


Next Page
OMB Control Number: 0694-0119 Expiration Date: December 31, 2020
NATIONAL SECURITY ASSESSMENT: USE OF SELECT SOFTWARE IN INFORMATION AND COMMUNICATIONS TECHNOLOGY

SCOPE OF ASSESSMENT
The U.S. Department of Commerce (DOC), Bureau of Industry and Security (BIS), Office of Technology Evaluation, is conducting a survey and assessment of the types of select security-related hardware and software products developed, manufactured, or marketed for use in information network devices and systems. The assessment covers a range of topics including technology sharing, information network devices incorporating software, software design, U.S. manufacturing, product end users, and related supply chain issues. Information on organization finances, capital expenditures, research and development spending is also collected for this assessment. The resulting aggregate data and subsequent analysis will allow the U.S. Government and industry to understand the extent to which certain types of information network technologies are employed in products sold by organizations operating in the United States. Additionally, this assessment will allow both public and private sector stakeholders to benchmark industry practices and raise awareness of any issues of concern.
RESPONSE TO THIS SURVEY IS REQUIRED BY LAW
A response to this survey is required by law (50 U.S.C. App. Sec. 2155). Failure to respond can result in a maximum fine of \$10,000, imprisonment of up to one year, or both. Information furnished herewith is deemed confidential and will not be published or disclosed except in accordance with Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C App. Sec. 2155). Section 705 prohibits the publication or disclosure of this information unless the President determines that its withholding is contrary to the national defense. Information will not be shared with any non-government entity, other than in aggregate form. The information will be protected pursuant to the appropriate exemptions from disclosure under the Freedom of Information Act (FOIA), should it be the subject of a FOIA request. Notwithstanding any other provision of law, no person is required to respond to nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB Control Number.
BURDEN ESTIMATE AND REQUEST FOR COMMENT
Public reporting burden for this collection of information is estimated to average 14 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information to BIS Information Collection Officer, Room 6883, Bureau of Industry and Security, U.S. Department of Commerce, Washington, D.C. 20230, and to the Office of Management and Budget, Paperwork Reduction Project (OMB Control No. 0694-0119), Washington, D.C. 20503.
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Table of Contents	
I	Cover Page
II	Table of Contents
III	General Instructions
A	Organization Information
Product & Service Overview	
1a	Information Network Products
1b	Suppliers of Software Technologies
1c	Sources of Software Content
1d	Hardware and Software Products Designed and Manufactured
1e	U.S. Information Network Products Containing Kaspersky Hardware and Software
1f	Collaboration and Development Activities
1g	Technologies Deployed & Terms of Technology License
1h	Technologies Used for Internal Business Operations
1i	End Uses - Critical Infrastructure
1j	End Users
1k	Operating Systems
1l	Modes of Accessing Technologies for Product Development
1m	Clones & Counterfeits
Hardware Product Integration	
2a	Technology Types/Version Numbers
2b	Functions-Capabilities/Methods
2c	Certs/Interfaces
2d	System Access/Data Access
2e	Functional Conditions for Kaspersky Technologies/Limits on Kaspersky in Systems
2f	Internal-External/Third Party Services
Software Product Integration	
3a	Technology Types/Version Numbers
3b	Functions-Capabilities/Methods
3c	Certs/Interfaces
3d	System Access/Data Access
3e	Functional Conditions for Kaspersky Technologies/Limits on Kaspersky in Systems
3f	Internal-External/Third Party Services
Hardware Telemetry Integration	
4a	Direct Communications, Types of Communications
4b	Receiving Methods, Returning Info
4c	Passive Indicators, All Indicators
Software Telemetry Integration	
5a	Direct Communications, Types of Communications
5b	Receiving Methods, Returning Info
5c	Passive Indicators, All Indicators
Tracking Practices	
6	Practices for Tracking Technologies Integrated into Products
Financial Information	
7a	Sales & Financial Information
7b	Research & Development and Capital Expenditures
Other Information	
8	Cybersecurity
9	Challenges and Outreach
10	Certification Page
X	Glossary
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act	

General Instructions	
A.	<p>Your organization is required to complete this survey on information network hardware and software-related products that your organization has developed, manufactured, or marketed since 2014. You must complete the survey using the DOC/BIS template which is Microsoft Excel based and can be downloaded from the secure Census Bureau portal: https://respond.census.gov/ICTsoftware</p> <p>If you are not able to download the survey document, at your request, BIS staff will e-mail the Excel survey template directly to you.</p> <p>For your convenience, a PDF version of the survey and required drop-down content is available on the BIS website to aid internal data collection. DO NOT SUBMIT the PDF version of the survey as your response to BIS. Should this occur, your organization will be required to resubmit the survey in the requested Excel format.</p>
B.	<p>Respond to every question. Surveys that are not fully completed will be returned for completion. Use the comment boxes to provide any information to supplement responses provided in the survey form. Make sure to record a complete answer in the cell provided, even if the cell does not appear to expand to fit all of the information. The survey includes an extensive glossary for your convenience, referring to the glossary while completing the survey is recommended. COMPLETE Section 1 before proceeding to respond to other parts of the survey as it drives auto-population functions supporting other survey sections and blocks out survey segments not pertinent to your organization.</p> <p>DO NOT CUT AND PASTE RESPONSES WITHIN THIS SURVEY. Survey inputs should be completed by typing in responses or by using a drop-down menu. The use of cut and paste can corrupt the survey template. If your survey response is corrupted as a result of cut and paste responses, a new survey will be sent to your organization for immediate completion.</p>
C.	<p>Do not disclose any classified information in this survey form.</p>
D.	<p>Submission of completed survey documents should be done through the secure Census Bureau portal: https://respond.census.gov/ICTsoftware Do not E-Mail surveys to BIS.</p>
E.	<p>Questions related to the survey should be directed to BIS survey support staff at softwaresurvey@bis.doc.gov</p> <p>E-mail is the preferred method of contact.</p> <p>You may also speak with a member of the BIS survey support staff by calling (202) 482-1688.</p>
F.	<p>For questions related to the overall scope of this National Security assessment, contact softwaresurvey@bis.doc.gov or:</p> <p>Jason Bolton, Program Manager, Industrial Studies Office of Technology Evaluation, Room 1093 U.S. Department of Commerce 1401 Constitution Avenue, NW Washington, DC 20230</p> <p>DO NOT submit completed surveys to Mr. Bolton's postal or personal e-mail address. All surveys must be submitted electronically to the secure Census Bureau portal.</p>
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act	

Organization Information

Provide the following information for this organization:

A.	Type of Company Response Facility/Organization Name Street Address City State Zip Code Website Phone Number	Corporate/Whole Organization Division/Business Unit Publicly Traded Privately Held	Point of Contact Regarding this Survey: Name Title Phone Number E-mail Address City State
-----------	--	---	---

B. Is your organization publicly traded or privately held? Yes No. If publicly traded, provide its stock ticker symbol.

Provide the following information for your parent organization(s), if applicable.

C.	Parent Organization #1 Parent Name Street Address City State/Province Country Postal Code/Zip Code	Parent Organization #2 Parent Name Street Address City State/Province Country Postal Code/Zip Code
-----------	--	--

Provide the following identification codes, as applicable, for your organization.

D.	Primary Data Universal Numbering System (DUNS) Code Primary NAICS Code (6-digit) Find DUNS codes at www.duns.com Find primary NAICS codes at www.naics.com Find CAGE codes at www.gsa.gov/cage	Primary Commercial and Government Entity (CAGE) Code Additional Commercial and Government Entity (CAGE) Code	Additional Commercial and Government Entity (CAGE) Code Additional Commercial and Government Entity (CAGE) Code
-----------	--	---	--

E. Indicate how your organization participates or plans to participate in 5G communication networks.

	Equipment	Software	Description of expected participation in 5G communication networks
Items to be used in 5G network infrastructure			
Items that will use/rely on 5G networks			

What key activities does your organization engage in to ensure that its supply chain is secure and supports the security of your organization's products?

What steps could the USG take to better enable your organization's use of suppliers that will help ensure its products' security?

Report the 1) Government agencies to which your organization sells hardware products, software products, and services; and 2) Estimate the percent of hardware and software products sold directly to government entities and the percent sold by resellers.

	Yes No	Yes No	Yes No				
Organization	Hardware Products	Software Products	Services	% of Total U.S. Sales Sold Directly to U.S. Organizations	% of Total U.S. Sales by Company Authorized Resellers	Comments	
F. Dept. of Defense							
Civilian U.S. Govt. Agencies							
State Governments							
Local Governments							
U.S. Regional Govt. Organizations							
U.S. Tribal Governments							
U.S. Territories (see Glossary)							

Comments:

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 1.a - Types of Information Network Products		1	2		3	4	5	
Product Category	Types of Hardware/Software Technologies	Designed	Manufactured	Distributed	Marketed	Marketed Products Made by Other Companies	Use Third-Party Companies to Procure the Products that This Organization Sells	Use Third-Party Companies to Service or Upgrade Products Sold by Your Organization
A.	Network Infrastructure Devices Routers - Home Office/Small Office Routers - Enterprise/Internet Service Provider Grade Switches - Home Office/Small Office Switches - Enterprise/Internet Service Provider Grade Small Office (not including switches/routers) Enterprise/Internet Service Provider Grade (not including switches/routers) Industrial (not including switches/routers) Internet of Things (IoT) (not including switches/routers) Gateways (not including switches/routers) Gateways - Other (not including switches/routers) Other [Define in Comment Box]							
B.	Network Security Devices Antivirus Scanning Application - Host Based Antivirus Scanning Appliances - Enclave Boundary (Gateway-based) Firewalls - Host Based Firewalls - Network Appliance Intrusion Detection Systems (IDS) Security Information and Event Management (SIEM) Web Proxies/Content Filtering Other [Define in Comment Box]							
C.	Intrusion Detection Host Intrusion Detection Network Intrusion Detection Host Intrusion Prevention Network Intrusion Prevention Systems (NIPS) Unified Threat Management (UTM) Systems Honeypot Network Tar Pit Solutions Data Loss Prevention (DLP) Data Recovery Other [Define in Comment Box]							
D.	Network Systems Virtual Private Network (VPN) Virtual Private Server (VPS) Virtualization Software - Bare Metal Hypervisor Virtualization Software - Work Station-Based Software Defined Networking (SDN) solution Other [Define in Comment Box]							
E.	Other Products Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked Computer Operating Systems Controller Devices Networked Storage Devices Networked Systems Printers-Copiers-Scanners Networked Printers Networked Scanners Health Management Systems - Network Connected Health Systems/Devices - Network Connected Physical Access Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Other [Define in Comment Box]							
Comments:								

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Both
None

Yes
No

Yes
No

Yes
No

Yes
No

Yes
No

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Both
None

Section 1.c - Sources of Software Content for Information Network Hardware & Software Products Designed and Manufactured, Licensing Practices, and Units Sold									
Instruction: Using drop-down responses accessed by clicking on the empty response cell, for each technology listed in the left column that was designed, manufactured, marketed, or distributed by your organization since 2014.									
1) State whether:									
A. the software used in your hardware and software products is:									
B. internally developed hardware products containing:									
C. internally developed software products containing:									
2) Estimate the number of U.S. and non-U.S. entities:									
3) For the identified types of products, state the number of units sold in the last year:									
[*Note: Respond to "Gateway" categories only where your organization has specific products specified as "Gateways" in the "Types of Hardware/Software" column.]									
Types of Hardware/Software	Hardware/Software Product Based on Internally Developed Software	Hardware/Software Product Internally Developed/Incorporating Known Open-Source Software	Hardware/Software Product Third-Party Proprietary Software	Hardware/Software Product Licensed/Shared	Number of Entities In the U.S. to Which Your Organization Has Licensed/Shared Its Technologies (Excludes Commercial, Institutional & Retail Sales)	Number of Entities Outside the U.S. to Which Your Organization Has Licensed/Shared Its Technologies (Excludes Commercial, Institutional & Retail Sales)	Number of Units Sold in Last Year - Hardware Products	Number of Units Sold in Last Year - Software Products	Comments
A. Network Infrastructure Devices									
Routers - Home Office/Small Office									
Routers - Enterprise/Internet Service Provider Grade									
Switches - Home Office/Small Office									
Switches - Enterprise/Internet Service Provider Grade									
Gateways - Home Office/Small Office (not including switches/routers)									
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)									
Gateways - Cloud (not including switches/routers)									
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)									
Gateways - Mobile Secure Gateways (not including switches/routers)									
Gateways - Other (not including switches/routers)									
Other [Define in Comment Box]									
B. Network Security Devices									
Antivirus Scanning Application - Host Based									
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)									
Firewalls - Host Based									
Firewalls - Network Appliance									
Firewalls - Cloud									
Firewalls - Virtualized									
Web Application Firewalls									
End Point Detection & Response (EDR)									
Deep Packet Inspection (DPI) Appliance									
Security Information and Event Management (SIEM)									
Web Proxies/Content Filtering									
Other [Define in Comment Box]									
C. Intrusion Detection/Prevention Systems									
Host Intrusion Detection (HIDS)									
Network Intrusion Detection Systems (NIDS)									
Host Intrusion Prevention Systems (HIPS)									
Network Intrusion Prevention Systems (NIPS)									
Unified Threat Management (UTM) Systems									
Honeypot									
Network Tar Pit Solutions									
Data Loss Prevention (DLP)									
Data Recovery									
Other [Define in Comment Box]									
D. Network Systems									
Virtual Private Network (VPN)									
Virtual Private Server (VPS)									
Virtualization Software - Bare Metal Hypervisor									
Virtualization Software - Work Station-Based Hypervisor									
Software Defined Networking (SDN) solutions									
Other [Define in Comment Box]									
E. Other Products									
Industrial Control Systems - Networked									
Supervisory Control and Data Acquisition (SCADA)-Networked									
Computer Operating Systems									
Computer Firmware									
Systems-On-Chip, Microcontroller Devices									
Memory and Data Storage Devices									
Mobile Device Operating Systems									
Multi-Function Devices - Printers-Copiers-Scanners									
Networked Printers									
Networked Scanners									
Health Management Systems - Network Connected									
Health Systems/Devices - Network Connected									
Physical Access Control Systems - Network Connected									
Physical Security Video Monitoring Systems - Network Connected									
Telepresence Systems (Audio & Video Conferencing Systems)									
Other [Define in Comment Box]									
Comments:									

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Other IP
Other

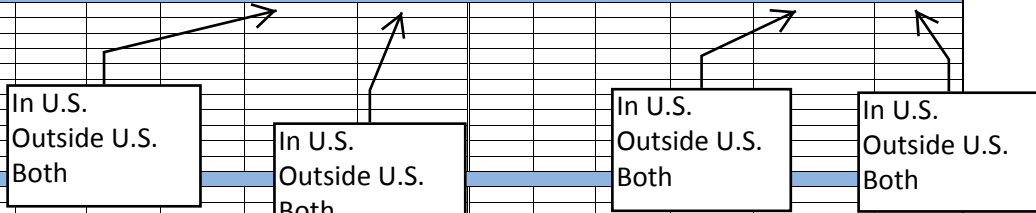
Section 1.d - Number of Hardware and Software Products Designed and Manufactured, Deployment Span, and Location

Instruction: Using drop-down responses accessed by clicking on the empty response cell, for each technology listed in the left column:

- 1) State the number of distinct hardware- and software-related products (models) that your organization has marketed/distributed since 2014.
- 2) Estimate the percentage of these products that were designed and manufactured externally outside of your organization-owned facilities.
- 3) State the in-service life of the specified hardware and software products.
- 4) Indicate whether the enabling software code for your hardware and software products is written at company or contractor sites located in the United States, outside of the United States, or both.

[Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways.]

