e.g. health data), or government or financial information from users of the software or hardware. Such vulnerabilities can be introduced at the network, cloud service or individual product data, allow traffic monitoring or surveillance, and be resistant to detection by private purchasers or telecommunications carriers. Once detected, the existence of such vulnerabilities may be extremely costly or impossible to remediate.

Vulnerabilities to data integrity can be created by including an adversary's hardware and software into U.S. networks and systems. This incorporated hardware and software could then pose opportunities to add or remove important information, modify files or data streams, slow down, or otherwise modify the normal transmission or availability of data across U.S. networks. Such capabilities could be exercised in areas as diverse as financial market communications, satellite communications or control, or other sensitive consumer information. For example, hypothetically, a foreign adversary could disrupt the U.S. economy by using access to

transmission or processing of data in automated or algorithmic trading on major stock or similar exchange to delay or distort trades. Such trading and privileged access to market movement and trends, or other manipulation, could disrupt and harm the operation of major exchanges.

A foreign adversary could also exploit vulnerabilities provided by the incorporation of hardware and software into U.S. environments by fully or partially closing down critical networks or functions at key times. These types of attacks are known as denial of service attacks. Such attacks could cause widespread problems, such as if they occur during periods of crisis, or they could be used selectively by targeting individual corporations, infrastructure elements, or other important infrastructure functions. They could also be masked to make the source of the disruption difficult to attribute, and therefore difficult to trace and perhaps stop.

Such risks can be substantially increased by incorporating the software and equipment from unreliable adversaries into the U.S. telecommunications infrastructure. However, these risks are not necessarily confined to infrastructure environments. They could, for example, be present in the use of cloud services, as well as in the widespread use of consumer devices such as handsets, networked surveillance cameras, drones or other Internet of Things devices.

The costs of these attacks on the ICTS supply chain and on ICTS used by or for the benefit of the U.S. Government is unknown, but the number of attacks by foreign adversaries on the ICTS supply chain are known to be increasing. These costs are not simply borne by the U.S. Government, either. Most private industry uses ICTS or is involved in the ICTS supply chain at some point, so any disruption to that supply chain increases costs to those firms, to consumers, and to the U.S. Government. Because any serious disruption to the ICTS supply chain would

affect all users of ICTS, and because the impacts of these disruptions is incalculable but likely, even at present, very large, the benefits of this Rule are significant. However, they are also incalculable. The Government cannot know at this time the types of malicious actions that will be directed at the ICTS supply chain, nor the potential or actual impact of those events prior to them occurring. Nonetheless, given the ubiquity of ICTS in the modern economy and especially in critical infrastructure, the benefits of preventing significant disruptions or harms to the ICTS supply chain would be very high, and would likely outweigh the costs associated with the Rule identified above.

This Rule provides a process through which many of the direct and indirect costs to the telecommunications infrastructure and to users of ICT products and services in the U.S. can be avoided or ameliorated. It provides the means of bringing to bear the information and analytical resources of the U.S. government to address supply chain issues before they arise, and which may be beyond the means of individual telecommunications carriers or other U.S. ICTS purchasers or users to address on their own. As noted above, the costs associated with the potential attacks, loss of service, or disruption to the ICTS supply chain are not known at this time, and are in actuality unknowable due to the generally clandestine nature of the attacks and the fact that they may or may not occur. However, by deterring, preventing, or mitigating these attacks, this rule will provide the United States with substantial, though unknowable, economic benefits as well as benefits to the national security of the United States.

Regulatory Alternatives

The Department considered several alternatives to this regulation to reduce the cost. For example, the Department considered excluding certain sectors and functions of ICTS

transactions with the intent to narrow the regulatory scope of the Rule while still protecting National Security. Specifically, the Department examined the feasibility of excluding: (1) ICTS Transactions that involve only the acquisition of commercial items as defined by Federal Acquisition Regulation Part 2.101; (2) ICTS Transactions that are used solely for the purpose of cybersecurity mitigation or legitimate cybersecurity research; and (3) ICTS Transactions under which a United States person is subject to a security control agreement, special security agreement, or proxy agreement approved by a cognizant security agency to offset foreign ownership, control, or influence pursuant to the National Industrial Security Program regulations (32 C.F.R. part 2004).

Ultimately, however, the Department decided against adding the above regulatory alternatives. The exclusion process for specific exemptions could inadvertently allow similar yet suspicious transactions to be cleared, undermining the Rule's National Security objectives. For instance, a company that is headquartered in a foreign adversary country may, to some extent, be involved in legitimate cybersecurity research and development initiatives performed under the National Cooperative Research and Production Act, 15 U.S.C. §§ 4301-06, and the foreign company may study foreign equipment to gain insights on new innovations or potential network security risks. However, that same company may also be conducting operations during other ICTS transactions that could harm U.S. National Security interests. The Department sought to remove both the possibility for confusion as well as the ability for malicious actors to argue that some legitimate cybersecurity research performed by a company would exempt all cybersecurity research by a company, legitimate or otherwise. For that and other reasons contained herein, the Department determined that the Rule should specifically identify types of ICTS Transactions that

likely most affect U.S. National Security, rather than exempting classes of ICTS Transactions from review under the Rule.