Types of Hardware/Software Technologies	1		2		3		4		1		2		3		4	
	Number of Distinct Hardware Products	Estimated Percent of Hardware Products Designed Externally	Estimated Percent of Hardware Products Manufactured Externally	Estimated In-Service Life of Hardware Products Before Replacement - Number of Years	Company Locations where Enabling Product Software Code is Written	Contractor/Partner Locations where Enabling Product Software Code is Written	Number of Distinct Software Products	Estimated Percent of Software Products Designed Externally	Estimated Percent of Software Products Manufactured Externally	Estimated In-Service Life of Software Products Before Replacement - Number of Years	Company Locations where Enabling Product Software Code is Written	Company Contractor Locations where Enabling Product Software Code is Written				
A. Network Infrastructure Devices																
Routers - Home Office/Small Office																
Routers - Enterprise/Internet Service Provider Grade																
Switches - Home Office/Small Office																
Switches - Enterprise/Internet Service Provider Grade																
Gateways - Home Office/Small Office (not including switches/routers)																
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																
Gateways - Cloud (not including switches/routers)																
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																
Gateways - Mobile Secure Gateways (not including switches/routers)																
Gateways - Other (not including switches/routers)																
Other [Define in Comment Box]																
B. Network Security Devices																
Antivirus Scanning Application - Host Based																
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																
Firewalls - Host Based																
Firewalls - Network Appliance																
Firewalls - Cloud																
Firewalls - Virtualized																
Web Application Firewalls																
End Point Detection & Response (EDR)																
Deep Packet Inspection (DPI) Appliance																
Security Information and Event Management (SIEM)																
Web Proxies/Content Filtering																
Other [Define in Comment Box]																
C. Intrusion Detection/Prevention Systems																
Host Intrusion Detection (HIDS)																
Network Intrusion Detection Systems (NIDS)																
Host Intrusion Prevention Systems (HIPS)																
Network Intrusion Prevention Systems (NIPS)																
Unified Threat Management (UTM) Systems																
Honeypot																
Network Tar Pit Solutions																
Data Loss Prevention (DLP)																
Data Recovery																
Other [Define in Comment Box]																
D. Network Systems																
Virtual Private Network (VPN)																
Virtual Private Server (VPS)																
Virtualization Software - Bare Metal Hypervisor																
Virtualization Software - Work Station-Based Hypervisor																
Software Defined Networking (SDN) solutions																
Other [Define in Comment Box]																
E. Other Products																
Industrial Control Systems - Networked																
Supervisory Control and Data Acquisition (SCADA)-Networked																
Computer Operating Systems																
Computer Firmware																
Systems-On-Chip, Microcontroller Devices																
Memory and Data Storage Devices																
Mobile Device Operating Systems																
Multi-Function Devices - Printers-Copiers-Scanners																
Networked Printers																
Networked Scanners																
Health Management Systems - Network Connected																
Health Systems/Devices - Network Connected																
Physical Access Control Systems - Network Connected																
Physical Security Video Monitoring Systems - Network Connected																
Telepresence Systems (Audio & Video Conferencing Systems)																
Other [Define in Comment Box]																
Comments:																



BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 1.e - Types of U.S. Information Network Products Containing Kaspersky Hardware and Software									
Instruction: Identify the specific types of information network hardware and software products that your organization has designed, manufactured, marketed, or distributed since 2014 that incorporate or otherwise use any hardware, software, intellectual property or other technology sold or provided by Kaspersky Lab (all mentions of "Kaspersky" throughout the survey refer to Kaspersky Lab) or its designated distributors and resellers. Use comment boxes as necessary to describe organization actions. [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways.]									
Types of Hardware/Software Technologies	Activities Involving Network Products Utilizing Kaspersky Hardware/Software Products and Technologies					Marketed Under Your Organization's Name Products Made by Other Companies <i>(Use Comments box to identify manufacturers)</i>	Use Third-Party Companies to Procure the Products that your Organization Sells That Contain Kaspersky Technologies	Use Third-Party Companies to Service and Upgrade Products that your Organization Sells That Contain Kaspersky Technologies	Comments
	Use of Kaspersky Products/Technologies	Designed	Manufactured	Marketed	Distributed				
A. Network Infrastructure Devices									
Routers - Home Office/Small Office									
Routers - Enterprise/Internet Service Provider Grade									
Switches - Home Office/Small Office									
Switches - Enterprise/Internet Service Provider Grade									
Gateways - Home Office/Small Office (not including switches/routers)									
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)									
Gateways - Cloud (not including switches/routers)									
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)									
Gateways - Mobile Secure Gateways (not including switches/routers)									
Gateways - Other (not including switches/routers)									
Other [Define in Comment Box]									
B. Network Security Devices									
Antivirus Scanning Application - Host Based									
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)									
Firewalls - Host Based									
Firewalls - Network Appliance									
Firewalls - Cloud									
Firewalls - Virtualized									
Web Application Firewalls									
End Point Detection & Response (EDR)									
Deep Packet Inspection (DPI) Appliance									
Security Information and Event Management (SIEM)									
Web Proxies/Content Filtering									
Other [Define in Comment Box]									
C. Intrusion Detection/Prevention Systems									
Host Intrusion Detection (HIDS)									
Network Intrusion Detection Systems (NIDS)									
Host Intrusion Prevention Systems (HIPS)									
Network Intrusion Prevention Systems (NIPS)									
Unified Threat Management (UTM) Systems									
Honeypot									
Network Tar Pit Solutions									
Data Loss Prevention (DLP)									
Data Recovery									
Other [Define in Comment Box]									
D. Network Systems									
Virtual Private Network (VPN)									
Virtual Private Server (VPS)									
Virtualization Software - Bare Metal Hypervisor									
Virtualization Software - Work Station-Based Hypervisor									
Software Defined Networking (SDN) solutions									
Other [Define in Comment Box]									
E. Other Products									
Industrial Control Systems - Networked									
Supervisory Control and Data Acquisition (SCADA)-Networked									
Computer Operating Systems									
Computer Firmware									
Systems-On-Chip, Microcontroller Devices									
Memory and Data Storage Devices									
Mobile Device Operating Systems									
Multi-Function Devices - Printers-Copiers-Scanners									
Networked Printers									
Networked Scanners									
Health Management Systems - Network Connected									
Health Systems/Devices - Network Connected									
Physical Access Control Systems - Network Connected									
Physical Security Video Monitoring Systems - Network Connected									
Telepresence Systems (Audio & Video Conferencing Systems)									
Other [Define in Comment Box]									
Comments:									
<p>If your organization has not knowingly used Kaspersky Products/Technologies since 2014 (i.e. "no" was selected for every technology listed), certify in the box to the right via dropdown and proceed to section 6 of this survey.</p> <p>It is a criminal offense to willfully make a false statement or representation to any department or agency of the United States Government as to any matter within its jurisdiction (18 U.S.C. §1001).</p>									
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act									



Hardware
Software
Both
None
(Options for all drop-downs on this Tab are the same with the one exception at the bottom)

This organization has not used Kaspersky technologies or products since 2014



Section 1.f - Product and Services Collaboration and Development Activities With Kaspersky Laboratory Organizations

Instruction: 1) For all of the products or services listed in the left column that your organization, designs, manufactures, markets, or distributes:
 A) State whether your organization has engaged with Kaspersky since 2014 in any of the following categories:
 B) Indicate whether the use of Kaspersky technologies is required for the product.
 2) Identify all types of technology partnership programs that your organization is a provider of support services for Kaspersky products.
 [Partnership = Focused research, product development, technology exchanges involving otherwise collect commissions or other compensation for incorporation of Kaspersky tech
 *Note: Respond to "Gateway" categories only where your company designs, manufactures, markets, or distributes products or services that use Kaspersky technology to function, or use of Kaspersky technology with Products/Services Sold That Require Kaspersky Technology to Function, or Use of Kaspersky technology with Products/Services is Optional

Types of Technologies Offered by Your Organization that Involve Collaboration or Development With Kaspersky	Product Consulting Collaboration With Kaspersky	Product Design Collaboration with Kaspersky	Products at Customers' Request into Customer Organization's Hardware /Software Products	Other	Functional Development		Technology Partnership	Kaspersky Affiliate Program	Distribute Kaspersky Products	Provide Support Services for Kaspersky Products	Other (Use Comment Box)	Comments
					Yes	No						
A. Network Infrastructure Devices												
Routers - Home Office/Small Office												Yes No
Routers - Enterprise/Internet Service Provider Grade												
Switches - Home Office/Small Office												
Switches - Enterprise/Internet Service Provider Grade												
Gateways - Home Office/Small Office (not including switches/routers)												
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)												
Gateways - Cloud (not including switches/routers)												
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)												
Gateways - Mobile Secure Gateways (not including switches/routers)												
Gateways - Other (not in list)												
Other (Define in Comment Box)												
B. Network Security Devices												
Antivirus Scanning Applications												
Antivirus Scanning Appliances												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
Endpoint Detection & Response												
Deep Packet Inspection (DPI) Appliances												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
Other (Define in Comment Box)												
C. Intrusion Detection/Prevention Systems												
Host Intrusion Detection (HIDS)												
Network Intrusion Detection Systems (NIDS)												
Host Intrusion Prevention Systems (HIPS)												
Network Intrusion Prevention Systems (NIPS)												
Unified Threat Management (UTM) Systems												
Honeypot												
Network Tar Pit Solutions												
Data Loss Prevention (DLP)												
Data Recovery												
Other (Define in Comment Box)												
D. Network Systems												
Virtual Private Network (VPN)												
Virtual Private Server (VPS)												
Virtualization Software - Bare Metal Hypervisor												
Virtualization Software - Work Station-Based Hypervisor												
Software Defined Networking (SDN) solutions												
Other (Define in Comment Box)												
E. Other Products												
Industrial Control Systems - Networked												
Supervisory Control and Data Acquisition (SCADA)-Networked												
Computer Operating Systems												
Computer Firmware												
Systems-On-Chip, Microcontroller Devices												
Memory and Data Storage Devices												
Mobile Device Operating Systems												
Multi-Function Devices - Printers-Copiers-Scanners												
Networked Printers												
Networked Scanners												
Health Management Systems - Network Connected												
Health Systems/Devices - Network Connected												
Physical Access Control Systems - Network Connected												
Physical Security Video Monitoring Systems - Network Connected												
Telepresence Systems (Audio & Video Conferencing Systems)												
Other (Define in Comment Box)												
Comments:												

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 1.g - Kaspersky Technologies Deployed in Organization Products & Terms of Tech				
Instruction: 1) For each Kaspersky product type listed in the left column, identify those which your organization has used since 2014 for inclusion in the hardware or software (including services) products that your organization designs, manufactures, markets, or distributes. [Respond to all category blocks]			Instruction: 2) For each product type, identify the terms of technology that are licensed for inclusion in the products you use. [Respond to all category blocks]	
Types of Kaspersky Product/Associated Intellectual Property	Applications of Kaspersky Technologies/ Associated Intellectual Property in Your Organization's Products	Primary Reason for Using Kaspersky Product	Secondary Reason for Using Kaspersky Product	Single Technology
Kaspersky Advanced Sandbox				
Kaspersky Analysis Engines				
Kaspersky Anti-Virus				
Kaspersky VirusDesk				
Kaspersky Application Control/Dynamic Whitelisting				
Kaspersky Application Launch Control - Corporate Servers				
Kaspersky Automated Vulnerability Assessment				
Kaspersky Automated Vulnerability Patch Management				
Kaspersky Business Hub				
Kaspersky Cloud Security				
Kaspersky Cyber Security Services [Security Education/Training]				
Kaspersky Data Center Security				
Kaspersky Device Control				
Kaspersky Distributed Denial of Service (DDOS)				
Kaspersky Embedded Systems Security				
Kaspersky Endpoint Security				
Kaspersky Endpoint Security - Cloud				
Kaspersky Endpoint Security for Business Advanced				
Kaspersky Expert Services [Penetration, Application Security, Digital Forensics, Malware Analysis]				
Kaspersky HuMachine				
Kaspersky Hybrid Cloud Security				
Kaspersky Industrial Cyber Security				
Kaspersky Internet Security				
Kaspersky Internet Security for MAC				
Kaspersky Maintenance Service Agreement				
Kaspersky Mobile Security				
Kaspersky Multi-Layered Sensor Architecture				
Kaspersky Password Manager				
Kaspersky Private Security Network				
Kaspersky Professional Services				
Kaspersky Security Center				
Kaspersky Security for Storage [anti-virus]				
Kaspersky Security for Virtualization - Agentless				
Kaspersky Security for Virtualization - Light Agent				
Kaspersky Security for Windows 365				
Kaspersky Security for Windows Server				
Kaspersky Security Network				
Kaspersky Security Virtual Machine				
Kaspersky Small Office Security				
Kaspersky System Watcher [Anti-Ransom, Anti-Exploitation]				
Kaspersky Threat Intelligence				
Kaspersky Threat Management & Defense				
Kaspersky Total Security				
Kaspersky Web Control				
Kaspersky Whitelisting - Cloud Empowered				
Other (Describe in Comment Box)				
Pre-2014 Kaspersky Hardware & Software Products				
Comments:				

Annual License Fee
 Multi-Year License Fee
 One-Time Payment
 Information Sharing Agreement
 Free
 None
 Other*

Hardware
 Software
 Both
 None

Annual License Fee
 Multi-Year License Fee
 One-Time Payment
 Information Sharing Agreement
 Free
 None
 Other*

Brand Recognition
 Ease of Use
 Lowest Pricing
 Performance/ Effectiveness
 Reliability
 Integration Time/ Latency
 Technical Support
 Technical
 Collaborations
 Technical Superiority
 No Competitive Equivalent
 Contract Terms/Financing
 Kaspersky Financial
 Rebates
 Full-Service Network Security Services
 Satisfying Customer Requests
 Other
 (Use Comment Box)

Brand Recognition
 Ease of Use
 Lowest Pricing
 Performance/ Effectiveness
 Reliability
 Integration Time/ Latency
 Technical Support
 Technical
 Collaborations
 Technical Superiority
 No Competitive Equivalent
 Contract Terms/Financing
 Kaspersky Financial
 Rebates
 Full-Service Network Security Services
 Satisfying Customer Requests
 Other
 (Use Comment Box)

Section 1.h - Kaspersky Technologies Used for Internal Business Operations

[Previous Page](#) [Next Page](#)

Instruction:
 1) Identify all of the Kaspersky technologies listed below that your organization has used in any way since 2014 to support its internal business operations and information networks.
 2) For each Kaspersky technology that your organization utilizes internally, identify whether its use is in the form of a purchased hardware or software product; procured services that support your operations with enabling hardware or software using Kaspersky technologies; or other types of goods that utilize Kaspersky technologies.