II. Final Regulatory Flexibility Analysis

The Department has examined the economic implications of the Rule on small entities as required by the Regulatory Flexibility Act (RFA). The RFA requires an agency to describe the impact of a rule on small entities by providing a regulatory flexibility analysis. The Department published an initial regulatory flexibility analysis in the proposed rule issued on November 27, 2019 (84 FR 65316) and now publishes a final regulatory flexibility analysis. This final rule is likely to have a significant economic impact on a substantial number of small entities.

A statement of the significant issues raised by public comments or by the Chief Counsel for Advocacy of the Small Business Administration in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments.

Many commenters discussed the possibility that this Rule could present significant economic costs. For example, Comment [DOC-2019-0005-0019] stated that "Commerce's proposed Rules would result in an extremely broad and unprecedented increase in regulatory jurisdiction over private ICT transactions. The Notice [of proposed rulemaking] thus marks a watershed regulatory moment for companies in or adjacent to the ICT market – which is to say, virtually every company in United States – given the government's newfound stance that it can determine key terms of what ICT companies can buy, sell, or use. As a result, this proceeding and the rules that result from it inescapably will impose additional costs on ICT companies, such as the increased practical need – even absent a legal requirement – to document supply chain risk

management analysis in the event a transaction is investigated, along with related due diligence to consider the as-yet uncertain possibilities for government intervention." As discussed above, in the Regulatory Impact Analysis (RIA), the Department estimated costs associated with developing and implementing a plan to conduct due diligence on potentially covered transactions, including estimating the number of small entities that could be affected by the Rule and the economic impact on those small entities.

Statement of the Objectives of, and Legal Basis for, the Final Rule

A description of this Rule, why it is being implemented, the legal basis, and the purpose of this Rule are contained in the **SUMMARY** and **SUPPLEMENTARY INFORMATION** sections of this preamble, as well as in the preamble to the Notice of Proposed Rulemaking issued on November 27, 2019 (84 FR 65316), and are not repeated here.

A Description and, Where Feasible, Estimate of the Number of Small Entities to Which the Final Rule Applies

Small Business Administration (SBA) size standards for businesses are based on annual receipts and average employment. For the purpose of this analysis we define a small business as one employing fewer than 500 persons. This definition allows us to use 2017 Census data on firm employment by NAICS industry to estimate the number of affected small entities.

In the RIA discussed above, the Department identified 4,533,000 firms that imported significant amounts of goods and services potentially subject to review under the Rule. This formed our upper bound estimate for the total number of affected entities. By replicating this

methodology with firm employment data, the Department finds that 4,516,000 of these firms, about 99.6 percent, have less than 500 employees. Assuming the lower bound estimate of 268,000 affected entities is also made up of 99.6 percent small businesses, the Department estimates that between 266,995 and 4,516,000 small businesses will be potentially affected by this Rule.

Federal Rules That May Duplicate, Overlap or Conflict with the Final Rule

The Department did not identify any federal rules that duplicates, overlaps, or conflicts with this Rule.

Description and Estimate of Economic Effects on Entities, by Entity Size and Industry

In the Costs section of the RIA, the Department estimates that costs to all affected entities will range between approximately $235 million and $20.2 billion (annualized at 7%), or about $2,800 to $6,300 per entity. The Department estimated the costs to small entities using the same methodology. All small entity calculations and assumptions can be found in Tables 10 through 14 below. These tables are analogous to Tables 2 through 7, above. While most of the assumptions below are identical to those found in the previous estimates, there are three important adjustments to assumptions in the small entity cost estimates:

1. Entities potentially impacted by the Rule reduced by 0.4 percent to account for our finding that 99.6 percent of all affected entities have less than 500 employees.
2. Small entities are less likely to have the resources to develop and implement a compliance plan. This analysis thus reduces estimates of the share of small firms likely to engage in these activities accordingly.

3. Small entities engage in fewer transactions than large entities. This analysis reduces the estimates of the number of transactions subject to the Rule per small firm accordingly.

As a result of these adjustments, the Department estimates that costs to affected small entities will range between approximately $109 million and $10.9 billion, or about $1,800 and $3,900 per small entity.

Table 10: Estimates for the Annualized Cost of the ICTS Supply Chain Rule to Small Entities

Costs to Businesses (Aggregated)	Low estimate	High estimate
1. Learning about the Rule (annualized at 7%)	$24,842,956	$840,396,400
2. Developing a plan (annualized at 7%)	$71,953,033	$3,651,079,474
3. Implementing the plan	$12,634,200	$6,410,913,600
4. Compliance with potential investigations	$41,283	$10,320,800
Total (annualized at 7%)	$109,471,472	$10,912,710,274

Table 11: Framework for Estimating Costs to Small Entities Associated with Learning about the Rule

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the Rule	266,995	4,516,000	We found that 99.6% of potentially affected firms have less than 500 employees, so we lower the estimates in line 1 of tables 3, 4 and 5 by 0.4%.
2	Share of potentially impacted entities likely to devote time and resources to learning about the Rule	0.4	0.8	We assume small businesses are less likely than large businesses to read the Rule, so we lower our estimates slightly from those found in table 2.
3	Entities learning about the Rule	106,798	3,612,800	Line 1 * Line 2
4	Operations manager hours	2	2	This is an estimate of how long it is likely to take an operations manager to read and understand the Rule.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity	237	237	Line 4 * Line 5
7	Lawyer hours	10	10	This is an estimate of how long it is likely to take a lawyer to read and understand the Rule.
8	Lawyer hourly wage, doubled to account for benefits and overhead ($)	140	140	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
9	Lawyer cost per entity	1,397	1,397	Line 7 * Line 8
10	Total initial cost per entity to learn about Rule ($)	1,634	1,634	Line 6 + Line 9
11	Annualized cost per entity over 10 years at 7% rate ($)	233	233	Line 10 is a onetime cost per firm to learn about the Rule. Line 11 annualizes that onetime cost over 10 years at a 7% discount rate (following FDAs precedent).
12	Total annualized costs ($)	24,842,956	840,396,400	Line 3 * Line 11

Table 12: Framework for Estimating Costs to Small Entities Associated with Developing a Plan

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the Rule	266,995	4,516,000	We found that 99.6% of potentially affected firms have less than 500 employees, so we lower the estimates in line 1 of tables 3, 4 and 5 by 0.4%.
2	Share of potentially impacted entities likely to devote time and resources to developing a plan	0.2	0.6	We assume small businesses are less likely than large businesses to develop a plan, so we lower our estimates slightly from those found in table 3.
3	Entities developing a plan	53,399	2,709,600	Line 1 * Line 2
4	Operations manager hours	80	80	This is an estimate of how long it is likely to take an operations manager to develop a plan for conducting supply chain risk management analysis and related due diligence for transactions that may be subject to investigation.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity	9,464	9,464	Line 4 * Line 5
7	Annualized cost per entity over 10 years at 7% rate ($)	1,347	1,347	Line 6 is a onetime cost per firm to learn about the Rule. Line 7 annualizes that onetime cost over 10 years at a 7% discount rate (following FDAs precedent).
8	Total annualized costs ($)	71,953,033	3,651,079,474	Line 3 * Line 7

Table 13: Framework for Estimating Costs to Small Entities Associated with Implementing a Compliance Plan

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the Rule	266,995	4,516,000	We found that 99.6% of potentially affected firms have less than 500 employees, so we lower the estimates in line 1 of tables 3, 4 and 5 by 0.4%.
2	Share of potentially impacted entities likely to implement a plan	0.2	0.6	We assume small businesses are less likely than large businesses to implement a plan, so we lower our estimates slightly from those found in table 4.
3	Entities implementing a plan	53,399	2,709,600	Line 1 * Line 2
4	Number of transactions subject to the Rule per firm per year	1	10	We assume small businesses engage in fewer transactions than large businesses, so we lower our estimates slightly from those found in table 4.
5	Operations manager hours to perform analysis and due diligence per transaction	2	2	This is an estimate of the number of hours we expect would be needed to perform analysis and due diligence for each transaction.
6	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
7	Operations manager cost per transaction	237	237	Line 5 * Line 6
8	Operations manager annual cost per entity ($)	237	2,366	Line 4 * Line 7
9	Total annual cost ($)	12,634,200	6,410,913,600	Line 3 * Line 8

Table 14: Framework for Estimating Costs Associated with Compliance with Investigations

Line	Item	Low Estimate	High Estimate	Basis for Estimate
1	Number of investigations per year	1	250	Low estimate is based on the assumption that firms will likely avoid transactions that they deem to be at risk for investigation. High estimate is based on the assumption that the Department of Commerce devotes a high level of resources towards investigations
2	Operations manager hours to respond to and cooperate with each investigation	160	160	We estimate approximately one month of work.
3	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
4	Operations manager cost per investigation ($)	18,928	18,928	Line 2 * Line 3
5	Lawyer hours per investigation	160	160	We estimate approximately one month of work.
6	Lawyer hourly wage, doubled to account for benefits and overhead ($)	140	140	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
7	Lawyer cost per investigation ($)	22,355	22,355	Line 5 * Line 6
8	Total cost per investigation ($)	41,283	41,283	Line 7 + Line 4
9	Total annual cost ($)	41,283	10,320,800	Line 8 * Line 1

Potential Economic Impact of the Rule on Small Entities

Small businesses, as opposed to larger firms, may not have the same ability to deal with the burdens, both direct and indirect, associated with the Rule. Faced with the various costs associated with compliance, firms will have to absorb those costs and/or pass them along to their consumers in the form of higher prices. Either action will reduce the profits of firms. Due to their lack of market power, and their lower profit margins, small firms may find it difficult to pursue either or both of those responses while remaining viable.