Types of Kaspersky Product/Associated Intellectual Property	Your organization's Internal Business Operations and Network Systems	Products	Services	Other (Describe in Comment Box)	Comments
Kaspersky Advanced Sandbox					
Kaspersky Analysis Engines					
Kaspersky Anti-Virus					
Kaspersky VirusDesk					
Kaspersky Application Control/Dynamic Whitelisting					
Kaspersky Application Launch Control - Corporate Servers					
Kaspersky Automated Vulnerability Assessment					
Kaspersky Automated Vulnerability Patch Management					
Kaspersky Business Hub					
Kaspersky Cloud Security					
Kaspersky Cyber Security Services [Security Education/Training]					
Kaspersky Data Center Security					
Kaspersky Device Control					
Kaspersky Distributed Denial of Service (DDOS)					
Kaspersky Embedded Systems Security					
Kaspersky Endpoint Security					
Kaspersky Endpoint Security - Cloud					
Kaspersky Endpoint Security for Business Advanced					
Kaspersky Expert Services [Penetration, Application Security, Digital Forensics, Malware Analysis]					
Kaspersky HuMachine					
Kaspersky Hybrid Cloud Security					
Kaspersky Industrial Cyber Security					
Kaspersky Internet Security					
Kaspersky Internet Security for MAC					
Kaspersky Maintenance Service Agreement					
Kaspersky Mobile Security					
Kaspersky Multi-Layered Sensor Architecture					
Kaspersky Password Manager					
Kaspersky Private Security Network					
Kaspersky Professional Services					
Kaspersky Security Center					
Kaspersky Security for Storage [anti-virus]					
Kaspersky Security for Virtualization - Agentless					
Kaspersky Security for Virtualization - Light Agent					
Kaspersky Security for Windows 365					
Kaspersky Security for Windows Server					
Kaspersky Security Network					
Kaspersky Security Virtual Machine					
Kaspersky Small Office Security					
Kaspersky System Watcher [Anti-Ransom, Anti-Exploit]					
Kaspersky Threat Intelligence					
Kaspersky Threat Management & Defense					
Kaspersky Total Security					
Kaspersky Web Control					
Kaspersky Whitelisting - Cloud Empowered					
Other (Describe in Comment Box)					
Pre-2014 Kaspersky Hardware & Software Products [Use Comment Box]					
Comments:					

Yes
No

Hardware
Software
Both
None

Hardware
Software
Both
None

Hardware
Software
Both
None

Previous Page	Section 1.1 - End Uses of Hardware and Software Products Sold Containing Kaspersky Technologies											Next Page						
Instruction: For each of the U.S. critical infrastructure sectors shown in the top of the table, identify the types of information technology products containing any Kaspersky technologies sold to them (directly or indirectly) by your organization since 2014. [*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways". Do not report as "Gateways" in the response section routers/switches that also act as gateways.]																		
U.S. Critical Infrastructure Sectors Purchasing Your Organization's Products that Contain Kaspersky Technologies -> Types of Kaspersky Product/Associated Intellectual Property	Chemicals: Basic Chemicals, Specialty Chemicals, Agricultural Chemicals, Pharmaceuticals, Consumer Products	Commercial Facilities: Lodging, Retail, Sports Facilities	Communications: TV, Computer, Internet, Cable, Satellite	Critical Manufacturing: Primary Metals, Electrical Equipment, Machinery, Manufacturing, Transportation Equipment	Dams: Food Control, Navigation Locks, Levees	Defense Industrial Base: Domestic and Foreign Supply Chain	Emergency Services: Emergency Management, Public Works	Energy: Power Generation, Petroleum Refining, Chemical Refining, Fuel Production, Transportation	Financial Services: Banking, Securities, Funds Transfers	Food and Agriculture: Production, Transportation, Inspection, Inspection	Government Facilities: Embassies, Consulates, Laboratories, Court House	Elections Infrastructure: Voting Equipment, Database, Software	Healthcare and Public Health: Hospitals, Drug Makers, Research Labs	Information Technology: IT Products and Services, Internet Infrastructure	Nuclear: Nuclear Reactors, Materials, and Waste	Transportation Systems: Aviation, Highway, Maritime, Pipelines, Rail, Ports	Water and Waste Water Systems: Sewerage, Wastewater Treatment Plants, Irrigation	Other [Explain in Comment Box Below]
A. Network Infrastructure Devices																		
Routers - Home Office/Small Office																		
Routers - Enterprise/Internet Service Provider Grade																		
Switches - Home Office/Small Office																		
Switches - Enterprise/Internet Service Provider Grade																		
Gateways - Home Office/Small Office (not including switches/routers)																		
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																		
Gateways - Cloud (not including switches/routers)																		
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																		
Gateways - Mobile Secure Gateways (not including switches/routers)																		
Gateways - Other (not including switches/routers)																		
Other [Define in Comment Box]																		
B. Network Security Devices																		
Antivirus Scanning Application - Host Based																		
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																		
Firewalls - Host Based																		
Firewalls - Network Appliance																		
Firewalls - Cloud																		
Firewalls - Virtualized																		
Web Application Firewalls																		
End Point Detection & Response (EDR)																		
Deep Packet Inspection (DPI) Appliance																		
Security Information and Event Management (SIEM)																		
Web Proxies/Content Filtering																		
Other [Define in Comment Box]																		
C. Intrusion Detection/Prevention Systems																		
Host Intrusion Detection (HIDS)																		
Network Intrusion Detection Systems (NIDS)																		
Host Intrusion Prevention Systems (HIPS)																		
Network Intrusion Prevention Systems (NIPS)																		
Unified Threat Management (UTM) Systems																		
Honeypot																		
Network Tar Pit Solutions																		
Data Loss Prevention (DLP)																		
Data Recovery																		
Other [Define in Comment Box]																		
D. Network Systems																		
Virtual Private Network (VPN)																		
Virtual Private Server (VPS)																		
Virtualization Software - Bare Metal Hypervisor																		
Virtualization Software - Work Station-Based Hypervisor																		
Software Defined Networking (SDN) solutions																		
Other [Define in Comment Box]																		
E. Other Products																		
Industrial Control Systems - Networked																		
Supervisory Control and Data Acquisition (SCADA)-Networked																		
Computer Operating Systems																		
Computer Firmware																		
Systems-On-Chip, Microcontroller Devices																		
Memory and Data Storage Devices																		
Mobile Device Operating Systems																		
Multi-Function Devices - Printers-Copiers-Scanners																		
Networked Printers																		
Networked Scanners																		
Health Management Systems - Network Connected																		
Health Systems/Devices - Network Connected																		
Physical Access Control Systems - Network Connected																		
Physical Security Video Monitoring Systems - Network Connected																		
Telepresence Systems (Audio & Video Conferencing Systems)																		
Other [Define in Comment Box]																		
Comments																		

Hardware
Software
Both
None
(Options for all drop-downs on this Tab are the same)

Section 1.j - End Users of Hardware and Software Products Sold Containing Kaspersky Technologies

Instruction: For each of the U.S. critical infrastructure sectors shown, identify your organization's top five customers in the U.S. by volume since 2014, and your primary type of information technology product containing any Kaspersky technologies sold to them (directly or indirectly).
 Primary Product dropdown menus are populated based on the information you provided in Section 1e of this survey.

Critical Infrastructure Sector	1				2				3			
	Primary Product Provided	Customer Name	Customer DUNS	Customer City, State	Primary Product Provided	Customer Name	Customer DUNS	Customer City, State	Primary Product Provided	Customer Name	Customer DUNS	Customer City, State
Chemicals Basic, Specialty, and Agricultural Chemicals, Pharmaceuticals, Consumer Products												
Commercial Facilities Lodging, Retail, Sports Facilities												
Communications Broadcast, Telephone, Internet, Cable, Satellite												
Critical Manufacturing Primary Metals, Electrical Equipment, Machinery Manufacturing, Transportation Equipment												
Dams Flood Control, Navigation Locks, Levees												
Defense Industrial Base Domestic and Foreign Supply Chain												
Emergency Services Fire, Police, Emergency Management, Public Works												
Energy Power Generation, Petroleum Production, Coal Mining, Fuel Transportation												
Financial Services Banking, Securities, Funds Transfers												
Food and Agriculture Production, Transportation, Inspection, Importation												
Government Facilities Buildings, Military Installations, Laboratories, Court Houses												
Elections Infrastructure Voting Equipment, Databases, Software												
Healthcare and Public Health Hospitals, Drug Makers, Research Labs												
Information Technology IT Products and Services, Internet Functionality												
Nuclear Nuclear Reactors, Materials, and Waste												
Transportation Systems Aviation, Highway, Maritime, Pipelines, Rail, Ports												
Water and Waste Water Systems Sewer, Filtration, Water Treatment Plants, Irrigation												
Comments												

Primary Product dropdown menus are populated based on the information you provided in Section 1e of this survey.

Primary Product dropdown menus are populated based on the information you provided in Section 1e of this survey.

Primary Product dropdown menus are populated based on the information you provided in Section 1e of this survey.

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

[Previous Page](#)

[Next Page](#)

Section 1.k - Operating Systems on Which Organization's Products Containing Kaspersky Technologies Were Designed to Function

Instruction: Identify the hardware and software products containing Kaspersky technologies sold since 2014 by your organization that can function with, or be integrated with, any of the computer operating systems and mobile device operating systems listed below.

Computer Operating Systems				Network Operating Systems			
Chrome OS	<input type="checkbox"/>	Linux Workstation	<input type="checkbox"/>	Cisco - IOS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hypervisor - KVM	<input type="checkbox"/>	Red Hat Linux Sever	<input type="checkbox"/>	Juniper Networks - JUNOS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hypervisor - VMWare ESX	Hardware Software Both None	Red Hat Linux Workstation	Hardware Software Both None	Juniper Networks - ScreenOS	Hardware Software Both None	<input type="checkbox"/>	<input type="checkbox"/>
Hypervisor - Xen/XenServer		Linux Server		Open Networking Foundation - ONOS			
Hypervisor - Microsoft Hyper V		Linux		Open Networking Foundation - Stratum			
Hypervisor - Other (Describe in Comment Box)	<input type="checkbox"/>	Berkeley Software Distribution (BSD) - Unix-like Operating System	<input type="checkbox"/>	VyOS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mac OS	<input type="checkbox"/>	VMWorks	<input type="checkbox"/>	Nokia AlcatelLucent: Service Router OS (SROS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows Server	<input type="checkbox"/>	Custom Operating Systems	<input type="checkbox"/>	Open Source Projects: Dresden-wireless Router (DD/WRT) or OPEN Wireless Router (Open-WRT)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows 10	Hardware Software Both None	Industrial Operating Systems	Hardware Software Both None	Cumulus Linux	Hardware Software Both None	<input type="checkbox"/>	<input type="checkbox"/>
Windows 7		Proprietary Operating Systems		Open Source Linux (and variants)			
Older Windows Versions		Other (specify here)		Other (specify here)			
Linux Server	<input type="checkbox"/>	Other (specify here)	<input type="checkbox"/>	Other (specify here)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mobile Operating Systems							
Android	<input type="checkbox"/>	iOS - Apple	<input type="checkbox"/>	Blackberry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:							

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 1.1 - Modes of Accessing Kaspersky Technologies for Product Development-Production									
Instruction: For each product type listed in the left column, identify the means by which your organization gains access to Kaspersky technologies for hardware and software integrated into the products that your organization designs, manufactures, markets, or distributes. [*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]									
Means of Accessing Kaspersky Product	Packaged Software Purchased Directly from Kaspersky Installed by Your Organization's Staff	Packaged Software Sold by Kaspersky Authorized Third Party Reseller	Packaged Software Downloaded Directly from Kaspersky Servers	Software Installed at Your Organization's Product Manufacturing Facilities by Kaspersky Employees	Software Installed at Your Product Manufacturing Facilities by Kaspersky-Authorized Third-Party Firms	Software Purchased Through a Cloud (e.g. AWS Marketplace, Azure Services, etc.)	Other	Comments	
A. Network Infrastructure Devices									
Routers - Home Office/Small Office									
Routers - Enterprise/Internet Service Provider Grade									
Switches - Home Office/Small Office									
Switches - Enterprise/Internet Service Provider Grade									
Gateways - Home Office/Small Office (not including switches/routers)	Yes	Yes	Yes	Yes	Yes	Public Cloud Private Cloud Both			Yes
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)	No	No	No	No	No				No
Gateways - Cloud (not including switches/routers)									
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)									
Gateways - Mobile Secure Gateways (not including switches/routers)									
Gateways - Other (not including switches/routers)									
Other [Define in Comment Box]									
B. Network Security Devices									
Antivirus Scanning Application - Host Based									
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)									
Firewalls - Host Based									
Firewalls - Network Appliance									
Firewalls - Cloud									
Firewalls - Virtualized									
Web Application Firewalls									
End Point Detection & Response (EDR)									
Deep Packet Inspection (DPI) Appliance									
Security Information and Event Management (SIEM)									
Web Proxies/Content Filtering									
Other [Define in Comment Box]									
C. Intrusion Detection/Prevention Systems									
Host Intrusion Detection (HIDS)									
Network Intrusion Detection Systems (NIDS)									
Host Intrusion Prevention Systems (HIPS)									
Network Intrusion Prevention Systems (NIPS)									
Unified Threat Management (UTM) Systems									
Honeypot									
Network Tar Pit Solutions									
Data Loss Prevention (DLP)									
Data Recovery									
Other [Define in Comment Box]									
D. Network Systems									
Virtual Private Network (VPN)									
Virtual Private Server (VPS)									
Virtualization Software - Bare Metal Hypervisor									
Virtualization Software - Work Station-Based Hypervisor									
Software Defined Networking (SDN) solutions									
Other [Define in Comment Box]									
E. Other Products									
Industrial Control Systems - Networked									
Supervisory Control and Data Acquisition (SCADA)-Networked									
Computer Operating Systems									
Computer Firmware									
Systems-On-Chip, Microcontroller Devices									
Memory and Data Storage Devices									
Mobile Device Operating Systems									
Multi-Function Devices - Printers-Copiers-Scanners									
Networked Printers									
Networked Scanners									
Health Management Systems - Network Connected									
Health Systems/Devices - Network Connected									
Physical Access Control Systems - Network Connected									
Physical Security Video Monitoring Systems - Network Connected									
Telepresence Systems (Audio & Video Conferencing Systems)									
Other [Define in Comment Box]									
Comments:									

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 1.m - Kaspersky Technologies Deployed in Organization Products - Clones & Counterfeits

Instruction: For each product type listed in the left column that was sold by your organization since 2014 identify whether your organization continues to use Kaspersky technologies or the year during which Kaspersky technologies stopped being incorporated into these products. Then identify those products suspected to have been subject to unauthorized production; and counterfeit production. State whether any of the unauthorized production of goods and the cloned/counterfeit products used any Kaspersky technology and services. For those products containing Kaspersky technologies, use the comments areas describe the scale and scope of the overproduction, product counterfeiting, and distribution.
 [*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]

Types of Kaspersky Product/Associated Intellectual Property	Ongoing/Termination of Use of Kaspersky Technology in Organization's Hardware Products	Ongoing/Termination of Use of Kaspersky Technology in Organization's Software Products	Comments	Unauthorized, Cloned/ Counterfeit Hardware Products	Unauthorized, Cloned/ Counterfeit Software Products	Comments
A. Network Infrastructure Devices						
Routers - Home Office/Small Office						
Routers - Enterprise/Internet Service Provider Grade						
Switches - Home Office/Small Office						
Switches - Enterprise/Internet Service Provider Grade						
Gateways - Home Office/Small Office (not including switches/routers)						
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)						
Gateways - Cloud (not including switches/routers)						
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)						
Gateways - Mobile Secure Gateways (not including switches/routers)						
Gateways - Other (not including switches/routers)						
Other [Define in Comment Box]						
B. Network Security Devices						
Antivirus Scanning Application - Host Based						
Antivirus Scanning Appliances - Enclave Boundary (Gateway)						
Firewalls - Host Based						
Firewalls - Network Appliance						
Firewalls - Cloud						
Firewalls - Virtualized						
Web Application Firewalls						
End Point Detection & Response (EDR)						
Deep Packet Inspection (DPI) Appliance						
Security Information and Event Management (SIEM)						
Web Proxies/Content Filtering						
Other [Define in Comment Box]						
C. Intrusion Detection/Prevention Systems						
Host Intrusion Detection (HIDS)						
Network Intrusion Detection Systems (NIDS)						
Host Intrusion Prevention Systems (HIPS)						
Network Intrusion Prevention Systems (NIPS)						
Unified Threat Management (UTM) Systems						
Honeypot						
Network Tar Pit Solutions						
Data Loss Prevention (DLP)						
Data Recovery						
Other [Define in Comment Box]						
D. Network Systems						
Virtual Private Network (VPN)						
Virtual Private Server (VPS)						
Virtualization Software - Bare Metal Hypervisor						
Virtualization Software - Work Station-Based Hypervisor						
Software Defined Networking (SDN) solutions						
Other [Define in Comment Box]						
E. Other Products						
Industrial Control Systems - Networked						
Supervisory Control and Data Acquisition (SCADA)-Networked						
Computer Operating Systems						
Computer Firmware						
Systems-On-Chip, Microcontroller Devices						
Memory and Data Storage Devices						
Mobile Device Operating Systems						
Multi-Function Devices - Printers-Copiers-Scanners						
Networked Printers						
Networked Scanners						
Health Management Systems - Network Connected						
Health Systems/Devices - Network Connected						
Physical Access Control Systems - Network Connected						
Physical Security Video Monitoring Systems - Network Connected						
Telepresence Systems (Audio & Video Conferencing Systems)						
Other [Define in Comment Box]						
Comments:						

Ongoing Use
Halted Prior to 2015
Halted 2015
Halted 2016
Halted 2017
Halted 2018
Halted 2019

Ongoing Use
Halted Prior to 2015
Halted 2015
Halted 2016
Halted 2017
Halted 2018
Halted 2019

Unauthorized Production
Counterfeit Production
Both
None

Yes
No
Unknown

Section 2.a - Embedding of Kaspersky Software into Manufacturers Information Technology Hardware Products										
<p>Instruction: For the information network hardware products sold by your organization since 2014 that incorporate or otherwise contain embedded Kaspersky technologies (hardware or software) provide:</p> <ol style="list-style-type: none"> 1) the Total Number of Models Produced. 2) the Name(s) and corresponding Model/Series number for each product sold by your organization. 3) the Year of first customer shipment for each distinct model number. 4) the number of versions produced of each distinct product model. <p>[*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]</p> <p>Enter all additional product names and model numbers. Information on additional product model numbers shall be entered in successive form blocks that are reached by scrolling this page to the right → → →</p>										
Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Technology Type/Versions										
Hardware Products Sold By Your Organization that Contain Kaspersky Technology	State the Total Number of Models Produced Since 2014 Containing Kaspersky Technologies	Product Name #1	#1 Your Organization's Product Model/Series Number	Year of First Customer Shipment	Number of Versions Produced with New Features/Capabilities	Comments	Product Name #2	#2 Your Organization's Product Model/Series Number	Year of First Customer Shipment	Number of Versions Produced with New Features/Capabilities
A. Network Infrastructure Devices										
Routers - Home Office/Small Office										
Routers - Enterprise/Internet Service Provider Grade										
Switches - Home Office/Small Office										
Switches - Enterprise/Internet Service Provider Grade										
Gateways - Home Office/Small Office (not including switches/routers)										
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)										
Gateways - Cloud (not including switches/routers)										
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)										
Gateways - Mobile Secure Gateways (not including switches/routers)										
Gateways - Other (not including switches/routers)										
Other [Define in Comment Box]										
B. Network Security Devices										
Antivirus Scanning Application - Host Based										
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)										
Firewalls - Host Based										
Firewalls - Network Appliance										
Firewalls - Cloud										
Firewalls - Virtualized										
Web Application Firewalls										
End Point Detection & Response (EDR)										
Deep Packet Inspection (DPI) Appliance										
Security Information and Event Management (SIEM)										
Web Proxies/Content Filtering										
Other [Define in Comment Box]										
C. Intrusion Detection/Prevention Systems										
Host Intrusion Detection (HIDS)										
Network Intrusion Detection Systems (NIDS)										
Host Intrusion Prevention Systems (HIPS)										
Network Intrusion Prevention Systems (NIPS)										
Unified Threat Management (UTM) Systems										
Honeypot										
Network Tap PII Solutions										
Data Loss Prevention (DLP)										
Data Recovery										
Other [Define in Comment Box]										
D. Network Systems										
Virtual Private Network (VPN)										
Virtual Private Server (VPS)										
Virtualization Software - Bare Metal Hypervisor										
Virtualization Software - Work Station-Based Hypervisor										
Software Defined Networking (SDN) solutions										
Other [Define in Comment Box]										
E. Other Products										
Industrial Control Systems - Networked										
Supervisory Control and Data Acquisition (SCADA)-Networked										
Computer Operating Systems										
Computer Firmware										
Systems-On-Chip, Microcontroller Devices										
Memory and Data Storage Devices										
Mobile Device Operating Systems										
Multi-Function Devices - Printers-Copiers-Scanners										
Networked Printers										
Networked Scanners										
Health Management Systems - Network Connected										
Health Systems/Devices - Network Connected										
Physical Access Control Systems - Network Connected										
Physical Security Video Monitoring Systems - Network Connected										
Telepresence Systems (Audio & Video Conferencing Systems)										
Other [Define in Comment Box]										
Comments										

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 2 b - Integration/Embedding of Kaspersky Software into Domestic Manufacturers Information Technology Hardware Product

Instruction: For each type of information technology hardware product identified on the previous page as incorporating or otherwise containing any Kaspersky technologies (hardware or software):
 1) Provide the Kaspersky product model (Autopopulated)
 2) State the functions and capabilities of the Kaspersky software
 3) Specify the methods used for integrating Kaspersky technologies into your organization's products. [Respond to all category blocks]
 [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways". Do not report as "Gateways" in the response section routers/switches that also act as gateways.]

Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right. → → → →

	#1 Your Organization's Product Model/Series Number	Description of Functions/Capabilities of Kaspersky Software Integrated into Your Organization's Hardware Products										Comments	#2 Your Organization's Product Model/Series Number	Description of Functions/Capabilities of Kaspersky Software Integrated into Your Organization's Hardware Products										Comments		
		Local Anti-Virus	Cloud Anti-Virus	E-mail Scanning	Identify Theft	IP Loss Prevention	Network Intrusion Detection/Prevention	Reverse Proxy	Other (Use Comment Box)	Completed Together	Translated			Executable	Other (Use Comment Box)	Local Anti-Virus	Cloud Anti-Virus	E-mail Scanning	Identify Theft	IP Loss Prevention	Network Intrusion Detection/Prevention	Reverse Proxy	Other (Use Comment Box)		Completed Together	Translated
A. Network Infrastructure Devices																										
Routers - Home Office/Small Office Routers - Enterprise/Internet Service Provider Grade Switches - Home Office/Small Office Switches - Enterprise/Internet Service Provider Grade Gateways - Home Office/Small Office (not including switches/routers) Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers) Gateways - Cloud (not including switches/routers) Gateways - Modular Internet-of-Things (IoT) (not including switches/routers) Gateways - Mobile Secure Gateways (not including switches/routers) Gateways - Other (not including switches/routers) Other [Define in Comment Box]																										
B. Network Security Devices																										
Antivirus Scanning Application - Host Based Antivirus Scanning Appliances - Enclave Boundary (Gateway-based) Firewalls - Host Based Firewalls - Network Appliance Firewalls - Cloud Firewalls - Virtualized Web Application Firewalls End Point Detection & Response (EDR) Deep Packet Inspection (DPI) Appliance Security Information and Event Management (SIEM) Web Proxies/Content Filtering Other [Define in Comment Box]																										
C. Intrusion Detection/Prevention Systems																										
Host Intrusion Detection (HIDS) Network Intrusion Detection Systems (NIDS) Host Intrusion Prevention Systems (HIPS) Network Intrusion Prevention Systems (NIPS) Unified Threat Management (UTM) Systems Honeypot Network Tar Pit Solutions Data Loss Prevention (DLP) Data Recovery Other [Define in Comment Box]																										
D. Network Systems																										
Virtual Private Network (VPN) Virtual Private Server (VPS) Virtualization Software - Bare Metal Hypervisor Virtualization Software - Work Station-Based Hypervisor Software Defined Networking (SDN) solutions Other [Define in Comment Box]																										
E. Other Products																										
Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked Computer Operating Systems Computer Firmware Systems-On-Chip, Microcontroller Devices Memory and Data Storage Devices Mobile Device Operating Systems Multi-Function Devices - Printers-Copiers-Scanners Networked Printers Networked Scanners Health Management Systems - Network Connected Health Systems/Devices - Network Connected Physical Access Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Other [Define in Comment Box]																										
Comments																										

Yes
 No
 Not Applicable
 (Options for all drop-downs on this Tab)

Yes
 No
 Not Applicable
 (Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Previous Page	Section 2.c - Integration/Embedding of Kaspersky Software into Manufacturers' Information Technology Hardware Product														Next Page	
<p>Instruction: For the types information network hardware products identified on the previous page as incorporating or otherwise containing embedded Kaspersky technologies, provide:</p> <p>1) Applicable model numbers [Autopopulate];</p> <p>2) Associated application program interfaces (APIs); and</p> <p>3) The method for signing software publication certificates associated with your organization's products. [Respond to all category blocks]</p> <p>[*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways]</p> <p>Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right. --> --> --></p>																
Hardware Products Sold By Your Organization that Contain Kaspersky Technology	#1 Your Organization's Product Model/Series Number	Associated Application Program Interfaces (APIs)										Method for Signing Software Publication Certificate				Comments
		Development - Pipeline	Production - Pipeline	Testing - Pipeline	Representational State Transfer (REST)	Shared Memory	Simple Object Access Protocol (SOAP)	Available	Data Exchange Interface (DXI)	Other (Use Comment Box)	Private Key - Signed	Co-Signed Private Key	Shared Key - Signed	Not Signed	None	
Hardware Products Sold By Your Organization that Contain Kaspersky Technology	#2 Your Organization's Product Model/Series Number	Associated Application Program Interfaces (APIs)										Method for Signing Software Publication Certificate				Comments
		Development - Pipeline	Production - Pipeline	Testing - Pipeline	Representational State Transfer (REST)	Shared Memory	Simple Object Access Protocol (SOAP)	Available	Data Exchange Interface (DXI)	Other (Use Comment Box)	Private Key	Co-Signed Private Key	Shared Key	Not Signed	None	
A. Network Infrastructure Devices																
Routers - Home Office/Small Office																
Routers - Enterprise/Internet Service Provider Grade																
Switches - Home Office/Small Office																
Switches - Enterprise/Internet Service Provider Grade																
Gateways - Home Office/Small Office (not including switches/routers)																
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																
Gateways - Cloud (not including switches/routers)																
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																
Gateways - Mobile Secure Gateways (not including switches/routers)																
Gateways - Other (not including switches/routers)																
Other (Define in Comment Box)																
B. Network Security Devices																
Antivirus Scanning Application - Host Based																
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																
Firewalls - Host Based																
Firewalls - Network Appliance																
Firewalls - Cloud																
Firewalls - Virtualized																
Web Application Firewalls																
End Point Detection & Response (EDR)																
Deep Packet Inspection (DPI) Appliance																
Security Information and Event Management (SIEM)																
Web Proxies/Content Filtering																
Other (Define in Comment Box)																
C. Intrusion Detection/Prevention Systems																
Host Intrusion Detection (HIDS)																
Network Intrusion Detection Systems (NIDS)																
Host Intrusion Prevention Systems (HIPS)																
Network Intrusion Prevention Systems (NIPS)																
Unified Threat Management (UTM) Systems																
Honeypot																
Network Tap Pit Solutions																
Data Loss Prevention (DLP)																
Data Recovery																
Other (Define in Comment Box)																
D. Network Systems																
Virtual Private Network (VPN)																
Virtual Private Server (VPS)																
Virtualization Software - Bare Metal Hypervisor																
Virtualization Software - Work Station-Based Hypervisor																
Software Defined Networking (SDN) solutions																
Other (Define in Comment Box)																
E. Other Products																
Industrial Control Systems - Networked																
Supervisory Control and Data Acquisition (SCADA)-Networked																
Computer Operating Systems																
Computer Firmware																
Systems-On-Chip, Microcontroller Devices																
Memory and Data Storage Devices																
Mobile Device Operating Systems																
Multi-Function Devices - Printers-Copiers-Scanners																
Networked Printers																
Networked Scanners																
Health Management Systems - Network Connected																
Health Systems/Devices - Network Connected																
Physical Access Control Systems - Network Connected																
Physical Security Video Monitoring Systems - Network Connected																
Telepresence Systems (Audio & Video Conferencing Systems)																
Other (Define in Comment Box)																
Comments																

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Previous Page	Section 2.d - Integration/Embedding of Kaspersky Software into Manufacturers' Information Technology Hardware Products														Next Page
Instruction: For the types information technology hardware products identified on the previous page as incorporating or otherwise containing embedded Kaspersky technologies, provide: 1) Model numbers (Autopopulated); 2) Types of data that can be accessed; [Respond to all category blocks] 3) Levels of System Access available to Kaspersky software. [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.] Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right --> -->															
Hardware Products Sold By Your Organization that Contain Kaspersky Technology	Types of Data That Can Be Accessed							Levels of System Access Available to Kaspersky Software							Comment
	#1 Your Organization's Product Model/Series Number	System Configuration	Proprietary Business Data	Application Customization Data	Application Customization Data	Other (Use Comment Box)	System Data	Application Data	User Data	Non-Root Access	Root-Level Access	System Kernel	Other (Use Comment Box)		
	Types of Data That Can Be Accessed							Levels of System Access Available to Kaspersky Software							Comment
	#2 Your Organization's Product Model/Series Number	System Configuration	Proprietary Business Data	Application Customization Data	Application Customization Data	Other (Use Comment Box)	System Data	Application Data	User Data	Non-Root Access	Root-Level Access	System Kernel	Other (Use Comment Box)		
A. Network Infrastructure Devices															
Routers - Home Office/Small Office															
Routers - Enterprise/Internet Service Provider Grade															
Switches - Home Office/Small Office															
Switches - Enterprise/Internet Service Provider Grade															
Gateways - Home Office/Small Office (not including switches/routers)															
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)															
Gateways - Cloud (not including switches/routers)															
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)															
Gateways - Mobile Secure Gateways (not including switches/routers)															
Other [Define in Comment Box]															
B. Network Security Devices															
Antivirus Scanning Application - Host Based															
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)															
Firewalls - Host Based															
Firewalls - Network Appliance															
Firewalls - Cloud															
Firewalls - Virtualized															
Web Application Firewalls															
End Point Detection & Response (EDR)															
Deep Packet Inspection (DPI) Appliance															
Security Information and Event Management (SIEM)															
Web Proxies/Content Filtering															
Other [Define in Comment Box]															
C. Intrusion Detection/Prevention Systems															
Host Intrusion Detection (HIDS)															
Network Intrusion Detection Systems (NIDS)															
Host Intrusion Prevention Systems (HIPS)															
Network Intrusion Prevention Systems (NIPS)															
Unified Threat Management (UTM) Systems															
Honeypot															
Network Tar Pit Solutions															
Data Loss Prevention (DLP)															
Data Recovery															
Other [Define in Comment Box]															
D. Network Systems															
Virtual Private Network (VPN)															
Virtual Private Server (VPS)															
Virtualization Software - Bare Metal Hypervisor															
Virtualization Software - Work Station-Based Hypervisor															
Software Defined Networking (SDN) solutions															
Other [Define in Comment Box]															
E. Other Products															
Industrial Control Systems - Networked															
Supervisory Control and Data Acquisition (SCADA)-Networked															
Computer Operating Systems															
Computer Firmware															
Systems-On-Chip, Microcontroller Devices															
Memory and Data Storage Devices															
Mobile Device Operating Systems															
Multi-Function Devices - Printers-Copiers-Scanners															
Networked Printers															
Networked Scanners															
Health Management Systems - Network Connected															
Health Systems/Devices - Network Connected															
Physical Access Control Systems - Network Connected															
Physical Security Video Monitoring Systems - Network Connected															
Telepresence Systems (Audio & Video Conferencing Systems)															
Other [Define in Comment Box]															

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 2.6 - Integration/Embedding of Kaspersky Technologies into Manufacturers' Information Technology Hardware Products - Functional Conditions for Kaspersky Technologies/Limits on Kaspersky in Syst

Instruction:
 1) Identify the methods by which Kaspersky software in your network hardware systems can perform its functions; and
 2) Specify the measures invoked by your organization to isolate Kaspersky software and services from the rest of the system. [Respond to all category blocks]
 *Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways". Do not report as "Gateways" in the response section routers/switches that also act as gateways.
 Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right. —>>>