A similar situation will hold with respect to the indirect impacts of the Rule. Small firms downstream of impacted industries are likely to face increases in the prices of ICT products they use as inputs and either absorb the increase in cost and/or raise their prices. Given this situation, it is possible that the Rule will have a more substantial adverse impact on small firms relative to

larger firms.

A Description of, and an Explanation of the Basis for, Assumptions Used

Small Business Administration (SBA) size standards for businesses are based on annual receipts and average employment. For the purpose of this analysis, the Department defines a small business as one employing fewer than 500 persons. This definition allows the Department to use 2017 Census data on firm employment by NAICS industry to estimate the number of affected small entities. The Department does not have access to sufficiently detailed data on firm employment and receipts to make use of the full set of SBA size standard thresholds.

The Department notes, however, that 84% of SBA employee thresholds are above 500, and 91% of SBA receipt thresholds are above $6 million. Census data show that average receipts for firms employing less than 500 employees are $2.2 million. Thus, using our threshold of 500 employees we estimate that 99.6% of affected entities are small businesses which is likely a slight underestimate.

Description of any Significant Alternatives to the Final Rule that Accomplish the Stated Objectives of Applicable Statutes and That Minimize any Significant Economic Impact of the Rule on Small Entities

This Rule will allow the Secretary to review ICTS transactions to determine whether they present an undue or unacceptable risk to the national security, a function which is currently not performed by any other private or public entity. As noted above, private industry often lacks the incentive, information, or resources to review their ICTS purchases for malicious suppliers or other potentially bad actors in the ICTS supply chain. The Federal Government is uniquely

situated to engage in this task and does not have the incentive or legal concerns that private actors in the ICTS supply chain might have.

The Department considered two regulatory alternatives to reduce the burden on small entities: 1) excluding small entities with 5 or fewer employees, and 2) excluding certain industries and sectors. However, the Department determined that neither of these two alternatives would achieve the goal of protecting the national security, nor would they eliminate the Rule's significant economic impact on a substantial number of small entities. First, the Department considered providing an exemption for small entities that have 5 or fewer employees. ("smallest entities"). According to the Census Bureau's most recent dataset of number of firms by employee count, about 61% of all firms have less than 5 employees. Second, the Department examined the feasibility of eliminating the application of the Rule to certain small entities involved in specific industries or sectors by excluding: (a) ICTS Transactions that involve only the acquisition of commercial items as defined by Federal Acquisition Regulation Part 2.101; (b) ICTS Transactions that are used solely for the purpose of cybersecurity mitigation or legitimate cybersecurity research; and (c) ICTS Transactions under which a United States person is subject to a security control agreement, special security agreement, or proxy agreement approved by a cognizant security agency to offset foreign ownership, control, or influence pursuant to the National Industrial Security Program regulations (32 CFR part 2004).

Ultimately, the Department decided against adopting either of these regulatory alternatives. Exempting certain industries or sectors or eliminating the application of the Rule to smallest entities could inadvertently allow potentially problematic transactions, that are

substantially similar to those conducted by non-exempt entities to avoid review, undermining the Rule's national security objectives. For example, a company that is headquartered in a foreign adversary country, regardless of its size or main industry sector, maybe involved in legitimate cybersecurity research and development initiatives performed under the National Cooperative Research and Production Act, 15 U.S.C. §§ 4301-06, and the foreign company may study foreign equipment to gain insights on new innovations or potential network security risks. However, that same company may also be conducting operations during other ICTS transactions that could harm U.S. national security interests. By promulgating the chosen alternative for the Rule, the Department sought to remove both the possibility for confusion as well as the ability for malicious actors to argue that some legitimate cybersecurity research performed by a company would exempt all cybersecurity research by a company, legitimate or otherwise. Thus, the Rule applies to types of ICTS Transactions most affecting U.S. national security as opposed to exempting entire industries, sectors, or regulated smallest entities from review.

Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 states that, for each rule or group of related rules for which an agency is required to prepare a FRFA, the agency shall publish one or more guides to assist small entities in complying with the rule, and shall designate such publications as "small entity compliance guides." The agency shall explain the actions a small entity is required to take to comply with a rule or group of rules.