Hardware Products Sold By Your Organization that Contain Kaspersky Technology	Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Functional Conditions for Kaspersky Software/Limits on Kaspersky in Systems																												
	Methods by Which Kaspersky Technology Can Perform Its Functions					Measures Invoked to Isolate Kaspersky Software & Services from Rest of System					Methods by Which Kaspersky Technology Can Perform Its Functions					Measures Invoked to Isolate Kaspersky Software & Services from Rest of System													
	#1 Your Organization's Product Model/Serial Number	Internet Access	Operating System Policy Limits	User Privileges	System Services	Non-system Level Privileges	Other (Use Comment Box)	Blocked Functions	Code Modification	Privilege Level Limitations	Memory Management	Library Configuration	CPU Demand Limits	Other (Use Comment Box)	Comments	#2 Your Organization's Product Model/Serial Number	Internet Access	Operating System Policy Limits	User Privileges	System Services	Non-system Level Privileges	Other (Use Comment Box)	Blocked Functions	Code Modification	Privilege Level Limitations	Memory Management	Library Configuration	CPU Demand Limits	Other (Use Comment Box)
A. Network Infrastructure Devices																													
Routers - Home Office/Small Office																													
Routers - Enterprise/Internet Service Provider Grade																													
Switches - Home Office/Small Office																													
Switches - Enterprise/Internet Service Provider Grade																													
Gateways - Home Office/Small Office (not including switches/routers)																													
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																													
Gateways - Cloud (not including switches/routers)																													
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																													
Gateways - Mobile Secure Gateways (not including switches/routers)																													
Gateways - Other (not including switches/routers)																													
Other (Define in Comment Box)																													
B. Network Security Devices																													
Antivirus Scanning Application - Host Based																													
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																													
Firewalls - Host Based																													
Firewalls - Network Appliance																													
Firewalls - Cloud																													
Firewalls - Virtualized																													
Web Application Firewalls																													
End Point Detection & Response (EDR)																													
Deep Packet Inspection (DPI) Appliance																													
Security Information and Event Management (SIEM)																													
Web Proxies/Content Filtering																													
Other (Define in Comment Box)																													
C. Intrusion Detection/Prevention Systems																													
Host Intrusion Detection (HIDS)																													
Network Intrusion Detection Systems (NIDS)																													
Host Intrusion Prevention Systems (HIPS)																													
Network Intrusion Prevention Systems (NIPS)																													
Unified Threat Management (UTM) Systems																													
Honeypot																													
Network Tar Pit Solutions																													
Data Loss Prevention (DLP)																													
Data Recovery																													
Other (Define in Comment Box)																													
D. Network Systems																													
Virtual Private Network (VPN)																													
Virtual Private Server (VPS)																													
Virtualization Software - Bare Metal Hypervisor																													
Virtualization Software - Work Station-Based Hypervisor																													
Software Defined Networking (SDN) solutions																													
Other (Define in Comment Box)																													
E. Other Products																													
Industrial Control Systems - Networked																													
Supervisory Control and Data Acquisition (SCADA)-Networked																													
Computer Operating Systems																													
Computer Firmware																													
Systems-On-Chip, Microcontroller Devices																													
Memory and Data Storage Devices																													
Mobile Device Operating Systems																													
Multi-Function Devices - Printers-Copiers-Scanners																													
Networked Printers																													
Networked Scanners																													
Health Management Systems - Network Connected																													
Health Systems/Devices - Network Connected																													
Physical Access Control Systems - Network Connected																													
Physical Security Video Monitoring Systems - Network Connected																													
Telepresence Systems (Audio & Video Conferencing Systems)																													
Other (Define in Comment Box)																													

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 785(d) of the Defense Production Act

Section 2.f - Product Design, Manufacturing, and Servicing of Hardware Products Containing Kaspersky Technologies - Internal-External/Third Party Services																		
<p>Instruction: For the information technology hardware products containing Kaspersky technologies that your organization sells:</p> <p>1) Indicate whether your organization's hardware products are designed internally by organization staff, externally by contractors, or by both organization employees and external contractors;</p> <p>2) State whether your organization formally designates third-party companies as "Manufacturer Authorized" to service and upgrade the products sold by your organization.</p> <p>[*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]</p> <p>Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right-->--></p>																		
Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Product Design, Service and Upgrade Practices																		
Hardware Products Sold By Your Organization that Contain Kaspersky Technology	#1 Your Organization's Product Model/Series Number	Was this product designed internally or externally?	Do you formally designate third-party companies as "Manufacturer Authorized" to service and upgrade this product?	Comments	#2 Your Organization's Product Model/Series Number	Was this product designed internally or externally?	Do you formally designate third-party companies as "Manufacturer Authorized" to service and upgrade this product?	Comments										
A. Network Infrastructure Devices																		
Routers - Home Office/Small Office																		
Routers - Enterprise/Internet Service Provider Grade																		
Switches - Home Office/Small Office																		
Switches - Enterprise/Internet Service Provider Grade																		
Gateways - Home Office/Small Office (not including switches/routers)	<div style="border: 1px solid black; padding: 5px; width: 50px; text-align: center;">Internal External Both</div>	<div style="border: 1px solid black; padding: 5px; width: 50px; text-align: center;">Yes No</div>			<div style="border: 1px solid black; padding: 5px; width: 50px; text-align: center;">Internal External Both</div>	<div style="border: 1px solid black; padding: 5px; width: 50px; text-align: center;">Yes No</div>												
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																		
Gateways - Cloud (not including switches/routers)																		
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																		
Gateways - Mobile Secure Gateways (not including switches/routers)																		
Gateways - Other (not including switches/routers)																		
Other [Define in Comment Box]																		
B. Network Security Devices																		
Antivirus Scanning Application - Host Based																		
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																		
Firewalls - Host Based																		
Firewalls - Network Appliance																		
Firewalls - Cloud																		
Firewalls - Virtualized																		
Web Application Firewalls																		
End Point Detection & Response (EDR)																		
Deep Packet Inspection (DPI) Appliance																		
Security Information and Event Management (SIEM)																		
Web Proxies/Content Filtering																		
Other [Define in Comment Box]																		
C. Intrusion Detection/Prevention Systems																		
Host Intrusion Detection (HIDS)																		
Network Intrusion Detection Systems (NIDS)																		
Host Intrusion Prevention Systems (HIPS)																		
Network Intrusion Prevention Systems (NIPS)																		
Unified Threat Management (UTM) Systems																		
Honeypot																		
Network Tar Pit Solutions																		
Data Loss Prevention (DLP)																		
Data Recovery																		
Other [Define in Comment Box]																		
D. Network Systems																		
Virtual Private Network (VPN)																		
Virtual Private Server (VPS)																		
Virtualization Software - Bare Metal Hypervisor																		
Virtualization Software - Work Station-Based Hypervisor																		
Software Defined Networking (SDN) solutions																		
Other [Define in Comment Box]																		
E. Other Products																		
Industrial Control Systems - Networked																		
Supervisory Control and Data Acquisition (SCADA)-Networked																		
Computer Operating Systems																		
Computer Firmware																		
Systems-On-Chip, Microcontroller Devices																		
Memory and Data Storage Devices																		
Mobile Device Operating Systems																		
Multi-Function Devices - Printers-Copiers-Scanners																		
Networked Printers																		
Networked Scanners																		
Health Management Systems - Network Connected																		
Health Systems/Devices - Network Connected																		
Physical Access Control Systems - Network Connected																		
Physical Security Video Monitoring Systems - Network Connected																		
Telepresence Systems (Audio & Video Conferencing Systems)																		
Other [Define in Comment Box]																		

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 3.a - Embedding of Kaspersky Software into Manufacturers Information Technology Software Products										
Instruction: For the information network software products sold by your organization since 2014 that incorporate or otherwise contain embedded Kaspersky software technologies provide: 1) The Total Number of Models Produced. 2) The Name(s) and corresponding Model/Series number for each product sold by your organization. 3) The Year of first customer shipment for each distinct model number. 4) The number of versions produced of each distinct product model. [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.] Enter all additional product names and model numbers. Information on additional product model numbers shall be entered in successive form blocks that are reached by scrolling this page to the right --> -->										
Integration of Kaspersky Software, Hardware, & Services in Software Systems - Technology Type/Versions										
Software Products Sold By Your Organization that Contain Kaspersky Technology [Auto-Populate This List Below from 1d]	State the Total Number of Models Produced Since 2014 Containing Kaspersky Technologies	Product Name #1	#1 Your Organization's Product Model/Series Number	Year of First Customer Shipment	Number of Versions Produced with New Features/Capabilities	Comments	Product Name #2	#2 Your Organization's Product Model/Series Number	Year of First Customer Shipment	Number of Versions Produced with New Features/Capabilities
A. Network Infrastructure Devices										
Routers - Home Office/Small Office										
Routers - Enterprise/Internet Service Provider Grade										
Switches - Home Office/Small Office										
Switches - Enterprise/Internet Service Provider Grade										
Gateways - Home Office/Small Office (not including switches/routers)										
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)										
Gateways - Cloud (not including switches/routers)										
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)										
Gateways - Mobile Secure Gateways (not including switches/routers)										
Gateways - Other (not including switches/routers)										
Other [Define in Comment Box]										
B. Network Security Devices										
Antivirus Scanning Application - Host Based										
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)										
Firewalls - Host Based										
Firewalls - Network Appliance										
Firewalls - Cloud										
Firewalls - Virtualized										
Web Application Firewalls										
End Point Detection & Response (EDR)										
Deep Packet Inspection (DPI) Appliance										
Security Information and Event Management (SIEM)										
Web Proxies/Content Filtering										
Other [Define in Comment Box]										
C. Intrusion Detection/Prevention Systems										
Host Intrusion Detection (HIDS)										
Network Intrusion Detection Systems (NIDS)										
Host Intrusion Prevention Systems (HIPS)										
Network Intrusion Prevention Systems (NIPS)										
Unified Threat Management (UTM) Systems										
Honeypot										
Network Tier PII Solutions										
Data Loss Prevention (DLP)										
Data Recovery										
Other [Define in Comment Box]										
D. Network Systems										
Virtual Private Network (VPN)										
Virtual Private Server (VPS)										
Virtualization Software - Bare Metal Hypervisor										
Virtualization Software - Work Station-Based Hypervisor										
Software Defined Networking (SDN) solutions										
Other [Define in Comment Box]										
E. Other Products										
Industrial Control Systems - Networked										
Supervisory Control and Data Acquisition (SCADA)-Networked										
Computer Operating Systems										
Computer Firmware										
Systems-On-Chip, Microcontroller Devices										
Memory and Data Storage Devices										
Mobile Device Operating Systems										
Multi-Function Devices - Printers-Copiers-Scanners										
Networked Printers										
Networked Scanners										
Health Management Systems - Network Connected										
Health Systems/Devices - Network Connected										
Physical Access Control Systems - Network Connected										
Physical Security Video Monitoring Systems - Network Connected										
Telepresence Systems (Audio & Video Conferencing Systems)										
Other [Define in Comment Box]										
Comments:										

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 3.b - Integration/Embedding of Kaspersky Software into Domestic Manufacturers Information Technology Software Products

Instruction: For each type of information technology software product identified on the previous page as incorporating or otherwise containing any Kaspersky software technologies:
 1) Provide Kaspersky product model (Autopopulated)
 2) State the functions and capabilities of the Kaspersky software
 3) Specify the methods used for integrating Kaspersky technologies into your organization's products. [Respond to all category blocks]
 [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]
 Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right --> -->

	#1 Your Organization's Product Model/Series Number	Description of Functions/Capabilities of Kaspersky Software Integrated into Your Organization's Software Products	Description of Methods for Integrating Kaspersky Software into Your Organization's Software Products	Comments
	#2 Your Organization's Product Model/Series Number	Description of Functions/Capabilities of Kaspersky Software Integrated into Your Organization's Software Products	Description of Methods for Integrating Kaspersky Software into Your Organization's Software Products	Comments
A. Network Infrastructure Devices				
Routers - Home Office/Small Office				
Routers - Enterprise/Internet Service Provider Grade				
Switches - Home Office/Small Office				
Switches - Enterprise/Internet Service Provider Grade				
Gateways - Home Office/Small Office (not including switches/routers)				
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)				
Gateways - Cloud (not including switches/routers)				
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)				
Gateways - Mobile Secure Gateways (not including switches/routers)				
Gateways - Other (not including switches/routers)				
Other [Define in Comment Box]				
B. Network Security Devices				
Antivirus Scanning Application - Host Based				
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)				
Firewalls - Host Based				
Firewalls - Network Appliance				
Firewalls - Cloud				
Firewalls - Virtualized				
Web Application Firewalls				
End Point Detection & Response (EDR)				
Deep Packet Inspection (DPI) Appliance				
Security Information and Event Management (SIEM)				
Web Proxy/Content Filtering				
Other [Define in Comment Box]				
C. Intrusion Detection/Prevention Systems				
Host Intrusion Detection (HIDS)				
Network Intrusion Detection Systems (NIDS)				
Host Intrusion Prevention Systems (HIPS)				
Network Intrusion Prevention Systems (NIPS)				
Unified Threat Management (UTM) Systems				
Honeypot				
Network Tar Pit Solutions				
Data Loss Prevention (DLP)				
Data Recovery				
Other [Define in Comment Box]				
D. Network Systems				
Virtual Private Network (VPN)				
Virtual Private Server (VPS)				
Virtualization Software - Bare Metal Hypervisor				
Virtualization Software - Work Station-Based Hypervisor				
Software Defined Networking (SDN) solutions				
Other [Define in Comment Box]				
E. Other Products				
Industrial Control Systems - Networked				
Supervisory Control and Data Acquisition (SCADA)-Networked				
Computer Operating Systems				
Computer Firmware				
Systems-On-Chip, Microcontroller Devices				
Memory and Data Storage Devices				
Mobile Device Operating Systems				
Multi-Function Devices - Printers-Copiers-Scanners				
Networked Printers				
Networked Scanners				
Health Management Systems - Network Connected				
Health Systems/Devices - Network Connected				
Physical Access Control Systems - Network Connected				
Physical Security Video Monitoring Systems - Network Connected				
Telepresence Systems (Audio & Video Conferencing Systems)				
Other [Define in Comment Box]				
Comments:				

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 3.c - Integration/Embedding of Kaspersky Software into Manufacturers' Information Technology Software Products

Previous Page Next Page

Instruction: For the types of information network software products identified on the previous page as incorporating or otherwise containing embedded Kaspersky software technologies, provide:

- 1) Applicable model numbers (Autopopulate);
- 2) Associated application program interfaces (APIs); and
- 3) The method for signing software publication certificates associated with Kaspersky technologies being integrated into your organization's products. [Respond to all category blocks]

["Note: Respond to 'Gateway' categories only where your organization designs, manufactures, markets or distributes specific products specified as 'Gateways.' Do not report as 'Gateways' in the response section routers/switches that also act as gateways.]

Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right --> --> -->

Software Products Sold By Your Organization that Contain Kaspersky Technology	#1 Your Organization's Product Model/Series Number	Associated Application Program Interfaces (APIs)										Method for Signing Software Publication Certificate	Comments	#2 Your Organization's Product Model/Series Number	Associated Application Program Interfaces (APIs)										Method for Signing Software Publication Certificate	Comments			
		Development - Pipeline	Production - Pipeline	Testing - Pipeline	Representational State Transfer (REST)	Shared Memory	Simple Object Access Protocol	Available	Data Exchange Interface (DXI)	Other (Use Comment Box)	Private Key				Co-Signed/Private Key	Shared Key	Not Signed	None	Other (Use Comment Box)	Development - Pipeline	Production - Pipeline	Testing - Pipeline	Representational State Transfer (REST)	Shared Memory			Simple Object Access Protocol	Available	Data Exchange Interface (DXI)
A. Network Infrastructure Devices																													
Routers - Home Office/Small Office																													
Routers - Enterprise/Internet Service Provider Grade																													
Switches - Home Office/Small Office																													
Switches - Enterprise/Internet Service Provider Grade																													
Gateways - Home Office/Small Office (not including switches/routers)																													
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																													
Gateways - Cloud (not including switches/routers)																													
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																													
Gateways - Mobile Secure Gateways (not including switches/routers)																													
Gateways - Other (not including switches/routers)																													
Other [Define in Comment Box]																													
B. Network Security Devices																													
Antivirus Scanning Application - Host Based																													
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																													
Firewalls - Host Based																													
Firewalls - Network Appliance																													
Firewalls - Cloud																													
Firewalls - Virtualized																													
Web Application Firewalls																													
End Point Detection & Response (EDR)																													
Deep Packet Inspection (DPI) Appliance																													
Security Information and Event Management (SIEM)																													
Web Proxies/Content Filtering																													
Other [Define in Comment Box]																													
C. Intrusion Detection/Prevention Systems																													
Host Intrusion Detection (HIDS)																													
Network Intrusion Detection Systems (NIDS)																													
Host Intrusion Prevention Systems (HIPS)																													
Network Intrusion Prevention Systems (NIPS)																													
Unified Threat Management (UTM) Systems																													
Honeypot																													
Network Tar Pit Solutions																													
Data Loss Prevention (DLP)																													
Data Recovery																													
Other [Define in Comment Box]																													
D. Network Systems																													
Virtual Private Network (VPN)																													
Virtual Private Server (VPS)																													
Virtualization Software - Bare Metal Hypervisor																													
Virtualization Software - Work Station-Based Hypervisor																													
Software Defined Networking (SDN) solutions																													
Other [Define in Comment Box]																													
E. Other Products																													
Industrial Control Systems - Networked																													
Supervisory Control and Data Acquisition (SCADA)-Networked																													
Computer Operating Systems																													
Computer Firmware																													
Systems-On-Chip, Microcontroller Devices																													
Memory and Data Storage Devices																													
Mobile Device Operating Systems																													
Multi-Function Devices - Printers-Copiers-Scanners																													
Networked Printers																													
Networked Scanners																													
Health Management Systems - Network Connected																													
Health Systems/Devices - Network Connected																													
Physical Access Control Systems - Network Connected																													
Physical Security Video Monitoring Systems - Network Connected																													
Telepresence Systems (Audio & Video Conferencing Systems)																													
Other [Define in Comment Box]																													
Comments:																													

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Previous Page	Section 3.d - Integration/Embedding of Kaspersky Software into Manufacturers' Information Technology Software Products															Next Page											
<p>For the types information technology software products identified on the previous page as incorporating or otherwise containing embedded Kaspersky software technologies, provide:</p> <p>1) Model numbers (Autopopulated);</p> <p>2) Types of data that can be accessed; [Respond to all category blocks]</p> <p>3) Highest possible levels of system access available to Kaspersky software.</p> <p>[*Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]</p> <p>Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right > -></p>																											
Software Products Sold By Your Organization that Contain Kaspersky Technology	Types of Data That Can Be Accessed							Highest Possible Levels of System Access Available to Kaspersky Software							Comment												
	#1 Your Organization's Product Series/Model Number	System Configuration	Proprietary Business Data	Application Data	Customization Data	Other (Use Comment Box)	System Data	Application Data	User Data	Non-Root Access	Root-Level Access	System Kernel	Other (Use Comment Box)	#2 Your Organization's Product Series/Model Number		System Configuration	Proprietary Business Data	Application Data	Customization Data	Other (Use Comment Box)	System Data	Application Data	User Data	Non-Root Access	Root-Level Access	System Kernel	Other (Use Comment Box)
A. Network Infrastructure Devices																											
Routers - Home Office/Small Office																											
Routers - Enterprise/Internet Service Provider Grade																											
Switches - Home Office/Small Office																											
Switches - Enterprise/Internet Service Provider Grade																											
Gateways - Home Office/Small Office (not including switches/routers)																											
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																											
Gateways - Cloud (not including switches/routers)																											
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																											
Gateways - Mobile Secure Gateways (not including switches/routers)																											
Gateways - Other (not including switches/routers)																											
Other [Define in Comment Box]																											
B. Network Security Devices																											
Antivirus Scanning Application - Host Based																											
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																											
Firewalls - Host Based																											
Firewalls - Network Appliance																											
Firewalls - Cloud																											
Firewalls - Virtualized																											
Web Application Firewalls																											
End Point Detection & Response (EDR)																											
Deep Packet Inspection (DPI) Appliance																											
Security Information and Event Management (SIEM)																											
Web Proxies/Content Filtering																											
Other [Define in Comment Box]																											
C. Intrusion Detection/Prevention Systems																											
Host Intrusion Detection (HIDS)																											
Network Intrusion Detection Systems (NIDS)																											
Host Intrusion Prevention Systems (HIPS)																											
Network Intrusion Prevention Systems (NIPS)																											
Unified Threat Management (UTM) Systems																											
Honeypot																											
Network Tar Pit Solutions																											
Data Loss Prevention (DLP)																											
Data Recovery																											
Other [Define in Comment Box]																											
D. Network Systems																											
Virtual Private Network (VPN)																											
Virtual Private Server (VPS)																											
Virtualization Software - Bare Metal Hypervisor																											
Virtualization Software - Work Station-Based Hypervisor																											
Software Defined Networking (SDN) solutions																											
Other [Define in Comment Box]																											
E. Other Products																											
Industrial Control Systems - Networked																											
Supervisory Control and Data Acquisition (SCADA)-Networked																											
Computer Operating Systems																											
Computer Firmware																											
Systems-On-Chip, Microcontroller Devices																											
Memory and Data Storage Devices																											
Mobile Device Operating Systems																											
Multi-Function Devices - Printers-Copiers-Scanners																											
Networked Printers																											
Networked Scanners																											
Health Management Systems - Network Connected																											
Health Systems/Devices - Network Connected																											
Physical Access Control Systems - Network Connected																											
Physical Security Video Monitoring Systems - Network Connected																											
Telepresence Systems (Audio & Video Conferencing Systems)																											
Other [Define in Comment Box]																											

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 3.e Integration/Embedding of Kaspersky Technologies into Manufacturers' Information Technology Software Products - Functional Conditions for Kaspersky Technologies/Limits on Kaspersky in Syst																													
Instruction: 1) Identify the methods by which Kaspersky software in your network software systems can perform its functions; and 2) Specify the measures invoked by your organization to isolate Kaspersky software and services from the rest of the system. [Respond to all category blocks] (Note: Responses to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.) Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right. --->>>																													
Software Products Sold By Your Organization that Contain Kaspersky Technology	Methods by Which Kaspersky Technology Can Perform Its Functions						Measures Invoked to Isolate Kaspersky Software & Services from Rest of System				Methods by Which Kaspersky Technology Can Perform Its Functions						Measures Invoked to Isolate Kaspersky Software & Services from Rest of System												
	#1 Your Organization's Product Model/Series Number	Internet Access	Operating System Policy Limits	User Applications	System Services	Non-system Level Privileges	Other (Use Comment Box)	Blocked Functions	Code Modification	Privilege Level Limitations	Memory Management	Library Configuration	CPU Demand Limits	Other (Use Comment Box)	Comments	#2 Your Organization's Product Model/Series Number	Internet Access	Operating System Policy Limits	User Applications	System Services	Non-system Level Privileges	Other (Use Comment Box)	Blocked Functions	Code Modification	Privilege Level Limitations	Memory Management	Library Configuration	CPU Demand Limits	Other (Use Comment Box)
A. Network Infrastructure Devices																													
Routers - Home Office/Small Office																													
Routers - Enterprise/Internet Service Provider Grade																													
Switches - Home Office/Small Office																													
Switches - Enterprise/Internet Service Provider Grade																													
Gateways - Home Office/Small Office (not including switches/routers)																													
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																													
Gateways - Cloud (not including switches/routers)																													
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																													
Gateways - Mobile Secure Gateways (not including switches/routers)																													
Gateways - Other (not including switches/routers)																													
Other (Define in Comment Box)																													
B. Network Security Devices																													
Antivirus Scanning Application - Host Based																													
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																													
Firewalls - Host Based																													
Firewalls - Network Appliance																													
Firewalls - Cloud																													
Firewalls - Virtualized																													
Web Application Firewalls																													
End Point Detection & Response (EDR)																													
Deep Packet Inspection (DPI) Appliance																													
Security Information and Event Management (SIEM)																													
Web Proxies/Content Filtering																													
Other (Define in Comment Box)																													
C. Intrusion Detection/Prevention Systems																													
Host Intrusion Detection (HIDS)																													
Network Intrusion Detection Systems (NIDS)																													
Host Intrusion Prevention Systems (HIPS)																													
Network Intrusion Prevention Systems (NIPS)																													
Unified Threat Management (UTM) Systems																													
Honeypot																													
Network Tar Pit Solutions																													
Data Loss Prevention (DLP)																													
Data Recovery																													
Other (Define in Comment Box)																													
D. Network Systems																													
Virtual Private Network (VPN)																													
Virtual Private Server (VPS)																													
Virtualization Software - Bare Metal Hypervisor																													
Virtualization Software - Work Station-Based Hypervisor																													
Software Defined Networking (SDN) solutions																													
Other (Define in Comment Box)																													
E. Other Products																													
Industrial Control Systems - Networked																													
Supervisory Control and Data Acquisition (SCADA)-Networked																													
Computer Operating Systems																													
Computer Firmware																													
Systems-On-Chip, Microcontroller Devices																													
Memory and Data Storage Devices																													
Mobile Device Operating Systems																													
Multi-Function Devices - Printers-Copiers-Scanners																													
Networked Printers																													
Networked Scanners																													
Health Management Systems - Network Connected																													
Health Systems/Devices - Network Connected																													
Physical Access Control Systems - Network Connected																													
Physical Security Video Monitoring Systems - Network Connected																													
Telepresence Systems (Audio & Video Conferencing Systems)																													
Other (Define in Comment Box)																													

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Yes
No
Not Applicable
(Options for all drop-downs on this Tab)

Section 3.f - Integration of Kaspersky Software & Services in Software Systems - Product Design, Service and Upgrade Practices									
Instruction: For the information technology software products containing Kaspersky technologies that your organization sells: 1) Indicate whether your organization's software products are designed internally by company staff, externally by contractors, or by both company employees and external contractors; 2) State whether your organization formally designates third-party companies as "Manufacturer Authorized" to service and upgrade the products sold by your organization. [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways.] Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right-->									
Integration of Kaspersky Software, Hardware, & Services in Software Systems - Product Design, Service and Upgrade Practices									
Software Products Sold By Your Organization that Contain Kaspersky Technology	#1 Your Organization's Product Series/Model Number	Was this product designed internally or externally?	Do you formally designate third-party companies as "Manufacturer Authorized" to service and upgrade this product?	Comments	#2 Your Organization's Product Series/Model Number	Was this product designed internally or externally?	Do you formally designate third-party companies as "Manufacturer Authorized" to service and upgrade this product?	Comments	
A. Network Infrastructure Devices									
Routers - Home Office/Small Office									
Routers - Enterprise/Internet Service Provider Grade									
Switches - Home Office/Small Office									
Switches - Enterprise/Internet Service Provider Grade									
Gateways - Home Office/Small Office (not including switches/routers)									
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)									
Gateways - Cloud (not including switches/routers)									
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)									
Gateways - Mobile Secure Gateways (not including switches/routers)									
Gateways - Other (not including switches/routers)									
Other [Define in Comment Box]									
		↑	↑			↑	↑		
	Internal External Both		Yes No		Internal External Both		Yes No		
B. Network Security Devices									
Antivirus Scanning Application - Host Based									
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)									
Firewalls - Host Based									
Firewalls - Network Appliance									
Firewalls - Cloud									
Firewalls - Virtualized									
Web Application Firewalls									
End Point Detection & Response (EDR)									
Deep Packet Inspection (DPI) Appliance									
Security Information and Event Management (SIEM)									
Web Proxies/Content Filtering									
Other [Define in Comment Box]									
C. Intrusion Detection/Prevention Systems									
Host Intrusion Detection (HIDS)									
Network Intrusion Detection Systems (NIDS)									
Host Intrusion Prevention Systems (HIPS)									
Network Intrusion Prevention Systems (NIPS)									
Unified Threat Management (UTM) Systems									
Honeypot									
Network Tar Pit Solutions									
Data Loss Prevention (DLP)									
Data Recovery									
Other [Define in Comment Box]									
D. Network Systems									
Virtual Private Network (VPN)									
Virtual Private Server (VPS)									
Virtualization Software - Bare Metal Hypervisor									
Virtualization Software - Work Station-Based Hypervisor									
Software Defined Networking (SDN) solutions									
Other [Define in Comment Box]									
E. Other Products									
Industrial Control Systems - Networked									
Supervisory Control and Data Acquisition (SCADA)-Networked									
Computer Operating Systems									
Computer Firmware									
Systems-On-Chip, Microcontroller Devices									
Memory and Data Storage Devices									
Mobile Device Operating Systems									
Multi-Function Devices - Printers-Copiers-Scanners									
Networked Printers									
Networked Scanners									
Health Management Systems - Network Connected									
Health Systems/Devices - Network Connected									
Physical Access Control Systems - Network Connected									
Physical Security Video Monitoring Systems - Network Connected									
Telepresence Systems (Audio & Video Conferencing Systems)									
Other [Define in Comment Box]									

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 4.a - Integration/Embedding of Kaspersky Technologies into Manufacturers Information Technology Hardware - Telemetry I: Direct Comm, Types of Comm										
Types of Devices that Communicate With Kaspersky	#1 Your Company's Product Series/Model Number (autofilled from Section 2a)	Communicates with Kaspersky Connected Systems	Types of Communications Received/Sent	Types of Associated Communications Detection Events/Alert Events	Comments	#2 Your Company's Product Series/Model Number	Communicates with Kaspersky Connected Systems	Types of Communications Received/Sent	Types of Associated Communications Detection Events/Alert Events	Comments
		Kaspersky Security Network Kaspersky Infrastructure Kaspersky Affiliate Other (Comment Box)	No Kaspersky Telemetry Alert (SNMP, Syslog, etc.) Bug Fix Reports System Operations Remote Command/Control System Performance Data System Updates User Data Unknown/Encrypted Detection Events, No Sample Intake Sample Intake Sample Correlate Cloud Scanning Cloud Scanning - Sample Correlate Cloud Scanning - Sample Consent No User Data Other Alert, User Data Proxy Events	Kaspersky Security Network Kaspersky Infrastructure Kaspersky Affiliate Other (User Comment Box) No Kaspersky Telemetry			Alerts Bug Fix Reports System Operations Remote Command/Control System Performance Data System Updates User Data Unknown/Encrypted Detection Events, No Sample Intake Detection Events, Sample Correlate Sample Correlate Sample Intake Cloud Scanning - Sample Cloud Scanning - No User Data Other Alert, Proxy Events			
A. Network Infrastructure Devices										
Routers - Home Office/Small Office										
Routers - Enterprise/Internet Service Provider Grade										
Switches - Home Office/Small Office										
Switches - Enterprise/Internet Service Provider Grade										
Gateways - Home Office/Small Office (not including switches/routers)										
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)										
Gateways - Cloud (not including switches/routers)										
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)										
Gateways - Mobile Secure Gateways (not including switches/routers)										
Gateways - Other (not including switches/routers)										
Other [Define in Comment Box]										
B. Network Security Devices										
Antivirus Scanning Application - Host Based										
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)										
Firewalls - Host Based										
Firewalls - Network Appliance										
Firewalls - Cloud										
Firewalls - Virtualized										
Web Application Firewalls										
End Point Detection & Response (EDR)										
Deep Packet Inspection (DPI) Appliance										
Security Information and Event Management (SIEM)										
Web Proxies/Content Filtering										
Other [Define in Comment Box]										
C. Intrusion Detection/Prevention Systems										
Host Intrusion Detection (HIDS)										
Network Intrusion Detection Systems (NIDS)										
Host Intrusion Prevention Systems (HIPS)										
Network Intrusion Prevention Systems (NIPS)										
Unified Threat Management (UTM) Systems										
Honeypot										
Network Tap Pit Solutions										
Data Loss Prevention (DLP)										
Data Recovery										
Other [Define in Comment Box]										
D. Network Systems										
Virtual Private Network (VPN)										
Virtual Private Server (VPS)										
Virtualization Software - Bare Metal Hypervisor										
Virtualization Software - Work Station Based Hypervisor										
Software Defined Networking (SDN) solutions										
Other [Define in Comment Box]										
E. Other Products										
Industrial Control Systems - Networked										
Supervisory Control and Data Acquisition (SCADA)-Networked										
Computer Operating Systems										
Computer Firmware										
Systems-On-Chip, Microcontroller Devices										
Memory and Data Storage Devices										
Mobile Device Operating Systems										
Multi-Function Devices - Printers-Copiers-Scanners										
Networked Printers										
Networked Scanners										
Health Management Systems - Network Connected										
Health Systems/Devices - Network Connected										
Physical Access Control Systems - Network Connected										
Physical Security Video Monitoring Systems - Network Connected										
Telepresence Systems (Audio & Video Conferencing Systems)										
Other [Define in Comment Box]										

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 4.b - Integration/Embedding of Kaspersky Technologies into Manufacturers Information Technology Hardware - Telemetry 2: Receiving Methods, Returning Info

[Previous Page](#) [Next Page](#)

Instruction: For the hardware products reported in Section 4.a as utilizing Kaspersky software or associated Kaspersky services that allow your organization's products to commun with the Kaspersky Security Network, Other Kaspersky infrastructure, or Third-Parties with known supporting-contract relationships with Kaspersky - identify the:

1) Methods used for Receiving Updates, Signatures, Instructions;
 2) Modes used for Returning Information Directly Back to Kaspersky.

If your response is "unknown", select Yes for "Other" and explain in the comment box at right why your organization does not know this information.
 [Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]

Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right → →

Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Methods for Receiving/Modes for Returning Information												
Types of Devices that Communicate	Methods for Receiving Updates, Signatures, Instructions					Comments	Methods for Receiving Updates, Signatures, Instructions					Comments
	#1 Your Organization's Product Series/Model Number	Direct Connection to Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)	Connection to Self-Hosted Aggregator (FTP Other (describe in Comment Box)		#2 Your Organization's Product Series/Model Number	Direct Connection to Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)	Connection to Self-Hosted Aggregator	
A. Network Infrastructure Devices												
Routers - Home Office/Small Office												
Routers - Enterprise/Internet Service Provider Grade												
Switches - Home Office/Small Office												
Switches - Enterprise/Internet Service Provider Grade												
Gateways - Home Office/Small Office (not including switches/routers)												
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)												
Gateways - Cloud (not including switches/routers)												
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)												
Gateways - Mobile Secure Gateways (not including switches/routers)												
Gateways - Other (not including switches/routers)												
Other [Define in Comment Box]												
B. Network Security Devices												
Antivirus Scanning Application - Host Based												
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
End Point Detection & Response (EDR)												
Deep Packet Inspection (DPI) Appliance												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
Other [Define in Comment Box]												
C. Intrusion Detection/Prevention Systems												
Host Intrusion Detection (HIDS)												
Network Intrusion Detection Systems (NIDS)												
Host Intrusion Prevention Systems (HIPS)												
Network Intrusion Prevention Systems (NIPS)												
Unified Threat Management (UTM) Systems												
Honeypot												
Network Tar Pit Solutions												
Data Loss Prevention (DLP)												
Data Recovery												
Other [Define in Comment Box]												
D. Network Systems												
Virtual Private Network (VPN)												
Virtual Private Server (VPS)												
Virtualization Software - Bare Metal Hypervisor												
Virtualization Software - Work Station-Based Hypervisor												
Software Defined Networking (SDN) solutions												
Other [Define in Comment Box]												
E. Other Products												
Industrial Control Systems - Networked												
Supervisory Control and Data Acquisition (SCADA)-Networked												
Computer Operating Systems												
Computer Firmware												
Systems-On-Chip, Microcontroller Devices												
Memory and Data Storage Devices												
Mobile Device Operating Systems												
Multi-Function Devices - Printers-Copiers-Scanners												
Networked Printers												
Networked Scanners												
Health Management Systems - Network Connected												
Health Systems/Devices - Network Connected												
Physical Access Control Systems - Network Connected												
Physical Security Video Monitoring Systems - Network Connected												
Telepresence Systems (Audio & Video Conferencing Systems)												
Other [Define in Comment Box]												

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

Instruction: For the hardware products reported in Section 4.a as utilizing Kaspersky software or associated Kaspersky services that allow your organization's products to communicate with the Kaspersky Security Network, Other Kaspersky Company infrastructure, or Third-Parties with known supporting or contract relationships with Kaspersky - identify the:
1) Indicators for Passively Detecting Kaspersky in Hardware Products;
2) Report All Indicators Associated with Communications with Kaspersky.
[Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways.]
Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right -- -->

Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Passive Detection in Hardware/Communications Indicators																													
Types of Devices that Communicate Directly	Indicators for Passively Detecting Kaspersky in Hardware Products										Report All Indicators Associated With Communications With Kaspersky		Indicators for Passively Detecting Kaspersky in Hardware Products						Report All Indicators Associated With Communications With Kaspersky				Comments						
	#1 Your Organization's Product Series/Model Number	Updates	Signature	Instructions	Added Services/ Functionality	Hash Changes	Increased Memory Use	Registry Entries	Other (Use Comment Box)	Internet Protocol Addresses	Domains	Unique Indicators	Other (Use Comment Box)	Comments	#2 Your Organization's Product Series/Model Number	Updates	Signature	Instructions	Added Services/ Functionality	Hash Changes	Increased Memory Use	Process Identification		Registry Entries	Other (Use Comment Box)	Internet Protocol Addresses	Email Addresses	Domains	Unique Indicators
A. Network Infrastructure Devices																													
Routers - Home Office/Small Office																													
Routers - Enterprise/Internet Service Provider Grade																													
Switches - Home Office/Small Office																													
Switches - Enterprise/Internet Service Provider Grade																													
Gateways - Home Office/Small Office (not including switches/routers)																													
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																													
Gateways - Cloud (not including switches/routers)																													
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																													
Gateways - Mobile Secure Gateways (not including switches/routers)																													
Gateways - Other (not including switches/routers)																													
Other (Define in Comment Box)																													
B. Network Security Devices																													
Antivirus Scanning Application - Host Based																													
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																													
Firewalls - Host Based																													
Firewalls - Network Appliance																													
Firewalls - Cloud																													
Firewalls - Virtualized																													
Web Application Firewalls																													
End Point Detection & Response (EDR)																													
Deep Packet Inspection (DPI) Appliance																													
Security Information and Event Management (SIEM)																													
Web Proxies/Content Filtering																													
Other (Define in Comment Box)																													
C. Intrusion Detection/Prevention Systems																													
Host Intrusion Detection (HIDS)																													
Network Intrusion Detection Systems (NIDS)																													
Host Intrusion Prevention Systems (HIPS)																													
Network Intrusion Prevention Systems (NIPS)																													
Unified Threat Management (UTM) Systems																													
Honeycot																													
Network Tar Pit Solutions																													
Data Loss Prevention (DLP)																													
Data Recovery																													
Other (Define in Comment Box)																													
D. Network Systems																													
Virtual Private Network (VPN)																													
Virtual Private Server (VPS)																													
Virtualization Software - Bare Metal Hypervisor																													
Virtualization Software - Work Station-Based Hypervisor																													
Software Defined Networking (SDN) solutions																													
Other (Define in Comment Box)																													
E. Other Products																													
Industrial Control Systems - Networked																													
Supervisory Control and Data Acquisition (SCADA)-Networked																													
Computer Operating Systems																													
Computer Firmware																													
Systems-On-Chip, Microcontroller Devices																													
Memory and Data Storage Devices																													
Mobile Device Operating Systems																													
Multi-Function Devices - Printers-Copiers-Scanners																													
Networked Printers																													
Networked Scanners																													
Health Management Systems - Network Connected																													
Health Systems/Devices - Network Connected																													
Physical Access Control Systems - Network Connected																													
Physical Security Video Monitoring Systems - Network Connected																													
Telepresence Systems (Audio & Video Conferencing Systems)																													
Other (Define in Comment Box)																													

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

Section 5a - Integration/Embedding of Kaspersky Technologies Into Manufacturers Information Technology Software - Telemetry I: Direct Comm. Types of Communications										
Instruction: 1) Identify the software products designed, manufactured, marketed or distributed by your company that incorporate Kaspersky software or associated Kaspersky services that allow your organization's products to communicate with the Kaspersky security network, Kaspersky infrastructure, and Kaspersky affiliates. 2) Specify the types of communications that your organization's software products send or receive to/from Kaspersky networks. 3) State the types of communications/alert events that are associated with the software products marketed by your organization that incorporate Kaspersky software. *Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways". Do not report as "Gateways" in the response section routers/switches that also act as gateways.) Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right - - -										
Types of Devices that Communicate With Kaspersky	#1 Your Company's Product Series/Model Number (utilized from Section 3a)	Communicates with Kaspersky Connected Systems	Types of Communications Received/Sent	Types of Associated Communications Detection Events/Alert Events	Comments	#2 Your Company's Product Series/Model Number	Communicates with Kaspersky Connected Systems	Types of Communications Received/Sent	Types of Associated Communications Detection Events/Alert Events	Comments
A. Network Infrastructure Devices Routers - Home Office/Small Office Routers - Enterprise/Internet Service Provider Grade Switches - Home Office/Small Office Switches - Enterprise/Internet Service Provider Grade Gateways - Home Office/Small Office (not including switches/routers) Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers) Gateways - Cloud (not including switches/routers) Gateways - Modular Internet-of-Things (IoT) (not including switches/routers) Gateways - Mobile Secure Gateways (not including switches/routers) Gateways - Other (not including switches/routers) Other (Define in Comment Box)										
B. Network Security Devices Antivirus Scanning Application - Host Based Antivirus Scanning Appliances - Enclave Boundary (Gateway-based) Firewalls - Host Based Firewalls - Network Appliance Firewalls - Cloud Firewalls - Virtualized Web Application Firewalls End Point Detection & Response (EDR) Deep Packet Inspection (DPI) Appliance Security Information and Event Management (SIEM) Web Proxy/Content Filtering Other (Define in Comment Box)										
C. Intrusion Detection/Prevention Systems Host Intrusion Detection (HIDS) Network Intrusion Detection Systems (NIDS) Host Intrusion Prevention Systems (HIPS) Network Intrusion Prevention Systems (NIPS) Unified Threat Management (UTM) Systems Honeypot Network Tar Pit Solutions Data Loss Prevention (DLP) Data Recovery Other (Define in Comment Box)										
D. Network Systems Virtual Private Network (VPN) Virtual Private Server (VPS) Virtualization Software - Bare Metal Hypervisor Virtualization Software - Work Station-Based Hypervisor Software Defined Networking (SDN) solutions Other (Define in Comment Box)										
E. Other Products Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked Computer Operating Systems Computer Firmware Systems On-Chip, Microcontroller Devices Memory and Data Storage Devices Mobile Device Operating Systems Multi-Function Devices - Printers/Copiers-Scanners Networked Printers Networked Scanners Health Management Systems - Network Connected Health Systems/Devices - Network Connected Physical Access Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Other (Define in Comment Box)										

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

Section 5.b - Integration/Embedding of Kaspersky Technologies into Manufacturers Information Technology Software - Telemetry 2: Receiving Methods, Returning Information

Instruction: For the software products reported in Section 5.a as utilizing Kaspersky software or associated Kaspersky services that allow your organization's products to communicate with the Kaspersky Security Network, Other Kaspersky company infrastructure, or Third-Parties with known supporting-contract relationships with Kaspersky - identify the:

1) Methods used for Receiving Updates, Signatures, Instructions;
 2) Modes used for Returning Information Directly Back to Kaspersky.

[Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/switches that also act as gateways.]

Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right -->

Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Methods for Receiving/Modes for Returning Information												
Types of Devices that Communicate	Methods for Receiving Updates, Signatures, Instructions				Comments	Methods for Receiving Updates, Signatures, Instructions				Modes for Returning Information Back to Kaspersky		
	#1 Your Organization's Product Series/Model Number	Direct Connection to Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)		#2 Your Organization's Product Series/Model Number	Direct Connection to Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)	Direct Connection to Self-Hosted Mirror	Aggregator	Other (Describe in Comment Box)
A. Network Infrastructure Devices												
Routers - Home Office/Small Office												
Routers - Enterprise/Internet Service Provider Grade												
Switches - Home Office/Small Office												
Switches - Enterprise/Internet Service Provider Grade												
Gateways - Home Office/Small Office (not including switches/routers)												
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)												
Gateways - Cloud (not including switches/routers)												
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)												
Gateways - Mobile Secure Gateways (not including switches/routers)												
Gateways - Other (not including switches/routers)												
Other [Define in Comment Box]												
B. Network Security Devices												
Antivirus Scanning Application - Host Based												
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
End Point Detection & Response (EDR)												
Deep Packet Inspection (DPI) Appliance												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
Other [Define in Comment Box]												
C. Intrusion Detection/Prevention Systems												
Host Intrusion Detection (HIDS)												
Network Intrusion Detection Systems (NIDS)												
Host Intrusion Prevention Systems (HIPS)												
Network Intrusion Prevention Systems (NIPS)												
Unified Threat Management (UTM) Systems												
Honeypot												
Network Tar Pit Solutions												
Data Loss Prevention (DLP)												
Data Recovery												
Other [Define in Comment Box]												
D. Network Systems												
Virtual Private Network (VPN)												
Virtual Private Server (VPS)												
Virtualization Software - Bare Metal Hypervisor												
Virtualization Software - Work Station-Based Hypervisor												
Software Defined Networking (SDN) solutions												
Other [Define in Comment Box]												
E. Other Products												
Industrial Control Systems - Networked												
Supervisory Control and Data Acquisition (SCADA)-Networked												
Computer Operating Systems												
Computer Firmware												
Systems-On-Chip, Microcontroller Devices												
Memory and Data Storage Devices												
Mobile Device Operating Systems												
Multi-Function Devices - Printers-Copiers-Scanners												
Networked Printers												
Networked Scanners												
Health Management Systems - Network Connected												
Health Systems/Devices - Network Connected												
Physical Access Control Systems - Network Connected												
Physical Security Video Monitoring Systems - Network Connected												
Telepresence Systems (Audio & Video Conferencing Systems)												
Other [Define in Comment Box]												

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 5.c - Integration/Embedding of Kaspersky Technologies into Manufacturers Information Technology Software - Telemetry 3: Passive Indicators, All Indicate

Instruction: For the software products reported in Section 5.a as utilizing Kaspersky software or associated Kaspersky services that allow your organization's products to communicate with the Kaspersky Security Network, Other Kaspersky Company infrastructure, or Third-Parties with known supporting or contract relationships with Kaspersky - identify the:
 1) Indicators for Passively Detecting Kaspersky in Software Products.
 2) Report All Indicators Associated with Communications with Kaspersky.
 *Note: Respond to "Gateway" categories only where your organization designs, manufactures, markets or distributes specific products specified as "Gateways." Do not report as "Gateways" in the response section routers/ switches that also act as gateways]
 Enter all additional product names and model numbers. Information on additional product model numbers may be entered in successive form blocks that are reached by scrolling this page to the right -- -- --

Types of Devices that Communicate Directly	Integration of Kaspersky Software, Hardware, & Services in Hardware Systems - Passive Detection in Hardware/Communications Indicators														Comments													
	Indicators for Passively Detecting Kaspersky in Hardware Products							Indicators for Passively Detecting Kaspersky in Hardware Products								Report All Indicators Associated With Communications With												
#1 Your Organization's Product Series/Model Number	Updates	Signature	Instructions	Added Services/Functionality	High Changes	Increased Memory Use	Registry Entries	Other (Use Comment Box)	Internet Protocol Addresses	Domains	Unique Indicators	Other (Use Comment Box)	#2 Your Organization's Product Series/Model Number	Updates	Signature	Instructions	Added Services/Functionality	High Changes	Increased Memory Use	Process Identification	Registry Entries	Other (Use Comment Box)	Internet Protocol Addresses	Email Addresses	Domains	Unique Indicators	Other (Use Comment Box)	Comments
A. Network Infrastructure Devices																												
Routers - Home Office/Small Office																												
Routers - Enterprise/Internet Service Provider Grade																												
Switches - Home Office/Small Office																												
Switches - Enterprise/Internet Service Provider Grade																												
Gateways - Home Office/Small Office (not including switches/routers)																												
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)																												
Gateways - Cloud (not including switches/routers)																												
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)																												
Gateways - Mobile Secure Gateways (not including switches/routers)																												
Gateways - Other (not including switches/routers)																												
Other (Define in Comment Box)																												
B. Network Security Devices																												
Antivirus Scanning Application - Host Based																												
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																												
Firewalls - Host Based																												
Firewalls - Network Appliance																												
Firewalls - Cloud																												
Firewalls - Virtualized																												
Web Application Firewalls																												
End Point Detection & Response (EDR)																												
Deep Packet Inspection (DPI) Appliance																												
Security Information and Event Management (SIEM)																												
Web Proxies/Content Filtering																												
Other (Define in Comment Box)																												
C. Intrusion Detection/Prevention Systems																												
Host Intrusion Detection (HIDS)																												
Network Intrusion Detection Systems (NIDS)																												
Host Intrusion Prevention Systems (HIPS)																												
Network Intrusion Prevention Systems (NIPS)																												
Unified Threat Management (UTM) Systems																												
Honeypot																												
Network Tar Pit Solutions																												
Data Loss Prevention (DLP)																												
Data Recovery																												
Other (Define in Comment Box)																												
D. Network Systems																												
Virtual Private Network (VPN)																												
Virtual Private Server (VPS)																												
Virtualization Software - Bare Metal Hypervisor																												
Virtualization Software - Work Station-Based Hypervisor																												
Software Defined Networking (SDN) solutions																												
Other (Define in Comment Box)																												
E. Other Products																												
Industrial Control Systems - Networked																												
Supervisory Control and Data Acquisition (SCADA)-Networked																												
Computer Operating Systems																												
Computer Firmware																												
Systems-On-Chip, Microcontroller Devices																												
Memory and Data Storage Devices																												
Mobile Device Operating Systems																												
Multi-Function Devices - Printers-Copiers-Scanners																												
Networked Printers																												
Networked Scanners																												
Health Management Systems - Network Connected																												
Health Systems/Devices - Network Connected																												
Physical Access Control Systems - Network Connected																												
Physical Security Video Monitoring Systems - Network Connected																												
Telepresence Systems (Audio & Video Conferencing Systems)																												
Other (Define in Comment Box)																												

Yes
No
(Options for all drop-downs on this Tab)

Yes
No
(Options for all drop-downs on this Tab)

Previous Page	2014 or Earlier 2015 2016 2017 2018 2019 Not Implemented	2014 or Earlier 2015 2016 2017 2018 2019 Not Implemented	2014 or Earlier 2015 2016 2017 2018 2019 Not Implemented	Frequency of List Updates
Instruction: Identify the year that you first began using the product with regard to any products it is used to protect. (Note: Respond to "Gateways" in the response section routers/switches that also act as gateways.)				Weekly Monthly Quarterly Semi-Annually Annually Event-Driven Only None
A. Network Infrastructure Devices				
Routers - Home Office/Small Office	2014 or Earlier	2014 or Earlier	2014 or Earlier	
Routers - Enterprise/Internet Service Provider Grade	2015	2015	2015	
Switches - Home Office/Small Office	2016	2016	2016	
Switches - Enterprise/Internet Service Provider Grade	2017	2017	2017	
Gateways - Home Office/Small Office (not including switches/routers)	2018	2018	2018	
Gateways - Enterprise/Internet Service Provider Grade (not including switches/routers)	2019	2019	2019	
Gateways - Cloud (not including switches/routers)	Not Implemented	Not Implemented	Not Implemented	
Gateways - Modular Internet-of-Things (IoT) (not including switches/routers)				
Gateways - Mobile Secure Gateways (not including switches/routers)				
Gateways - Other (not including switches/routers)				
Other (Define in Comment Box)				
B. Network Security Devices				
Antivirus Scanning Application - Host Based	2014 or Earlier	2014 or Earlier	2014 or Earlier	
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)	2015	2015	2015	
Firewalls - Host Based	2016	2016	2016	
Firewalls - Network Appliance	2017	2017	2017	
Firewalls - Cloud	2018	2018	2018	
Firewalls - Virtualized	2019	2019	2019	
Web Application Firewalls	Not Implemented	Not Implemented	Not Implemented	
End Point Detection & Response (EDR)				
Deep Packet Inspection (DPI) Appliance				
Security Information and Event Management (SIEM)				
Web Proxies/Content Filtering				
Other (Define in Comment Box)				
C. Intrusion Detection/Prevention Systems				
Host Intrusion Detection (HIDS)				
Network Intrusion Detection Systems (NIDS)				
Host Intrusion Prevention Systems (HIPS)				
Network Intrusion Prevention Systems (NIPS)				
Unified Threat Management (UTM) Systems				
Honeyypot				
Network Tar Pit Solutions				
Data Loss Prevention (DLP)				
Data Recovery				
Other (Define in Comment Box)				
D. Network Systems				
Virtual Private Network (VPN)				
Virtual Private Server (VPS)				
Virtualization Software - Bare Metal Hypervisor				
Virtualization Software - Work Station-Based Hypervisor				
Software Defined Networking (SDN) solutions				
Other (Define in Comment Box)				
E. Other Products				
Industrial Control Systems - Networked				
Supervisory Control and Data Acquisition (SCADA)-Networked				
Computer Operating Systems				
Computer Firmware				
Systems-On-Chip, Microcontroller Devices				
Memory and Data Storage Devices				
Mobile Device Operating Systems				
Multi-Function Devices - Printers-Copiers-Scanners				
Networked Printers				
Networked Scanners				
Health Management Systems - Network Connected				
Health Systems/Devices - Network Connected				
Physical Access Control Systems - Network Connected				
Physical Security Video Monitoring Systems - Network Connected				
Telepresence Systems (Audio & Video Conferencing Systems)				
Other (Define in Comment Box)				

Section 7.a- Sales, Balance Sheet, and Income Statement			
From 2017-2019, provide your organization's U.S. and non-U.S. sales information.			
Reporting Schedule:		Reporting Level:	
Sales		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12	
		2017	2018
			2019
A.	Total Sales, all Customers U.S./Non-U.S.	Calender Year Fiscal year	Corporate/Whole Organization Division/Business Unit
Provide breakouts of each type of Information Network Hardware, Software, and Services. Page of total sales:			
B.	All Customers		
C.	U.S. Customers		
D.	U.S. Government		
E.	U.S. Department of Defense		
Income Statement (Select Line Items):		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12	
		2017	2018
			2019
A.	Net Sales (and other revenue)		
B.	Cost of Goods Sold		
C.	Total Operating Income (Loss)		
D.	Earnings Before Interest and Taxes		
E.	Net Income		
Balance Sheet (Select Line Items):		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12	
		2017	2018
			2019
A.	Cash		
B.	Inventories		
C.	Current Assets		
D.	Total Assets		
E.	Current Liabilities		
F.	Total Liabilities		
G.	Retained Earnings		
H.	Total Owners Equity		
Kaspersky Specific Items:		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12	
		2017	2018
			2019
A.	Total Revenue (\$\$) Earned from Selling, Incorporating, or Otherwise Promoting Kaspersky Technologies		
B.	Total Costs (\$\$) Associated with Licensing/Use of Kaspersky technologies used in your organization's Hardware and Software Products		
Comments:			

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Yes
No

[Previous Page](#)
[Next Page](#)

Section 7.b- Research & Development and Capital Expenditures

A. Does your organization perform Research and Development (R&D)? If "No", leave part B blank and proceed to part C below.

In Part B, record your organization's total R&D expenditures for 2017-2019.

Research & Development Reporting Schedule:				
Research & Development Reporting Level:				
Research & Development Category		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12		
		2017	2018	2019
1	Total R&D Expenditures			
B.	2 Total Information Network Hardware, Software and Related Product R&D Expenditures	Corporate/Whole Organization		Calendar Year
	3 Basic Research (as a % of B2)	Division/Business Unit		Fiscal Year
	4 Applied Research (as a % of B2)			
	5 Product/Process Development (as a % of B2)			
	Total of 3 - 5 (must equal 100%)		0%	0%

In Part C, report your organization's capital expenditures for 2017-2019. If your organization has no capital expenditures in this period, enter "0" for each year.

Capital Expenditure Reporting Schedule:				
Capital Expenditure Reporting Level:				
Capital Expenditure Category		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12		
		2017	2018	2019
1	Total Capital Expenditures			
C.	2 Total Information and Communications Technology Hardware, Software, and Related Product Capital Expenditures	Corporate/Whole Organization		Calendar Year
	3 Machinery and Equipment (as a % of C2)	Division/Business Unit		Fiscal Year
	4 IT, Computers, and Software (as a % of C2)			
	5 Land, Buildings, and Leasehold Improvements (as a % of C2)			
	6 Other (as a % of C2) (specify here)			
Total of 3 - 6 (must equal 100%)		0%	0%	0%

Comments:

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Section 8 - Cyber Security

Indicate which of the following security measures are in place at this location:

Account Monitoring and Control		Investment in Authorized/Unauthorized Software	
Application Software Security		Limitation of Network Ports and Services	
Boundary Defense		Mail Monitoring, & Analysis of Audit Logs	
Continuous Vulnerability Assessment		Malware Defenses	
A. Controlled Access Based on Need to Know		Penetration Tests and Red Team Exercises	
Controlled Use of Administrative Privileges		Secure Configurations on Hardware	
Data Protection		Secure Configurations of Network Devices	
Data Recovery Capability		Secure Network Engineering	
Incident Response and Management		Security Skills Assessments and Training	
Inventory of Authorized/Unauthorized Devices		Wireless Access Control	
Other (specify here)		Other (specify here)	

Identify any impacts or actions resulting from malicious cyber activity at your location in the past three years:

Impacts Experienced		Actions Undertaken	
IT downtime		Re-evaluation of international partnerships	
Costs from damage assessment/remediation		Significant change in R&D strategy	
Loss of sales/Business interruption		Exit from markets or market segments	
Exfiltration of Commercially Sensitive Information		Exit from product or business line	
Damage to IT infrastructure		Major new investment in cyber security	
Damage to company production capabilities or systems		Other (specify here)	
Theft of software and/or source code		Other (specify here)	
Other (specify here)		Other (specify here)	

Does your organization have defined, written protocols in place for responding to a cyber security breach?

Explain:

Is your organization able to detect the theft of, or unauthorized access to, Commercially Sensitive Information?

Does your organization have a supply chain risk management (SCRM) program in place?

How many days on average does it take for your organization to implement a software patch across all your networked systems?

If an event occurred that resulted in the loss of access to a significant portion of your organization's data, how long do you estimate it would take to restore full functionality from system backups?

Explain:

Indicate if your organization routinely encrypts sensitive data in each of the following:

Yes	No	Yes	No
(at rest)		Transmitted internally	Transmitted externally

Does your organization restrict or prohibit external data/cloud storage provider(s) from storing commercially sensitive information outside of the U.S.?

Is your organization aware of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information?
<http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>

Comments:

The U.S. Government encourages the reporting of suspected or confirmed cybersecurity incidents to the Federal Bureau of Investigation (FBI) or the Cyber Security and Infrastructure Agency (CISA). Local FBI field offices can be identified at <http://www.fbi.gov/contact-us/field>; the FBI's 24/7 Cyber Watch (CyWatch) can be contacted by phone at 855-292-3937, or by email at CyWatch@ic.fbi.gov; and cybersecurity incidents and vulnerabilities can be reported to CISA at <https://www.us-cert.gov/report>. No-cost technical assistance can be requested from CISA using the same website address.

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Yes
No

Yes
No

Yes
No

Yes
No

Always
Sometimes
Never

Yes
No

Yes
No

Section 9: Challenges and Outreach

Identify the issues that have impacted your location in the past three years. For each issue, indicate Yes/No. Then, rank your location's top five issues (1 being the most important issue; 2 being the next most important issue, etc.) and explain the affirmative issues where examples and narrative will aid the U.S. Government's understanding of your concerns.

Type of Issue	A	B	C
	-Yes/No-	Rank Top 5	
Aging equipment, facilities, or infrastructure			
Aging workforce			
Counterfeit parts			
Cyber security			
Domestic competition			
Environmental regulations/remediation			
Export controls/ITAR & EAR			
Financing/credit availability			
Foreign competition			
Government acquisition process			
Government purchasing volatility			
Government regulatory burden			
A. Healthcare			
Industrial espionage - domestic			
Industrial espionage - foreign			
Input availability			
Intellectual property/patent infringement			
Labor availability/costs			
Natural disasters (including disease/quarantine)			
Obsolescence			
Pension costs			
Proximity to customers			
Proximity to suppliers			
Qualifications/certifications			
Quality of inputs			
R&D costs			
Reduction in USG demand			
Taxes			
Trade disputes/tariffs			
Worker/skills retention			
Other (specify here)			

Identify any impacts or actions resulting from the COVID-19 pandemic at your location, ranking the top three most significant impacts and top three most important actions (1 being the most important issue; 2 being the next most important issue, etc.):


Impacts Experienced	-Yes/No-	Rank Top 3	Actions Taken	-Yes/No-	Rank Top 3
Increased cost of materials			Reduce workforce		
Inability to access work location			Increase online/remote work capabilities		
Inability to fulfill contracts			Seek government assistance		
Reduced sales			Delay or reject new contracts		
B. Foreign supplier manufacturing delays			Begin to produce pandemic-related products		
Domestic supplier manufacturing delays			Increase use of domestic suppliers		
Increased demand			Reduce use of suppliers located in China		
Transportation-based disruptions			Reduce use of suppliers located outside the U.S. and China		
Financing difficulties			Increase inventories		
Labor shortages			Increase supplier redundancy		
Other (specify here)			Other (specify here)		

Identify any USG actions that would have best mitigated COVID-19 impacts to this location:

There are many federal and state government programs available to aid your location's competitiveness. If you would like more information regarding such services, select the areas of interest and the Bureau of Industry and Security (BIS) will follow-up accordingly.	
Additive Manufacturing	R&D through Small Business Innovation Research
Business Continuity Plan/Disease Pandemic Relief	Reshoring/Creating Domestic Supply Chains
Cyber Security	Security Clearances and Attaining Cleared Facility Status
C. Export Growth and Impacts	Supply Chain Improvements and Impacts
Export Licensing (ITAR/EAR)	Supply Chain Vulnerability Reporting to USG
Government Procurement Guidelines	Sustainability
Lean and Quality Management	Technology Driven Marketplace Intelligence
New Product Development	Technology Scouting
Pandemic Preparation and/or Response	Workforce/Technical Labor Resources

If needed or appropriate, identify any supply chain vulnerabilities affecting your location that have not been identified elsewhere in this survey:

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Previous Page	Next Page		
Section 10 - Certification			
<p>The undersigned certifies that the information herein supplied in response to this questionnaire is complete and correct to the best of his/her knowledge. It is a criminal offense to willfully make a false statement or representation to any department or agency of the United States Government as to any matter within its jurisdiction (18 U.S.C. §1001).</p> <p>Once this survey is complete submit it via our Census Bureau web portal at https://respond.census.gov/ICTsoftware. Be sure to retain a copy for your records and to facilitate any necessary edits or clarifications.</p>			
Organization Name			
Organization's Internet Address			
Name of Authorizing Official			
Title of Authorizing Official			
E-mail Address			
Phone Number and Extension			
Date Certified			
Is your organization is interested in USG assistance in removing specific software products embedded in your products?	<table border="1"> <tr> <td>Yes</td> </tr> <tr> <td>No</td> </tr> </table> 	Yes	No
Yes			
No			
Provide any additional comments or any other information you wish to include regarding this survey assessment:			
How many hours did it take to complete this survey?			
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act			

Section	Content
Section 1	Section 1: Introduction to the document, detailing the purpose and scope of the report.
Section 2	Section 2: Overview of the project, including key objectives and milestones.
Section 3	Section 3: Detailed description of the methodology used for data collection and analysis.
Section 4	Section 4: Presentation of the results, including tables and charts.
Section 5	Section 5: Discussion of the findings and their implications.
Section 6	Section 6: Conclusion and recommendations for future work.
Section 7	Section 7: Appendix containing supplementary data and references.
Section 8	Section 8: Glossary of terms used throughout the document.
Section 9	Section 9: Acknowledgments to those who assisted in the project.
Section 10	Section 10: Final remarks and contact information for the author.